

Installation Manual

NC-PASS Authenticator
Version 2.0

MVS Operating Environment

© Copyright 2001 PassGo Technologies Ltd. All rights reserved.
Proprietary and Confidential Information of PassGo Technologies Ltd.

Publication number PAI0001.003

Third Edition (October 2001)

Published by:

PassGo Technologies Ltd, Horton Manor, Ilminster, Somerset, TA19 9PY, England.

This book refers to a number of hardware and software products that are produced by other companies. In most, if not all cases, the names of these products are claimed as trademarks by the companies that manufacture them. It is not our intention to claim either the products or their names or trademarks as our own.

Changes will be made periodically to the information contained in this book. If your book does not accurately reflect the level of product you are using, this may be due to a fix being applied to the product which has still to be released as a book update.

Preface

Purpose of this book

This book describes the installation procedures for the startup and running of NC-PASS Authenticator.

The complete range of books associated with NC-PASS Authenticator is as follows:

- NC-PASS Authenticator Installation Manual (this manual)
- NC-PASS Authenticator Administration Manual - Volume 1
- NC-PASS Authenticator Administration Manual - Volume 2
- NC-PASS Authenticator User Guide

For information on NCI language statements, refer to the NCI/XF VTAM Toolkit documentation.

Who should read this book

This book is intended for use by technical staff who are responsible for the installation of NC-PASS Authenticator.

NC-PASS Authenticator installation requirements

Operating system	MVS ESA, MVS XA
Network Software	ACF/VTAM 3.3 and higher
TCP/IP communications (if using)	TCP/IP for MVS version 2.2.1 or above.

National characters

All references to national characters in this book are in English (U.S.) format. The table below shows four commonly-used national characters with their English (U.K.), French and German equivalents:

Hex Value	English (U.S.)	English (U.K.)	French	German
X'4A'	¢	\$	°	Ä
X'5B'	\$	£	\$	\$
X'7B'	#	#	£	#
X'7C'	@	@	à	§

Technical Newsletters included in NC-PASS Authenticator v2.0 books.

The information in the following Technical Newsletters (TNLs), issued since the previous issue of the NC-PASS v2.0 books, is now included in these books:

Technical Newsletter reference number	Title
PA20.TNL001	Restructured menus
PH203.TNL001	Support for the ActivCard token
PH203.TNL002	Support for the Digipass token
PH202.TNL003	The NC-PASS TCP/IP interface
PH203.TNL003	Efficiency improvements
PH203.TNL004	RACF Passticket support
PH202.TNL005	Encryption of transmissions over APPC and TCP/IP
PH202.TNL006	User ID translation
PH202.TNL007	Batch message auditing
PH202.TNL009	The LOAD RESTORE CONTROL TABLES panel
PH202.TNL010	APPC LINK STATUS panel
PH202.TNL011	Additional messages
PH202.TNL012	Home Node Processing via the TLI
PH202.TNL013	Backward compatibility for NC-PASS
PH202.TNL014	Format of NC-PASS WTO messages

Readers' comment forms

Forms for readers' comments are provided at the back of this manual.

Any information you return may be used or distributed by the authors in any manner considered appropriate without incurring any obligation whatsoever.

Table of contents

Preface

Chapter 1 Preparation

Chapter 2 Downloading NC-PASS

Chapter 3 The VTAM environment

Chapter 4 System changes

Chapter 5 Starting NC-PASS

Chapter 6 Post-installation considerations

Chapter 7 Applying fixes and zaps

Chapter 8 Getting started

Index

This page intentionally left blank

Chapter 1 - Preparation

Introduction	1.2
Installation considerations	1.2
Security aspects	1.3
Upgrading and applying maintenance	1.4
Upgrade	1.4
Maintenance	1.4
Providing information for installation	1.5

Introduction

This chapter consists of

- explanatory text
- installation instructions.

Those instructions that are mandatory are highlighted by a diamond (◆) in the left hand margin.

Installation considerations

The NC-PASS product tape is supplied with an Installation Guide which provides the latest information on the supplied system. Any installation information provided by the Installation Guide takes precedence over information in this chapter. The Installation Guide will always reflect the latest information.

The minimum steps you must carry out to install NC-PASS are:

- download the product from tape
- install the NC-PASS libraries
- define a VTAM node on which to run the product.

WARNING: If you are installing NC-PASS in the same MVS system as another PassGo Technologies product (eg NC-ACCESS) and you are using SMP/E, you must use a different CSI dataset for each product.

Additional components

The following table is an installation checklist of the additional NC-PASS components that you may want to use and the tasks that must be carried out if you want to use them:

If you want to...	Then you must...
control which LU to LU sessions VTAM will allow or deny by using the VSSE (SME) component	install the session management exit ITEXCAA. Authorize the load library in APF list or through PPT to enable Cross memory services between NC-PASS and the SME.
enable applications to communicate with NC-PASS via an APPC interface	define a VTAM APPC (LU6.2) node definition.
communicate with other NC-PASS jobs to <ul style="list-style-type: none">• authenticate users cross-domain• propagate SME rules.	define a VTAM MHO (LU0) node definition.
use the TLI function of NC-PASS to enable non-NC-PASS jobs to communicate with NC-PASS	Authorize the load library in APF list or through PPT.
interface with a security product to: <ul style="list-style-type: none">• validate access requests• administer NC-PASS userid data from a RACF database.	Reassemble the security product source member. Define suitable access rights to the NC-PASS datasets. Authorize the load library in APF list or through PPT.

Security aspects

You should be aware that unauthorized use of NC-PASS facilities could cause a breach of system security. Access to NC-PASS as an administrator **MUST** be restricted.

Upgrading and applying maintenance

The procedures that you follow in this manual will differ depending on whether you are upgrading from a previous release or applying maintenance. You can determine which procedures to use by the format of the instructions you are following, as shown below.

Upgrade

If you are upgrading from:

- NC-PASS Authenticator/Secure v1.4
- NC-PASS Authenticator/Secure v1.4 and NC-PASS VSSE v2.0
- NC-PASS VSSE v2.0.

to NC-PASS Authenticator v2.0.4, follow the installation instructions as provided in this manual. Special considerations for upgrade will be highlighted in the text as follows:

UPGRADE

Additional instructions for upgrade.

Maintenance

If you are applying maintenance to NC-PASS Authenticator/Secure v2.0.1, v2.0.2 or v2.0.3 to provide NC-PASS Authenticator/Secure v2.0.4, follow the installation instructions as provided in this manual. Special considerations for maintenance will be highlighted in the text as follows:

MAINTENANCE

Additional instructions for maintenance.

Installing maintenance incorporates changes to PDS libraries and changes to VSAM files. The PANEL, PDLIB and LOAD libraries created have maintenance fixes already applied.

The PDS libraries can be changed in two ways; either create new libraries or copy replace to existing libraries. It is recommended that you create new libraries.

The VSDD VSAM file is deleted and redefined and the latest record definitions copied from tape using REPRO; the VSDD contains no user data.

Ensure backups are available before starting maintenance.

Applying maintenance program fixes using the MP product

If you want to apply PDLIB fixes only, all or selectively, refer to *Chapter 7 - Applying fixes and zaps*.

Providing information for installation

- ◆ Answer the questions below about installation standards, prefixes, volumes and catalogues. These answers will be used throughout the subsequent installation sections.

UPGRADE/MAINTENANCE

if you still have the answers entered into your original install, use these and make changes as required.

The space used when installing NC-PASS on 3380 disk drives is approximately 550 tracks.

- ◆
 1. What is your installation dataset name?
This dataset will contain members required to download the products from tape and is represented by **INSTALL**.

Note: Do **not** use 'CNTL' in the **INSTALL** name as this is used later; for instance use 'CUSTOMER.ACC.INSTALL'.

- ◆
 2. What are the **PREFIX** first and second level qualifiers for your partitioned datasets?

- ◆
 3. What are the **VSAMPFX** first and second level qualifiers for your VSAM datasets?

- ◆
 4. What volume will receive your partitioned datasets **VOLSER**?

- ◆
 5. What volume will receive your VSAM datasets **VSAMVOL**?

- ◆
 6. What volume forms the user catalogue name and is used for your VSAM datasets **CATVOL**? (**CATVOL** represents the last six characters of the catalogue name as follows: CATALOG.MVSICF1.V**CATVOL**)

If aliases are used in your master catalog, this option is not required.

7. **UPGRADE/MAINTENANCE**

What is your current NC-PASS VSAM prefix, **VSMOPFX**?

This page intentionally left blank

Chapter 2 - Downloading NC-PASS

Copying the INSTALL dataset	2.2
Installing NC-PASS libraries	2.3
SMP/E installation jobs	2.3
Installation steps	2.3

Copying the INSTALL dataset

- ◆ Load the NC-PASS Installation Dataset by creating an IEBCOPY job an example of which is shown below. The members of the install dataset are used to download the products from tape and execute NC-PASS.
- ◆ Modify **INSTALL** and **VOLSER** using the replies in *Providing information for installation* on page 1.5.
- ◆ Modify **serial-number** to match the serial number on the tape label.

UPGRADE/MAINTENANCE

- ◆ **Always** copy file 14 from tape (the file containing the JCL required to download the product), because changes to the install members may occur between maintenance tapes

```
//JOB CARD JOB
// EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SYSUT3 DD UNIT=3380, SPACE=(80,(30, 5))
//INDD DD DSN=CK.NCPASS.INSTALL,
// DISP=OLD,
// UNIT=TAPE,
// VOL=SER=*serial-number*,
// LABEL=(14,SL)
//OUTDD DD DSN=*INSTALL*,
// UNIT=DISK,
// DISP=(NEW,CATLG),
// VOL=SER=*VOLSER*,
// SPACE=(TRK,(5,1,10))
//SYSIN DD *
COPY INDD=INDD,OUTDD=OUTDD
```

- ◆ Run the JCL.

Installing NC-PASS libraries

Install the libraries either using SMP/E or directly using the jobs supplied in the **INSTALL** dataset.

If you want to install...	go to the section below entitled....
using SMP/E	<i>SMP/E installation jobs</i>
without using SMP/E	<i>Installation steps</i>

SMP/E installation jobs

MAINTENANCE

SMP/E does not apply to maintenance. Go to the section entitled *Installation steps* below.

WARNING: If you are installing NC-PASS in the same MVS system as another PassGo Technologies product (eg PassGo) and you are using SMP/E, you must use a different CSI dataset for each product.

◆ The following jobs are supplied in the **INSTALL** dataset. **The region size for SMP/E must be 6 MB to run the JCL.** Modify the jobs according to the instructions contained within them:

SESMPA	creates the PDS files for the product
SESMPB	creates PDS and CSI files for SMP/E
SESMPC	loads the CSI dataset with information about NC-PASS
SESM Pins	runs SMP/E receive apply and accept

When these jobs are completed successfully, the NC-PASS partitioned datasets have been downloaded.

◆ When modifying the install JCL member (PASSINST, PASSMNT or PASSMNT2 as appropriate), you must make changes to the IEFBR14 and CPYPASS flags within the member in order to omit the steps already completed by the SMP/E install.

◆ Continue with the section entitled *Installation steps* below.

Installation steps

If JES3, go to *Loading NC-PASS for JES3 only* on page 2.5.

- ◆ 1. Modify member **PASSIAMS** of **INSTALL** dataset by using the replies in *Providing information for installation* on page 1.5. This member is used by the batch job submitted below and defines the following NC-PASS VSAM files:
- the central administration file (CAF)
 - the VSAM data definition file (VSDD)
 - the fix control database used by the maintenance program.

UPGRADE

HELP and MESSAGES are no longer held on the CAF thereby reducing the size of the file. Help text and messages are now held in separate PDS members.

The VSAM sample definition member PASSIAMS defines VSAM clusters with the following share options for security reasons:

SHR(2 3)

If you wish to modify the share options, do so now.

The use of RLS (Record Level Sharing) overrides the share options specified in the VSAM definitions. If you are preparing your NC-PASS system to benefit from the Passplex feature, you need to use RLS with your VSAM files. This is done by specifying RLS=NRI on the VSAM DDs in the JCL to run your NC-PASS job. The combination of Passplex and RLS give near 24x7 availability and improved authentication throughput on Sysplex systems with SMS managed DASD.

UPGRADE

If you are converting from NC-PASS V1.4, replace the references to PASSINST below with **PASSMNT**.

If you are converting from NC-PASS VSSE V2.0, replace the references to PASSINST below with **PASSMNT**.

If you are currently running NC-PASS V1.4 and NC-PASS VSSE V2.0, replace the references to PASSINST below with **PASSMNT2**.

MAINTENANCE

If you are converting from NC-PASS Authenticator/Secure v2.0.1, v 2.0.2 or v2.0.3, replace the references to PASSINST below with **PASSMNT**.

- ◆ 2. Modify member **PASSINST** of **INSTALL** dataset by using the replies in *Providing information for installation* on page 1.5. Follow the instructions within the member.
- ◆ 3. Modify the job card to installation standards.
- ◆ 4. Check the disk and tape parameters, and modify to your installation standards if necessary.
- ◆ 5. Submit the **PASSINST** job and check the output. Successful completion of this job gives you the files required to run NC-PASS.

UPGRADE

If you are converting from NC-PASS v1.4 you will have to redefine the ESDS files used for recording CAF updates. Redefine with **PREFIX*.CNTL(TBACK)*.

Loading NC-PASS for JES3 only

1. Modify member **PASSIAMS** of the **INSTALL** dataset using the replies in *Providing information for installation* on page 1.5. This member is used by the batch job submitted below and defines the following NC-PASS VSAM files:
 - the central administration file (CAF)
 - the VSAM data definition file (VSDD)
 - the fix control database.

UPGRADE

HELP and MESSAGES are no longer held on the CAF thereby reducing the size of the file. Help text and messages are now held in separate PDS members.

2. Modify member **ZJES31** of **INSTALL** by using the replies in *Providing information for installation* on page 1.5.
3. Modify the job card to installation standards.
4. Check the disk and tape parameters.
5. Submit the **ZJES31** job and check the output.

UPGRADE/MAINTENANCE

If you are converting from an earlier version of NC-PASS, or applying maintenance, replace the references to ZJES32 below with **ZJES33**.

6. Modify member **ZJES32** of **INSTALL**.
7. Submit the **ZJES32** job and check the output.

UPGRADE

If you are converting from NC-PASS v1.4 you will have to redefine the ESDS files used for recording CAF updates. Redefine with **PREFIX*.CNTL(TBACK)*.

This page intentionally left blank

Chapter 3 - The VTAM environment

Introduction	3.2
VTAM node and ACB definitions	3.2
The VTAM Session Management Exit	3.4
Activating the exit	3.9
Backing out the exit	3.9

Introduction

Changes to the VTAM environment may be required in the following areas:

- VTAM node and ACB definitions
 - product node (minimum requirement for product installation)
 - MHO node
 - APPC node
 - printer ACB names
- Session Management Exit.

VTAM node and ACB definitions

Review the contents of the SEVTAM member which contains the following node definitions:

Node definition	Name	Required for
NC-PASS	PASS	This is the node to which you connect to logon to NC-PASS. It is the minimum requirement for product installation.
MHO	PASSMHO	Required if your NC-PASS job will communicate with other NC-PASS jobs, running on different MVS or VM systems connected by VTAM. The MHO system uses the IBM protocol LU0. Refer to the NC-PASS Authenticator Administration Manual, Volume 2, <i>Chapter 1 - Communicating with other systems</i> for full details.
APPC	PASSAPPC	Required if your NC-PASS job will communicate with different platforms such as PCs, thereby enabling such users to benefit from the features of NC-PASS. See also <i>APPC requirements</i> on page 3.3. The APPC system uses the IBM protocol LU6.2. Refer to the NC-PASS Authenticator Administration Manual, Volume 2, <i>Chapter 1 - Communicating with other systems</i> for full details.

Some sample printer stub ACBNames are also provided within SEVTAM; if these names are changed, changes will be required in the NC-PASS administration panels. Refer to *VTAM printer definitions* on page 2.10 (Volume 1) of the NC-PASS Authenticator Administration Manual.

UPGRADE

An APPC node is required for LU6.2 communications.

If you are upgrading from:

- NC-PASS Authenticator/Secure v1.4
- NC-PASS Authenticator/Secure v1.4 and NC-PASS VSSE v2.0
- NC-PASS VSSE v2.0.

to NC-PASS Authenticator v2.0.4 and you intend using APPC, refer to *APPC requirements* on page 3.3 and make the required changes to your current SEVTAM member.

If there are no additional nodes, no changes are required.

If you intend using cross-domain sessions and dynamic cross-domain allocation is not used, update your cross-domain resource definition to include the nodes.

You are strongly recommended to use the supplied definitions at least for initial testing and evaluation. Other definitions to VTAM refer to the names used. After a period of familiarization, during which you are customizing the product, you may want to amend the VTAM definitions to match your installation standards.

APPC requirements

◆ If you want to use APPC, the following samples in the **INSTALL** library should be reviewed:

- add the sample SEMODTAB to your existing modetable and reassemble, or select a suitable existing entry
- update the PASSAPPC in SEVTAM to match the modetable and entry names
- select a suitable LU6.2 port based on the sample in SEPORT
- if your current USSTAB does not include a suitable entry, add a USSTAB entry based on the sample in SEUSSTAB.

The changes made to include an APPC definition may require a restart of VTAM or an NCP gen.

◆ Copy member SEVTAM from **INSTALL** to your SYS1.VTAMLST library.

◆ Activate the application major and minor nodes by specifying the following command:

```
V NET,ACT,ID=member
```

where *member* is your chosen VTAMLST or SEVTAM member name.

The VTAM Session Management Exit

The VTAM Session Management Exit, ISTEEXCAA, is used by the VSSE component of NC-PASS. VSSE uses this exit to control which LU to LU sessions VTAM will allow or deny.

If you do not intend to use the VSSE component, you do not need to install this exit. Continue the installation process from *Chapter 4 - System changes*.

If you want to install the exit, note that it can be installed at any time and is **not** a prerequisite to installing the main product.

UPGRADE

If you are already using an earlier version of the PassGo Technologies exit ISTEEXCAA, you must replace it with this version.

If you are updating from V1.4, note that the VTAM Authorization Exit (ISTAUCAT), is no longer required.

How you install the exit will depend on which version of VTAM you are running and whether you already use the ISTEEXCAA exit.

Current use of the VTAM ISTEEXCAA exit

If you already use the VTAM exit ISTEEXCAA for other purposes and would still like it to run in conjunction with the PassGo Technologies product, there are two jobs in the distributed JCL library to accomplish this. This is described in *Linking your ISTEEXCAA exit to the PassGo Technologies exit* on page 3.8. However, **we recommend that this is done after the PassGo Technologies exit has been successfully installed and tested.**

Installing the ISTEEXCAA exit (VTAM version 3.4.1 and higher)

- ◆ 1. From the NC-PASS load module library, copy SEEXCAAB to SYS1.VTAMLIB or one of the libraries in the VTAMLIB concatenation, renaming it to ISTEEXCAA. (If ISTEEXCAA already exists on that library, save it under a different name first.)
- ◆ 2. Enter the following command

```
F NET,EXIT,ID=ISTEEXCAA,OPTION=ACT
```
- 3. If code 10 is returned, you already have a copy of ISTEEXCAA running. Enter the following commands

```
F NET,EXIT,ID=ISTEEXCAA,OPTION=INACT
F NET,EXIT,ID=ISTEEXCAA,OPTION=REPL
```
- 4. The exit can be disabled at any time from the master console by entering:

```
F NET, EXIT,ID=ISTEEXCAA,OPTION=INACT
```

The operator has the facility to stop, start and replace VTAM exits via VTAM's MODIFY EXIT command. (Refer to the *VTAM operations manual* for full command details.) The format of the command is:

```
F NET,EXIT,ID=ISTEEXCAA,OPTION=option
```

where *option* can be:

- ACT which activates the exit after it has been deactivated using the INACT option. The ACT option **always** calls ISTEEXCAA with the initialization function code X'FE' to allow other functions to be selected.
- INACT which deactivates the exit. It **always** calls ISTEEXCAA with termination function X'FF' before stopping.
- REPL which replaces ISTEEXCAA with a new copy. It **always** implies 'ACT' but only presents function X'FE' (initialization) if an INACT option was performed first.

Overview of the ISTEEXCAA exit (VTAM version 3.3)

ISTEEXCAA must reside in the Link Pack Area (LPA) and an IPL is required to enable a new version; because of this we provide two modes of operation.

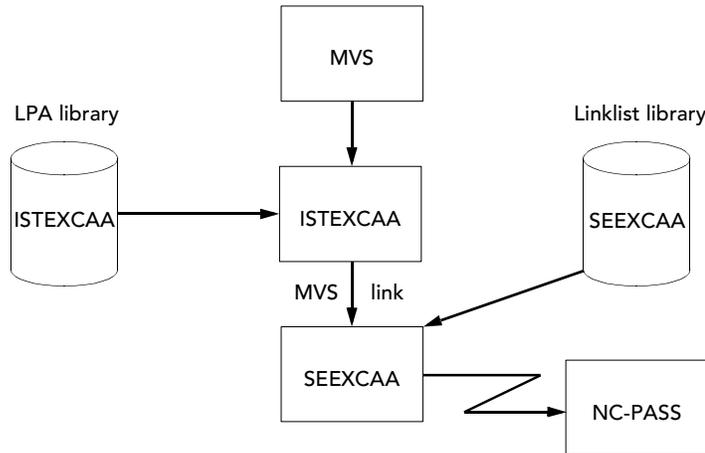
Test mode

The PassGo Technologies supplied ISTEEXCAA module uses the MVS LINK macro to pass control to a module called SEEXCAA. Two versions of the SEEXCAA load module are supplied. The test mode method allows switching between the A and B versions to be done without an IPL. Only an LLA REFRESH is required.

- SEEXCAA - If renamed to SEEXCAA, acts as a dummy module performing no function
- SEEXCAAB - the main processing component of the exit system. It can be called in one of two ways as described below:
 - rename it to SEEXCAA to be called by ISTEEXCAA as described previously
 - rename it to ISTEEXCAA to be invoked directly by VTAM.

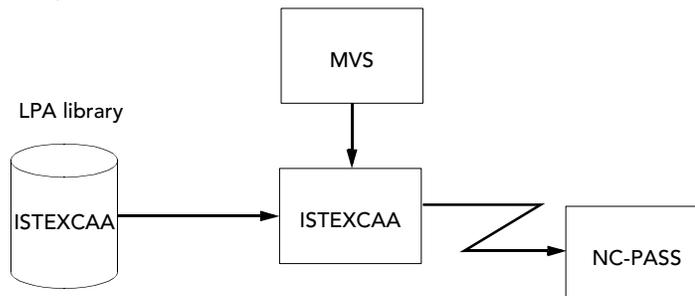
Before IPLing with the supplied version of ISTEEXCAA enabled, you must copy either SEEXCAA or SEEXCAAB into a linklist library and rename it SEEXCAA.

To switch versions of SEEXCAA after the IPL, replace the SEEXCAA module in the linklist library with the other version and refresh the LLA, by entering the command F LLA,REFRESH at the system console. This allows the SME to be enabled or disabled without an IPL.



Production mode

For greater efficiency and security, SEEXCAAB should be renamed ISTEEXCAA and executed from the LPA. This version will require an IPL to enable it and another to disable or modify it.



Installing the ISTEEXCAA exit (VTAM version 3.3)

- ◆ 1. Copy the ISTEEXCAA module from the **PREFIX*.LOAD* library to SYS1.SVCLIB. (If you are using test mode, copy module SEEXCAA into a linklist library selecting the A version for the dummy code or the B version for real code.)
- ◆ 2. **If you are running MVS/XA**, create the member IEALPAVE in SYS1.PARMLIB that contains the following control card starting in column 1:

```
SYS1.SVCLIB ISTEEXCAA
```

If you are running MVS/ESA, create the member IEALPAVE in SYS1.PARMLIB that contains the following control card starting in column 1:

```
INCLUDE LIBRARY(SYS1.SVCLIB) MODULES(ISTEEXCAA)
```

Linking your ISTEEXCAA exit to the PassGo Technologies exit

If you already use the VTAM exit ISTEEXCAA for other purposes and would still like it to run in conjunction with the PassGo Technologies product, there are two jobs in the distributed JCL library to accomplish this.

Note: It is recommended that this is done **after** the PassGo Technologies exit has been successfully installed and tested.

Register conventions used are as described in the *VTAM Customization Manual*. When control is passed to the PassGo Technologies version of the exit from an existing exit, the same entry convention must be obeyed.

The jobs in the distributed JCL library (*PREFIX*.CNTL) are called LINKUS1 and LINKUS2 as described below:

LINKUS1

This job links your current exit behind the PassGo Technologies exit as follows:

- your ISTEEXCAA is saved on your library as SAVEXCAA
- your CSECT is renamed to OLDEXIT before being merged in with our (PassGo Technologies) modules to form SEEXCAA on your SYS1.VTAMLIB (or VTAMLIB concatenated library)
- our ISTEEXCAA is linkedited over your old one in SYS1.VTAMLIB
- In this case, your exit is called before any checking is done by the PassGo Technologies exit. If your exit returns any condition code other than zero, it is honored, and no further checking is performed.

If you make a change to your exit that either adds extra, or removes unwanted, function calls, it will not be possible to action this change without restarting VTAM. However you can action logic changes by re-linkediting and replacing the exit.

LINKUS2

This job links your current exit to call the PassGo Technologies exit as follows:

- your exit is selected from the linkedit output library
- the PassGo Technologies exit is selected from the distributed NC-PASS load library and its CSECT is renamed to CKSSME
- the linkedited version is saved as ISTEEXCAA on your output load library.

In this case, you must have a call to another module in your existing ISTEEXCAA as follows:

```
L      R15,=V(CKSSME)
BALR   R14,R15
```

When your exit calls the PassGo Technologies exit, it must present the data in exactly the same way as when VTAM presents the data to your exit. CKSSME must be called for the following functions:

```
BEGIN (code X'FE')
SECONDARY AUTHORIZATION (code X'01')
END (code X'FF')
```

WARNING: Whenever a link-edit of any of these modules is performed it is imperative that the RMODE is set to 24.

SSCT names generated by NC-PASS

The distributed copy of VSSE will generate at least two (and possibly three) SSCTs in CSA on the MVS system under which it runs. These SSCT names are:

- XMS1 the Cross Memory Server (XMS) tasks's default SSCT name. The SME uses XMS to communicate with NCI.
- PAS1 common table storage between the VTAM Session Management Exit and the NC-PASS job controlling the tables and setting global options.
- PASX This is used only if you have an existing ISTEEXCAA type VTAM exit and want to link-edit it behind the PassGo Technologies exit. (See distributed JCL member LINKUS1.) If you use this method, this SSCT will contain exit function request information specific to your exit.

If any other product uses SSCTs with one of the above names, results from VSSE (and the other products) may be unpredictable. Refer to the NC-PASS Authenticator Administration Manual, Volume 1, *Communications* on page 8.78. If you want to change any of these default names, customization fixes AUC0101 (PAS1), AUC0102 (XMS1) and AUC0103 (PASX) (*PREFIX*.FIXLIST) allow the SSCT names to be changed.

WARNING: If you change the SSCT id XMS1, the corresponding SSCT id on the CROSS SYSTEM COMMUNICATIONS HOST FUNCTION panel must also be changed to match it. Refer to the NC-PASS Authenticator Administration Manual, Volume 1, *Communications* on page 8.78.

Activating the exit

The presence of ISTEEXCAA at VTAM startup will result in the exit automatically being active.

Backing out the exit

If you have problems installing the VTAM Session Management Exit and want to back out the exit, the following command can be entered from the system console. Note that the command will only be effective if the problem is due to the SME denying sessions. If VTAM is not responding, the only solution is a restart of VTAM.

At VTAM 3.4.1 or higher

1. Enter the following:

```
F VTAM,EXIT,ID=ISTEEXCAA,OPTION=INACT
```

and rename ISTEEXCAA to SEEXCAAB.

VTAM 3.3

If you have a TSO session perform the following steps:

1. Rename SEEXCAA to SEEXCAAB on SYS1.SVCLIB.
2. Copy SEEXCAAA to SYS1.SVCLIB and rename it to SEEXCAA on that library (or rename the version you saved in Step A back to ISTEEXCAA)
3. Refresh the LLA as follows:

```
F LLA,REFRESH
```

If you do not have a TSO session, re-IPL the system without specifying the new MLPA member.

Note: There are a number of ways of backing out the exit after installation. For example, if you inadvertently load a control table that stops all sessions, refer to the NC-PASS Authenticator Administration Manual, Volume 1, *Stopped sessions recovery* on page 8.77.

This page intentionally left blank

Chapter 4 - System changes

Security product interface	4.2
Re-assembling source members	4.2
Changes to your system	4.2
Authorization and IPL requirements	4.3

Security product interface

Each supported security product is distributed in the LOAD and SOURCE libraries. You are recommended to reassemble these source members; see *Re-assembling source members* below. The source members in question for NC-PASS are SEACF2 (CA-ACF2), SERACF (RACF), SESAC (SAC) and SETOPS (CA-Top Secret).

◆ Make suitable updates to allow protection and access to the new NC-PASS datasets. The PROCEDURE or batch JCL will require read access to the *PREFIX*.CNTL/LOAD/PANELS/PBLIB libraries and control access to the VSAM files.

◆ When a procedure is being run, add the started task name to the started procedures table (ICHRIN03).

Note: To use with security applications, NC-PASS must be run from an authorized library.

When an administrator defines userids to NC-PASS, if required he can specify a proprietary security product to be used when the user logs on. This is explained in the NC-PASS Authenticator Administration Manual, Volume 1, *Chapter 3 - Controlling user access*.

When a user logs on, the appropriate module is called to perform password checking by the appropriate security product. In all cases, the terminal in use and any userid, password or new password entered by the user are passed to the assembler module. Each of the assembler modules are supplied with NC-PASS in both source and load form.

Re-assembling source members

If you cannot logon with the supplied modules and receive the message *CKSE0029-5 user invalid*, the appropriate sample source member should be re-assembled and copy replaced to the load library. This is most likely to be required when your security system version differs from that of the supplied sample load module.

Refer to *PREFIX*.SOURCE and *PREFIX*.MACLIB for the sample members and sample ASMSAMP JCL.

The source members SETOPS and SERACF are supplied assembled without message support; the message support is commented out within the source. If you do not want these messages to be displayed to users, see the comment in panel ESE2002 in *PREFIX*.PANELS.

If the random password feature is to be used, the source must be re-assembled with the message support code included.

Changes to your system

When making changes, the following steps should be carried out.

- ◆
- for RACF and CA-ACF2, authorize the load libraries either through the Program Properties Table (PPT) or the Authorized Program Facility (APF)
 - for CA-Top Secret, authorize the load libraries either through the Program Properties Table (PPT) or the Authorized Program Facility (APF), and update the CA-Top Secret security matrix as follows:
 - Facility (USER3=NAME=NCPASS)
 - Facility (NCPASS=PGM=NCS,NOABEND, NOASUBM, NOLAB,AUTHINIT)
 - Facility (NCPASS=MRO,MULTIUSER,NORNDPW,TENV,NOTSOC)
 - Facility (NCPASS=NOXDEF,ACTIVE)

Allow all users to access NC-PASS by entering:
TSS ADD(ALL) FACILITY(NCPASS)

Authorization and IPL requirements

You will need to authorize the load library in APF list or through PPT if you want to use cross-memory services (XMS) to:

- enable NC-PASS to communicate with the SME
- use the TLI function of NC-PASS to enable non-NC-PASS jobs to communicate with NC-PASS.

You may need to re-IPL the system for the following reasons:

- for APF authorization
- to refresh the LPA when running the exit under VTAM 3.3 (not higher) using the IEALPAVE member created on page 3.7.

If you do IPL, you will need to reactivate SEVTAM.

This page intentionally left blank

Chapter 5 - Starting NC-PASS

Starting up	5.2
Updating startup parameters	5.2
Starting NC-PASS	5.4
Logging on for the first time	5.5
Starting NC-PASS subsequently	5.6
Conversion notes	5.7
Basic verification	5.8
VSSE exit check	5.8

Starting up

This section describes how to start NC-PASS.

Updating startup parameters

Review members PSOPT and PSTDT.

UPGRADE

Use the **new** PSOPT member. You can however use your existing PSTDT.

Member PSOPT

Member PSOPT of dataset *PREFIX*.CNTL contains the following startup options:

Startup option	Description
ACBNAME= <i>acbname</i>	The ACBNAME as defined in SYS1.VTAMLST.
CODE= <i>product code</i>	Defines the authorization code, based on the CPU serial number, which enables NC-PASS to run as a licensed product. This can be specified more than once; NC-PASS selects the highest level authorized. There is no default; the CODE can only be obtained from your support office.
CONNECT-MESSAGE=YES/NO	Enter YES for a message to be written to the log whenever a user, initially or on return from another application, connects to NC-PASS. Enter NO to suppress the message.
EXTENDED-MODIFY=YES/NO	Enter YES to enable entry of the full range of NCI language statements from a system console. Enter NO to restrict operator commands to the primary control set.
LOG-PAGE-LENGTH= <i>nn</i>	Determines the number of lines on a log page up to a maximum of 99.
NON-SWAP=YES/NO	Determines if the address space is to run non-swappable or not. Enter YES to run non-swappable or No to run swappable. If the task is not running from APF-authorized libraries, YES will cause a warning message to be issued.
PANEL-STORAGE= <i>xxxK</i>	Specifies the maximum amount of storage which will be used to hold NCI panels built in storage, defined in Kilobytes.

Startup option	Description
PROD-MODE=YESINO	<p>No is the default and causes an open and close for every PANEL and EXEC routine when initially created (loaded into storage). This option is required when PANEL or PBLIB libraries have a secondary space allocation.</p> <p>YES means PANEL and PBLIB libraries are opened at startup and kept open until shutdown. Each panel build avoids opening and closing the library. PROD-MODE=YES is for the duration of the job and cannot be switched on and off.</p> <p>Restrictions</p> <p>When panels are being edited, a dataset may extend into secondary extents, so PROD-MODE=YES is restricted to PANEL and PBLIB libraries without secondary space allocation.</p> <p>At sites with a DFP version above 2.2, PANEL and PBLIB concatenations are checked automatically at startup. If any dataset in the PANEL library concatenation has a secondary space quantity defined, then PROD-MODE=YES will be disabled for the PANEL library, and likewise for PBLIB.</p> <p>Sites with a DFP 2.2 or below must ensure that no secondary allocation is possible for any dataset in the PANEL and PBLIB concatenations; failure to observe this restriction will cause unpredictable errors during PANEL/EXEC creation.</p>
BACKUP-WAIT= <i>nn</i>	Determines the wait time in seconds before NCPASS attempts reallocation. (See <i>Using the backup recovery facility</i> on page 3.4 of the Administration Manual - Volume 2.)
RECOVERY-ON=YES	Enter YES to enable NCPASS trans logging to TLOG1 and TLOG2.

Modify member **PSOPT** of dataset **PREFIX*.CNTL* as follows.

1. To authorize the use of NC-PASS place your authcode in member PSOPT by updating the `CODE=` parameter with the code supplied by your support office. The value you supply in the `CODE=` parameter determines the product you are authorized to use and hence the menu structure you will see.

UPGRADE

Warning: you cannot use the code from your previous version. You must obtain a new code from your support office.

2. If the sample ACBNAME was changed in the VTAM step, update the ACBNAME parameter in member PSOPT to reflect the new ACBNAME.

Member PSTDT

The member **PSTDT** of the **PREFIX** dataset is supplied with a PANEL ESE0052. This should not be changed for initial testing. See *Chapter 6 - Post-installation considerations* for further details.

Starting NC-PASS

◆ Use your replies from *Providing information for installation* on page 1.5 to amend member PASSJCL of dataset *PREFIX*.CNTL.

◆ Modify the jobcard values appropriate to your installation standards.

UPGRADE

Member PASSJCL has changed from previous versions. For example, help and messages are now held in PDS members which must be included in the runtime JCL.

◆ Run PASSJCL.

The following message should be produced on the NC-PASS NCILOG at startup

```
NCINIT - ADDRESS SPACE RUNNING AUTHORIZED
```

Note: The JCL which runs the NC-PASS job has been prepared so that it can be changed to run as a procedure with the minimum of effort. To do this, remove the PEND and EXEC statements and copy the JCL to your procedure library.

During the initial startup of NC-PASS the following messages are issued at startup on the system console. If these messages are not seen, the installation steps have not been completed.

```
+NC-PASS CKUT0540-4 DATABASE INITIALIZATION COMPLETED  
+jobname - NOW ACCEPTING TERMINAL LOGONS
```

Logging on for the first time

- ◆ When NC-PASS has initialized, logon to the application by connecting to PASS from USSTAB.

UPGRADE

Log on with your existing administration userid to display the administration menu. Proceed to the section entitled *Conversion notes* on page 5.7.

- ◆ Follow the instructions on the panels.

Your authorized USERID is MASTER, this id is used for the initial log on only.

Connecting to NC-PASS and using the MASTER userid cause the following messages to be issued:

```
+NC-PASS CKUT0692-4 INITIAL CUSTOMIZATION OF SYSTEM STARTED
+NC-PASS CKUT0694-4 INITIAL USE OF MASTER USERID IN PROGRESS
+NC-PASS CKUT0697-4 CUSTOMIZATION OF SYSTEM HAS FINISHED
```

You are asked to assign a new confidential userid, as shown on the panels on the following page. The MASTER user profile is then deleted.

UPGRADE

If you are upgrading from NC-PASS v1.4 and you do not use the userid MASTER, you should create a new CAF without the MASTER record. The following code copies the existing CAF to a new CAF omitting the MASTER record:

```
//REPRO2 EXEC PGM=IDCAMS,REGION=512K
//SYSPRINT DD SYSOUT=X
//INPUT1 DD DSN=CURRENT.CAF,DISP=SHR
//OUTPUT1 DD DSN=NEW.CAF,DISP=SHR
//SYSIN DD *
  REPRO INFILE(INPUT1) -
        OUTFILE(OUTPUT1) REPLACE -
        FROMKEY(X'00000000000000000000000000000000') -
        TOKEY(X'3BD4C1E2E3D9403FFFFFFFFFFFFFFFF')
  REPRO INFILE(INPUT1) -
        OUTFILE(OUTPUT1) REPLACE -
        FROMKEY(X'3BD4C1E2E3D940400000000000000001') -
        TOKEY(X'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF')
//
```

The following panels are displayed only for initial customization.

```
Date:12/12/1997          NC-PASS INSTALLATION (1 OF 2)          Userid:TSG0001
Time:08:04:20                                     Terminal:A01MS009
```

```
This is the initial logon after NC-PASS has been installed on the system.

No access to the system is currently allowed until you have completed the
INSTALLATION steps.

Ensure you follow the instructions carefully, any error will result in the
complete system having to be re-installed.

Automatic system logging has been invoked and you cannot exit from this
procedure until all steps have been completed.
```

```
Enter the supplied authorized userid => _____
```

```
CKSE0692-4 Initial customization of system started
```

```
Date:12/12/1997          NC-PASS INSTALLATION (2 OF 2)          Userid:TSG0001
Time:08:05:03                                     Terminal:A01MS009
```

```
You must now assign a new userid, the default profile for this user is that of
a system administrator with no password protection.
```

```
Enter the new administrator's userid => _____
```

```
The next panel displayed will be the system administration menu, the profile
for the userid entered above can be changed by following option 2 from this
menu, it is strongly recommended that password protection should be added to
this profile.
```

```
PFK3 from the administration menu will exit from the security system and the
system logo will be displayed, this logo can be altered to meet with specific
site standards.
```

```
Press the <ENTER> key to display the administration menu.
```

```
CKSE0694-4 - Initial use of master userid in progress
```

This completes the installation process.

Starting NC-PASS subsequently

Further startups of NC-PASS will issue the following message:

```
+NC-PASS CKUT0534-4 SYSTEM INITIALIZATION STARTED
```

Conversion notes

UPGRADE

If you are upgrading from NC-PASS 1.4 or from NC-PASS VSSE 2.0 to NC-PASS 2.0, all your existing settings should be carried forward, although they may appear in a different place. For example in NC-PASS VSSE 2.0, the cross memory services identifier is set on the CROSS MEMORY SERVICES panel (6); in NC-PASS 2.0 it is set on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1).

If you are currently using XMS or MHO, the parameters will be transferred, **but not enabled**. This allows the copying of the 1.4 CAF without stopping the system.

If you are currently using an NC-PASS 1.4 authorization control table refer to the NC-PASS Authenticator Administration Manual, Volume 1, *Converting an NC-PASS 1.4 authorization control table to V2.0* on page 8.83.

If you use PASSMNT2 to combine an existing NC-PASS 1.4 and NC-PASS VSSE 2.0 into a single NC-PASS 2.0 system you are advised to note the contents of the VSSE GLOBAL OPTIONS screen in the NC-PASS VSSE system. These options will be set to default in the new system as they cannot be copied. For further details refer to the NC-PASS Authenticator Administration Manual, Volume 1, *Converting an NC-PASS 1.4 authorization control table to V2.0* on page 8.83.

Basic verification

When you have completed the first logon complete the following steps to verify the installation:

1. From the ADMINISTRATION MENU select option 3 to browse the log. The BROWSE NC-PASS LOG panel will be displayed.
2. Press <F9>. The NCILOG will be displayed.
3. Enter M on the command line and press <F7>. The top of the log will be displayed showing the startup options used.
4. Press <F8>. The second page of the log will be displayed.
5. Check for the NCINIT message:
Address space running authorized
6. Press <F8>. The third page of the log will be displayed.
A message indicates the version of NCI and a fixgrid the current fix level.
7. Enter F IDENT, press <Enter>. The message indicating the VTAM version identifier is found.
8. Enter M on the command line and press <F7>. The top of the log will be displayed.
9. From the command line enter F 540 and press <Enter>. The message
Database initialization completed
is displayed. This message only occurs at the first startup.
10. Repeat step 9 with 535. The message
System initialization completed
is displayed.
11. Enter M on the command line and press <F7>. The top of the log will be displayed.
12. To check that you have installed the correct product, from the command line enter F 3612 and press <Enter>. The following line should be displayed:
11:55:22 CKSE3612-4 NC-PASS VERSION 2.0.4 AUTHENTICATOR
13. Press <F3> to exit to the ADMINISTRATION MENU via the BROWSE NC-PASS LOG panel.

UPGRADE

Conversion messages will also be output to the log.

VSSE exit check

If you have installed the VSSE exit, ISTECAAA, complete the following steps to verify that NC-PASS is successfully communicating with the exit:

1. Select option 4.1 - CROSS SYSTEM COMMUNICATIONS - HOST.
2. In the Cross Memory Communications section, enter Y in the **Enable XMS** field and XMS1 in the **XMS Identifier** field. Press <Enter>. Message CKxx3033 with return code 0 should be displayed.
3. Press <F3> to exit to the ADMINISTRATION MENU.
4. Choose option 7.5 (Global options). If no error messages are displayed at the bottom of this screen, then NC-PASS is successfully communicating with the exit. If error messages are displayed refer to the Administration Manual, Volume 2, *Chapter 6 - Messages and abend codes*.
5. Press <F12> to cancel out of this panel and return to the ADMINISTRATION menu.

Chapter 6 - Post-installation considerations

Post-installation considerations	6.2
TDT options	6.2
Using the NC-PASS trial mode facility	6.2
Re-initializing the database	6.2
Running under a session manager	6.2
Using SecurID tokens with NC-PASS	6.3
Using NC-PASS with NCI/XF or NC-SPE	6.4
Customization	6.4
Using MVS MODIFY(F) and STOP(P)	6.5

Post-installation considerations

This chapter describes some of the post installation issues that you should consider before using NC-PASS.

TDT options

The member PSTDT of the *PREFIX* dataset is supplied with a PANEL ESE0052. If you want to use the terminal profile maintenance option to control terminal access, amend the TDT to read PANEL ESE0032.

Using the NC-PASS trial mode facility

A trial mode facility is provided so that users who have not been allocated NC-PASS security tokens can logon using the NC-PASS procedure.

Enabling trial mode

Trial mode is enabled by entering Y at the Trial Mode prompt on the LOGON DEFAULTS panel (1.2). The remaining fields on this panel are provided for overall tailoring of the product and are not used to enable trial mode.

Assigning a user to a trial token

Having enabled trial mode and enabled the required token type, you should assign each user to a 'trial' token. For each token type there are 10 trial token records provided on the distribution tape that contain trial data. These records are numbered 1 through 10 and can be listed using the LIST TOKENS panel (provided by option 1 on the NC-PASS ADMINISTRATION MENU).

A trial mode user is assigned to a trial token through the LIST TOKENS panel. Enter A in the 'S' column by the required token number and press <Enter>. The TOKEN DETAIL panel will be displayed in a layout appropriate to the Token type.

Refer to the NC-PASS Authenticator Administration Manual, Volume 1, *Chapter 5 - Token administration* for token panel layouts and instructions for their use.

Re-initializing the database

If errors are encountered and you want to start from a fresh database, or you want to create a second copy of NC-PASS, use member DEFVSAM in *PREFIX*.CNTL. This will create both CAF and VSDD in the same format as a new install. DEFVSAM2 uses an existing CAF as the base.

If however you are running NC-PASS together with NC-ACCESS and you want to re-initialize the NC-PASS side of the CAF use member PSDELETE followed by member PSREPRO in the *PREFIX*.CNTL.

Running under a session manager

If NC-PASS is defined as an application in a session manager such as MULTSESS/HPO or NC-ACCESS, then the NC-PASS application should have a vterm of UNQNODE. If this is not defined, problems will be encountered when the session has been terminated and attempts are made to restart a session with NC-PASS; a **vterm already in use** error message will be issued.

Using SecurID tokens with NC-PASS

Complete this section only if your users will be using either of the two types of SecurID tokens.

The SecurID tokens are the only tokens that require external data to be loaded to the NC-PASS database. This step processes those records supplied on tape with the tokens and C.D.M. (Code Display Module).

The SecurID TRIAL data supplied with the NC-PASS product includes a system record. Each batch of SecurID tokens is accompanied by a tape, a system record is included on this tape. This system record should replace the TRIAL system record.

When further batches of tokens need to be loaded the system record must not be replaced.

The STARTUP option `TOKEN=SD,Y` or `TOKEN=SD,N` controls whether the SecurID system record is overwritten. If loading INITIAL production token data specify `TOKEN=SD,Y`. If loading ADDITIONAL production token data specify `TOKEN=SD,N`.

If you want to install NC-PASS for use with SecurID tokens, carry out the following steps.



Modify member 'PSBATCH' of *PREFIX*.CNTL by using the instructions within the member. The dataset name of the data records is required. Your NC-PASS authorization code is also required to authorize the execution of this batch job.

Submit and run the job.

SecurID synchronization

If you are using SecurID tokens, synchronization of the NC-PASS database is required whenever NC-PASS is started; when NC-PASS is in production this should be automated as part of the startup. This can be done by updating the operator menu option to synchronize at startup. When a test system is running, synchronization can be done by an administration user. Avoid logging on with SecurID authentication until synchronization has taken place.

The synchronization of a SecurID token system is critical (particularly in a production NC-PASS system) and should be performed at each startup.

Using NC-PASS with NCI/XF or NC-SPE

NC-PASS cannot run in the same address space as NCI/XF or NC-SPE.

Running in separate address spaces

You may do this in one of two ways:

- LOGAPPL the terminals to NC-PASS and connect to the NCI/XF system passing CINIT data; this allows NC-PASS to replace NCI/XF or NC-SPE logon processing while retaining NCI/XF menuing functions

OR

- LOGAPPL terminals to the NCI/XF or NC-SPE system and use TLI functions to communicate with NC-PASS. Refer to the NC-PASS Authenticator Administration Manual, Volume 2, *Chapter 2 - Transaction Level Interface (TLI)*.

Customization

NC-PASS is distributed with a wide variety of example logos and several exits. The logos are described in the NC-PASS Authenticator Administration Manual, Volume 2, *Chapter 4 - Customization* and the exits in the NC-PASS Authenticator Administration Manual, Volume 2, *Chapter 5 - Exit processing*. It is recommended that you create a small panel library and concatenate this library in your NC-PASS JCL. Copy into this library any logos or exits you wish to use in your NC-PASS system. This will allow simple and smooth maintenance updates. When the maintenance libraries are created the libraries can be switched without impact on your customizations. It should be noted that some fixes may be applied to logos or exits so before starting your NC-PASS, browse the maintenance copies of the relevant panels and if they have been changed either repeat the change or recustomize the maintenance copy. A small load library should be similarly defined if you assemble your own security exit.

Using MVS MODIFY(F) and STOP(P)

NC-PASS can be controlled from the MVS system console using the MVS MODIFY(F) and STOP(P) commands. The available range of functions depends on the value specified in the EXTENDED-MODIFY startup option. Note that NCPASS in the following example is the jobname.

The primary control set is available regardless of the value specified for the EXTENDED-MODIFY startup option. The primary commands allow normal or abnormal termination of NC-PASS from a system console:

P NCPASS	requests NCPASS to shutdown.
F NCPASS,ABEND	requests NCPASS to terminate with a dump.
F NCPASS,ABEND <i>lunam</i>	requests NCPASS to terminate with a dump and format the control blocks for the terminal named in <i>luname</i> .

The extended control set is available only if EXTENDED - MODIFY = YES was specified at NC-PASS startup and comprises the complete set of language statements with the exception of those which are clearly inappropriate for a system console.

Operations such as deleting a panel from storage, executing a routine or starting and stopping the NC-PASS trace may be carried out by entering the appropriate language statement as the text of a MODIFY command:

F NCPASS,*command operand operand operand*

This page intentionally left blank

Chapter 7 - Applying fixes and zaps

Applying fixes and zaps	7.2
The Maintenance Program product for panel maintenance	7.2
Installing the MP product	7.3
Applying zaps	7.4
+VERIFY data cards	7.4
Output from the MP program	7.5
Error messages	7.5

Applying fixes and zaps

This section provides details of applying fixes and zaps and includes an overview of the Maintenance Program product (MP).

The Maintenance Program product for panel maintenance

The Maintenance Program product (MP) provides the facility for modifying prebuilt panels (PBLIBs).

MP uses the following files:

- FIXCNTL a VSAM KSDS file containing records indicating maintenance to PBLIBs. The key is 17 bytes long and starts at position 0.
- PBLIB containing the prebuilt panels.
- SYSIN containing the control LRECL fixed 80 byte 'cards'
- FIXFILE containing the actual ZAP data, the LRECL fixed 132 byte 'cards'.

The three stages of processing are shown in the following table:

Processing stage	MVS systems
1. Create the FIXCNTL database	All installation options define a FIXCNTL database and load one blank record in step AMS001.
2. Synchronize the PBLIB records against the FIXCNTL database	Each installation job includes a final step for this processing stage. A sample job is supplied.
3. Apply MP fixes to PBLIBs.	A batch job is supplied to read the FIXCNTL database to check prerequisites and apply the fix.

Using MP

Installing a product, or doing a full maintenance install, loads down PBLIBs with all the current MP fixes applied to the level shown on the documentation. You can individually load the MPFIXES file and select fixes. This may be a useful method for an individual fix, but may not be the best way to apply several fixes. MP fixes may also need distributed panels or VSAM data or both. If so, apply the fix by installing full maintenance.

Hardcopy fixes

MP is most useful when fixes have been supplied in hardcopy, usually by fax. The following table shows how to apply a hardcopy MP fix.

MVS systems
Copy the PBLIB members that are to be zapped to a new library. Add the library to the JCL to allow for ease of testing and backing out of the fix if required.
Sample members are included.
MPFIX in *PREFIX*.CNTL
Edit the member to use your PBLIB and FIXCNTL database.
Enter the fix after the //FIXFILE DD * JCL statement.
Execute the job and check the output.

Errors

The fix includes a checksum. Failure to key the fix precisely will give a checksum error. Common errors are:

- leaving numbers on in edit
- using incorrect international characters like £ or \$.

Check the hex values, which are given in the comments. The comment section is not part of the checksum and need not be keyed.

Backing out a fix

Delete the PBLIB members from the concatenated library and resynchronize.

Installing the MP product

To run MP the following installation steps are required. These are run during the installation job stream.

- install PassGo Technologies products containing the MP product
- create the FIXCNTL.DATABASE
- synchronize the PBLIBs against the FIXCNTL.DATABASE.

MVS systems

A cluster is defined with a KEY of 17 bytes, and a dummy record repro'd onto that cluster. Any maintenance data is then copied to the FIXCNTL.DATABASE from the PBLIBs. A job recreating and synchronizing the FIXCNTL is supplied in member MPSYNC in *PREFIX*.CNTL.

Applying zaps

Sample JCL is provided to load zaps as shown below. This is supplied as member MPFIX on *PREFIX*.CNTL.

MVS systems sample JCL

```
//*JOB CARD JOB (ACNT) , 'MP' , CLASS=?, MSGCLASS=?
//*
//STEP1 EXEC PGM=MP
//STEP CAT DD DSN=CATALOG.MVSICF1.V*CATVOL* , DISP=SHR
//STEP LIB DD DSN=*PREFIX*.LOAD , DISP=SHR
//FIXCNTL DD DSN=*VSAMPFX*.FIXCNTL.DATABASE , DISP=SHR
//SYS PRINT DD SYSOUT=*
//SYS DUMP DD SYSOUT=*
//*
//*PBLIB RECEIVING FIXES
//*
//PBLIB DD DSN=*PREFIX*.PBLIB , DISP=SHR
//SYS IN DD*
+RECEIVE ALL
+LIST*
//*
//*USE THE FOLLOWING DD IF APPLYING MPFIXES FROM HARDCOPY
//*
//FIXFILE DD*
//***** DATA CARDS HERE *****
```

A single FIXCNTL database should be maintained for each product tape. If more than one set of PBLIBs is installed from the tape, include all the PBLIBs in the MPSYNC step (please see the JCL extract on the previous page for the MPSYNC step). If the FIXCNTL database has to be recovered, simply redefine, repro and sync the PBLIBs in again.

+VERIFY data cards

The cards (in FIXFILE) that follow a +VERIFY statement are known as +VERIFY data cards. They are present to ensure that subsequent data cards which will modify the NCI/XF panel will, in fact, modify the correct area of the panel.

The verify data card is matched against the card in the panel; if a mismatch occurs then this will be reported as a +CHECKSUM= error.

In order to reduce typing and consequent errors for fixes that are distributed by fax, the MP program will allow case mismatch between verify data cards and the original panel statement. It will also allow a different number of leading spaces before the NCI verb, and will only cross check the non blank characters on the verify data card against the panel card and not vice versa. The number of non-blank characters typed on a verify data card must match that distributed by PassGo Technologies. For example the following cards will match.

```
IF &SYSDATE = <--- verify data card
if &sysdate = '01/01/91' <--- original NCI statement
```

In this example, even if you chose to type the characters 'IF' in lower case, the MP program will still accept the verify. Should a +CHECKSUM ERROR occur, the above rules may help determine whether the typing error is on a verify data card or a replacement NCI data card.

Output from the MP program

After applying maintenance, MP will write a report to the SYSPRINT file which should be checked to ensure maintenance was applied correctly.

When a fix is applied successfully the following type of output is expected:

```
MAINTENANCE PROGRAM: MAINTENANCE APPLIED BY THIS RUN
+RECEIVE NCB0302
  FIX NCB0302 APPLIED SUCCESSFULLY
    MEMBER @UTSTATS UPDATED IN DATASET CKDNGF1.NCI.PBLIB
```

Should a fix not apply successfully, the input FIXFILE and SYSIN should be carefully examined for typing errors if the input fix has been developed at the customer site (based on a fax transmission for instance).

If a fix is typed in error then MP will report a problem according to the type of error. It will initially check that the construction of a fix is correct. For instance the mandatory control cards (+ZAP, +MEMBER, +VERSION and +CHECKSUM) must be present and report on constructional errors (eg that the +MEMBER card has been omitted).

If the mandatory control cards are correct, the subsequent edit control and data cards are processed sequentially and examined. Should an edit control card be invalid it will be reported with an appropriate error message (eg +DELETE/+REPLACE CARD IS NOT PRECEDED BY +VERIFY AND VERIFY DATACARDS), but if an actual NCI/XF data card is in error this will be reported as a +CHECKSUM error. MP uses a checksum technique to ensure the checksum value of all NCI/XF data cards matches the value on the +CHECKSUM= card.

Error messages

The following example output error messages and error actions may help determine typing errors in input fixfiles.

FIX xxxx MISSING FROM FIXFILE

Explanation: Either the name of the fix is mistyped on the +ZAP card in FIXFILE or the name is mistyped on the +SELECT xxxx card in SYSIN or the fix is not present in the FIXFILE dataset.

System action: None.

User response: Check and correct the above.

FIX NCB0312 IN ERROR. FIX REJECTED LAST FIX TO @UTSTATS (3.1.0) WAS NCB0311, A +PREZAP CARD MUST BE CODED.

Explanation: You have probably omitted a +PREZAP card, which should follow the +ZAP card in FIXFILE.

System action: None.

User response: Check and correct the above.

**FIX SYB0033 IN ERROR. FIX REJECTED
+INSERT MUST BE FIRST EDIT CONTROL CARD FOR NEW MEMBER**

Explanation: The member to be zapped is not in the library.

System action: None.

User response: Check member name is correct.

**FIX xxxx IN ERROR
+REPLACE CARD IS NOT PRECEDED BY +VERIFY AND VERIFY DATACARDS**

Explanation: You have probably omitted a +VERIFY (edit control card) from the fix in FIXFILE. This card should precede any verify data cards.

System action: None.

User response: Check and correct the above.

FIX REJECTED. +CHECKSUM= xxxx IS INVALID FOR MEMBER xxxx

Explanation: Either the checksum number on the +CHECKSUM card has been mistyped or there is a typing error on an NCI/XF data card. NCI/XF language statements are indentation-sensitive so the number of blank columns which precede the NCI verb must be typed exactly as required. All data cards after a +VERIFY card must be carefully checked. In the case of a fax distributed by PassGo Technologies, for instance, the cards must exactly match its format. For verify data cards the MP program will allow case mismatch and an inexact number of blank characters before the first non-blank character. Please refer to the section entitled *+VERIFY data cards* on page 7.4.

System action: None.

User response: Special characters have different HEX values according to the country in which the fix is being created. The comments within the MP fix in FIXFILE contain a special character table of the appropriate HEX values for non-numeric fax data. Should a special character (eg \$ or £) be typed with an incorrect hex value, this will be sufficient to cause a + CHECKSUM error. Ensure the HEX values of your fix are identical to the comments in the fix. Check that your editor profile does not use NUMBERS ON. Print your fix and compare it with the hardcopy received from PassGo Technologies. If this fails to identify the error, fax your fix to the PassGo Technologies support office.

**FIX xxxx IN ERROR. FIX REJECTED
CONTROL CARD NOT RECOGNIZED:(FIXFILE CARDS DISCARDED UNTIL NEXT +ZAP)**

Explanation: For example:
+BREZAP=NCB0311

A control card was not recognized. Any card starting with a + character is an MP control card and must be immediately followed by a valid MP command. In this example the second input card in a fix (in FIXFILE) should have been coded as +PREZAP=NCB0311.

System action: The fix will not be applied.

User response: Check and correct the above cards.

Chapter 8 - Getting started

Planning for NC-PASS	8.2
Identifying the level of network protection	8.2
Identifying authentication requirements for remote platforms	8.3
Identifying userid controls	8.3
Identifying audit requirements	8.5
What the NC-PASS books contain	8.6
Installation Manual	8.6
Administration Manual - Volume 1	8.6
Administration Manual - Volume 2	8.8
NCI language statements	8.8
User Guide	8.8
Using NC-PASS menus	8.9
Selecting options	8.10
Fastpath menu skipping	8.11
Panel referencing in this manual	8.11
Making changes to panel data	8.12
Using the line editor	8.12

Planning for NC-PASS

Security can be defined as the protection of resources from accidental or deliberate modification, destruction or unauthorized access.

NC-PASS Authenticator provides many functions to help achieve the level of protection needed for your installation. The factors that determine what functions to select are:

- your installation's security objectives
- the security measures already in place.

For example, your installation may require security for all or some of its applications; you can use NC-PASS to identify and protect them.

You may want to implement enhanced security for specific high-risk users, but to ensure that other users are unaffected.

Each installation will have its own objectives; this section provides a guide to a number of access control objectives and how NC-PASS can be used to achieve them.

Identifying the level of network protection

NC-PASS allows you to specify different levels of protection for your network using the Session Management Exit (SME). In all cases you can use the NC-PASS audit facilities to report on access to those resources. The following list identifies several network access control objectives and how NC-PASS can be used to achieve them.

Objective	NC-PASS function	Refer to the Administration Manual...
Dial-in protection	NC-PASS instructs VTAM via the IBM Session Management Exit (SME) to control access to applications. You can define permitted connections across the whole of the VTAM network. The access permissions and restrictions are held in a control table which is administered on-line.	<i>Chapter 8 - The VTAM Session Security Exit (VSSE) (Vol 1).</i> <i>Denying access to a specific application from dial-in lines on page 9.28 (Vol 1).</i>
Control of inter-network access	If your network is linked to many other networks, the NC-PASS VSSE control table can be defined to allow access only between specific networks.	<i>Chapter 8 - The VTAM Session Security Exit (VSSE) (Vol 1).</i>
Protection of a sensitive application from unauthorized access	NC-PASS can protect applications by allowing access only to specific userids. Where that userid is not initially specified (eg from a dial-in terminal via USSTAB) NC-PASS can ACQUIRE the terminal to force the user to provide that information.	<i>Denying access to a specific application from dial-in lines on page 9.28 (Vol 1).</i> <i>Using ACQUIRE to protect sensitive applications from dial-ins on page 9.10 (Vol 1).</i>
To permit access to resources at specified times only.	NC-PASS allows you to specify at what times a session with the specified resource can take place. (For example, an application can be accessed only in office hours.)	<i>Preventing access to an application at specific times on page 9.34 (Vol 1).</i> <i>Chapter 7 - Restricting access by date and time (Vol 1).</i>

Identifying authentication requirements for remote platforms

For remote platforms which support the Advanced Program to Program Communication Protocol (APPC), NC-PASS provides authentication from the host via an APPC Transaction Level Interface (TLI).

If you want to ...	Then ...	Refer to the Administration Manual ...
use the host as an authentication server for remote platforms	you can specify a link to a remote platform which can transmit authentication requests via the APPC TLI.	<i>Applications using the APPC interface</i> on page 1.11 (Volume 2). <i>APPC/TCP/IP TLI</i> on page 2.15 (Volume 2).
use the host to centrally maintain an audit trail.	you can specify that requests are made to NC-PASS to write messages to the log using one of the APPC TLI functions.	<i>General message request (Process code 06)</i> on page 2.30 (Volume 2).

Identifying userid controls

Your organization's userid structure is probably well-established by department or function or both. As part of the planning for NC-PASS, you need to understand the responsibilities of the various users, the resources to which they need access to do their job and the security in place for each user.

Classification of users by NC-PASS

NC-PASS classifies users into three groups:

- Administrator
- Operator
- User.

A user classified as an NC-PASS administrator has the overall responsibility for the NC-PASS system and access to the NC-PASS on-line administration function; the security controls for this user need careful consideration.

If you are a large site, you may need more than one administrator - NC-PASS supports a hierarchy of administrators.

Users classified as Operator have access to operator functions within NC-PASS.

Users classified as User are end-users and have no access to the NC-PASS administrator or operator functions.

Controlling user access

NC-PASS allows you to specify different levels of protection for your users. The following list identifies several access control objectives and how NC-PASS can be used to achieve them.

Objective	NC-PASS function	Refer to the Administration Manual...
Use existing userid security database as a basis for NC-PASS.	You can add additional data to a RACF userid profile, which NC-PASS will extract when the user attempts to logon.	<i>Chapter 6 - Administering users from an external security database (Vol 1).</i>
Authentication of userids with access to sensitive data	You can assign all or selected users to personal authentication devices. When the user attempts to logon, information from the device must be provided in addition to userid and password.	<i>User profile creation on page 3.20 (Vol 1) and Chapter 5 - Token administration (Vol 1).</i>
To control access to a sensitive transaction.	NC-PASS provides a Transaction Level Interface which allows communication from an application to NC-PASS. Before allowing a user to process a sensitive transaction, eg a funds transfer transaction, the user can be authenticated or re-authenticated at this point.	<i>Chapter 2 - Transaction Level Interface (TLI) (Vol 2), Terminal risk profile creation on page 3.35 (Vol 1).</i>
To stop repeated unsuccessful attempts to gain access to the system.	NC-PASS allows you to specify a maximum retry limit, after which the userid is locked and cannot gain access to the system until reset by the administrator. Alternatively, you can specify a temporary lock period for users, or terminals, or both, which will be actioned if an unsuccessful attempt is made to logon; the greater the number of unsuccessful attempts, the longer the userid/terminal is locked.	<i>Retry maximum on page 3.22 (Vol 1). Defining terminals to NC-PASS on page 3.14 (Vol 1) and User profile creation on page 3.20 (Vol 1).</i>
To stop access to the system outside of normal hours.	You can specify date/time restrictions for all or specified userids and all or specified terminals.	<i>Risk profiles overview on page 3.5 (Vol 1) and Chapter 7 - Restricting access by date and time (Vol 1).</i>

Identifying audit requirements

NC-PASS audit facilities can help your installation detect attempted security breaches. NC-PASS allows you to specify your audit and reporting requirements. The following list identifies several audit objectives and how NC-PASS can be used to achieve them.

Objective	NC-PASS function	Refer to the Administration Manual...
Audit of attempts to access network resources	NC-PASS provides a powerful audit facility which allows you to specify which audit messages are to be logged and their destination.	<i>SME action auditing</i> on page 10.16 (Vol 1).
To monitor system messages	Each NC-PASS message has a predefined severity level. A message can be selectively routed, on the basis of its severity level, to its destination(s).	<i>Message routing</i> on page 10.4 (Vol 1).
Identifying unsuccessful attempts to perform a specified function	NC-PASS provides automatic message processing facilities which allow you to alter the severity of NC-PASS messages, or replace one message with another, if specified criteria are met. For example, if a warning message is issued to a particular user five times during a ten minute period, the severity of the message could be increased so a Netview alert would be issued and an alternative message could be displayed to the user.	<i>Automatic message processing</i> on page 10.7 (Vol 1).
Monitoring logon attempts	NC-PASS provides a facility to produce statistical reports detailing logon attempts.	<i>Logon statistics</i> on page 11.13 (Vol 1).

What the NC-PASS books contain

The following books are contained in the NC-PASS Authenticator product documentation set:

- NC-PASS Authenticator Installation Manual (this manual)
- NC-PASS Authenticator Administration Manual - Volume 1
- NC-PASS Authenticator Administration Manual - Volume 2
- NC-PASS Authenticator User Guide

This section provides brief details of the contents of each chapter.

Installation Manual

Chapter	Title	Contents
Chapter 1	Preparation	Discusses installation and upgrade considerations.
Chapter 2	Downloading NC-PASS	Describes how to download the files required to run NC-PASS and how to install the NC-PASS libraries.
Chapter 3	The VTAM environment	Describes the sample VTAM nodes provided, when they are required, and how to install the SME if required.
Chapter 4	System changes	Describes the security product source members and the changes that are required to your system.
Chapter 5	Starting NC-PASS	Shows how to start NC-PASS for the first time after installation and how to verify that the system has installed correctly.
Chapter 6	Post-installation considerations	Discusses a number of features that may be required.
Chapter 7	Applying fixes and zaps	Describes the Maintenance Program product and how to install and run it.
Chapter 8	Getting started	This chapter. Describes planning and implementation considerations, provides an overview of this book and describes how to use the on-line menuing system.

Administration Manual - Volume 1

Chapter	Title	Contents
Chapter 1	NC-PASS overview	Describes the NC-PASS Security Managers set of products and discusses the features and facilities of each component.
Chapter 2	Defining system parameters	How to set options that have a global effect on the system, eg how the date is displayed on panels, the data displayed at logon, defining printers etc.

Chapter	Title	Contents
Chapter 3	Controlling user access	Describes how to specify access restrictions based on <ul style="list-style-type: none"> - the supplied userid - the date and time of the request - where the request originated.
Chapter 4	Using risk profiles to control access	Discusses a number of access control objectives and how you can use risk profiles to achieve them.
Chapter 5	Token administration	Describes the token devices supported, how to set them up on the system and the various methods by which they can be assigned to users.
Chapter 6	Administering users from an external security database	Describes the advantages of storing NC-PASS data on an external security database and how this feature is implemented.
Chapter 7	Restricting access by date and time	Describes how to specify access restrictions based on specified dates or times or both, including specifying the requirement for token authentication at specified times.
Chapter 8	The VTAM Session Security Exit (VSSE)	Describes how the session management exit works and explains how to build and test control tables. For customers converting from NC-PASS 1.4, describes how to convert authorization tables to NC-PASS 2.0 control tables.
Chapter 9	Using VSSE to achieve access control objectives	Discusses and gives examples of using VSSE to protect resources.
Chapter 10	Auditing	Describes the various audit facilities within NC-PASS, eg message routing and message escalation. Explains SME audit messages and how to route and suppress them as required.
Chapter 11	Printing and displaying reports	Explains the system information required to print from NC-PASS and describes the various reports which can be produced, giving examples of each type of report.
Chapter 12	Remote administration via MHO	Explains how an administrator on one NC-PASS system can store or load a rule on another NC-PASS system.
Chapter 13	Batch administration	Explains the overall structure of all batch functions. Describes the purpose of each function, what input is required and what output is delivered.
Appendix A	VSSE field names and flags	Provides a complete list of all default VSSE field names and flags.

Administration Manual - Volume 2

Chapter	Title	Contents
Chapter 1	Communicating with other systems	Describes the three types of communication links, MHO, APPC and XMS. Shows how to define and enable the links. Describes the use of the mainframe as an authentication server for remote platforms.
Chapter 2	Transaction Level Interface (TLI)	Describes both high-and low-level interfaces between NC-PASS and application programs. This feature allows authentication to be carried out at the transaction level, thereby restricting access to sensitive transactions.
Chapter 3	Administration file backup and recovery	Describes how to re-create the ADMINDB file in the event of a disaster and subsequent loss of data.
Chapter 4	Customization	Describes how to customize logo panels, menus etc.
Chapter 5	Exit processing	Describes the exits available in NC-PASS and when they are invoked.
Chapter 6	Messages and abend codes	Describes NC-PASS messages, NCI messages and NCI abend codes.

NCI language statements

For information on NCI language statements, refer to the NCI/XF VTAM Toolkit documentation.

User Guide

For each supported token, the User Guide provides instructions on how to use tokens to access the system and, where applicable, how to set and change PINs. For those sites that enable user self-registration or replacement, step by step instructions are provided to guide the user through these procedures.

Using NC-PASS menus

As an administrator, you have access to the NC-PASS AUTHENTICATOR menu as shown below:

```
Date:12/12/1997          NC-PASS 2.0 AUTHENTICATOR          Userid:TSG0001
Time:09:00                                     Terminal:A01MS268

      Option => _____

                1 System Administration
                2 Operator Function menu
                3 Browse System Log
                4 Cross System Communications
                5 User profile Administration
                6 Terminal Administration
                7 VSSE options
                8 Token Administration

F1=Help  F3=End  F7=Up  F8=Down
```

Each option either provides a sub-menu (eg option 1) or an administration panel (eg option 3).

All menus are arranged in the same way, with an **Option** field at the top of the panel, and a list of available options below.

Selecting options

To select an option in most menus you normally enter an option number in the **Option** field and press <Enter>.

Some NC-PASS menus require two or more entries in the **Option** field. For instance, if you want to define a new user profile:

- select option 5 from the NC-PASS 2.0 AUTHENTICATOR menu to provide the USER PROFILE MAINTENANCE MENU
- select option 1 from USER PROFILE MAINTENANCE MENU by entering both the option number and the userid for the profile being defined.

You can optionally include another userid as a third entry to provide a model on which to base a new profile. This is shown in the sample panel below.

```
Date:12/12/1997          USER PROFILE MAINTENANCE MENU          Userid:TSG0001
Time:09:00                                     Terminal:A01MS242

Option => 1 TSG0123 MODUID

          1 Define a new user profile
          2 Change a user profile
          3 Delete a user profile
          4 Display a user profile
          5 List user profiles
          6 Userid risk profile
          7 Date and time definitions
          8 Process locked users
          9 Reset a users internal password
         10 Cancel passcode

F1=Help  F3=End  F7=Up  F8=Down
```

This entry would display panel PROFILE DETAIL FOR TSG0123 prefilled with the same profile details as userid MODUID.

The NC-PASS menus which require two or more entries in the **Option** field are as follows:

- USER PROFILE MAINTENANCE MENU (5)
Options 1, 2, 3 and 4 of this menu require both the option number and a userid to be entered (option 1 can also include a model userid).
- SYSTEM ADMINISTRATION MENU (1)
Option 7 of this menu requires both the option number and a panel name to be entered.
- TERMINAL ADMINISTRATION MENU (6).
Option 5 of this menu requires both the option number and a member name to be entered.

Fastpath menu skipping

Consecutive menus can be skipped by entering the menu option numbers at the **Option** prompt and separating the numbers with a period. For example if you want to go to the MESSAGE ROUTING panel directly from the NC-PASS 2.0 AUTHENTICATOR menu, enter:

1.3.1

and press <Enter>.

If you have selected a menu and wish to transfer to a panel which is provided by another menu, you can go directly to the new panel by entering the equals sign (=) at the **Option** prompt (to start the option path at the top level menu) followed by the option path from that menu.

For example, if you wish to go to the MESSAGE ROUTING panel directly from the SYSTEM FUNCTION MENU, enter:

=1.3.1

The equal sign effectively starts a selection sequence from the NC-PASS 2.0 AUTHENTICATOR menu, and the numbers 1.3 and 1 select the MESSAGE MAINTENANCE MENU and the MESSAGE ROUTING panel respectively.

Panel referencing in this manual

To provide a method of referencing panels within the text of this manual, panel titles are appended with the sequence of options (in brackets) that are required to access the panel from the NC-PASS 2.0 AUTHENTICATOR menu. For example, the MESSAGE ROUTING panel is referenced (1.3.1) and the LIST MENU DEFINITIONS panel is referenced (1.8).

Making changes to panel data

Some administration panels require you to use the line editor to add or amend information on a panel. This section provides a guide to using the line editor commands.

Using the line editor

Enter the appropriate line commands on the lines to which they apply by overtyping the editor-generated line number. These commands are primarily concerned with the manipulation of the text lines. The following standard edit line commands are available in selected NC-PASS panels.

C	- Copy line	M	- Move line	MM	- Move block
CC	- Copy block	A	- After	B	- Before
I	- Insert line	R	- Repeat line	RR	- Repeat block
D	- Delete line	DD	- Delete block		

Copying and moving

Use the COPY and MOVE line commands to reformat the page being edited by moving or copying single lines or numbers of lines. Type an M (MOVE) or C (COPY) command against the first line to be processed. Define blocks of text by specifying the MM or CC commands at the beginning and end of the block. Move the text to a destination identified as being A (AFTER) or B (BEFORE) any other text line (except a line within the block being copied or moved).

M	places the selected text at the specified location and removes the original line(s).
C	places the selected text at the specified location and retains the original line(s).

The source and target locations for a move or copy operation can be on different pages. To move or copy text across pages, first identify the text to be moved or copied by inserting M or C commands in the appropriate places. Having marked the text to be processed, scroll through the remaining text until the target point is displayed on the screen. Enter an A or B command to cause the marked text to be moved or copied.

Multiple Move and Copy

You can perform multiple move and copy operations at the same time, provided all text has a common target destination. You can specify these commands as part of a single move/copy operation and can mix move and copy operations, provided that block commands do not overlap.

No moving or copying of text takes place until you enter a B or A line command. You can enter as many C or M line commands as you require to identify multiple lines or blocks of text to be passed to a common location. Selected lines will be identified by the words MOVE or COPY appearing in place of the line numbers.

When you enter a B or A command, all the stacked M and C commands will be processed and the appropriate text placed at the target location. Stacked M and C commands are processed one after the other, starting from the top.

You can automatically repeat copied or moved text after insertion at the target point by specifying a numeric suffix to the B or A command to indicate the number of times the text is to be repeated.

Excluding lines

The block move/copy facilities provide a powerful tool for manipulating and formatting text. However you may want to process a large block of text, **excepting** a few of the lines within the block. The line editor provides this facility by allowing specific lines to be excluded from a block M or C operation.

No text manipulation is performed until you enter a B or A command. As you enter each M and C line command, the source lines are marked for moving or copying by the words MOVE or COPY replacing the line numbers.

You can exclude lines from a block move or copy operation by removing the words MOVE or COPY before entering the final B or A command. When the stacked move/copy commands are processed, only those lines with the MOVE and COPY identifiers in their line number field will be processed.

You can combine this technique with the use of multiple move/copy commands, as previously described, to enable sophisticated and powerful text manipulation in a single pass.

Inserting

There are two commands available for adding new lines. The most appropriate command to use will depend on whether or not you want unused new lines to be removed. Use the INSERT line command to insert single or multiple lines.

To insert a line, enter the single character I in the line command area. When you press <Enter>, a new line is generated immediately after the line containing the insert command. You can insert a number of lines by specifying a numeric value after the I command to indicate the number of new lines required. You can also generate blank lines by using this command. Enter an INSERT command, as normal, then enter a SPACE character on the line or lines which are to be left blank.

If you have specified the insertion of trailing blanks, either by default or as a result of a NULLS OFF command, the inserted line(s) will be prefilled with blanks (hex '40'), otherwise the new lines will contain nulls (hex '00').

If you enter text into any of the inserted lines, the lines will be assigned line numbers and become part of the panel when you press the <Enter> key. Inserted lines into which no text has been entered will be automatically removed the next time you press <Enter>.

Repeating lines

Use the R (REPEAT) line command to copy and insert a line of text immediately after itself. A line can be repeated any number of times. You can repeat a block of text by entering RR in the command area at the start and end of the block.

Deleting

Use the DELETE line command to delete single or multiple lines.

To delete a line, enter the single character D in the line command area, overtyping the line number. You can delete multiple contiguous lines by following the D command with a numeric value which indicates the number of lines to delete, starting with the line containing the command.

To delete a block of text the characters DD are entered in the line command area (again overtyping the line number) at the beginning and the end of the block.

Multiple INSERT and DELETE commands may be entered and will be processed from the top down.

This page intentionally left blank

Index

A

APPC

- node definition 3.2
- requirement for NCP gen 3.3
- requirements 3.3

authorization control table conversion 5.7

authorizing the load library 4.3

B

backing out the SME 3.9

C

CODE= parameter, PSOPT 5.3

console commands 6.5

controlling NC-PASS 6.5

conversion from previous versions 5.7

CPYPASS flag 2.3

D

DEFVSAM member 6.2

DEFVSAM2 member 6.2

E

ESE0032 panel 6.2

F

F command (MVS) 6.5

fastpath menu skipping 8.11

fixes

- applying 7.2
- backing out 7.3
- hardcopy 7.3

G

global options, converting from NC-PASS 1.4 5.7

H

HELP text, where held 2.3

I

IEALPAVE member 3.7

IEFBR14 flag 2.3

INSTALL dataset 2.2

installation

- considerations 1.2
- JES3 2.5
- NC-PASS libraries 2.3
- post-installation considerations 6.2
- providing information for 1.5
- security product interfaces 4.2
- verification 5.8
- VTAM environment 3.2

IPL requirements 4.3

ISTEXCAA exit

linking 3.8

J

JES3 installation 2.5

L

libraries, installation of 2.3

line editor 8.12

linking ISTEXCAA exits 3.8

LINKUS1 3.8

LINKUS2 3.8

load library, authorization 4.3

logging on for the first time 5.5

M

Maintenance Program product

see MP

MASTER userid 5.5

menus

- fastpath skipping 8.11
- how to use 8.9
- selecting options 8.10

messages

CKUT0692-4 5.5

CKUT0694-4 5.5

CKUT0697-4 5.5

messages, MP 7.5

MESSAGES, where held 2.3

MHO node definition 3.2

MODIFY(F) and STOP(P) commands 6.5

MP

error messages 7.5

installing 7.3

output from 7.5

using 7.2

N

NC-PASS

controlling 6.5

libraries, installation of 2.3

logging on for the first time 5.5

menus, how to use 8.9

node definition 3.2

planning for 8.2

running under a session manager 6.2

starting 5.2

trial mode facility 6.2

node and ACB definitions 3.2

O

operator commands 6.5
operator console commands 6.5

P

P command (MVS) 6.5
panel referencing 8.11
PAS1 3.9
PASS node definition 3.2
PASSAPPC node definition 3.2
PASSIAMS member 2.3
PASSINST member 2.4
PASSJCL member 5.4
PASSMHO node definition 3.2
PASSMNT member 2.4
 replacing PASSINST 2.4
PASSMNT2 member 2.4
 converting global options 5.7
Passplex 2.4
PASX 3.9
PBLIB fixes, applying 7.2
PROD-MODE startup parameter 5.3
PSDELETE member 6.2
PSOPT member 5.2
PSREPRO member 6.2
PSTDT member
 changing panel names in 6.2
 reviewing at startup 5.2

R

RACF
 authorizing load libraries 4.2
 security product interface 4.2
Record Level Sharing 2.4

S

SEACF2 source member 4.2
SecurID tokens, loading external data 6.3
security products
 changes to your system 4.2
 re-assembling source members 4.2
 source members 4.2
SEEXCAAA 3.6
SEEXCAAB 3.6
SEMOTAB sample 3.3
SEPORT sample 3.3
SERACF source member 4.2
SESAC source member 4.2
SESMPA job 2.3
SESMPB job 2.3
SESMPC job 2.3
SESM Pins job 2.3
session management exit
 see SME
session manager, running NC-PASS under 6.2
SETOPS source member 4.2
SEUSSTAB sample 3.3
SEVTAM member 3.2

shutdown
 from the system console 6.5

SME

backing out the exit during install 3.9
installing
 SEEXCAAA 3.6
 SEEXCAAB 3.6

SMP/E installation

 region size for 2.3

SSCT, NC-PASS names 3.9

starting NC-PASS 5.2

startup parameters

ACBNAME 5.2
BACKUP-WAIT 5.3
CODE 5.2
CONNECT-MESSAGE 5.2
EXTENDED-MODIFY 5.2
LOG-PAGE-LENGTH 5.2
NON-SWAP 5.2
PANEL-STORAGE 5.2
PROD-MODE 5.3
RECOVERY-ON 5.3
updating 5.2

STOP(P) and MODIFY(F) commands 6.5

stopping NC-PASS with the P command 6.5

Sysplex 2.4

system console, controlling NC-PASS from 6.5

T

TDT, options 6.2

Terminal Definitions Table

 see TDT

TOKEN=SD startup parameter 6.3

trial mode facility 6.2

U

upgrading, introduction 1.4

V

verifying the installation 5.8

VSSE exit check 5.8

VTAM

 APPC node definition 3.2

 installing the Session Management Exit 3.4

 MHO node definition 3.2

 restarting after APPC definition 3.3

X

XMS1 3.9

Z

zaps 7.2

ZJES31 member 2.5

ZJES32 member 2.5

ZJES33 member 2.5

Reader's Comment Form

If you find any discrepancy in the information contained in this publication, please complete this form and mail it to the address below.

The authors may use, or distribute, any of the information you supply in any way they consider appropriate without incurring any obligation whatsoever.

Publication number PAI0001.003 - Third Edition (October 2001)

Please write your comments below and on the following page and return this form to the

Documentation Manager
PassGo Technologies Ltd.
Horton Manor
Ilminster, Somerset
TA19 9PY
England

Reader's Comment Form

N
C

P
A
S
S

A
u
t
h
e
n
t
i
c
a
t
o
r

I
n
s
t
a
l
l
a
t
i
o
n

M
a
n
u
a
l