

Administration Manual - Volume 1

NC-PASS Secure
Version 2.0

MVS Operating Environment

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

Publication number PSA1001.003

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 administrative procedures for the startup and running of NC-PASS Secure.

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

NC-PASS Secure Administration Manual - Volume 1 (this manual)

NC-PASS Secure Administration Manual - Volume 2

NC-PASS Secure Installation Manual

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 security and administrative staff who are responsible for the protection of system resources.

NC-PASS Secure 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 manual 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 Secure 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
PS20.TNL002	Restructured menus
PH203.TNL003	Efficiency improvements
PH203.TNL004	RACF Passticket support
PH202.TNL003	The NC-PASS TCP/IP interface
PH202.TNL005	Encryption of transmissions over APPC and TCP/IP
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 NC-PASS overview

Chapter 2 Defining system parameters

Chapter 3 Controlling user access

Chapter 4 Using risk profiles to control access

Chapter 5 Administering users from an external security database

Chapter 6 Restricting access by date and time

Chapter 7 The VTAM Session Security Exit (VSSE)

Chapter 8 Using VSSE to achieve access control objectives

Chapter 9 Auditing

Chapter 10 Printing and displaying reports

Chapter 11 Remote administration via MHO

Chapter 12 Batch administration

Appendix A VSSE field names and flags

Index

Table of contents - Volume 2

Preface

Chapter 1 Communicating with other systems

Chapter 2 Transaction Level Interface (TLI)

Chapter 3 Administration file backup and recovery

Chapter 4 Customization

Chapter 5 Exit processing

Chapter 6 Messages and abend codes

Index

This page intentionally left blank

Chapter 1 - NC-PASS overview

NC-PASS Network Security Managers	1.2
Network entry level protection	1.2
Application/transaction protection	1.3
Product profiles	1.4
NC-PASS VSSE	1.5
How does it work?	1.5
NC-PASS Secure	1.7
How does it work?	1.7
NC-PASS Authenticator	1.13
How does it work?	1.13

NC-PASS Network Security Managers

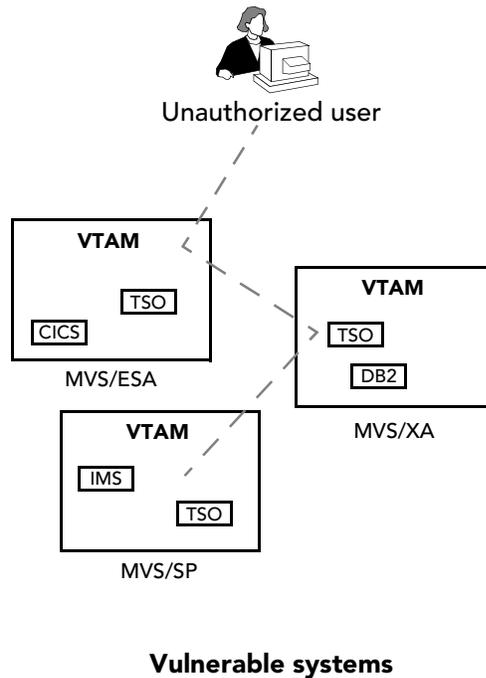
Whether you require security for your entire mainframe network or a single transaction, NC-PASS Network Security Managers provide a wide range of user authentication and access controls.

NC-PASS Network Security Managers give you the ability to authenticate users via any of the seven leading dynamic password tokens at three levels:

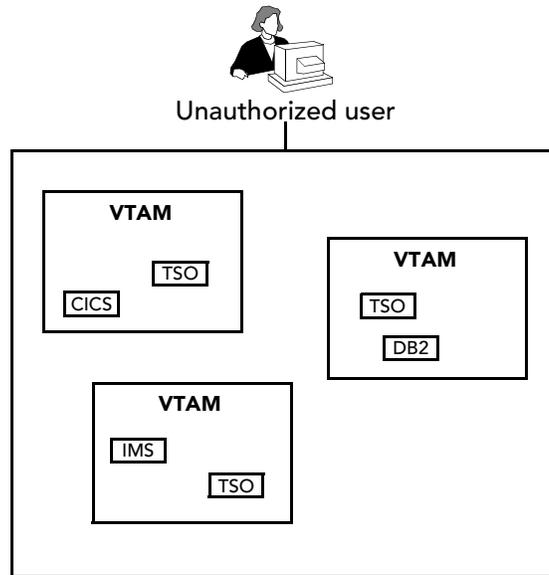
- network entry
- application selection
- transaction.

Network entry level protection

Resource security systems do not protect your mainframe network. Anyone can enter a network, roam around at will and probe for weaknesses.



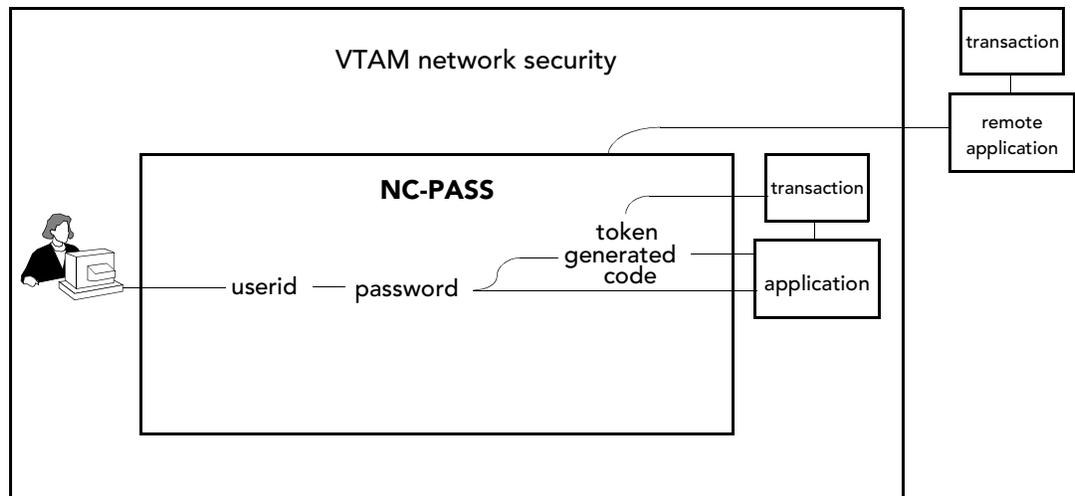
NC-PASS Network Security Manager products extend security defenses from the kernel of the individual mainframe systems to the network periphery so users are validated before they enter the network.



Mainframe protection at network level

Application/transaction protection

NC-PASS Network Security Manager products protect information by directing the user via userid and password to permitted applications only. In addition, you can force users to provide additional personal token authentication information either at the application level or the transaction level or both.



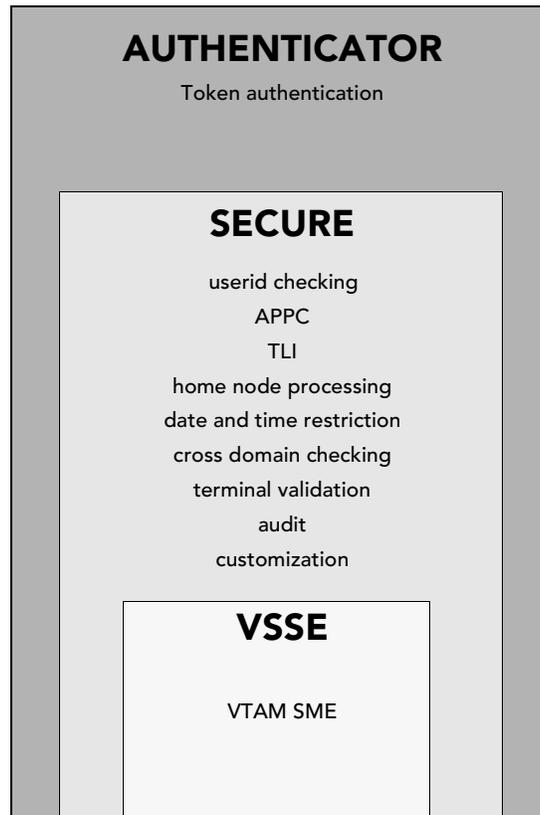
Product profiles

The NC-PASS Network Security Managers range comprises the following products:

Product	Operating environment
NC-PASS Authenticator	MVS
NC-PASS Secure	MVS
NC-PASS VSSE	MVS

MVS based products

On MVS systems, the three levels of NC-PASS are shown below. All the features of a lower (inner) level are available at the higher (outer) level; therefore NC-PASS Secure incorporates all the features of NC-PASS VSSE and NC-PASS Authenticator incorporates all the features of NC-PASS Secure:



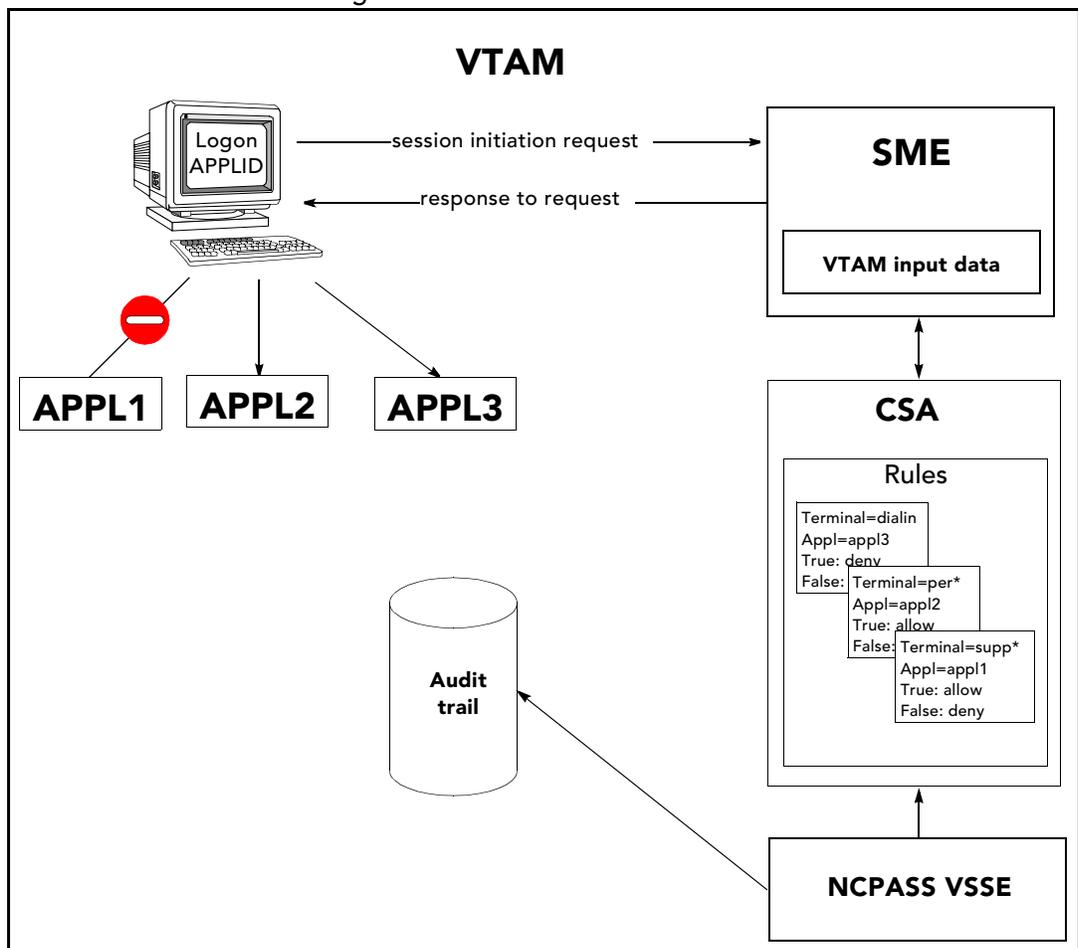
Details of each product are provided in this chapter.

NC-PASS VSSE

NC-PASS VSSE (VTAM Session Security Exit) utilizes the Session Management Exit (SME) provided by VTAM to control which LU to LU sessions VTAM will allow or deny. This includes terminal to application, application to printer, peer to peer and Network Job Entry (NJE) sessions. Only authorized connections can take place as defined in NC-PASS VSSE.

How does it work?

At the establishment of any VTAM session, the SME references the VSSE rules table stored in the Common Storage Area (CSA). This table has been defined by the administrator using NC-PASS on-line administration panels. The SME matches entries in the rule table against the session information provided by VTAM and allows or denies the session according to the rules.



Features

NC-PASS VSSE enables you to:

- control network access and routing, including access from dial-in lines and specific terminals
- prevent network jumping by allowing you to deny traffic based on originating or destination network
- restrict network access to specific times and dates
- identify breaches in security with the powerful audit and message escalation features of NC-PASS
- make immediate on-line updates - no need to restart VTAM when changes are made
- use the supplied TEST facility to 'dry run' your control system before it is used in production.

Therefore NC-PASS VSSE offers a more powerful and easy to administer alternative to an in-house written SME, with the benefit of full support from PassGo Technologies Ltd.

NC-PASS Secure

NC-PASS Secure provides active network security and protection of information by directing the user, via userid and password to permitted applications only.

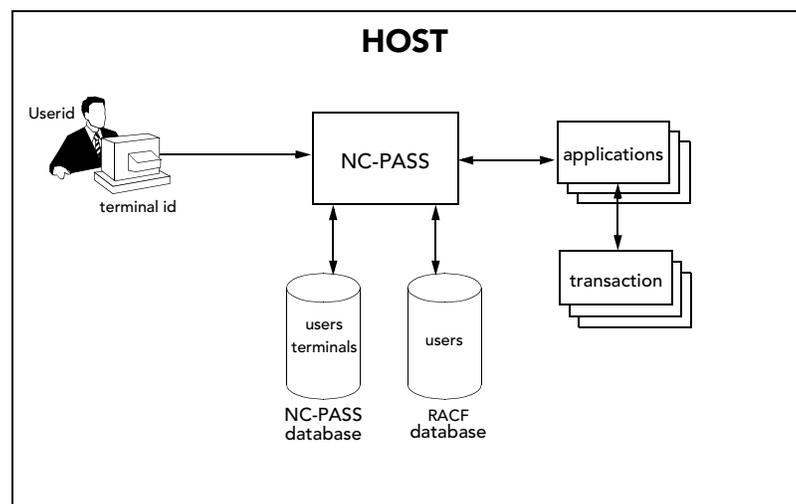
Incorporating all the features of NC-PASS VSSE (see *NC-PASS VSSE* on page 1.5), NC-PASS Secure adds a further feature to VSSE rule checking, allowing sensitive applications to be userid protected.

How does it work?

NC-PASS Secure validates each user ensuring that each user is allowed access to appropriate and necessary data only.

The NC-PASS database

NC-PASS has a central database containing access control information for the users and terminals using the system. The basic NC-PASS environment, providing database access from a single processor system, is illustrated below.



Records containing sensitive data in the database are protected by a cryptographic checksum, to prevent unauthorized modification of stored information. Any existing security system residing on the computer (eg RACF) will provide an additional level of protection for ultimate database security.

Some user profile information can be stored on the RACF database to reduce the duplication of entries on the NC-PASS database thereby reducing the security administrator's workload.

User hierarchy

Three types of user can be defined to the NC-PASS database:

- Administrators (A)
- Operators (O)
- Users (U).

An Administrator can define new users and change the access control information for existing users; therefore in the most secure environment only a minimal number of administrators should be defined.

If this is not feasible, you can define a hierarchical structure consisting of authority groups in which administrators, operators and users may be assigned one of 255 authority levels.

Any number of groups can be created to distribute administrative responsibility, and if required, an administrator can be assigned an overall group authority to provide access to all defined groups. An administrator can use all administration and operator functions and also use the security interface function itself to connect to another application.

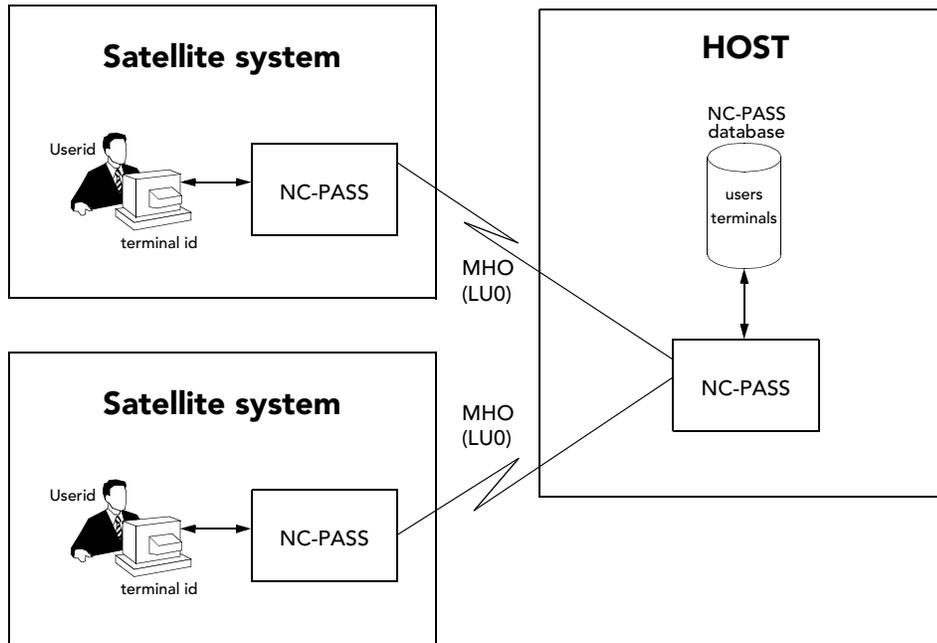
An Operator can access the operator function menu to perform tasks such as system shutdown, backup of the NC-PASS database, and under certain conditions (set up by the administrator) can also use administration functions. The default menus, however, do not allow an operator to access the administration panels. Menus can be tailored to individual access requirements.

A User has no access to operator or administrator functions.

Centralized authentication

NC-PASS can be run on a single host system with a database containing access control information for users on other nodes in the network. External users are routed to the host system for authentication.

This allows all administration to be performed at a centralized site as shown in the diagram below.

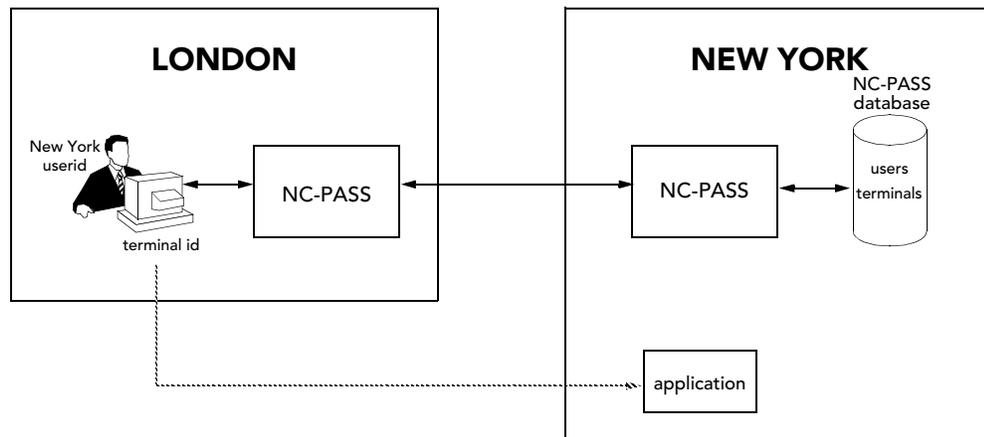


Home node processing

In multi-node networks, NC-PASS databases may be held on individual nodes supporting definitions for users and terminals assigned to that node. Users connecting to a node that is not the machine they would normally connect to, can specify the name of the machine where they want to be authenticated.

This feature, known as Home Node Processing, is useful on large networks where users normally access the system from their own node, but may occasionally travel to other offices and want to gain access.

The multi-node method also avoids unnecessary duplication of definitions across systems, and reduces administration.



In the same way, administrators wishing to use administration panels on their home node may gain access from any other node.

The Transaction Level Interface (TLI) can be used to make the Home Node Processing facility available to front end applications. Refer to *Using the TLI to request Home Node Processing* on page 3.48.

Features

NC-PASS Secure incorporates a number of access control features, a summary of which is described below.

Administration

NC-PASS provides a flexible and easy-to-use administration system through an on-line menu-driven interface. As an option, multiple administration menus can be defined to restrict commands to different administrators.

Audit

Flexible audit facilities are provided to ensure attempted breaches of security are not only stopped but recorded too.

All administration and access function messages are written to NC-PASS logs and may optionally be written to the system console for on-line browsing. Fast retrieval of potentially important messages, such as logon failures is therefore provided.

Actions can also be selectively audited depending on frequency within a given period.

Authentication with NCI/XF

Users of NCI/XF can use NC-PASS exit routines to authenticate users and perform VTAM authorization against authentication bypass.

Controlled environment

Once a terminal is connected to NC-PASS it remains in a controlled environment until authentication is complete. A user cannot exit the authentication system without operator or system programming involvement until verification has completed.

The system is based on controlling the sessions allowed on the network and seeking additional verification of the user's identity. The central administration of complex networks, provided by NC-PASS maximizes security and reduces administration overheads.

Customization

NC-PASS is written in the NCI language, ensuring easy customization to your requirements.

Date and time restrictions

Userids, terminals and applications can be protected from access at specified times or dates.

Interface with major access control systems

NC-PASS Secure supports all major access control systems. Resident security products such as RACF, CA-ACF2 and CA-Top Secret are invoked to verify userids and passwords before access is allowed.

Protection against authentication bypass

In a network where not all nodes are protected by NC-PASS, the potential for bypassing authentication exists. If a user on an unprotected node issues logon commands to an application within a protected node, access to the application may be granted without authentication.

To prevent this occurring NC-PASS provides the VTAM Session Security Exit (VSSE) to ensure that all access to applications has been authorized by NC-PASS.

NC-PASS Secure provides additional protection against users of dial-in terminals presented with USSTAB, by acquiring such terminals before system access is allowed.

Test copies of NC-PASS could be used to force unauthorized entry; to prevent this possibility occurring, you can define NC-PASS so it cannot run concurrently with copies of itself.

Reporting

NC-PASS Secure provides a facility to extract detailed information from records in the Central Administration File (CAF), such as user profiles and terminal profiles.

Storing authentication data on external security databases

There is a facility to store some userid profile information on the RACF database thereby reducing duplication of this information onto the NC-PASS database with a corresponding reduction in the security administrator's work.

Terminal control

In addition to network security and authorization, NC-PASS Secure provides the facility to control access to the network based on terminal id.

Transaction level interface (TLI)

NC-PASS Secure gains considerable flexibility by extending all the security features beyond the VTAM network front end to the transaction level. Validation or authentication of the user through the TLI can be implemented at any point. This is achieved through communication to the main NC-PASS job, so all administration, auditing and control functions are available.

Two types of TLI are provided; those that use the Cross Memory Services (XMS) component of NC-PASS and those that use the Advanced Program to Program Communications protocol (APPC).

TLI can also be used to protect sensitive transactions, such as challenging a user attempting to raise an insurance claim payment in excess of a certain value, by requesting userid and password validation from within the transaction.

Users can be checked as to whether and when they were authenticated so the administrator can insist any transaction is restricted to authenticated users or that the user is re-authenticated.

The audit facility allows any action in an MVS VTAM network to be audited centrally giving a complete picture of users' access to a network including the applications and transactions used.

Trusted front end

NC-PASS Secure, when running with VTAM version 3.4.1 or above can allow cross domain access to users only from an authorized front end such as NC-ACCESS SPE or TPX. NC-PASS Secure pre-notifies the SME to allow a cross domain session from a trusted front end. All other attempted cross domain sessions can be denied.

NC-PASS Authenticator

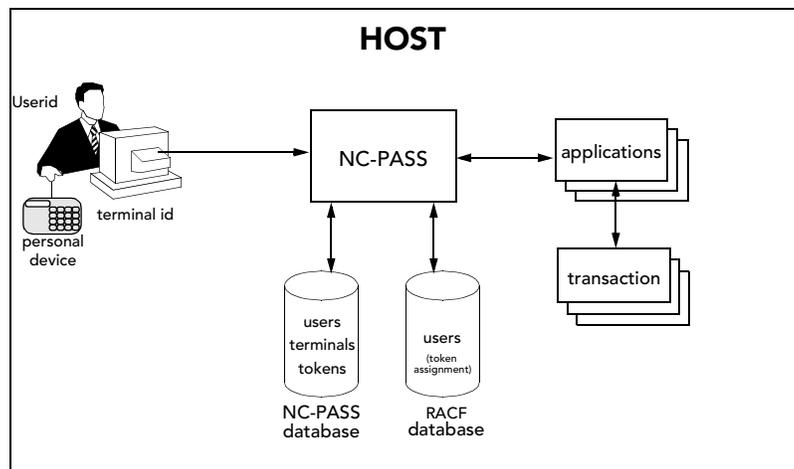
NC-PASS Authenticator incorporates all the features of NC-PASS Secure (see *NC-PASS Secure* on page 1.7) and adds the capability of authentication using personal devices. It is now generally agreed that in order to validate a user's identity, three items are required - most frequently, a userid, a user-changeable password and a personal device generated code.

The idea of a user providing at least three items is the basis of security within NC-PASS Authenticator. Once this level of security is in place, further extensions are possible. For example, before a personal code is provided, the generating device (or token) may require information only the user knows such as a personal identification number or PIN.

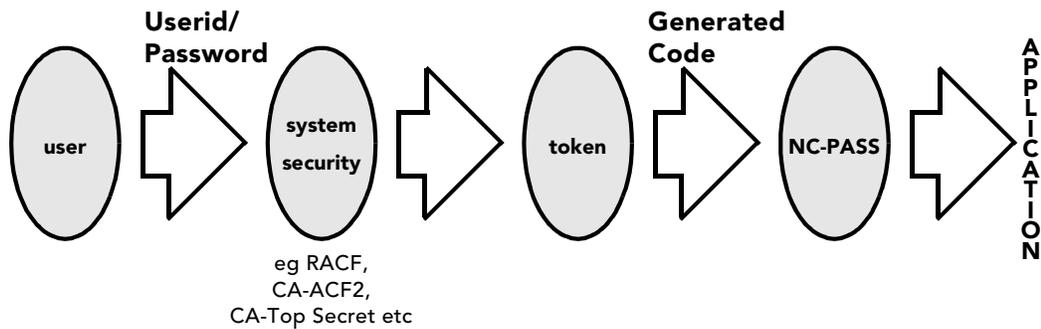
How does it work?

NC-PASS Authenticator supports several different personal devices or tokens, all of which provide a code to be input when additional authentication is required, either at logon or when requested by TLI to protect sensitive transactions or applications.

Information about these personal devices is also held in the NC-PASS database and, if required, token assignment information can be held in an external security database.



Essentially the devices either display a Pseudo Random Number (PRN) which the user must enter when challenged, or require entry of a PIN number, known only to the user, to provide a code for entry when challenged. In both cases possession of the token assigned to the userid in use is added to userid and password requirements to prevent unauthorized access.



Features

Assigning tokens to users

Tokens can be assigned to users

- by the administrator entering the userid(s) to be assigned to a specific token using the NC-PASS token administration panels
- by individual users using the NC-PASS self registration facility
- initiated by a token serial number stored on an external security database.

Forcing the use of a token device at specific times or dates

The administrator can force a user to be authenticated using a token at specified times, eg outside normal working hours.

Chapter 2 - Defining system parameters

Setting global system options	2.2
Using the GENERAL SYSTEM OPTIONS panel	2.2
Panel/userid toggle	2.4
Determining logon options	2.5
Using the LOGON DEFAULTS panel	2.5
VTAM printer definitions	2.7
Deleting a panel from storage	2.9
System shutdown	2.10
System statistics	2.11
General information	2.11
Storage use	2.12
VSM queues	2.13
Writing the statistics to the system log	2.14
Trace options	2.15

Setting global system options

You can set system parameters that will be actioned across the NC-PASS system as a whole.

Using the GENERAL SYSTEM OPTIONS panel

Use the GENERAL SYSTEM OPTIONS panel (1.1), shown below, to amend global system options.

```
Date:12/12/1997          GENERAL SYSTEM OPTIONS          Userid:TSG0001
Time:09:00              Terminal:A01MS242

General options:
Date format              => 3          1=YYYY/MM/DD 2=MM/DD/YYYY
                          3=DD/MM/YYYY 4=DDMMYYYY
Separator character      => /          Separates date elements for formats 1-3
Idle time                => 0          Specify idle time for administration and
                          logo panels before timeout occurs.
Length of log           => 999       The limit on the number of lines to be
                          retained in the NC-PASS message log
Concurrent systems      => Y          Enter 'Y' to permit other NC-PASS systems
                          to be started
Default user profile    => _____ When creating user profiles this name can
                          be used instead of a model name

External security options:
Default logon node      => _____ Default for remote node on logon
Accept RACF PassTickets => Y          Y/N
RACF PTKTDATA name     => TSOCK01

F1=Help  F3=End  F12=Can
```

Input fields

Field	Description
Date format	<p>Enter 1, 2, 3 or 4 to specify the required date format that you want to display on all NC-PASS panels. The day, month and year elements, for options 1, 2 and 3, are separated by a character defined in the Separator character field.</p> <p>The following examples show how August 12th 1997 would be displayed using each of the formats. The slash character (/) is used as a separator.</p> <ul style="list-style-type: none">(1) YYYY/MM/DD 1997/08/12(2) MM/DD/YYYY 08/12/1997(3) DD/MM/YYYY 12/08/1997(4) DDMMYYYY 12AUG1997 <p>Note: NC-PASS v2.0 supports dates beyond year 2000. All displayed dates contain the century in the first two digits of the year (eg 12/12/1997). This functionality is provided by all years with the last two digits 84 through 99 being preceded by 19, and all years with the last two digits 00 through 83 being preceded by 20.</p>

Field	Description
Separator character	If you have specified options 1, 2 or 3 in the Date format field, enter the character you want to separate the day, month and year elements in all NC-PASS displayed date fields.
Idle time	Enter the time in minutes that can elapse, when a terminal is inactive, before the user is automatically logged off. If zero is specified, this feature is disabled. This applies to both administration and logo panels.
Length of log	Enter the maximum number of lines to be retained in the message log. This is the NC-PASS log that can be browsed using option 3 of the ADMINISTRATION MENU.
Concurrent systems	Set to N to issue a system ENQUEUE (or lock) to prevent other NC-PASS systems running with this copy. This eliminates the risk of an unauthorized user gaining access via an alternative route. When this field is changed from N to Y a DEQUEUE (or unlock) is issued immediately, allowing other systems to run with this system. If the field is changed from Y to N, an ENQUEUE will be issued not immediately but when the job next starts up.
Default user profile	Enter the name of a default user profile to be used as a model when defining new user profiles. Refer to <i>Using another profile as a model</i> on page 3.20 for further details.
Default logon node	If required, enter the default node name to be displayed on the logon panel. A blank entry means that this node is the default.
Accept RACF PassTickets	Enter Y to allow the use of RACF PassTickets during NC-PASS authentication. NC-PASS will accept a RACF PassTicket, in place of a password, during administrator logon (typically via a terminal emulation product).
RACF PTKTDATA name	Enter the profile name which was defined to the PTKTDATA class on your RACF database for the NC-PASS application. If the value does not match that on the RACF database, RACF PassTickets will not be verified correctly. This field is only applicable if RACF PassTickets are accepted (see Accept RACF PassTickets field above).

Note: If you are using NC-PASS as a front end application to authenticate and connect users to other applications, you should be aware of the following restriction:

- if you design your system such that users logging on to NC-PASS are authenticated by a RACF PassTicket, this ticket cannot be used when connecting to other applications, since the PassTicket is a one-time only password. In this situation a null value will be passed as the password in the CINIT data for the application to be connected to.

Function keys

Key	Function
F1	displays help information.
F3	saves changes and returns to previous screen.
F12	Cancels changes and returns to previous screen.

Panel/userid toggle

Option 1.9 allows you to switch between the display of *Userid:* and *Panel name:* in the top right hand corner of your screen.

Determining logon options

You can specify a number of parameters that will determine the data required, and the information displayed, during the logon procedure.

Using the LOGON DEFAULTS panel

Use the LOGON DEFAULTS panel (1.2) to determine logon options, as shown below.

```
Date:12/12/1997          LOGON DEFAULTS          Userid:TSG0001
Time:09:00                Terminal:A01MS242

  Informational messages => Y Y/N    Should users see an explanation
                                of any logon failure.

  Default userid         => _____ Default user profile to be used
                                for acquire authentication.

  External user profile  => Y Y/N    Search external security database
                                to supplement user profile.

  Continue logon        => N Y/N    Should logon continue if
                                supplementary data is invalid.

F1=Help  F3=End  F12=Can
```

Input fields

Field	Description
Informational messages	Enter Y to provide the user with informational messages in the event of a logon failure; this shows the user the reason for the failure. Enter N to display only the message CKxx0461 ACCESS DENIED. In this case, you can consult the NC-PASS log to determine the reason the logon attempt failed.
Default userid	specify a default user profile to be used when NC-PASS acquires a terminal and the user has specified a userid that is not defined. This default userid can be used to restrict userid checking to the SME itself, rather than using NC-PASS. Refer to <i>Using ACQUIRE to protect sensitive applications from dial-ins</i> on page 8.10 for further details.
External user profile	enter Y to specify that when a user attempts to logon, a search is to be made for userid profile data on an external security database. This field is set to N when NC-PASS is installed. Refer to <i>Chapter 5 - Administering users from an external security database</i> for further details.

Field	Description
Continue logon	enter Y to specify that, if the logon process extracts data from an external security database and that data is invalid, the logon process will continue. Refer to <i>Chapter 5 - Administering users from an external security database</i> for further details.

Function keys

Key	Function
F1	displays help information.
F3	saves changes and returns to previous panel.
F12	cancel changes and returns to previous panel.

Function keys

Key	Description
F1	displays help information.
F3	saves changes and returns to previous panel.
F7	pages down the list of printer definitions.
F8	pages up the list of printer definitions.
F12	cancel changes and returns to previous panel.

Deleting a panel from storage

Before a panel can be processed, it must be found in storage; if it is not found, it must be LOADED from the panel library.

A panel or subroutine can be deleted from storage allowing an updated member to be loaded into storage the next time it is accessed. This facility is provided on the SYSTEM ADMINISTRATION MENU (1).

Select this option (7) from the menu, and provide the name of the panel to be deleted, by entering

7 panelname

at the **Option** prompt and pressing <Enter>.

This option is useful if a LOGO panel has been changed, since the logo can be updated without stopping and starting NC-PASS.

System shutdown

The SYSTEM SHUTDOWN panel (2.1) provides an immediate system shutdown facility.

If you are certain that the system is to be shut down enter Y at the **Confirm system shutdown** prompt, and press <Enter>. The system will be shut down immediately.

Alternatively, to return to the OPERATOR FUNCTION MENU without shutting the system down, leave the panel unchanged, and press <F3>.

```
Date:12/12/1997          SYSTEM SHUTDOWN          Userid:TSG0001
Time:09:00                Terminal:A01MS254

Type 'Y' below and press <ENTER> to shut down the system:
  Confirm system shutdown => Y Y/N

The system will shut down immediately. No warning will be given.

F3=End
```

System statistics

Choose option 4 from the OPERATOR FUNCTION MENU (2) to display system details under the following categories:

- general information
- storage use
- VSM storage.

You can also specify that the information displayed on these panels is written to the system log at regular intervals.

Press the <F10> and <F11> keys to display the next and previous panels respectively.

General information

General information on the current status of your system is provided by the SYSTEM MONITOR - GENERAL INFORMATION panel (2.4) as shown below.

```
Date:12/12/1997      SYSTEM MONITOR - GENERAL INFORMATION      Userid:TSG0001
Time:09:00          Terminal:A01MS262
                    NC-PASS Version 2.0 SECURE

Job CKPASS1Q NCI vers 4.1 XF System MVS 31BIT CPU id 112087 Region 4,096 Kb
  Prod-mode YES   Nonswap YES   Authorised YES

Startup on 12/12/1997 at 08:00      CPU seconds since startup SRB      19.264
                                          TCB      267.408
Current Panels in use                    Total      286.672
Current Execs in use                      475
Current system queues                     86   VTAM subarea 1      and ACB NODEPS
Current user queues                       14   VTAM buffer shortages
Current system variables                   215  RPL user field errors
Current user variables                     1246 Maximum concurrent Status calls
Total successful scavenges                 0   Maximum concurrent Status stg
Total failed scavenges                    0
Panels and execs deleted                   23  Active users        6

F3=End  F10=Previous  F11=Next
```

There are no entry fields in this panel. All fields provide information and most are self explanatory. Those which require further explanation are as follows:

Field	Description
Job	On an MVS system this is the JCL jobname executing NCI.
NCI vers	This indicates the release level of NCI running on this system.
System	This is the operating system that NCI is running under.
Prod-mode	This is the setting, either YES or NO, of the startup option PROD-MODE.
Nonswap	This is the selected NON-SWAP startup option which can be either YES or NO. The default for NC-PASS is yes.

Field	Description
Authorized	On an MVS system this indicates if NCI is running APF authorized.
VTAM ACB name	This is the name of the ACB that NCI is currently running under.
VTAM buffer shortages	This is the count of VTAM buffer shortages found by NCI.

Storage use

Press <F11> at the SYSTEM MONITOR - GENERAL INFORMATION panel (2.4) to display the SYSTEM MONITOR - STORAGE USE panel as shown below.

Date:12/12/1997		SYSTEM MONITOR - STORAGE USE		Userid:TSG0001	
Time:09:00				Terminal:A01MS262	
Region Size	4,194,304	All storage figures are in bytes.			
		Below 16-Mb.		Above 16-Mb.	
Total storage		1,053,944		3,185,064	
Maximum size storage free		3,047,424			
Program storage		537,352		64,640	
User queue storage				1386	
System queue storage				95,280	
Terminal control block storage				3,216	
Current Panel storage				1,368,072	
Highest Panel storage used				1,368,072	
Maximum Panel storage possible				10,485,760	
Total Getmain/Freemain SVC's issued	2840		SVC's bypassed	619762	
F3=End F10=Previous F11=Next					

There are no entry fields in this panel. All fields provide information and most are self explanatory. Those which require further explanation are as follows:

Field	Description
User queue storage	This is the total storage currently in use by NCI for user queues. If queue storage is allocated above the 16 MB line this figure will be preceded by 'X'.
System queue storage	This is the current amount of storage in use by NCI for system queues. If queue storage is allocated above the 16 MB line this figure will be preceded by 'X'.
Current Panel storage	This is the current panel storage. If panel storage is allocated above the 16 MB line this figure will be preceded by 'X'.
Highest panel storage used	This is the 'high water' panel storage in bytes (i.e. the highest level reached).
Total Getmain/Freemain SVC's issued	This is the total number of GETMAIN/ FREEMAIN SVC's issued by the Virtual Storage Manager (VSM).
SVC's bypassed	This is the total number of GETMAIN/ FREEMAIN SVC's bypassed by the Virtual Storage Manager (VSM).

VSM queues

Press <F11> at the SYSTEM MONITOR - STORAGE USE panel to display the SYSTEM MONITOR - VSM STORAGE panel as shown below.

```
Date:12/12/1997          SYSTEM MONITOR - VSM STORAGE          Userid:TSG0001
Time:09:00                Terminal:A01MS262

Virtual Storage Manager Queues

  BELOW 16MB
  QUEUE  USED   LEFT
  SIZE  ELEMENT ELEMENT
    8      9    119
   16     10   246
   24      0   128
   32     14   114
   40      0    64
   48      3    29
   56      0    16
   64      0    16
   72      1    15
   80      0    16
   88      2    14
   96      1    15
  104      0     8
  112      0     8

  ABOVE 16MB
  QUEUE  USED   LEFT
  SIZE  ELEMENT ELEMENT
    8      52   460
   16   3870   226
   24   4782   338
   32     88   168
   40     87   41
   48   1059   29
   56    112   16
   64     93  323
   72     16   80
   80     65   31
   88     28   36
   96    219  197
  104    549   11
  112     0   112

F3=End  F7=Up  F8=Down  F10=Previous  F11=Next
```

Each NCI variable is stored in a queue with elements of an appropriate byte length. Storage is accessed either below the 16 MB line (24 bit addressing) or above the 16 MB line (31 bit addressing). The above panel provides the following queue information

Below 16 mb This is the amount of data held below the 16 MB line, divided into queue byte lengths and the number of each queue length that is used or remaining.

Above 16 mb This is the amount of data held above the 16 MB line, divided into queue byte lengths and the number of each queue length that is used or remaining.

Writing the statistics to the system log

Press <F11> at the SYSTEM MONITOR - VSM STORAGE panel to display the SYSTEM MONITOR - LOGGING OPTIONS panel as shown below:

```
Date:12/12/1997      SYSTEM MONITOR - LOGGING OPTIONS      Userid:TSG0001
Time:09:00          Terminal:A01MS255

The information displayed on the System Information and Storage Use screens may
be sent to the log at regular intervals.

Activate Monitor      => N Y/N
Interval between logs => 60 minutes

Press <ENTER> to action changes

F3=End  F9=Browse Log  F10=Previous  F11=Next
```

Input Fields

Field	Description
Activate Monitor	Enter Y to write the information from the General information and Storage use panels to the system log.
Interval between logs	Only applicable if you have specified Y in the Activate Monitor field. NC-PASS will write the information to the log at specified intervals. Enter the time in minutes that is to elapse between each log of the information.

Press <F9> to browse the system log. Press <F3> on the system log browse panel to return to this panel.

Trace options

If you experience problems in the course of NC-PASS processing and you require help from your local support office, you may be asked to provide VTAM tracing information at the earliest opportunity.

NCI tracing is ideally performed with two terminals active; the terminal on which the problem has occurred, and a terminal on which an administrator can enter trace commands. The appropriate trace commands can be entered on the TRACE OPTIONS panel (2.5) on the administrator's terminal.

Note: This panel is normally used only on advice from your PassGo Technologies support office.

This page intentionally left blank

Chapter 3 - Controlling user access

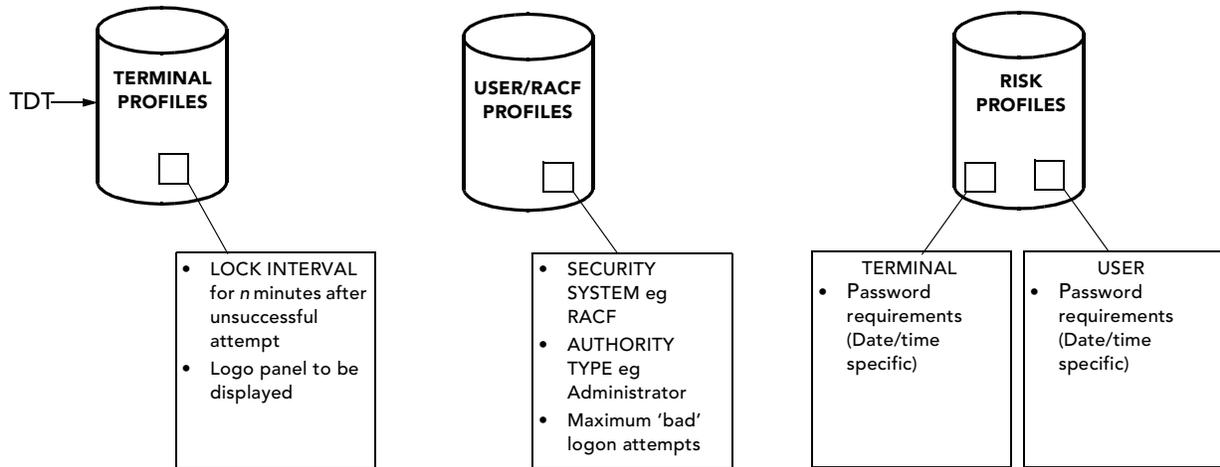
Introduction	3.2
Terminal profiles overview	3.3
User profiles overview	3.4
Risk profiles overview	3.5
Verifying a user	3.12
Defining terminals to NC-PASS	3.14
The TDT	3.14
Terminal profiles	3.17
User profile creation	3.20
Using another profile as a model	3.20
Profile definition	3.21
Profile deletion	3.25
Specifying connection routes	3.26
Listing user profiles	3.29
Printing user profiles	3.31
Terminal risk profile creation	3.33
Entering terminal risk data	3.33
User risk profile creation	3.35
Entering user risk data	3.35
Locking userids and terminals	3.37
Locked users	3.37
Locked terminals	3.39
Escalated terminals and users	3.42
Resetting escalated terminals and users	3.43
Example	3.44
PassTickets	3.45
Why are PassTickets used?	3.45
Further information	3.45
Configuration	3.45
Home node processing	3.47
Using the TLI to request Home Node Processing	3.48
Processing considerations	3.59
Audit	3.59
TLI Home Node Processing between different versions of NC-PASS	3.59

Introduction

NC-PASS provides the facility to set up a number of profile records which will allow or deny system access depending on various criteria. The data that NC-PASS expects the user to provide for authentication at logon time depends on the data specified in these profile records:

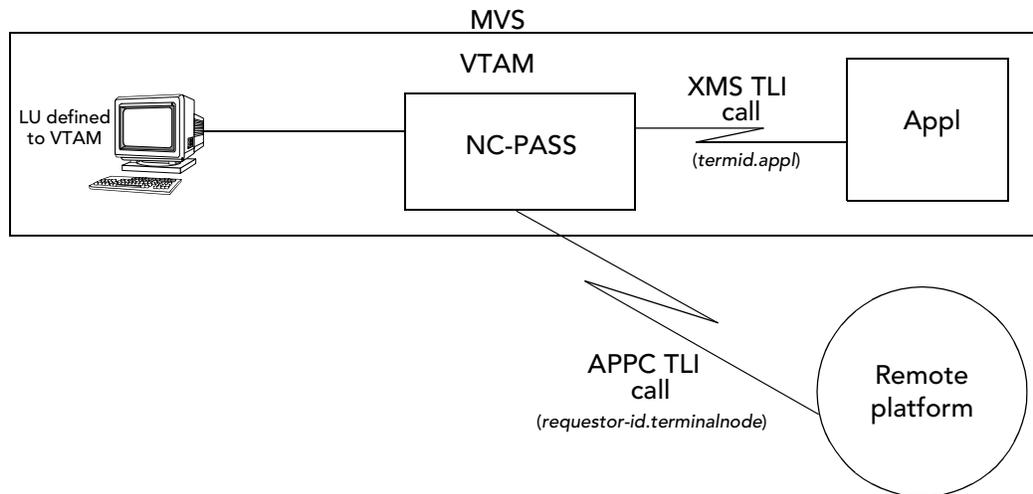
- terminal profile
- user profile (and optionally RACF profile)
- risk profile

Each of these profile types is described below and on the following pages. A diagram explaining how NC-PASS uses these profile records when verifying a user is provided on page 3.12. The following diagram shows the type of information stored in each profile type.



Terminal profiles overview

A terminal profile can be created for two categories of terminal, real terminals and imaginary terminals. In this context, a terminal is therefore a generic access route as shown in the diagram below:



Real terminals

A real terminal is a physical terminal for which there is a VTAM luname. This includes virtual terminals. Real terminals are defined to NC-PASS through the Terminal Definitions Table (TDT). Entries in the TDT can either

- specify which logo panel will be displayed to the user attempting to log on from this terminal
- or
- point to a terminal profile record in which you can specify
 - the logo panel to be displayed when a user logs on from that terminal
 - a temporary lock period to be used if a user has a number of unsuccessful logon attempts from that terminal.

Any real terminal not specified in the TDT, either specifically or by a generic or masked entry, will not be allowed to connect to NC-PASS.

Imaginary terminals

If an application makes a call to NC-PASS using an XMS Transaction Level Interface (TLI) function, the TLI call includes parameters specifying the terminal id and application nodename relating to the calling transaction. You can therefore specify an imaginary terminal id in the format *termid.appl*.

If an application makes a call to NC-PASS using the APPC Transaction Level Interface (TLI) function, the TLI call includes parameters specifying the network id and nodename. You can therefore specify an imaginary terminal id in the format *requestor-id.terminalnode*.

For details of the XMS and APPC TLIs, refer to *Chapter 2 - Transaction Level Interface (TLI)* (Volume 2).

You would define a terminal profile entry for an imaginary terminal only if you wanted to specify a temporary lock period for that access route (which would be actioned if an unsuccessful attempt was made from that access route).

User profiles overview

User profile records allow you to define a list of userids (specific or generic) from which access attempts are permitted. Users can only be validated using userids for which a profile record exists.

A user profile controls the user's access to specific systems. Additional security can be provided by limiting the number of unsuccessful logon attempts a user can make. Some of the restrictions that can be imposed on userids are listed below. Some of this information can be stored on a RACF database: refer to *Chapter 5 - Administering users from an external security database* for further details.

Access period restrictions

It is possible to set up a userid in advance but specify that it cannot be used until a given date. Similarly a cut off date after which access will be denied can be set up. This would be useful for example for userids set up for contract staff.

Password validation

Support for CA-ACF2, RACF, SAC, CA-Top Secret or internal password processing is provided by NC-PASS.

Authority options

Userids can be set up as one of three types:

administrator	has access to all NC-PASS functions
operator	has access to a limited range of NC-PASS functions
user	will normally use only the security interface and will not be allowed access to administrator or operator functions.

If initial menus have not been set up, administrator and operator ids will be presented with default menus at logon which allow access to the NC-PASS functions for which they are authorized. A user may have an initial menu defined but cannot access administrator or operator functions from it. See *The default NC-PASS menu structure* on page 4.13 (Volume 2) for full details of the default menus available.

Individual userids may be assigned to authority groups by administrators for ease of maintenance.

Administrators are also assigned an authority level and can only administer userids at an equal or lower level than themselves.

Connection routes

After a successful logon, a user can be routed to a specific application.

Maximum logon attempts

You can specify the maximum number of unsuccessful logon attempts a user can make before the userid is locked out. The userid will remain locked until the administrator unlocks it allowing it to attempt logons again.

Lock periods

You can specify a temporary lock period following an incorrect logon attempt by a user. The lock period increases at each unsuccessful attempt. This prevents quick random 'guessing' of passwords.

Risk profiles overview

The objective of a risk profile is to enable you to specify the appropriate validation requirements given the following three factors:

- the userid specified
- where the request originated (ie terminal id, or a TLI request)
- date and time of day of request.

For example, you may want to restrict a group of administrative staff, and the terminals in the administration offices, to system access during office hours only.

Risk profiles can therefore be created for those userids and access routes which you want to ensure are protected with the requirement for a password or token or both. You can store user risk data on a RACF database: refer to *Chapter 5 - Administering users from an external security database* for further details.

Risk profiles allow you to specify that the level of validation is higher at a specific time; for instance it is possible to prevent access at weekends by allowing access on Monday through Friday only. Within this period specific start and end times can also be defined, for example to allow access between the hours of 08:00 and 18:00 only. The two restrictions can be combined to allow access at different times on each day of the week.

Risk profiles are optional; if the appropriate user/terminal risk profile does not exist NC-PASS will use default validation. This is explained in *Keyword interpretation* on page 3.8.

A diagram explaining how NC-PASS uses these profile records when verifying a user is provided on page 3.12.

Specifying system risk information

This risk information is stored in two records, as described below.

User risk information

Typically, there will be a number of userids that have special privileges in your system; access to sensitive applications, supervisory authority over other userids etc.

Unauthorized use of these userids would be a serious security risk to your business and as such they need to be protected. The user risk profile allows you to specify these high-risk userids and the special protection they require, eg

- userid ADMIN1 cannot be used at weekends
- userid TECHSUPP must always be password authenticated.

Terminal risk information

In this context, a terminal is a generic access route. This can be:

- a real terminal
- a TLI request.

Refer to *Terminal profiles overview* on page 3.3 for an explanation of generic access routes.

Overall system risk

If specified, the risk values from both profiles are combined to determine the overall risk assessment; NC-PASS uses this combined assessment to determine the validation requirements for this access request.

User risk profiles

The following diagram shows a representation of a user risk profile record:

Userid	Date/time	B					C
		STATEHOL	WORKWEEK	EVENING	WEEKEND	OUTHOURS	
AD*		LOCK	,Y	,Y	LOCK	LOCK	
ADM*		LOCK	,Y	,Y	,Y	LOCK	
MKT*		LOCK	,D	,Y	LOCK	LOCK	
SYSSUP		,Y	,Y	,Y	,Y	,Y	,Y
TSG*		,Y	,Y	,Y	,Y	LOCK	

The following text explains the different parts of the diagram above:

- A This column contains the high-risk userids in your system against which a risk assessment is to be made. Userids can be specified generically, eg the entry TSG* means any userid starting with 'TSG'.

NC-PASS tries to match the incoming userid with a userid in this column by finding a best-fit match, eg in the table above, userid ADMIN1 would match with ADM* rather than AD*, since ADM* is the 'best fit'.

- B These columns are headed by date/time definitions. Each definition relates to a specific range of dates or times or both. If a userid match is found in column A, NC-PASS searches the date/time definitions from left to right to find a match for the time or date, or both of the access request. Details of how to create date/time definitions are provided in *Chapter 6 - Restricting access by date and time*.

- C Whenever a match is found, NC-PASS extracts the keywords at the intersection between the matched userid and the matching date/time definition.

Keywords are in the format *a,v* where:

a relates to token authentication (not applicable for NC-PASS Secure)

v relates to password validation

Refer to *Keyword interpretation* on page 3.8 for descriptions of each keyword and details of how NC-PASS determines the validation requirements from the keywords extracted.

Refer to *User risk profile creation* on page 3.35 for details of the USER RISK PROFILE panel (5.6).

Terminal risk profiles

The following diagram shows a representation of a terminal risk profile record:

Date/time Access route	B					
	STATEHOL	WORKWEEK	EVENING	WEEKEND	OUTHOOURS	ALWAYS
ADM*	LOCK	,Y	,Y	LOCK	LOCK	
ADMT*	LOCK	,Y	,Y	,Y	LOCK	
NET1.DIAL*	LOCK	,Y	,F	LOCK	LOCK	
TRMRECEP		,B				
XFER.FUND	,Y	,Y	,Y	,Y	,Y	,Y

C

The following text explains the different parts of the diagram above:

- A This column contains the high-risk access routes in your system against which a risk assessment is to be made. Refer to *Terminal profiles overview* on page 3.3 for an explanation of access routes.

Access routes can be specified generically, eg the entry ADM* means any access route starting with 'ADM'.

An access route can refer to a:

Terminal id the LU name of a terminal as defined to VTAM.

Transaction id the name of a transaction, in the format xxx.yyy as provided through a TLI call from an application to NC-PASS.

For an XMS TLI call, xxx is the data specified by parameter 'TERMID=' and yyy is the data specified by parameter 'APPL=' in the TLI call.

For an APPC TLI call, xxx is the data specified by parameter REQUESTOR and yyy is the data specified by parameter TERMINAL/NODE in the TLI call.

NC-PASS tries to match the access route data with an access route id in this column by finding a best-fit match, eg in the table above, ADMTERM1 would match with ADMT* rather than ADM*, since ADMT* is the 'best fit'.

- B These columns are headed by date/time definitions. Each definition relates to a specific range of dates or times or both. If a terminal id match is found in column A, NC-PASS searches the date/time definitions from left to right to find a match for the time or date, or both of the access request. Details of how to create date/time definitions are provided in *Chapter 6 - Restricting access by date and time*.

- C Whenever a match is found, NC-PASS extracts the keywords at the intersection between the matched access route and the matching date/time definition.

Keywords are in the format a,v where:

a relates to token authentication (not applicable for NC-PASS Secure)

v relates to password validation

Refer to *Keyword interpretation* on page 3.8 for descriptions of each keyword and details of how NC-PASS determines the authentication/validation from the keywords extracted.

Refer to *Terminal risk profile creation* on page 3.33 for details of the TERMINAL RISK PROFILE panel (6.2).

Keyword interpretation

The following keywords are supported (the underlined letter shows the permitted abbreviation):

LOCK
Force (valid only in terminal risk profiles),
Bypass (valid only in terminal risk profiles)
Yes
No
Default (or blank)

Keywords are in the format a,v where:

a relates to token authentication (not applicable for NC-PASS Secure)
v relates to password validation

Note: Since token authentication is not applicable for NC-PASS Secure, you must enter a comma (,) followed by the required password keyword.

When NC-PASS is requested to verify a user, the date and time of the access request is matched with the appropriate date/time definition and the corresponding keywords, if specified, are extracted from the user and terminal risk profiles. These keywords are combined to determine the overall risk assessment. NC-PASS uses this combined assessment to determine the authentication/validation requirements for the user, for this access request, as shown in the table below.

Password validation (second keyword)

Password keyword in the USER risk profile	Corresponding password keyword in the TERMINAL risk profile	the RESULT is...
(any)	F	a password MUST be used from this access route, irrespective of any other settings.
(any)	B	a password is not required for this access route, irrespective of any other settings.
Y	Y,N,D or blank	a password is required for this request.
N	Y,N,D or blank	a password is not required for this request.
D or blank	Y	a password is required for this request.
D or blank	N	a password is not required for this request.
D or blank	D or blank	if the user profile specifies password checking, NC-PASS will prompt for a password, otherwise no password is required.

As can be seen from the table above, for a given time period, a 'Yes' or 'No' keyword in a user risk profile will always override a 'Yes' or 'No' keyword in a terminal risk profile.

If you want all users to provide password details when accessing the system from a particular access route, use the 'Force' password keyword in the terminal risk profile against the required access route and time period.

If you do not want users to provide password details when accessing the system from a particular access route, use the 'Bypass' password keyword in the terminal risk profile against the required access route and time period.

Defaults

If password validation is specified as **Default** (or blank) in the user risk profile, NC-PASS will use the corresponding keyword from the terminal risk profile and vice versa.

If password validation is specified as **Default** (or blank) in both the user and terminal risk profiles, the requirement for a password depends on whether password validation has been specified for this user.

Note: NC-PASS uses keyword **Default** if no matching risk profile record is found. Refer to *Verifying a user* on page 3.12.

Access control examples

This section shows how you can achieve certain objectives using the terminal and user risk profiles. Each example shows one or two settings to illustrate the specified objective; these can be combined to achieve more complex objectives.

Objective: To deny access to any user from terminal TERM1 at weekends.

```
Date:12/12/1997          TERMINAL RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS26

Line Commands: D=Delete  F=Find  N=New

                DATE/TIME DEFINITIONS
0  TERMINAL          STATEHOL WORKWEEK EVENING  WEEKEND  OUTHOURS ALWAYS
   TERM1                LOCK
```

Objective: To deny access to USER1 during the time specified by the OUTHOURS definition.

```
Date:12/12/1997          USER RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS268

Line Commands: D=Delete  F=Find  N=New

                DATE/TIME DEFINITIONS
0  USER              STATEHOL WORKWEEK EVENING  WEEKEND  OUTHOURS ALWAYS
   USER1                LOCK
```

Objective: To ensure that USER1 uses a password in the evening.

```
Date:12/12/1997          USER RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS268

Line Commands: D=Delete  F=Find  N=New

                DATE/TIME DEFINITIONS
0  USER              STATEHOL WORKWEEK EVENING  WEEKEND  OUTHOURS ALWAYS
   USER1                ,Y
```

Objective: To ensure that all users use a password when logging on from terminal TERM1 at the weekend.

```
Date:12/12/1997          TERMINAL RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS26

Line Commands: D=Delete  F=Find  N=New

                DATE/TIME DEFINITIONS
0  TERMINAL          STATEHOL WORKWEEK EVENING  WEEKEND  OUTHOURS ALWAYS
   TERM1                ,F
```

Objective: To bypass the need for a password for any user when logging on from terminal TERM1 during normal office hours.

```
Date:12/12/1997          TERMINAL RISK PROFILE          Userid:TSG0001
Time:09:00              Terminal:A01MS26

Line Commands: D=Delete  F=Find  N=New

                DATE/TIME DEFINITIONS
0 TERMINAL      STATEHOL WORKWEEK EVENING  WEEKEND  OUTHOURS ALWAYS
  TERM1                ,B
```

Objective: To ensure that user ADM1 uses a password outside normal working hours, but not during normal office hours.

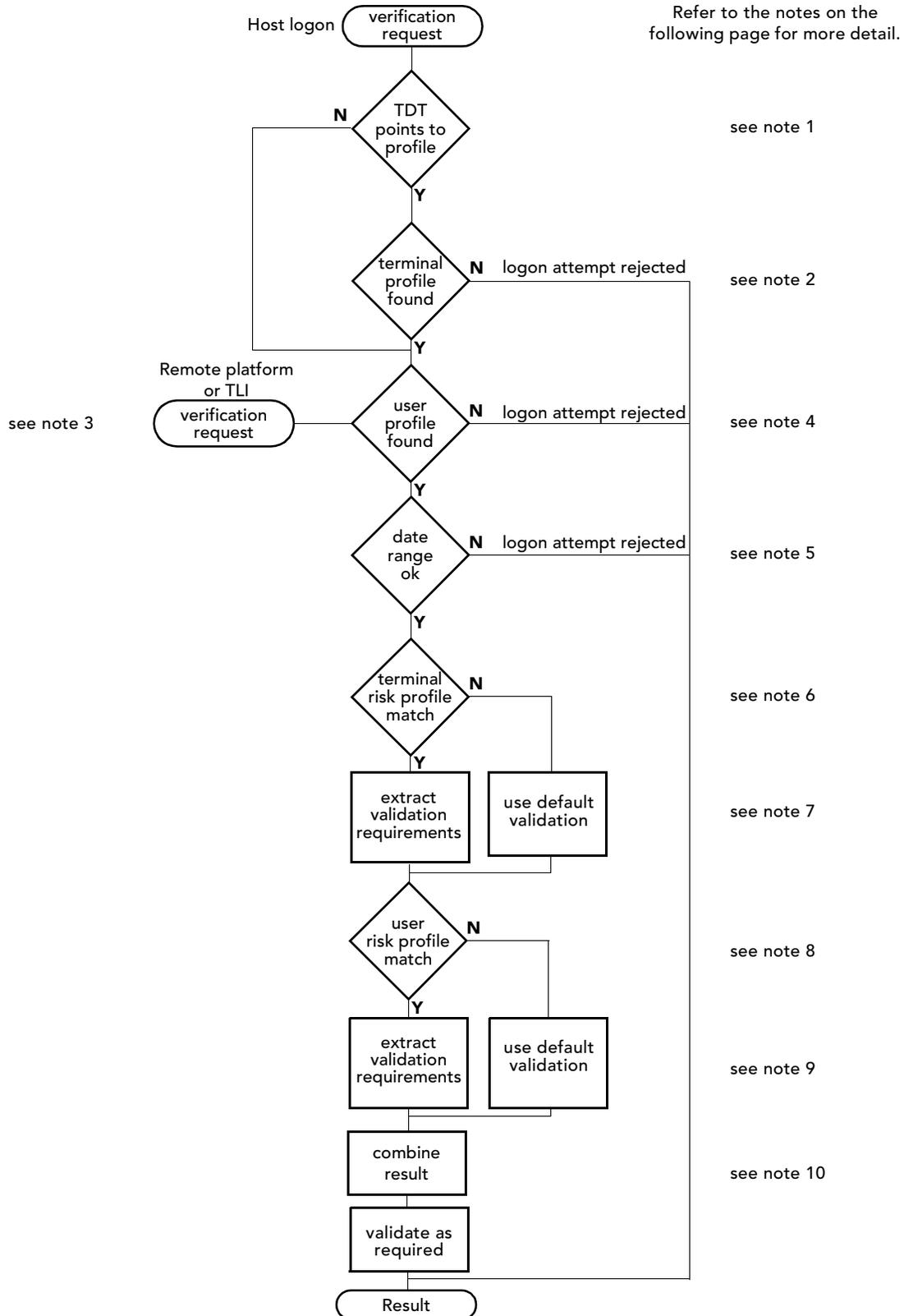
```
Date:12/12/1997          USER RISK PROFILE          Userid:TSG0001
Time:09:00              Terminal:A01MS268

Line Commands: D=Delete  F=Find  N=New

                DATE/TIME DEFINITIONS
0 USER          STATEHOL WORKWEEK EVENING  WEEKEND  OUTHOURS ALWAYS
  ADM1                ,Y      ,N      ,Y      ,Y      ,Y      ,Y
```

Verifying a user

The diagram below is an illustration of how the profile record types are used when NC-PASS receives a verification request. (For simplicity, the diagram concentrates on profile records and does not include userid or terminal lock checking, etc.)



- Note 1. A TDT entry can either simply specify a logo panel to be displayed at logon, or point to a terminal profile record. If the TDT entry for that terminal specifies that a terminal profile record exists for the terminal, NC-PASS will access the profile record and extract the appropriate information. If the TDT specifies a terminal profile record, but one does not exist, NC-PASS will reject the logon request.
- Note 2. NC-PASS searches for a match with the terminals specified on the TERMINAL PROFILE MAINTENANCE panel (6.1). If no match is found, the logon attempt will be rejected.
- Note 3. Terminal profiles are not applicable for verification requests from remote platforms or from TLI calls from user programs.
- Note 4. NC-PASS searches for a user profile record for the specified userid. The userid on the profile record may be defined generically, ie a logon attempt by userid TSG0001 could match with a profile record for TSG00*. NC-PASS searches for a best fit match, eg if user profile records existed for TSG* and for TSG00*, NC-PASS would match with TSG00*.
- If no match is found, the verification process will end with an appropriate error result code.
- If a match is found, NC-PASS extracts the data from the user profile (and from the RACF user profile if specified - refer to *Chapter 5 - Administering users from an external security database* for further details).
- Note 5. NC-PASS checks the **No logon before** and **No logon after** fields on the matched user profile to determine whether a date restriction is in force for this profile. If there is a date specified and the date is outside the permitted date range, the verification process will end with an appropriate error result code.
- Note 6. If no date restriction has been specified, or the logon date falls within the permitted range, NC-PASS searches the terminal risk profile record for a matching entry. Entries in this record can refer to real or imaginary terminal ids. Refer to *Terminal profiles overview* on page 3.3 for an explanation of these terms. If a match is found, the date/time definitions are searched from left to right.
- Note 7. If a match is found, the appropriate keyword is extracted. If no match is found, either with the terminal id or with a date/time definition, NC-PASS uses the keyword 'Default' for validation.
- Note 8. NC-PASS searches the user risk profile record for a matching entry.
- Note 9. If a match is found, the appropriate keyword is extracted. If no match is found, either with the user id or with a date/time definition, NC-PASS uses the keyword 'Default' for validation.
- Note 10. The keywords extracted from the terminal and user risk profiles are combined to determine the overall risk assessment. Refer to *Keyword interpretation* on page 3.8 for details.

Defining terminals to NC-PASS

When a user logs on at a terminal controlled by NC-PASS, the first panel displayed is the logo that has been assigned to the terminal either through:

- the Terminal Definitions Table (TDT)

OR a combination of both:

- the TDT
- the NC-PASS Terminal Profile.

The TDT

The TDT describes all the terminals available to the system, and for each terminal provides a panel name for the initial logo to be displayed at logon.

Any terminal not specified in the TDT, either specifically or by a generic or masked entry, will not be allowed to connect to NC-PASS.

Defining a TDT

The TDT is a member of a dataset pointed to by the TDT DD statement in the startup JCL for NC-PASS.

If NC-PASS is up and running and you have created a new TDT member (or amended an old one), you can define the member as the new TDT by selecting option 5 from the TERMINAL ADMINISTRATION MENU (6).

Enter the name of the new member with the option number as follows:

Option => 5 *membername*

Press the <Enter> key to delete the old TDT from storage and load the updated member into storage.

Sample TDT

```
*
*   Terminal Definitions For Pensions Department
*
*       The terminal group is made up of:
*           LOCAL006 and LOCAL007
*           all REMOTE terminals
*           terminals in SUBAREA 01
*           (luname bytes 3-4 = 01)
*
GROUP PENSIONS
PANEL ESE0052
TERMINAL LOCAL006
TERMINAL LOCAL007 D4B32782
TERMINAL REMOTE*
TERMINAL ++01++++

*
*   Terminal Definitions for all other terminals
*
GROUP OTHERS
PANEL LOG01
TERMINAL *
```

Statement syntax

- All statement cards must begin in column 1
- Each statement must start on a new line
- Only CAPITAL LETTERS are allowed
- An asterisk (*) in column 1 denotes a comment
- Operands must be delimited by at least one space.

Defining groups

An unlimited number of different groups may be defined. Each group must contain the following statements:

a **GROUP** statement,

followed by:

a **PANEL** statement,

followed by:

as many **TERMINAL** statements as are needed, to define all the terminals in the group.

Search order

When a terminal first logs on to NC-PASS, the in-storage TDT is searched top down until the first **TERMINAL** statement which matches the luname of the terminal is encountered. The terminal is then assigned to the group as defined by the preceding **GROUP** statement, and the panel defined by the preceding **PANEL** statement is displayed.

Any terminal not specified in the TDT, either specifically or by a generic or masked entry, will not be allowed to connect to NC-PASS.

Variables set

The TDT **GROUP** name, to which a terminal belongs, is stored in the variable *&usrgrp*, and the initial panel named in the **PANEL** statement is stored in variable *&usrrest*. Variables *&usrlogt*, *&usrnlog*, *&usrnsim*, *&usrnres*, *&usruppr* may also be set depending on other options specified.

GROUP statement

GROUP *groupname* UPPER NOLOG NOSIM NORES

where:

<i>groupname</i>	defines a group name. Choose any name up to 8 characters in length.
UPPER	If coded, this optional parameter causes all data transmitted to the terminals in the group to be translated to uppercase. This is of use with Katakana terminals.
NOLOG	Specify this optional operand for groups of terminals which are NOT LOGAPPL'd to NC-PASS.
NOSIM	Specify this optional operand for terminals for which a SIMLOGON should not be issued, such as terminals on dial-up lines or connected through emulators which terminate a connection at session take-down before SIMLOGON is scheduled.
NORES	Specify this optional operand for terminals for which a restart should not be issued following a RSHUTD request.

PANEL statement

PANEL *panelname*

where:

<i>panelname</i>	defines the panel that will be displayed when a terminal in this group first connects to NC-PASS or when a RESTART statement is executed.
------------------	---

TERMINAL statement

TERMINAL *termname logmode*

where:

<i>termname</i>	Identifies the terminal(s) that comprise the group. Generic names are supported as well as <i>masking</i> , for example: LOCAL* - terminals prefixed LOCAL. ++ABC+- terminals with lunames having characters ABC in columns 3 through 5.
<i>logmode</i>	Specify this optional operand to force a particular LOGMODE table entry to be used when any terminal defined by <i>termname</i> connects, for example: TERMINAL LOCAL4EF D4C32783 Logmode D4C32783 will be used to bind the terminal, overriding the logmode used in the logon request.

Each GROUP may contain as many TERMINAL statements as are needed to define all the required terminals.

Terminal profiles

A terminal profile can be created for two categories of terminal, real terminals and imaginary terminals. The terminal profile therefore defines a number of access routes, as described in *Terminal profiles overview* on page 3.3.

Real terminals

A terminal profile entry for a real terminal provides logon details applicable to specific terminals, including temporary lock periods for users who have made a number of invalid attempts to logon from the specified terminal.

A terminal profile is linked to a TDT by entering the panel statement PANEL ESE0032 in the TDT for that terminal.

Terminals defined in this way will be controlled by the Terminal Profile which will provide the panel name for initial logo display and the temporary lock period.

For example,

```
GROUP PENSIONS  
PANEL ESE0052  
TERMINAL PENS*  
  
GROUP POLICY  
PANEL ESE0032  
TERMINAL POL*  
TERMINAL TP*
```

specifies that

- terminals starting with PENS will display panel ESE0052 at logon
- terminals starting with POL or TP have a terminal profile which specifies:
 - the logo to be displayed at logon
 - the basic lock interval for the terminal if a user makes a number of invalid logon attempts.

Imaginary terminals

Imaginary terminals are described on page 3.3. You would define a terminal profile entry for an imaginary terminal only if you wanted to specify a temporary lock period for that access route (which would be actioned if a number of unsuccessful attempts were made from that access route). See *INTERVAL* on page 3.19 for details of how to specify a temporary lock period.

Access route restrictions

Other access route restrictions, such as the requirement for token authentication, can be defined for any terminal, real or imaginary, on the Terminal Risk Profile. Refer to *Risk profiles overview* on page 3.5.

Access can also be controlled through the terminal locking facility of NC-PASS. Terminals, real or imaginary, can be individually locked or unlocked by accessing the PROCESS LOCKED TERMINALS panel (6.4) and entering the appropriate command. Refer to *Locking userids and terminals* on page 3.37.

Specifying terminal profile entries

Specify a terminal profile by selecting option 6.1 from the NC-PASS SECURE MENU.

```

Date:12/12/1997          TERMINAL PROFILE MAINTENANCE          Userid:TSG0001
Time:09:00                                     Terminal:A01MS242

      GROUP   PANEL   TERMINAL   INTERVAL
000001 SDAUSERS ESE7202 A01MS231     000
000002                                     A01MS232     000
000003                                     B*           000
000004 WW1USERS ESE7302 A01MS233     002
000005                                     C*           000
000006 CATCHALL ESE0052 *             000
*****

F1=Help  F2=Risk  F3=End  F7=Up  F8=Down  F12=Can

```

Changes to the panel are made using the line editor. Refer to the Installation Manual, *Chapter 8 - Getting started* for further details.

Input fields

Field	Description
(line number)	this is the line number of the display.
GROUP	this is an optional field which can be used to identify a group of terminals with a meaningful name. The field is only for display purposes and is not used by the system.
PANEL	determines the logo panel to be displayed for the specified terminal(s). If the field is not entered, the previous PANEL field entry in the list will be used. The PANEL field on line 1 must be completed. If the corresponding entry in the TERMINAL column refers to an imaginary terminal, this entry is ignored.
TERMINAL	the terminal profile id. This can be either a real or an imaginary terminal. See <i>Terminal profiles</i> on page 3.17 for definitions of real and imaginary terminals. For real terminals, enter a specific or generic terminal id. To specify a generic terminal id (group of terminals), you can enter a common 'stub' followed by an asterisk (*). The plus sign (+) can also be used to identify specific characters. For example, to define a profile for all terminals beginning with A and having a third character of 1, enter A+1*. For imaginary terminals, enter a specific or generic terminal id in the format <i>termid.appl</i> or <i>network.node</i> as described in <i>Imaginary terminals</i> on page 3.17. The maximum length of this field is 21 characters including the period.

Field	Description
INTERVAL	<p>Enter the basic time interval, in minutes, to be used to calculate a temporary terminal lock period following an incorrect entry by the user. Each time a user makes an incorrect access attempt from this route, the terminal lock period is incremented according to the formula:</p> $L = 2^{(A-1)} \times B$ <p>where:</p> <ul style="list-style-type: none"> L is the lock period A is the number of invalid logon attempts B is the minutes entry in this field <p>Where the result of the calculation exceeds a lock time of one week, a permanent lock is issued for the access route. An INTERVAL of zero disables the feature (ie access routes are not locked after an unsuccessful logon attempt).</p>

Function keys

Key	Function
F1	displays help information.
F2	displays the TERMINAL RISK PROFILE panel.
F3	saves any changes made and returns to the previous screen.
F7	scrolls down the list of terminal profiles.
F8	scrolls up the list of terminal profiles.
F12	cancels any changes and returns to the previous screen.

User profile creation

To set up a new user profile select option 5 from the NC-PASS SECURE MENU to provide the USER PROFILE MAINTENANCE MENU shown below. At the **Option** input field, enter 1 followed by a space and the userid to be created, an example of which is shown below:

```
Date:12/12/1997          USER PROFILE MAINTENANCE MENU          Userid:TSG0001
Time:09:00                                     Terminal:TCP00018

      Option => 1 NEWUSER

          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

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

This will display the PROFILE DETAIL FOR *USERID* panel, an example of which is shown on the following page.

Using another profile as a model

You can specify that a new user profile is to be modeled on an existing profile. If you specify a model profile, the new profile will be a copy of the model profile, including the connect data definitions; you can then amend specific fields as required. To specify a model userid you can:

- specify a user profile in the **Default user profile** field on the GENERAL SYSTEM OPTIONS panel (1.1) which will be used as a model for all new profiles
- specify a model userid profile as the third parameter at the option prompt above. For example enter

```
1 NEWUSER MODEL
```

to specify that you want to create a new profile called NEWUSER based on an existing profile called MODEL. This will override any profile name specified as the default on the GENERAL SYSTEM OPTIONS panel (1.1).

Profile definition

Options 1, 2 and 4 from the USER PROFILE MAINTENANCE MENU provide the PROFILE DETAIL FOR *USERID* panel shown below.

User profile details can be created, changed, or displayed in this panel depending on the option selected. This panel allows you to set up the required definition for the userid to be created. Once created, enter the appropriate values for the userid, described below and on the following page. When you have completed all fields press <F3> to save and end.

```
Date:12/12/1997          PROFILE DETAIL FOR NEWUSER          Userid:TSG0001
Time:09:00              Terminal:A01MS268

Comment => _____
=> _____

Password validation => N      A,I,N,R,S,T
Authority type      => U      A,O,U
Authority group     => *      (Code or *)
Authority level     => 1      (1 - 255)
Initial menu        => _____
Retry maximum       => 0      0-99
No logon before     => _____ (DD/MM/YYYY)
No logon after      => _____ (DD/MM/YYYY)

Basic lock interval => 0      Minutes
Use external profile => N      Y/N
For Internal password processing specify the following:
Change password every => 0 number of days
Change password every => 0 number of logons
Created:              By:                Updated:              By:

F1=Help F2=Risk F3=End F6=Connect data F12=Can
```

This panel can also be displayed by using the C or V line commands from the LIST USERS panel (5.5).

The following input fields descriptions refer to option 1 (Define a new user profile) and option 2 (Change a user profile). The same fields are display only for option 4 (Display a user profile).

Input fields

Field	Description
Comment	Enter information about the user or user profile which may be relevant (such as personal details). This data is held for information only. The first line will be displayed on the LIST USERS panel (5.5).

Field	Description
Password validation	<p>Enter the required value from the list below:</p> <ul style="list-style-type: none"> A represents CA-ACF2 validation I represents internal password validation N represents no validation R represents RACF validation S represents SAC validation T represents CA-Top Secret validation. Refer also to <i>CA-Top Secret random password support</i> on page 4.7 (Volume 2). <p>Note: Passwords are always encrypted within NC-PASS and when being transmitted over communications links.</p>
Authority type	<p>Enter the required value from the list below:</p> <ul style="list-style-type: none"> A represents administrator O represents operator U represents user <p>If initial menus have not been set up for any or all of these user types, default menus will be displayed.</p>
Authority group	<p>Enter a three character code defining a group of users in which this userid is to be included. Such groups can only be administered by an administrator assigned to a higher level generic group or one with an asterisk (*) specified in the Authority group field (this gives the administrator access to all groups). For example an administrator of authority group A* can administer any userids beginning with an A eg AB1234, A0123 etc.</p>
Authority level	<p>Enter a number in the range 1 through 255. The highest level is 1. An administrator can only administer equal or lower levels to his own and therefore should not be coded at the lowest level.</p>
Initial menu	<p>Specify the id of the menu to be displayed as the user's primary option menu. If omitted, a default menu will be displayed. Refer to <i>Menus</i> on page 4.13 (Volume 2) for further details.</p>
Retry maximum	<p>specify the number of times, in the range 1 through 99, that the user may attempt to logon. If the number of unsuccessful attempts exceeds this number, the userid will be locked until it is reset by the administrator using option 5.8 of the NC-PASS SECURE MENU.</p> <p>Note: If 0 is specified unlimited retries are allowed, unless you specify a value in the Basic lock interval field.</p>
No logon before	<p>Specify the date on which the userid may first access the system. The date format is determined by an entry in the GENERAL SYSTEM OPTIONS panel (1.1). If omitted the userid has immediate access to the system, unless a date/time definition is specified which contains such a restriction.</p> <p>If you enter a date in this field and you also specify a Date/Time definition which contains a DATE START entry, NC-PASS will use the later of the two dates when authenticating the user.</p>

Field

No logon after

Description

Specify the last date on which the userid may access the system. The date format is determined by an entry in the GENERAL SYSTEM OPTIONS panel (1.1). If omitted the userid has indefinite access to the system, unless a date/time definition is specified which contains such a restriction.

If you enter a date in this field and you also specify a Date/Time definition which contains a DATE END entry, NC-PASS will use the **earlier** of the two dates when authenticating the user.

Field

Basic lock interval

Description

Note: This field is read-only if you have specified that data is to be extracted from a RACF user profile record for this user.

Enter the basic time interval, in minutes, to be used to calculate a temporary userid lock period following an incorrect logon entry by the user. Each time the user makes an incorrect logon attempt that would result in a lock being applied, the userid lock period is incremented according to the formula:

$$L = 2^{(A-1)} \times B$$

where:

L is the lock period

A is the number of invalid logon attempts

B is the minutes entry in this field

The userid can be unlocked by an administrator using option 5.8 from the NC-PASS SECURE MENU.

When the value of this field is non-zero, then the **Retry maximum** specified for the user on this panel will be ignored.

If 0 is specified in this field, the temporary lock facility is disabled and the **Retry maximum** field is activated.

Example

User TSG0583 has attempted to log on to the system, but is not allowed access at this time of day.

The basic lock interval specified for the user profile for TSG0583 is 5 minutes.

$$\begin{aligned} \text{The user is locked for } & 2^0 * 5 \text{ minutes} \\ & = 1 * 5 \text{ minutes} \\ & = 5 \text{ minutes} \end{aligned}$$

After five minutes have expired, the lock is released, and the user is allowed to try again. The user is still not allowed access, so the user is locked again for a longer period of time.

$$\begin{aligned} \text{The user is locked for } & 2^1 * 5 \text{ minutes} \\ & = 2 * 5 \text{ minutes} \\ & = 10 \text{ minutes} \end{aligned}$$

When the lock period exceeds one week, the lock becomes permanent until unlocked using option 5.8 from the NC-PASS SECURE MENU.

Field	Description
Use external profile	Set this field to Y to specify that NC-PASS will make use of the 'Keyword Definitions' prepared on the CAF, to consider the extraction of specific fields for this userid from an externally stored source. (For example the Installation Data field on a RACF user profile.) Refer to <i>Chapter 5 - Administering users from an external security database</i> for details. Note: The External user profile field on the LOGON DEFAULTS panel (1.2) must be set to Y, if an external database is to be searched.
Change password every	These fields apply only to internal password processing. They define the duration of a user password either in days or number of logons, at the end of which the user will be prompted to provide a new password at logon.

Display fields

Field	Description
Created/By	These fields show at what time, on what date and by which administrator, the profile was created.
Updated/By	These fields show at what time, on what date and by which administrator, the profile was updated.

Function keys

Key	Function
F1	displays help information.
F2	displays the USER RISK PROFILE panel.
F3	saves the information and returns to the previous screen.
F6	displays the CONNECT DEFINITION for <i>USERID</i> panel. This allows you to set up the route the user will take when signing on. See the section entitled <i>Specifying connection routes</i> on page 3.26 for further details.
F12	Cancels all changes and returns to the previous screen.

Profile deletion

You can delete a user profile by entering 3 *userid* at the USER PROFILE MAINTENANCE MENU. A confirmation panel is then displayed which allows you to confirm the deletion or escape to the previous screen.

Specifying connection routes

As an administrator, you can specify the application or menu to which the user will be transferred after a successful logon attempt, thereby simplifying and speeding up the logon procedure. For example you can specify that after a successful logon for user TSG0023 the Pensions menu will be displayed.

The connect data definition provides the information used by the system after successful logon to transfer the user to the required destination. You can specify the connect data definitions by one of the following methods:

- using line editor commands on the CONNECT DEFINITION for *USERID* panel an example of which is shown on the next page. (For details of line editor commands refer to the Installation Manual, *Chapter 8 - Getting started*)
- specifying the data on a RACF database; refer to *Chapter 5 - Administering users from an external security database* for further details.

The CONNECT DEFINITION for *USERID* panel

From the PROFILE DETAIL FOR *USERID* panel, press <F6> to display the following panel.

```
Date:12/12/1997          CONNECT DEFINITION for NEWUSER          Userid:TSG0001
Time:09:00                Terminal:A01MS268

'Code' relates to name in 'Dest': N=Nodename E=Exec K=Keyword M=Menu

      CODE DEST      TERMID  DATA PASSED TO APPLICATION  USER COMMENT
000001 M  PROLLM    *      SYSUSER/SYSPASS              Payroll
***** *  *****  *****  *****

F1=Help  F3=End  F6=User profile  F7=Up  F8=Down  F12=Can
```

Note: If you have specified that connect data for this user is to be extracted from a RACF database, a similar panel to that shown above is displayed, but all fields are read-only. If you want to make changes to the connect data for this user, these changes must be made on the RACF user profile record. Refer to *Chapter 5 - Administering users from an external security database* for further details.

Input fields

Field	Description
CODE	determines how the name given in DEST is interpreted. See the table below for details.
DEST	determines the destination for data passed at connect time.

CODE	DEST
N	provides the name of a VTAM application eg CICS.
E	provides the name of an EXEC written in the NCI language (no EXECs are provided). If you are using an EXEC, code the following to resolve keywords before user processing:)ROUTINE * EXEC @SECINIT 'SYSUSER SYSPASS' LOG &cCINIT *
K	contains one of the following keywords: ADMIN the user is routed to the NC-PASS SECURE MENU ACCESS the user is routed to NC-ACCESS (if installed and running in the same address space as NC-PASS). APPL the user is routed to an application specified by the user at the APPL prompt at the logo.
M	provides the name of a menu definition.

Field	Description
TERMID	This provides a means of restricting the user to specific terminals. The terminal id entry may be generic (e.g. ABC* will only allow access from terminals starting with ABC). The normal setting is a single asterisk (*) to give access from any terminal. Specific characters in the terminal id may also be identified with a plus sign (+) to denote that any character is to be matched in the specified position.
DATA PASSED TO APPLICATION	varies depending on the contents of DEST, as shown in the table below:

If DEST contains....	The DATA PASSED TO APPLICATION field is....
the name of a VTAM application	the CINIT data which is to be passed to the VTAM application
the name of an EXEC written in NCI	the data which is to be passed to the EXEC as a parameter in &cCINIT
a keyword	not applicable
a menu	not applicable

Field	Description
-------	-------------

The following keywords, (which can be abbreviated to the first four characters), if included in DATA PASSED TO APPL, will be translated

- SYSUSER - becomes the current userid.
- SYSPASS - becomes the current user's password.
- SYSTEM - becomes the current user's terminal id.
- SYSOLDP - becomes the current user's old password.
- SYSNEWP - becomes the current user's new password.

(effectively the same as SYSPASS)

Variables can also be passed in CINIT data. For example, if you enter:

```
SYSU/SYSP/&data./HELLO
```

NC-PASS will resolve the first three entries and pass the complete string to the application.

There must be a period (.) after the variable name otherwise NC-PASS does not know where the name ends - in this example an omitted period (.) would cause a default of &data/HE because eight character names are the default for NC-PASS.

USER COMMENT For information only - not used in any processing.

Function keys

Key	Function
F1	displays help information.
F3	saves the information and returns to the NC-PASS SECURE MENU.
F6	returns to the PROFILE DETAIL FOR <i>USERID</i> panel, as previously described.
F7	displays the previous list of tokens.
F8	displays the next list of tokens.
F12	Cancels all changes and returns to the USER PROFILE MAINTENANCE MENU.

Listing user profiles

To view the details for all or a number of userids, select option 5 from the USER PROFILE MAINTENANCE MENU. This will display the LIST USERS panel as shown below:

```
Date:12/12/1997          LIST USERS          Userid:TSG0001
Time:09:00              Terminal:A01MS262

Userid => *_____

Line commands: C=Change V=View D=Delete

S USERID  COMMENT                UPDATED   TIME   BY
_ ACCAB    Accounts Dept - Ann Brown   06/05/1997 15:58 ADMIN
_ ACCJJ    Accounts Dept - John Jones  08/08/1997 09:04 ADMIN
_ ACCTS    Accounts Dept - supervisor  06/10/1997 14:16 TSG0001

F1=Help  F3=End  F6=Print  F7=Up  F8=Down
```

Input fields

Field	Description
Userid	can be used to select the information displayed in the list; only userids which match the selection criteria will be displayed. This field may be specified generically using an asterisk (*) to denote that only characters preceding the asterisk are to be matched. A single asterisk (*) means that all userids will be displayed.

Display fields

Field	Description
USERID	provides a userid on each line of the panel as determined by the above Userid selection field.
COMMENT	contains information entered into the comment line of the user profile.
UPDATED	the date the user profile was last updated.
TIME	the time the user profile was last updated.
BY	who last updated the user profile.

Line commands

The line commands C, V and D can be entered in column S against the appropriate userid to perform the following functions:

- C provides the PROFILE DETAIL FOR *USERID* panel where changes to the user profile can be made.
- V displays the PROFILE DETAIL FOR *USERID* panel in a read only format, for viewing only.
- D displays the CONFIRM PROFILE DELETION panel. Enter Y to confirm the deletion of the user profile or N to return to the previous screen.

Any number of selections can be made in the LIST USERS panel, and selected panels will be displayed in rotation (that is, on closing one panel, the next panel will be displayed).

Function keys

Key	Function
F1	displays help information.
F3	saves the information and returns to the previous screen.
F6	produces a USER PROFILES report. See the section entitled <i>Printing user profiles</i> on page 3.31 for further details.
F7	displays the previous list of tokens.
F8	displays the next list of tokens.

Printing user profiles

The LIST USERS panel (5.5) provides the facility to print a report containing the details of one or more specified userids. To use this facility enter the required specific or generic userid at the **Userid** prompt and press <Enter>. For example enter TSG* to display only those userids that begin TSG. The LIST USERS panel will display the specified userids; press <F6> to print a report. A print details panel will be displayed on which you must enter details of your printer.

Note: Before VTAM printers can be used by NC-PASS they must be defined on the VTAM PRINTER DEFINITIONS panel (1.6). See the section entitled *VTAM printer definitions* on page 2.7.

Press <Enter> to start printing the report, an example of which is shown on the following page.

Report requested by - SYS0001
on Terminal - A01MS009
Job Name - HQPENS1Q

Selection conditions:
Userid => TSG*

TSG0001 PROFILE DETAIL

Token assignment =>
Comment => Tech. support group
=>

Password validation => R (A,N,R,S,T,I)
Authority type => A (A,0,U)
Authority group => * (Code OR *)
Authority level => 1 (1 - 255)
Initial menu =>
Retry maximum => 0 (0 - 99)
No logon before => (MM/DD/YYYY)
No logon after => (MM/DD/YYYY)
Use external profile=> N (Y/N)
For internal password processing specify the following:
Change password every => 0 (number of days)
Change password every => 0 (number of logons)

Created: 01/03/1996 15:21 By: ADMIN Updated: 06/05/1997 15:58 By: ADMIN

CODE	DEST	TERMID	DATA PASSED TO APPLICATION	USER COMMENT
0001	K	ADMIN	*	

TSG0093 PROFILE DETAIL

Token assignment =>
Comment => Tech. support group
=>

Password validation => N (A,N,R,S,T,I)
Authority type => A (A,0,U)
Authority group => * (Code OR *)
Authority level => 1 (1 - 255)
Initial menu =>
Retry maximum => 0 (0 - 99)
No logon before => (DD/MM/YYYY)
No logon after => (DD/MM/YYYY)
Use external profile=> N (Y/N)
For internal password processing specify the following:
Change password every => 0 (number of days)
Change password every => 0 (number of logons)

Created: 01/03/1996 15:21 By: ADMIN Updated: 06/05/1997 15:58 By: ADMIN

CODE	DEST	TERMID	DATA PASSED TO APPLICATION	USER COMMENT
0001	K	ADMIN	*	

End of report. 2 profiles printed

Terminal risk profile creation

Select option 6.2 from the NC-PASS SECURE MENU or press <F2> from the TERMINAL PROFILE MAINTENANCE panel (6.1) to display the panel below:

```
Date:12/12/1997          TERMINAL RISK PROFILE          Userid:TSG0001
Time:09:00              Terminal:A01MS264

Line Commands: D=Delete  F=Find  N=New

          DATE/TIME DEFINITIONS
O TERMINAL          STATEHOL  WORKWEEK  EVENING  WEEKEND  OUTHOURS  ALWAYS
-----
RECEPT           ,Y      ,Y      ,Y      ,Y      ,Y      ,Y
TERM1*             ,F      ,F      ,F      ,F      ,F      ,F
TERM2*             LOCK    ,D      ,D      ,D      ,Y      ,F
XFER.CICS          ,Y      ,Y      ,Y      ,Y      ,Y      ,Y
10010220.8001601F* ,N      ,N      ,N      ,N      ,N      ,N

F1=Help  F3=End  F7=Up  F8=Down  F9=Swap  F12=Can
```

The date/time definitions displayed in the panel above are the defaults provided for your use. You can display the complete list of definitions using the DATE AND TIME DEFINITIONS panel (5.7); from this panel, use line command C against a definition to display the data for that definition.

If required, you can change the data for the default definitions; for example if you want the WORKWEEK definition to specify Monday through Friday between 07:30 and 19:30, you can amend this definition accordingly. Alternatively, you can create your own definition, for example NORMHRS, and overwrite WORKWEEK above with the name of your definition.

Entering terminal risk data

If you want to create a new entry in the panel above, use the N line command on the first line under the O column header, followed by the specific or generic terminal id for which a risk entry is to be created. Under each of the date/time definitions, specify the risk keywords for that time period. Input fields are fully described on the following page.

Changing existing entries

If you want to change an existing entry, overwrite the data with the new details and press <Enter> to display the new data. When you have made all your required changes, press <F3> to save and end.

Input fields

Field	Description
DATE/TIME DEFINITIONS	If required, overtype the name of a definition which specifies the required time period. Date/Time definitions are created using the DATE AND TIME DEFINITIONS panel (5.7). Refer to <i>Chapter 6 - Restricting access by date and time</i> .
TERMINAL	Enter the terminal id (specific or generic) for which a risk assessment is to be made, as described below: real terminals enter the LU name of the terminal as defined to VTAM. imaginary terminals: via APPC TLI enter the imaginary terminal in the format <i>requestor.node</i> . via XMS TLI enter the transaction identifier in the format <i>function.application</i> where the values are the contents of the parameters 'TERMID=' and 'APPL=' passed via the TLI call. You can also enter a group name as defined on the SME GROUP DEFINITIONS panel (7.2). Refer to <i>Grouping data</i> on page 7.51. (keywords Under each date/time definition, specify keywords (or abbreviations) as appropriate: LOCK <u>F</u> orce <u>B</u> ypass <u>Y</u> es <u>N</u> o <u>D</u> efault (or blank) Keywords are specified in the format <i>a,v</i> where <i>a</i> relates to token authentication and <i>v</i> relates to password validation. Since token authentication is not applicable to NC-PASS SECURE, you must enter the comma (,) first. Refer to <i>Keyword interpretation</i> on page 3.8 for details.

Line commands

You can use line commands F and N only on the first line in the column headed **O**. Option D can be used on any line in the **O** column. Line commands D, F or N perform the following functions

- D deletes the entry for the selected terminal id.
- F finds the first entry that matches the **TERMINAL** specified and displays that and all following entries. For example enter

```
O TERMINAL
E A02*
```

to start the display with the first terminal id that starts with A02.

- N adds a new entry using the input fields described above.

Function keys

Key	Description
F1	displays help information.
F3	saves any changes and returns to the previous screen.
F7	displays the previous screen of terminal ids.
F8	displays the next screen of terminal ids.
F9	displays the USER RISK PROFILE panel.
F12	Cancels any changes and returns to the previous screen.

User risk profile creation

Select option 6 from the USER PROFILE MAINTENANCE menu (5) or press <F2> from the PROFILE DETAIL FOR *USERID* panel to display the panel below:

```
Date:12/12/1997          USER RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS264

Line Commands: D=Delete  F=Find  N=New

          DATE/TIME DEFINITIONS
O USER          STATEHOL  WORKWEEK  EVENING  WEEKEND  OUTHOURS  ALWAYS
-----
ADMIN*          ,Y          ,Y          ,Y          ,Y          ,Y          ,Y
MGRMJ1          ,Y          ,Y          ,Y          ,Y          ,Y          ,Y

F1=Help  F3=End  F7=Up  F8=Down  F9=Swap  F12=Can
```

The date/time definitions displayed in the panel above are the defaults provided for your use. You can display the complete list of definitions using the DATE AND TIME DEFINITIONS panel (5.7); from this panel, use line command C against a definition to display the data for that definition.

If required, you can change the data for the default definitions; for example if you want the WORKWEEK definition to specify Monday through Friday between 07:30 and 19:30, you can amend this definition accordingly. Alternatively, you can create your own definition, for example NORMHRS, and overtype WORKWEEK above with the name of your definition.

Entering user risk data

If you want to create a new entry in the panel above, use the N line command on the first line under the O column header, followed by the specific or generic userid for which a risk entry is to be created. Under each of the date/time definitions, specify the risk keywords for that time period. Input fields are fully described on the following page.

Changing existing entries

If you want to change an existing entry, overtype the data with the new details and press <Enter> to display the new data. When you have made all your required changes, press <F3> to save and end.

Input fields

Field	Description
DATE/TIME DEFINITIONS	If required, overtype the name of a definition which specifies the required time period. Date/Time definitions are created using the DATE AND TIME DEFINITIONS panel (5.7). Refer to <i>Chapter 6 - Restricting access by date and time</i> .
USER	Enter the userid (specific or generic) for which a risk assessment is to be made.
(keywords	Under each date/time definition, specify keywords (or abbreviations) as appropriate: LOCK <u>Y</u> es <u>N</u> o <u>D</u> efault (or blank) Keywords are specified in the format a,v where a relates to token authentication and v relates to password validation. Since token authentication is not applicable to NC-PASS SECURE, you must enter the comma (,) first. Refer to <i>Keyword interpretation</i> on page 3.8 for details.

Line commands

You can use line commands F and N only on the first line in the column headed **O**. Option D can be used on any line in the **O** column. Line commands D, F or N perform the following functions

- D deletes the entry for the selected userid.
- F finds the first entry that matches the **USER** specified and displays that and all following entries. For example enter

```
O USER  
E TSG*
```

to start the display with the first userid that starts with TSG.
- N adds a new entry using the input fields described above.

Function keys

Key	Description
F1	displays help information.
F3	saves any changes and returns to the previous screen.
F7	displays the previous screen of userids.
F8	displays the next screen of userids.
F9	displays the TERMINAL RISK PROFILE panel.
F12	Cancels any changes and returns to the previous screen.

Locking userids and terminals

This section describes how userids and terminals are locked.

Locked users

A userid can be locked, that is barred from accessing the system, for any of the following reasons:

- the user profile has been set up with a Maximum Retry value; this has been exceeded. This means that $n+1$ incorrect attempts have been made to logon to the system using this userid (where the Maximum Retry value is set to n)
- the user profile has been set up with a Basic Lock Interval value greater than zero and the user has made an incorrect attempt to logon. This creates a temporary lock, with an expiry date. (If the expiry date, calculated by a given formula, is greater than one week, a permanent lock is created)
- the administrator has specified in the AUTOMATIC MESSAGE PROCESSING panel (1.3.2), that the user will be locked if certain criteria are met. (For example if a specific message is issued to a particular user and terminal more than twice in one minute the userid will be locked)
- the administrator has specified a lock through the PROCESS LOCKED USERS panel (5.8). This could be done, for example, while a user is on holiday.

A userid can be locked or unlocked only by an administrator with sufficient authority. This authority is determined by three entries in the administrator's profile definition:

Authority type	must be A (Administrator).
Authority group	the administrator must have control over the group to which the userid to be locked or unlocked, belongs.
Authority level	the administrator must be at the same or a higher level than the userid to be locked or unlocked (1 being the highest level, 255 the lowest).

Examples of authority settings are shown below:

Administrator id profile		Userid profile		Lock/unlock allowed?
Group	Level	Group	Level	
AB*	4	AB1234	20	YES
*	1	any	any	YES
C1	1	C2345	90	NO
C*	5	C2345	2	NO

The PROCESS LOCKED USERS panel (5.8), an example of which is shown below, displays a list of locked users within the NC-PASS system and provides the facility to lock or unlock individual users or groups of users.

```

Date:12/12/1997          PROCESS LOCKED USERS          Userid:TSG0001
Time:09:00              Terminal:A01MS258

Enter the userid to be locked and reason for locking below:
  Userid => _____ Specific or generic userid to be locked
  Reason => _____

Line commands: U=Unlock

S  USERID  REASON                EXPIRES   TIME  UPDATED   TIME  BY
_  BISACCT  annual leave                11/12/1997 09:15 TSG0001
_  BNLO011  2 BAD LOGON ATTEMPTS        11/12/1997 08:59 *SYSTEM*
_  BNLO123  1 BAD LOGON ATTEMPTS        13/12/1997 10:30 11/12/1997 10:00 *SYSTEM*
_  TSG0456  lost token                   11/12/1997 09:13 TSG0001

F1=Help  F3=End  F6=Terminal Lock  F7=Up  F8=Down

```

Input fields

Field	Description
Userid	determines the userid(s) to be locked. To specify a group of userids beginning with the same series of characters, enter the common 'stub' of characters followed by an asterisk (*). For example, to lock all userids beginning with TSG, enter TSG*. A single asterisk, however, is not permitted in this field because it would lock and deny subsequent access to ALL users. Note: It is your responsibility not to enter a generic userid such as A* (or a combination of userids) that would have the same effect as entering *.
Reason	enter the reason for locking a user or group of users. This is for information only.

Line commands

The line command U can be entered in column S against the appropriate userid to perform the following function:

U unlocks a locked userid.

Display fields

Field	Description
USERID	contains the id of a locked user.
REASON	contains the reason for the id being locked.
EXPIRES	indicates the date on which a temporarily locked id will be unlocked.
TIME	indicates the time at which a temporarily locked id will be unlocked.
UPDATED	indicates the date on which the id was locked.
TIME	indicates the time at which the id was locked.
BY	indicates who issued the lock command for a permanently locked id. If locked by the system due to incorrect logon(s) this field will display *SYSTEM*.

Function keys

Key	Function
F1	displays help information.
F3	saves the information and returns to the previous screen.
F6	displays the PROCESS LOCKED TERMINALS panel (6.4).
F7	displays the previous list of userids.
F8	displays the next list of userids.

Locked terminals

You can specify a lock for both real and imaginary terminals. Refer to *Terminal profiles overview* on page 3.3 for a description of the two types of terminal.

When a terminal has been locked a user will be unable to access the system(s) using this terminal, until you have unlocked it.

Terminals can be locked for any of the following reasons:

- the terminal profile has been set up with a basic lock interval value greater than zero and the user has made an incorrect attempt to logon. This creates a temporary lock, with an expiry date. If the expiry date, calculated by a given formula, is greater than one week, a permanent lock is created
- the administrator has specified in the AUTOMATIC MESSAGE PROCESSING panel (1.3.2), that the terminal will be locked if certain criteria are met. (For example if a specific message is issued to a particular terminal more than twice in one minute the terminal will be locked)
- the administrator has specified a lock through the PROCESS LOCKED TERMINALS panel (6.4). This could be done, for example, when a new series of terminals has been installed but is not yet in use.

A single terminal or group of terminals can be locked or unlocked by any administrator. A user cannot have access to any application or administration function through a locked terminal. When a terminal is locked, the appropriate logon panel is displayed on that terminal until it is unlocked.

The PROCESS LOCKED TERMINALS panel (6.4) displays a list of all locked terminals within the NC-PASS system and provides the facility to unconditionally lock or unlock terminals or group of terminals.

```

Date:12/12/1997          PROCESS LOCKED TERMINALS          Userid:TSG0001
Time:09:00              Terminal:A01MS258

Enter lock information below:
Terminal(s) => _____ Specific or generic terminal ID to lock
Reason      => _____

Line commands: U=Unlock

S  TERMINAL          LOCKED----- LOCK EXPIRES-----
   REASON          DATE       TIME BY      DATE       TIME
-  A01MS230        12/12/1997 11:55 TSG0001
   unused
-  A05IT005        12/12/1998 11:58 *SYSTEM* 12/12/97  12:02
   2 BAD LOGON ATTEMPTS

F1=Help  F3=End  F6=User Lock  F7=Up  F8=Down

```

Input fields

Field	Description
Terminal	<p>determines the terminal(s), real or imaginary, to be locked.</p> <p>real terminals enter the LU name of the terminal as defined to VTAM. To specify a group of terminals beginning with the same series of characters, enter the common 'stub' of characters followed by an asterisk (*). For example, to lock all terminals beginning with T012, enter T012*. A single asterisk, however, is not permitted in this field because it would lock and deny subsequent access to ALL terminals.</p> <p>Note: It is your responsibility not to enter a generic terminal id such as A* (or a combination of terminal ids) that would have the same effect as entering *.</p> <p>imaginary terminals:</p> <p>via APPC TLI enter the imaginary terminal in the format <i>requestor.node</i>.</p> <p>via XMS TLI enter the transaction identifier in the format <i>function.application</i> where the values are the contents of the parameters 'TERMID=' and 'APPL=' passed via the TLI call.</p>
Reason	<p>enter the reason for locking a terminal or group of terminals. This is for information only.</p>

Line commands

The line command U can be entered in column S against the appropriate terminal(s) to perform the following function:

U unlocks a locked terminal.

Display fields

Field	Description
TERMINAL	contains the id of a locked terminal.
REASON	contains the reason for the terminal being locked. If the terminal has been locked by an administrator, this field will contain the text input by the administrator when the terminal was locked. If the terminal has been locked by the system, a system generated message will be displayed.
LOCKED	
DATE	indicates the date on which a permanently locked terminal was locked.
TIME	indicates the time at which a permanently locked terminal was locked.
BY	indicates who issued the lock command for a permanently locked terminal. If locked by the system due to, for example, incorrect logon(s) this field will display *SYSTEM*.
LOCK EXPIRES	
DATE	indicates the date on which a temporarily locked terminal will be unlocked.
TIME	indicates the time at which a temporarily locked terminal will be unlocked.

Function keys

Key	Function
F1	displays help information.
F3	saves the information and returns to the previous screen.
F6	displays the PROCESS LOCKED USERS panel.
F7	displays the previous list of terminals
F8	displays the next list of terminals.

Escalated terminals and users

An escalated terminal or user is one which has had an incident recorded against it, according to the conditions specified in the AUTOMATIC MESSAGE PROCESSING panel (1.3.2).

The RESET ESCALATED TERMINALS AND USERS panel (1.3.3) provides the facility to reset escalated terminals and users.

Note: The reset command resets the permanent escalation record. This means that future messages will be issued as normal unless and until the rules specified by the administrator are breached again, as described in the following simple example:

The administrator creates the following entry in the AUTOMATIC MESSAGE PROCESSING panel (1.3.2).

```

----- SELECTION -----
- TIME -
ID  FREQ PERIOD  START END TERM USER  TERM USER SEV  ALTERNATE
                                MESSAGE
000001 0001 03 00:15 00:00 23:59 N  Y          E  0          0123

```

The following events occur:

Time	Event	NC-PASS escalation action
09:00	Message 0001 is issued to user TSG0001	None.
09:01	Message 0001 is issued to user TSG0001	None.
09:03	Message 0005 is issued to user TSG0001	None.
09:04	Message 0001 is issued to user TSG0001	None.
09:05	Message 0001 is issued to user TSG0001	NC-PASS writes a permanent escalation record and changes this and all subsequent messages to message number 0123, severity 0.
09:06	Message 0001 is issued to user TSG0001	NC-PASS changes this message to message number 0123, severity 0.
09:07	The administrator resets the record for userid TSG0001.	The permanent escalation record is reset.
09:08	Message 0005 is issued as normal.	None.
09:09	Message 0001 is issued to user TSG0001	NC-PASS will immediately write a permanent escalation record and change this and all subsequent messages to message number 0123, severity 0, because the number of times this message has been issued to this user, in the period specified above, has been exceeded.

Resetting escalated terminals and users

If the selection conditions specified in the AUTOMATIC MESSAGE PROCESSING panel (1.3.2) for a terminal or user have been satisfied, and the message severity and/or message number have been permanently escalated, option 1.3.3 will provide the following panel.

```
Date:12/12/1997      RESET ESCALATED TERMINALS AND USERS      Userid:TSG0001
Time:10:00          Terminal:A01MS258

Line commands: R=Reset

S  DATE          TIME          TERMINAL          USER          MSG  FQ  PER          TIME OF DAY
_  12/12/1997    09:12:14    A01MS123          0075  01  00:30  00:00  23:59
_  12/12/1997    09:29:44    10010220.8001601FB41  0520  02  00:01  00:00  23:59

F1=Help  F3=End  F7=Up  F8=Down  F10=Left  F11=Right
```

Press <F11> to display additional display fields.

Line commands

The line command R can be entered in column S against the appropriate line to perform the following function:

R resets a terminal or user. This will remove the permanent escalation record.

Display fields

Field	Description
DATE	the date on which the escalation took place.
TIME	the time at which the escalation took place.
TERMINAL	the id of the escalated terminal. This can be a real or imaginary terminal. Refer to <i>Terminal profiles overview</i> on page 3.3 for an explanation of these terminal types.
USER	the userid of the escalated user.
MSG	the original four digit message number.
FQ	the number of times the message was issued before escalation occurred. This is the value recorded in the FREQ field on the AUTOMATIC MESSAGE PROCESSING panel (1.3.2).
PER	the period in which the messages were issued.

Field	Description
TIME OF DAY	
START/END	the period during which the message causing the escalation was issued.
Press <F11> to page right to display the following fields:	
SEL	
T	Y shows that the message was issued to a specific terminal or terminals (otherwise N is displayed).
U	Y shows that the message was issued to a specific user or users (otherwise N is displayed).
ESC	
T	E shows that the message to the terminal was escalated.
U	E shows that the message to the user was escalated.
S	displays the severity of the message to be issued.
ALT	displays the number of the alternative message to be issued.

Function Keys

Key	Function
F1	displays help information.
F3	ends the display and returns to the previous panel.
F7	displays the previous screen of escalated terminals and users.
F8	displays the next screen of escalated terminals and users.
F10	scrolls left.
F11	scrolls right.

Example

In the panel on page 3.43 a permanent escalation record is displayed for terminal A01MS123. An event occurred to produce the record as follows:

The event occurred at 09:12:14 on 12th December 1997.

Message 0075 was issued more than the permitted frequency of once, within a period of 30 minutes (it was issued at 09:12:14 and once prior to 09:12:14).

The message was issued to the same terminal on both occasions.

The identity of the user was not taken into consideration. The message could have been issued to different users using the same terminal.

There was no critical period. The time of day was not considered.

The resulting escalation record has the following effect:

Message 0006 at severity level 0 will replace all subsequent issues of messages to terminal A01MS123, regardless of user.

Other terminals are not affected. They receive all messages, including 0075, as usual.

PassTickets

RACF v1.9.2 includes a Secured Signon function which provides an alternative to the RACF password associated with specific user profiles. The feature is known as a PassTicket.

The RACF PassTicket is a short-life, one-time-only password which becomes invalid after use or, if not used, after approximately 10 minutes. The RACF PassTicket is derived from the userid, application name, system time (GMT) and a secret data encryption key.

PassTickets can only be used with RACF v1.9.2 or above, on the host MVS system on which NC-PASS is running. With RACF v1.9.2, the Secured Signon SPE (Small Programming Enhancement) APAR OY65281 is also required.

Why are PassTickets used?

Typically, PassTickets are for use over emulators. If a user's password is sent across the network in clear text, it could be illegally intercepted and used by an unauthorized person. It is not always possible to encrypt a password, since the target application or system may not be able to decrypt it.

The use of PassTickets removes the need to send clear text passwords across the network.

Further information

For full details of RACF PassTickets, their definition, life expectancy and use, refer to the IBM manual *RACF Secured Signon SPE Information Package (SC23-3765)*.

Configuration

The configuration required to allow the verification of RACF PassTickets by NC-PASS can be split into the following steps:

On the platform that requests a RACF PassTicket

Complete the step below on the platform that requests a PassTicket.

Step 1 Ensure that the application name passed to NC-PASS on the process code 55 call (request for RACF PassTicket) is the same as that defined in Step 1 of the RACF configuration below.

On RACF

The following steps assume that you already have a RACF PTKTDATA class defined.

Step 1 Choose a RACF application profile name for NC-PASS. It is recommended that you use the acbname of NC-PASS as specified in the ACBNAME= startup option for NC-PASS.

Step 2 Define the NC-PASS application profile name to the RACF PTKTDATA class and associate it with a secret data encryption key, eg

```
RDEFINE PTKTDATA NCPASS-profile-name SSIGNON(KEYMASKED(key))
```

This allows NC-PASS to accept RACF PassTickets.

The key can be any valid hex data, for example x'FOF1F2F3F4F5F6F7F8'. Further details are supplied in your RACF documentation.

Step 3 Activate the RACF PTKTDATA class and refresh RACF (once all the changes have been made) by entering the following commands:

```
SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA) REFRESH
```

On NC-PASS

Complete the steps below to allow RACF PassTickets to be accepted by NC-PASS.

Step 1 Log on to NC-PASS as an administrator and select option 1 **System Administration** from the main menu.

Step 2 Select option 1, **General system options**, to display the GENERAL SYSTEM OPTIONS panel.

```
Date:12/12/1997          GENERAL SYSTEM OPTIONS          Userid:TSG0001
Time:09:00              Terminal:A01MS242

General options:
Date format              => 3          1=YYYY/MM/DD 2=MM/DD/YYYY
                          3=DD/MM/YYYY 4=DDMMMYYYY
Separator character     => /          Separates date elements for formats 1-3
Idle time                => 0          Specify idle time for administration and
                          logo panels before timeout occurs.
Length of log           => 999       The limit on the number of lines to be
                          retained in the NC-PASS message log
Concurrent systems      => Y          Enter 'Y' to permit other NC-PASS systems
                          to be started
Default user profile    => _____ When creating user profiles this name can
                          be used instead of a model name

External security options:
Default logon node      => _____ Default for remote node on logon
Accept RACF PassTickets => Y          Y/N
RACF PTKTDATA name     => TSOCK01

F1=Help  F3=End  F12=Can
```

Step 3 Enter Y in the **Accept RACF PassTickets** field.

Step 4 Enter the NC-PASS application profile name, as chosen in Step 1 under the heading *On RACF* on page 3.45, in the **RACF PTKTDATA name** field.

Step 5 Press <F3> to save your entries. NC-PASS is now configured to accept PassTickets as part of an authentication request.

Home node processing

In multi-node networks, NC-PASS databases can be held on individual nodes supporting definitions for users assigned to that node.

Home node processing is a valuable feature on large networks where users want to access the system from different locations.

A user need only be defined to NC-PASS on the 'home' node, ie the location from which he normally operates. When connecting to a node which is not the machine to which the user would normally connect, he can specify the name of his home node; NC-PASS on the home node will perform validation as normal.

To use the home node processing feature, the following administrative tasks must be performed:

- NC-PASS must be installed on the home node and any remote node to which the user can connect
- MHO communications must be set up on the user's home node and any remote node to which they can connect - refer to *Chapter 1 - Communicating with other systems (Volume 2)*
- users must be defined to NC-PASS on the node to which they normally connect.

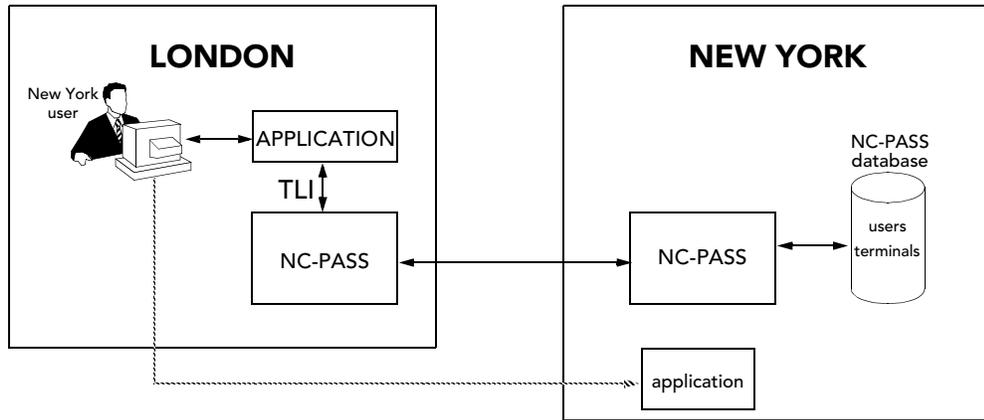
When a user attempts to logon from a remote node, he must specify the name of the home node on the logon panel in order to use the home node feature.

The name of the home node is the name specified by the administrator, on the home node, in the **MHO host nodename** field on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1).

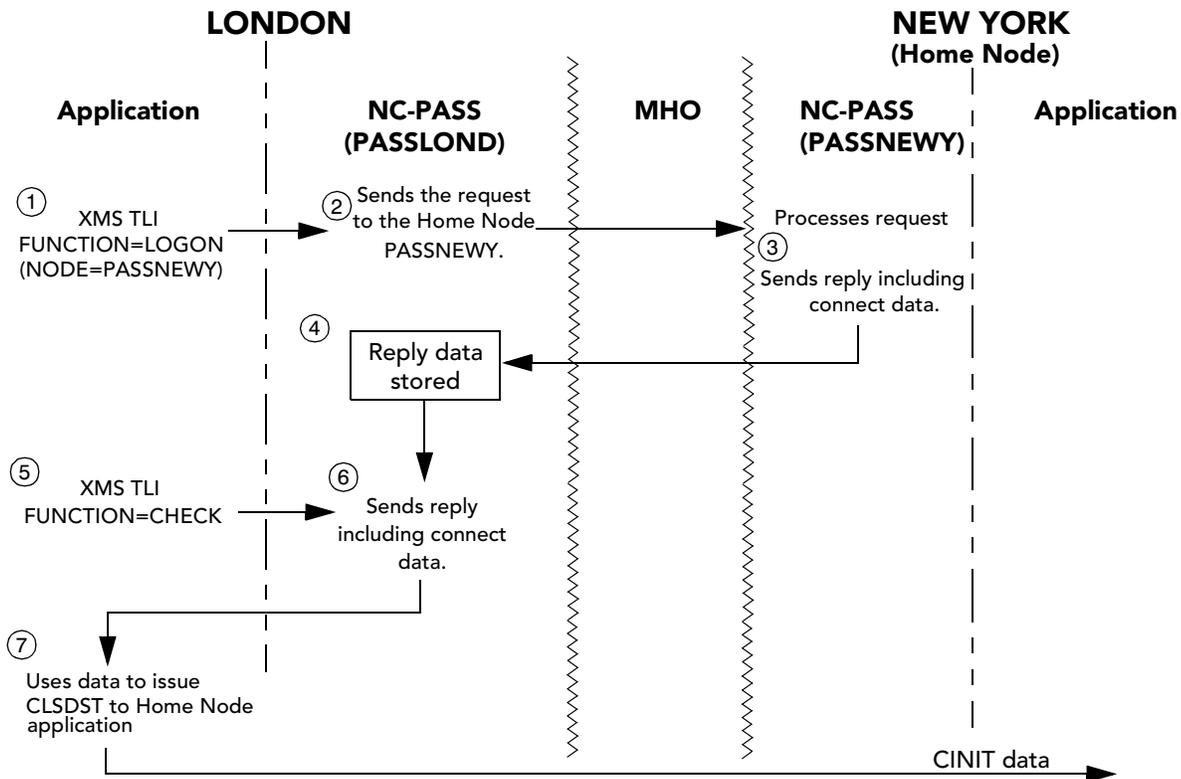
If the administrator has specified a symbolic name, the user can specify this name instead.

Using the TLI to request Home Node Processing

The Transaction Level Interface (See *Chapter 2 - Transaction Level Interface (TLI)* in Volume 2) can be used to return the userid's connect information; this allows the Home Node Processing facility to be available to front-end applications (for example session managers) that invoke NC-PASS to initiate security checking, as shown in the diagram below.



When an application sends a FUNCTION=LOGON or FUNCTION=CHECK TLI request to the local NC-PASS, with the NODE=home-node parameter specified, the Home Node NC-PASS includes the connect data fields in its reply. A diagrammatic representation of this is shown below, where PASSLOND and PASSNEWY are the MHO nodenames of the two NC-PASS jobs.



PROCESSING OVERVIEW

The two TLI functions that are available for Home Node Processing are described on the following pages.

FUNCTION=LOGON

The LOGON function authenticates a userid according to the criteria specified for that userid in NC-PASS. For example, if the user profile specifies that a RACF password must be used, this data must be provided or the user will fail the check.

This function is specified with the following mandatory parameters:

RETAREA= <i>returnarea</i>	<p>This is an area used to return information to the application making the LOGON request.</p> <p>This keyword is mandatory for the SEXMITNC, SEXMITOS and SEXMIT interfaces.</p> <p>If not supplied, variable <i>&usrretc</i> will be set to 20(X'14') and the message 'NC-PASS TLI PARAMETER ERROR - NO RETURN AREA SPECIFIED' will be output.</p> <p>The destination of this message will be:</p> <table><tr><td>SEXMITNC</td><td>NCI log</td></tr><tr><td>SEXMITOS</td><td>SYSLOG (console)</td></tr><tr><td>SEXMIT</td><td>SYSLOG (console)</td></tr><tr><td>SEXMITTS</td><td>Screen (TPUT)</td></tr></table> <p>The format of the RETAREA parameter is described in <i>Reply to FUNCTION=LOGON (Home Node processing)</i> on page 3.54.</p>	SEXMITNC	NCI log	SEXMITOS	SYSLOG (console)	SEXMIT	SYSLOG (console)	SEXMITTS	Screen (TPUT)
SEXMITNC	NCI log								
SEXMITOS	SYSLOG (console)								
SEXMIT	SYSLOG (console)								
SEXMITTS	Screen (TPUT)								
USERid=xxxxxxx	<p>The userid to be authenticated (maximum 8 characters).</p>								
XMSID=xxxx	<p>The 4 byte XMS Identifier used by the target NC-PASS system.</p> <p>The default is XMS1.</p>								

The following optional parameters can also be specified for this function:

MSG= <i>message text</i>	<p>Allows the calling application to issue audit messages. <i>message-text</i> can be a text string or an NC-PASS message number.</p>
NODE=xxxxxxx	<p>This is the MHO node used by NC-PASS to communicate with other NC-PASS systems.</p> <p>If specified, the LOGON request will be routed to the system identified by the node. You can specify the symbolic node name instead of the VTAM nodename if required.</p> <p>LOGONs routed to other NC-PASS systems are always processed asynchronously. To obtain the results of the LOGON, code FUNCTION=CHECK.</p> <p>If omitted, the default is the local node.</p>
NEWPass (or NPASS) =xxxxxxx	<p>The new password specified by the userid (maximum 8 characters).</p>

OUTPUT= <i>destination</i>	<p>Determines the destination of the trace output:</p> <ul style="list-style-type: none"> N - NCI log (default for SEXMITNC). If the program is not running under NCI, OUTPUT=W is assumed. T - TSO terminal using the TPUT macro (default for SEXMITTS). If the program is not running under TSO, OUTPUT=W is assumed. W - Output to operator console (default for SEXMITOS).
PASSword=xxxxxxx	The user's password (maximum 8 characters).
RETID= <i>variable</i>	<p>A 4-byte area required to obtain the data returned by a previous asynchronous (XMSOPT=ASY) function request. Data from the previous asynchronous function is obtained using FUNCTION=RETDATA passing RETID as one of its parameters.</p> <p>An asynchronous function request will always generate a RETID.</p>
TERMid=xxxxxxx	The id of the terminal to which the user is attempting to logon.
TIMEOUT= <i>nnnn</i>	The timeout interval, in hundredths of seconds, used with XMSOPT=SYN to establish a maximum time to wait for a reply.
TRACElevel= <i>n</i>	<p><i>n</i> is a number from 0 through 9 specifying the level of tracing to be performed during execution of the LOGON. 0 means no tracing and 9 means full tracing. This parameter should normally only be used on request from your local support office.</p> <p>The default is 0.</p>
VRM= <i>vrnm</i>	<p>The minimum version of NC-PASS that supports the functions required, where:</p> <ul style="list-style-type: none"> <i>v</i> is the version number <i>r</i> is the release number <i>m</i> is the modification level <p>To use the Home Node feature, this parameter must be set to 202.</p>

XMSOPT=*process*

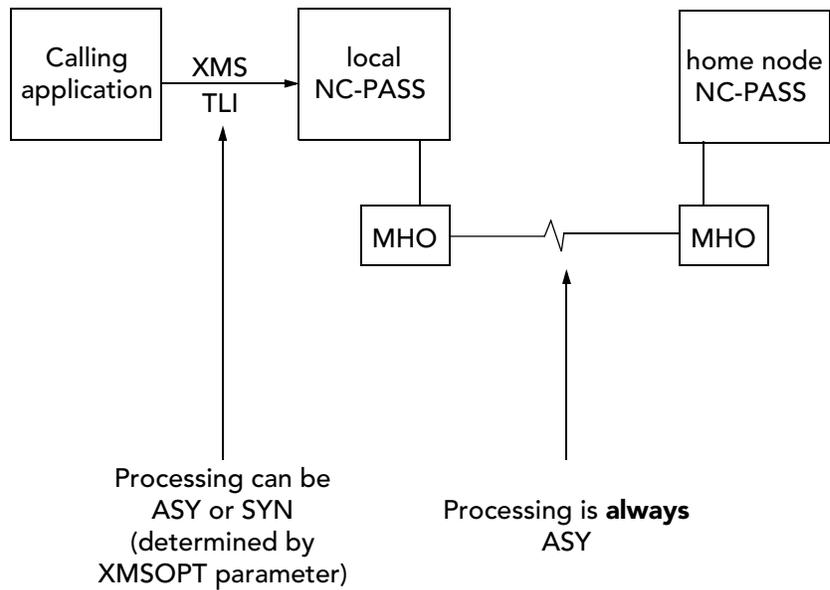
This determines the type of communication process **to the local NC-PASS** and can be one of the following:

SYN - The LOGON is processed synchronously; the calling program will stop processing until the reply to the LOGON has been received from the local NC-PASS. For home node processing, the reply to the LOGON shows whether the LOGON request has been successfully passed to the Home Node. SYN is the default.

ASY - The LOGON is processed asynchronously. This allows the calling program to continue processing while NC-PASS is processing the LOGON request. The calling program will have to make a further FUNCTION=RETDATA call to obtain the result of the asynchronous call.

NOR - No reply will be returned from the LOGON to the calling program.

The diagram below explains the processing options.



FUNCTION=CHECK

This function is used to check the result from a previous TLI call, for example FUNCTION=LOGON.

When an MHO node has been specified in a FUNCTION=LOGON call, the processing to satisfy that request will be carried out by another NC-PASS system; this processing is asynchronous with the XMS function.

To discover the result of the FUNCTION=LOGON call, your application must issue one or more further TLI calls using the CHECK function.

This function is specified with the following mandatory parameters:

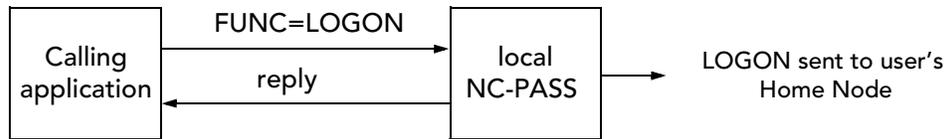
RETAREA= <i>returnarea</i>	<p>This is an area used to return information to the application making the CHECK request.</p> <p>If not supplied, variable <code>&usrretc</code> will be set to 20(X'14') and the message 'NC-PASS TLI PARAMETER ERROR - NO RETURN AREA SPECIFIED' will be output.</p> <p>The destination of this message will be:</p> <table><tr><td>SEXMITNC</td><td>NCI log</td></tr><tr><td>SEXMITOS</td><td>SYSLOG (console)</td></tr><tr><td>SEXMIT</td><td>SYSLOG (console)</td></tr><tr><td>SEXMITTS</td><td>Screen (TPUT)</td></tr></table> <p>The format of <i>returnarea</i> is described in <i>Reply to FUNCTION=CHECK request (Home Node processing)</i> on page 3.55.</p>	SEXMITNC	NCI log	SEXMITOS	SYSLOG (console)	SEXMIT	SYSLOG (console)	SEXMITTS	Screen (TPUT)
SEXMITNC	NCI log								
SEXMITOS	SYSLOG (console)								
SEXMIT	SYSLOG (console)								
SEXMITTS	Screen (TPUT)								
TXID= <i>xxxx</i>	<p>Transaction id returned by previous asynchronous call, ie the LOGON. This is returned in positions 5 through 8 of the <i>returnarea</i>.</p>								
USERid= <i>xxxxxxxx</i>	<p>The userid to be checked (maximum 8 characters).</p>								
XMSID= <i>xxxx</i>	<p>The 4 byte XMS Identifier used by the target NC-PASS system.</p> <p>The default is XMS1.</p>								

The following optional parameters can also be specified for this function:

MSG= <i>message text</i>	Allows the calling application to issue audit messages. <i>message-text</i> can be a text string or an NC-PASS message number.
OUTPUT= <i>destination</i>	Determines the destination of the trace output: <ul style="list-style-type: none">N - NCI log (default for SEXMITNC). If the program is not running under NCI, OUTPUT=W is assumed.T - TSO terminal using the TPUT macro (default for SEXMITTS). If the program is not running under TSO, OUTPUT=W is assumed.W - Output to operator console (default for SEXMITOS).
RETID= <i>variable</i>	<p>A 4-byte area required to obtain the data returned by a previous asynchronous (XMSOPT=ASY) function request. Data from the previous asynchronous function is obtained using FUNCTION=RETDATA passing RETID as one of its parameters.</p> <p>An asynchronous function request will always generate a RETID.</p>
TERMid= <i>xxxxxxxx</i>	The id of the terminal to which the user is attempting to logon.
TIMEOUT= <i>nnnn</i>	The timeout interval, in hundredths of seconds, used with XMSOPT=SYN to establish a maximum time to wait for a reply.
TRACElevel= <i>n</i>	<p><i>n</i> is a number from 0 through 9 specifying the level of tracing to be performed during execution of the CHECK. 0 means no tracing and 9 means full tracing. This parameter should normally only be used on request from your local support office.</p> <p>The default is 0.</p>
VRM= <i>vrn</i>	<p>The minimum version of NC-PASS that supports the functions required, where:</p> <ul style="list-style-type: none"><i>v</i> is the version number<i>r</i> is the release number<i>m</i> is the modification level <p>To use the Home Node feature, this parameter must be set to 202 or later.</p>
XMSOPT= <i>process</i>	<p>This determines the type of communication process and can be one of the following:</p> <ul style="list-style-type: none">ASY - The CHECK is processed asynchronously. This allows the calling program to continue processing while NC-PASS is processing the CHECK. The calling program will have to make a further FUNCTION=RETDATA call to obtain the result of the asynchronous call.NOR - No reply will be returned from the CHECK to the calling program.SYN - The CHECK is processed synchronously; the calling program will stop processing until the CHECK has completed. This is the default.

Reply to FUNCTION=LOGON (Home Node processing)

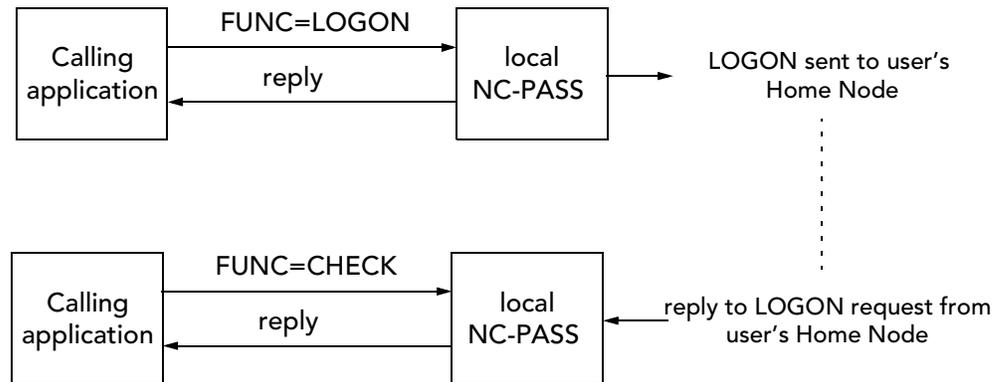
In the scenario shown in the following diagram, replies from the local NC-PASS are stored in the return area in the format shown below.



Position	Format	Contents
1 - 4	zoned decimal	NC-PASS message number generated by the TLI function. If this field contains a number other than: 0000 (LOGON function passed to Home Node SUCCESSFUL) the local NC-PASS has been unable to send the LOGON request to the user's Home Node. The message relating to the number returned in this field will be output between messages CKxx3047 and CKxx3048. Refer to <i>Audit</i> on page 3.59.
5 - 8	zoned decimal	The transaction identifier (TXID) generated by NC-PASS for TLI functions that result in an MHO call.

Reply to FUNCTION=CHECK request (Home Node processing)

In the scenario shown in the following diagram, replies from the local NC-PASS are stored in the return area in the format shown below.



Replies from NC-PASS are stored in the return area in the format shown below.

Position	Format	Contents
1 - 4	zoned decimal	NC-PASS message number generated by the TLI function. If this field contains a number other than: 2064 (LOGON SUCCESSFUL) or 0061 (PASSWORD EXPIRED) or 0025 (NEW PASSWORD UNACCEPTABLE) the user has failed validation/authentication. The message relating to the number returned in this field will be output between messages CKxx3047 and CKxx3048. Refer to <i>Audit</i> on page 3.59.
5 - 8	zoned decimal	The transaction identifier (TXID) generated by NC-PASS for TLI functions that result in an MHO call.
30 - 37	char	Nodename of the target application. This field is returned only if the VRM= parameter is specified as 202 or later.
38 - 102 (max)	char	CINIT data from the user's connect definitions. This is variable length and may be encrypted. Refer to <i>Encryption of the CINIT field</i> on page 3.58. This field is returned only if the VRM= parameter is specified as 202.

Values returned in the Nodename and CINIT fields

The values returned in the Nodename and CINIT data fields in the return area, are dependent on the values stored for the user profile on the remote NC-PASS system.

Each userid on the remote NC-PASS system has a Connect Definition, an example of which is shown below. (This information can either be held on the NC-PASS database or on an external security database, eg RACF.)

The Connect Definition specifies the destination to which the user will be connected after successful authentication/validation.

Connect definitions are fully described in *The CONNECT DEFINITION for USERID panel* on page 3.26.

```
Date:12/12/1997          CONNECT DEFINITION for NEWUSER          Userid:TSG0001
Time:09:00              Terminal:A01MS268

'Code' relates to name in 'Dest': N=Nodename E=Exec K=Keyword M=Menu

      CODE DEST      TERMID  DATA PASSED TO APPLICATION  USER COMMENT
000001 N   PROLLM   *        SYSUSER/SYSPASS              Payroll
***** *   *****  *****  *****

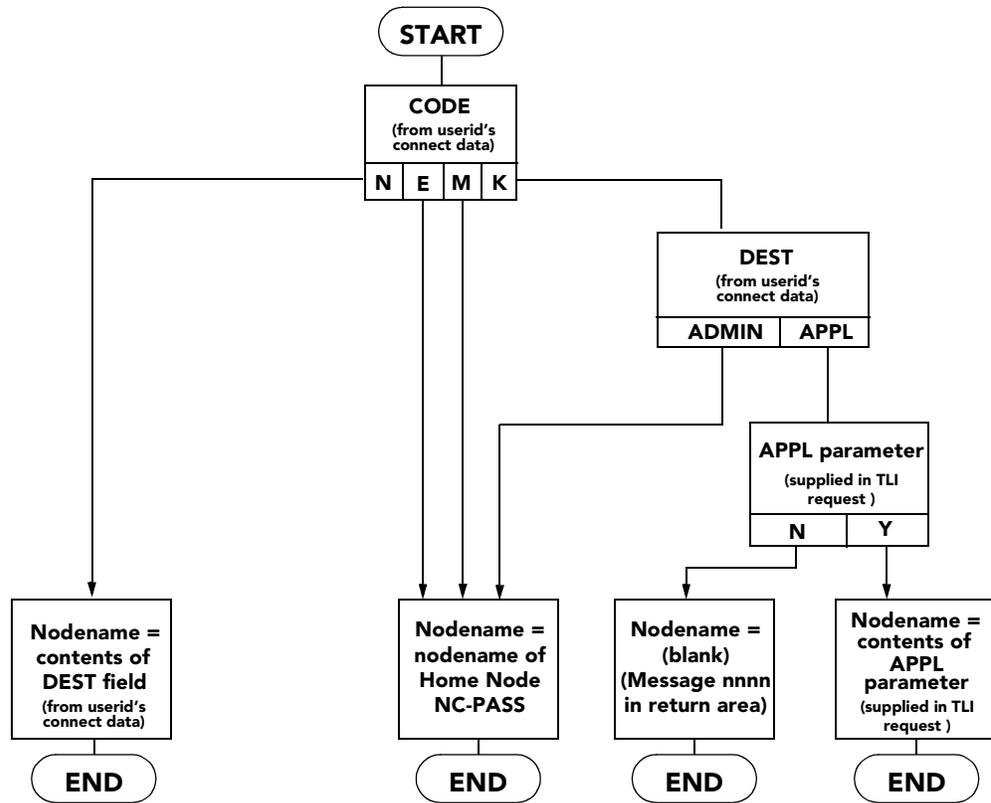
F1=Help  F3=End  F6=User profile  F7=Up  F8=Down  F12=Can
```

During Home Node Processing, NC-PASS uses the CODE, DEST and DATA PASSED TO APPLICATION fields to determine the information to be returned to the calling NC-PASS, as described on the following pages.

The TERMID and USER COMMENTS fields are not accessed for Home Node Processing.

How the Nodename to be returned is determined

The data returned to the calling application for Nodename (position 30-37 of the return area) is determined by source information from the user's profile connect data and, optionally, the TLI APPL parameter, as shown in the diagram below.



How the CINIT data to be returned is determined

The contents of the DATA PASSED TO APPLICATION field from the user's profile connect data are returned to the calling application as CINIT data (position 38-*nnn* of the return area).

The contents of this field are passed 'as is', there is no translation of variables or keywords.

Encryption of the CINIT field

The CINIT data is a variable length field of up to 65 characters in length, starting in position 38.

If the user's connect data contains 'K' in the CODE field and 'ADMIN' in the DEST field, the user will be transferred to NC-PASS as an administrator after a successful logon attempt. In this case, the contents of the CINIT field are encrypted before transmission to the local node.

When NC-PASS at the user's home node is presented with encrypted CINIT data, it will be decrypted before use.

In all other circumstances, ie where the user is transferred to an application other than NC-PASS after a successful logon, the CINIT data is transmitted in clear text.

Note: When the CINIT data is encrypted, it is your responsibility to test the length of the variable to ensure no trailing blanks will be decrypted and cause validation to fail.

Data extraction example

The following example shows how to retrieve the CINIT data using NCI.

In an NCI application, code

```
SET &cinit = &retarea (38:)
```

where:

&cinit is the name of the variable to be set.

&retarea is the variable containing the contents of the return area.

As the CINIT data is of variable length, you must code the retarea positions as (38:) meaning from position 38 to the end, rather than specifying an end position, ie (38:50).

This will ensure that the correct length of data will be extracted from the return area.

Coding an incorrect end position will cause unpredictable results.

Note: The above example is coded using NCI. Whatever language you use, you must ensure that the correct length of data is extracted from the return area.

Processing considerations

This section highlights the processing considerations when connecting a user to a target application, following authentication on his home node NC-PASS system using TLI calls.

Return of CINIT data

CINIT data is returned in positions 38-102 of the return area only for FUNC=LOGON and FUNC=CHECK TLI calls.

If processing is such that further TLI calls are made (that do not return CINIT data) before the user is connected to his target application, you must ensure that your application stores the CINIT data for subsequent use. This could happen, for example, where a user's password has expired and is changed before connection to the application.

Password change

CINIT data may contain a user's password. If a TLI call results in the return of message 0061 (Password expired), the CINIT data will contain the existing password. If processing is such that further TLI calls are made to change the user's password, prior to connection, the application must ensure that:

- the CINIT data is stored before the call to change the password, and
- on successful completion of the change password request, the password stored as part of CINIT is replaced by the new password, prior to application connect.

Audit

The following messages will be output from a TLI call:

```
CKxx3047 PROCESSING TLI REQUEST (JOB=xmjobname FUNC=function)
...
  other audit message as appropriate eg CKxx0024 PASSWORD INVALID
...
CKxx3048 TLI PROCESSING COMPLETED (RC=rc)
```

where

<i>xmjobname</i>	is the name of the job from where the TLI call originated.
<i>function</i>	is the TLI function requested, eg AUTH.
<i>rc</i>	is one of the following return codes: 0 completed successfully 4 more information required 8 failed 20 invalid parameters.

Messages are documented in *Chapter 6 - Messages and abend codes* (Volume 2).

TLI Home Node Processing between different versions of NC-PASS

TLI Home Node Processing is supported (ie Connect Data is returned) when NC-PASS v2.0, modification level 2 or above is running on both the Home Node and the local node and the TLI VRM parameter is set to 202 or above.

If either the Home Node or the local node is running a previous version of NC-PASS (ie NC-PASS v2.0 modification level 1 and below), TLI Home Node Processing is not supported (ie Connect Data is not returned).

This page intentionally left blank

Chapter 4 - Using risk profiles to control access

Introduction	4.2
Auditing	4.2
Protecting dial-in to the host	4.3
Operational requirements	4.3
Security objective	4.3
Administration	4.3
Example 1	4.5
Example 2	4.6
Preventing a userid from gaining access at specified times	4.7
Example scenario	4.7
Security objective	4.7
Administration	4.7
Processing	4.8

Introduction

The concept of risk profiles was introduced in *Chapter 3 - Controlling user access*.

Before reading this chapter you should be familiar with the following subjects:

- user profiles
- terminal profiles
- risk profiles.

This chapter provides a number of examples of how to use risk profiles to achieve access control objectives.

Auditing

NC-PASS produces a complete audit record of all logon attempts, both failed and successful, which you can record permanently. Refer to *Chapter 9 - Auditing*.

Protecting dial-in to the host

This section describes a scenario in which steps are taken to protect access to the host from dial-in terminals. Two examples are provided to show how NC-PASS processes a user's attempt to log on.

Operational requirements

Sales staff need to dial in to a customer enquiry application running on the host.

Each salesman has:

- a single unique userid that is password protected by RACF in the format Sxxaaa where xx is the sales region number and aaa is the salesman's initials.

Session requests from terminals accessing the system via dial-in lines are allocated from a pool of terminal ids whose names are prefixed by D. Dial-in terminals are LOGAPPL'd to NC-PASS.

Security objective

The security administrator wants to ensure that:

- dial-ins are only allowed during the sales force's working hours, typically between 8 a.m. and 8 p.m.
- users dialling in are always password verified to confirm they are who they say they are.

Administration

The following steps have been carried out:

1. RACF userids for each salesman have been created and defined.
2. An NC-PASS user profile record has been created for userid S*. RACF password validation is specified and a connect definition to the customer enquiry application has been defined. (Refer to *Chapter 3 - Controlling user access*).

3. The following entries have been defined on the terminal risk profile:

```

Date:12/12/1997          TERMINAL RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS264

Line Commands: D=Delete  F=Find  N=New

                                DATE/TIME DEFINITIONS
0 TERMINAL                      STATEHOL  WORKWEEK  EVENING  WEEKEND  OUTHOURS  ALWAYS
-----
ADM*                             Y         Y         Y         Y         Y         Y
D*                               LOCK     ,F       ,F       LOCK     LOCK     LOCK
RECEPT10                       ,B
SUPERV*                          LOCK     ,Y       ,Y       ,F       ,F       LOCK

F1=Help  F3=End  F7=Up  F8=Down  F9=Swap  F12=Can

```

The date/time definitions have been created as follows:

- STATEHOL contains the dates of all state holidays.
- WORKWEEK Monday through Friday, 08:00 through 18:00.
- EVENING Monday through Friday, 18:00 through 20:00.
- WEEKEND Saturday and Sunday, 00:00 through 23:59.
- OUTHOURS Monday through Friday, 20:00 through 08:00.
- ALWAYS All days, dates and times.

(Refer to *Chapter 6 - Restricting access by date and time*).

4. No user risk profile has been created.

Example 1

A member of the Sales team dials in to the host on Wednesday morning at 9 a.m. using userid S02BGF.

NC-PASS searches the appropriate profile records:

User profile	NC-PASS on the host finds a match with user profile S*. This specifies that RACF password validation is in force.
Terminal risk profile	a match is found with D*. The date and time of the verification request matches with the WORKWEEK definition. The keywords at the intersection of the matching terminal id (D*) and the matching date/time definition (WORKWEEK) are extracted.
User risk profile	no match is found for userid S02BGF. NC-PASS will use the keyword 'Default' for validation when determining the risk for this userid.

The keywords from the terminal and user risk profiles are combined as follows:

	User	Terminal	Result
Validation	Default	F	password is required

Refer to *Keyword interpretation* on page 3.8 for further details.

A panel is displayed requesting password details.

If the correct password details are entered, the user will be logged on to the host and connected to the application. If he enters the wrong password, logon will be denied.

This ensures that a user **must** provide two items of information in order to logon from a dial-in line:

- a valid userid
- a password

Example 2

In addition to its sales staff, the company employs a number of administrative staff who have a userid in the format *Axxnnn* where *xx* is the sales region number for which they provide a service, and *nnn* is the employee's initials. Administrative staff do not have RACF passwords.

An employee attempts to dial in to the host on Wednesday evening at 7 p.m. using his userid A01ABH.

NC-PASS accesses the appropriate profile records:

User profile	NC-PASS on the host finds a match with user profile A*. This specifies that no password validation is in force.
Terminal risk profile	a match is found with D*. The date and time of the verification request matches with the EVENING definition. The keywords at the intersection of the matching terminal id (D*) and the matching date/time definition (EVENING) are extracted.
User risk profile	no match is found for userid A01ABH. NC-PASS will use the keyword 'Default' for validation when determining the risk for this userid.

The keywords from the terminal and user risk profiles are combined as follows:

	User	Terminal	Result
Validation	Default	F	password is required

Refer to *Keyword interpretation* on page 3.8 for further details.

The risk profiles insist that a password is used; since the employee does not have a password, NC-PASS does not allow the logon attempt.

Preventing a userid from gaining access at specified times

This section provides an example of the steps required to ensure authorized use of a userid.

Example scenario

A company's office hours are from 9 a.m. to 5:30 p.m. All clerical staff have a userid in the format CHQ abc where abc are the initial letters of the user's first, middle and last name respectively.

Security objective

All clerical staff userids must be password controlled and only available for use in office hours.

Administration

The following steps have been carried out on the host:

1. RACF userids for each member of staff have been created and defined.
2. An NC-PASS user profile record has been created for userid CHQ*. RACF password validation is specified. (Refer to *Chapter 3 - Controlling user access*).

3. The following entries have been defined on the user risk profile:

```

Date:12/12/1997          USER RISK PROFILE          Userid:TSG0001
Time:09:00                Terminal:A01MS266

Line Commands: D=Delete  F=Find  N=New

                                DATE/TIME DEFINITIONS
0 USER                STATEHOL  WORKWEEK  EVENING  WEEKEND  OUTHOURS  CATCHALL
-----
CHQ*                   LOCK      ,Y       LOCK     LOCK     LOCK      LOCK

F1=Help  F3=End  F7=Up  F8=Down  F9=Swap  F12=Can

```

The date/time definitions have been created as follows:

STATEHOL	contains the dates of all state holidays.
WORKWEEK	Monday through Friday, 09:00 through 17:30.
EVENING	Monday through Friday, 17:30 through 20:00.
WEEKEND	Saturday and Sunday, 00:00 through 23:59.
OUTHOURS	Monday through Friday, 20:00 through 09:00.
CATCHALL	All days, dates and times.

(Refer to *Chapter 10 - Restricting access by date and time*).

Processing

The entry in the USER column on the risk profile shows the generic identifier for the clerical users. This entry means that a logon attempt by clerical staff will only be allowed, during office hours, if the user logging on provides the correct password details.

Any attempt to access the system outside of office hours, using a userid starting with CHQ, will be rejected.

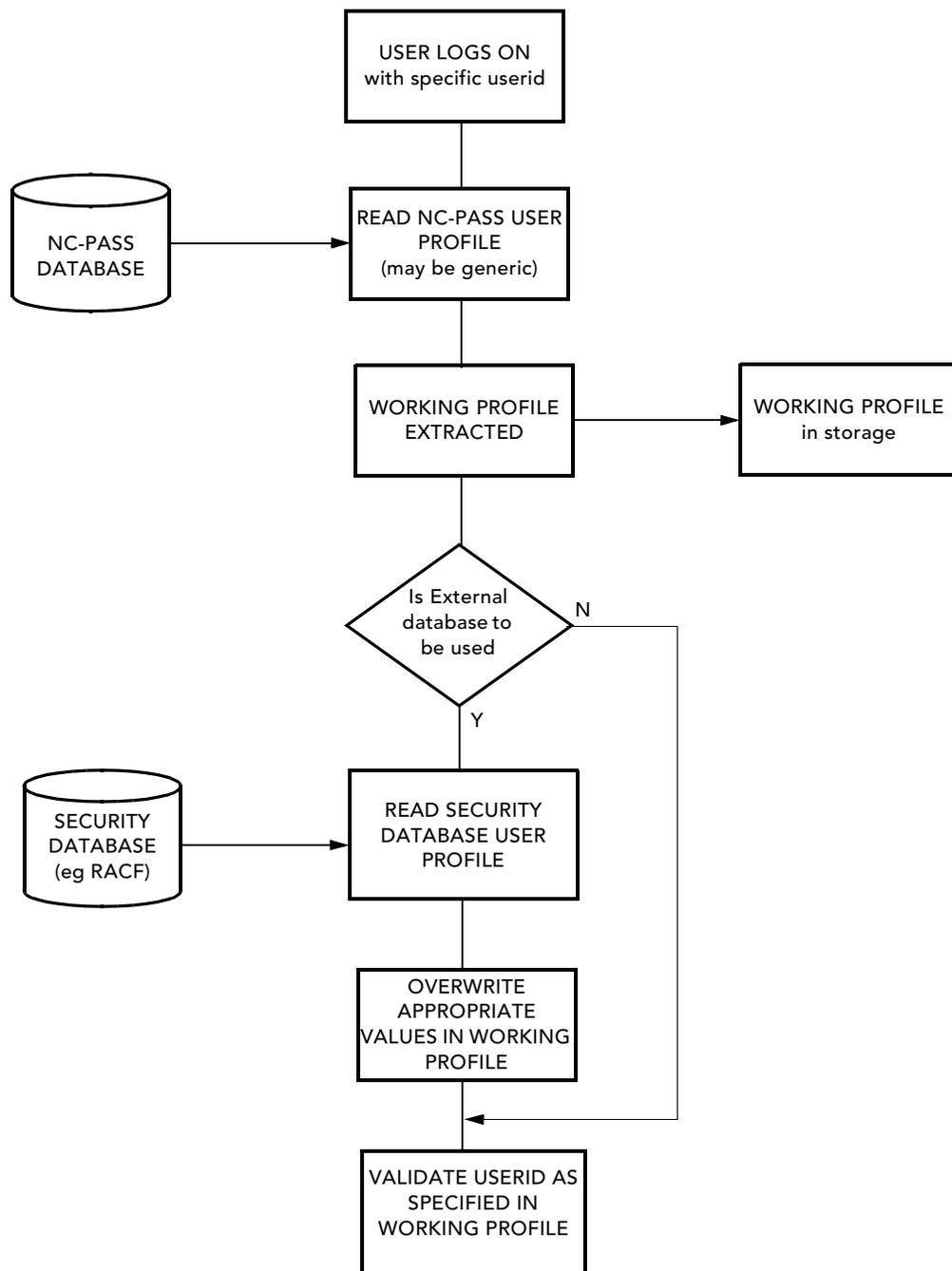
Chapter 5 - Administering users from an external security database

Determining userid validation requirements	5.2
Advantages of storing data on an existing security database	5.3
Setting up the system	5.3
Storing data on RACF	5.4
Editing the INSTALLATION DATA field	5.5
Examples of storing user risk profile data on RACF	5.5
Setting NC-PASS parameters	5.6
Specifying the use of an external security database	5.6
Data fields and keywords	5.6
How NC-PASS extracts the data	5.8
Specifying multiple keywords for a given field	5.10
Data validation	5.10
KEYWORD DEFINITIONS panel	5.12

Determining userid validation requirements

When a user attempts to logon through NC-PASS, a userid profile is built from data stored in the NC-PASS database. This userid profile is used to determine whether user access is allowed and if so, what user validation information is required.

Using the external security database function, you can store selected userid profile data on an external security database. When the user attempts to logon through NC-PASS, this data is extracted and used to build the userid profile, overriding any data previously extracted from the NC-PASS database, as shown in the diagram below.



Advantages of storing data on an existing security database

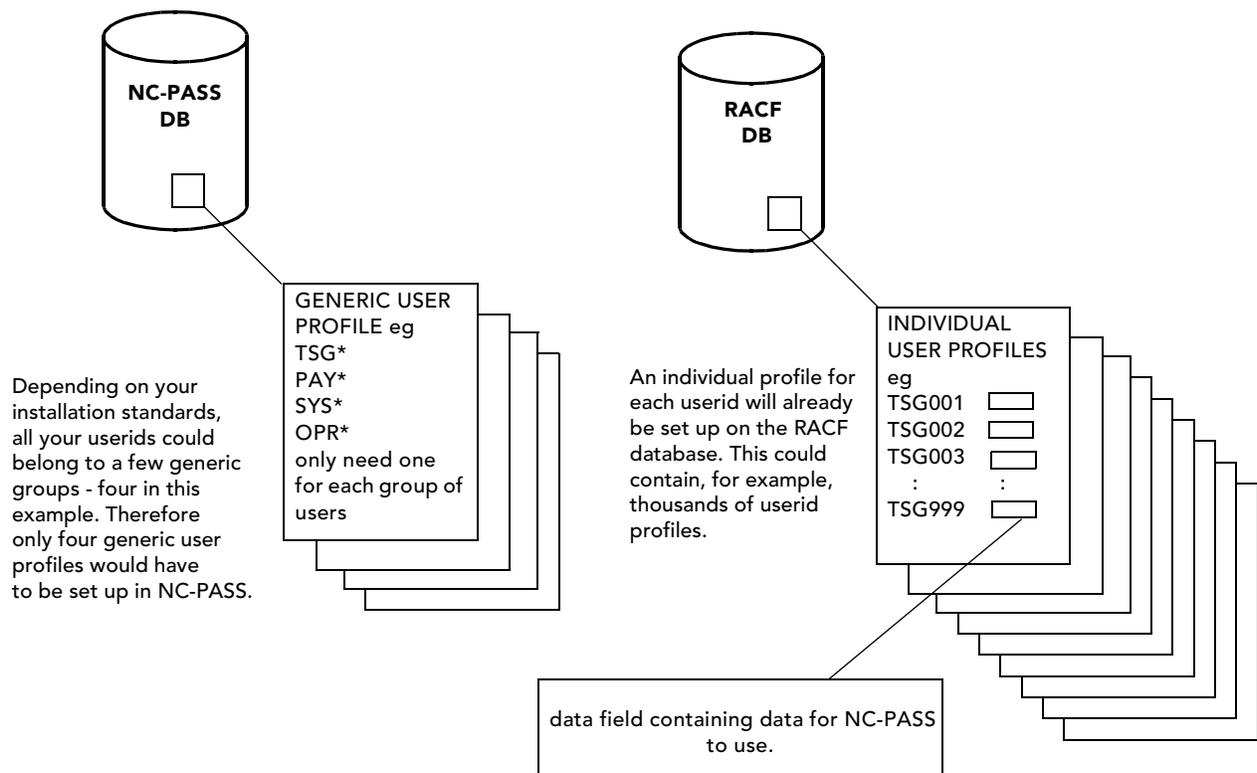
The use of this function can:

- minimize the duplication of user profile details on NC-PASS and external security databases
- reduce your workload and confine the work to a familiar environment, eg RACF

Note: This function is currently supported for RACF only.

Basic processing requires that a user logging on through NC-PASS matches with a profile (probably a generic profile).

An example of the userid data held on both databases is shown in the diagram below.



Setting up the system

To use this function, you must

- determine the data you want to store on RACF
- enter the required data on the RACF userid profile records
- make the function operational by specifying system parameters on NC-PASS.

Storing data on RACF

NC-PASS data is stored in the INSTALLATION DATA field on RACF databases.

The data takes the format of a *keyword* followed by a *value* where:

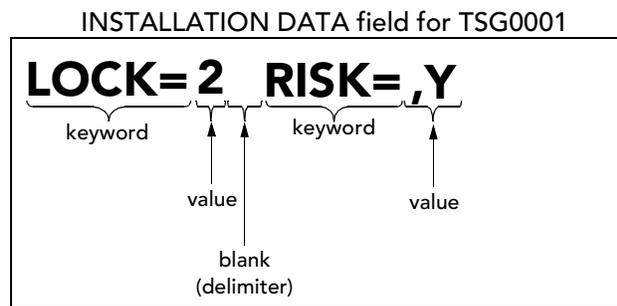
keyword is a predefined tag, set up on NC-PASS, to identify a specific user profile field name.

value is the value entered for this field name.

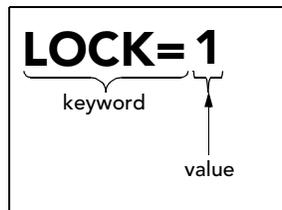
Refer to *Data fields and keywords* on page 5.6 for details of setting up keywords on NC-PASS.

Keywords and their associated values can be held in any order in the installation data field.

Each entry in the INSTALLATION DATA field must be delimited by a space. For example, if LOCK=' has been defined as the keyword to identify the lock interval field and 'RISK=' to identify the user risk field, the following examples show the contents of the INSTALLATION DATA field for RACF userid profiles TSG0001 and TSG0002:



INSTALLATION DATA field for TSG0002



When specifying an entry, the keyword must exactly match that specified on NC-PASS. For example, if a keyword of 'LOCK=' is specified in NC-PASS, LOCK=*value* must be specified on the security database. Similarly, if a keyword of 'LOCK#' is specified, LOCK#*value* must be entered on the security database.

Editing the INSTALLATION DATA field

You can store data in this field either by using the ALTUSER and ADDUSER commands or by using the standard RACF panels. Refer to the appropriate RACF documentation for further details.

RACF does not provide an edit facility for this field; the text you enter will replace any text currently held there. PassGo Technologies Ltd. therefore supply a customization to the standard RACF panel which will display the current contents of the field and allow you to edit the contents.

To use this facility, copy the sample member supplied in *PREFIX*.SOURCE called CKSRDATA into your REXX EXEC or CLIST library. If a REXX library is used, concatenate it to SYSEXEC DD. A CLIST library must be concatenated to SYSPROC DD. This facility is only available with TSO/E and REXX support.

Amended versions of panels ICHP40 and ICHP422 are supplied in library *PREFIX*.SOURCE. Either copy these into your own ISPLIB library or examine them and make the changes shown to your own RACF panels.

Examples of storing user risk profile data on RACF

Risk values stored in RACF for a specific userid

Result

Y,Y/N,N

NC-PASS will extract user risk profile values Y,Y for an access attempt during the period specified by the date/time definition in column 1 (STATEHOL).

NC-PASS will extract user risk profile values N,N for an access attempt during the period specified by the date/time definition in column 2 (WORKWEEK).

NC-PASS will use the system default values for the user risk profile for an access attempt during the periods specified by date/time definitions in columns 3 through 6 (EVENING, WEEKEND, OUTHOURS and CATCHALL).

//Y,Y///N,N

NC-PASS will extract user risk profile values Y,Y for an access attempt during the period specified by date/time definition in column 3 (EVENING).

NC-PASS will extract user risk profile values N,N for an access attempt during the period specified by date/time definition in column 6 (CATCHALL).

NC-PASS will use the system default values for the user risk profile for an access attempt during the periods specified by date/time definitions in columns 1, 2, 4 and 5 (STATEHOL, WORKWEEK, WEEKEND and OUTHOURS).

N,N/N,N/N,N/N,N/N,N/Y,Y

NC-PASS will extract user risk profile values N,N for an access attempt during the periods specified by date/time definitions in columns 1 through 5 (STATEHOL, WORKWEEK, EVENING, WEEKEND and OUTHOURS).

NC-PASS will extract user risk profile values Y,Y for an access attempt during the period specified by the date/time definition in column 6 (CATCHALL).

NC-PASS uses the user risk values in conjunction with the terminal risk values to determine the overall risk assessment; refer to *Terminal risk profile creation* on page 3.33.

Setting NC-PASS parameters

To use the external security database feature you must specify:

- an NC-PASS global system option to indicate that an external security database is to be used
- an NC-PASS option to indicate that an external security database is to be used for this user
- which data fields will be extracted from the security database and define keywords to be used by NC-PASS when searching the external security database
- an NC-PASS system option to indicate whether or not a logon attempt is to be allowed to continue if invalid data is held on the external security database.

Specifying the use of an external security database

Enter Y in the **External user profile** field on the LOGON DEFAULTS panel (1.2) if an external database is to be searched. The default is N. (Refer to the section entitled *Determining logon options* on page 2.5 for a full description of this panel.)

Enter Y in the **Use external profile** field on the PROFILE DETAIL FOR *USERID* panel (5.2) for those userids for whom external data is to be held.

Data fields and keywords

Keywords are used to identify user profile field names that have been stored on an external security database.

For example if you define the keyword 'LCK=' to identify lock interval data, the RACF INSTALLATION DATA field for a user could contain the entry LCK=*num* where 'LCK=' is the keyword defined on NC-PASS identifying the lock interval field and '*num*' is the number of minutes used to calculate a temporary lock period for a userid following an incorrect logon.

The table on the following page describes the field names that can be held externally, the default keywords associated with each field name and how NC-PASS uses the external data to build the working profile. A full description of each field is provided in the appropriate chapter.

Field name	Default keyword	Data Description	Permissible values
Connect data	CONNECT=	This data is used at logon to replace the user profile connect data. Data can be entered as variables and the resolved values passed to a VTAM application. For details of the connect data feature see <i>Specifying connection routes</i> on page 3.26.	a/b/c/d where a = CODE (K,E,N or M) b = DEST c = TERMID d = DATA For details of the values above, see <i>The CONNECT DEFINITION for USERID panel</i> on page 3.26.
Lock interval	LOCK=	This data overwrites the lock interval specified on a user profile, to determine how long the user will be locked for in the event of an invalid log on attempt.	Time interval in minutes. See <i>Basic lock interval</i> on page 3.24.
User risk	RISK=	The user risk profile allows you to specify high-risk userids with special privileges, such as access to sensitive applications and the special protection they require.	$a_1, v_1 / a_2, v_2 / a_3, v_3 / a_4, v_4 / a_5, v_5 / a_6, v_6$ where <i>a</i> is the authentication keyword and <i>v</i> is the validation keyword. Valid keywords are shown on page 5.8. There are up to six pairs of values, separated by the slash character (/) which equate to the six columns of DATE/TIME DEFINITIONS on the USER RISK PROFILE panel (see panel on page 3.35)

Keywords

Keywords are shown on the KEYWORD DEFINITIONS panel (1.5), as shown on page 5.12. NC-PASS provides default keywords; you can replace these defaults with your own keywords if required. Keywords must conform to the following standards:

minimum length	1
maximum length	8
first character	A through Z and national characters
remaining characters	as the first character plus the equal sign (=)

How NC-PASS extracts the data

Keyword definitions are stored on the NC-PASS CAF and are retained over NC-PASS restarts.

The default list of keywords is provided for the initial system startup. These are all enabled, but the initial startup default for the **External user profile** field on the LOGON DEFAULTS panel (1.2) is set to N. This prevents the new system starting immediately, without administrator action.

All the extracted data is validated in the same way as data entered on NC-PASS panels. If invalid, processing can continue depending on the contents of the **Continue Logon** field. Refer to *Data validation* on page 5.10 for further details.

If the field name to which a keyword applies is enabled, NC-PASS will scan the INSTALLATION DATA field in the RACF database for an exact match to the characters specified on the KEYWORD DEFINITIONS screen.

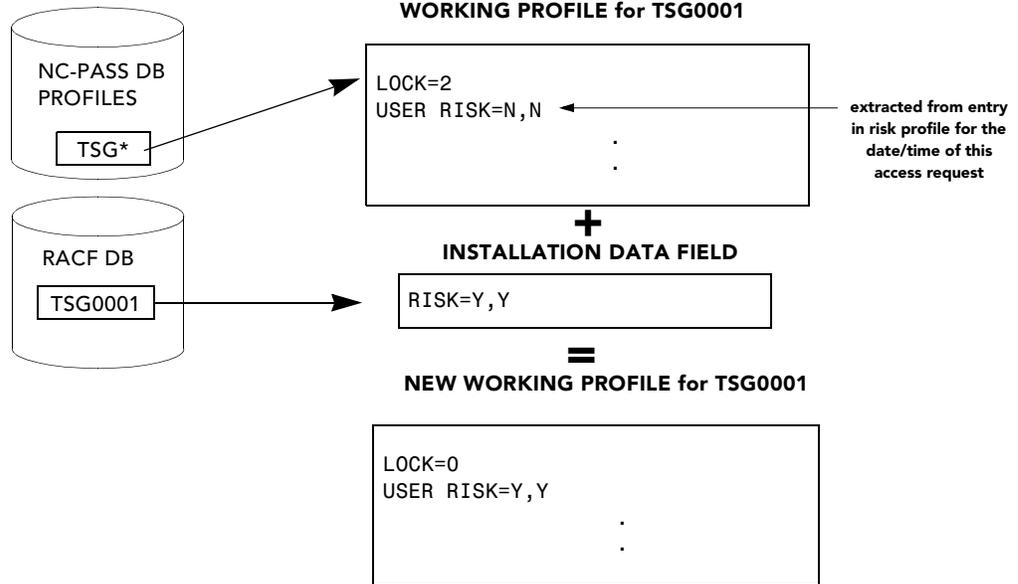
If a match is found, NC-PASS will use the value extracted from the RACF database to build the user profile.

If no match is found, NC-PASS will use the **system default value**. For example, if no match is found for the keyword for lock interval, a default value of zero would be used.

The example on the following page illustrates the extraction process.

In the example below, user TSG0001 attempts to logon. The **External user profile** field is set to Y, the **Use external profile** field is set to Y on the TSG* user profile record and the following keyword definitions have been enabled:

- Bypass flag (keyword BY=)
- User risk (keyword RISK=).



Note: In the example above, the LOCK INTERVAL field is set to 2 on the NC-PASS profile record for user TSG*. However, since the keyword for this field has been enabled but no entry has been found on RACF for user TSG0001, NC-PASS uses the default value (0) for this user.

Specifying multiple keywords for a given field

Normally a single keyword will be used to identify a given NC-PASS data field. You can however specify up to three keywords for any field. Typically this facility would be used when you want to phase in a change of keyword to conform to new naming standards. The following examples show how NC-PASS extracts data when more than one keyword has been specified for a given field.

Example

A keyword of LCK= has been defined to identify the lock interval field. This keyword is currently used in many RACF userid profiles.

Due to a change in naming standards, the administrator must now use a new keyword LOCK=. This change is to be phased in over a period of months. Two keywords are specified and enabled:

Keyword 1 - LCK=

Keyword 2 - LOCK=

	INSTALLATION DATA FIELD entries	
<i>existing user</i>	TSG0001	...LCK=1
<i>existing user</i>	TSG0002LCK=4
<i>new user</i>	TSG0099LOCK=1

NC-PASS searches for keyword 2 first. If found (eg for user TSG0099) its value is extracted and used to build the working profile and no further searching for this keyword occurs. If no match is found for keyword 2 (eg for user TSG0001), keyword 1 is then searched for. If a match is found, the value is extracted and used to build the working profile. If not, the value, if any, specified on the NC-PASS database will be used.

Data validation

When data is entered in the INSTALLATION DATA field on a RACF database, no validation is performed to ensure the data is valid for NC-PASS. Validation takes place when the data is extracted.

For example, valid NC-PASS values for the **Basic lock interval** field for a userid are numbers between 0 and 99.

Since no validation is carried out at RACF data entry, if you entered LOCK=T in the INSTALLATION DATA field, where 'LOCK=' is the keyword that identifies the **Basic lock interval** field, the value T will be stored.

If an external database is searched for user profile data, the values found will be used to build the working user profile as explained in *Determining userid validation requirements* on page 5.2.

If invalid data is found on the external database, the result of the search will depend on the setting of the **Continue logon** field.

Set the **Continue logon** field on the LOGON DEFAULTS panel (1.2) to Y to specify that if any of the data stored on the RACF database is incorrect, the logon should continue using the NC-PASS default values. The default value for the **Continue logon** field is N, which would result in the user being denied access if extracted data was invalid.

Mismatched keywords

No facility is provided to check or report whether keywords set in RACF match those on the NC-PASS database. For example, if you specify a keyword 'LOCK=' to identify the basic lock interval field, and you accidentally specify the entry 'LCK=*value*' in the INSTALLATION DATA field for a user, NC-PASS will not find a match and the basic lock interval will not be extracted.

Care should therefore be taken when setting them up.

KEYWORD DEFINITIONS panel

Fields that can be stored on an external security database and their associated keywords are displayed on the KEYWORD DEFINITIONS panel (1.5), shown below.

```
Date:12/12/1997                KEYWORD DEFINITIONS                Userid:TSG0001
Time:09:00                    Terminal:A01MS261

This panel displays a list of field names. They are made available for use with
NC-PASS by the specification of one or more keywords, and by being enabled.
Their purpose is to permit the extraction of data from an external source.

Line commands: C=Change  D=Disable  E=Enable

S  FIELD NAME                KEYWORD  ENABLED  UPDATED  TIME  BY
  Connect data              CONNECT=   N    08/08/1997 18:12 *SYSTEM*
  Lock interval             LOCK=     N    08/08/1997 18:12 *SYSTEM*
  User risk definition      RISK=     N    08/08/1997 18:12 *SYSTEM*

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

Line commands

The line commands C, D, and E can be entered in column S against the required definition to perform the following functions:

- C allows you to change the keywords for the selected definition by displaying the KEYWORD ASSIGNMENT panel.
- D disables the selected definition. The RACF database will not be searched using this keyword.
- E enables the selected definition. If the system option specifying the use of an external database is set to Y, NC-PASS will use the keywords assigned to this field to search the RACF database to extract userid profile data.

Display fields

Field	Description
FIELD NAME	The names of the fields that can be stored on an external security database.
KEYWORD	The keyword assigned to the field name. *MANY* indicates that more than one keyword has been assigned to the field name.
ENABLED	The status of the field name, Y indicates that it is enabled, N that it is disabled.
UPDATED	The date on which the definition was last altered.
TIME	The time at which the definition was last altered.
BY	The user that last altered the definition.

Function keys

Key	Function
F1	Displays help information.
F3	Executes any line commands and returns to the previous panel.
F7	Displays the previous screen of field names and keywords.
F8	Displays the next screen of field names and keywords.

Assigning keywords

Use line command C against the appropriate field name to provide the KEYWORD ASSIGNMENT panel, an example of which is shown below. This panel allows the administrator to maintain a list of up to three keywords relating to a given field name. For example, the use of multiple keywords enables any changes of keyword to be phased in over a period of time, instead of running a batch conversion program.

```
Date:12/12/1997                KEYWORD ASSIGNMENT                Userid:TSG0001
Time:09:00                    Terminal:A01MS268

This panel permits maintenance of a list of up to three keywords.
When NC-PASS uses the keywords entered below, the search for a match will be
performed from first to third keyword. The latest match will be used.

Field name => Lock interval

Type the required keywords below and press <ENTER>:

Keyword 1 => LOCK= _____
Keyword 2 => _____
Keyword 3 => _____

These keywords apply to the basic lock interval which may apply to a user
profile.

F1=Help  F3=End  F12=Can
```

Input Fields

Field	Description
Keyword <i>n</i>	The keywords associated with the displayed field name. If more than one keyword is specified, NC-PASS will use the highest numbered keyword to extract the appropriate value from the external security database. If no match is found, NC-PASS will try to find a match with the next keyword down.

Display Field

Field	Description
Field name	The field name selected from the previous KEYWORD DEFINITIONS panel.

Function keys

Key	Function
F1	Displays help information.
F3	Saves any changes and returns to the previous panel.
F12	Cancels any changes and returns to the previous panel.

Chapter 6 - Restricting access by date and time

Introduction	6.2
Purpose	6.2
Date/time definitions in risk profiles	6.2
Date/time definitions in VSSE control tables	6.2
Creating date and time definitions	6.3
Specifying definition names	6.4
Specifying date and time periods	6.5

Introduction

You may want to increase system security by restricting access to particular users or terminals at specified times.

NC-PASS provides the facility to restrict access by date, time and day of the week.

You can specify the following restrictions for users, terminals, transactions and applications:

- allow access on specific days of the week eg Monday through Friday only
- allow access only at specific times. Using this facility will enable you to, for example, restrict a part-time member of staff's userid to allow them access only during their normal hours of work, eg 08:00 through 13:00. As the id cannot be used to access the system outside these hours, it no longer represents a potential threat to security
- allow access only between certain dates eg January 3rd through February 4th. This could be used, for example, to ensure that a userid set up for a temporary member of staff is not available before or after their period of work or to cater for company vacations.

Purpose

The purpose of date/time definitions is to specify periods of time that have some significance for your company.

For example, your company's normal 'office hours' may be Monday through Friday from 09:00 through 17:00 and Saturday from 09:30 through 13:00. You can specify a date time definition, called for example OFCHOURS, to include these times and exclude all others.

You may also have operations staff who work shifts. You can define the times of each shift in date/time definitions, eg SHIFT1, SHIFT2 and SHIFT3.

These definitions can then be used to define whether access is allowed at a given time and if so, what password requirements are in force at that time.

Date/time definitions can be used in Risk profiles and in VSSE control tables.

Date/time definitions in risk profiles

Date/time definitions are used to specify the password requirements at specific times of the day for users and terminals specified in risk profiles. For example, specific users may be allowed to logon in normal working hours without a password, but must be password protected at other times. Refer to *Risk profiles overview* on page 3.5 for details of creating and using risk profiles.

Date/time definitions in VSSE control tables

Refer to *Preventing access to an application at specific times* on page 8.34 for an example of the use of date/time definitions for control tables.

Creating date and time definitions

Date and time periods are specified in definitions created using the DATE AND TIME DEFINITIONS panel (5.7). A definition contains the access period which will be checked by NC-PASS. Use the C line command to make changes to existing definitions (including those you have just defined).

The definition names created in this panel can be used to specify the required date/time restrictions for:

- userids (refer to *User profiles overview* on page 3.4)
- terminals (refer to *Risk profiles overview* on page 3.5)
- VSSE control tables. (Refer to *Preventing access to an application at specific times* on page 8.34.)

The following sample definitions are provided:

WORKWEEK
EVENING
WEEKEND
STATEHOL
OUTHOURS
ALWAYS

Depending on your site requirements, you can:

- use the sample definitions provided
- amend the samples as required
- create your own definitions with names of your choice
- use the sample definitions as a model for your own definitions.

Specifying definition names

```

Date:12/12/1997          DATE AND TIME DEFINITIONS          Userid:TSG0001
Time:09:00              Terminal:A01MS244

Line commands: C=Change D=Delete

S  DEFINITION  COMMENTS          UPDATED   TIME  BY
-  EMERGENC   Emergency support hours  05/11/1997 13:55 SYS0023
-  NORMAL     Office hours           06/11/1997 11:33 TSG0001
-  OUTSIDE    Out of office hours    06/11/1997 11:35 TSG0001
-  PAYROLL    Payroll run            06/12/1997 17:11 TSG0001

To create a new definition complete the fields below and press <ENTER>:
Definition name =>_____ Model definition => _____

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

```

Input fields

Field	Description
Definition name	Enter the name of the new definition to be added.
Model definition	This is an optional field in which you can enter the name of an existing definition on which to model your new definition. The new definition will contain the same data as the model.

Line commands

The line commands C and D can be entered in column S against the required definition to perform the following functions:

- C allows you to change the selected definition by displaying the DATE AND TIME DEFINITIONS FOR *DEFINITION* panel.
- D deletes the selected definition.

Display fields

Field	Description
DEFINITION	The definition name.
COMMENTS	Optional explanatory comments.
UPDATED	The date on which the definition was last updated.
TIME	The time at which the definition was last updated.
BY	The user that last updated the definition.

Function keys

Key	Function
F1	Provides help information.
F3	Saves any changes and returns to the previous screen.
F7	Displays the previous list of definitions.
F8	Displays the next screen of definitions.

Specifying date and time periods

Enter line command C against the required definition on the DATE AND TIME DEFINITIONS panel to provide the DATE AND TIME DEFINITION *DEFINITION* panel, an example of which is shown below.

```
Date:12/12/1997      DATE AND TIME DEFINITION OUTHOURS      Userid:TSG0001
Time:09:00          Terminal:A01MS244

Definition comment => Out of office hours

Line commands: A=After B=Before D=Delete M=Move N=New

S DAYS          DATE          TIME
M T W T F S S  START          END          START  END
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-  Y Y Y Y Y N N          18:31  24:00
-  Y Y Y Y Y N N          00:01  08:29

F1=Help F3=End F7=Up F8=Down F12=Can
```

Entries are processed top down, ie the first matching day, date and time will be used. New entries are added in alphabetical order. Use the A, B and M line commands to change the order, if required.

This example panel specifies that if the OUTHOURS definition is specified in a user or terminal risk profile, a match will be found if the user attempts access

- Monday through Friday from 18:31 through midnight
- Monday through Friday from midnight through 08:29.

No match will be found at any time on a Saturday or Sunday.

Input fields

Field	Display
Definition comment	Enter an explanatory comment, if required.
DAYS M T W T F S S	Represents the days of the week Monday through Sunday. Enter Y to include this day in the specified definition. Enter N to exclude it from the definition.
DATE START	Enter the start date of the required time period. If there is no date restriction, leave blank. If specified, the start date must be before the end date. Use the standard date format for your system, ie the same as the current date displayed on the panel.
DATE END	Enter the last date of the required time period. If there is no date restriction, leave blank. If specified, the end date must be after the start date. Use the standard date format for your system, ie the same as the current date displayed on the panel.
TIME START	Enter the start time of the required time period. If omitted a default time of 00:00 will be used. If specified, the start time must be before the end time. (HH:MM format)
TIME END	Enter the end time of the required time period. If omitted a default time of 24:00 will be used. If specified, the end time must be after the start time. (HH:MM format)

Line commands

The line commands A, B, D, M and N can be entered in column S against the required definition to perform the following function:

A/B	to move a definition to a different position in the list, insert an M command against the field to be moved. Tab to the target position and enter either an A to move the selected field to the position AFTER this field or a B to move the selected field to the position BEFORE this field.
D	deletes the selected definition.
M	identifies a definition which is to be moved to another position in the list. Use in conjunction with the A and B line commands.
N	adds a new entry using the input fields described above. The entry will be added to the top of the list.

Function keys

Key	Function
F1	Provides help information.
F3	Saves any changes and returns to the previous screen.
F7	Displays the previous list of definitions.
F8	Displays the next screen of definitions.
F12	Cancels any changes and returns to previous screen.

Chapter 7 - The VTAM Session Security Exit (VSSE)

Introduction to VTAM sessions	7.2
Logical units	7.2
Example sessions	7.3
Overview	7.5
Control table definition	7.5
SME data definitions	7.9
Actions	7.15
Example control table	7.17
Creating a new control table - example	7.19
Creating the group definitions	7.20
Creating the master rule	7.24
Creating lower level rules	7.30
Viewing the control table outline	7.31
Control table build	7.32
The VSSE OPTIONS menu	7.32
Rule maintenance	7.32
Changing/creating a rule	7.35
Changing an array	7.37
Changing the order of fields in an array	7.40
Changing a column within an array	7.41
Adding a column to an array	7.44
Printing a rule	7.48
Viewing a control table outline	7.49
Grouping data	7.51
Defining a group	7.52
Defining group values	7.53
Control table test before loading	7.55
Using the test function	7.55
Test function panels	7.61
Test results	7.64
The LOAD/RESTORE CONTROL TABLES panel	7.65
Displaying the LOAD/RESTORE CONTROL TABLES panel	7.65
System startup	7.69
Building a reference table of other NC-PASS systems	7.69
Displaying information about SME Control Tables	7.70
Setting global options	7.73
Implications of global options settings	7.75
Setting control operator functions	7.76
Stopped sessions recovery	7.77
SME flag settings	7.77
Reactivating a backed-out table	7.77
Communications	7.78
Communication from NC-PASS to the SME	7.79
Communication from the SME to NC-PASS	7.79
Userid processing	7.80
Specifying the USERID field in rules	7.81
Converting an NC-PASS 1.4 authorization control table to V2.0	7.83
Statement conversion	7.83
Conversion example	7.85
Conversion report	7.86
The AUTHORIZATION CONTROL TABLE CONVERSION panel	7.87
Communication between different versions of NC-PASS	7.88
Exchanging control table data	7.88

Introduction to VTAM sessions

There are a number of ways in which a session can be requested, examples of which are shown below:

- VTAM initiates eg LOGAPPL
- a terminal initiates eg LOGON *applid* from USSTAB
- an application initiates eg a session manager issues a REQSESS instruction
- a third party LU initiates eg CLSDST PASS.

Logical units

NC-PASS refers to five categories of logical unit:

- **Primary Logical Unit** (PLU)
- **Secondary Logical Unit** (SLU)
- **Originating Logical Unit** (OLU)
- **Destination Logical Unit** (DLU)
- **Initiating Logical Unit** (ILU).

PLU and SLU

Typically, the PLU is the application and the SLU is the terminal, however there are situations where this is not the case. For example, the REQSESS macro instruction is used to initiate a session in which the application program (eg a session manager) will act as the SLU.

OLU and DLU

In any session request, VTAM sets flag field PUSEIND to a specific value depending on whether the PLU is the target resource or not. (The target resource is the LU with which VTAM is being requested to start a session. For example if a terminal requests a session with an application, the application is the target resource.)

Similarly SUSEIND is set to a specific value depending on whether the SLU is the target resource or not. Using this information, VSSE determines the 'from' and 'to' ends of a session partnership and builds IMAGINARY fields called OLU and DLU respectively.

OLU type fields will always contain data about the 'from' end of a session partnership and DLU type fields will always contain data about the 'to' end of the partnership.

NC-PASS audit messages make use of these imaginary fields. Refer to *SME action auditing* on page 9.16.

ILU

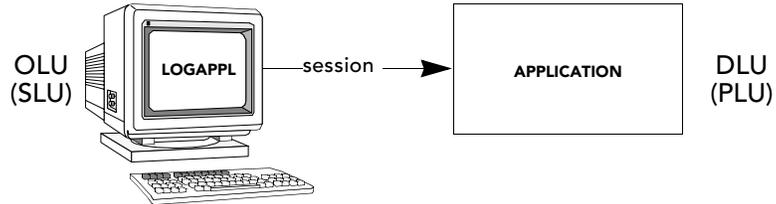
The ILU fields are present only when a third party LU initiated the session, ie a CLSDST PASS. The ILU is the application that requested the session.

Note: ILU fields are only available at VTAM 3.4.1 and above.

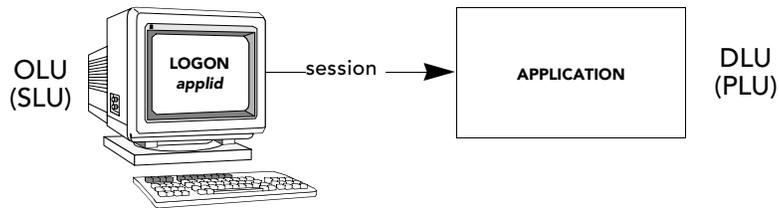
Example sessions

The examples below show the resource to which the five categories of LU apply, in different session initiation requests.

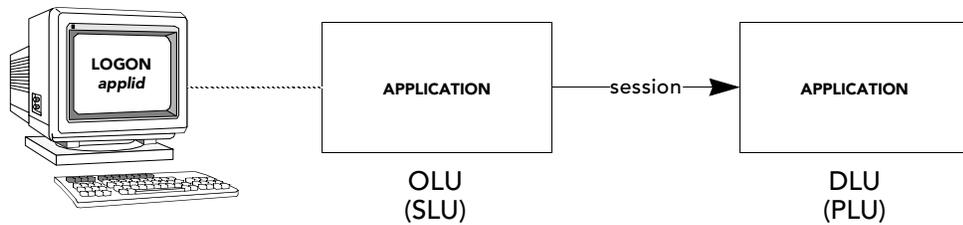
VTAM initiates session



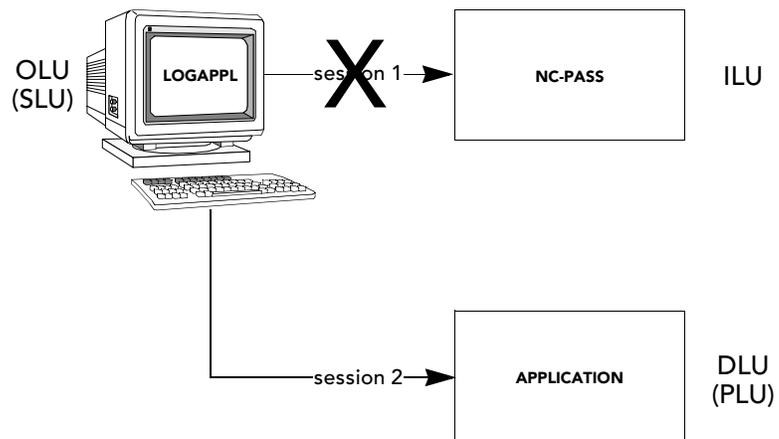
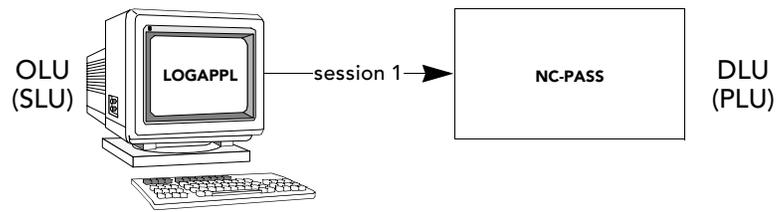
Terminal initiates session



Application initiates session



Third party LU initiation



Overview

Note: This chapter introduces the VTAM Session Security Exit (VSSE). It explains the structure of a rule and the panels used to build, test and load the rule. Refer to *Chapter 8 - Using VSSE to achieve access control objectives* for examples of using VSSE rules.

When VTAM receives a session initiation request, it passes data relating to that request to the Session Management Exit (SME). VSSE checks this input data against a control table which is defined to the system by an administrator using on-line panels in NC-PASS. The table is used to check one or all of the data elements passed to the SME by VTAM, for specific values.

A control table is constructed from authorization arrays within rules.

At the lowest level, elements of a control table equate to expressions, for example:

Terminal id starts with 'TLP'

Network id equals 'NTA'

These expressions resolve to a TRUE or FALSE condition. A specific action is defined to be executed for each condition. Refer to the subsection entitled *Actions* on page 7.15, for details of the different types of actions available.

The VTAM administrator can define any number of control tables in NC-PASS, one of which is loaded into CSA, from where the SME can access it. This table is known as the Active Control Table (ACT).

Control table definition

Control table processing is based on a hierarchical structure. Each control table comprises one or more rules. Each rule consists of one or more authorization arrays.

Authorization arrays

Each authorization array is made up of a set of field names, each with a corresponding set of values. All data passed to the SME by VTAM can be referenced by one of these field names. For example, typically the terminal id is referenced by field SLNETLU and the application by field PLNETLU.

Field names and values are arranged in columns in an array. The heading for each column is a field name. Immediately under the heading is the operator to be used when comparing input values. This can either be EQ (equals) or NE (not equal to). The values listed under the column heading are the values that will be compared with the field name value contained in the SME VTAM data. Each of the values is checked in turn. An example is shown below.

PLNETLU	SLNETLU
EQ	NE
A01PAYRL	TERM001
	TERM002

If the operator is EQ, the processing logic is:

IF *field name* equal to xxxx **or** equal to yyyy or equal to....
THEN condition is TRUE
ELSE condition is FALSE.

If the operator is NE, the processing logic is:

IF *field name* not equal to xxxx **and** not equal to yyyy and not equal to....
THEN condition is TRUE
ELSE condition is FALSE.

When processing has completed for any column and the resulting condition is true, either the next column in the array is checked or, if this is the last column in the array, the TRUE action for that array is processed.

When processing has completed for any column and the resulting condition is false, the FALSE action for that array is processed.

Example

The following example shows a simple rule with one array to protect application A01PAYR by allowing sessions only from terminals TERM001 and TERM002. No other application is protected:

PLNETLU	SLNETLU
EQ	NE
A01PAYRL	TERM001
	TERM002

TRUE: DENY FALSE: ALLOW

Session 1: User on terminal TERM001 requests a session with application A01PAYRL.

PLNETLU	SLNETLU
EQ	NE
A01PAYRL	TERM001
	TERM002

TRUE: DENY FALSE: ALLOW

```
graph LR; A["PLNETLU  
EQ  
A01PAYRL"] -- True --> B["SLNETLU  
NE  
TERM001  
TERM002"]; B -- False --> C["FALSE: ALLOW"]; A -- True --> D["TRUE: DENY"];
```

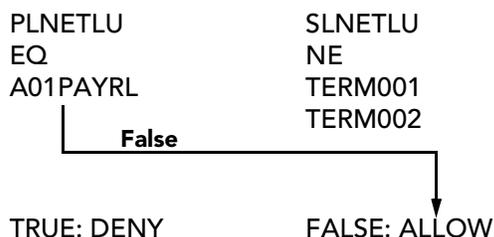
Session 2: User on terminal TERM003 requests a session with application A01PAYRL.

PLNETLU	SLNETLU
EQ	NE
A01PAYRL	TERM001
	TERM002

TRUE: DENY FALSE: ALLOW

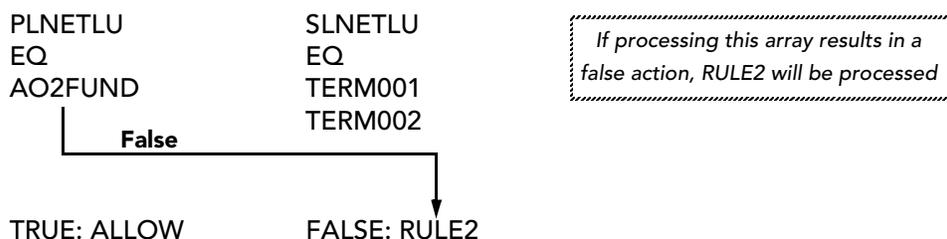
```
graph LR; A["PLNETLU  
EQ  
A01PAYRL"] -- True --> B["SLNETLU  
NE  
TERM001  
TERM002"]; B -- True --> C["TRUE: DENY"]; A -- True --> D["FALSE: ALLOW"];
```

Session 3: User on terminal TERM003 requests a session with application A01TSO.



Control table structure

One of the actions that can be associated with an authorization array is to execute another rule.



A control table is defined by the first rule in the structure, known as the master rule.

Any rule can be the master rule. When the administrator issues the command to load a control table, he gives the name of the rule which he wants to be at the top of the structure for this control table. This can be the name of any rule defined to the system as described in the example below.

Example

The administrator has defined four rules to the system.

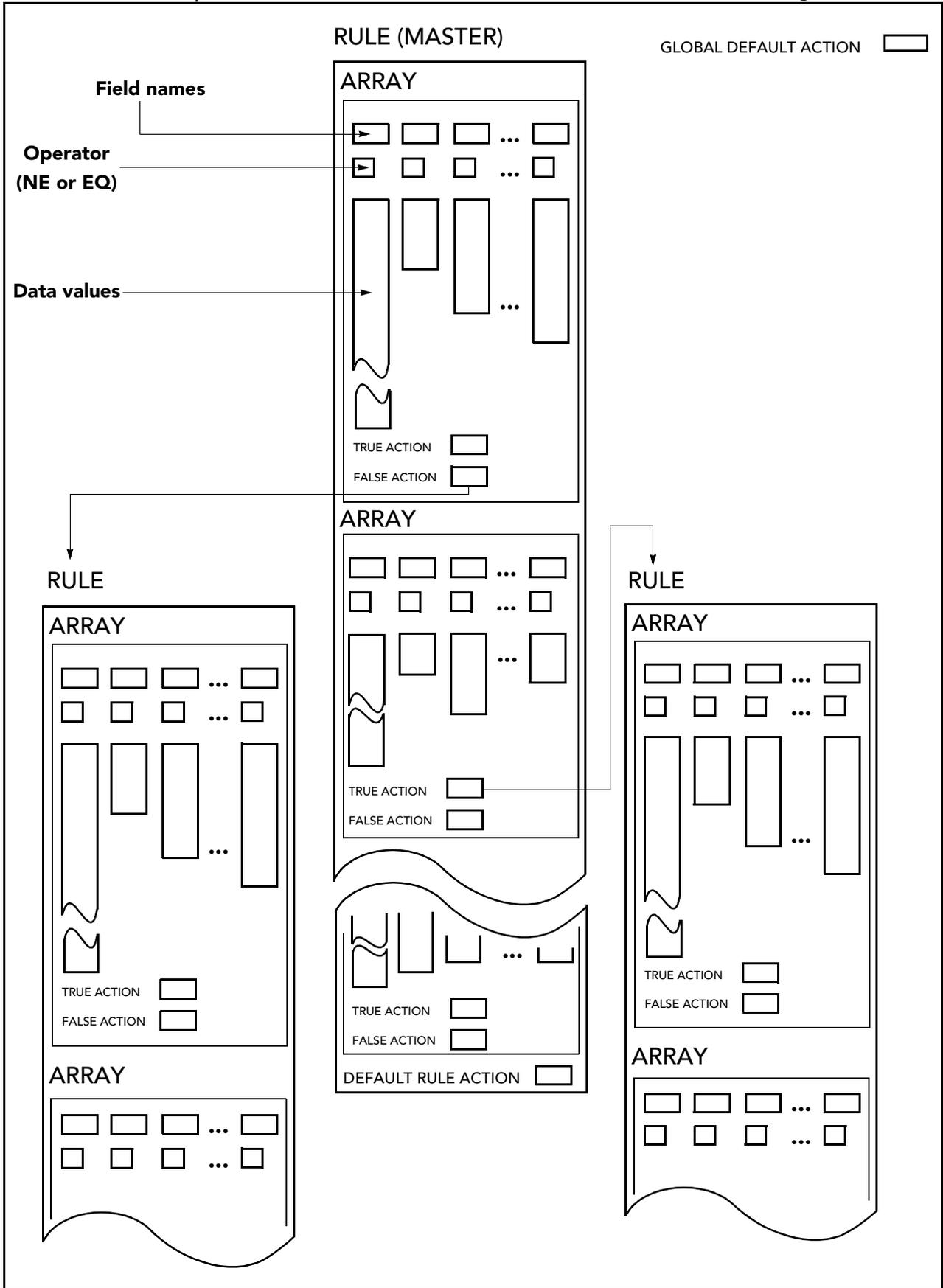
- RULEA (has an authorization array with an action that calls RULEB)
- RULEB (has an authorization array with an action that calls RULEC)
- RULEC
- RULED.

If the administrator specifies a control table name of...	the structure of the control table is...	
RULEA	Master rule	RULEA
	Lower level rules	RULEB and RULEC
RULEB	Master rule	RULEB
	Lower level rules	RULEC
RULEC	Master rule	RULEC
	Lower level rules	none
RULED	Master rule	RULED
	Lower level rules	none

A control table is therefore a logical structure or view.

A default action for a rule can be specified. This will be executed when the rule has been processed without any of the array-defined actions resulting in a termination of either the rule or control table processing. If the master rule has no default action, the global default action is used.

A representation of the structure of a control table is shown in the diagram below:



SME data definitions

Whenever a session request is initiated, all the details relating to that session request (such as terminal id, application id, type of session etc) are passed to the SME by VTAM.

The data passed to the SME by VTAM will be referenced in the authorization arrays via field names. For example, typically the terminal name will be referenced via field name SLNETLU.

Field name types

The data referenced via the field name can be one of the following types:

Type	Meaning															
Fixed	This data has a fixed position in the data provided by VTAM. This data will always be present in the input data string, regardless of the type of session request. An example of a data field that will always be present is SLNETLU, the SLU device name.															
Variable	<p>These are fields which may or may not be present depending on how the logical unit has been defined to VTAM.</p> <p>For example, the PLU's cross-domain resource manager major node (PHCVR06), its cross-domain resource major node (PHCVR07), cross-domain resource manager (PHCVR10) and cross-domain resource (PHCVR24) will only be set if the PLU has been set up as a cross-domain resource. The PLU's LAN major node (PHCVR28) is only relevant if the LU is defined to VTAM as a local area network resource.</p>															
Imaginary	<p>OLU and DLU fields have been set up to indicate the 'from' and 'to' ends of a session partnership.</p> <p>Fields containing data relating to the 'from' end (the LU from which the request is sent) are prefixed OL (eg OLNETLU); fields containing data relating to the 'to' end (the LU with which a session is requested) are prefixed DL (eg DLNETLU).</p> <p>These fields are known as imaginary fields because NC-PASS creates these fields from data contained in other fields passed to the SME.</p>															
Flag	<p>A flag field is a one byte field. The data definition allows specific bit patterns to be given symbolic names which can be used in authorization arrays.</p> <p>For example the following bit settings for flag field EXRRS11 (Related session information byte 1) indicate the session initiator:</p> <table border="1"> <thead> <tr> <th>Bit settings</th> <th>Symbolic name</th> <th>Session initiator</th> </tr> </thead> <tbody> <tr> <td>--00 ----</td> <td>EX1AUTO</td> <td>Autologon session (VARY LOGON, LOGAPPL)</td> </tr> <tr> <td>--01 ----</td> <td>EX1PLU</td> <td>PLU requested the session (SIMLOGON, OPNDST ACQUIRE)</td> </tr> <tr> <td>--10 ----</td> <td>EX1SLU</td> <td>SLU requested the session (USS logon, INIT SELF)</td> </tr> <tr> <td>--11 ----</td> <td>EX1OLU</td> <td>Some other LU requested the session: third party initiated (CLSDST PASS)</td> </tr> </tbody> </table>	Bit settings	Symbolic name	Session initiator	--00 ----	EX1AUTO	Autologon session (VARY LOGON, LOGAPPL)	--01 ----	EX1PLU	PLU requested the session (SIMLOGON, OPNDST ACQUIRE)	--10 ----	EX1SLU	SLU requested the session (USS logon, INIT SELF)	--11 ----	EX1OLU	Some other LU requested the session: third party initiated (CLSDST PASS)
Bit settings	Symbolic name	Session initiator														
--00 ----	EX1AUTO	Autologon session (VARY LOGON, LOGAPPL)														
--01 ----	EX1PLU	PLU requested the session (SIMLOGON, OPNDST ACQUIRE)														
--10 ----	EX1SLU	SLU requested the session (USS logon, INIT SELF)														
--11 ----	EX1OLU	Some other LU requested the session: third party initiated (CLSDST PASS)														
Date/time	This type of field contains a date/time definition as created using the DATE and TIME DEFINITIONS panel (5.7). Refer to <i>Chapter 6 - Restricting access by date and time</i> .															

Field descriptions

Details of all network defined field names and flags are provided in the IBM publication entitled VTAM Customization. A full list of all network defined field names and flags is provided on-line.

The following list describes some of the most commonly used fields.

Some fields can also be referenced by one or more alias names. Where applicable, the alias names are shown in brackets under the main field name.

LU related fields

Field name	Description
ILNETLU (LU3) (MENU)	<p>This field is present only if the session request is a CLSDST PASS. It refers to the Initiating Logical Unit (ILU) ie a third party LU requesting a session between two other unconnected LUs.</p> <p>Note: This field is not available at VTAM 3.3 and below.</p>
DLNETLU (LU2)	<p>This field contains the name of the Destination Logical Unit (DLU), ie the name of the LU at the 'to' end of a session partnership.</p> <p>For example, if a terminal requests a session with an application, this field will contain the VTAM nodename of the requested application. In this example, the value in this field is identical to the value held in field PLNETLU.</p>
OLNETLU (LU1)	<p>This field contains the name of the Originating Logical Unit (OLU), ie the name of the LU at the 'from' end of a session partnership.</p> <p>For example, if a terminal requests a session with an application, this field will contain the terminal id. In this example, the value in this field is identical to the value held in field SLNETLU.</p>
PLNETLU (APPL)	<p>This field contains the name of the Primary Logical Unit (PLU) as defined within the network.</p> <p>For example, if a terminal requests a session with an application, this field will contain the VTAM nodename of the requested application.</p>
SLNETLU (TERMINAL)	<p>This field contains the name of the Secondary Logical Unit (SLU) as defined within the network.</p> <p>For example, if a terminal requests a session with an application, this field will contain the terminal id.</p>

VTAM (SSCP) related data fields

Field name	Description
DLUSSCP (LU2VTAM)	This field contains the VTAM id (SSCPNAME) of the VTAM that contains the Destination Logical Unit (DLU), ie the VTAM id that contains the LU at the 'to' end of a session partnership.
EVSSCP (THISVTAM)	This refers to the host VTAM id where the SME is operating. It is a unique name to the network and is the name that is present in SYS1.VTAMLST(ATCSTRxx) against the parameter SSCPNAME.
ILUSSCP (LU3VTAM) (MENUVTAM)	<p>This field is present only if the session request is a CLSDST PASS. It refers to the Initiating Logical Unit (ILU), ie a third party LU requesting a session between two other unconnected LUs.</p> <p>This field contains the VTAM id (SSCPNAME) that contains the ILU.</p> <p>Note: This field is not available at VTAM 3.3 and below.</p>
OLUSSCP (LU1VTAM)	This field contains the VTAM id (SSCPNAME) of the VTAM that contains the Originating Logical Unit (OLU), ie the VTAM id that contains the LU at the 'from' end of a session partnership.
PLUSSCP (APPLVTAM)	This field contains the VTAM id (SSCPNAME) of the VTAM that contains the Primary Logical Unit (PLU) as defined within the network.
SLUSSCP (TERMVTAM)	This field contains the VTAM id (SSCPNAME) of the VTAM that contains the Secondary Logical Unit (SLU) as defined within the network.

Network related data fields

Field name	Description
DLNETID (LU2NET)	This field contains the network id of the network containing the Destination Logical Unit (DLU), ie the network that contains the LU at the 'to' end of a session partnership.
EVNAMAD	This field is set only when the session request is to a Logical Unit (LU) in another network. It refers to the next network id in the direction of the Destination Logical Unit (DLU) that will process the session request.
EVNAMA0	This field is set only when the session request is from a Logical Unit (LU) in another network. It refers to the previous network id in the direction of the Originating Logical Unit (OLU) that processed the session request.
EVNETID (THISNET)	This refers to the local network name where the SME is operating. It is a unique name and is the same name that is present in SYS1.VTAMLST(ATCSTRxx) against the parameter NETID.
ILNETID (LU3NET) (MENUNET)	<p>This field is present only if the session request is a CLSDST PASS. It refers to the Initiating Logical Unit (ILU), ie a third party LU requesting a session between two other unconnected LUs.</p> <p>This field contains the network id (NETID) of the LU that requested the session, ie the ILU.</p>
OLNETID (LU1NET)	This field contains the network id of the network containing the Originating Logical Unit (OLU), ie the network that contains the LU at the 'from' end of a session partnership.
PLNETID (APPLNET)	This field contains the network id of the network containing the Primary Logical Unit (PLU).
SLNETID (TERMNET)	This field contains the network id of the network from where the Secondary Logical Unit (SLU) session was generated.

Session request related data fields

Flag field	Description
EXRRSI1	Related Session Information - byte 1

Symbolic name	Description
EX1AUTO	The session request was automatically generated. (VARY/LOGON/LOGAPPL). This includes sessions that are initiated at machine power up, operator driven requests and terminals that are LOGAPPLed to applications.
EX1OLU	This indicates that a third party LU specifically requested a session between a terminal and another application, eg a CLSDST PASS.
EX1PLU	PLU requested the session (SIMLOGON, OPNDST ACQUIRE).
EX1SLU	This indicates that the SLU requested the session (USS logon, INIT SELF).

NC-PASS fields

Field	Description
TIMES	This field can be used to specify a date/time definition to restrict access to a resource based on date or time. Refer to <i>Preventing access to an application at specific times</i> on page 8.34.
USERID	This field can be used to check that only authorized users gain access to a resource. Refer to <i>Userid processing</i> on page 7.80 and <i>Protecting sensitive applications</i> on page 8.3.

Field name values

The following table shows the types of values that can be associated with a field name.

Value	Description	Example
Literals	The actual value contained in a field name, for instance, a terminal id. You can also define a literal as a generic using the mask characters asterisk (*) and plus (+). The asterisk (*) is a multiple character mask, the plus sign (+) a single character mask. Only one asterisk (*) is allowed, at the end of the literal. Plus signs (+) can be placed anywhere in the literal.	T01L424
Group names	Lists of related data. For example, the administrator can define a group containing a number of network ids. The administrator can type in the group name when referring to these network ids rather than each individual network ID in turn. Groups are defined using the SME GROUP DEFINITIONS (7.2) panel.	TSGRP
Symbolic names	These names relate to bit patterns contained in the data passed to SME by VTAM. They are predefined by PassGo Technologies Ltd. Refer to <i>Appendix A - VSSE field names and flags</i> for a list of symbolic names.	EX1SLU
Field names	Can be defined as a reference to a value against which a test will be performed. For example, this would allow a comparison to be made between the network id for the SLU and that of the PLU.	PLNETID
Date/time	These names refer to date and time definitions and allow access to be restricted to specific periods of time. Refer to <i>Chapter 6 - Restricting access by date and time</i> .	

Note: A flag field is a one byte field. A symbolic name has specific bits set within one byte. It therefore follows that a flag field can only be associated with symbolic data values (either a single value or a group of values). During array processing the bits set in the symbolic names are compared with the input flag byte.

NULL

Not all fields may be present every time the data is passed to the SME. The symbolic value NULL can be entered to cater for this situation. When an array is processed that includes this data value with the operator EQ, the result will be TRUE if no data for this field type is passed to the SME as shown in the example below:

Field name	PHCVR02 (APPL major node)
Comparator	EQ
Values	TSO NULL

Field PHCVR02 may or may not be present in the data passed to the SME. If the field is not present in the input string for a given session initiation request, the result will be TRUE in the above example. If it is present, only the value TSO will result in the true action ALLOW.

Field name	PHCVR02 (APPL major node)
Comparator	NE
Values	NULL

In the above example, the result would be TRUE if any data for field PHCVR02 (regardless of value) is passed to the SME.

Actions

Processing of an authorization array will result in either a TRUE or a FALSE condition; you can define actions for both of these conditions. Blank entries are allowed; actions must be explicitly defined using the SME ARRAY EDIT panel.

You can also specify a default action for a rule on the RULE EDIT panel. This will be executed when the rule has been processed and none of the array defined actions has resulted in a termination of either rule or control table processing.

The following table shows the actions available:

Entering the action	means...	and control table processing will...
ACQUIRE	the session request is denied and the terminal is acquired by NC-PASS which displays the NC-PASS logo, requesting further information from the user before access to a sensitive application is allowed. Refer to <i>Chapter 8 - Using VSSE to achieve access control objectives</i> .	stop
ALLOW	the session will be allowed unconditionally	stop
DENY (when the global option STOP is set to Y)	the session will not be allowed (and DENY audit messages will be produced). See also <i>Stopping a session</i> on page 7.16.	stop
DENY (when the global option STOP is set to N)	the session will be allowed (and DENY audit messages will be produced).	stop
EXIT (in lower level rules)	processing will exit the current rule and return to the next array in the rule which called the current rule.	continue
EXIT (in the master rule)	the default action for that rule will be executed.	stop
NEXT (for an array)	the next array in the rule will be processed. (if all arrays have been processed the default action for the rule will be processed)	continue
rulename	the rule <i>rulename</i> will be processed.	continue
WARN	the session will be allowed, but a warning message will be issued (and WARN audit messages will be produced).	stop

The overall control table default action will be executed if the master rule has been processed and has resulted in the execution of the default master rule action where there is either:

- no default action
- a default action of EXIT.

Note: The maximum number of levels of rules is 16. The maximum size of a control table is 32 KB.

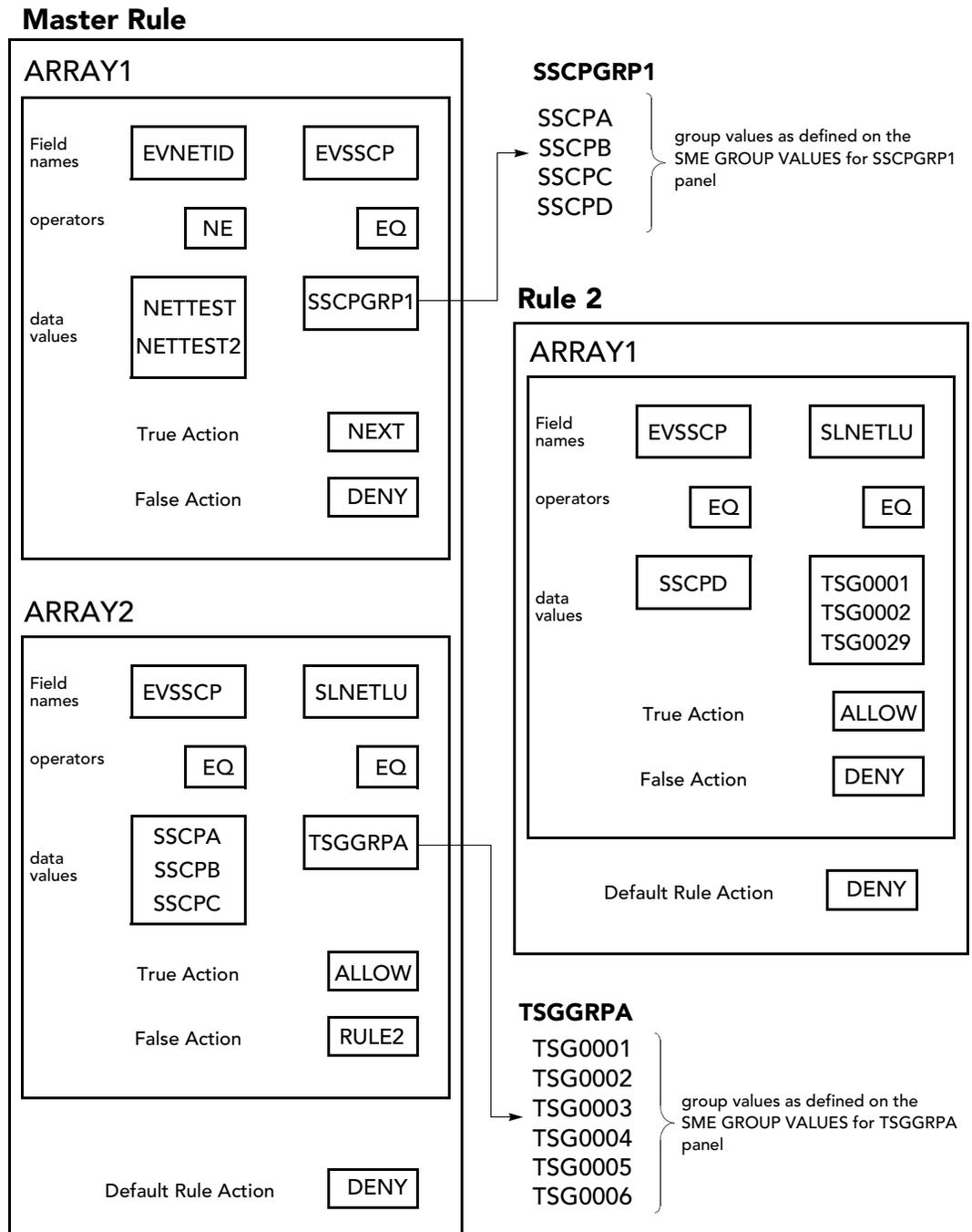
Stopping a session

To deny access to a session, the following conditions must be met:

- ITEXCAA must be installed and enabled (see *the Installation Manual, Chapter 3 - The VTAM environment*)
- the STOP option on the GLOBAL OPTIONS panel (7.5) must be set to Y. Refer to *Setting global options* on page 7.73
- the ENABLE option on the GLOBAL OPTIONS panel (7.5) must be set to Y. Refer to *Setting global options* on page 7.73
- a control table must be loaded as the Active Control Table (ACT). Refer to the section entitled *The LOAD/RESTORE CONTROL TABLES panel* on page 7.65
- a rule/array within the ACT has to be processed with a resulting DENY action.

Example control table

Example data from a control table is shown in the diagram below.

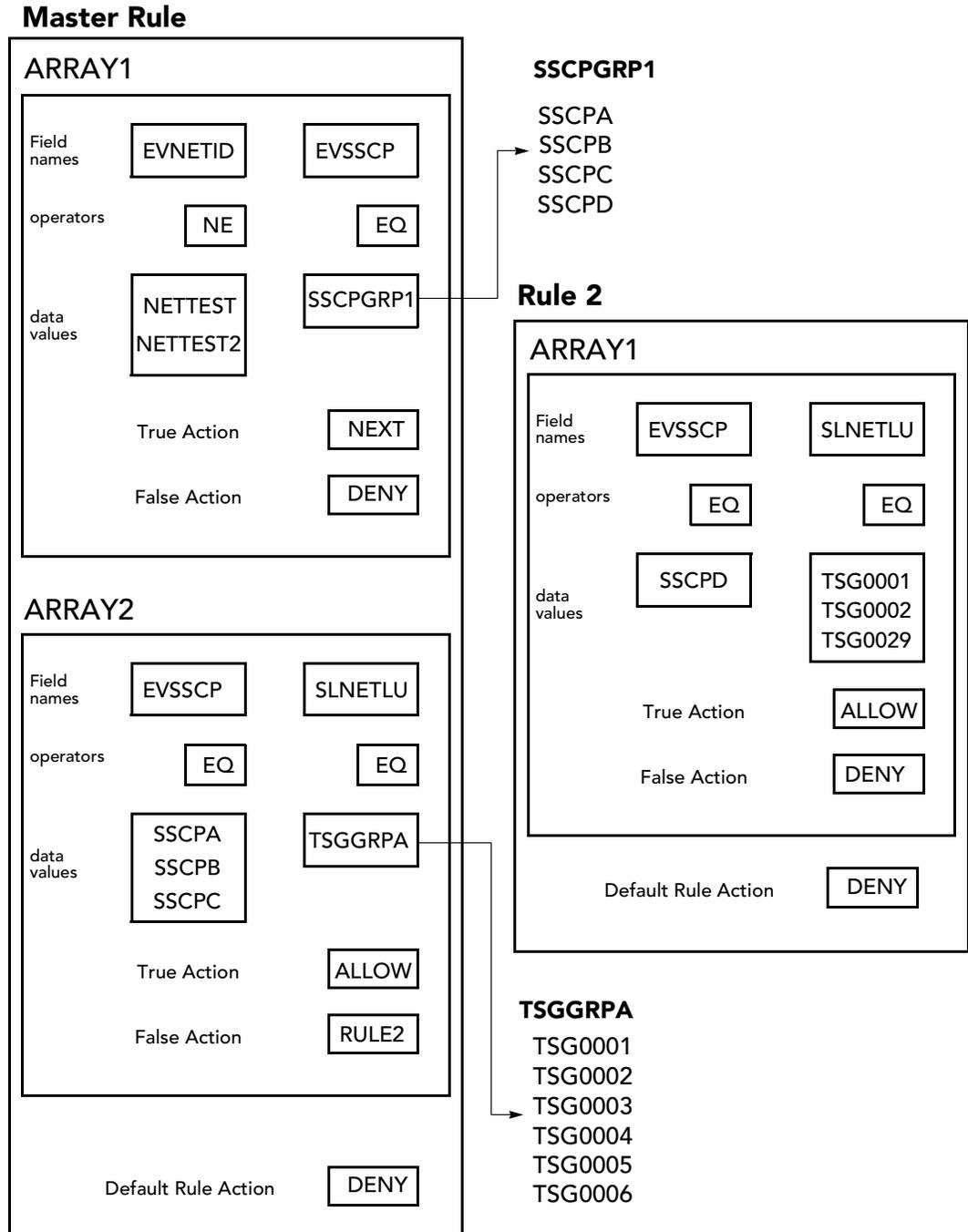


An explanation of the processing path using this table is described in the table on the following page

Rule	Array	Field	If the input value is...	then...
Master	ARRAY1	EVNETID	not equal to NETTEST and not equal to NETTEST2	The next column in the array (EVSSCP) is processed.
			NETTEST or NETTEST2	the FALSE action (DENY) is processed and the session initiation request fails.
		EVSSCP	SSCPA or SSCPB or SSCPC or SSCPD	since this is the last column in ARRAY1, the true action (NEXT) is processed. In this case, NEXT means process the next array (ARRAY2) in the rule.
			any value other than those listed above	the FALSE action (DENY) is processed and the session initiation request fails.
	ARRAY2	EVSSCP	SSCPA or SSCPB or SSCPC	the next column in the array (SLNETLU) is processed.
			any value other than those listed above	the FALSE action (RULE2) is processed. Processed will continue with ARRAY1 of RULE2.
		SLNETLU	TSG0001 or TSG0002 or TSG0003 or TSG0004 or TSG0005 or TSG0006	since this is the last column in ARRAY2, the TRUE action (ALLOW) is processed. The session initiation request is allowed.
			any value other than those listed above	the FALSE action (RULE2) is processed. Processing will continue with ARRAY1 of RULE2.
Rule2	ARRAY1	EVSSCP	SSCPD	the next column in the array (SLNETLU) is processed.
			any value other than SSCP	the FALSE action (DENY) is processed and the session initiation request fails.
		SLNETLU	TSG0001 or TSG0002 or TSG0029	since this is the last column in ARRAY1, the true action (ALLOW) is processed. The session initiation request is allowed.
			any value other than those listed above	the FALSE action (DENY) is processed and the session initiation request fails.

Creating a new control table - example

The instructions on the following pages show how you would create the example control table shown below.



The panels shown in the following example are fully described in the section entitled *Control table build* on page 7.32.

Creating the group definitions

You can define groups of related data to use when creating rules. For instance, in this example, two groups SSCPGRP1 and TSGGRPA have been defined. These group together SSCP names and terminal identifiers respectively.

You define the group using the SME GROUP DEFINITIONS panel (7.2); the group name can then be used in rule creation.

Note: You can define groups before or after control table creation. For this example the groups are being created first.

```
Date:12/12/1997          SME GROUP DEFINITIONS          Userid:TSG0001
Time:09:00              Terminal:T31CNS02

Line commands: C=Change D=Delete

S  GROUP NAME  COMMENTS              UPDATED  TIME  BY

To define a new group complete the fields below and press the <ENTER> key:
  Group Name => _____ Comments => _____

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

Step 1

Enter SSCPGRP1 at the **Group Name** prompt and suitable text at the **Comments** prompt and press <Enter>. The following screen will be displayed:

```
Date:12/12/1997          SME GROUP DEFINITIONS          Userid:TSG0001
Time:09:01              Terminal:T31CNS01

Line commands: C=Change D=Delete

S  GROUP NAME  COMMENTS                UPDATED   TIME BY
-  SSCPGRP1    SSCP GROUP 1           12/12/1997 09:01 TSG0001

To define a new group complete the fields below and press the <ENTER> key:
  Group Name => _____ Comments => _____

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

Step 2

Enter TSGGRPA at the **Group Name** prompt and suitable text at the **Comments** prompt and press <Enter>. The following panel will be displayed:

```
Date:12/12/1997          SME GROUP DEFINITIONS          Userid:TSG0001
Time:09:02              Terminal:T31CNS01

Line commands: C=Change D=Delete

S  GROUP NAME  COMMENTS                UPDATED   TIME BY
-  SSCPGRP1    SSCP GROUP 1           12/12/1997 09:01 TSG0001
-  TSGGRPA     TERMINAL GROUP A       12/12/1997 09:02 TSG0001

To define a new group complete the fields below and press the <ENTER> key:
  Group Name => _____ Comments => _____

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

Step 3 Enter the line command C under the S column against group SSCPGRP1 to add fields to the group. The following panel will be displayed:

```

Date:12/12/1997          SME GROUP SSCPGRP1          Userid:TSG0001
Time:09:03              Terminal:T31CNS01

Group comment => SSCP_GROUP 1

Line commands: D=Delete

S  DATA VALUES          TYPE

To add a new data value, complete the fields below and press <ENTER> :
  Data value => _____ Data type => _

F1=Help  F3=End  F6=Fields  F7=Up  F8=Down

```

Step 4 Enter SSCPA at the **Data value** prompt and press <Enter>. A message confirming that a data value has been added to the group will be displayed. Repeat this step for all the values in the group. The following panel will be displayed:

```

Date:12/12/1997          SME GROUP SSCPGRP1          Userid:TSG0001
Time:09:03              Terminal:T31CNS01

Group comment => SSCP_GROUP 1

Line commands: D=Delete

S  DATA VALUES          TYPE
-  SSCPA
-  SSCPB
-  SSCPC
-  SSCPD

To add a new data value, complete the fields below and press <ENTER> :
  Data value => _____ Data type => _
CKSE3269-9 Literal added to SSCPGRP1 list (Userid=TSG0001)

F1=Help  F3=End  F6=Fields  F7=Up  F8=Down

```

Step 5

Repeat steps 3 and 4 for group TSGGRPA using the group values shown in the example diagram. At the end the following panel will be displayed:

```
Date:12/12/1997          SME GROUP TSGGRPA          Userid:TSG0001
Time:09:03              Terminal:T31CNS01

Group comment => TERMINAL GROUP A

Line commands: D=Delete

S  DATA VALUES          TYPE
-  TSG0001
-  TSG0002
-  TSG0003
-  TSG0004
-  TSG0005
-  TSG0006

To add a new data value, complete the fields below and press <ENTER> :
  Data value => _____ Data type => _
CKSE3269-9 Literal added to SSCPGRP1 list (Userid=TSG0001)

F1=Help  F3=End  F6=Fields  F7=Up  F8=Down
```

These group names can now be used in control table creation.

Creating the master rule

A new rule is created by using option 1 (Rule maintenance) from the VSSE OPTIONS menu (7).

Step 1 To create a new rule enter the name in the **Rule** field and press <Enter>. For this example, the top level rule called MRULE will be created as shown on the following panel:

```
Date:12/12/1997                RULE MAINTENANCE                Userid:TSG0001
Time:09:05                    Terminal:T31CNS01

Line commands: C=Change  D=Delete  O=Outline  P=Print

S Rule      Comments                Default  Updated   Time  By
_ ADMRULE   ADMIN ONLY                WARN     11/11/1997 12:12 TSG0001
_ TRULE     TEST RULE                  ALLOW    11/11/1997 12:14 TSG0001

To add a new rule, complete the following fields:
Rule => MRULE Model Rule => _____

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

MRULE will be added to the list of rules.

Step 2 To add arrays to the new rule enter the C line command against MRULE. The following panel will be displayed:

```
Date:12/12/1997                RULE EDIT                Userid:TSG0001
Time:09:05                    Rule: MRULE              Terminal:T31CNS01

Default action => _____ Comment => _____

Line commands: A=After  B=Before  C=Change  D=Delete  M=Move

S Array      Number  Comments                True action  False action

To add a new array to the rule, complete the following fields:
Array => _____ Model array => _____ Model rule => _____

F1=Help  F3=End  F6=Prt  F7=Up  F8=Down  F12=Can
```

Step 3 Rule MRULE has two arrays, ARRAY1 and ARRAY2. Enter ARRAY1 at the **Array** prompt and press Enter. ARRAY1 will display under the Array column in the middle of the screen.

Step 4 Repeat this for ARRAY2.

Step 5 Tab to the **Default action** field. This is the default action for the rule. For this example, type DENY and press <Enter>.

Step 6 Tab to the **Rule comment** field and type TEST MASTER RULE.

The following panel will be displayed:

```
Date:12/12/1997                RULE EDIT                Userid:TSG0001
Time:09:06                    Rule: MRULE              Terminal:T31CNS01

Default action => DENY      Comment => TEST MASTER RULE

Line commands: A=After  B=Before  C=Change  D=Delete  M=Move

S Array   Number  Comments                True action  False action
_ ARRAY1   1
_ ARRAY2   2

To add a new array to the rule, complete the following fields:
  Array => _____ Model array => _____ Model rule => _____

F1=Help  F3=End  F6=Prt  F7=Up  F8=Down  F12=Can
```

Step 7 Enter the line command C against ARRAY1 under the S column to create the details for this array. The following panel will be displayed:

```
Date:12/12/1997                SME ARRAY EDIT          Userid:TSG0001
Time:09:06                    Rule: MRULE             Array: ARRAY1(1)       Terminal:T31CNS01
Array comment => _____
Line commands: C=Change D=Delete

Field:
Comp :

Data :
  and
Type

True action => _____ False action => _____

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

Step 8 Enter a comment in the **Array comment** field if required. For this example, type TEST ARRAY 1.

Step 9 Complete the True and False actions for this array. For this example, enter the values NEXT and DENY respectively.

Step 10 Press <F2> to insert the field names and data values for this array. The following panel will be displayed:

```
Date:12/12/1997          SME ARRAY/FIELD EDIT          Userid:TSG0001
Time:09:07              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => TEST ARRAY 1
Line commands: D=Delete  I=Include symbolic values  L=List group contents
+-----+
Field: | _____ |
Comp  : |  _  |
Data  : |
and   |
Type  |
      |
New   |
Data  : |
      |
+-----+
True action => NEXT      False action => DENY

F1=Help  F3=End  F6=Groups  F7=Up  F8=Down  F9=Fields  F12=Can
```

Step 11 Enter the first field name in the array. For this example, enter EVNETID in the **Field** field and press <Enter>.

Note: If you are unsure of a field name, press <F9> to provide a list of all available field names. Type S against the required name and press <F3>. This will place the selected field name at the Field prompt in the above panel. If an alias name has been specified, you can enter either the alias name or the default name. Where specified, alias names will be displayed in the rule.

Step 12 Enter the comparison operator in the **Comp** field. For this example enter NE.

Step 13 Enter the first data value in the **New Data** field. For this example, enter NETTEST and press <Enter>.

Step 14 Repeat step 13 for all data values. For this example, add one more data value, NETTEST2.

Step 15 Press <F3> to save and end. The panel will now display:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:08              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => TEST ARRAY 1
Line commands: C=Change D=Delete

Field:      EVNETID
Comp :      NE

Data :      NETTEST
and        NETTEST2
Type

True action => NEXT      False action => DENY

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

Step 16 Press <F2> to insert the next column in the array. The following panel will be displayed:

```
Date:12/12/1997          SME ARRAY/FIELD EDIT          Userid:TSG0001
Time:09:07              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => TEST ARRAY 1
Line commands: D=Delete  I=Include symbolic values  L=List group contents

+-----+
Field: |      |      EVNETID
Comp : |  _  |      NE
Data : |      |      NETTEST
and   |      |      NETTEST2
Type  |      |
New   |      |
Data : |      |
+-----+

True action => NEXT      False action => DENY

F1=Help  F3=End  F6=Groups  F7=Up  F8=Down  F9=Fields  F12=Can
```

Step 17 Repeat steps 11 through 13 for the second column in ARRAY1.

Note: The system recognizes the name of the group SSCPGRP1 which was input in the section entitled *Creating the group definitions* on page 7.20.

Step 18 Press <F3> to save and end. The column headers (the field names) are initially stored in reverse order of input, ie the last column entered is the first in the list as shown below:

```

Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => TEST ARRAY 1
Line commands: C=Change D=Delete

Field:   EVSSCP           EVNETID
Comp :   EQ              NE

Data :   SSCPGRP1 G       NETTEST
and
Type     NETTEST2

True action => NEXT      False action => DENY

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can

```

Step 19 Processing of the fields in an array is from left to right. For efficient processing, you must decide the appropriate order in which the fields are to be stored in the array. In this example, the column headed EVNETID should be processed first and therefore the order in which the columns are currently stored must be changed. Press <F5> to provide the CHANGE SME ARRAY FIELD ORDER panel as shown below:

```

Date:12/12/1997          CHANGE SME ARRAY FIELD ORDER          Userid:TSG0001
Time:09:00              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01

Line commands: A=After  B=Before  M=Move

S Field
- EVSSCP
- EVNETID

F1=Help  F3=End  F7=Up  F8=Down  F12=Can

```

Step 20 The fields are displayed in their current order. Enter line command M against field EVSSCP and line command A against field EVNETID to move field EVSSCP after field EVNETID. Press <Enter>. Field EVNETID is now the first column in the array.

Step 21 Press <F3> to display the following panel:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => TEST ARRAY 1
Line commands: C=Change D=Delete

Field:   EVNETID          EVSSCP
Comp :   NE              EQ

Data :   NETTEST          SSCPGRP1 G
and     NETTEST2

Type

True action => NEXT      False action => DENY

CKSE3359-9 Field order changed
F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

Step 22 All the data for ARRAY1 in rule MRULE has now been entered. Press <F3> to end.

Step 23 Repeat steps 7 through 18 to enter the example data for ARRAY2. All the data for rule MRULE has now been entered. The following panel should be displayed:

```

Date:12/12/1997                RULE EDIT                Userid:TSG0001
Time:09:00                      Rule: MRULE                Terminal:T31CNS01

Default action => DENY      Comment => TEST MASTER RULE

Line commands: A=After  B=Before  C=Change  D=Delete  M=Move

S Array      Number  Comments                True action  False action
_ ARRAY1     1    TEST ARRAY 1           NEXT        DENY
_ ARRAY2     2    TEST ARRAY 2           ALLOW        RULE2

To add a new array to the rule, complete the following fields:
Array => _____ Model array => _____ Model rule => _____

F1=Help  F3=End  F6=Prt  F7=Up  F8=Down  F12=Can

```

Note: In this example when you enter RULE2 as the false action for ARRAY2, a warning message will be displayed to alert you that RULE2 has not yet been defined to the system

Step 24 Press <F3> to end. A message confirming that rule MRULE has been changed will be displayed on the RULE MAINTENANCE (7.1) panel.

Creating lower level rules

Follow the same sequence of steps above to create the lower level rule, RULE2, using data from the example diagram at the beginning of the section.

Viewing the control table outline

A control table comprises one or more rules, identified by the name of its top level (or only) rule. You can view the outline of the control table you have created by entering line command O against the required rule name on the RULE MAINTENANCE panel (7.1).

Using the data created in the previous example, enter the line command O against **MRULE** to display the following structure.

```

Date:12/12/1997                               OUTLINE                               Userid:TSG0001
Time:09:00                                     Terminal:A01MS247

Line commands: C=Change  O=Outline

Level => 1                                     --S-Rule-----
Arrays within rule => 2                       |  _ MRULE      |
Default action => DENY                       |-----|
                                           |
                                           |-----|
                                           |
--S-Array---1-                               |             |
|  _ ARRAY1  |                               |  _ ARRAY2  |
|-----|
                                           |
                                           |-----|
                                           |
---(T)------(F)-----                    |             |
|  NEXT      DENY  | |  ALLOW  _ RULE2  |
|-----|
                                           |-----|
                                           |
F1=Help  F3=End  F7=Up  F10=Left  F11=Right

```

This panel describes the level currently being viewed and allows you to view lower levels if required. Enter O under the S column of RULE2 to display the following panel:

```

Date:12/12/1997                               OUTLINE                               Userid:TSG0001
Time:09:00                                     Terminal:T31CNS01

Line commands: C=Change  O=Outline

Level => 2                                     --S-Rule-----
Arrays within rule => 1                       |  _ RULE2      |
Default action => DENY                       |-----|
                                           |
                                           |-----|
                                           |
--S-Array---1-                               |             |
|  _ ARRAY1  |                               |             |
|-----|
                                           |
                                           |-----|
                                           |
---(T)------(F)-----                    |             |
|  ALLOW      DENY  |
|-----|
                                           |-----|
                                           |
F1=Help  F3=End  F7=Up  F10=Left  F11=Right

```

These two panels show the structure of the example control table.

Control table build

This section provides a detailed description of the panels required to create a control table. The input fields, display fields, line commands and function keys for each panel are described.

On line functions are available to allow the administrator to:

- add, change, delete and view RULES
- add, move change, delete and view AUTHORIZATION ARRAYS
- add, change and delete group definitions.

The VSSE OPTIONS menu

Option 7 from the NC-PASS SECURE MENU provides the VSSE OPTIONS panel displayed below:

```
Date:12/12/1997          VSSE OPTIONS          Userid:TSG0001
Time:09:00              Terminal:T31CNS01

Option => _____

          1 Rule maintenance
          2 List groups of data
          3 Load/restore control tables
          4 Test control table
          5 Set global options
          6 Control operator functions
          7 Date and time definitions
          8 Rule administration via MHO
          9 Authorization control table conversion

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

Options 1 and 2 provide the panels to enable you to create a control table. Enter the appropriate number at the **Option** prompt.

Rule maintenance

The rule maintenance option displays a list of all the rules that have been defined to your system. The panel displayed allows you to browse the list of rules, edit an existing rule, add a new rule or view the outline of the control table containing a specified rule.

Choose option 1 from the VSSE OPTIONS menu (7) to provide the RULE MAINTENANCE panel (7.1) shown below:

```

Date:12/12/1997          RULE MAINTENANCE          Userid:TSG0001
Time:09:05              Terminal:T31CNS01

Line commands: C=Change D=Delete O=Outline P=Print

S Rule      Comments                Default  Updated  Time By
ADMRULE      ADMIN ONLY                WARN       11/11/1997 12:12 TSG0001
MRULE        TEST MASTER RULE          DENY       12/12/1997 09:00 TSG0001
RULE2        TEST LOWER RULE           DENY       12/12/1997 09:01 TSG0001
TRULE        TEST RULE                ALLOW      11/11/1997 12:14 TSG0001

To add a new rule, complete the following fields:
Rule => _____ Model Rule => _____

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

```

Input fields

Field	Description
Rule	<p>You can use this field either to enter the name of a rule that you want to change or to add a new rule to the list.</p> <p>To change a rule enter the name of a rule that has previously been defined to the system. The RULE EDIT panel for that rule will be displayed. (If you are unsure of the name of an existing rule you can browse the list of rules on these panels using the <F7> and <F8> keys as appropriate.) You can then use the C line command against the required rule.</p> <p>To add a new rule enter the name of the new rule. You can use up to eight characters, consisting of letters, numbers and national characters.</p> <p>The new rule will be added to the list of rules. You can then use the C line command to add array information to the rule.</p> <p>Note: When you create a new rule, its name is initially added to the bottom of the list of rules. When the screen is next refreshed, the rule will be placed in alphabetical order.</p>
Model rule	<p>This is an optional field in which you can enter the name of an existing rule on which to model your new rule. The new rule structure and data will be identical to the model rule.</p>

Line commands

The line commands C, D, O and P can be entered in column S to perform the following functions:

- C provides the RULE EDIT panel for the specified rule. This panel allows you to add arrays to, move arrays in, or delete arrays from, the specified rule. You can also add or change the default action for the rule.
- D deletes the specified rule. A panel asking for confirmation is displayed.
- O provides the OUTLINE panel. This panel allows you to view the outline of the specified rule.
- P produces the SME RULES report. See *Printing a rule* on page 7.48.

Display fields

Field	Description
More	Rules are displayed in alphabetical order. If there are more rules than can be displayed on one screen, the word More and a plus sign (+) or a minus sign (-) or both will be displayed under the terminal identifier on the top right of the panel. The plus and minus signs indicate that further rules can be displayed by pressing <F8> or <F7> respectively.
Rule	A list of all the rules defined to the system.
Comments	A brief description of the rule, for information only.
Default	The action that will be executed when the rule has been processed and none of the array defined actions have resulted in a termination of either rule or control table processing.
Updated	The date when the rule was last updated.
Time	The time when the rule was last updated.
By	The userid of the user who last updated the rule.

Function keys

Key	Function
F1	displays help information.
F3	ends the display and returns to the previous panel.
F7	displays the previous screen of rules.
F8	displays the next screen of rules.

Changing/creating a rule

To change a rule, either enter line command C against the required rule name or enter the rulename at the **Rule** field on the RULE MAINTENANCE panel (7.1). The panel shown below will be displayed.

You can make the following changes to an existing rule:

- add or change arrays
- delete arrays
- add or change the default action.

To add a new rule, enter its name at the Rule field on the RULE MAINTENANCE panel and press <Enter>. To add arrays to the rule, enter line command C against the new rule name and press <Enter>.

The following panel will be displayed. (For new rules, initially there will be no entries under the Array, Number, Comments and action columns).

```

Date:12/12/1997                                RULE EDIT                                Userid:TSG0001
Time:09:00                                     Rule: RULENAME                            Terminal:T31CNS01

Default action => _____ Comment => _____

Line commands: A=After  B=Before  C=Change  D=Delete  M=Move

S Array      Number  Comments                                True action  False action
_  A1         1      TEST NETID                             ALLOW        NEXT
_  A2         2      TEST TERMID                            ALLOW        WARN

To add a new array to the rule, complete the following fields:
  Array => _____ Model array => _____ Model rule => _____

F1=Help  F3=End  F6=Prt  F7=Up  F8=Down  F12=Can

```

Input fields

Field	Description
Array	Enter the name of a new array to be added to this rule. Note: If you enter an array that has already been defined for this rule, the SME ARRAY EDIT panel will be displayed for the specified array.
Model array	If you want to model this array on an existing array, enter the name of the model array here. If the model array is in another rule you must enter the name of the rule in the Model rule field. The new array will have an identical structure to the model array.

Field	Description
Model rule	If you are modeling the new array on an existing array, enter the name of the rule containing the model array.
Default action	Enter the default action for the rule. The default action will be executed if the rule is processed and none of the array-defined actions results in a termination of either rule or control table processing. Note: NEXT is not valid as a default action for a rule.
Comment	Enter a brief description of the rule, if required.

Line command

The line commands A, B, C, D and M can be entered in column S to perform the following functions:

- A/B To move an array to a different position in the Array list, enter an M command against the array to be moved and press <Enter>. Tab to the target position and enter either an A to move the selected array to the position AFTER this array or a B to move the selected array to the position BEFORE this array.
- C provides you with the SME ARRAY EDIT panel for the specified array.
- D deletes the specified array.
- M identifies an array which is to be moved to another position in the Array list for this rule. Use in conjunction with the A and B line commands.

Display fields

Field	Description
More	If there are more than 11 arrays in the rule, the word More and a plus sign (+) or a minus sign (-) or both will be displayed under the terminal identifier on the top right of the panel. The plus and minus signs indicate that further arrays can be displayed by pressing <F8> or <F7> respectively.
Array	A list of the array names in the specified rule. Initially this list will be empty when you are creating a new rule.
Number	The position of the array in the rule. The positions can be changed using the A, B and M line commands as described above.
Comments	A brief description of the rule.
True action	The action that will be executed if processing of the array results in a TRUE condition.
False action	The action that will be executed if processing of the array results in a FALSE condition.

Function keys

Key	Function
F1	displays help information.
F3	saves any changes made and returns to the previously displayed panel.
F6	provides the SME rules report. See <i>Printing a rule</i> on page 7.48.
F7	displays the previous screen of arrays for this rule.
F8	displays the next screen of arrays for this rule.
F12	cancels any changes made and returns to the previously displayed panel.

Changing an array

Enter the line command C against the required array name on the RULE EDIT panel to provide the following panel:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: RULENAME  Array: A1(1)      Terminal:T31CNS01
Array comment => TEST NETID
Line commands: C=Change D=Delete

Field:      EVNETID          EVSSCP
Comp :      EQ              EQ

Data :      NETA            SSCPG1  G
and         NETB
Type        NETC

True action => ALLOW  False action => NEXT

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

If you want to:

- edit an existing column in the array use the C line command against the field name that heads the required column.
- add a new column to the array press the <F2> key. Refer to the subsection entitled *Adding a column to an array* on page 7.44.

Refer to the following text for descriptions of the fields on the panel.

Input fields

Field	Description
Array comment	Enter a brief description of the array, if required.
True action	The action that will be executed if processing of the array results in a TRUE condition.
False action	The action that will be executed if processing of the array results in a FALSE condition.

Line commands

The line commands C and D can be entered against the column header field names to perform the following functions:

- C Allows you to add new values to, or delete existing values from the data value list for that column.
- D Deletes the specified column and all its values.

Function keys

Key	Function
F1	displays help information. If you position the cursor against a field name and press <F1>, a description of the field will be displayed. Press <F1> with the cursor at any other position to display panel help information.
F2	provides the panel that allows you to insert a new column in the array.
F3	saves any changes made to the array and returns to the RULE EDIT panel.
F5	provides the SME ARRAY FIELD ORDERING panel which enables you to change the position of columns in the array.
F10	displays the previous screen of fields for the current array.
F11	displays the next screen of fields for the current array.
F12	cancels any changes made to the array and returns to the RULE EDIT panel.

Display fields

Field	Description
More	The word More and a left (<) or right sign (>) or both will be displayed under the terminal identifier on the top right of the panel, if there are additional columns to display. The left and right signs indicate that further columns can be displayed by pressing <F10> or <F11> respectively.
Field	The name of the field against which comparisons are to be made during array processing. This name can be the original name as specified by PassGo Technologies or an alias name.

Field	Description										
Comp	The comparison operator, either EQ (equal to) or NE (not equal to).										
Data and Type	<p>This field is a list in the format:</p> <p style="margin-left: 40px;"><i>data</i> <i>type</i></p> <p><i>Data</i> is the value to be matched during array processing for this field.</p> <p><i>Type</i> can be one of the following values:</p> <table border="0" style="margin-left: 40px;"> <tr> <td>D</td> <td>(Date/time definition)</td> </tr> <tr> <td>F</td> <td>(Field)</td> </tr> <tr> <td>G</td> <td>(Group)</td> </tr> <tr> <td>V</td> <td>(Value)</td> </tr> <tr> <td>blank</td> <td>(Literal)</td> </tr> </table> <p>Refer to <i>Field name values</i> on page 7.14 for details.</p>	D	(Date/time definition)	F	(Field)	G	(Group)	V	(Value)	blank	(Literal)
D	(Date/time definition)										
F	(Field)										
G	(Group)										
V	(Value)										
blank	(Literal)										

Changing the order of fields in an array

During control table processing, input data from the session initiation request is compared with the field values held in the control table arrays. Fields displayed on the SME ARRAY EDIT panel are processed from left to right. The order in which the fields are held can affect the efficiency of the comparison process. You can therefore change the order in which fields are stored in an array to maximize the efficiency of control table processing. Press <F5> to provide the following panel:

```
Date:12/12/1997          CHANGE SME ARRAY FIELD ORDER          Userid:TSG0001
Time:09:00              Rule: TRULE          Array: ARNET(4)          Terminal:T31CNS01

Line commands: A=After  B=Before  M=Move

S Field
- EVSSCP
- EVNETID
- DHCVR14

F1=Help  F3=End  F7=Up  F8=Down  F12=Can
```

Display fields

Field	Description
Field	The field names contained in the current array. If alias names have been entered for any of the fields, they will be displayed in preference to the VSSE field names.

Line commands

The line commands A, B and M can be entered against the column header field names to perform the following functions:

- A/B To move a field to a different position in the Array, insert an M command against the field to be moved. Tab to the target position and enter either an A to move the selected field to the position AFTER this field or a B to move the selected field to the position BEFORE this field.
- M identifies a field which is to be moved to another position in the Array. Use in conjunction with the A and B line commands.

Function keys

Key	Function
F1	displays help information.
F3	saves changes made to the order and returns to the SME ARRAY EDIT panel.
F7	scrolls up the list of fields.
F8	scrolls down the list of fields.
F12	cancels changes made to the order and returns to the SME ARRAY EDIT panel.

Changing a column within an array

Enter the line command C against the required field names on the SME ARRAY EDIT panel to provide the following panel:

```
Date:12/12/1997          SME ARRAY/FIELD EDIT          Userid:TSG0001
Time:09:00              Rule: MRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => NET/VTAM
Line commands: D=Delete  I=Include symbolic values  L=List group contents
+-----+
Field: |   EVNETID   |   EVSSCP
Comp  : |   EQ        |   EQ
Data  : |   NETA     |   SSCPG1  G
and   : |   NETB     |
Type  : |   NETC     |
      |         |
New   : |         |
Data  : |         |
      |         |
+-----+
True action => ALLOW      False action => NEXT

F1=Help  F3=End  F6=Groups  F7=Up  F8=Down  F9=Fields  F12=Can
```

The column to be edited is displayed as a boxed column. If you have entered more than one C line command, the next column to be edited will be displayed as a boxed column when you have finished editing the current boxed column.

Input fields

Enter the values described below and on the following page. When you have completed all the changes, press <F3> to save and end.

Field	Description
Comp	Change the comparison operator if required; EQ means equal to, NE means not equal to.
Data and type	Delete existing values if required using the D line command.

Field	Description
New data	<p>The new data entry consists of two fields, the data and its type. Enter additional data values if required, press the tab key, and enter the data type. Data values can be literals, symbolic values, group fields or field names.</p> <p>Literals Enter the value only, ie TSG0001. The default type is literal. You cannot enter a literal value in a column headed by a Flag field.</p> <p>Symbolic All the values associated with the field name entered in the Field input field have been automatically added to the column. Use the D line command to remove those not required. You can subsequently use the I line command to refresh the list to include all the associated symbolic values.</p> <p>Group Enter the name of the group, tab and enter G, or press <F6> to provide a list of groups. Refer to the <F6> entry in the list of function keys on the following page.</p> <p>Note: If you specify the name of a group that has already been defined to the system, you do not have to specify its type (G); the system will automatically insert this when you press <Enter> or <F3>.</p> <p>Field names Enter the name of the field, or its alias, tab and enter F. Alternatively, press <F9> to provide a list of fields.</p> <p>Date/time Only applicable if the Field name is TIMES. Enter the name of a date/time definition, tab and enter D, or press <F6> to provide a list of definitions. Refer to the F6 entry in the list of function keys on the following page.</p> <p>Note: If you specify the name of a definition that not yet been defined to the system, a warning message will be issued.</p>

Line commands

The line commands D, I and L can be entered against the data values entries to perform the following functions:

- D deletes the specified data value.
- I only applicable for data items with a V in the type field (symbolic data values). If you have previously deleted a symbolic value from the list of data values, this line command will refresh the list to include all symbolic values associated with the flag field.
- L only applicable for data items with a G in the type field. Displays the SME GROUP VALUES for *GROUPNAME* panel for the specified group.

Function keys

Key	Function
F1	displays help information. If you position the cursor against a field name or a symbolic value and press <F1>, a description of the field or value will be displayed. Press <F1> with the cursor at any other position to display panel help information.
F3	saves any changes made to the column.
F6	If you are editing a column headed by the field name TIMES , press this key to display the DATE AND TIME DEFINITION panel. If you are editing a column headed by any other field name, press this key to display the SME GROUP DEFINITIONS panel. Enter S against the required definition or group and press <F3>. The selection will automatically be entered in the Data and Type field.
F7	allows you to scroll up through the list of data values.
F8	allows you to scroll down through the list of data values.
F9	provides the FIELD LIST panel. Enter S against the required field and press <F3>. The name will automatically be entered in the Data and Type field. If an alias name has been assigned to a field, this name will also be displayed on the FIELD LIST panel. An asterisk (*) in the S column in the FIELD LIST panel indicates that this field, or an alias, is already used by the current column and cannot be reselected. The letter F following a field name indicates that this field is a flag field. Note: If the column header field name is a flag field, the list of fields on the FIELD LIST panel is restricted to flag fields only. Similarly, if the column header field name is a non-flag field, no flag fields will be included on the FIELD LIST panel. This is because you cannot mix flag and non-flag fields.
F12	cancels any changes made to the column.

Display fields

Field	Description
More	The word More and a plus sign (+) or a minus sign (-) or both will be displayed under the terminal identifier on the top right of the panel, if there are additional data values to display. The plus and minus signs indicate that further values can be displayed by pressing <F8> or <F7> respectively.
Array comment	The description of the array.
Field	The name of the field against which comparisons are to be made during array processing.
True action	The action that will be executed if processing of the array results in a TRUE condition.
False action	The action that will be executed if processing of the array results in a FALSE condition.

Adding a column to an array

Press <F2> on the SME ARRAY EDIT panel to provide the following panel:

```

Date:12/12/1997          SME ARRAY/FIELD EDIT          Userid:TSG0001
Time:09:00              Rule: LRULE          Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => NET/VTAM
Line commands: D=Delete I=Include symbolic values L=List group contents
+-----+
Field: | _____ |          EVNETID          EVSSCP
Comp : |    _    |          EQ          EQ
Data : |          |          NETA          SSCPG1  G
and   |          |          NETB
Type  |          |          NETC
New
Data : |          |
+-----+
True action => ALLOW      False action => NEXT

F1=Help  F3=End  F6=Groups  F7=Up  F8=Down  F9=Fields  F12=Can

```

Existing columns are displayed to the right of the new (boxed) column to be inserted.

Input fields

Enter the values described below and on the following page. When you have completed all the new data values, press <F3> to save and end.

Field	Description
Field	<p>Enter the name of the field containing the SME VTAM data which is to be matched with the values specified below and press <Enter>. Fields can be network defined, imaginary or flags. You can enter an alias name for any field if one has been defined.</p> <p><F12> provides the FIELD LIST panel. Refer to the F12 entry in the list of PF keys below.</p>
Comp	<p>Enter the appropriate comparison operator; EQ means equal to, NE means not equal to.</p>

Field	Description
New data	<p>Enter the data value, press the tab key, and enter the data type. Data values can be literals, symbolic values, group fields or field names.</p> <p>Literals Enter the value only, ie TSG0001. The default type is literal. You cannot enter a literal value in a column headed by a Flag field.</p> <p>Symbolic All the values associated with the data value entered in the Field input field have been automatically added to the column. Use the D line command to remove those not required.</p> <p>Group Enter the name of the group, tab and enter G, or press <F6> to provide a list of groups. Refer to the <F6> entry in the list of function keys on the following page.</p> <p>Note: If you specify the name of a group that has already been defined to the system, you do not have to specify its type (G); the system will automatically insert this when you press <Enter> or <F3>.</p> <p>Field names Enter the name of the field, tab and enter F, or press <F12> to provide a list of fields.</p> <p>Date/time Only applicable if the Field name is TIMES. Enter the name of a date/time definition, tab and enter D, or press <F6> to provide a list of definitions. Refer to the <F6> entry in the list of function keys on the following page.</p> <p>Note: If you specify the name of a definition that has not yet been defined to the system, a warning message will be displayed.</p>

Line commands

The line commands D, I and L can be entered against the data fields to perform the following functions:

- D deletes the specified data value.
- I only applicable for data items with a V in the type field (symbolic data values). If you have previously deleted a symbolic value from the list of data values, this line command will refresh the list to include all symbolic values associated with the flag field.
- L only applicable for data items with a G in the type field (Group values). Provides the SME GROUP VALUES for *GROUPNAME* panel.

Display fields

Field	Description
More	The word More and a plus sign (+) or a minus sign (-) or both will be displayed under the terminal identifier on the top right of the panel, if there are additional data values to display. The plus and minus signs indicate that further values can be displayed by pressing <F8> or <F7> respectively.
Array comment	The description of the array.
True action	The action that will be executed if processing of the array results in a TRUE condition.
False action	The action that will be executed if processing of the array results in a FALSE condition.

Function keys

Key	Function
F1	displays help information. If you position the cursor against a field name or a symbolic value and press <F1>, a description of the field or value will be displayed. Press <F1> with the cursor at any other position to display panel help information.
F3	saves the array with the new column. The new column is displayed as the first column on the screen. You can change the order if you want. Refer to the subsection entitled <i>Changing the order of fields in an array</i> on page 7.40.
F6	If you are editing a column headed by the field name TIMES , press this key to display the DATE AND TIME DEFINITION panel. If you are editing a column headed by any other field name, press this key to display the SME GROUP DEFINITIONS panel. Enter S against the required definition or group and press <F3>. The selection will automatically be entered in the Data and Type field.
F7	scrolls up through the list of data values.
F8	scrolls down through the list of data values.

Key	Function
F9	<p>Provides the FIELD LIST panel. This function can be used to select a field name for the Field field or for the New data field.</p> <p>If an alias name has been assigned to a field, this name will also be displayed on the FIELD LIST panel.</p> <p>An asterisk (*) in the S column in the FIELD LIST panel indicates that this field, or an alias, is already used by the current array/column and cannot be reselected.</p> <p>The letter F following a field name indicates that this field is a flag field.</p> <p>Field Enter S against the required field and press <F3>. The name will automatically be entered in the Field input field.</p> <p>If the field selected is a symbolic (flag) field, the system will automatically enter all associated symbolic values in the Data and Type fields.</p> <p>New data Enter S against the required fields and press <F3>. The selected fields will be entered in the Data and Type input fields.</p> <p>Note: If the column header field name is a flag field, the list of fields on the FIELD LIST panel is restricted to flag fields only. Similarly, if the column header field name is a non-flag field, no flag fields will be included on the FIELD LIST panel. This is because you cannot mix flag and non-flag fields.</p>
F12	<p>cancels any changes made to the array and returns to the SME ARRAY EDIT panel.</p>

Printing a rule

Use the P line command on the RULE MAINTENANCE panel (7.1) or press <F6> on the RULE EDIT panel to produce an SME RULES report for the requested rules.

A panel will be displayed in which you must provide details of your printer. Refer to the section entitled *Producing reports from administration panels* on page 10.16 for further details.

When you have entered the appropriate details, press <Enter> to start printing the report, an example of which is shown below:

```
Date 12/12/1997          NC-PASS REPORT          PAGE    1
TIME 09:00              SME RULES

-----

Report requested by - TSG0001
                   on Terminal - A01MS009
                   Job Name - CKDTSG12
=====

RULE NAME.....: MRULE
RULE COMMENTS.....: MASTER RULE
DEFAULT ACTION.....: DENY

-----

ARRAY NAME.....: ARRAY1
ARRAY COMMENT.....: TEST ARRAY 1

  FIELD NAME  COMP  FIELD DATA

  EVNETID    EQ    NETTEST      NETTEST2
  EVSSCP     EQ    SSCPGRP1 (G)

TRUE ACTION.....: NEXT                      FALSE ACTION.....: DENY

-----

ARRAY NAME.....: ARRAY2
ARRAY COMMENT.....: TEST ARRAY 2

  FIELD NAME  COMP  FIELD DATA

  SLNETLU    EQ    ADM*

TRUE ACTION.....: ALLOW                      FALSE ACTION.....: DENY

-----

The following groups were found in the above rule.

  GROUP NAME      GROUP DATA          TYPE

  SSCPGRP1       SSCPA
                  SSCPB
                  SSCPC
                  SSCPD

=====

End of report. 1 rule printed
```

Notes

1. If there are any Groups in the rule, they will be printed at the end of the report.
2. If there are any Date/time definitions in the rule, they will be printed at the end of the report.
3. Details of lower level rules are not printed.
4. Data types are identified as follows:
 - F Field
 - V Symbolic
 - G Group
 - D Date/time definition.

The following list describes the additional information displayed on the panel:

Field	Description
More	The word More will be displayed under the terminal identifier if: <ul style="list-style-type: none">• there are additional arrays to view. (A left (<) or right (>) symbol will show the direction)• there are rules above or below the rule currently being displayed. (A plus (+) or minus sign (-) denotes a higher or lower level rule respectively.)
Level	The current level being displayed: 1 the top level rule >1 lower level rules.
Arrays within rule	The total number of arrays constituting this rule. (Only three arrays can be displayed on any one screen. Use <F10> and <F11> to view other arrays.)
Default action	The default action for the rule displayed.

Function keys

Key	Function
F1	displays help information.
F3	ends the display and returns to the previously displayed panel.
F7	returns to the previously displayed <i>level-1</i> . Not applicable at level 1.
F10	moves the display three arrays to the left.
F11	moves the display three arrays to the right.

Grouping data

You can categorize a number of data values by classifying them as a single group. You can use the group name as a data value when creating a control table array, rather than the individual data values. For instance you could group together terminal ids used by a particular department.

Groups can be set up containing literal values or flag field values. Groups cannot reference other group definitions. An example of a group definition is shown below:

Example

Group name	Data values	Type
TSGGRP1	TSG00*	literal
	TSG0998	literal
	TSG0999	literal

This group contains all terminal ids that start with 'TSG00' and terminal ids TSG0998 and TSG0999.

An example of the use of this group in an array is shown below:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: TRULE      Array: ARRAY1(1)      Terminal:T31CNS01
Array comment => _____
Line commands: C=Change D=Delete

Field:      SLNETLU
Comp :      EQ

Data :      TSGGRP1  G
and        TSGGRP5  G
Type       TSG1111

True action => NEXT      False action => DENY

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

SLNETLU is the name of the field containing the SLU identifier. During processing of this array, the input data (in this example, the terminal identifier) will be compared with the data values held in groups TSGGRP1 and TSGGRP5 and with the literal value TSG1111. If a match is found with any of the values held in the two groups or with the value TSG1111, the result will be a TRUE condition.

Defining a group

Enter **2** at the **Option** prompt on the VSSE OPTIONS (7) panel to provide the following panel:

```
Date:12/12/1997          SME GROUP DEFINITIONS          Userid:TSG0001
Time:09:02              Terminal:T31CNS01

Line commands: C=Change D=Delete

S  GROUP NAME  COMMENTS          UPDATED  TIME  BY
_  SSCPGRPT    TEST SYSTEM      11/11/97 14:58 TSG0001
_  TSGGRP1     TSG TEAM 1       11/11/97 10:02 TSG0001

To define a new group complete the fields below and press the <ENTER> key:
  Group Name => _____ Comments => _____

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

To create a new group, enter the details at the input fields described below. To edit an existing group, enter the line command C in the S column against the required group and press <Enter>.

Input fields

Field	Description
Group Name	Enter the name of the new group. You can use up to eight characters consisting of letters, numbers and national characters. (In the USA for example, national characters are the dollar sign (\$), the at symbol (@) and the hash symbol (#). In the UK national characters are the pound sign (£), the at symbol (@) and the hash symbol (#).
Comments	Enter a comment to document the group name. Used as reference information only.

Line commands

The line commands C and D can be entered in column S to perform the following functions:

- C provides editing facilities for the specified group through the SME GROUP VALUES for *GROUPNAME* panel.
- D deletes the specified group. A panel requesting confirmation of the deletion will be displayed.

Display fields

Field	Description
More	Groups are displayed in alphabetical order. This field shows a plus sign (+) if there are more groups on the next screen and a minus sign (-) if there are more groups on a previous screen.
GROUP NAME	A list of all the group names defined to the system.
COMMENTS	Reference information.
UPDATED	The date on which the group was last updated.
TIME	The time at which the group was last updated.
BY	The userid of the user who last updated the group.

Function keys

Key	Function
F1	displays help information.
F3	saves any changes made and returns to the previously displayed panel.
F7	displays the previous screen of group names.
F8	displays the next screen of group names.

Defining group values

Enter the line command C in the S column against the required group on the SME GROUP DEFINITIONS panel to provide the following screen:

```
Date:12/12/1997          SME GROUP TSGGRPA          Userid:TSG0001
Time:15:34                Terminal:T31CNS01

Group comment => TERMINAL GROUP A

Line commands: D=Delete

S  DATA VALUES          TYPE
-  TSG0001
-  TSG0002
-  TSG0003
-  TSG0004
-  TSG0005
-  TSG0006

To add a new data value, complete the fields below and press <ENTER> :
Data value => _____ Data type => _

F1=Help  F3=End  F6=Fields  F7=Up  F8=Down
```

Use this screen to define new values to the group or to delete existing values.

Input fields

Field	Description
Data value	Enter a literal value, a symbolic field value or a field name. Use <F6> to view and select field names.
Data type	Valid values are: L (Literal) V (symbolic Value) F (Field name).

Line commands

The line command D can be entered in column S to perform the following function:

D deletes the specified data value.

Display fields

Field	Description
DATA VALUES	The list of literals, field names or symbolic values which constitute the group.
TYPE	The type of data value: Field a field name Symbolic a symbolic value (blank) a literal value.

Function keys

Key	Function
F1	displays help information.
F3	saves any changes made and returns to the SME GROUP DEFINITIONS panel.
F6	provides the FIELD LIST panel which allows you to select a field name for inclusion in the data values list.
F7	displays the previous screen of data values.
F8	displays the next screen of data values.

Control table test before loading

An on line function is available to allow administrators to test the processing logic of a control table before it is used in a production environment.

Using the test function

Before loading a control table, it must be tested to ensure that the processing paths have been correctly defined. The following examples use the data specified in the Example control table earlier in this chapter.

The panels shown in the following examples are fully described in the section entitled *Test function panels* on page 7.61.

Testing a single rule

An action in array can make a call to another rule. A control table is therefore a hierarchical structure which can comprise a number of rules. If you are building a complex structure, you may want to test each rule in turn, often before you have even defined the lower level rules to the system.

For example, after completing Step 20 in Creating a new control table earlier in this chapter, you can test the processing logic of the top level rule MRULE before you go on to define RULE2 to the system, as described below:

Step 1

Choose option 4 from the VSSE OPTIONS panel (7) to provide the SME CONTROL TABLE TESTING panel (7.4) as shown below

```
Date:12/12/1997          SME CONTROL TABLE TESTING          Userid:TSG0001
Time:09:00              Terminal:T31CNS01

Test name => _____ Press <F5> to list previous tests.
Rule name => _____ Press <F9> to list rule names.
Single rule test => N Y/N

Line commands (flag fields only): I=Include X=Exclude

S  FIELD NAME  TYPE  FIELD DATA

To run a test enter data for selected fields and press <F2> :

F1=Help  F2=Run  F3=End  F5=Tests  F7=Up  F8=Down  F9=Rules  F12=Can
```

Step 2 Enter a name for the new test, for example MTEST and press <Enter>. A message informing you that a test called MTEST has not been found will be displayed.

Step 3 Tab to the Rule name field and type MRULE.

Step 4 Tab to the Single rule test field, type Y and press <Enter>. The following panel will be displayed.

```

Date:12/12/1997          TEST CONTROL TABLE BUILD ERRORS          Userid:TSG0001
Time:09:00                Terminal:T31CNS01

The following messages were issued during creation of a control table

CKSE3263-4 Rule RULE2 does not exist - Control Table build incomplete

F3=End  F7=Up  F8=Down

```

As the Single rule test field on the SME CONTROL TABLE TESTING panel (7.4) was set to Y, this message is displayed for information only.

Step 5 Press <F3> to return to the SME CONTROL TABLE TESTING panel (7.4) as shown below:

```

Date:12/12/1997          SME CONTROL TABLE TESTING          Userid:TSG0001
Time:09:00                Terminal:T31CNS01

Test name => MTEST Press <F5> to list previous tests.
Rule name => MRULE Press <F9> to list rule names.
Single rule test => Y Y/N

Line commands (flag fields only): I=Include X=Exclude

S  FIELD NAME  TYPE  FIELD DATA
  EVNETID      _____
  EVSSCP       _____
  SLNETLU      _____

To run a test enter data for selected fields and press <F2> :

F1=Help  F2=Run  F3=End  F5=Tests  F7=Up  F8=Down  F9=Rules  F12=Can

```

The FIELD NAME column has been prefilled with the field names defined in MRULE. These cannot be changed. (If alias names have been defined for any of the fields, the alias names will be displayed.)

Step 6 Enter the data required to check the rule. For this example, check the path that leads to the False action in ARRAY 2, by entering the following values against the appropriate field:

EVNETID **NETA**
EVSSCP **SSCPD**
SLNETLU **TSG0029**

Step 7 Press <F2> to run the test. The following panel will be displayed:

```
Date:12/12/1997          CONTROL TABLE TEST RESULTS          Userid:TSG0001
Time:09:00                Terminal:T31CNS01

Test name          => MTEST
Control table name => MRULE

Action taken       => RULE2          The action defined by the decision
                                   rule.
Action type        => FALSE          The action type to which the action
                                   taken was assigned.
Decision rule      => MRULE          The name of the rule in which the
                                   decision was made.
Decision array     => ARRAY2(2)      The array and its number in which the
                                   decision was made.
Last field         => EVSSCP          The last field in the array to be
                                   accessed before the decision was made.
Field comparator   => EQ             The comparator used for the incoming
                                   data and the field values defined.
Last field data    => SSCP           The last data to be cross referenced
                                   before the decision was made.

F1=Help  F3=End
```

This panel provides the information regarding the path taken through the rule. In this example, the value SSCP correctly caused the False action (RULE2) to be processed. Since this is a single rule test, RULE2 is not itself tested.

Step 8 Press <F3> to return to the SME CONTROL TABLE TESTING panel (7.4).

Step 9 Press <F3> to save the test called MTEST.

Testing a complete control table

The following example also uses the data specified in the Example control table earlier in this chapter.

After defining RULE2 to the system, you can test the processing logic of the complete control table, as described below:

Step 1 Choose option 4 from the VSSE OPTIONS panel (7) to provide the SME CONTROL TABLE TESTING panel (7.4) as shown below.

```
Date:12/12/1997          SME CONTROL TABLE TESTING          Userid:TSG0001
Time:09:00              Terminal:T31CNS01

Test name => _____ Press <F5> to list previous tests.
Rule name => _____ Press <F9> to list rule names.
Single rule test => N Y/N

Line commands (flag fields only): I=Include X=Exclude

S  FIELD NAME  TYPE  FIELD DATA

To run a test enter data for selected fields and press <F2> :

F1=Help  F2=Run  F3=End  F5=Tests  F7=Up  F8=Down  F9=Rules  F12=Can
```

Step 2 Enter a name for the new test, for example CTTEST and press <Enter>. A message informing you that a test called CTTEST has not been found will be displayed.

Step 3 Tab to the Rule name field and type MRULE.

Step 4 Leave the Single rule test field at its default value N and press <Enter>. The following panel will be displayed:

```
Date:12/12/1997          SME CONTROL TABLE TESTING          Userid:TSG0001
Time:09:00              Terminal:T31CNS01

Test name => CTTEST  Press <F5> to list previous tests.
Rule name => MRULE   Press <F9> to list rule names.
Single rule test => N Y/N

Line commands (flag fields only): I=Include X=Exclude

S  FIELD NAME  TYPE  FIELD DATA
  EVNETID
  EVSSCP
  SLNETLU

To run a test enter data for selected fields and press <F2> :

F1=Help  F2=Run  F3=End  F5=Tests  F7=Up  F8=Down  F9=Rules  F12=Can
```

Note: If a rule name has been specified as a true or false action in the control table you are testing and that rule has not yet been defined to the system, the control table test will fail. Either define the rule to the system and resume the test, or use the single rule test facility instead.

Step 5 The FIELD NAME column has been prefilled with the field names defined in MRULE. These cannot be changed. Enter the data required to check the rule. For this example, check the path that leads to the True action in ARRAY 1 of RULE2, by entering the following values against the appropriate field:

```
EVNETID  NETA
EVSSCP   SSCPD
SLNETLU  TSG0029
```

Step 6 Press <F2> to run the test. The following panel will be displayed:

```
Date:12/12/1997          CONTROL TABLE TEST RESULTS          Userid:TSG0001
Time:09:00                Terminal:T31CNS01

Test name          => CTTEST
Control table name => MRULE

Action taken       => ALLOW          The action defined by the decision
                                   rule.
Action type        => TRUE           The action type to which the action
                                   taken was assigned.
Decision rule      => RULE2         The name of the rule in which the
                                   decision was made.
Decision array     => ARRAY1(1)     The array and its number in which the
                                   decision was made.
Last field         => SLNETLU       The last field in the array to be
                                   accessed before the decision was made.
Field comparator   => EQ           The comparator used for the incoming
                                   data and the field values defined.
Last field data    => TSG0029       The last data to be cross referenced
                                   before the decision was made.

F1=Help  F3=End
```

This panel provides the information regarding the path taken through the rule. In this example, the session request would be ALLOWed.

Step 7 Press <F3> to return to the SME CONTROL TABLE TESTING panel (7.4).

Step 8 Press <F3> to save the test called CTTEST.

Test function panels

Choose option 4 from the VSSE OPTIONS panel (7) to display the following panel:

```
Date:12/12/1997          SME CONTROL TABLE TESTING          Userid:TSG0001
Time:09:00              Terminal:T31CNS01

Test name => _____ Press <F5> to list previous tests.
Rule name => _____ Press <F9> to list rule names.
Single rule test => N Y/N

Line commands (flag fields only): I=Include X=Exclude

S  FIELD NAME  TYPE  FIELD DATA

To run a test enter data for selected fields and press <F2> :

F1=Help  F2=Run  F3=End  F5=Tests  F7=Up  F8=Down  F9=Rules  F12=Can
```

Input fields

Field	Description
Test name	<p>Enter the name of the test you want to run. This can be an existing test name (<F5> provides the CONTROL TABLE TEST LIST panel which lists all previous tests) or a new test.</p> <p>If you enter an existing test name all data from this test will be loaded in the appropriate fields on the panel. You can change these if required.</p> <p>If you enter a new test name, an informative message will be displayed. You must then complete the Rule name field for the new test.</p>

Field	Description
Rule name	<p>This field will be prefilled if you have specified an existing test. You can change this if required.</p> <p>Use this field in conjunction with the Single rule test field to test either an entire control table or a single rule.</p> <p>To test a control table, enter the name of the rule which is to be the master rule in this control table test and set the Single rule test field to N. (<F9> provides the RULE SELECTION LIST panel, from which you can select a rule to test.)</p> <p>Note: If the specified rule name contains references to other rule names which have not been defined to the system, the control table build will fail. A panel will be displayed giving details of the rule names which caused the build to fail.</p> <p>To test a single rule, enter the name of the rule and set the Single rule test field to Y. (<F9> provides the RULE SELECTION LIST panel, from which you can select a rule to test.)</p>
Single rule test	Enter Y to test a single rule. Enter N to test a complete control table.
FIELD DATA	<p>Enter the required test data values against the appropriate field name.</p> <p>This column will be prefilled with all possible symbolic values if the field name is a flag field. Use the X line command to exclude unwanted symbolic names.</p>

Display fields

Field	Description
FIELD NAME/TYPE	<p>The system prefills these columns with all the field names (column headers) and types from the arrays which constitute the rule entered in the Rule name field above. These cannot be changed.</p> <p>Note: An asterisk (*) next to a field name indicates that the field has been deleted from the rule since the last time this test was run. The field is provided for information only and has no effect on the test.</p>

Line commands

The line commands I and X apply only to flag field entries. These commands can be entered in column S to perform the following functions:

- I Includes all the symbolic names associated with the flag field in the test. This command will typically be used after one or more X commands have removed symbolic names from the test.
- X Excludes the specified symbolic name from the test.

Function keys

Key	Function
F1	displays help information.
F2	runs the test using the data supplied.
F3	ends the test and returns to the previously displayed panel. The test name and associated rule data are saved.
F5	provides the CONTROL TABLE TEST LIST panel from which you can select a test to run.
F7	scrolls up the list of field names. The word More and a minus sign (-) indicate that there more names to view above the current display.
F8	scrolls down the list of field names. The word More and a plus sign (+) indicate that there more names to view below the current display.
F9	provides the RULE SELECTION LIST panel, from which you can select a rule to test.
F12	cancel the test and returns to the previously displayed panel. No data is saved.

Test results

Press <F2> on the SME CONTROL TABLE TESTING panel to run the test. The following CONTROL TABLE TEST RESULTS panel will be displayed.

```
Date:12/12/1997          CONTROL TABLE TEST RESULTS          Userid:TSG0001
Time:09:00              Terminal:T31CNS01

Test name                => COMPTST
Control table name => MRULE

Action taken             => WARN          The action defined by the decision
                                   rule.
Action type              => TRUE          The action type to which the action
                                   taken was assigned.
Decision rule            => TERMRULE      The name of the rule in which the
                                   decision was made.
Decision array           => AADM(1)       The array and its number in which the
                                   decision was made.
Last field               => SLNETLU       The last field in the array to be
                                   accessed before the decision was made.
Field comparator         => EQ            The comparator used for the incoming
                                   data and the field values defined.
Last field data          => TSG0001       The last data to be cross referenced
                                   before the decision was made.

F1=Help  F3=End
```

Display fields

The fields displayed describe the array, rule and field in which control table processing would stop given the data specified for the test.

Function keys

- | Key | Function |
|-----|--|
| F1 | displays help information. |
| F3 | ends the display and returns to the SME CONTROL TABLE TESTING panel (7.4). |

The LOAD/RESTORE CONTROL TABLES panel

Two copies of the control table can be held in CSA at any one time:

- an Active Control Table (ACT) - the table that the SME is currently processing
- a Backup Control Table (BCT) - a copy of the ACT.

The LOAD/RESTORE CONTROL TABLES panel comprises three sections containing fields that:

- allow you to load a new Control Table
WARNING: The current ACT becomes the BCT and the current BCT will be removed from CSA.
- display details about the Control Tables loaded or moved by this NC-PASS
- display details about the Control Tables currently in CSA.

Displaying the LOAD/RESTORE CONTROL TABLES panel

Enter option 3 on the VSSE OPTIONS panel to display the LOAD/RESTORE CONTROL TABLES panel (7.3) shown below:

```
Date:12/12/1997          LOAD/RESTORE CONTROL TABLES          Userid:TSG0001
Time:09:44                Terminal:A01MS048

To load a Control table from NC-PASS complete the fields below and press <F5> :
JOBNAME          => CKPASS1Q
MASTER RULE NAME => _____
DEFAULT ACTION   => ALLOW   ALLOW, DENY or WARN
REFRESH          => Y Y/N Refresh the active Control table at job startup
CONFIRM          => Y Y/N Display confirmation panel

Control tables loaded or moved by this NC-PASS:
TABLE NAME      JOBNAME DATE      TIME
ACTIVE MASTER1 CKPASS1Q 02/12/1997 08:32
BACKUP None     N/A      N/A         N/A

Control tables in CSA:
TABLE NAME      STATUS  ORIGINALLY LOADED          LAST MOVED
JOBNAME DATE      TIME JOBNAME
ACTIVE MASTER  ACTIVE  CKPASS1Q 02/12/1997 08:32 CKPASS1Q
BACKUP None    N/A     N/A         N/A     N/A

F1=Help  F2=Act  F3=End  F5=Load  F6=Rest  F9=Rules
```

Loading a Control Table

The fields in the first section of the LOAD/RESTORE CONTROL TABLES panel are described below.

Input fields

Field	Description
MASTER RULE NAME	<p>Enter the name of the master rule for the control table which is to be made the ACT.</p> <p>When this is processed, ie when you press <F5>:</p> <ul style="list-style-type: none">the Backup Control Table is removed from CSA,the Active Control Table becomes the Backup Control Table, <p>the Control Table specified in this MASTER RULE NAME field becomes the Active Control Table.</p>
DEFAULT ACTION	<p>Enter the action that will be executed if none of the array defined actions results in a termination of control table processing. The default action provided is ALLOW.</p>
REFRESH	<p>Enter Y or N. The default value is N. See <i>System startup</i> on page 7.69 for details.</p>
CONFIRM	<p>Specify whether changes made to this panel require confirmation by entering Y or N. The default value is N.</p>

Display field

Field	Description
JOBNAME	<p>This is the name extracted from the JCL statement. It is provided for convenience on the panel as a quick reference.</p> <p>If the panel is used to load or restore a Control Table, then this name will be used by NC-PASS.</p>

Displaying details about Control Tables loaded or moved by this NC-PASS

The fields in the second section of the LOAD/RESTORE CONTROL TABLES panel are described below.

Display fields

Field	Description
TABLE	Indicates whether the table is the Active or Backup Control Table according to the NC-PASS job.
NAME	The name of the Control Table.
JOBNAME	This is the name extracted from the JCL statement when the Control Tables were loaded by this NC-PASS job. This name is stored in the Central Administration File (CAF).
DATE	The date when this NC-PASS job loaded the Control Table.
TIME	The time when this NC-PASS job loaded the Control Table.

Displaying details about the Control Tables currently in CSA

The fields in the third section of the LOAD/RESTORE CONTROL TABLES panel are described below.

Display fields

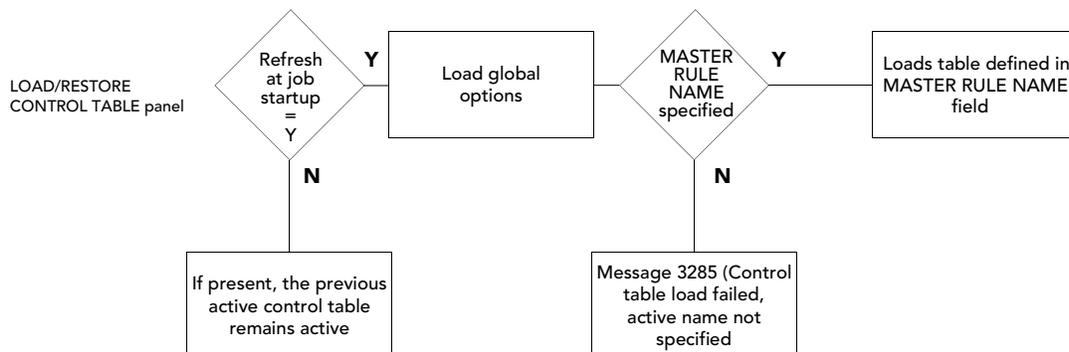
Field	Description
TABLE	Indicates whether the table is the Active or Backup Control Table according to the NC-PASS job.
NAME	The name of the Control Table that is currently active.
STATUS	For the Active Control Table, this field may be set to: Active which is the normal state. Backed out if the remote back out procedure has been executed, ie the Control Table has been disabled. If the Active Control Table in CSA is backed out, it will not be reactivated by stopping and starting the NC-PASS job. <F2> reactivates a backed out table. Refer to <i>Stopped sessions recovery</i> on page 7.77. N/A which means Not Applicable and will be displayed if no Control Table has ever been loaded. For the Backup Control Table, this field will always be N/A .
ORIGINALLY LOADED	
JOBNAME	The name of the NC-PASS job that loaded the Control Table into CSA.
DATE	The date when the Control Table was loaded into CSA.
TIME	The time when the Control Table was loaded into CSA.
LAST MOVED	
JOBNAME	The name of the NC-PASS job that last moved (ie loaded or restored) the Control Table in CSA.

Function keys

Key	Function
F1	provides help information
F2	activates the Active Control Table in CSA. If the table has been backed out, as indicated in the STATUS field, it will be changed to ACTIVE by pressing this key.
F3	ends the current display and returns to the previous panel.
F5	removes the Backup Control Table from CSA, moves the Active Control Table to be the new Backup Control Table and loads the table specified in the MASTER RULE NAME field as the new Active Control Table. The STATUS of the Active Control Table is not changed by the load process.
F6	removes the current Active Control Table from CSA and replaces it with the Backup Control Table.
F9	provides the RULE SELECTION LIST from which the name of a Control Table can be selected. The selected name will be entered in the MASTER RULE NAME field.

System startup

The following diagram explains the control table load processing at system startup:



Building a reference table of other NC-PASS systems

Whenever an MHO link is established with another NC-PASS system, both systems exchange the following information:

- network id
- SSCP name
- VTAM node id.

In addition, whenever a control table is loaded, NC-PASS sends all arrays which contain references to the USERID, SLNETID and SLUSSCP fields in the same array to all NC-PASS systems with which it has a link. This information is used to determine which NC-PASS jobs require particular CSA update information.

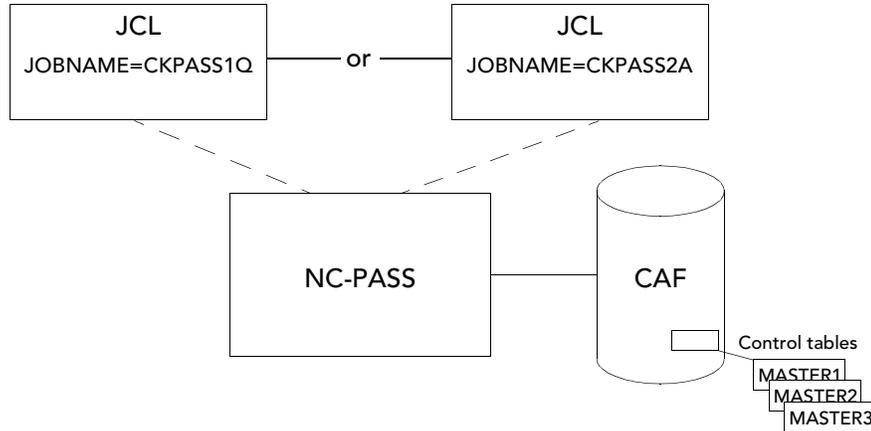
Each NC-PASS builds a reference table based on this information which will serve as a lookup table when a resource in one VTAM domain requests a session with a resource in another VTAM domain. The use of this data is described in *Protecting sensitive applications* on page 8.3.

Note: The information described above is also transmitted to other NC-PASS systems whenever the current load table changes, eg:

- a new table is loaded
- the ACT is backed out
- the ACT and BCT are switched.

Displaying information about SME Control Tables

The following diagram shows an example NC-PASS system. Both sets of JCL exist, but only one is run at a time.



Using the scenario above, the examples below and on the following pages show a sequence of events and the resulting changes to the details displayed about the SME Control Tables.

The event is described, followed by an example of the information displayed on the LOAD/RESTORE CONTROL TABLES panel after the specified event.

Note: A full description of all the fields on this panel is provided in the section entitled *The LOAD/RESTORE CONTROL TABLES panel* on page 7.65.

Date	Time	Event
12/12/1997	08:32	Job CKPASS1Q is run. The NC-PASS job starts and the administrator loads MASTER1 as the Active Control Table.

```

Date:12/12/1997          LOAD/RESTORE CONTROL TABLES          Userid:TSG0001
Time:08:35                Terminal:A01MS048

To load a Control table from NC-PASS complete the fields below and press <F5> :
JOBNAME                   => CKPASS1Q
MASTER RULE NAME => MASTER1
DEFAULT ACTION           => ALLOW   ALLOW, DENY or WARN
REFRESH                   => N Y/N Refresh the active Control table at job startup
CONFIRM                   => Y Y/N Display confirmation panel

Control tables loaded or moved by this NC-PASS:
TABLE NAME      JOBNAME  DATE       TIME
ACTIVE MASTER1  CKPASS1Q  12/12/1997 08:32
BACKUP None     N/A       N/A        N/A

Control tables in CSA:
TABLE NAME      STATUS   ORIGINALLY LOADED          LAST MOVED
JOBNAME DATE       TIME JOBNAME
ACTIVE MASTER1  ACTIVE  CKPASS1Q 12/12/1997 08:32 CKPASS1Q
BACKUP None     N/A     N/A       N/A   N/A

F1=Help  F2=Act  F3=End  F5=Load  F6=Rest  F9=Rules
    
```

Date	Time	Event
12/12/1997	10:00	The administrator loads MASTER2 as the Active Control Table.

```

Date:12/12/1997          LOAD/RESTORE CONTROL TABLES          Userid:TSG0001
Time:10:05              Terminal:A01MS048

To load a Control table from NC-PASS complete the fields below and press <F5> :
JOBNAME                => CKPASS1Q
MASTER RULE NAME      => MASTER2
DEFAULT ACTION        => ALLOW   ALLOW, DENY or WARN
REFRESH               => N Y/N Refresh the active Control table at job startup
CONFIRM               => Y Y/N Display confirmation panel

Control tables loaded or moved by this NC-PASS:
TABLE NAME      JOBNAME DATE      TIME
ACTIVE MASTER2  CKPASS1Q 12/12/1997 10:00
BACKUP MASTER1  CKPASS1Q 12/12/1997 10:00

Control tables in CSA:
TABLE NAME      STATUS  ORIGINALLY LOADED      LAST MOVED
JOBNAME DATE      TIME JOBNAME
ACTIVE MASTER2  ACTIVE  CKPASS1Q 12/12/1997 10:00 CKPASS1Q
BACKUP MASTER1  N/A     CKPASS1Q 12/12/1997 08:32 CKPASS1Q

F1=Help  F2=Act  F3=End  F5=Load  F6=Rest  F9=Rules

```

Date	Time	Event
12/12/1997	10:30	The NC-PASS job is shut down. Job CKPASS2A is run. The administrator has specified REFRESH=N, so the previous Control Table remains active.

```

Date:12/12/1997          LOAD/RESTORE CONTROL TABLES          Userid:TSG0001
Time:10:35              Terminal:A01MS048

To load a Control table from NC-PASS complete the fields below and press <F5> :
JOBNAME                => CKPASS2A
MASTER RULE NAME      =>           
DEFAULT ACTION        => ALLOW   ALLOW, DENY or WARN
REFRESH               => N Y/N Refresh the active Control table at job startup
CONFIRM               => Y Y/N Display confirmation panel

Control tables loaded or moved by this NC-PASS:
TABLE NAME      JOBNAME DATE      TIME
ACTIVE MASTER2  CKPASS1Q 12/12/1997 10:00
BACKUP MASTER1  CKPASS1Q 12/12/1997 10:00

Control tables in CSA:
TABLE NAME      STATUS  ORIGINALLY LOADED      LAST MOVED
JOBNAME DATE      TIME JOBNAME
ACTIVE MASTER2  ACTIVE  CKPASS1Q 12/12/1997 10:00 CKPASS1Q
BACKUP MASTER1  N/A     CKPASS1Q 12/12/1997 08:32 CKPASS1Q

F1=Help  F2=Act  F3=End  F5=Load  F6=Rest  F9=Rules

```

Date	Time	Event
12/12/1997	14:30	The administrator loads MASTER3 as the Active Control Table.

```

Date:12/12/1997          LOAD/RESTORE CONTROL TABLES          Userid:TSG0001
Time:10:45              Terminal:A01MS048

To load a Control table from NC-PASS complete the fields below and press <F5> :
JOBNAME                => CKPASS2A
MASTER RULE NAME      => MASTER3
DEFAULT ACTION        => ALLOW   ALLOW, DENY or WARN
REFRESH               => N Y/N Refresh the active Control table at job startup
CONFIRM               => Y Y/N Display confirmation panel

Control tables loaded or moved by this NC-PASS:
TABLE NAME      JOBNAME  DATE      TIME
ACTIVE MASTER3  CKPASS2A  12/12/1997 14:30
BACKUP MASTER2  CKPASS2A  12/12/1997 14:30

Control tables in CSA:
TABLE NAME      STATUS  ORIGINALLY LOADED          LAST MOVED
JOBNAME  DATE      TIME  JOBNAME
ACTIVE MASTER3  ACTIVE  CKPASS2A  12/12/1997 14:30  CKPASS2A
BACKUP MASTER2  N/A     CKPASS1Q  12/12/1997 10:00  CKPASS2A

F1=Help  F2=Act  F3=End  F5=Load  F6=Rest  F9=Rules

```

Setting global options

You can set a number of global options affecting the use of the SME exit. These options are provided on the GLOBAL OPTIONS panel (7.5).

```
Date:12/12/1997          GLOBAL OPTIONS          Userid:TSG0001
Time:09:00              Terminal:A01MS242

To update the global options affecting the use of the SME exit, type enable
instructions (Y or N) below and press <ENTER>:

  E GLOBAL OPTION                      CSA STATUS

  Y Enable SME processing
  Y Continue to process the Active Control Table
  N Stop sessions if denied or no Control Table
  N Write trace data of initiation requests to the NCILOG
  N Receive ALLOW audit messages
  Y Permit remote back out of Active Control Table

New time out period for CSA entries => 90

Global options last updated by => PASS20

Specify whether changes made to data on this panel require confirmation:
Display confirmation panel => Y (Y or N)

F3=End  F12=Can
```

Input fields

Field	Description
Enable SME processing	Set this option to Y to enable SME processing. Set to N to disable SME processing and ALLOW ALL session requests.
Continue to process the Active Control Table	Set this option to Y to continue to process the Active Control Table when NC-PASS does not have an active cross memory link with the SME. If this option is set to N and NC-PASS VSSE is stopped, all sessions will be denied. The SME is aware that NC-PASS is active when the XMS link is active. Refer to <i>Chapter 1 - Communicating with other systems</i> (Volume 2) for further details.
Stop sessions if denied or no Control Table	Set this option to Y to stop sessions when a DENY action is processed or when no control table is loaded. N means do not stop sessions under any circumstances. WARNING: It is recommended that during testing this option is set to N. If you want to set it to Y ensure Control Table testing has been completed.
Write trace data of initiation requests to the NCILOG	Set this option to Y to send a trace of all session initiation requests to the NCI log.

Field	Description
Receive ALLOW audit messages	Set to Y to log audit messages when an ALLOW action is processed. Note: If the ALLOW switch is set to Y, every session initiation request will result in audit data being sent cross memory to NC-PASS. If the ALLOW switch is set to N, audit data will be sent only for those session initiation requests that result in action of DENY or WARN.
Permit remote back out of Active Control Table	Set to Y to indicate that the SME processing may be disabled (referred to in the product as Backed out), by submitting a batch job supplied by PassGo Technologies Ltd. The purpose of backing out the SME processing is to permit initiation of sessions following loading of a Control Table that has had the inadvertent effect of forbidding all session initiation requests. Refer to <i>Stopped sessions recovery</i> on page 7.77 for details. It is recommended that this option is set to Y during familiarization with the product and prior to loading a new Active Control Table.
New time out period for CSA entries	Enter the number of seconds after which unwanted CSA userid entries will be deleted. Refer to <i>Userid processing</i> on page 7.80.
Display confirmation panel	Enter Y to force the display of a confirmation of changes panel.

Display fields

Field	Description
CSA status	Shows the true values of the Global Options stored in CSA. If they differ from the values displayed in the enabled/disabled column on the left of the panel then this indicates that another NC-PASS system has changed them. The name of the last system to update the Global Options is displayed in the Global options last updated by field.
Global options last updated by	Displays the name of the NC-PASS job that was used to last update the global options.

Function keys

Key	Function
F1	displays help information.
F3	saves the changes made and returns to the previous screen.
F12	Cancels any changes and returns to the previous screen.
WARNING: Changes applied by pressing <Enter> are not cancelled by this key.	

Implications of global options settings

There are three stages in the loading of the NC-PASS VSSE components as described below:

1. **Install and activate the SME.**

At this stage the default processing for all sessions is ALLOW.

2. **Start the NC-PASS job.**

Starting the NC-PASS job also loads the global options.

If this is the first time NC-PASS has been loaded no Active Control Table will be present.

When restarting NC-PASS, the global options are loaded with the values set when these options were last updated.

The following table shows the effect (before a control table is loaded) of combined global option and system settings which would cause all sessions to be stopped:

GLOBAL OPTIONS panel			CROSS SYSTEM COMMUNICATIONS - HOST panel	
If you set CONTINUE to...	and STOP to...	and ENABLE to...	and set XMS ENABLE to...	all sessions will be...
Y/N	Y	Y	Y	DENIED
Y	Y	Y	N	DENIED

WARNING: If you end/lose your session with VSSE with the settings shown in the table above and with no control table loaded, all sessions, including subsequent attempts to connect to VSSE, will be denied (code 080A). See the section entitled *Stopped sessions recovery* on page 7.77.

3. **Create and load a control table.**

Sessions will be processed according to control table rules.

Setting control operator functions

You can allow the operator to perform certain functions with a MODIFY command, as described below:

LIST	Set to Y to allow the operator to display the names of the ACT, the BCT and the global options that have been set.
LOAD	Set to Y to allow the operator to load control tables.
RESTORE	Set to Y to allow the operator to restore the ACT from the BCT.
SET	Set to Y to allow the operator to set the following global options: CONT / NOCONT ENABLE / DISABLE STOP / NOSTOP TRACE / NOTRACE ALLOW / NOALLOW

These functions are provided on the CONTROL OPERATOR FUNCTIONS panel (7.6).

The operator interface to the SME is provided by the SMEOPER routine. To use this interface enter the following command at the operator console:

```
F jobname, EXEC SMEOPER parameters
```

where *parameters* are:

```
LIST  
LOAD control-table-name  
RESTORE  
SET <STOPINOSTOP> <CONTINOCNT> <TRACEINOTRACE> <ENABLEIDISABLE>  
<ALLOWINOALLOW>
```

Note: Some or all of the above may have been disabled by the administrator.

Stopped sessions recovery

If all your sessions are being stopped, it may be either for the reasons described in the section entitled *Implications of global options settings* on page 7.75 or because of the processing logic of the rule you have loaded as the ACT.

If you have defined the system such that all sessions are being stopped, check the following task list table in ascending sequence until you find a suitable recovery option:

	If...	then...
1.	you have a VSSE session	change STOP to NOSTOP.
2.	operator modify commands are enabled	change STOP to NOSTOP.
3.	you have a TSO session	Back out the SME by submitting the JCL held in *PREFIX*.CNTL(DISABLE) The back out program must be stored in an APF authorized load library.
4.	you have previously loaded *PREFIX*.CNTL(SME) (the backout JCL) to SYS1.PROCLIB as member <i>procname</i>	enter <i>S procname</i> at the operator console to back out the SME.
5.	you are running VTAM 3.4 or higher	<ul style="list-style-type: none">• vary the SME inactive by entering the following command: F VTAM,EXIT,ID=ISTEXCAA,OPTION=INACT• change STOP to NOSTOP.
6.	you are running VTAM3.3	<ul style="list-style-type: none">• rename processing module to dummy module• change STOP to NOSTOP.
7.	you are running VTAM3.3 (no TSO session)	<ul style="list-style-type: none">• IPL without specifying the new MLPA member.

SME flag settings

Two flags are maintained in CSA to determine whether the SME will use the loaded control table to check session initiation requests. These are the **SME Enabled** flag and the **SME Backed out** flag. Before the specified control table is enabled these two flags must be set as follows:

SME Enabled = Y This flag is set according to the value specified in the **Enable SME processing** field in the GLOBAL OPTIONS panel (7.5).

SME Backed out = N This flag is set to Y when options 3 or 4 in the above table have been actioned. It is reset when a new control table is loaded (<F2>) from the LOAD/RESTORE CONTROL TABLES panel (7.3).

Reactivating a backed-out table

After you have found and corrected the problem, press <F2> on the LOAD/RESTORE CONTROL TABLES panel to reactivate a backed-out table. Starting and stopping the NC-PASS job will **not** reactivate the table.

Communications

This section describes the communication interfaces between NC-PASS and the SME. The distributed copy of NC-PASS 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) task's default SSCT name. The SME uses XMS1 to communicate with NC-PASS regarding audit messages and actioning of the ACQUIRE keyword.
- 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 ISTECAA type VTAM exit and want to link-edit it behind the PassGo Technologies exit. If used, this SSCT will contain exit function request information specific to your exit.

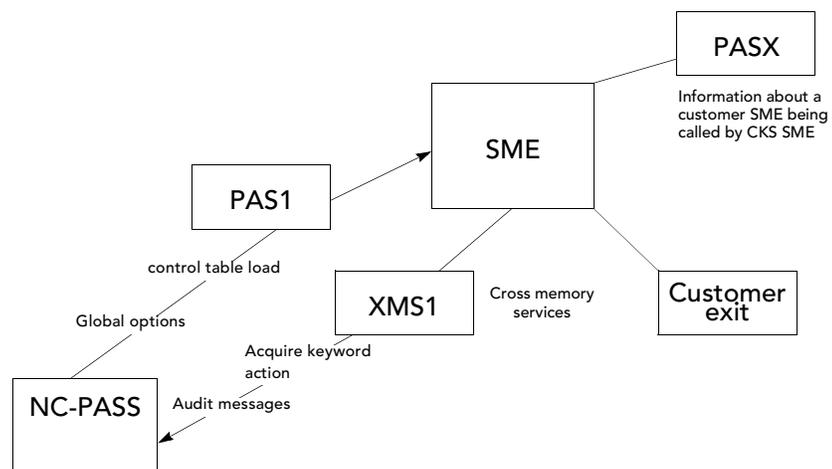
The cross memory services function is administered from option 1 of the CROSS SYSTEM COMMUNICATIONS panel (4). It is essential that the XMS task's SSCT name (default **XMS1**) is used in this panel in order for NC-PASS to receive audit messages and ACQUIRE data from the SME.

The SSCT entry PAS1, which is generated by NC-PASS when a control table is loaded, contains an identifier. The SME is able to determine the correct PAS1 SSCT by this identifier. It is possible that another application has created an SSCT entry using the name PAS1; in this case the absence of the identifier ensures that this entry will not be used.

During SSCT generation, if NC-PASS finds a PAS1 entry already exists that does not contain the identifier, it will create an additional PAS1 entry, with the identifier, for its own exclusive use.

More than one SSCTs called PAS1 are able to coexist without causing errors. However, if any other product on your machine uses SSCTs with one of the other names, results from NC-PASS VSSE (and the other products) are unpredictable. If you want to change any of these default names, customization fixes AUC0101 (PAS1), AUC0102 (XMS1) and AUC0103 (PASX) allow the default SSCT names to be changed.

The diagram below shows the links from and to NC-PASS and the SME.



Communication from NC-PASS to the SME

Communication from NC-PASS to the SME is via Extended/Common Services Area (E/CSA). Every time the SME is driven by VTAM it checks various flags held in CSA which are set via NC-PASS. These flags correspond to a particular processing function.

Communication from the operator's console is achieved via MODIFY commands issued to the NC-PASS address space.

Communication from the SME to NC-PASS

Communication from the SME to NC-PASS is via NCI's Cross Memory Services (XMS).

The cross memory services function is administered from option 1 of the CROSS SYSTEM COMMUNICATIONS panel (4); it may be stopped, started or restarted from this panel. Refer to *Chapter 1 - Communicating with other systems* (Volume 2).

(The cross memory services component also enables any non NC-PASS job - e.g. programs running under TSO, batch jobs, CICS - running in the same MVS system as NC-PASS to communicate with NC-PASS. Refer to *Chapter 2 - Transaction Level Interface (TLI)* (Volume 2) for further details.)

Userid processing

The field USERID offers a means of protecting applications by ensuring that access has first been authorized by NC-PASS. This applies to both single and cross-domain session requests.

Note: The USERID field is related to the %NCPASS function in previous releases.

When a userid is validated by NC-PASS, if the loaded rule contains the USERID field, data relating to that user is automatically stored in CSA before the SME is driven. The following data is stored for each CSA entry:

- the userid
- terminal id
- VTAM id of the terminal
- Network id of the terminal.

This data will be used by the SME when it encounters the USERID field in the currently loaded rule. The USERID field can be used to ensure access to a resource is protected by the requirement for an authenticated userid; since only NC-PASS can update the CSA with this userid data, it follows that access to such a resource will only be allowed for given userids and those userids must have been authenticated by NC-PASS.

Note: The ACQUIRE keyword can be used to allow NC-PASS to acquire a terminal to request authentication information - refer to *Using ACQUIRE to protect sensitive applications from dial-ins* on page 8.10.

The CSA entry associated with a userid will be flagged as re-usable under the following conditions:

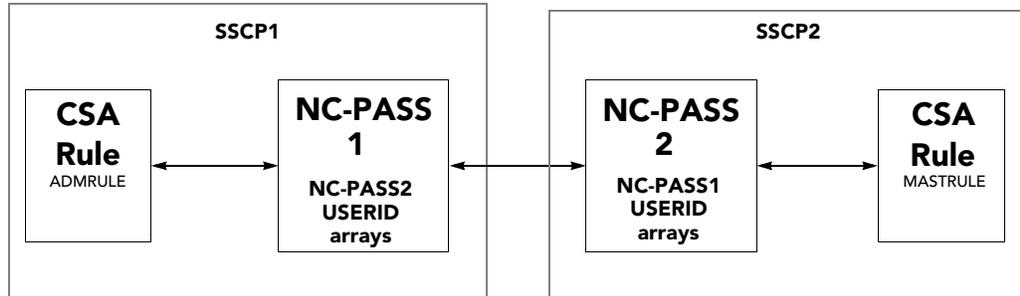
- a match has been found during control table processing
- the CSA timeout period specified in the GLOBAL OPTIONS panel (7.5) has been exceeded.

Specifying the USERID field in rules

When a new rule is loaded by NC-PASS, the rule will be examined for any USERID fields that may be present. Any arrays which contain occurrences of the following three fields (including alias names if specified), in the same array, will be extracted and sent to all other NC-PASS jobs that have active MHO links with the host:

USERID, SLNETID and SLUSSCP

On receipt, each NC-PASS will translate this information back into each of the USERID arrays it represents and load it into a lookup table. If there are a number of NC-PASS jobs in a large network it will be likely that each NC-PASS will build a number of lookup tables representing each of the other NC-PASS jobs with USERID rule data.



Lookup tables are used by NC-PASS to control cross-domain session requests and are referenced under the following conditions:

- VSSE is active
- NC-PASS is about to connect a user to an application.

When the SME processes a control table containing the field USERID, it will determine whether there is a userid entry in CSA (ie a user that has already been authenticated by NC-PASS) which matches with the userid specified in the rule, defined against the USERID field within the rule.

For example if an array in the loaded rule contains, amongst others, the entry:

```
... USERID ...  
... EQ ...  
... ACC* ...
```

then the CSA will be searched for any userid entry where the userid starts with ACC.

If an entry is found, the userid check is satisfied and the space occupied by the userid entry is marked as reusable.

The purpose of lookup tables is for NC-PASS to decide whether other NC-PASS jobs need to be sent a CSA update request in anticipation of an impending CLSDST PASS. Any look up table that has a matching entry for the application requested will result in a CSA update request being sent to that NC-PASS.

If a control table is backed out, or a new control table is loaded, NC-PASS will send the new information to all other NC-PASS jobs with which it has a link.

Note: This functionality does provide restrictions and will only function correctly if the rule that represents the active control table has been set up correctly. Refer to *Guidelines for using the USERID field in rules* on page 7.82.

Refer to *Chapter 8 - Using VSSE to achieve access control objectives* for examples of the use of the USERID field.

Guidelines for using the USERID field in rules

The following points represent the guidelines that should be used when constructing a rule that is to have USERID checking:

1. Arrays that do not specify USERID, SLUSSCP (or alias TERMVTAM) and SLNETID (or alias TERMNET) **in the same array**, will NOT be propagated to other NC-PASS systems.
2. The following example shows how the system B administrator could protect a single sensitive application like a payroll application using the field USERID:

ARRAY1		RULE PROLL		
TERMINAL	TERMVTAM	TERMNET	APPL	USERID
EQ	EQ	EQ	EQ	EQ
A01*	VTAM01	NET01	PAYROLL	ACC* ADMIN
TRUE: ALLOW		FALSE: NEXT		

ARRAY2	
APPL	
EQ	
A01*	
TRUE: DENY	FALSE ALLOW

Array 1 would be transmitted to System A as described on page 7.81. System A would only issue a CSA update request to System B if a logon request resulted in a match with all the criteria specified in array 1, so reducing the number of transactions sent over MHO. Such a request would be, for example, a request from a user defined to NC-PASS with connect data specifying the Payroll application.

3. As illustrated above, any restrictions to terminals, VTAMS and NETWORK that are allowed access to the application should also be defined in the same array. Only then will the array be propagated to other NC-PASS systems.
4. the only allowable comparator is EQ; for the purpose of look-up tables, using NE will be treated as if it were EQ.

Converting an NC-PASS 1.4 authorization control table to V2.0

You can convert an authorization control table created in v1.4 of NC-PASS to an NC-PASS v2.0 rule by using the AUTHORIZATION CONTROL TABLE CONVERSION panel (7.9).

The following information is required:

- the dataset and member name of the authorization control table to be converted
- the name of the new rule to be created.

Statement conversion

Command and control statements are converted as detailed below.

Command statement conversion

The format of a command in an NC-PASS 1.4 authorization table is:

S=sluname.slunet.sluvtam,P=pluname.plunet.pluvtam,O=originator

During conversion, this data will be interpreted as follows:

NC-PASS 1.4 command entry	NC-PASS 2.0 generated field name
SLUNAME	SLNETLU
SLUNET	SLNETID
SLUVTAM	SLUSSCP
PLUNAME	PLNETLU
PLUNET	PLNETID
PLUVTAM	PLUSSCP

Originator command entries are converted to the following fields and values. F indicates a Flag field.

NC-PASS 1.4 originator command entry	NC-PASS 2.0 field	NC-PASS 2.0 value
%NCPASS	USERID	*
%UNKNOWN	EXRRS11 (F)	EX1OLU
%SLU	EXRRS11 (F)	EX1SLU
%VTAM	EXRRS11 (F)	EX1AUTO
%PLU	EXRRS11 (F)	EX1PLU

Note: Command entry lines that have only one field value difference for the same field, from the previous line, will be combined into one array.

Comment lines

Comment lines are ignored and are not translated.

Control statement conversion

The following table provides a list of NC-PASS 1.4 control statements with their equivalent function in version 2.0.

NC-PASS 1.4 control statement	NC-PASS 2.0
ID <i>nnnn</i>	not required.
CODE <i>xxx</i>	not required.
WTO/NOWTO	No direct translation. The SME always sends audit data to NC-PASS for DENY actions. If required, these audit messages can be selectively suppressed using SEEXIT17. Refer to the section entitled SME action auditing in the chapter entitled <i>Message processing</i> .
STOP/NOSTOP	Translates to global option STOP/NOSTOP.
TRACE/NOTRACE	Translates to global option TRACE/NOTRACE.
WTOR/NOWTOR	No direct translation. You can allow the operator to perform certain functions with a MODIFY command. Permissions are set on the CONTROL OPERATOR FUNCTIONS panel (7.6)

WARNING: V1.4 Control statements that translate to V2.0 global options will not be actioned automatically. The translated global options will be displayed at the bottom of the AUTHORIZATION CONTROL TABLE CONVERSION panel (7.9) after a successful conversion. If required, the administrator will have to manually enter these options via the SET GLOBAL OPTIONS panel (7.5).

The following table provides a list of NC-PASS 1.4 WTOR statements with the equivalent function in version 2.0.

NC-PASS 1.4 WTOR statement	NC-PASS 2.0
REFRESH	Loading and restoring of control tables can be actioned: by the administrator using the LOAD/RESTORE CONTROL TABLES panel (7.3). See the section entitled <i>The LOAD/RESTORE CONTROL TABLES panel</i> on page 7.65. if permitted, by the operator via the SMEOPER routine. See the section entitled <i>Setting control operator functions</i> on page 7.76.
LIST	You can view a control table using the Outline command against the appropriate rule on the RULE MAINTENANCE panel (7.1). See the subsection entitled <i>Viewing the control table outline</i> on page 7.31. You can produce a hardcopy print of a rule using the rule print facility. See the section entitled.

Conversion example

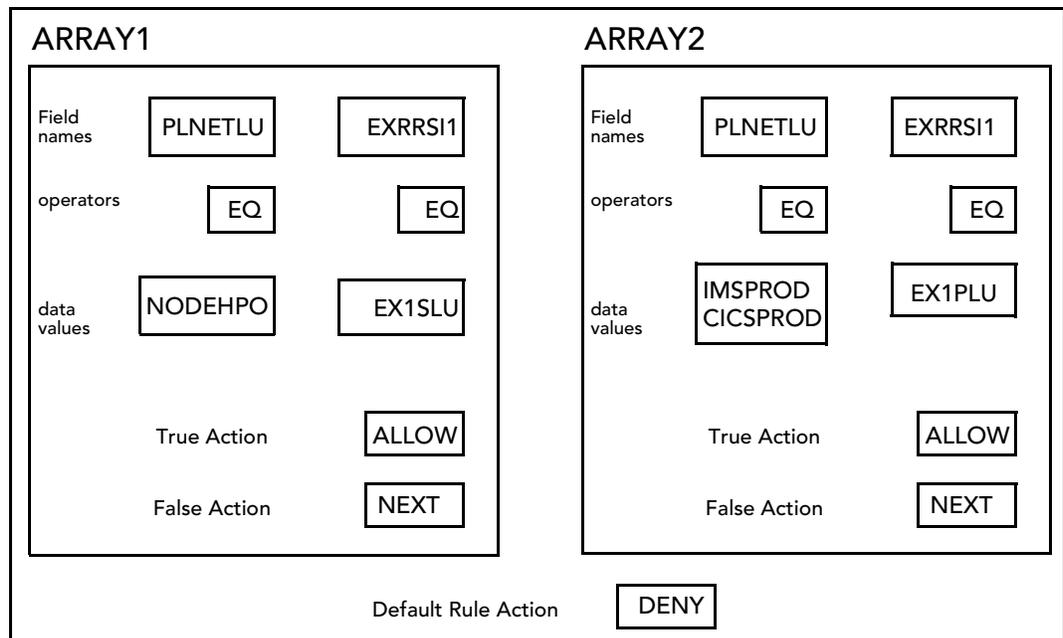
The following example shows an authorization control table from NC-PASS 1.4 followed by the rule to which it would be converted by the conversion program. For this example, the new rule is given the name R123.

Authorization control table

```
*****
* NC-PASS 1.4 Authorization Control Table *
*****
*
/CODE ZH123QQQ
/WTO
/NOSTOP
/TRACE
+S=*. * . *, P=NODEHPO. * . *, O=%SLU
+S=*. * . *, P=IMSPROD. * . *, O=%PLU
+S=*. * . *, P=CICSPROD. * . *, O=%PLU
*
*****
```

Converted rule

The converted rule can be diagrammatically represented as follows:



The following lines have **not** been converted:

- /CODE Not required for NC-PASS version 2.0.
- /WTO Refer to the *Chapter 9 - Auditing* for details of how to route and suppress DENY audit messages.
- /NOSTOP Translates to the global option STOP=NO. The NC-PASS conversion process does not apply this automatically. This option can be set via the SET GLOBAL OPTIONS panel (7.5).
- TRACE Translates to the global option TRACE=YES. The NC-PASS conversion process does not apply this automatically. This option can be set via the SET GLOBAL OPTIONS panel (7.5).
- * comment lines are not converted.

The AUTHORIZATION CONTROL TABLE CONVERSION panel

To convert an NC-PASS 1.4 authorization table to a new NC-PASS 2.0 rule, use the AUTHORIZATION CONTROL TABLE CONVERSION panel (7.9). Enter the required data and press <F5> to run the conversion. An example of this panel, after the conversion program has been run, is shown below:

```

Date:12/12/1997      AUTHORIZATION CONTROL TABLE CONVERSION      Userid:TSG0001
Time:09:00                                           Terminal:T31CNS01

To convert an NC-PASS 1.4 authorization control table to a new NC-PASS 2.0
rule, complete the fields below and press <F5> :

Enter the dataset and member name that require conversion:
  Dataset name  => CKDABC1.CNTL(CT123)

Enter the rule name that will be generated by the conversion routine:
  Rule name    => RULE123

Enter Y for an authorization control table and rule print after conversion:
  Print request => N Y/N

Any control statements that translate to global option updates that are
found during the conversion process will be displayed below. These updates
will not be actioned automatically and are displayed for reference only.
Global option updates can be applied by using the SET GLOBAL OPTIONS panel.

Global options found => *** STOP=Y TRACE=N ***

CKSE3379-9 Control table conversion from V1.4 to V2.0 completed
F3=End F5=Conv F12=Can
  
```

Input fields

Field	Description
Dataset name	enter the name of the authorization control table to be converted in the format dataset(member).
Rule name	enter the name of the rule to be created. (If you specify the name of an existing rule, you will be asked whether you want to overwrite that rule).
Print request	Enter Y to print a copy of the authorization array and the new rule after conversion. (After conversion, you will be asked to provide details of the printer to be used to print the report).

Display fields

Field	Description
Global option updates found	Control statements in the V1.4 authorization array are translated as follows: /STOP STOP=Y /NOSTOP STOP=N /TRACE TRACE=Y /NOTRACE TRACE=N Applicable options will be displayed as appropriate.

Function keys

Key	Function
F3	ends the current display and returns to the previous panel.
F5	runs the conversion program.
F12	cancels any input data and returns to the previous panel.

Communication between different versions of NC-PASS

NC-PASS v2.0 and NC-PASS v1.4 systems linked by MHO can exchange control table data and tell remote NC-PASS systems of either version to make CSA updates. This is required for %NCPASS processing.

This data is held in a different format depending on the version of NC-PASS, therefore NC-PASS v2.0 systems translate data to/from v1.4 format as required.

Exchanging control table data

This section describes how information is exchanged:

- between two NC-PASS v2.0 systems
- between two NC-PASS v1.4 systems
- from an NC-PASS v1.4 system to an NC-PASS v2.0 system
- from an NC-PASS v2.0 system to an NC-PASS v1.4 system.

NC-PASS v2.0 systems

Whenever a control table is loaded in an NC-PASS v2.0 system, NC-PASS sends all arrays which contain references to the USERID, SLNETID and SLUSSCP fields in the same array to all NC-PASS systems with which it has a link.

Each NC-PASS builds a reference table based on this information which will serve as a lookup table when a resource in one VTAM domain requests a session with a resource in another VTAM domain. The use of this data is described in *Protecting sensitive applications* on page 8.3.

Note: The information described above is also transmitted to other NC-PASS systems whenever the current load table changes, eg:

- a new table is loaded
- the ACT is backed out
- the ACT and BCT are switched.

NC-PASS v1.4 systems

Whenever an authorization control table is loaded in an NC-PASS v1.4 system, NC-PASS sends all entries which have O=%NCPASS defined, to all NC-PASS systems with which it has a link.

Each NC-PASS builds a reference table based on this information which will serve as a lookup table when a resource in one VTAM domain requests a session with a resource in another VTAM domain.

Note: The information described above is also transmitted to other NC-PASS systems whenever the current authorization table changes.

Mixed environments

When an NC-PASS v2.0 system sends information to, or receives information from, an NC-PASS v1.4 system, the NC-PASS v2.0 system recognizes that it is communicating with- a downlevel system and translates the information into the required format.

The format of an entry in an NC-PASS v1.4 authorization table is:

S=sluname.slunet.sluvtam,P=pluname.plunet.pluvtam,O=originator

During translation, this data will be interpreted as follows:

NC-PASS v1.4 command entry	NC-PASS v2.0 generated field name
SLUNAME	SLNETLU
SLUNET	SLNETID
SLUVTAM	SLUSSCP
PLUNAME	PLNETLU
PLUNET	PLNETID
PLUVTAM	PLUSSCP

NC-PASS v1.4 to v2.0

'O=%NCPASS' originator command entries sent from a v1.4 system to a v2.0 system are translated to 'USERID=*'.

NC-PASS v2.0 to v1.4

'USERID=userid' fields to be sent from a v2.0 system to a v1.4 system are translated by the v2.0 system and sent as 'O=%NCPASS'.

This page intentionally left blank

Chapter 8 - Using VSSE to achieve access control objectives

Identifying access control requirements	8.2
Protecting sensitive applications	8.3
Example scenario	8.4
Example rules	8.4
Protecting the sensitive application from LOGAPPL'd terminals	8.7
Using ACQUIRE to protect sensitive applications from dial-ins	8.10
ACQUIRE function features	8.21
Checking access to a specific application based on terminal id	8.22
Example	8.23
Denying cross domain access to a specific application	8.25
Example	8.26
Denying access to a specific application from dial-in lines	8.28
Example	8.28
Checking access to all applications based on SSCP	8.30
Example	8.31
Preventing access to an application at specific times	8.34
Example	8.35
General considerations when building a rule	8.38
System-generated session requests	8.38
Session 'races'	8.38

Identifying access control requirements

NC-PASS VSSE allows control over which sessions, between two logical units, VTAM will allow or deny. Session types include terminal to application, application to printer, peer to peer, etc.

Its primary uses are in controlling network access/routing, access from dial-in lines and access from specific terminals.

This section provides a number of examples of access control requirements.

Note: For simplicity, each requirement is described in isolation; in reality, a rule will combine many access control checks.

The following access control objectives are discussed:

- protecting sensitive applications from dial-in lines
- checking access to a specific application based on userid
- checking access to a specific application based on terminal id
- denying cross domain access to a specific application
- denying access to a specific application from dial-in lines
- checking access to all applications based on SSCP name
- preventing access to an application at specific times.

Each example discusses:

- the access control objective
- the field names that will be used to build this part of the rule
- an example scenario.

WARNING: The examples shown on the following pages are not intended to be working samples and are provided purely for illustration purposes. When creating rules, you must use data to suit your own operating requirements.

Protecting sensitive applications

Using NC-PASS and the SME (Session Management Exit), applications can be categorized as sensitive or non-sensitive. In the case of non-sensitive applications, the logon request can be allowed to continue with no further validation. Sensitive applications are those which require further validation. In this context, a sensitive application is one which is protected by the requirement for a userid. The userid is stored in CSA which can only be amended by NC-PASS; this will only occur following successful validation.

USSTAB, as provided as a default by IBM, has no facility to capture a userid, therefore sensitive applications that require userid information to be present in CSA cannot be accessed directly from dial-in terminals. In order to perform the required level of userid validation such terminals must be ACQUIRED by NC-PASS via the SME.

To achieve this protection, the following features are available when defining rules:

- USERID field
- ACQUIRE keyword.

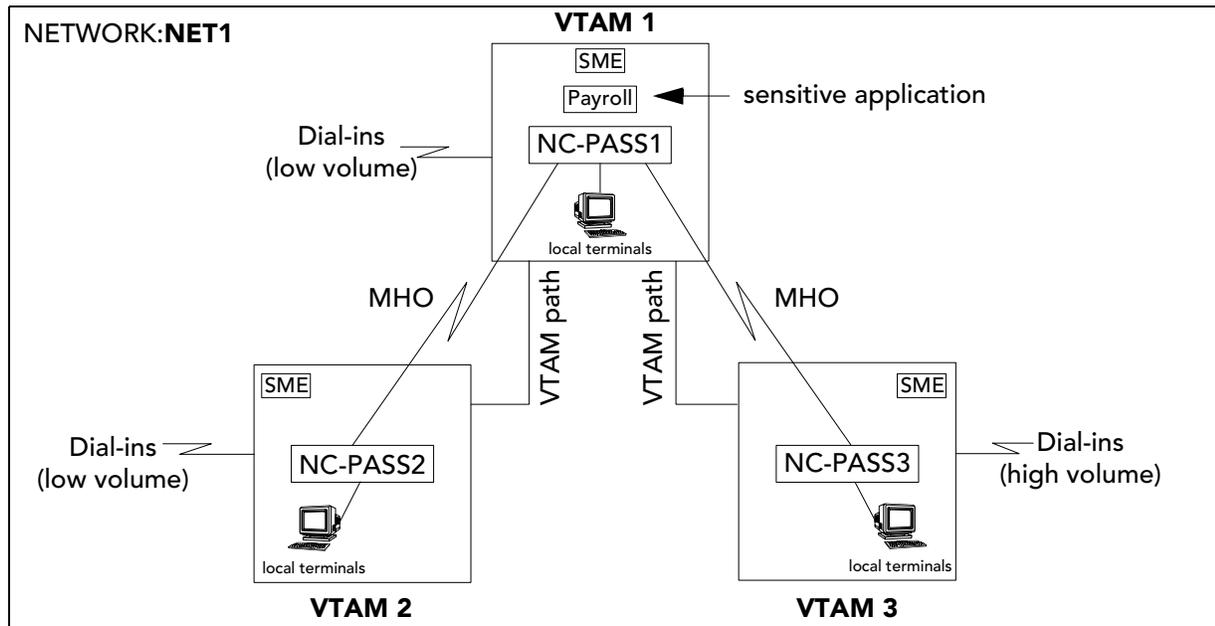
If the application and terminal are not in the same VTAM domain then the session request is cross-domain. Cross-domain session requests as well as single-domain session requests can be protected using the ACQUIRE keyword.

ACQUIRE processing supports cross domain session requests in the same way as NC-PASS 1.4 and will also provide backwards compatibility to support NC-PASS 1.4 TLI calls (function code 6) from external session managers.

The following sections explain how the USERID field and ACQUIRE keyword are used to protect a sensitive application. An example rule and scenario are used to illustrate the various processing features.

Example scenario

The following example shows three linked NC-PASS systems running in three separate VTAM domains, each with an active SME. NC-PASS1 is linked via MHO to NC-PASS2 and NC-PASS3. All local terminals are LOGAPPL'd to NC-PASS. The examples show how the USERID field and the ACQUIRE action can be used to protect a sensitive application, both from session requests from LOGAPPL'd terminals and from unauthorized access via dial-in terminals.



Example rules

The rules RULE1, RULE2 and RULE3 (shown on the following page) are provided as an example of how to protect the sensitive application, PAYROLL, in VTAM1. RULE1, RULE2 and RULE3 are loaded in NC-PASS1, NC-PASS2 and NC-PASS3 respectively.

Rule purpose

The normal route to the sensitive application PAYROLL is from local terminals defined to the local VTAM. However there is also the risk of unauthorized access from dial-in terminals to all three VTAMs, although the volume of dial-in traffic is the greatest in VTAM3.

The rules have the following combined function:

- to ensure that access to the PAYROLL application will only be granted to userids PAY0001, PAY0002 and PAY0003, from any NC-PASS, after they have been successfully authenticated by NC-PASS
- to protect unauthorized access from dial-in lines by acquiring dial-in terminals. This forces users to provide authentication information and so be successfully authenticated by NC-PASS before being allowed to access the PAYROLL application
- to balance the task of acquiring terminals by allowing NC-PASS1 to acquire dial-in terminals from VTAM1 or VTAM2, but to ensure that dial-in terminals to VTAM3 are acquired by NC-PASS3; this reduces the load on NC-PASS1.

Fields used in the example rules

The following field names are used in the rules:

EVSSCP	contains the VTAM id where the SME is operating.
EXRRS11	contains details of the type of session request.
PLALLUN	contains the alias name of the PLU (application).
PLNETLU	contains the name of the Primary Logical Unit (PLU) as defined within the network. For example, if a terminal requests a session with an application, this field will contain the VTAM nodename of the requested application.
SLNETID	contains the network id of the network from where the Secondary Logical Unit (SLU) session was generated.
SLUSSCP	contains the VTAM id (SSCPNAME) of the VTAM that contains the Secondary Logical Unit (SLU) as defined within the network.
USERID	contains the userid specified to NC-PASS.

Note: The rules are not intended to be working samples and are provided for illustration purposes only.

RULE1 (VTAM1)

```

ARRAY:R1APPL
PLNETLU
EQ
PAYROLL

TRUE:NEXT  FALSE:ALLOW

ARRAY:R1USER
SLNETID  SLUSSCP  PLNETLU  USERID
EQ        EQ        EQ        EQ
NET1      VTAM1    PAYROLL  PAY*
           VTAM2
           VTAM3

TRUE:ALLOW  FALSE:NEXT

ARRAY:TERMTAM
SLUSSCP
EQ
VTAM3

TRUE:DENY  FALSE:NEXT

ARRAY:R1CLSDST
EXRRS1
EQ
EX1OLU  V

TRUE:DENY  FALSE:ACQUIRE
    
```

RULE2 (VTAM2)

```

ARRAY:R2APPL
PLALLUN  PLNETLU
NE        NE
PAYROLL  PAYROLL

TRUE:ALLOW  FALSE:NEXT

ARRAY:R2USER
SLNETID  SLUSSCP  PLNETLU  USERID
EQ        EQ        EQ        EQ
NET1      VTAM2    PAYROLL  PAY*

TRUE:ALLOW  FALSE:DENY
    
```

RULE3 (VTAM3)

```

ARRAY:R3APPL
PLALLUN  PLNETLU
NE        NE
PAYROLL  PAYROLL

TRUE:ALLOW  FALSE:NEXT

ARRAY:R3USER
USERID
EQ
PAY*

TRUE:ALLOW  FALSE:NEXT

ARRAY:R3CLSDST
EXRRS1
EQ
EX1OLU  V

TRUE:DENY  FALSE:ACQUIRE
    
```

Exchange of information

After the three rules are loaded into CSA in their respective VTAMs, the NC-PASSes will exchange rule information relating to their loaded rules. Arrays containing the fields **USERID**, **SLNETID** and **SLUSSCP**, in the same array, will be propagated to other NC-PASSes **with which the NC-PASS has an MHO link**. In the above example, a copy of the following arrays will be sent:

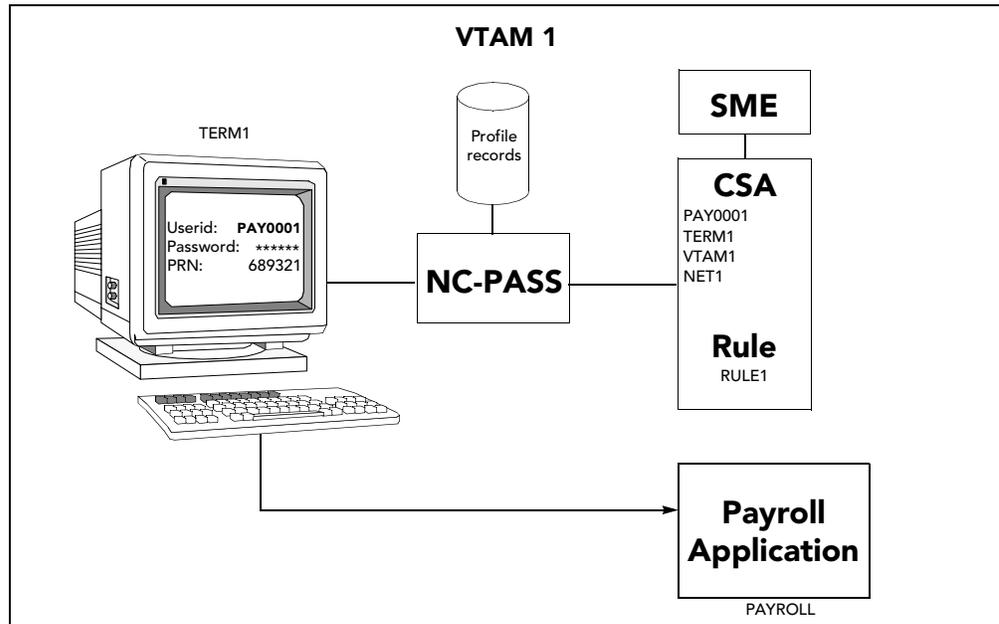
Array	From	To
R1USER	NC-PASS1	NC-PASS2 NC-PASS3
R2USER	NC-PASS2	NC-PASS1

Protecting the sensitive application from LOGAPPL'd terminals

The following examples assume that the rules RULE1, RULE2 and RULE3 are loaded in their respective CSAs as described in the section entitled *Example rules* on page 8.4.

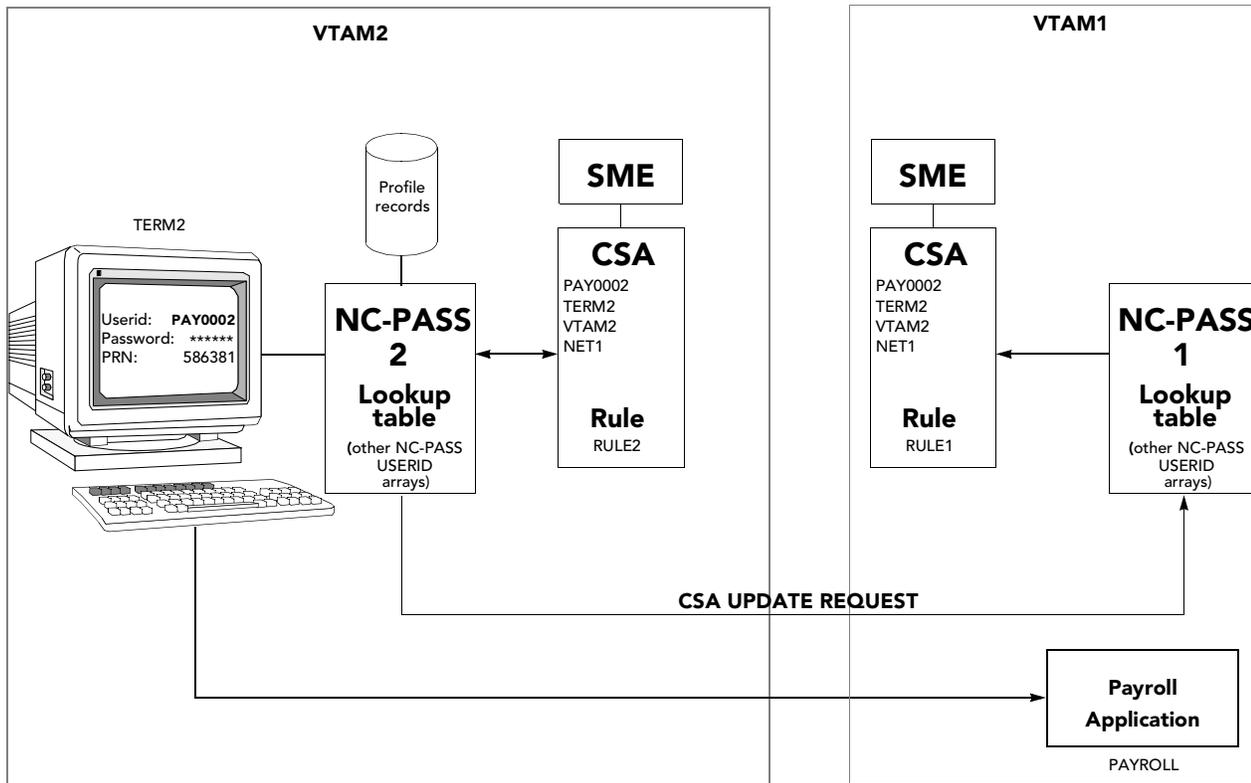
In the examples below, usersid PAY0001, PAY0002 and PAY0003 are defined to NC-PASS 1, 2 and 3 respectively. All three users are RACF password protected. The connect definition for each userid specifies the PAYROLL application.

Example 1 - terminal and application in the same VTAM



1. When user PAY0001 logs on, NC-PASS prompts for password and token details. If the user provides the correct password details, NC-PASS writes an entry for this userid to CSA and issues a CONNECT request to connect the terminal (from which the session request originated) to the PAYROLL application.
2. Since the terminal and application are in the same VTAM domain (VTAM1), only the SME in VTAM1 is driven and rule RULE1 is processed.
3. The first array in RULE1, R1APPL, checks whether the requested application (PLNETLU) is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.
4. The True action is followed which is to process the next array, R1USER, which checks whether the given userid is authorized to access PAYROLL.
5. CSA is checked for an entry that matches the values allowed by the rule (USERID EQ PAY*). In this example, user PAY0001 has been successfully authenticated by NC-PASS and therefore an entry is found in CSA which matches the rule. The TRUE action is processed and access to the application is ALLOWed.

Example 2 - terminal and application in different VTAMs



1. When user PAY0002 logs on, NC-PASS2 prompts for password and token details. If the user provides the correct password details, NC-PASS2 writes an entry for this userid to its CSA.
2. As described in *Exchange of information* on page 8.6, NC-PASS2 has been sent a copy of the R1USER array from RULE1 which has been stored in its lookup table. NC-PASS2 checks this lookup table; the information provided for this session request matches the criteria specified in the R1USER array in RULE1. (Terminal network is NET1, terminal VTAM id is VTAM2, application is PAYROLL and USERID starts with PAY.) It therefore sends a CSA update request to NC-PASS1.
3. NC-PASS2 issues a CONNECT request to connect the terminal to the PAYROLL application.
4. Since the terminal is defined to VTAM2 and the application is in VTAM1, the SMEs in both VTAMs are driven. The session request will be allowed only if both SMEs process an ALLOW action.

SME processing in VTAM1

1. The first array in RULE1, R1APPL, checks whether the requested application (PLNETLU) is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.
2. The True action is followed which is to process the next array, R1USER, which checks whether the given userid is authorized to access PAYROLL.
3. CSA is checked for an entry that matches the values allowed by the rule (USERID EQ PAY*). In this example, since a CSA update request for user PAY0002 has been received by NC-PASS1, an entry is found in CSA which matches the rule. The TRUE action is processed and access to the application is ALLOWed.

SME processing in VTAM2

1. The first array in RULE2, R2APPL, checks whether the requested application (PLNETLU) is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.
2. The True action is followed which is to process the next array, R2USER, which checks whether the given userid is authorized to access PAYROLL.
3. CSA is checked for an entry that matches the values allowed by the rule (USERID EQ PAY*). In this example, user PAY0001 has been successfully authenticated by NC-PASS and therefore an entry is found in CSA which matches the rule. The TRUE action is processed and access to the application is ALLOWed.

ALLOW action processing

Since both SMEs have issued an ALLOW action, the session request is granted and the terminal is connected to the application.

Note: Similar processing to that described above would take place for terminals LOGAPPLed to NC-PASS3 that require connection to the PAYROLL application.

Using ACQUIRE to protect sensitive applications from dial-ins

While it is relatively easy to protect attempted system access from permanently attached terminals, dial in terminals present more of a problem. The dial in terminal can not be identified easily as it can be allocated a different line, and therefore a different terminal id, each time it dials in.

In general, a group of terminals is normally set aside for dial ins. When a dial in occurs and a connection is established between the participating modems, VTAM gains control of the terminal and presents it with USSTAB, which allows the user to attempt to logon to any application regardless of its sensitivity.

USSTAB, as provided as a default by IBM, has no facility to capture a userid, therefore sensitive applications that require userid information to be present in CSA can not be accessed directly from dial-in terminals. In order to perform the required level of userid validation such terminals must be ACQUIRED by NC-PASS via the SME.

Note: ACQUIRE processing can also be used where NC-PASS is not acting as a general network front end; the SME will instruct NC-PASS to ACQUIRE users who have not been validated by NC-PASS. A special NC-PASS logo will be provided for acquired terminals which will support validation as required.

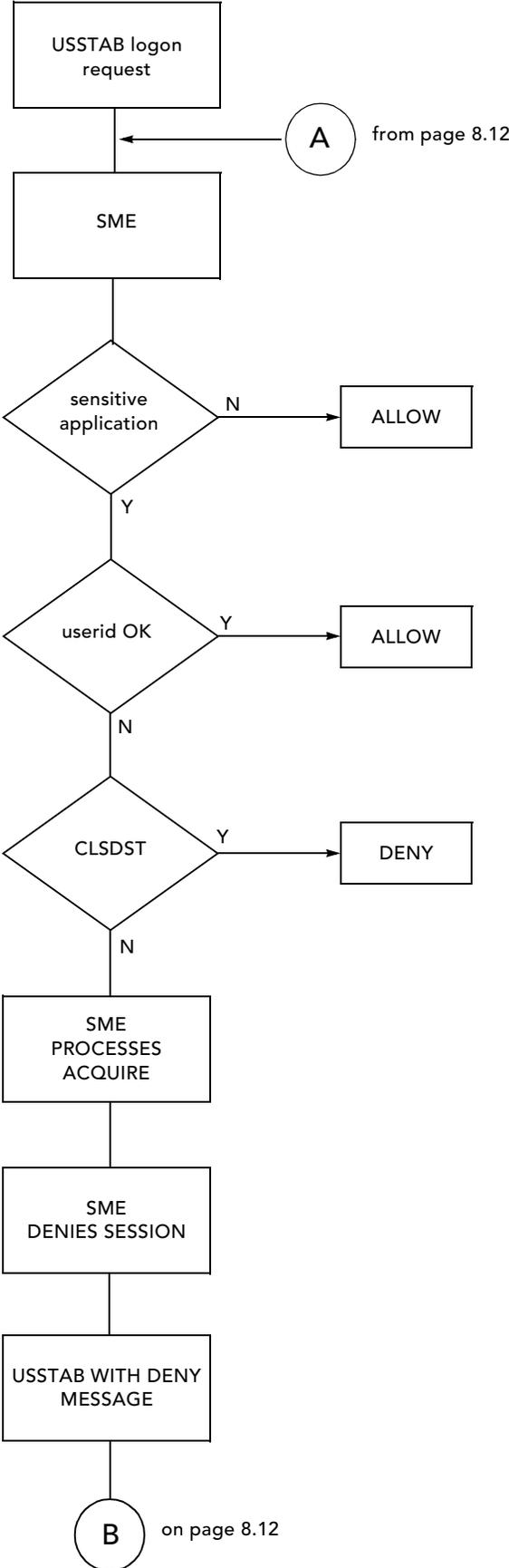
In general, a session request from a dial-in terminal to a sensitive application, protected by the ACQUIRE keyword, will invoke the SME three times. The following actions take place when a typical rule is loaded into CSA:

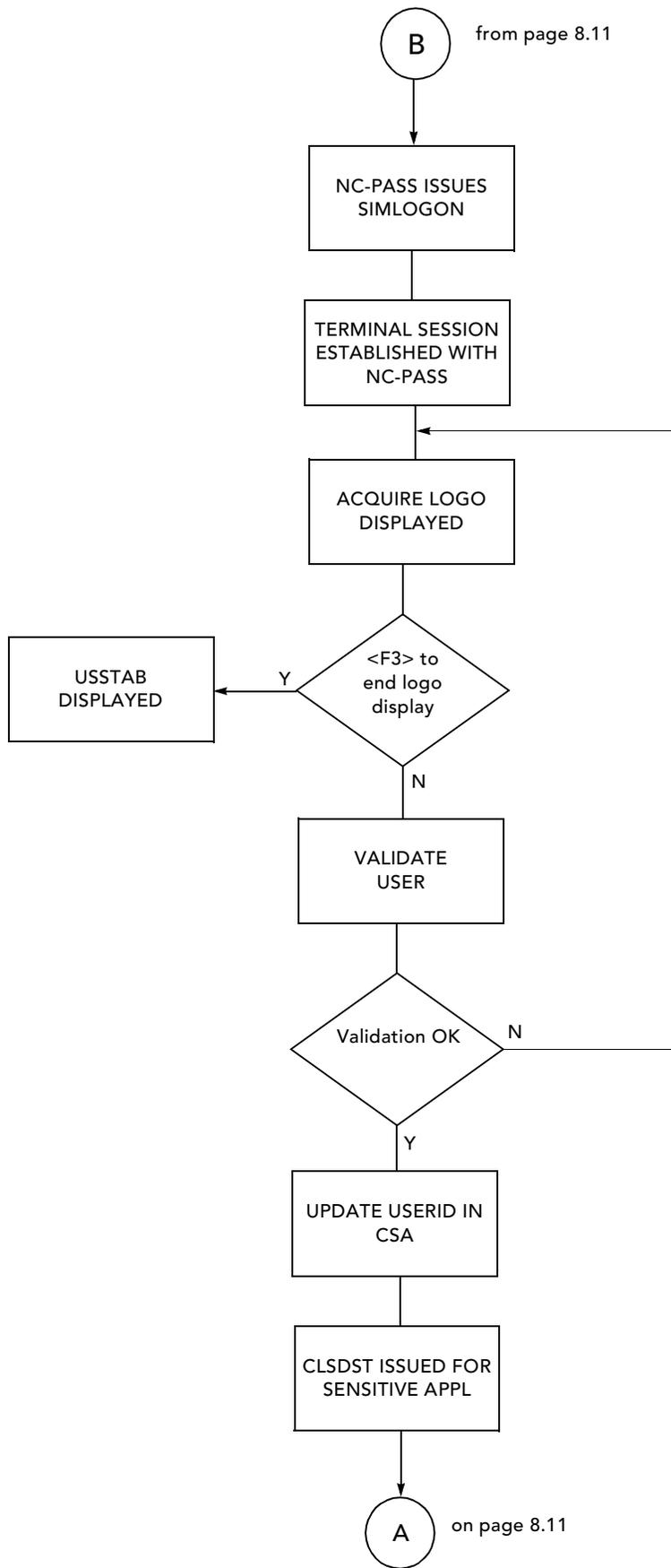
1. When the user attempts to logon to the application the first time through, (the first session request), the ACQUIRE keyword will be actioned as a result of the application being protected by the requirement for a userid.
2. The ACQUIRE results in the session being denied and the terminal being ACQUIRED by NC-PASS (a SIMLOGON, the second session request).
3. After successful validation, NC-PASS will issue a third party session request to connect the terminal to the application (a CLSDST PASS, the third session request). Assuming a valid userid (ie one that is permitted access to the sensitive application), the session request will be allowed.

The flow charts on the following pages illustrate this procedure. The following assumptions have been made;

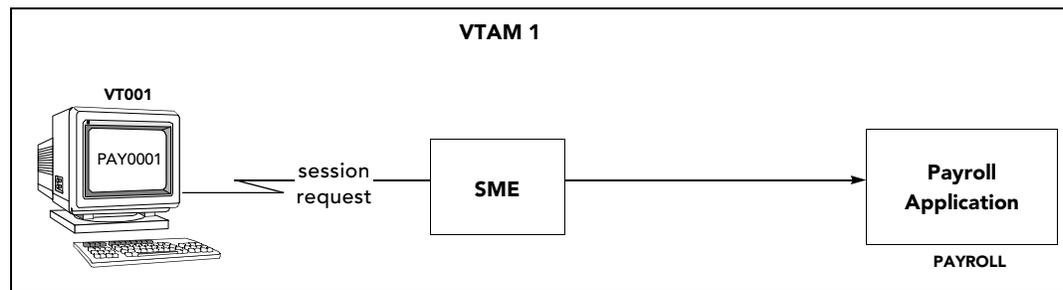
- the SME is installed
- an active control table has been loaded into CSA
- sensitive applications have been protected by the ACQUIRE keyword
- users requiring access to sensitive applications are defined against the USERID field (Refer to *Userid processing* on page 7.80)
- appropriate userid profiles have been set up on NC-PASS.

Processing outline for protected applications





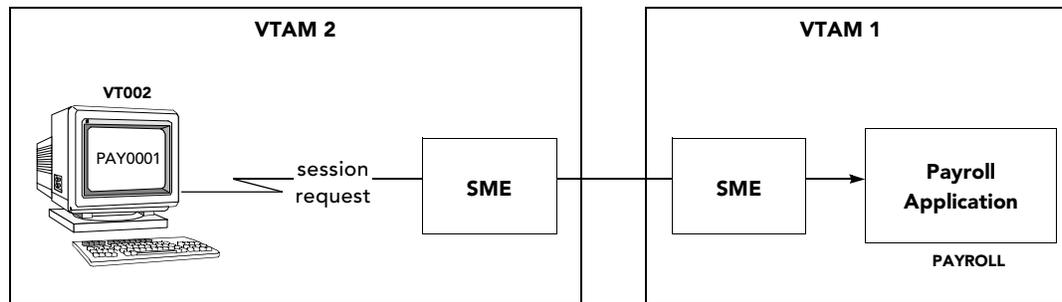
Example 3 - unauthorized access from a dial-in terminal defined to VTAM1



1. A terminal dials in to the system.
2. VTAM1 gains control over the terminal and provided it is not LOGAPPL'd or has a SIMLOGON queued, USSTAB is presented.
3. The user enters LOGON APPLID(PAYROLL) to request a logon to the payroll application. The SME is driven. (Since the application and the terminal are in the same VTAM domain, only the SME in VTAM1 is driven).
4. The first array in RULE1, R1APPL, checks whether the application is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive. No alias check is required in this array because the application is in the same VTAM domain as the SME; the real application name is known to VTAM1.
5. The True action is followed which is to process the next array, R1USER, which checks whether the given userid is authorized to access PAYROLL.
6. The user has not yet provided his userid and password to NC-PASS. Therefore no userid entry is found in CSA. The False action is followed and the third array, TERMVTAM is processed.
7. The purpose of this array is to check the origin of the dial-in terminal; if the dial-in originated from VTAM3, the terminal would be acquired by VTAM3. In this example, the terminal is defined to VTAM1 and the false action is processed.
8. The R1CLSDST array checks whether the request came directly from a terminal or was from NC-PASS (a CLSDST). In this case the request was made directly by the terminal so the False action is followed and the ACQUIRE keyword is actioned.
9. The ACQUIRE keyword results in the following processing:
 - the SME DENYs the original session request, ie the logon request from the dial in terminal to PAYROLL, and control remains directly with VTAM. USSTAB is presented to the dial-in terminal with an error message 'UNABLE TO ESTABLISH SESSION'
 - **at the same time**, the SME in VTAM1 informs NC-PASS1 that an ACQUIRE keyword has been actioned and NC-PASS1 issues a SIMLOGON request to ACQUIRE the terminal. The SME is driven for the second time. (Your rule must be coded to ALLOW NC-PASS to ACQUIRE the terminal, otherwise the SIMLOGON request will fail.) In this example, the SIMLOGON request will be ALLOWed as a result of processing the first array R1APPL.
10. Assuming the ACQUIRE is successful, the USSTAB display is replaced by the NC-PASS ACQUIRE logo screen.

11. For this example, the user enters PAY0001 as the userid and relevant password details. Alternatively he can press <F3> to return to USSTAB.
12. NC-PASS validates the given information. Assuming there is a user profile for PAY0001 or a default user profile has been specified and that all other details are valid, the following information is written to CSA for the user:
 - the userid requesting access to the sensitive system
 - the id of the requesting terminal
 - the VTAM id on which the requesting terminal is defined
 - the network id on which the requesting terminal is defined.
13. As described in *Exchange of information* on page 8.6, NC-PASS1 has a lookup table containing copies of arrays sent by other NC-PASSes. In this example, no lookup table match is found, therefore no CSA update requests are sent to other NC-PASSes.
14. A CLSDST PASS is issued by NC-PASS to connect the terminal to PAYROLL. RULE1 is processed again for this session request.
15. When the SME is driven for the third time, the same checks are performed as described on the previous page in steps 4 through 5.
16. CSA now contains an entry for userid PAY0001. PAY0001 matches the criteria for USERID and is therefore authorized to access the application; the True action is followed and access to PAYROLL is ALLOWed.

Example 4 - unauthorized access from a dial-in terminal defined to VTAM2



When a dial-in terminal which is defined to VTAM2 requests a session with an application in VTAM1, BOTH SMEs are driven; RULE1 loaded in the SME in VTAM1 and RULE2 loaded in the SME in VTAM2 ensure that, for a dial-in terminal, the ACQUIRE action is performed by the SME in VTAM1 as described in *Rule purpose* on page 8.4.

1. A terminal dials in to the system.
2. VTAM2 gains control over the terminal and provided it is not LOGAPPL'd or has a SIMLOGON queued, USSTAB is presented.
3. The user enters LOGON APPLID(PAYROLL) to request a logon to the payroll application.

SME processing - phase 1

The SMEs in both VTAMs are driven.

SME processing in VTAM1

1. The first array in RULE1, R1APPL, checks whether the application is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.
2. The True action is followed which is to process the next array, R1USER, which checks whether the given userid is authorized to access PAYROLL.
3. The user has not yet provided his userid and password to NC-PASS. Therefore no userid entry is found in CSA. The False action is followed and the third array, TERMVTAM is processed.
4. The purpose of this array is to check whether the dial-in terminal is defined to VTAM3; in this case the terminal is defined to VTAM2 and the next array R1CLSDST is processed.
5. The purpose of the R1CLSDST array is to check whether the request came directly from a terminal or was from NC-PASS (a CLSDST). In this case the request was made directly by the terminal so the False action is followed which means the session is DENYd and the ACQUIRE keyword is actioned.

SME processing in VTAM2

1. The first array in RULE2, R2APPL, checks whether the application is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.

Note: PLALLUN (application alias name) and PLNETLU (application name) have to be used in conjunction because the SME in VTAM2 only knows the application by its alias, ie, the name provided at USSTAB. This is because VTAM1 denied the session; the application is therefore unknown to VTAM2 and the application is assumed to be an alias.

2. The True action is followed which is to process the next array, R2USER. The purpose of this array is to check whether the given userid is authorized to access PAYROLL.
3. The user has not yet provided his userid and password to NC-PASS. Therefore no userid entry is found in CSA. The False action is followed and the session is DENYd.

SME processing - phase 2

The ACQUIRE keyword results in the following processing:

- the SME DENYs the original session request, ie the logon request from the dial in terminal to PAYROLL, and control remains directly with VTAM and USSTAB is presented to the dial-in terminal with an error message 'UNABLE TO ESTABLISH SESSION'
- **at the same time**, the SME informs NC-PASS1 that an ACQUIRE keyword has been actioned and NC-PASS1 issues a SIMLOGON request to ACQUIRE the terminal
- **Both SMEs are driven for the second time** because the terminal is defined to VTAM2 and the application (NC-PASS1) is in VTAM1. (Your rule must be coded to ALLOW NC-PASS to ACQUIRE the terminal, otherwise the SIMLOGON request will fail.) In this example, the SIMLOGON request will be ALLOWed as a result of processing the first arrays R1APPL and R2APPL respectively.

Assuming the ACQUIRE is successful, the USSTAB display is replaced by the NC-PASS ACQUIRE logo screen and the terminal becomes in session with NC-PASS1.

For this example, the user enters PAY0001 as the userid and relevant password details. Alternatively he can press <F3> to return to USSTAB.

NC-PASS1 validates the given information. Assuming there is a user profile for PAY0001 or a default user profile has been specified and that all other details are valid, the following information is written to CSA for the user:

- the userid requesting access to the sensitive system
- the id of the requesting terminal
- the VTAM id on which the requesting terminal is defined
- the network id on which the requesting terminal is defined.

As described in *Exchange of information* on page 8.6, NC-PASS1 examines the userid arrays in its lookup table and finds a match for this session request with array R2USER sent from NC-PASS2. (Net id is NET1, terminal's VTAM id is VTAM2, application is PAYROLL and USERID starts with PAY). NC-PASS1 therefore sends a CSA update request to NC-PASS2 for userid PAY0001.

On receipt of the confirmation from NC-PASS2, a CLSDST PASS is issued by NC-PASS1 to VTAM1 to connect the terminal in VTAM2 to PAYROLL.

SME processing - phase 3

Both SMEs are driven again for the third time for this session request.

SME processing in VTAM1

The same checks are performed as described in *SME processing in VTAM1* on page 8.15. This time a match for userid is found in CSA (as entered by NC-PASS after successful authentication) and the ALLOW action is processed.

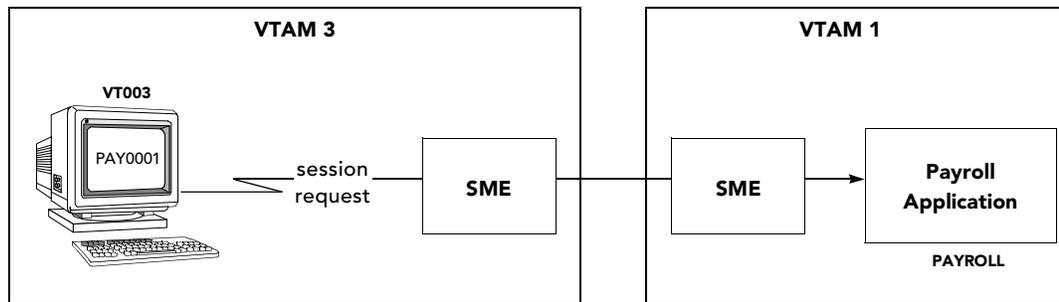
SME processing in VTAM2

The same checks are performed as described in *SME processing in VTAM2* on page 8.15. This time, a match for userid is found in CSA (as entered by the CSA update request from NC-PASS1) and the ALLOW action is processed.

ALLOW action processing

Since both SMEs have issued an ALLOW action, the session request is granted and the terminal is connected to the application.

Example 5 - Unauthorized access from a dial-in terminal defined to VTAM3



When a dial-in terminal which is defined to VTAM3 requests a session with an application in VTAM1, BOTH SMEs are driven; RULE1 loaded in the SME in VTAM1 and RULE3 loaded in the SME in VTAM3 ensure that, for a dial-in terminal, the ACQUIRE action is performed by the SME in VTAM3 as described in *Rule purpose* on page 8.4.

1. A terminal dials in to the system.
2. VTAM3 gains control over the terminal and provided it is not LOGAPPL'd or has a SIMLOGON queued, USSTAB is presented.
3. The user enters LOGON APPLID(PAYROLL) to request a logon to the payroll application.

SME processing - phase 1

The SME in both VTAMs is driven.

SME processing in VTAM1

1. The first array in RULE1, R1APPL, checks whether the application is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.
2. The True action is followed which is to process the next array, R1USER, which checks whether the given userid is authorized to access PAYROLL.
3. The user has not yet provided his userid and password to NC-PASS. Therefore no userid entry is found in CSA. The False action is followed and the third array, TERMVTAM is processed.
4. The purpose of this array is to check the origin of the dial-in terminal; if the dial-in originates from VTAM3, the terminal is to be acquired by VTAM3; in this case the terminal does originate from VTAM3 and the session is DENYd (since it will be ACQUIRED in VTAM3).

SME processing in VTAM3

1. The first array in RULE3, R3APPL, checks whether the application is sensitive or not. Application PAYROLL is listed in this array and is therefore sensitive.

Note: PLALLUN (application alias name) and PLNETLU (application name) have to be used in conjunction because the SME in VTAM3 only knows the application by its alias, ie, the name provided at USSTAB. This is because VTAM1 denied the session; the application is therefore unknown to VTAM3 and the application is assumed to be an alias.

2. The True action is followed which is to process the next array, R3USER, which checks whether the given userid is authorized to access PAYROLL.
3. The user has not yet provided his userid and password to NC-PASS. Therefore no userid entry is found in CSA. The False action is followed and the third array, R3CLSDST is processed.
4. The purpose of the R3CLSDST array is to check whether the request came directly from a terminal or was from NC-PASS (a CLSDST). In this case the request was made directly by the terminal so the False action is followed and the ACQUIRE keyword is actioned.

SME processing - phase 2

The ACQUIRE keyword results in the following processing:

- the SME DENYs the original session request, ie the logon request from the dial in terminal to PAYROLL, and control remains directly with VTAM and USSTAB is presented to the dial-in terminal with an error message 'UNABLE TO ESTABLISH SESSION'
- **at the same time**, the SME in VTAM3 informs NC-PASS3 that an ACQUIRE keyword has been actioned and NC-PASS3 issues a SIMLOGON request to ACQUIRE the terminal
- **Only the SME in VTAM3 is driven** because the terminal and application (NC-PASS3) are in the same VTAM domain. (Your rule must be coded to ALLOW NC-PASS to ACQUIRE the terminal, otherwise the SIMLOGON request will fail.) In this example, the SIMLOGON request will be ALLOWed as a result of processing the first arrays R1APPL and R3APPL respectively.

Assuming the ACQUIRE is successful, the USSTAB display is replaced by the NC-PASS ACQUIRE logo screen and the terminal becomes in session with NC-PASS3.

For this example, the user enters PAY0001 as the userid and relevant password details. Alternatively he can press <F3> to return to USSTAB.

NC-PASS3 validates the given information. Assuming there is a user profile for PAY0001 or a default user profile has been specified and that all other details are valid, the following information is written to CSA for the user:

- the userid requesting access to the sensitive system
- the id of the requesting terminal
- the VTAM id on which the requesting terminal is defined
- the network id on which the requesting terminal is defined.

As described in *Exchange of information* on page 8.6, NC-PASS3 examines the userid arrays in its lookup table and finds a match for this session request with array R1USER sent from NC-PASS1. (Terminal's network id is NET1, terminal's VTAM id is VTAM3, application is PAYROLL and USERID starts with PAY.) NC-PASS3 therefore sends a CSA update request to NC-PASS1 for userid PAY0001.

A CLSDST PASS is issued by NC-PASS3 to connect the terminal to PAYROLL.

SME processing - phase 3

Both SMEs are driven again for the third time for this session request.

SME processing in VTAM1

The same checks are performed as described in *SME processing in VTAM1* on page 8.18. This time, a match for userid is found in CSA (as entered by the CSA update request from NC-PASS3) and the ALLOW action is processed.

SME processing in VTAM3

The same checks are performed as described in *SME processing in VTAM3* on page 8.19. This time a match for userid is found in CSA (as entered by NC-PASS after successful authentication) and the ALLOW action is processed.

ALLOW action processing

Since both SMEs have issued an ALLOW action, the session request is granted and the terminal is connected to the application.

ACQUIRE function features

The following list of features apply to ACQUIRE processing:

- no access as an administrator is allowed from an ACQUIRE logo
- any existing user profile can be used for acquire validation but if a connect definition has been defined, it will be ignored since an acquired user has already specified the destination from USSTAB
- administrators, operators and users will all be treated in the same way for acquire processing
- there is a default user profile for acquire processing. This user profile will be used for validation when no matching profile is found for the supplied userid. See *Determining logon options* on page 2.5
- user and terminal locking will still apply to an acquired user
- It is not possible to issue a CONNECTR as an acquired user
- Unsuccessful access to a sensitive application due to an SME deny will return the user back to USSTAB. No message will therefore be issued to the user but the message will still be available for auditing by NC-PASS if required. All other messages, apart from CSA deletion/addition failure, will be returned back to the user who will remain at the ACQUIRE logo
- a timer task automatically deletes any unwanted ACQUIRE queue entries provided a user is not still at the logo. This is set by default to 30 - 60 seconds but is changeable in @SEEXIT0 by setting the variable *&*iacqti*. The contents of the variable represent a time wait period in multiples of 30 seconds. Validation failure will result in the default time period being used. The maximum allowable time period is 120 which represents 59.5 - 60 minutes
- LOSTERM processing will purge the ACQUIRE queue by removing any ACQUIRE entry for a terminal that has been lost.

Checking access to a specific application based on terminal id

The objective of this example is to protect a single application from access via unauthorized terminals.

The following network defined field names will be used to build the rule:

- DLNETLU contains the VTAM nodename of the requested application
- OLNETLU contains the terminal id.

Example

A pensions quotation application must be accessed only from two defined terminals in the New Business department. The application is running on VTAM nodename A01PENS1. The authorized terminal ids are T01NB001 and T01NB003. Session requests to this application from any other terminal are to be denied.

The SME ARRAY EDIT panel below shows example arrays to control access as described:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:08:44              Rule: RULEMAST  Array: PENS(1)      Terminal:A01MS247
Array comment => _____
Line commands: C=Change D=Delete

Field:    DLNETLU
Comp :    EQ

Data :    A01PENS1
and
Type

True action => RULEPENS  False action => OTHERULE

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

If the pensions quotation application is requested, the first array in rule RULEPENS (shown below) is processed. If a session with some other application is requested, rule OTHERULE (not shown) is processed.

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:08:48              Rule: RULEPENS  Array: NBTERMS(1)    Terminal:A01MS247
Array comment => _____
Line commands: C=Change D=Delete

Field:    OLNETLU
Comp :    EQ

Data :    T01NB001
and      T01NB003
Type

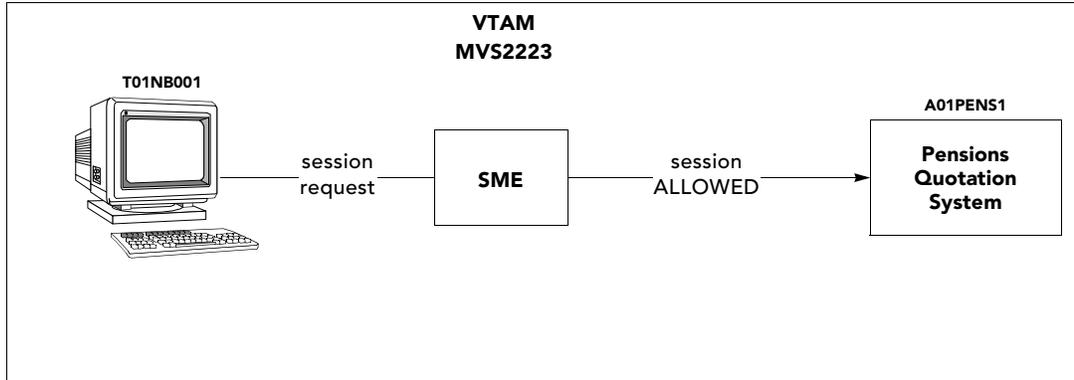
True action => ALLOW    False action => DENY

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

Audit messages

Allowed session

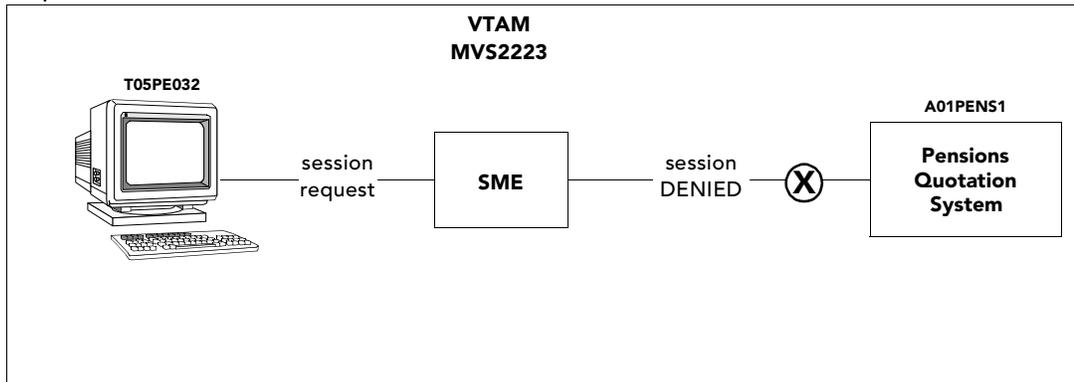
An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3345-4 SME ALLOW OLU=T01NB001 NETID=NETHQ SSCP=MVS2223
CKSE3346-4 SME ALLOW OLU=T01NB001 DLU=A01PENS1, NETID=NETHQ SSCP=MVS2223
CKSE3347-4 SME ALLOW OLU=T01NB001 RULE=RULEPENS ARRAY=NBTERMS(1)
CKSE3348-4 SME ALLOW OLU=T01NB001 FIELD=OLNETLU,EQ SUPPLIED DATA=T01NB001
```

Denied session

An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3353-4 SME DENY OLU=T05PE032 NETID=NETHQ SSCP=MVS2223
CKSE3354-4 SME DENY OLU=T05PE032 DLU=A01PENS1, NETID=NETHQ SSCP=MVS2223
CKSE3355-4 SME DENY OLU=T05PE032 RULE=RULEPENS ARRAY=NBTERMS(1)
CKSE3356-4 SME DENY OLU=T05PE032 IELD=OLNETLU,EQ SUPPLIED DATA=T05PE032
CKSE3357-4 SME DENY OLU=T05PE032 GLOBAL OPTION (STOP) = STOP
```

Denying cross domain access to a specific application

The objective of this example is to deny session requests to a specified application from terminals residing on a different VTAM to that of the application.

The following network defined field names will be used to build the rule:

DLNETLU	contains the VTAM nodename of the requested application
OLUSSCP	contains the VTAM name (SSCP) which controls the terminal
DLUSSCP	contains the VTAM name (SSCP) which controls the application.

Example

A marketing information application must be accessed only from authorized terminals residing in the same domain as the application. The application is running on VTAM nodename C10MKTG1. The VTAM id is MVS2223. Session requests to this application from any terminal outside the domain are to be denied.

The SME ARRAY EDIT panel below shows example arrays to control access as described:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:38              Rule: RULEMAST  Array: MKTG(1)      Terminal:A01MS247
Array comment => _____
Line commands: C=Change D=Delete

Field:    DLNETLU
Comp :    EQ

Data :    C10MKTG1
and
Type

True action => RULEMKTG  False action => OTHEREULE

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

If the marketing information application is requested, the first array in rule RULEMKTG (shown below) is processed. If a session with some other application is requested, rule OTHEREULE (not shown) is processed.

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:48              Rule: RULEMKTG  Array: TERMS(1)     Terminal:A01MS247
Array comment =>
Line commands: C=Change D=Delete

Field:    OLUSSCP
Comp :    EQ

Data :    DLUSSCP F ← Notice this is not a value,
                        but another field name
and
Type

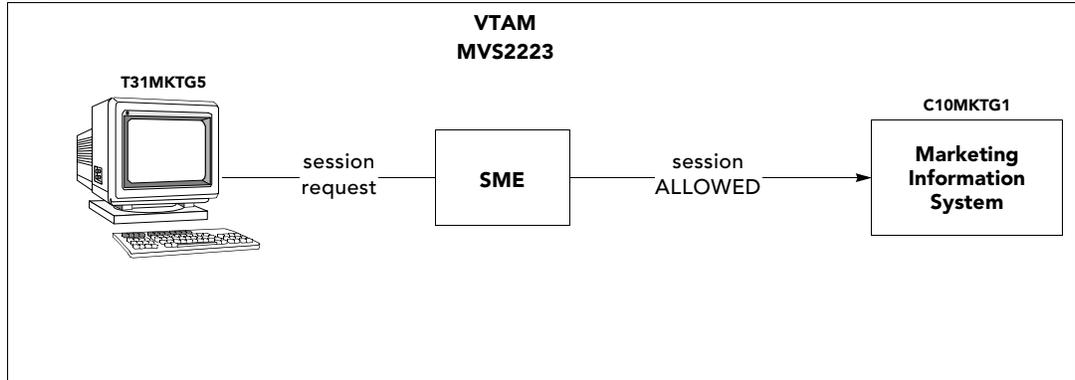
True action => ALLOW____  False action => DENY____

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

Audit messages

Allowed session

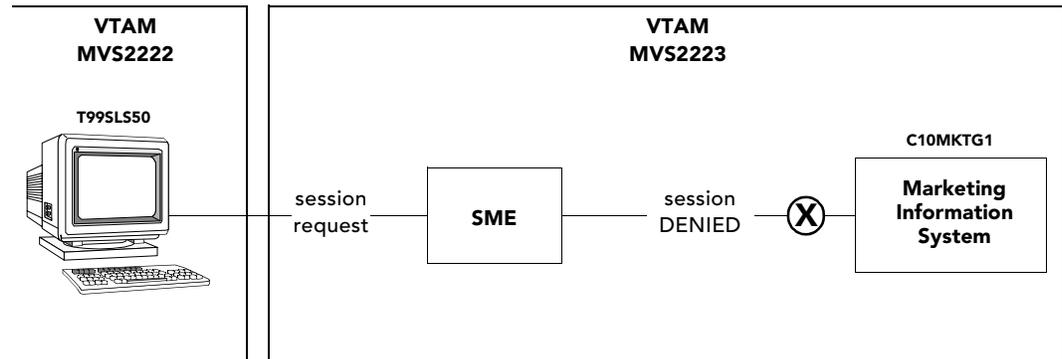
An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3345-4 SME ALLOW OLU=T31MKTG5 NETID=NETHQ SSCP=MVS2223
CKSE3346-4 SME ALLOW OLU=T31MKTG5 DLU=C10MKTG1 NETID=NETHQ SSCP=MVS2223
CKSE3347-4 SME ALLOW OLU=T31MKTG5 RULE=RULEMKTG ARRAY=TERMS(1)
CKSE3348-4 SME ALLOW OLU=T31MKTG5 FIELD=OLUSSCP EQ, SUPPLIED DATA=MVS2223
```

Denied session

An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3353-4 SME DENY OLU=T99SLS50 NETID=NETHQ SSCP=MVS2222
CKSE3354-4 SME DENY OLU=T99SLS50 DLU=C10MKTG1 NETID=NETHQ SSCP=MVS2223
CKSE3355-4 SME DENY OLU=T99SLS50 RULE=RULEMKTG ARRAY=TERMS(1)
CKSE3356-4 SME DENY OLU=T99SLS50 FIELD=OLUSSCP EQ, SUPPLIED DATA=MVS2222
CKSE3356-4 SME DENY OLU=T99SLS50 GLOBAL OPTION (STOP) = STOP
```

Denying access to a specific application from dial-in lines

The objective of this example is to deny session requests to a specified application from dial-in lines.

The following network defined field names will be used to build the rule:

DLNETLU contains the VTAM nodename of the requested application
OLNETLU contains the terminal id.

Example

A policyholder enquiry system must not be accessed via dial-in lines. The application is running on VTAM nodename P9POLENQ. Session requests from terminals accessing the system via dial-in lines are allocated from a pool of terminal ids whose names are prefixed by VT.

The SME ARRAY EDIT panel below shows an example array to control access as described:

```
Date:12/12/1997                SME ARRAY EDIT                Userid:TSG0001
Time:09:00                    Rule: RULEMAST  Array: DIAL(1)        Terminal:A01MS247
Array comment => _____
Line commands: C=Change D=Delete

Field:    DLNETLU            OLNETLU
Comp :    EQ                EQ
Data :    P9POLENQ          VT*
and
Type

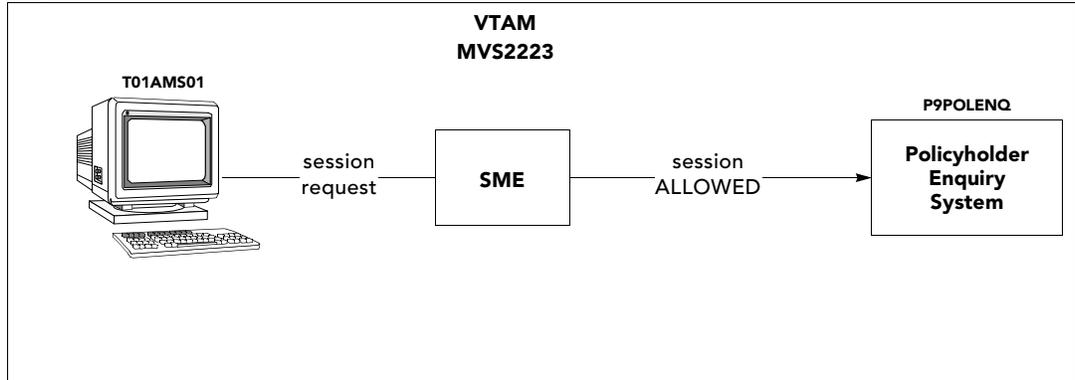
True action => DENY      False action => ALLOW

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

Audit messages

Allowed sessions

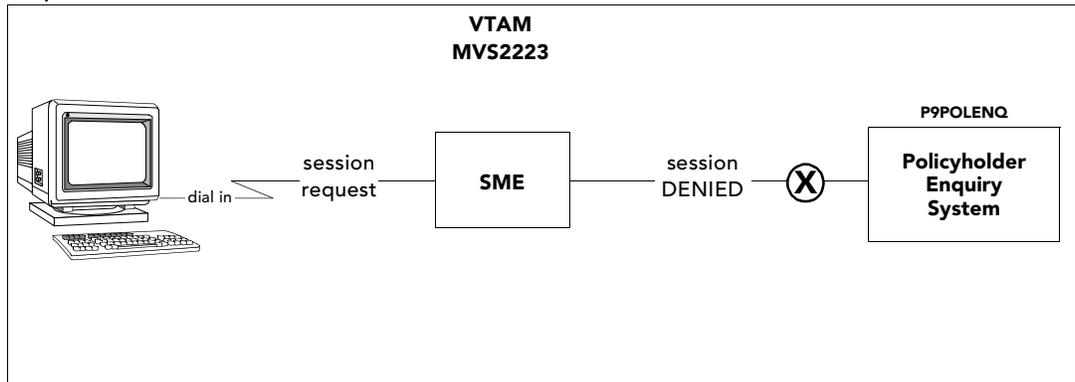
An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3345-4 SME ALLOW OLU=T01AMS01 NETID=NETHQ SSCP=MVS2223
CKSE3346-4 SME ALLOW OLU=T01AMS01 DLU=P9POLENQ NETID=NETHQ SSCP=MVS2223
CKSE3347-4 SME ALLOW OLU=T01AMS01 RULE=RULEMAST ARRAY=DIAL(1)
CKSE3348-4 SME ALLOW OLU=T01AMS01 FIELD=OLNETLU EQ, SUPPLIED DATA=T01AMS01
```

Denied sessions

An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3353-4 SME DENY OLU=VT032 NETID=NETHQ SSCP=MVS2223
CKSE3354-4 SME DENY OLU=VT032 DLU=P9POLENQ NETID=NETQ SSCP=MVS2223
CKSE3355-4 SME DENY OLU=VT032 RULE=RULEMAST ARRAY=DIAL(1)
CKSE3356-4 SME DENY OLU=VT032 FIELD=OLNETLU EQ, SUPPLIED DATA=VT032
CKSE3357-4 SME DENY OLU=VT032 GLOBAL OPTION (STOP) = STOP
```

Checking access to all applications based on SSCP

The objective of this example is to protect all applications running in a specific VTAM from access from any other VTAM.

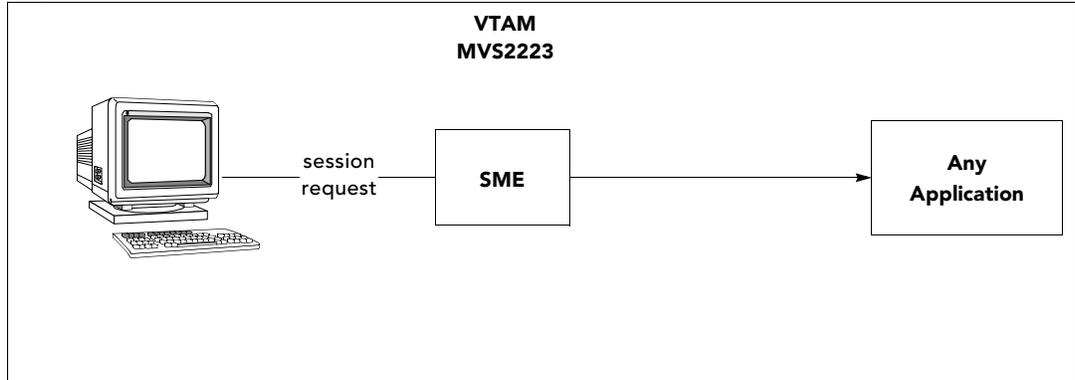
The following network defined field names will be used to build the rule:

EVSSCP	contains the VTAM id of the host where the SME is operating.
OLUSSCP	contains the VTAM name (SSCP) which controls the terminal.
DLUSSCP	contains the VTAM name (SSCP) which controls the application.

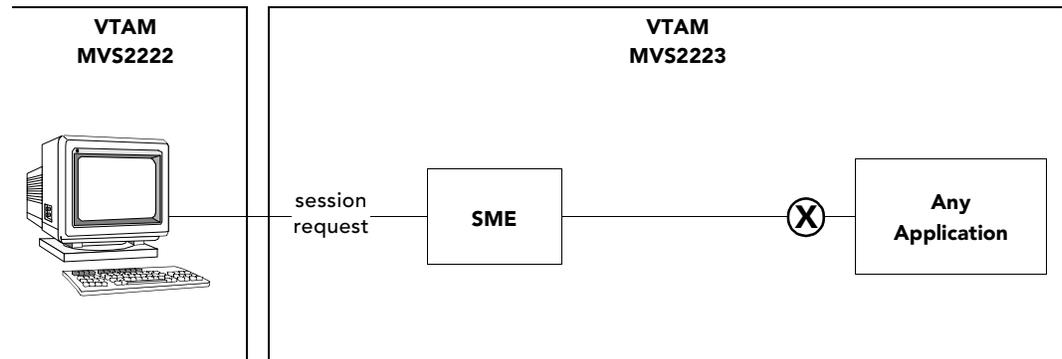
Example

A company wants to ensure that all its applications running in a specific VTAM are protected from outside access.

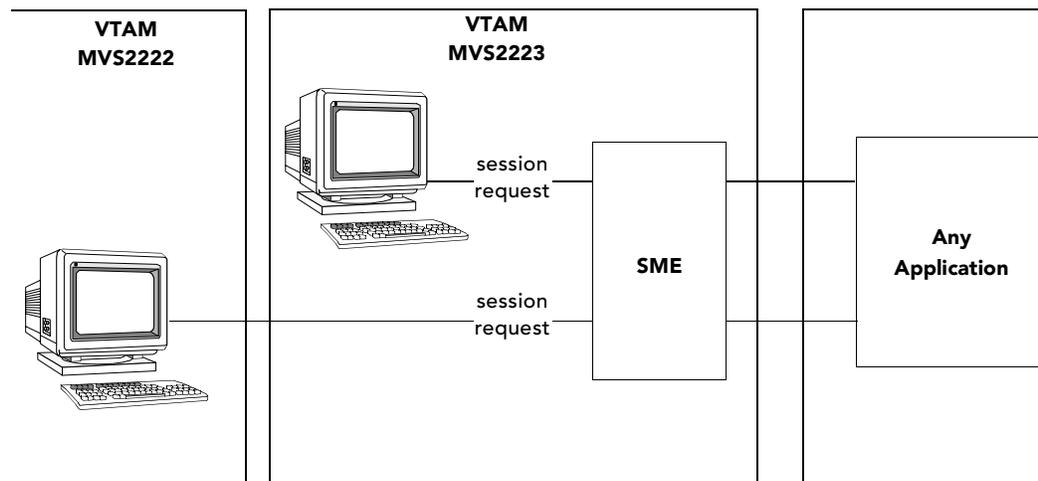
The administrator therefore must create a rule which **ALLOWS** this type of session request...



...DENYs this type of session request...



...and passes these types of session request to another part of the rule for further checking.



The SME ARRAY EDIT panel below shows example arrays to control access as described:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: RULEMAST  Array: VTAM(1)      Terminal:A01MS247
Array comment => _____
Line commands: C=Change D=Delete

Field:    DLUSSCP
Comp :    EQ

Data :    EVSSCP  F
and
Type

True action => THISVTAM  False action => DIFFVTAM

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

If the requested application is running in the same VTAM as the SME, the first array in rule THISVTAM (shown below) is processed. If the requested application is running in a different VTAM to the SME, rule DIFFVTAM (not shown) is processed.

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: THISVTAM  Array: TERMDOM(1)    Terminal:A01MS247
Array comment => _____
Line commands: C=Change D=Delete

Field:    OLUSSCP
Comp :    EQ

Data :    EVSSCP  F
and
Type

True action => ALLOW    False action => DENY

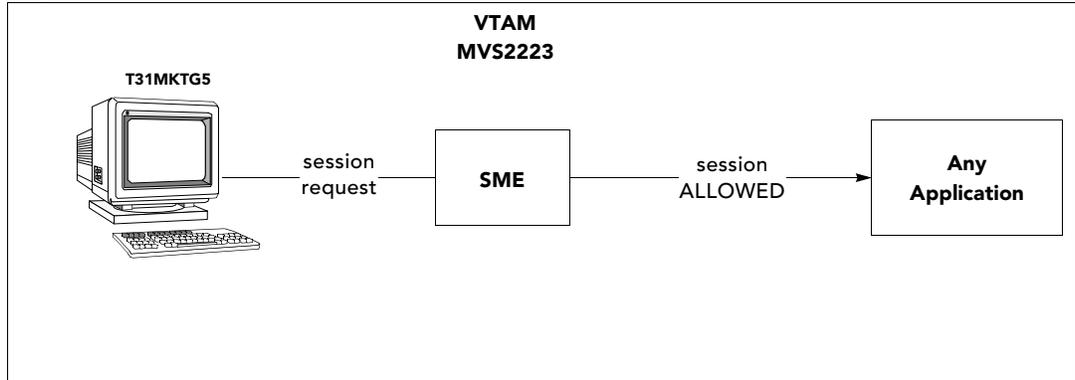
F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

This rule checks that the terminal is in the same VTAM domain as the SME.

Audit messages

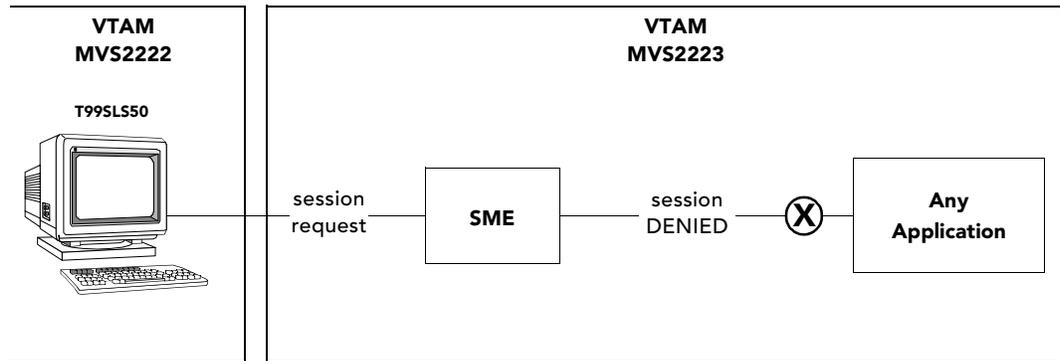
Allowed sessions

An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3345-4 SME ALLOW OLU=T31MKTG5 NETID=NETHQ SSCP=MVS2223
CKSE3346-4 SME ALLOW OLU=T31MKTG5 DLU=A01APPL1 NETID=NETHQ SSCP=MVS2223
CKSE3347-4 SME ALLOW OLU=T31MKTG5 RULE=THISVTAM ARRAY=TERMDOM(1)
CKSE3348-4 SME ALLOW OLU=T31MKTG5 FIELD=OLUSSCP EQ, SUPPLIED DATA=MVS2223
```

An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3353-4 SME DENY OLU=T99SLS50 NETID=NETHQ SSCP=MVS2222
CKSE3353-4 SME DENY OLU=T99SLS50 DLU=A01APPL1 NETID=NETHQ SSCP=MVS2223
CKSE3355-4 SME DENY OLU=T99SLS50 RULE=THISVTAM ARRAY=TERMDOM(1)
CKSE3356-4 SME DENY OLU=T99SLS50 FIELD=OLUSSCP EQ, SUPPLIED DATA=MVS2222
CKSE3356-4 SME DENY OLU=T99SLS50 GLOBAL OPTION (STOP) = STOP
```

Preventing access to an application at specific times

The objective of this example is to restrict access to an application at given times.

The following network defined field names will be used to build the rule:

- | | |
|---------|--|
| DLNETLU | contains the VTAM nodename of the requested application. |
| TIMES | contains the time restrictions as specified on the DATE AND TIME DEFINITIONS panel (5.7). Refer to <i>Chapter 6 - Restricting access by date and time</i> for further details. |

Example

A company wants to ensure that access to its Payroll system is allowed only on Wednesdays and Fridays from 09:00 to 15:00.

The SME ARRAY EDIT panels below show example arrays to control access as described:

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: MASTRULE Array: PAYAPPL(1) Terminal:A01MS265
Array comment => CHECK FOR PAYROLL APPL
Line commands: C=Change D=Delete

Field:   DLNETLU
Comp :   EQ

Data :   A01PAYR
and
Type

True action => NEXT      False action => OTHERULE

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

If the payroll application is requested, the next array in the rule (shown below) is processed. If a session with some other application is requested, rule OTHERULE (not shown) is processed.

```
Date:12/12/1997          SME ARRAY EDIT          Userid:TSG0001
Time:09:00              Rule: MASTRULE Array: TIME(2) Terminal:A01MS265
Array comment => CHECK ACCESS TIME IS OK
Line commands: C=Change D=Delete

Field:   TIMES
Comp :   EQ

Data :   PAYTIME D ← Notice this is not a value,
and                                     but a date/time definition
Type

True action => ALLOW    False action => DENY

F1=Help  F2=Ins  F3=End  F5=Order  F10=Left  F11=Right  F12=Can
```

If the time of access is within the specified limits, access is ALLOWed, otherwise access is DENYd.

The PAYTIME date/time definition has been specified as follows:

```
Date:12/12/1997          DATE AND TIME DEFINITION PAYTIME          Userid:TSG0001
Time:16:21              Terminal:A01MS25

Definition comment => Restriction - payroll system

Line commands: A=After  B=Before  D=Delete  M=Move  N=New

S DAYS          DATE          TIME
M T W T F S S  START        END          START    END
- - - - -
_ N N Y N Y N N          09:00      15:00

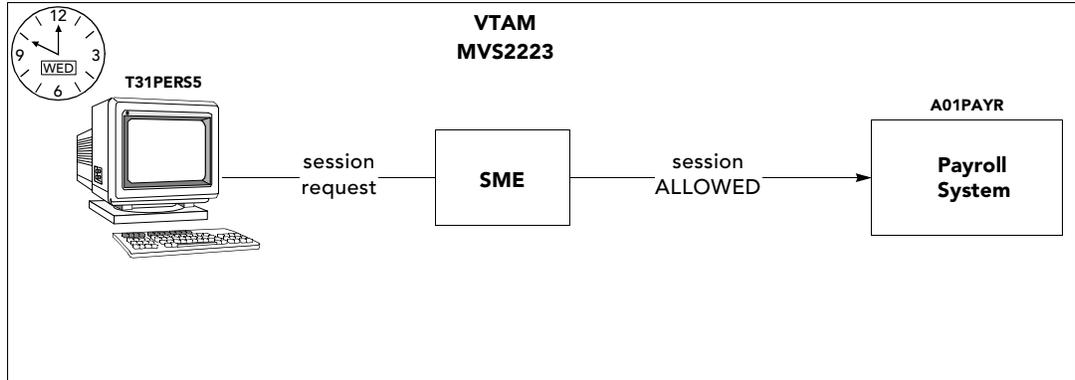
F1=Help  F3=End  F7=Up  F8=Down  F12=Can
```

Refer to *Creating date and time definitions* on page 6.3 for details of how to specify date/time definitions.

Audit messages

Allowed session

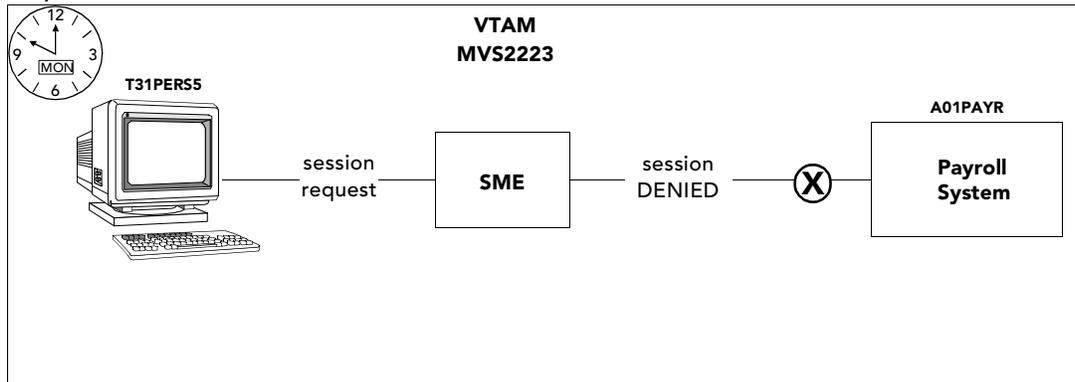
An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3345-4 SME ALLOW OLU=T31PERS5 NETID=NETHQ SSCP=MVS2223
CKSE3346-4 SME ALLOW OLU=T31PERS5 DLU=A01PAYR NETID=NETHQ SSCP=MVS2223
CKSE3347-4 SME ALLOW OLU=T31PERS5 RULE=MASTRULE ARRAY=TIME(2)
CKSE3348-4 SME ALLOW OLU=T31PERS5 FIELD=TIMES EQ, SUPPLIED DATA=10:00
```

Denied session

An example of the audit messages that could be produced for the following session request are listed below:



```
CKSE3345-4 SME DENY OLU=T31PERS5 NETID=NETHQ SSCP=MVS2223
CKSE3346-4 SME DENY OLU=T31PERS5 DLU=A01PAYR NETID=NETHQ SSCP=MVS2223
CKSE3347-4 SME DENY OLU=T31PERS5 RULE=MASTRULE ARRAY=TIME(2)
CKSE3348-4 SME DENY OLU=T31PERS5 FIELD=TIMES EQ, SUPPLIED DATA=MON
```

General considerations when building a rule

This section highlights potential problems that can occur if a rule is not correctly designed.

System-generated session requests

Ensure that your rule does not DENY required system-generated session requests. For example, when the SME processes the ACQUIRE keyword, the result is that NC-PASS queues a SIMLOGON request for the terminal. This SIMLOGON request is a session request in its own right, and the SME must ALLOW this request for the ACQUIRE to have the desired effect.

NC-PASS will also issue a CLSDST PASS session request when a user has been successfully validated by NC-PASS and has a CONNECT definition which routes him to specific applications. This CLSDST PASS is also a session request and must be ALLOWed by the SME for the connect function to have the desired effect.

If you have multiple VTAMs, each with an active SME and an NC-PASS v2.0 job running, these NC-PASSes will need to communicate with each other and exchange information. The SMEs must allow session requests between each NC-PASS v2.0 running in each of the VTAMs.

Session 'races'

The type of session 'race' that the ACQUIRE processing introduces can have interesting results when ACQUIRE is coded in several SMEs for the same application. If a user logs on at TERMINAL(A) in VTAM(A) trying to establish a session with APPL(B) running in VTAM(B) and ACQUIRE has been specified for APPL(B) in rules for SME(A) and SME(B) then depending on the speed of processing the user may find himself in session with PASS(A) or PASS(B). In general it is advisable to only code ACQUIRE in a rule loaded to the same VTAM as the VTAM in which the associated application is running.

Chapter 9 - Auditing

Message facilities	9.2
Routing messages	9.3
Automatic message processing overview	9.3
Browsing messages	9.3
Message routing	9.4
Severity levels	9.4
Processing of batch messages	9.6
NC-PASS active	9.6
NC-PASS inactive	9.6
Automatic message processing	9.7
Limiting to time of day or frequency	9.7
Processing the selection	9.10
Processing the action	9.10
SME action auditing	9.16
ACQUIRE	9.17
ALLOW	9.18
DENY	9.21
WARN	9.22
Browsing the NC-PASS message log	9.23
Selecting messages for display	9.23
Printing from the NC-PASS message log	9.27
NCI log control	9.28
The NCI LOG CONTROL panel	9.28
Overflow records	9.29
Archive file control	9.30
Defining an ESDS for archive files	9.30
The ARCHIVE FILE CONTROL panel	9.31
Factors affecting archive file control	9.32
Overflow records	9.32
Example 1	9.33
Example 2	9.33
Viewing archived and SMF messages	9.34
Making ESDS copies of SMF records	9.34
Printing archived messages	9.36
MHO routed messages	9.37
Messages from proprietary security systems	9.38
Example	9.38
Message processing using SMF files	9.40
Reading and displaying records written to SMF files	9.40
Supplied JCL to copy an SMF file to an ESDS VSAM file	9.41
NC-PASS message record layout (as written to SMF)	9.42
NC-PASS message record layout (as written to archive ESDS files)	9.43

Message facilities

The messages generated as a result of NC-PASS on-line processing can be routed to one or more of the following destinations:

- the user's terminal
- the system console
- the NC-PASS message log
- the NCI log
- an archive file
- IBM's System Management Facility
- NetView
- other NC-PASS systems via MHO.

Each NC-PASS message has a predefined severity level. Severity levels range from zero through nine, the highest severity being zero.

The following table defines the message type applicable at each severity level.

Severity level	Message type
0	No NC-PASS messages have this severity.
1	No NC-PASS messages have this severity.
2	No NC-PASS messages have this severity.
3	System warning messages (for example CKSE0537-3 SYSTEM INITIALIZATION FAILED).
4	System information messages (for example CKSE0535-4 SYSTEM INITIALIZATION COMPLETED).
5	Logon warning messages (for example CKSE0024-5 PASSWORD INVALID).
6	Logon information messages (for example CKSE0027-6 PLEASE ENTER A NEW PASSWORD).
7	No NC-PASS messages have this severity.
8	Panel warning messages (for example CKSE3277-8 RULE <i>rulename</i> DELETED).
9	Panel information messages (for example CKSE0005-9 THAT KEY HAS NO MEANING - PLEASE RETRY).

Messages produced from batch jobs that update the NC-PASS CAF are written to the job's NCI log and can also be routed in the same way, providing the following conditions are true:

- the NC-PASS system is active
- Cross Memory Services (XMS) is enabled. XMS is the means by which any job running in the same operating system as NC-PASS (eg programs running under TSO, batch jobs etc) can communicate with NC-PASS. XMS is described in *Chapter 1 - Communicating with other systems* (Volume 2).

Routing messages

A message can be selectively routed, on the basis of its severity level, to its destination(s). This facility is provided by the MESSAGE ROUTING panel (1.3.1) which allows each message severity level to be assigned to specific destinations. Non NC-PASS text messages, such as RACF and CA-Top Secret messages, can also be routed as a group to specific destinations.

Note: Messages routed to NetView must have been entered in the NetView user tables. The text of these messages will not be displayed if not included in the tables. For information on adding message text to the NetView user tables, refer to the IBM manual entitled NetView Customization Guide (publication number SC31-6016). See also *NetView Alert messages* on page 6.190 of the NC-PASS Secure Administration Manual - Volume 2.

Automatic message processing overview

The severity level of a message can be altered, and the message itself can be changed to another message, according to certain conditions specified in the AUTOMATIC MESSAGE PROCESSING panel (1.3.2). If the conditions laid out in this panel are met, the message or severity level or both will be changed automatically, on either a permanent or a temporary basis, as defined by action fields in the panel. The various functions that action fields can perform are described in the section entitled *Automatic message processing* on page 9.7.

Permanently changed messages and severity levels relate to a specific terminal or user and can be changed back to their original settings using the RESET ESCALATED TERMINALS AND USERS panel (1.3.3).

Browsing messages

If you want to browse messages which have been routed to...	then...
the NC-PASS message log	use the BROWSE NC-PASS LOG panel (3).
the NCI log	press <F9> in the BROWSE NC-PASS LOG panel (3).
an archive file	use the SELECT ARCHIVE AND SMF MESSAGES panel (1.3.6). To archive messages, archive files must first be assigned using the ARCHIVE FILE CONTROL panel (1.3.5).
SMF	use the SELECT ARCHIVE AND SMF MESSAGES panel (1.3.6). The messages must be copied to an archive file first.

Message routing

The MESSAGE ROUTING panel (1.3.1) displays a table of message severity levels and destinations as shown below.

```

Date:12/12/1997                                MESSAGE ROUTING                                Userid:TSG0001
Time:09:00                                       Terminal:A01MS262

Every message has a severity level. Enter 'X' in the table to route the
message. (Note that zero is the highest severity).

Output Route          Message Severity Level          Text
                      0  1  2  3  4  5  6  7  8  9  messages
User                  => -  -  -  X  X  X  X  -  X  X  => X
Console               => -  -  -  X  X  X  -  -  -  -  => -
Console Non/Delete   => -  -  -  -  -  -  -  -  -  -  => -
NC-PASS Message Log  => -  -  -  X  X  X  X  -  X  -  => -
NCI Log              => -  -  -  X  X  X  X  -  X  X  => X
Archive              => -  -  -  -  -  -  -  -  -  -  => X
NetView              => -  -  -  -  -  -  -  -  -  -  => -
SMF                  => -  -  -  -  -  -  -  -  -  -  => -
SMF Record Type      => ____ (128-255)
MHO                  => -  -  -  -  -  -  -  -  -  -  => -
MHO Nodename         => _____

F1=Help  F3=End  F12=Can
  
```

Severity levels

Message severity levels, as shown on the top row of the table, range from zero (highest severity) through nine. Place an X in the appropriate row/column to select a destination for a required severity level. When a message is generated by NC-PASS it will be routed according to its severity and the destination defined for that severity. Default entries are provided. Place an X in the **Text messages** column if non NC-PASS messages (such as CA-ACF2 messages) are to be routed to specific destinations.

Input fields

Message destinations are as follows:

User	the user's screen.
Console	the system console, (messages can scroll off the screen).
Console Non/Delete	the system console, (messages will remain on the screen until deleted by the operator).
NC-PASS Message log	the message log available through option 3 of the NC-PASS Secure menu.
NCI log	the NCI message log.
Archive	a predefined archive file (refer to the section entitled <i>Archive file control</i> on page 9.30).
NetView	IBM's network monitor.
SMF	IBM's system management facility. If the SMF output route is selected, the record type must be entered in the SMF record type field.

SMF Record Type	If the SMF output route is selected, the record type (between 128 and 255) must be entered in this field.
MHO	this routes messages via MHO to the nodename entered at the MHO Nodename field.
MHO Nodename	If the MHO route is selected, the MHO nodename must be entered in this field (eight characters).

Function keys

Key	Function
F1	displays help information.
F3	saves the values entered and returns to the previous panel.
F12	cancel any changes and returns to the previous panel.

Processing of batch messages

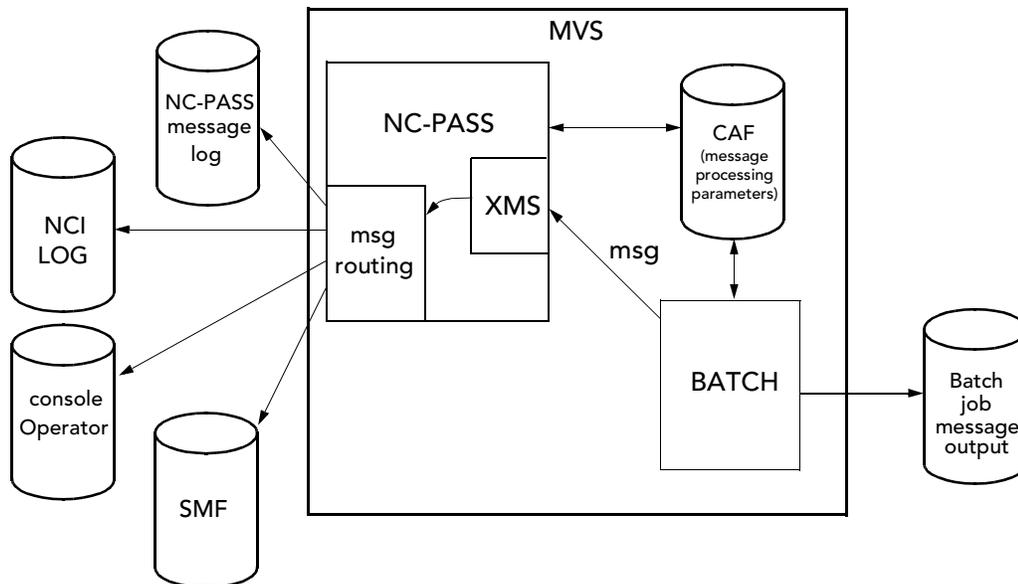
How messages from batch jobs are processed varies according to the status of NC-PASS, as shown below.

NC-PASS active

If the following conditions are true:

- the NC-PASS system is active
- Cross Memory Services (XMS) is enabled.

Audit messages produced by batch jobs are sent via XMS to the NC-PASS system in addition to being written to the job's NCI log. They can then be routed according to their severity and the destination specified for that severity in the MESSAGE ROUTING panel. This process is shown in the diagram below.



Note: Batch routines are run separately from NC-PASS but use similar JCL. The CAF (a VSAM database) must be defined to allow multiple reads and writes to enable batch jobs to run while NC-PASS is active. Do not attempt administration updates while the batch job is active.

NC-PASS inactive

If the NC-PASS system is not available or XMS is inactive, batch messages are routed only to the NCI log of the batch job, as they were before this enhancement. In this case the following message will be recorded on the NCI log:

```
CKxx3680-9 NC-PASS XMS UNAVAILABLE, BATCH MESSAGE AUDIT VIA NCI LOG ONLY
```

This indicates that the audit trail will not be recorded by an NC-PASS system.

Automatic message processing

Automatic message processing allows 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 it would be written to SMF and an alternative message could be displayed to the user.

Limiting to time of day or frequency

Limitations to the time of day and frequency of the message issued can be implemented; similarly messages issued to a specific userid or specific terminal or both can be used depending on the result required. Several examples are provided at the end of this section.

The AUTOMATIC MESSAGE PROCESSING panel (1.3.2) allows certain conditions to be specified which, if met, will automatically change the severity level and content of a message.

```
Date:12/12/1997          AUTOMATIC MESSAGE PROCESSING          Userid:TSG0001
Time:09:00              Terminal:A01MS262

----- SELECTION -----          ----- ACTION -----
- TIME -                          ALTERNATE
ID  FREQ PERIOD  START END TERM USER  TERM USER SEV  MESSAGE
000001 0002  10  00:15  00:00 23:59 Y  N          2
000002 0005   3  00:10  12:00 13:00 Y  Y          E  E  0    0491
***** **  ***** ***** *  *          *  *  *    ****

F1=Help  F3=End  F7=Up  F8=Down  F12=Can
```

Input fields

The panel is in line editor mode (refer to the NC-PASS Secure Installation Manual section *Making changes to panel data* on page 8.12).

SELECTION

The SELECTION columns determine the conditions under which the changes specified in the ACTION columns will occur.

Field

Description

ID

Enter the four digit number which identifies the message (for example, the message CKSE3345 is identified by 3345).

Field	Description
FREQ	Enter the number of times the message must be issued (within the constraints of the PERIOD, START and END fields) before the ACTION fields will be executed. A figure between 0 and 99 can be entered. If 0 is entered the action will be executed when the first message is issued (in this case PERIOD must be specified as 00:00).
PERIOD	Enter the period of time in which the number of messages specified in FREQ must be issued. If the number of messages specified in FREQ is greater than 0, the PERIOD cannot be set to 0. If met, the changes specified under ACTION will be invoked.
START/END	Specify the times of day, or window, in which the number of messages specified in FREQ will be checked for (within a period of time specified by PERIOD) to invoke the changes specified under ACTION.
TERM	Enter Y to specify that the message identified by ID must be issued <i>n</i> times (as specified by FREQ) to a specific terminal for the changes specified under ACTION to be executed. If you enter N the adjacent USER field must be set to Y. This field is ignored if FREQ is set to 0.
USER	Enter Y to specify that the message identified by ID must be issued <i>n</i> times (as specified by FREQ) to a specific user for the changes specified under ACTION to be executed. If you enter N, the adjacent TERM field must be set to Y. This field is ignored if FREQ is set to 0.

ACTION

These fields determine the action to be taken when the specified SELECTION conditions have been met.

Field	Description
TERM	<p>set to blank, E (Escalate) or L (Lock):</p> <ul style="list-style-type: none"> blank no permanent actions are to be taken (escalating or locking). The individual message will be processed according to the severity and alternate message specified. E this and all future messages for the terminal will be altered to the severity and alternate message specified. A permanent escalation record will be stored. Permanent escalations can be reset or viewed using the RESET ESCALATED TERMINALS AND USERS panel (1.3.3). Refer to the section entitled <i>Escalated terminals and users</i> on page 3.42. L the message will be issued and the terminal will be locked. Terminals can be reset using the PROCESS LOCKED TERMINALS panel (6.4). Refer to <i>Locked terminals</i> on page 3.39.

Field	Description
USER	<p>set to blank, E (Escalate) or L (Lock):</p> <p>blank no permanent actions are to be taken (escalating or locking). The individual message will be processed according to the severity and alternate message specified.</p> <p>E this and all future messages for the user will be altered to the severity and alternate message specified. A permanent escalation record will be stored. Permanent escalations can be reset or viewed using the RESET ESCALATED TERMINALS AND USERS panel (1.3.3). Refer to the section entitled <i>Escalated terminals and users</i> on page 3.42.</p> <p>L the message will be issued and the user will be locked. Users can be reset using the PROCESS LOCKED USERS panel (5.8). Refer to <i>Locked users</i> on page 3.37.</p>
SEV	this is the changed severity of the message, between 0 and 9 (0 is highest).
ALTERNATE MESSAGE	this is the number of the message to be issued in place of the original message.

Note: For messages output from batch CAF update jobs, the associated userid is the jobname of the batch process and the terminal ID is BATCH. You cannot lock terminals with an ID of BATCH, since no real terminal is involved.

Function keys

Key	Function
F1	displays help information.
F3	saves the changes made and returns to the MESSAGE MAINTENANCE MENU.
F7	displays the previous screen of messages.
F8	displays the next screen of messages.
F12	cancels any changes made and returns to the MESSAGE MAINTENANCE MENU.

Processing the selection

When a message is issued by NC-PASS:

- the selection conditions are evaluated
- if positive, actions are taken
- if negative, no action is taken but the original message is issued.

Although there are many possible selection combinations, one example is sufficient to describe the process.

Example

```
----- SELECTION -----  
- TIME -  
ID  FREQ  PERIOD  START  END  TERM  USER  
0184 03    00:20   09:00 11:00  Y     N
```

If message 0184 occurred three times in the last twenty minutes and the current time is between 09.00 hrs and 11.00 hrs and the messages were for the same terminal, but for any user, then carry out the actions (positive).

Processing the action

For the remainder of this section we will assume that the conditions put by a selection have been met and the actions are to be carried out.

There are two considerations:

- an action may be immediate
- an action may be immediate AND have future implications.

Actions are applied to terminals, users, severity levels and the message issued. If the options for the terminal and user are both blank, then ONLY immediate actions will be required.

The message numbers displayed in the examples below are for illustration purposes only.

Example 1 - immediate actions only

```
----- ACTION -----  
ALTERNATE  
TERM  USER  SEV  MESSAGE  
      3    0195
```

Immediate actions

The immediate action caused by this example is to amend the original severity of the message to 3 and to issue message 0195 instead. This happens once. The user sees the next screen expected.

Future actions

There are no future actions.

Administrator actions

None required.

Example 2 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM  USER  SEV  MESSAGE  
  E           7   0123
```

Immediate actions

The original severity of the message is amended to 7 and message 0123 will be issued instead. This happens once. The user sees the next screen expected. There is no 'locking out'.

An entry is recorded on the permanent escalation file. This entry may be viewed and reset using option 3 of the MESSAGE MAINTENANCE menu (1.3).

Future actions

All future messages issued by the same terminal, regardless of user or message serial number, will be amended to severity 7, message 0123. This will happen until the permanent escalation record of the incident has been reset.

Administrator actions

In order to allow processing to continue, the administrator must reset the permanent escalation record of the incident.

Example 3 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM  USER  SEV  MESSAGE  
           E    7   0123
```

Immediate actions

The original severity of the message is amended to 7 and message 0123 will be issued instead. This happens once. The user sees the next screen expected. There is no 'locking out'.

An entry is recorded on the permanent escalation file. This entry may be viewed and reset using option 3 of the MESSAGE MAINTENANCE menu (1.3).

Future actions

All future messages issued by the same user, regardless of terminal or message serial number, will be amended to severity 7, message 0123. This will happen until the permanent escalation record of the incident has been reset.

Administrator actions

In order to allow processing to continue, the administrator must reset the permanent escalation record of the incident.

Example 4 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM  USER SEV  MESSAGE  
  E    E    7
```

Immediate actions

The original severity of the message is amended to 7. This happens once. The user sees the next screen expected. There is no 'locking out'.

An entry is recorded on the permanent escalation file. This entry may be viewed and reset using option 3 of the MESSAGE MAINTENANCE menu (1.3).

Future actions

All future messages issued by the same user and terminal, regardless of message serial number, will be amended to severity 7. This will happen until the permanent escalation record of the incident has been reset.

Administrator actions

In order to allow processing to continue, the administrator must reset the permanent escalation record of the incident.

Example 5 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM  USER SEV  MESSAGE  
  L          0   0246
```

Immediate actions

The original severity of the message is amended to 0, and message 0246 will be issued instead. This happens once. The user does not see the next screen expected. The terminal is locked. The NC-PASS logo is displayed.

An entry is recorded on the list of locked terminals. Locked terminals may be viewed and unlocked on the PROCESS LOCKED TERMINALS panel (6.4).

Future actions

All future attempts to log on to NC-PASS using the same terminal will fail until the lock has been removed. Messages issued, and their severity, will remain unchanged. They will NOT be amended to severity 0, message serial number 0246.

Administrator actions

In order to allow processing to continue, the administrator must unlock the terminal.

Example 6 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM USER  SEV  MESSAGE  
   L     5   0134
```

Immediate actions

The original severity of the message is amended to 5, and message 0134 will be issued instead. This happens once. The user does not see the next screen expected. The user is locked out. The NC-PASS logo is displayed.

An entry is recorded on the list of locked users. Locked users may be viewed and unlocked on the PROCESS LOCKED USERS panel (5.8).

Future actions

All future attempts to log on to NC-PASS using the same userid will fail until the lock has been removed. Messages issued, and their severity, will remain unchanged. They will NOT be amended to severity 5, message serial number 0134.

Administrator actions

In order to allow processing to continue, the administrator must unlock the user.

Example 7 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM USER  SEV  MESSAGE  
   L   L    0   0123
```

Immediate actions

The original severity of the message is amended to 0, and message 0123 will be issued instead. This happens once. The user does not see the next screen expected. The user and terminal are locked out. The NC-PASS logo is displayed.

Entries are recorded on the list of locked users and the list of locked terminals.

Future actions

All future attempts to log on to NC-PASS using the same userid or terminal will fail until the locks have been removed. Messages issued, and their severity, will remain unchanged. They will NOT be amended to severity 0, message serial number 0123.

Administrator actions

In order to allow processing to continue, the administrator must unlock the user and terminal.

Example 8 - immediate actions and further considerations

```
----- ACTION -----  
                        ALTERNATE  
TERM USER  SEV  MESSAGE  
L   E      0   0123
```

Immediate actions

The original severity of the message is amended to 0, and message 0123 will be issued instead. This happens once. The user does not see the next screen expected. The terminal is locked out. The NC-PASS logo is displayed.

An entry is recorded on the list of locked terminals. A permanent escalation record has also been added.

Future actions

All future attempts to log on to NC-PASS using the same terminal will fail until the lock has been removed. Messages will be amended to severity 0, message 0123.

Note: If the same user tries to log on at another terminal, the log on procedure will issue a message. The message handling routine will read the permanent escalation record and lock THAT terminal as well. The NC-PASS logo will be redisplayed.

Administrator actions

The administrator must take care with resetting these consequences.

If the lock alone is removed, the user will log on and the log on procedure will issue a message. The message handling routine will check for permanent escalation, find a record, and lock the terminal again, issuing message 0123 at severity 0.

If the permanent escalation record alone is reset, the user will still be unable to log on at the SAME terminal because it is locked.

The administrator must therefore reset BOTH consequences to allow processing to continue.

Example 9 - immediate actions and further considerations

```
----- ACTION -----  
                          ALTERNATE  
TERM USER  SEV  MESSAGE  
E     L     0   0123
```

Immediate actions

The original severity of the message is amended to 0, and message 0123 will be issued instead. This happens once. The user does not see the next screen expected. The user is locked out. The NC-PASS logo is displayed.

An entry is recorded on the list of locked users. A permanent escalation record has also been added.

Future actions

All future attempts to log on to NC-PASS using the same userid will fail until the lock has been removed. Messages will be amended to severity 0, message 0123.

Note: If a different user tries to log on at the same terminal, the log on procedure will issue a message. The message handling routine will read the permanent escalation record and lock that user as well. The NC-PASS logo will be redisplayed.

Administrator actions

The administrator must take care with resetting these consequences.

If the lock alone is removed, the user will log on and the log on procedure will issue a message. The message handling routine will check for permanent escalation, find a record, and lock the terminal again, issuing message 0123 at severity 0.

If the permanent escalation record alone is reset, the user will still be unable to log on using the SAME userid because it is locked.

The administrator must reset BOTH consequences.

SME action auditing

A session initiation request will result in one of the following actions from the Active Control Table

- ACQUIRE
- ALLOW
- DENY
- WARN.

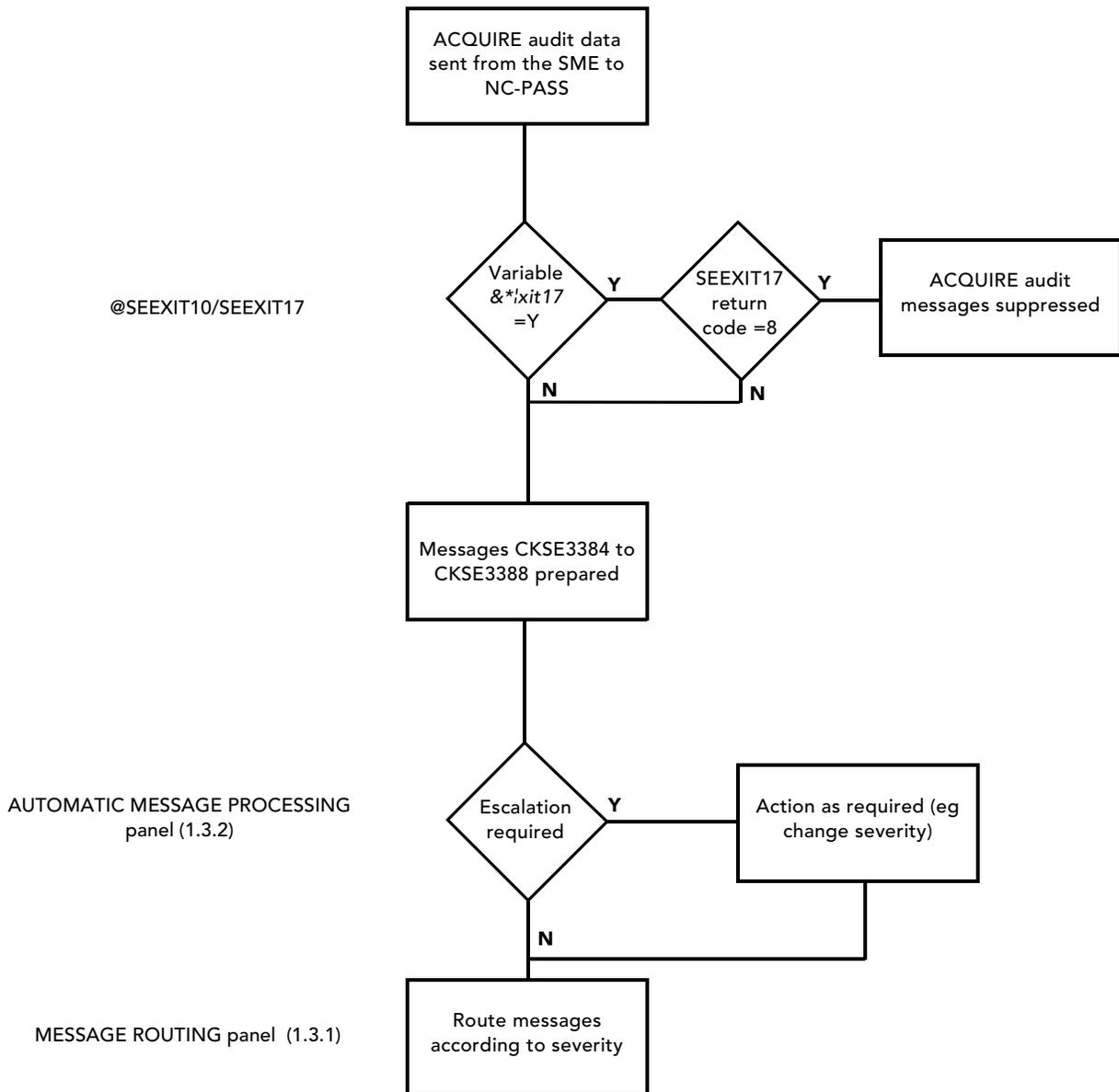
Audit trail facilities are provided for each of these actions. The diagrams on the following pages explain the audit process for each of the actions. It is assumed that:

- control table testing is complete
- the control table has been successfully loaded
- the SME is active
- XMS is active.

Note: The SME always sends audit data for actions of ACQUIRE, DENY and WARN.

ACQUIRE

The following diagram explains the audit process for an action of ACQUIRE.

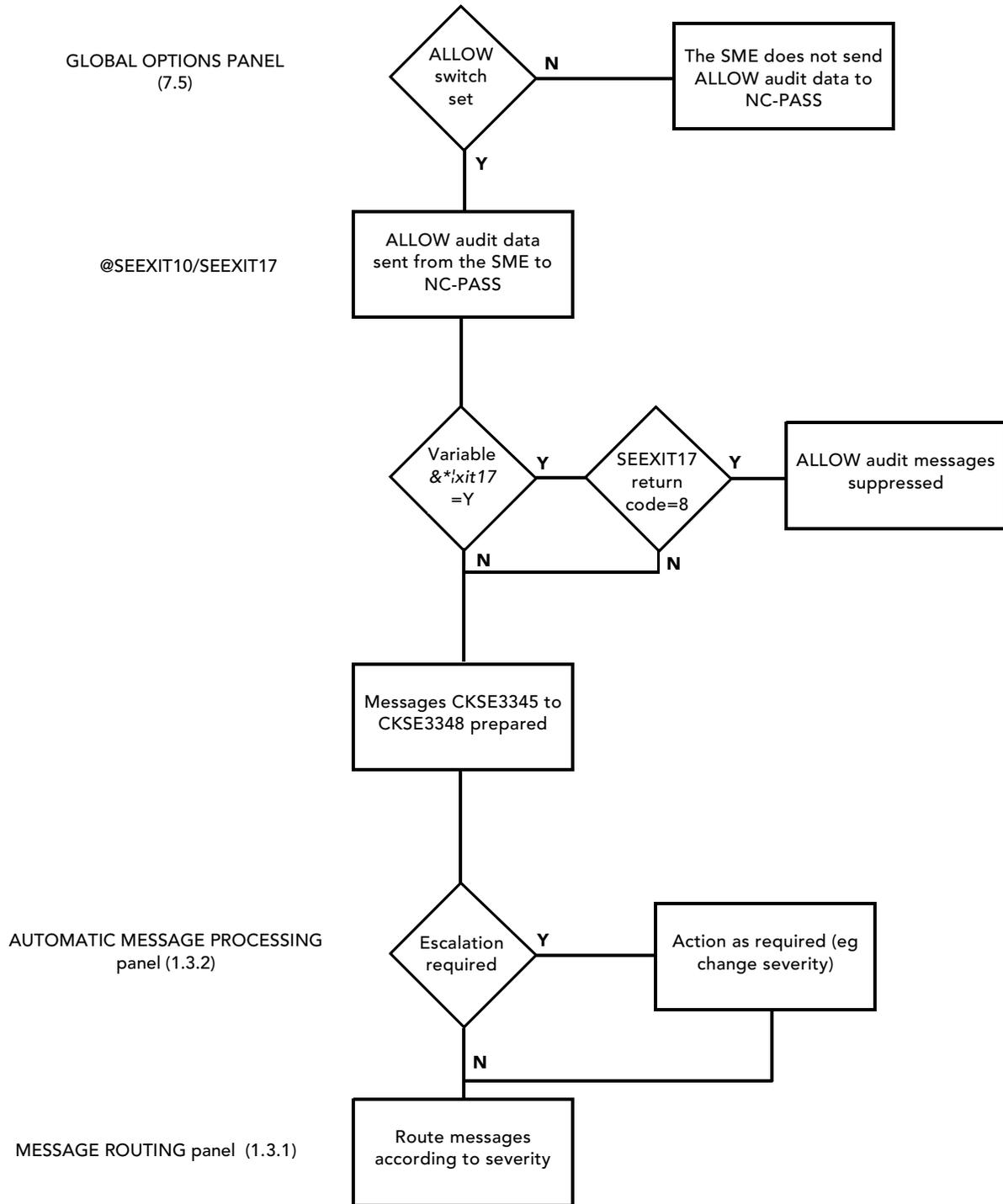


The SME always sends audit data to NC-PASS for ACQUIRE actions. If required these can be selectively suppressed using exit SEEXIT17. Refer to *Chapter 5 - Exit processing* (Volume 2) for further details.

Five ACQUIRE audit messages are produced; CKSE3384 through CKSE3388. These messages are severity level 4 (System information messages). Using the AUTOMATIC MESSAGE PROCESSING panel (1.3.2) and the MESSAGE ROUTING panel (1.3.1), you can route the messages according to your audit requirements, the principles of which are discussed in the section describing the ALLOW action messages. Refer also to the sections entitled *Message routing* on page 9.4 and *Automatic message processing overview* on page 9.3 for further details.

ALLOW

The following diagram explains the audit process for an action of ALLOW.



Filtering ALLOW audit messages

If you do not want to produce any audit messages for an action of ALLOW, set the ALLOW switch on the GLOBAL OPTIONS panel (7.5) to N. Refer to *Chapter 7 - The VTAM Session Security Exit (VSSE)* for further details.

Note: If the ALLOW switch is set to Y, every session initiation request will result in audit data being sent cross memory to NC-PASS. If the ALLOW switch is set to N, audit data will be sent only for those session initiation requests that result in action of DENY or WARN.

You can use SEEXIT17 to filter any audit message. For example, you can process ALLOW audit messages for a particular SSCP only and suppress those for all other SSCPs. Refer to *Chapter 5 - Exit processing (Volume 2)* for further details.

Four ALLOW audit messages are produced; CKSE3345 through CKSE3348. These messages are severity level 4 (System information messages). Using the AUTOMATIC MESSAGE PROCESSING panel (1.3.2) and the MESSAGE ROUTING panel (1.3.1), you can, for example, suppress any of these four while allowing the others to continue. An example of this is given below.

Example

The ALLOW switch on the GLOBAL OPTIONS panel (7.5) is set to Y. Variable `&*ixit17` is set to N in `@SEEXIT0` which means that exit SEEXIT17 will not be executed and no filtering of audit messages will occur.

Audit message CKSE3346-4 is to be sent to the NCI log; none of the other messages are required. The MESSAGE ROUTING panel (1.3.1) has been set as follows:

```

Date:12/12/1997                MESSAGE ROUTING                Userid:TSG0001
Time:09:00                    Terminal:A01MS262

Every message has a severity level. Enter 'X' in the table to route the
message. (Note that zero is the highest severity).

Output Route                Message Severity Level          Text
                             0  1  2  3  4  5  6  7  8  9  messages
User                        => -  -  -  -  -  X  X  -  X  X  => X
Console                    => -  -  -  X  -  X  -  -  -  -  => -
Console Non/Delete         => -  -  -  -  -  -  -  -  -  -  => -
NC-PASS Message Log       => -  -  -  X  X  X  X  -  X  -  => X
NCI Log                    => -  -  -  X  X  X  X  -  X  X  => X
Archive                    => -  -  -  -  -  -  -  -  -  -  => -
NetView                    => -  -  -  -  -  -  -  -  -  -  => -
SMF                        => -  -  -  -  -  -  -  -  -  -  => -
SMF Record Type           => ____ (128-255)
MHO                        => -  -  -  -  -  -  -  -  -  -  => -
MHO Nodename               => _____

F1=Help  F3=End  F12=Can

```

For details of this panel, refer to the section entitled *Message routing* on page 9.4.

The AUTOMATIC MESSAGE PROCESSING panel (1.3.2) has the following entries:

```

Date:12/12/1997          AUTOMATIC MESSAGE PROCESSING          Userid:TSG0001
Time:09:00                Terminal:A01MS262

----- SELECTION -----          ----- ACTION -----
- TIME -                          ALTERNATE
ID  FREQ PERIOD  START END TERM USER  TERM USER SEV  MESSAGE
000001 3345  00  00:00  00:00 23:59 Y  N           0
000002 3347  00  00:00  00:00 23:59 Y  N           0
000003 3348  00  00:00  00:00 23:59 Y  N           0
***** **** *  ***** ***** *  *           *  *  *           ****

F1=Help  F3=End  F7=Up  F8=Down  F12=Can

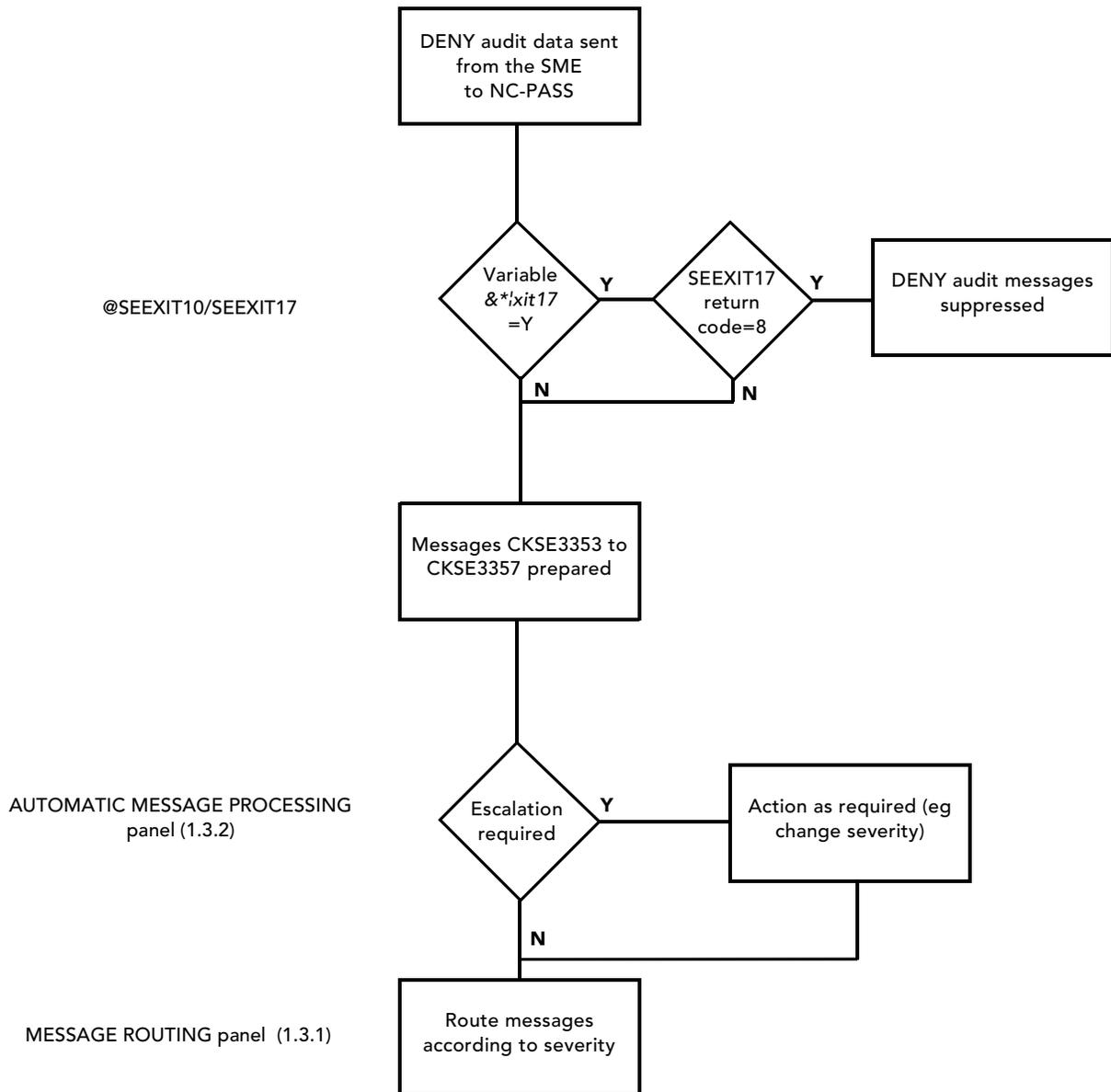
```

For details of this panel refer to the section entitled *Automatic message processing overview* on page 9.3.

Messages CKSE3345, CKSE3347 and CKSE3348 have been escalated to severity 0. The MESSAGE ROUTING panel (1.3.1) shows that messages with severity level 0 are not routed to any destination. Message CKSE3346 which has severity level 4 will be routed to the NC-PASS Message log and the NCI log.

DENY

The following diagram explains the audit process for an action of DENY.

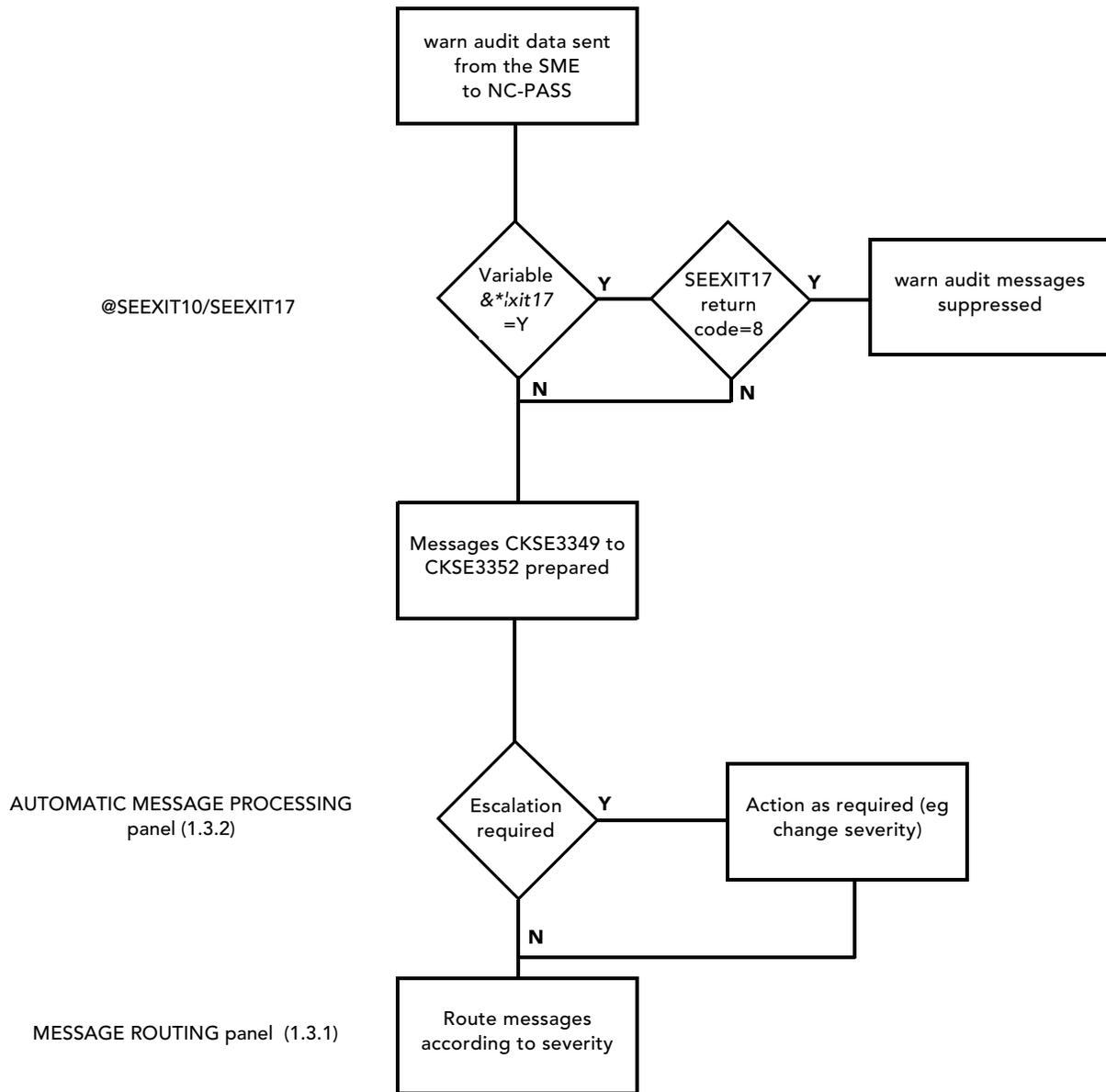


The SME always sends audit data to NC-PASS for DENY actions. If required these can be selectively suppressed using exit SEEXIT17. Refer to *Chapter 5 - Exit processing* (Volume 2) for further details.

Five DENY audit messages are produced; CKSE3353 through CKSE3357. These messages are severity level 4 (System information messages). Using the AUTOMATIC MESSAGE PROCESSING panel (1.3.2) and the MESSAGE ROUTING panel (1.3.1), you can route the messages according to your audit requirements, the principles of which are discussed in the section describing the ALLOW action messages. Refer also to the sections entitled *Message routing* on page 9.4 and *Automatic message processing overview* on page 9.3 for further details.

WARN

The following diagram explains the audit process for an action of WARN.



The SME always sends audit data to NC-PASS for WARN actions. If required these can be selectively suppressed using exit SEEXIT17. Refer to the NC-PASS Reference Manual *Chapter 5 - Exit processing* (Volume 2) for further details.

Four WARN audit messages are produced; CKSE3349 through CKSE3352. These messages are severity level 4 (System information messages). Using the AUTOMATIC MESSAGE PROCESSING panel (1.3.2) and the MESSAGE ROUTING panel (1.3.1), you can route the messages according to your audit requirements, the principles of which are discussed in the section describing the ALLOW action messages. Refer also to the sections entitled *Message routing* on page 9.4 and *Automatic message processing overview* on page 9.3 for further details.

Browsing the NC-PASS message log

A list of NC-PASS logged messages is provided by the BROWSE NC-PASS LOG panel (3) as shown below.

```
----- BROWSE NC-PASS LOG ----- Line 0 Col 1 80
Command => _____ Scroll => CSR

Date => * _____ DD/MM/YYYY Time => * _____ HH:MM:SS
Term => * _____ User => * _____ Msgid => * _____

***** TOP OF DATA *****
12/12/1997 09:59:49          SYSTEM  CKSE3612-4  NC-PASS SECURE
12/12/1997 09:59:50          SYSTEM  CKSE0534-4  SYSTEM INITIALIZATION STARTED
12/12/1997 10:00:30          SYSTEM  CKSE0535-4  SYSTEM INITIALIZATION COMPLETED
12/12/1997 10:01:20 A01MS043 MASTER  CKSE0500-6  LOGON - DEST=SEMENU00
***** BOTTOM OF DATA *****

F1=Help F3=End F5=Rfind F6=Print F7=Up F8=Down F9=Nlog F10=Left F11=Right
```

The number of lines available for display in this panel is determined by the **Length of log field** in the GENERAL SYSTEM OPTIONS panel (1.1).

Selecting messages for display

The five data fields at the top of the BROWSE NC-PASS LOG panel allow selection criteria to be specified in terms of date, time, terminal id, user id and message number. Specific or generic values may be entered. Generic entries are specified with an asterisk (*) or a plus sign (+) or both.

An asterisk shows that only characters preceding the asterisk are to be matched, as in the following example:

User=> ABC*

This selection will list all messages issued for userids beginning with the characters ABC.

A plus sign shows that any character in that position will be matched for selection, as in the following example:

User=> A+C*

This selection will list all userids beginning with the character A, having any character in the second position and the character C in the third position. Any combination of characters may follow the character C.

Input fields.

Command	Description
	To scroll the log in a specified direction, enter one of the following commands:
	UP <i>amount</i>
	DOWN <i>amount</i>
	LEFT <i>amount</i>
	RIGHT <i>amount</i>
	where <i>amount</i> is one of the following values:
	csr scrolls the line or column of data indicated by the cursor to the top, bottom, left or right of the page (the cursor must be positioned at the appropriate place after the command has been typed in, but before pressing <Enter>.)
	max scrolls the log to the end of the display area.
	page scrolls the log by one page.
	half scrolls the log by half a page.
	To find a specific occurrence in the log of a data string, enter one of the following commands:
	FIND <i>string</i> [<i>parameter</i>]
	RFIND
	where <i>string</i> is the data string to be found.
	The starting point and direction of the search are provided by <i>parameter</i> as follows:
	first begins the search at the start of the log (this is the default).
	last begins the search at the end of the log.
	prev begins the search immediately before the cursor. (The cursor must be positioned at the appropriate place after the command has been typed in, but before pressing <Enter>.) The search will proceed from the cursor to the start of the log.
	next begins the search immediately after the cursor. (The cursor must be positioned at the appropriate place after the command has been typed in, but before pressing <Enter>.) The search will proceed from the cursor to the end of the log.
	The RFIND command repeats the previous FIND command.
	To close the current panel and return to the previously displayed panel, enter the END command.

Description

Scroll	<p>Defines the amount of data that is scrolled. This can be set to one of the following values:</p> <ul style="list-style-type: none">PAGE scrolling will reposition the viewing window by one page in the requested direction.HALF scrolling will reposition the viewing window by half a page in the requested direction.CSR scrolling will reposition the viewing window such that the TOP, BOTTOM, LEFT or RIGHT of the screen will display the line or column at the current cursor position.MAX scrolling will position the viewing window as far as possible in the requested direction.<i>nnnn</i> scrolling will move the viewing window <i>nnnn</i> rows or columns in the requested direction. Leading zeros need not be specified.
Date	<p>the date or generic date which specifies the day or days when the required messages were generated. The date must be in the format shown in brackets next to this field.</p>
Time	<p>the time or generic time which specifies the period in which the required messages were generated. The time must be in the format shown in brackets next to this field.</p>
Term	<p>the specific or generic id of the terminal on which the required messages were generated.</p>
User	<p>the userid or generic userid of the user(s) associated with the required messages.</p>
Msgid	<p>the specific or generic number of the message(s) that you require to be listed. A message is constructed as follows:</p> <ul style="list-style-type: none">Company identifier - two charactersSystem identifier - two charactersMessage - four numeric digitsHyphen - one digitSeverity code - one digit

Function keys

Key	Function
F1	displays help information.
F3	returns to the previously displayed panel.
F5	repeats a previous FIND command. (This is equivalent to an RFINd command.)
F6	prints a report of the displayed log.
F7	presents the previous screen of the log. (This is equivalent to an UP command.)
F8	presents the next screen of the log. (This is equivalent to a DOWN command.)
F9	switches the display to the NCI log.
F10	scrolls the log to the left. (This is equivalent to a LEFT command.)
F11	scrolls the log to the right. (This is equivalent to a RIGHT command.)

NCI log control

Messages can be routed to the NCI log, as described in the section entitled *Message routing* on page 9.4. There are two NCI log datasets which can be switched either immediately or at a specific time of day.

The NCI LOG CONTROL panel

The NCI LOG CONTROL panel (1.3.4) provides the NCI log switching facility as shown below.

```
Date:12/12/1997          NCI LOG CONTROL          Userid:TSG0001
Time:09:00              Terminal:A01MS262

The NCI log files can be switched automatically at a given time each day, type
the time of day below:

    Time Hours   => 23 Leave both entry fields blank if automatic switching
    Minutes => 55 is not required

Press <F9> to switch NCI log files immediately:

    Current NCILOG file => NCILOG2

F1=Help  F3=End  F9=Log switch
```

Input fields

Field	Description
Time	Messages that are routed to the NCI log are written either to NCILOG1 or NCILOG2. You can switch these log datasets at a specific time of day by entering the daily switch time and pressing F3. If you do not want automatic switching, leave both fields blank.

Display fields

Field	Description
Current NCILOG file	Either NCILOG1 or NCILOG2.

Function Keys

Key	Function
F1	displays help information.
F3	saves a permanent record of any changed data and returns to the MESSAGE MAINTENANCE MENU.
F9	instantly switches the logs.

Overflow records

Non NC-PASS text messages can be routed to the NCI log and processed accordingly. If these messages are too long to be displayed on the screen, for example some produced by RACF, these can now be written by appending an overflow record. The message text of such a message is continued onto an overflow record prefixed with an upper case O.

This facility is automatically enabled unless variable `&*icus03` is set to NO in exit `@SEEXIT0`.

The ARCHIVE FILE CONTROL panel

The ARCHIVE FILE CONTROL panel (1.3.5) provides the facility to assign archive files for messages that have been designated for archiving by a message severity level (see the MESSAGE ROUTING panel in the section entitled *Message routing* on page 9.4).

Up to nine archive files may be defined in the ARCHIVE FILE CONTROL panel by entering the file name of each on successive lines. The files are VSAM ESDSs which are created by using AMS (Access Method Services). If fewer than nine files are specified, the first blank line will indicate the end of a 'set' of files, and all subsequent files will be ignored. The files can be switched from one to another on a daily basis by entering a time to switch over. If, for example, seven file names are entered and the system is running continuously over a seven day period, the files will be switched each day at a specified time. The cycle will repeat from the eighth day. If the system is closed at switch over time, the files will be switched when the system is next active at the specified time.

The current file is indicated on the panel as being 'Open' to the right of the file name.

```

Date:12/12/1997                ARCHIVE FILE CONTROL                Userid:TSG0001
Time:09:00                      Terminal:A01MS262

To open a file, type the number of the file below and press <F5>:
  Open file number => _

Specify the time to automatically switch archive files below:
  Hour => 00 HH  Minutes => 59 MM

Enter the names of the files to be used for archiving below:
  File 1 => DEV.ARCHIVE.FILE1                                     Open
  File 2 => DEV.ARCHIVE.FILE2
  File 3 => DEV.ARCHIVE.FILE3
  File 4 => _____
  File 5 => _____
  File 6 => _____
  File 7 => _____
  File 8 => _____
  File 9 => _____

Press <F6> to close active file.

F1=Help  F3=End  F5=Open  F6=Close

```

Input fields

Field	Description
Open file number	Enter a file number in the range 1 to 9 (as listed in the panel) of the file to be switched to when <F5> is pressed.
Hour /Minutes	Enter the daily switch over time for the automatic switching of the current archive file to the next file in sequence (as listed in the panel).
File 1 through File 9	Enter a VSAM ESDS file name to be used for archiving. The names of nine files can be entered to allow switching from one to another. Files can be switched automatically on a daily basis by entering the time in the Hour and Minutes fields, or switched directly by entering the name of the file to be opened in the Open file number field and pressing <F5>. Specific allocation of files through DD names using JCL is not required. Files are dynamically allocated.

Function keys

Key	Function
F1	displays help information.
F3	saves any changes and returns to the MESSAGE MAINTENANCE MENU.
F5	switches directly from the currently open file to the file number entered at the Open file number field.
F6	closes the current file without opening another file.

Factors affecting archive file control

For an archive file to be written to, the following four conditions must be met:

- the file must be open
- there must be at least one 'X' marked in the archive output row of the MESSAGE ROUTING panel
- the file must be specified in the ARCHIVE FILE CONTROL panel
- the file must have sufficient space to allow additional records to be written to it.

Even if a file is specified in the ARCHIVE FILE CONTROL panel, it is not accessible unless it is opened.

If there are insufficient files listed in the panel, or there are blank lines in the list, the routing of messages will revert to the first file in the list, and if this is full, archiving will cease (the presence of a blank line implies that no further files have been specified).

Examples of archive file control are provided on the next page.

Overflow records

Non NC-PASS text messages can be routed to specific destinations and processed accordingly. If these messages are too long to be displayed on the screen, for example some produced by RACF, these can now be written by appending an overflow record. The message text of such a message is continued onto an overflow record prefixed with an uppercase o (O).

This facility is automatically enabled unless variable `&*!cus04` is set to NO in exit `@SEEXIT0`.

Example 1

In this example, three consecutive files are listed. These three files will not be sufficient for the quantity of messages being sent and therefore each file will fill up in turn. When the third file is full the system will revert to the first file, and as the first file is full, message archiving will cease.

```
Date:12/12/1997                ARCHIVE FILE CONTROL                Userid:TSG0001
Time:09:00                    Terminal:A01MS251

To open a file, type the number of the file below and press <4F45>:
  Open file number => _

Specify the time to automatically switch archive files below:
  Hour => 00 HH  Minutes => 59 MM

Enter the names of the files to be used for archiving below:
  File 1 => DEV.ARCHIVE.FILE1                                Open
  File 2 => DEV.ARCHIVE.FILE2
  File 3 => DEV.ARCHIVE.FILE3
  File 4 => _____
  File 5 => _____
  File 6 => _____
  File 7 => _____
  File 8 => _____
  File 9 => _____

Press <F6> to close active file.

F1=Help  F3=End  F5=Open  F6=Close
```

Example 2

In this case, there are sufficient files listed, but with blank lines inadvertently inserted. The system will take the first blank line (following file 3) as the end of the list and revert to the first file. If the first file is full, archiving will cease.

```
Date:12/12/1997                ARCHIVE FILE CONTROL                Userid:TSG0001
Time:09:00                    Terminal:A01MS251

To open a file, type the number of the file below and press <F5>:
  Open file number => _

Specify the time to automatically switch archive files below:
  Hour => 00 HH  Minutes => 59 MM

Enter the names of the files to be used for archiving below:
  File 1 => DEV.ARCHIVE.FILE1                                Open
  File 2 => DEV.ARCHIVE.FILE2
  File 3 => DEV.ARCHIVE.FILE3
  File 4 => _____
  File 5 => _____
  File 6 => _____
  File 7 => DEV.ARCHIVE.FILE7
  File 8 => _____
  File 9 => DEV.ARCHIVE.FILE9

Press <F6> to close active file.

F1=Help  F3=End  F5=Open  F6=Close
```

Viewing archived and SMF messages

The SELECT ARCHIVE AND SMF MESSAGES panel (1.3.6) allows archived and SMF messages to be selected for viewing or printing.

Making ESDS copies of SMF records

An SMF record cannot be viewed directly. An ESDS copy of an SMF record must therefore be created using the JCL supplied in member SMFVSM of the CNTL dataset, and the name of the ESDS copy entered at the **ESDS DSN** prompt. In this case the SMF record type must be entered at the **SMF record type** prompt to select the appropriate type for viewing. Refer to the section entitled *Message processing using SMF files* on page 9.40.

```
Date:12/12/1997          SELECT ARCHIVE AND SMF MESSAGES          Userid:TSG0001
Time:09:00                Terminal:A01MS264

Type the name of the ESDS from which archived messages are to be selected:
  ESDS dataset name => _____
If the dataset was extracted from SMF, type the SMF record type below:
  SMF record type => ___ 128-255

Type any required search conditions below and press <ENTER> to browse or
press <F6> to print:
  Date           => * DD   => * MM   => * ____ YYYY
  Time           => * HH   => * MM
  System         => * _____
  Jobname        => * _____
  Terminal       => * _____
  User Id        => * _____
  Message Id     => * ____ 0000-9999
  Severity       => * ____ 0-9
  Remote         => * ____ Y/N
  Selection limit => 999 1-999

F1=Help  F3=End  F6=Print
```

Input fields

Field	Description
ESDS DSN	Enter the name of the entry sequenced dataset from which the messages are to be selected.
SMF record type	Enter the SMF record type of an SMF record to be viewed (which has been copied into the ESDS named above. Refer to the section entitled <i>Message processing using SMF files</i> on page 9.40). The SMF record type can be in the range 128 through 255, depending on the record type used to route messages to the SMF in the MESSAGE ROUTING panel. Only NC-PASS messages will be displayed. This entry will select the appropriate type from the ESDS copy for viewing.

Search criteria

Generic search criteria can be entered by entering an asterisk (*) after the specific characters to be matched. For example userids TSG0001 through TSG0099 can be selected by entering TSG00* in the **User Id** field.

A single asterisk (*) in any search field means the search is not constrained by this search field.

Field	Description
Date	Enter the elements of the date on which a match is to be performed (the date a message was issued).
Time	Enter the elements of the time on which a match is to be performed (the time a message was issued).
System	Enter the SMFID of the system under which NC-PASS is currently running.
Jobname	Enter the jobname(s) on which a match is to be performed (the NC-PASS job(s) which issued the messages).
Terminal	Enter the id of the destination terminal(s) on which a match is to be performed (the terminal(s) which caused the messages to be issued).
Userid	Enter the destination userid(s) on which a match is to be performed (the userid(s) which caused the messages to be issued).
Message Id	Enter the message number(s) on which a match is to be performed. Message numbers can be in the range 0000-9999.
Severity	Enter the message severity level(s) on which a match is to be performed.
Remote	Enter Y to limit messages to those generated remotely. Enter N to limit messages to those generated locally. Enter an asterisk (*) to select both local and remote.
Selection limit	Enter the maximum number of messages to select.

Function keys

Key	Function
F1	displays help information.
F3	closes this panel and returns you to the USER PROFILE MAINTENANCE MENU panel.
F6	prints the selected messages.

MHO routed messages

The ability to route messages via MHO allows messages to be accumulated in one place and the possibility of alerting operators on one system of events occurring on another.

Incoming MHO messages from other NC-PASS jobs can be routed to all 'Output Route' destinations except User.

MHO message routing occurs once only. If NC-PASS (A) routes a message to NC-PASS (B), and if NC-PASS (B) is set up to pass the same message severity level to NC-PASS (C), the message will *not* be passed to NC-PASS (C). This avoids the possibility of recursively passing a message between linked NC-PASSes.

Message escalation only occurs on the originating NC-PASS. When messages are received from another NC-PASS, they are not subject to automatic message processing as specified in the AUTOMATIC MESSAGE PROCESSING panel on the receiving system.

If the MESSAGE ROUTING panel (1.3.1) determines that the message will be added to the NC-PASS log, the updated BROWSE NC-PASS LOG panel will include the message as shown in the panel below.

```
----- BROWSE NC-PASS LOG ----- Line 0 Col 1 80
Command => _____ Scroll => CSR

Date => * _____ DD/MM/YYYY Time => * _____ HH:MM:SS
Term => * _____ User => * _____ Msgid => * _____

***** TOP OF DATA *****
12/12/1997 09:59:49 SYSTEM CKSE3612-4 NC-PASS SECURE
12/12/1997 09:59:50 SYSTEM CKSE0534-4 SYSTEM INITIALIZATION STARTED
12/12/1997 10:00:30 SYSTEM CKSE0535-4 SYSTEM INITIALIZATION COMPLETED
12/12/1997 10:01:20 A01MS043 MASTER CKSE0500-6 LOGON - DEST=SEMENU00
12/12/1997 10:01:54 SYSTEM CKSE0061-6 YOUR PASSWORD HAS EXPIRED - CHA
***** BOTTOM OF DATA *****

F1=Help F3=End F5=Rfind F6=Print F7=Up F8=Down F9=Nlog F10=Left F11=Right
```

Message processing using SMF files

The procedure for writing messages to SMF files is described in the following three steps:

1. In the MESSAGE ROUTING panel (1.3.1), indicate the message severity levels which apply to the messages you require to be routed to SMF files. Also specify the SMF record type (in the range 128 to 255). The MESSAGE ROUTING panel is described in the section entitled *Message routing* on page 9.4.
2. Ascertain the status of the current SMF files in use. This will tell you whether the record type you have specified in the MESSAGE ROUTING panel can be written to the SMF file.

To provide this information, enter the following command at the system console:

```
D SMF,O
```

This command displays:

- the member of SYS1.PARMLIB (the system parameter list) which is currently in use, as provided by MEMBER=SMFPRMxx
 - the parameters contained in the above member, one of which lists the record types to be written to the SMF file.
3. If the record type that was specified on the MESSAGE ROUTING panel is not on the list provided by the D SMF,O command, messages will not be written to the SMF file. This can be remedied by adding the record type to the list as follows:
 - edit the SMFPRMxx member to include the record type
 - at the system console enter T SMF=xx
 - confirm the addition by entering D SMF,O.

Reading and displaying records written to SMF files

NC-PASS cannot report directly from an SMF file. A batch job can, however, be set up to extract records of the appropriate record type and write them to a temporary file. The same batch job can then copy the temporary file to an ESDS file which can then be read.

The JCL to run this batch job is distributed with NC-PASS in member SMFVSM of the CNTL dataset. This JCL is listed on the following page.

An ESDS copy of an SMF file can be displayed by entering the ESDS dataset name and the SMF record type at the appropriate prompts on the SELECT ARCHIVED MESSAGE panel (refer to the section entitled *Viewing archived and SMF messages* on page 9.34).

Supplied JCL to copy an SMF file to an ESDS VSAM file

Note: If the following JCL is used to copy records into an ESDS VSAM file, the first two fields (SMFDLEN and SMFDOSEG) are stripped off and the record starts at SMFDOFLG. See record layout on the next page.

```
//*JOB CARD JOB (ACNT), 'SMF REPRO', CLASS=?, MSGCLASS=?
/*****\
/* THIS JCL: *
/* - DEFINES AN ESDS IN THE FORMAT REQUIRED FOR VIEWING *
/* SMF MESSAGES FROM NC-PASS *
/* - CREATES A TEMPORARY FILE TO CONTAIN NC-PASS MESSAGES *
/* EXTRACTED FROM THE SMF DATASET *
/* - REPRO'S THE TEMPORARY FILE TO THE ESDS DEFINED IN STEP 1 *
/* *
/*****\
/* MAKE THE FOLLOWING CHANGES TO THIS PARAMETER MEMBER :- *
/* *
/* *VSAMPFX* - ALL OCCURRENCES TO VSAM HIGH LEVEL QUALIFIER *
/* *VSAMVOL* - ALL OCCURRENCES TO VOLUME FOR ALLOCATION *
/* *CATVOL* - IF USER CATALOG REQUIRED *
/* *
/*****\
//ALLOC EXEC PGM=IDCAMS, REGION=412K
//*STEP CAT DD DSN=CATALOG.MVSICF1.V*CATVOL*, DISP=SHR
//SYS PRINT DD SYSOUT=*
//SYS IN DD *
DELETE (*VSAMPFX*.SMF) CLUSTER PURGE
DEFINE CLUSTER -
( NAME(*VSAMPFX*.SMF) -
TRACKS(5 1) -
NONINDEXED -
SHR(2 3) -
RECORDSIZE(130 130) -
VOLUME(*VSAMVOL*)) -
DATA -
( NAME(*VSAMPFX*.SMF.DATA) )
/*
//DUMP EXEC PGM=IFASMFDP, REGION=512K
/* SELECT SMF DATASET
//IN DD DSN=SYS1.MAN1, DISP=SHR
//OUT DD DSN=&TEMP, DISP=(NEW, PASS),
// UNIT=V10, SPACE=(CYL, (10, 10))
//SYS PRINT DD SYSOUT=*
/* SELECT APPROPRIATE SMF RECORD TYPE
//SYS IN DD *
INDD(IN, OPTIONS(DUMP))
OUTDD(OUT, TYPE(208))
/*
//REPRO EXEC PGM=IDCAMS, REGION=512K
//SYS PRINT DD SYSOUT=*
//IN DSN DD DSN=&TEMP, DISP=(OLD, DELETE)
//OUT DSN DD DSN=*VSAMPFX*.COPY, DISP=SHR
//SYS IN DD *
REPRO INFILE(IN DSN) -
OUTFILE(OUT DSN)
```

NC-PASS message record layout (as written to SMF)

The layout of NC-PASS message records written to SMF is as follows:

Offsets Dec Hex	Name	Length	Format	Source	Description
0 0	SMFD0LEN	2	binary	internal	Record length
2 2	SMFD0SEG	2	binary	internal	Segment descriptor
4 4	SMFD0FLG	1	binary	SVC83	System indicator Bit Meaning when set 0-4 Reserved 5 MVS/XA 6 VS2 7 Reserved
5 5	SMFD0RTY	1	binary	internal	Record type
6 6	SMFD0TME	4	binary	SVC83	Time, in hundredths of a second, record was moved to buffer
10 A	SMFD0DTE	4	packed	SVC83	Date record was moved to SMF buffer in the form 0CyydddF where: C is the century, ie 0 = 19yy 1 = 20yy F is the sign
14 E	SMFD0SID	4	EBCDIC	SMCASID	System identification (taken from SID parameter)
18 12	SMFD0JBN	8	EBCDIC	internal	The jobname of the NC-PASS job which issued the message
26 1A	SMFD0SP1	1	EBCDIC	internal	Blank
27 1B	SMFD0TRM	8	EBCDIC	internal	The terminal id for which the message was issued
35 23	SMFD0SP2	1	EBCDIC	internal	Blank
36 24	SMFD0USR	8	EBCDIC	internal	The userid for which the message was issued
44 2C	SMFD0SP3	1	EBCDIC	internal	Blank
45 2D	SMFD0COY	2	EBCDIC	internal	Company code (constant 'CK')
47 2F	SMFD0PRD	2	EBCDIC	internal	System code (constant 'SE')
49 31	SMFD0SER	4	EBCDIC	internal	Message serial number (0001 to 9999)
53 35	SMFD0HYP	1	EBCDIC	internal	Message severity level (0 to 9)
54 36	SMFD0SEV	1	EBCDIC	internal	Message severity level (0 to 9)
55 37	SMFD0SP4	1	EBCDIC	internal	Blank
56 38	SMFD0TXT	variable	EBCDIC	internal	Message text

NC-PASS message record layout (as written to archive ESDS files)

The layout of EBCDIC format message records written to archive ESDS files is as follows:

Offsets Dec Hex		Length	Description
0	0	6	Date (yymmdd) Note: To comply with year 2000 requirements: <ul style="list-style-type: none"> • when the year (yy) is 00 through 83, a format of 20yy is assumed • when the year (yy) is 84 through 99, a format of 19yy is assumed
6	6	6	Time (hhmmss)
12	C	4	The SMFID for MVS under which NC-PASS is running
16	10	8	The jobname of the NC-PASS job that issued the message
24	18	1	0 message produced locally (by this NC-PASS job) 1 message received by this NC-PASS job via MHO having been generated by a remote NC-PASS job.
25	19	8	The terminal id for which the message was issued
33	21	8	The userid for which the message was issued
41	29	2	Company code (constant 'CK')
43	2B	2	System code (constant 'SE')
45	2D	4	Message serial number (0001 to 9999)
49	31	1	Serial number delimiter (constant '-')
50	32	1	Message severity level (0 to 9)
51	33	1	Blank
52	34	75	Message text

This page intentionally left blank

Chapter 10 - Printing and displaying reports

The Printer Control Table (PCT)	10.2
Sample code defining a PCT	10.3
Report data extraction	10.4
Encryption	10.4
CAF record formats	10.5
Logon statistics	10.12
Producing a summary by date	10.13
Producing a full report	10.15
Producing reports from administration panels	10.16
VTAM printing	10.16

The Printer Control Table (PCT)

The Printer Control Table (PCT) is designed to provide escape sequences for multiple VTAM printers in an IBM network. A PCT is an assembled load module which must reside in a library in the STEPLIB chain of the NC-PASS job. The PCT forms part of the data sent to the print destination and consists of three separate areas, to define:

- initialization escape sequence
- special print functions
- termination escape sequence.

Escape sequences are special characters that instruct a printer what to do in a given situation. The initialization and termination escape sequences are device dependent and are concerned with such matters as skipping to the top of a page. The special function escape sequence is concerned with bold face, overtyping etc.

If no explicit PCT is specified in the panel, the system defaults to an EPSON LQ1500 model.

There are two PCTs contained in the load library:

- IOPNSCS - supports any non-SNA Character Strings (SCS) printer; SCS printers are defined as LU1 devices to VTAM
- IOP52023 - supports the IBM 5202-3 QUIET WRITER.

Note: These two PCTs are shipped as load modules and their source code is not accessible.

Sample code defining a PCT

```
*****
** PRINTER CONTROL TABLE FOR NON SCS PRINTER                               **
** NOTE - NON SCS PRINTERS CAN BE DRIVEN IN SDLC MODE                       **
**     NON SDLC MODE (STARTSTOP, CHAN ATTACHED OR BSC)                     **
*****
INIT    DC    AL4(INITAREA)    ADDRESS OF INITIALIZATION AREA
PARM    DC    AL4(INITAREA)    ADDRESS OF PARAMETER AREA
REST    DC    AL4(RESTAREA)    ADDRESS OF RESET PRINTER AREA
*****
** INITIALIZATION AREA                                                     **
** AMEND THE INITIALIZATION STRING(S) AS REQUIRED                           **
*****
INITAREA DC    AL2(INITLEN-2)    LENGTH OF INITIALIZATION AREA
          DC    X'0D'            CARRIAGE RETURN ONLY
INITLEN  EQU    *-INITAREA
*****
** PARAMETER AREA                                                         **
** ADD 3 BYTE OPTION AND CORRESPONDING STRING AS REQUIRED                   **
** STRING IS NOT NECESSARY IN ALL CASES                                   **
*****
PARMAREA DS    OH
PARMLEN  EQU    *-PARMAREA
          DC    X'FFFFFFF'        END OF TABLE INDICATOR
*****
** RESET PRINTER AREA                                                     **
** AMEND STRINGS AS REQUIRED                                               **
*****
RESTAREA DC    AL2(RESTLEN-2)    LENGTH OF RESET PRINTER AREA
          DC    X'0D'            CARRIAGE RETURN ONLY
RESTLEN  EQU    *-RESTAREA
          END
```

Notes

The string of characters after the INITAREA label defines the special sequence of commands sent to the printer before each print request. In the above example a simple carriage return X'0D' is used to initialize the printer.

The parameter area is that part of the PCT used for defining special print functions. NC-PASS does not currently support these options, so only a dummy parameter need be defined here.

The string of characters following the RESTAREA label defines the special sequence of commands sent to the printer after each print request. In the above example a simple carriage return X'0D' is used to terminate the printer.

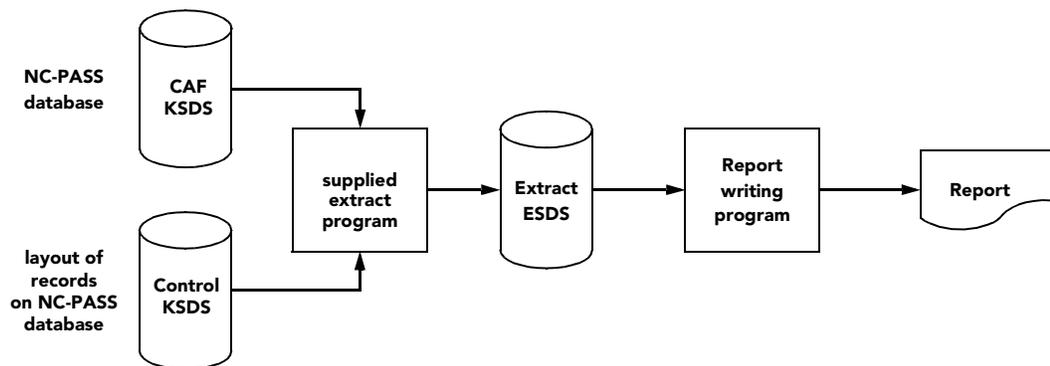
Report data extraction

NC-PASS provides a facility to extract detailed information from records in the Central Administration File (CAF), such as user profiles, terminal profiles, etc, and write this information to a VSAM ESDS file. The JCL to perform this function is provided on the product installation tape in the CNTL dataset member PRTDATA.

Extracted data can subsequently be used as input to a report writing program. You can write a report program in the language most suited to your installation, however a sample program written in the NCI/XF language has been provided (refer to JCL in the installation documentation). This sample program is provided in both the distributed panel and PBLIB libraries.

Note: You must have an NCI/XF license if you want to modify the sample. The version in the PBLIB library must be deleted for any modification to take effect.

The following diagram outlines the extract and report writing procedure.



All records in the extract ESDS file start with a 20 byte key. The first 2 bytes of the key define:

1. the group in which all similar record types are placed (for example, all records relating to user profiles will have a value of 1). This is placed in the first byte position.
2. the specific type of record (for example, user profile=0, user connect data=2). This is placed in the second byte position.

The rest of the key contains information that will vary according to record type.

Encryption

Passwords and other security sensitive data are encrypted. If you want other fields to be encrypted, refer to *WEXIT27 - the central administration file (CAF) read/write exit* on page 5.56 (Volume 2) for details of how to route records through a specified encryption/decryption procedure.

CAF record formats

The following records may be extracted from the CAF. The format of the extracted record is given in each case:

User profile record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	10
Profile userid	08	003	010	Specific or generic
(blank)	10	011	020	
Comments line 1	30	021	050	
Comments line 2	30	051	080	
Authority group	03	081	083	Specific or '*'
Authority level	03	084	086	Numeric 0 to 255
Authority type	05	087	091	USER,ADMIN,OPER
Password type	09	092	100	NONE,SAC,RACF,CA-ACF2 etc
Retry maximum	03	101	103	Numeric or 'N/A'
No logon before	05	104	108	Julian YYDDD format
No logon after	05	109	113	Julian YYDDD format
Update user	08	114	121	Last update by
Update date	05	122	126	Date last updated YYDDD
Update time	05	127	131	Time last updated HH:MM
Creation user	08	132	139	Created by
Creation date	05	140	144	Creation date
Creation time	05	145	149	Creation time
Initial menu	08	150	157	Initial menu
Passcode	01	158	158	Not applicable for NC-PASS Secure
Lock interval	02	159	160	Number of minutes

User connect data record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	12
Profile userid	08	003	010	Specific or generic
(blank)	10	011	020	
Code	08	021	028	ROUTINE:NODENAME:KEYWORD:MENU
Destination	08	029	036	
Terminal	08	037	044	Specific or generic
CINIT data	30	045	074	
Comments	19	075	093	

SME group header record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	15
Group name	08	003	010	
(blank)	10	011	020	
Comment	30	021	050	
Date of creation/update	05	051	055	YYDDD
Time of creation/update	05	056	060	HH:MM
User that created/updated	08	061	068	

SME group data record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	16
Group name	08	003	010	
(blank)	10	011	020	
Group data	40	021	060	
Data type	01	061	061	(blank)=data;F=field;S=symbolic name

SME rule data

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	17
Rule name	08	003	010	
(blank)	10	011	020	
Data indicator	01	021	021	R=rule; A=array; F=field; D=data
Rule data	31	022	052	See below for specific indicator type

SME rule data - data indicator R

Note: there are two entries for each rule.

Field	Length	From	To	Comment
First entry				
Default action	08	022	029	WARN, ALLOW, DENY
Date of creation/update	05	030	034	YYDDD
Time of creation/update	04	035	038	HHMM (no colon (:))
User	08	039	046	userid that last created/updated
Second entry				
Rule comment	31	022	052	

SME rule data - data indicator A**Note:** entries are grouped in pairs.

Field	Length	From	To	Comment
First entry				
Array comment	31	022	052	
Second entry				
Array name	08	022	029	
True action	08	030	037	NEXT, EXIT, ALLOW, WARN DENY, ACQUIRE
False action	08	038	045	NEXT, EXIT, ALLOW, WARN DENY, ACQUIRE

SME rule data - data indicator F

Field	Length	From	To	Comment
Field name	08	022	029	
Comparator	02	030	031	EQ or NE

SME rule data - data indicator D

Field	Length	From	To	Comment
Field name	08	022	029	
Data type	01	030	030	(blank)=literal data; G=group name; F=fieldname; V=symbolic name; D=date/time definition

Date/time header

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	18
Definition name	08	003	010	
(blank)	10	011	020	
Comment	30	021	050	
Date of creation/update	05	051	055	YYDDD
Time of creation/update	05	056	060	HH:MM
Userid that created/updated	08	061	068	

Date/time data

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	19
Definition name	08	003	010	
(blank)	10	011	020	
Monday access	01	021	021	Y or N
Tuesday access	01	022	022	Y or N
Wednesday access	01	023	023	Y or N
Thursday access	01	024	024	Y or N
Friday access	01	025	025	Y or N
Saturday access	01	026	026	Y or N
Sunday access	01	027	027	Y or N
Start date	05	028	032	YYDDD
End date	05	033	037	YYDDD
Start time	05	038	042	HH:MM
End time	05	043	047	HH:MM

Risk profile header

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	20
Header type	08	003	010	TERMHEAD/USERHEAD
(blank)	10	011	020	
Definition1 name	08	021	028	
Definition2 name	08	029	036	
Definition3 name	08	037	044	
Definition4 name	08	045	052	
Definition5 name	08	053	060	
Definition6 name	08	061	068	
Definition7 name	08	069	076	

Risk profile data

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	21
Header type	08	003	010	TERMDATA/USERDATA
(blank)	10	011	020	
Profile data	20	021	040	Userid or terminal id
Definition1 data	05	041	045	
Definition2 data	05	046	050	
Definition3 data	05	051	055	
Definition4 data	05	056	060	
Definition5 data	05	061	065	
Definition6 data	05	066	070	
Definition7 data	05	071	075	

Terminal lock record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	30
Terminal	08	003	010	Generic terminal id
(blank)	10	011	020	
Reason	30	021	050	
Locker	08	051	058	Userid that set lock
Lock date	05	059	063	Date locked YYDDD
Lock time	05	064	068	Time locked HH:MM
Current retry count	03	069	071	
Expire time	05	072	076	HH:MM
Expire date	05	077	081	YYDDD

Terminal profile record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	40
Terminal	08	003	010	Generic terminal id
(blank)	10	011	020	
Group	08	021	028	
Initial panel	08	029	036	
Terminal lock interval	03	037	039	

MHO node record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	50
Nodename	08	003	010	
(blank)	10	011	020	
Symbolic name	08	021	028	
Comments	50	029	078	
Enable	01	079	079	Y or N

Summary record

Field	Length	From	To	Comment
Sort key	20	001	020	
Record type	02	001	002	70
(blank)	18	003	020	
System version number	03	021	023	
Log length	06	024	029	Numeric
Trial mode flag	01	030	030	Y or N
Self registration	01	031	031	Not applicable for NC-PASS Secure
Preferred date format	08	032	039	With pref date separator
Users with tokens	06	040	045	Not applicable for NC-PASS Secure
Maximum users with tokens	08	046	053	Not applicable for NC-PASS Secure
Idle timeout	03	054	056	Y or N
Passcode PIN length	01	057	057	Not applicable for NC-PASS Secure
(Filler)	01	058	058	
Information logon messages	01	059	059	Y or N
LU0 enabled	01	060	060	Y or N
LU0 host nodename	08	061	068	
LU0 node password	08	069	076	
LU0 default logon nodename	08	077	084	
LU0 link check interval	03	085	087	In minutes. Numeric
LU0 symbolic nodename	08	088	095	
LU62 enabled	01	096	096	Y or N
LU62 nodename	08	097	104	
LU62 password	08	105	112	
LU62 node check interval	03	113	115	in minutes
LU62 symbolic name	08	116	123	
XMS identifier	04	124	127	
XMS work elements	03	128	130	
XMS enable	01	131	131	Y or N
MHO administration flag	01	132	132	
Transmission log length	03	133	135	
Allow MHO rule store	01	136	136	
Allow MHO rule load	01	137	137	

Field (Continued)	Length	From	To	Comment
Use MHO node as userid	01	138	138	
Acquire default userid	08	139	146	
CSA timeout	04	147	150	in seconds
List function	01	151	151	operator function
Load function	01	152	152	operator function
Restore function	01	153	153	operator function
Set function	01	154	154	operator function
STOP/NOSTOP	01	155	155	global option
TRACE/NOTRACE	01	156	156	global option
ENABLE/DISABLE	01	157	157	global option
CONT	01	158	158	global option
RECEIVE ALLOW	01	159	159	global option
ALLOW REMOVE BACKOUT	01	160	160	Y or N
Master rule name	08	161	168	this will not necessarily be active
Default action	08	169	176	
Default model user profile	08	177	184	
Printer ACB stub name	06	185	190	
No. of ACBs for printer pool	02	191	192	

Logon statistics

Option 1.4 of the NC-PASS SECURE MENU provides the REPORT PRODUCTION MENU as shown below.

```
Date:12/12/1997          REPORT PRODUCTION MENU          Userid:TSG0001
Time:09:00                                     Terminal:A01MS262

      Option => _____

                1 Log on statistics summary
                2 Log on statistics full report

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

Options 1 and 2 of the above menu provide panels which allow you to select previously loaded VSAM ESDS's for processing. An ESDS should contain messages from an archive file or copied from an SMF file.

A report can only be produced if log on messages have been routed to the file using the severity level on the MESSAGE ROUTING panel (1.3.1). The messages processed are those starting with the text 'LOGON' or 'ACCESS DENIED'.

You can select either printed or screen reports in full or summary format. The reports total the number of accepted and rejected logons.

Producing a summary by date

Select option 1 on the REPORT PRODUCTION MENU (1.4) to display the following panel.

```
Date:12/12/1997      LOG ON STATISTICS - SUMMARY BY DATE      Userid:TSG0001
Time:09:00          Terminal:A01MS262

This panel permits the selection of a file for evaluation to produce a report
of attempted 'log on' statistics. The report produced displays the number of
attempted log ons by hour within day.

Enter dataset name below and optionally SMF record type:
  ESDS DSN => NCPASS.ARCHIVE1
  SMF record type =>     (128-255)

Press <ENTER> to view the report.
Press <F6> to print the report without viewing.

F1=Help  F3=End  F6=Print
```

Enter the dataset name and press <Enter> to display the report:

```
Date:12/12/1997      LOG ON STATISTICS - SUMMARY BY DATE      Userid:TSG0001
Time:09:00          Terminal:A01MS262

DATE => 12/11/1997 (MM/DD/YYYY) ACCEPTED => 105   REJECTED => 6

TIME PERIOD ACCEPTED REJECTED      TIME PERIOD ACCEPTED REJECTED
00:00 00:59                                12:00 12:59           2         1
01:00 01:59                                13:00 13:59
02:00 02:59                                14:00 14:59
03:00 03:59                                15:00 15:59
04:00 04:59                                16:00 16:59
05:00 05:59                                17:00 17:59
06:00 06:59                                18:00 18:59
07:00 07:59                                19:00 19:59
08:00 08:59           9
09:00 09:59           94         5
10:00 10:59
11:00 11:59                                22:00 22:59
                                           23:00 23:59

F3=End  F6=Print  F7=Up  F8=Down
```

This panel displays the number of attempted logons by hour for that day. The total number of accepted and rejected logons for each hour is given.

If you want to print the report press <F6> to display the printer field amendment screen as described in *Producing reports from administration panels* on page 10.16.

Enter the appropriate details and press <Enter> to print the specified report. A sample report is shown below.

```
DATE 12.12.1997          NC-PASS REPORT          PAGE 1
TIME 11:20              LOG ON STATISTICS - SUMMARY BY DATE
-----
Report Requested by - TSG0001      Report period:
      on Terminal - A01MS262      From => 11.12.1997 (DD.MM.YYYY)
      Job Name - NCPASS           To => 11.12.1997

ESDS Dataset name
NCPASS.ARCHIVE1
-----
DATE => 11.12.1997 (DD.MM.YYYY) ACCEPTED => 105 REJECTED => 6

TIME PERIOD ACCEPTED REJECTED      TIME PERIOD ACCEPTED REJECTED
00:00 00:59                                12:00 12:59          2          1
01:00 01:59                                13:00 13:59
02:00 02:59                                14:00 14:59
03:00 03:59                                15:00 15:59
04:00 04:59                                16:00 16:59
05:00 05:59                                17:00 17:59
06:00 06:59                                18:00 18:59
07:00 07:59                                19:00 19:59
08:00 08:59          9                    20:00 20:59
09:00 09:59          94          5        21:00 21:59
10:00 10:59                                22:00 22:59
11:00 11:59                                23:00 23:59
REPORT TOTAL ACCEPTED => 105 REJECTED => 6
```

Producing a full report

Choose option 2 from the REPORT PRODUCTION MENU (1.4) to select a file from which to produce a full statistical report.

```

Date:12/12/1997          LOG ON STATISTICS - FULL REPORT          Userid:TSG0001
Time:09:00              Terminal:A01MS262

This panel permits the selection of a file for evaluation to produce a report
of attempted 'log on' statistics. The report produced displays all attempted
logons recorded on the file, in chronological order.

Enter dataset name below and optionally SMF record type:
  ESDS DSN => NCPASS.ARCHIVE1
  SMF record type =>      (128-255)

Press <ENTER> to view the report.
Press <F6> to print the report without viewing.

F1=Help  F3=End  F6=Print
  
```

Enter the dataset name, an example of which is shown above, and press <Enter>. The report will be displayed. All attempted logons are listed in chronological order.

If you want a printed report, press <F6> to display the printer field amendment screen. Enter the required details and press <Enter>. A printed report similar to the sample shown below will be provided.

```

DATE 12.12.1997          NC-PASS REPORT          PAGE 1
TIME 11:50              LOG ON STATISTICS - FULL REPORT
-----
  
```

```

Report Requested by - TSG0001          Report period:
      on Terminal - A01MS262          From => 12.10.1997 (MM.DD.YYYY)
      Job Name - NCPASS              To => 12.11.1997
  
```

```

ESDS Dataset name
NC-PASS.ARCHIVE1
-----
  
```

DATE	TIME	SYS	JOBNAME	TERMINAL	USER ID	ACCEPTED	DESTINATION
12.10.1997	08:05:37	IP01	NCPASS	A01MS225	TSG0054	Y	A01TSO
12.10.1997	08:05:57	IP01	NCPASS	A01MS231	TSG0001	N	
12.10.1997	08:15:59	IP01	NCPASS	A01MS226	TSG0326	N	
12.10.1997	08:26:03	IP01	NCPASS	A01MS326	TSG0002	N	
12.10.1997	08:36:09	IP01	NCPASS	A01MS207	ADM0001	Y	ADMIN
12.10.1997	08:45:16	IP01	NCPASS	A01MS154	SYS0001	Y	ADMIN
12.10.1997	08:52:22	IP01	NCPASS	A01MS209	TSG0022	Y	ADMIN
12.11.1997	08:00:07	IP01	NCPASS	A01MS231	TSG0001	Y	SYSTEM
12.11.1997	08:18:44	IP01	NCPASS	A01MS207	ADM0001	Y	SYSTEM
12.11.1997	08:40:27	IP01	NCPASS	A01MS226	TSG0326	Y	SYSTEM
12.11.1997	08:47:38	IP01	NCPASS	A01MS154	SYS0001	Y	SEMENU00

```

REPORT TOTAL ACCEPTED => 8 REJECTED => 3
  
```

Producing reports from administration panels

A number of administration panels provide a print option. These are as follows:

Panel	Report	Example on page
LIST USERS (5.5)	User profile	3.32
BROWSE NC-PASS/NCI LOG (3)	Message log	9.27
SELECT ARCHIVE AND SMF MESSAGES (1.3.6)	Archived messages	9.36
LOGON STATISTICS - SUMMARY BY DATE (1.4.1)	Logon statistics - summary by date	10.13
LOGON STATISTICS - FULL REPORT (1.4.2)	Logon statistics - full report	10.15
AUTHORIZATION CONTROL TABLE CONVERSION (7.9)	SME rules	7.86
RULE MAINTENANCE/EDIT (7.1)	SME rules	7.48

When the print option is selected the following panel will be displayed. The title of the panel is derived from the calling panel.

```

Date:12/12/1997                               LIST USERS                               Userid:TSG0001
Time:09:00                                     Terminal:A01MS262

Amend fields as required and press <ENTER> to initiate printing:
Printer           => T01HQC10 (VTAM only)
Printer type      => V      (V=VTAM, S=System)
Lines per page    => 60    (20-99)
Copies            => 1
Class            => -      (System only)
Forms            => _____ (System only)

Save as new default => N (Y/N)

F1=Help  F3=End  F12=Can
    
```

Complete the required fields and press <Enter> to print the required report.

VTAM printing

Before VTAM printers can be used by NC-PASS they must be defined to NC-PASS in the VTAM PRINTER DEFINITIONS panel (1.6). This panel is described in *VTAM printer definitions* on page 2.7.

Chapter 11 - Remote administration via MHO

Introduction	11.2
Storing and loading rules on remote NC-PASS systems	11.3
Sending a rule to other systems	11.5
Receiving rules from other systems	11.7
Effect of system option settings	11.9
MHO rule administration panels	11.10
Enabling MHO administration	11.10
Rule propagation	11.11
Selecting the remote nodes	11.13
Specifying rule receipt options	11.15
Auditing rule propagation	11.17
Viewing the log	11.17
Return codes	11.18

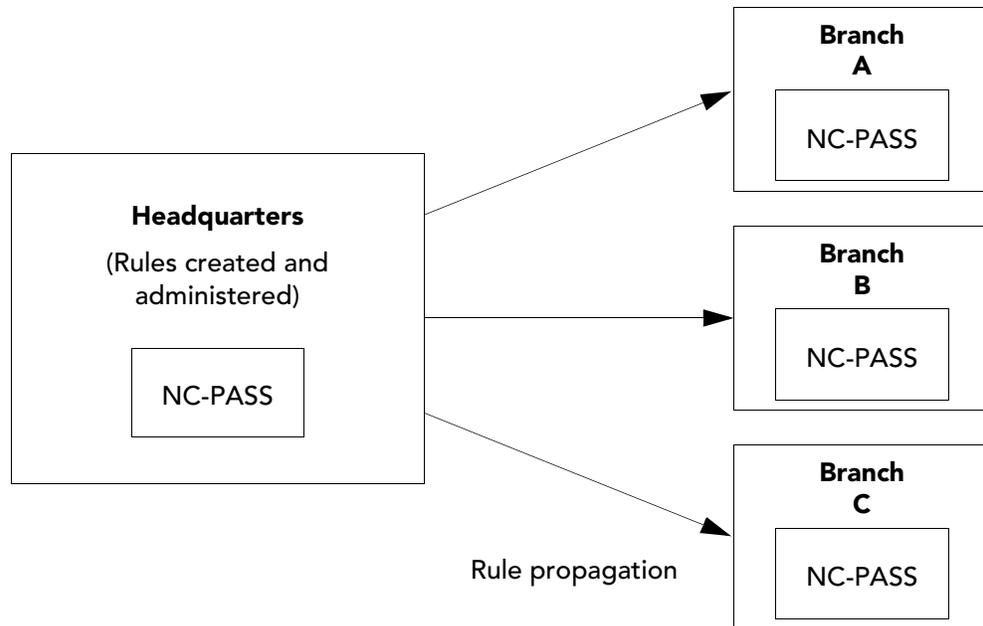
Introduction

The MHO administration facility allows you to carry out specified administration tasks on remote NC-PASS systems. Currently the only task supported is SME rule store and load. This facility allows central maintenance and administration of rules on all systems in the network.

Storing and loading rules on remote NC-PASS systems

This section describes the steps required to propagate rules to, and receive rules from, remote NC-PASS systems.

Once you have created and tested a rule, you can use the MHO administration feature to propagate rule definitions to all or selected NC-PASS systems with which this NC-PASS has an active MHO LU0 link. (Refer to *Chapter 1 - Communicating with other systems* (Volume 2) for details of how to define an MHO LU0 link.)



When you send a rule to another system, you can specify that the rule to be propagated is either:

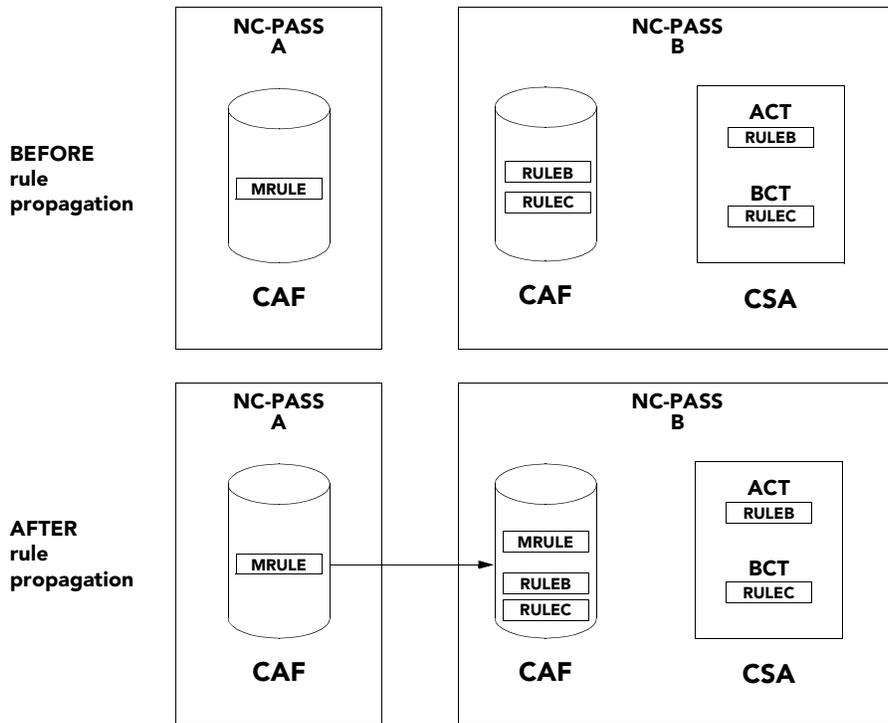
- stored on the specified remote systems' CAFs *or*
- stored on the specified remote systems' CAFs **and loaded as the Active Control Table** into the remote systems' CSA (Common Services Area).

The settings of system options on each NC-PASS will dictate whether rules can be sent to other systems and whether this NC-PASS can receive rules transmitted by other NC-PASS systems.

When a rule is propagated, all lower level rules, groups and date/time definitions are also propagated and stored on the remote systems' CAFs.

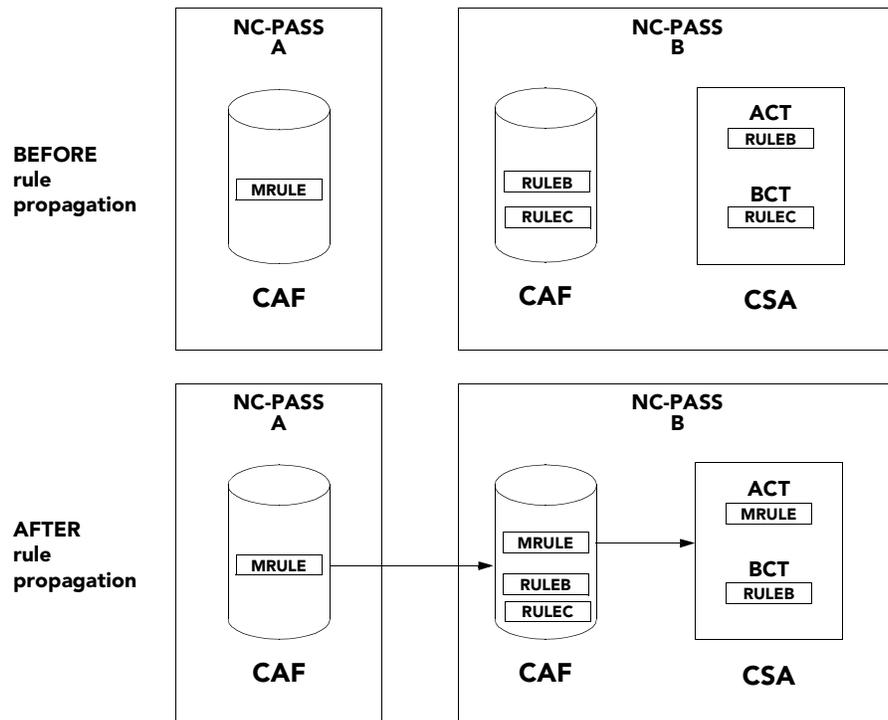
Note: If the global MHO administration option is not enabled, no rule transmissions from or to this NC-PASS will be allowed.

The following diagram illustrates storing a rule on a remote system (no load).



Example - storing a rule on a remote system

The following diagram illustrates storing **and loading** a rule on a remote system.



Example - storing and loading a rule on a remote system

Sending a rule to other systems

Rules can be propagated to any other linked NC-PASS providing the following conditions are met:

- remote MHO administration has been enabled
- an MHO LU0 link has been enabled and is active between the specified systems
- NC-PASS AUTHENTICATOR v2.0 or NC-PASS SECURE v2.0 is running on the specified systems.

The following example shows the steps required to propagate a rule to specified remote NC-PASS systems. For the purpose of this example, it is assumed that the appropriate MHO links have been enabled and that a required version of NC-PASS is running on the specified systems.

Refer to *MHO rule administration panels* on page 11.10 for a detailed description of the panels used in the example.

Step 1 Choose option 4 from the CROSS SYSTEM COMMUNICATIONS panel (4) to display the REMOTE ADMINISTRATION OPTIONS panel, as shown below:

```
Date:12/12/1997          REMOTE ADMINISTRATION OPTIONS          Userid:TSG0001
Time:09:00                                     Terminal:A01MS244

This panel allows entry of MHO administration options

Allow MHO administration => Y Y/N

Transmission log length => 100 0-999, If 0 is specified no transmissions
                                log will be kept

F1=Help  F3=End  F5=Log  F12=Can
```

Step 2 Set the **Allow MHO administration** field to Y to enable remote administration and press <F3> to save and end.

Step 3 Choose option 8 from the VSSE OPTIONS menu (7) to display the RULE ADMINISTRATION VIA MHO panel.

- Step 4** Choose option 1 to display the MHO RULE TRANSMISSION panel.
- Step 5** Enter the rule name to be propagated in the **Rule name** field. (<F9> provides a list of all rules defined to this system, from which one can be selected.)
- Step 6** Enter 1 in the **Transmit option** field to specify that the rule is to be stored, but not loaded, on the specified remote systems or enter 2 to specify that the rule is to be stored **and loaded** on the specified systems.

```

Date:12/12/1997           MHO RULE TRANSMISSION           Userid:TSG0001
Time:09:00                Terminal:A01MS268

This panel provides the facility to transmit a rule to one or more NC-PASS
systems. Select a transmission option from the list below. Specify the rule
name to be transmitted and press <F6> to select the target nodes. On return
press <F3> on this panel to perform the transmission.

Host NC-PASS system MHO Communications (LU0) details are as follows:
MHO Host nodename => A01HQ004  Status => *ACTIVE*
MHO Symbolic name => NEWYORK4

Select one of the following transmission options:
  Option => 1 1. Store the rule on the remote systems' CAFs.
              2. Store the rule, and load as the current active
                 control table on the remote systems.

Enter below the name of the rule to be transmitted, or press <F9> for a
list of the rules from which one may be selected:
  Rule name => MRULE

F1=Help  F3=End  F5=Log  F6=Nodes  F9=Rules  F12=Can

```

- Step 7** Press <F6> to display the MHO NODE SELECTION panel. (If the rule you are trying to transmit is incomplete, an error message will be displayed and the rule will not be transmitted.)

```

Date:12/12/1997           MHO NODE SELECTION           Userid:TSG0001
Time:09:00                Terminal:A01MS268

List options  S=Select

O E NODENAME SYMBOLIC TYPE      COMMENT          STATUS
S Y A01HQ001 NEWYORK1          *ACTIVE*
S Y A01HQ002 NEWYORK2          *ACTIVE*
S Y A01HQ003 NEWYORK3          *ACTIVE*
  N A02HQ005                      INACTIVE

F1=Help  F2=Select all  F3=End  F7=Up  F8=Down  F12=Can

```

- Step 8** Enter S against those systems to which the rule is to be propagated. (Press <F2> to automatically enter an S against all active nodes; you can then delete any selection that is not required.)
- Step 9** Press <F3> to return to the MHO RULE TRANSMISSION panel.
- Step 10** Check all details are correct and press <F3> to start the transmission.
- If the rule is transmitted, a message, similar to that shown below will be displayed on the MHO RULE TRANSMISSION panel:
- CKSE3468-4 MHO transmit no. 18 to A01HQ003, STORE RULE MRULE**
- If you have transmitted a rule to more than one node, the message relates to the last one selected.
- Note:** The transmission may be rejected by the remote system if the appropriate options have not been set on the remote system. See *Receiving rules from other systems* below.
- Step 11** You can view the MHO log to see all transmission details, as described in *Auditing rule propagation* on page 11.17.
-

Receiving rules from other systems

Rules can be received from any other linked NC-PASS providing the following conditions are met:

- remote MHO administration has been enabled
- an MHO LU0 link has been enabled and is active between the specified systems
- NC-PASS AUTHENTICATOR v2.0 or NC-PASS SECURE v2.0 is running on the specified systems
- remote VSSE processing has been enabled.

The example on the following page shows the steps required to enable the appropriate remote VSSE processing system options, depending on your requirements. It is assumed that the appropriate MHO links have been enabled and that NC-PASS is running on the specified systems.

Step 1 Choose option 4 from the CROSS SYSTEM COMMUNICATIONS panel (4) to display the REMOTE ADMINISTRATION OPTIONS panel, as shown below:

```
Date:12/12/1997          REMOTE ADMINISTRATION OPTIONS          Userid:TSG0001
Time:09:00                Terminal:A01MS244

This panel allows entry of MHO administration options

Allow MHO administration => Y Y/N

Transmission log length => 100 0-999, If 0 is specified no transmissions
                               log will be kept

F1=Help  F3=End  F5=Log  F12=Can
```

Step 2 Set the **Allow MHO administration** field to Y to enable remote administration and press <F3> to save and end.

Step 3 Choose option 2 from the RULE ADMINISTRATION VIA MHO panel (7.8) to display the MHO RULE RECEPTION panel as shown below:

```
Date:12/12/1997          MHO RULE RECEPTION          Userid:TSG0001
Time:09:00                Terminal:A01MS244

This administration panel provides the facility to control what actions may
be performed when this NC-PASS system receives a rule definition that has
been transmitted from a remote NC-PASS system using MHO.

Host NC-PASS system MHO Communications (LU0) details are as follows:
  MHO Host nodename => A01HQ004  Status => *ACTIVE*
  MHO Symbolic name => NEWYORK4

Specify below whether a rule received over MHO may be stored in the CAF:
  Permit rule to be stored in CAF => N Y/N

Specify below whether a rule received over MHO may be loaded into CSA after
being stored in the CAF:
  Permit rule to be loaded into CSA => N Y/N

Specify below whether the remote MHO nodename is to be used as the user id
when updating rule definitions on this NC-PASS system:
  Use MHO nodename as userid => N Y/N

F1=Help  F3=End  F5=Log  F12=Can
```

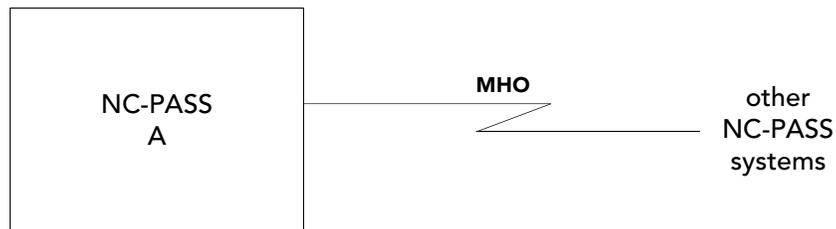
Step 4 If other NC-PASS systems are to be allowed to transmit and store a rule in this NC-PASS's CAF, enter Y in the **Permit rule to be stored in CAF** field.

Step 5 If other NC-PASS systems are to be allowed to store a rule in this NC-PASS's CAF and load the rule as the Active Control Table for this NC-PASS, enter Y in the **Permit rule to be loaded into CSA** field.

Step 6 Press <F3> to save and end.

Effect of system option settings

The following diagram shows an NC-PASS system with MHO links to other NC-PASS systems.



The table below provides a summary of the various system option settings and the effects of those settings for the NC-PASS system on which they have been defined. (The number shown in brackets refers to the panel containing the specified option).

System option settings on NC-PASS A			Effect		
Allow MHO administration (4.4)	Receive rules over MHO (7.8.2)	Allow rules to be loaded (7.8.2)	Can NC-PASS A send rules to other systems?	Can other systems STORE rules in NC-PASS A?	Can other systems LOAD rules in NC-PASS A?
N	Y or N	Y or N	N	N	N
Y	N	N	Y	N	N
Y	Y	N	Y	Y	N
Y	Y	Y	Y	Y	Y

MHO rule administration panels

This section provides detailed descriptions of the MHO rule administration panels.

If you want this NC-PASS to transmit a rule to other systems, you must:

- enable MHO administration
- specify the rule to be transmitted, to which remote systems it is transmitted and whether it is to be stored only or stored and loaded on the remote system.

If other NC-PASS systems are to be allowed to transmit rules to this NC-PASS you must:

- enable MHO administration
- set the appropriate rule receipt options.

Enabling MHO administration

Choose option 4 from the CROSS SYSTEM COMMUNICATIONS panel (4) to display the REMOTE ADMINISTRATION OPTIONS panel, as shown below:

```
Date:12/12/1997          REMOTE ADMINISTRATION OPTIONS          Userid:TSG0001
Time:09:00                                     Terminal:A01MS244

This panel allows entry of MHO administration options

Allow MHO administration => Y Y/N

Transmission log length => 100 0-999, If 0 is specified no transmissions
                               log will be kept

F1=Help  F3=End  F5=Log  F12=Can
```

Input fields

Field	Description
Allow MHO administration	Enter Y to allow this system's administrators to carry out administrative tasks on remote NC-PASS systems. Each task can be individually restricted. (Currently the only tasks available are VSSE rule store and load.) Enter N to disable remote administration.

Field	Description
Transmission log length	<p>Enter the number of lines you want to keep in the transmission log. This log is used to audit the transmission of administrative tasks. Messages associated with the transmissions will be written to the NCI log as normal.</p> <p>The maximum number of lines you can specify is 999. If you specify 0, the default, no log will be kept.</p>

Function keys

Key	Function
F1	displays help information.
F3	saves any changes made and returns to the previous panel.
F5	displays the MHO TRANSMISSION LOG panel. Refer to <i>Auditing rule propagation</i> on page 11.17.
F12	cancels any changes made and returns to the previous panel.

Rule propagation

To transmit a rule to other systems you define the rule to be propagated and the function to be performed (load/store) on the MHO RULE TRANSMISSION panel (7.8.1) then press <F6> to provide details of the remote NC-PASS systems to which the rule is to be propagated.

Choose option 1 from the RULE ADMINISTRATION VIA MHO panel (7.8) to display the MHO RULE TRANSMISSION panel, as shown below:

```

Date:12/12/1997                MHO RULE TRANSMISSION                Userid:TSG0001
Time:16:14                      Terminal:A01MS268

This panel provides the facility to transmit a rule to one or more NC-PASS
systems. Select a transmission option from the list below. Specify the rule
name to be transmitted and press <F6> to select the target nodes. On return
press <F3> on this panel to perform the transmission.

Host NC-PASS system MHO Communications (LU0) details are as follows:
  MHO Host nodename => A01HQ004  Status => *ACTIVE*
  MHO Symbolic name => NEWYORK4

Select one of the following transmission options:
  Option =>   1. Store the rule on the remote systems' CAFs.
              2. Store the rule, and load as the current active
                  control table on the remote systems.

Enter below the name of the rule to be transmitted, or press <F9> for a
list of the rules from which one may be selected:
  Rule name => _____

F1=Help  F3=End  F5=Log  F6=Nodes  F9=Rules  F12=Can

```

Input fields

Field	Description
Option	<p>Enter 1 to store this rule on the remote system. Enter 2 to store the rule and load it in the remote system's CSA as the Active Control Table.</p> <p>Note: If the remote system does not allow rules to be stored or loaded remotely, the remote system will reject the request and return the appropriate error code. All transmission details can be viewed on the Transmission log, if one is being maintained. Refer to <i>Auditing rule propagation</i> on page 11.17.</p>
Rule name	<p>Enter the name of the rule to be propagated to other NC-PASS systems or press <F9> to display a list of all rules defined to this system, from which one can be selected.</p> <p>Note: If you select a rule that is incomplete (eg a True or False action contains a reference to another rule which has not yet been defined), the transmission will be rejected.</p>

Display fields

Field	Description
MHO Host nodename	The name of the MHO node on this NC-PASS system. This is the name defined on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1) in the MHO Host nodename field.
Status	<p>The current status of the MHO system:</p> <p>*ACTIVE* the system is available</p> <p>INACTIVE the system is unavailable</p> <p>PENDING the system in the process of startup or shutdown and is not available.</p>
MHO Symbolic name	The symbolic name, if any, associated with this nodename. This is the name defined on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1) in the MHO Symbolic name field.

Function keys

Key	Function
F1	displays help information.
F3	transmits the specified rule and function (store or load) to the nodes selected. Details of all transmissions are logged on the Transmissions log, if one is maintained. Refer to <i>Auditing rule propagation</i> on page 11.17.
F5	displays the MHO TRANSMISSION LOG panel. Refer to <i>Auditing rule propagation</i> on page 11.17.
F6	displays the MHO NODE SELECTION panel, from which you select the remote nodes for rule propagation. See <i>Selecting the remote nodes</i> on page 11.13

Key	Function
F9	displays the RULE SELECTION LIST panel from which you can select the rule to be propagated.
F12	cancels any changes made and returns to the previous panel.

Selecting the remote nodes

Press <F6> on the MHO RULE TRANSMISSION panel (7.8.1) to display the MHO NODE SELECTION panel, as shown below:

```

Date:12/12/1997          MHO NODE SELECTION          Userid:TSG0001
Time:09:00              Terminal:A01MS268

List options  S=Select

O E NODENAME SYMBOLIC TYPE      COMMENT          STATUS
_ Y A01HQ001 NEWYORK1           *ACTIVE*
_ Y A01HQ002 NEWYORK2           *ACTIVE*
_ Y A01HQ003 NEWYORK3           *ACTIVE* D
_ N A02HQ005                     INACTIVE

F1=Help  F2=Select all  F3=End  F7=Up  F8=Down  F12=Can

```

List options

Enter list option S in the O column against the required nodenames to perform the following function:

- S Selects the nodename to which the rule specified is to be propagated. (Alternatively, press <F2> to enter an S against all active nodes.)

Note: You can only select a node if:

- the link has been enabled and is currently active
- the linked system is running NC-PASS AUTHENTICATOR v2.0 or NC-PASS SECURE v2.0.

When all required nodes have been selected, press <F3> to return to the MHO RULE TRANSMISSION panel.

Display fields

Field	Description
E	Y means the MHO link, to the corresponding nodename, is enabled. N means the link is disabled.

Field	Description
NODENAME	The name of the MHO node on the remote system.
SYMBOLIC	The symbolic name associated with the node, if one has been defined.
TYPE	reserved for future use.
COMMENT	Comment text describing the node, as defined on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1).
STATUS	The current status of the MHO system: *ACTIVE* the system is available. *ACTIVE* D there is an active link to the system, but the linked system is running an earlier version of NC-PASS. Rule propagation to this system is not available. INACTIVE the system is unavailable. PENDING the system in the process of startup or shutdown and is not available.

Function keys

Key	Function
F1	displays help information.
F2	Enters an S line command against all active links.
F3	returns to the MHO RULE TRANSMISSION panel.
F7	pages up through the list of nodes.
F8	pages down through the list of nodes.
F12	cancels the selection and returns to the previous panel.

Specifying rule receipt options

Choose option 2 from the RULE ADMINISTRATION VIA MHO panel (7.8) to display the MHO RULE RECEPTION panel, as shown below:

```
Date:12/12/1997          MHO RULE RECEPTION          Userid:TSG0001
Time:09:00              Terminal:A01MS268

This administration panel provides the facility to control what actions may
be performed when this NC-PASS system receives a rule definition that has
been transmitted from a remote NC-PASS system using MHO.

Host NC-PASS system MHO Communications (LU0) details are as follows:
  MHO Host nodename => A01HQ004  Status => *ACTIVE*
  MHO Symbolic name => NEWYORK4

Specify below whether a rule received over MHO may be stored in the CAF:
  Permit rule to be stored in CAF => N Y/N

Specify below whether a rule received over MHO may be loaded into CSA after
being stored in the CAF:
  Permit rule to be loaded into CSA => N Y/N

Specify below whether the remote MHO nodename is to be used as the user id
when updating rule definitions on this NC-PASS system:
  Use MHO nodename as userid => N Y/N

F1=Help  F3=End  F5=Log  F12=Can
```

Input fields

Field	Description
Permit rule to be stored in CAF	<p>Specify Y to allow other NC-PASS systems to store rules in this NC-PASS's CAF.</p> <p>If you specify N and a remote NC-PASS transmits a rule to this NC-PASS, the transmission will be rejected. The rule is not stored and an error return code is sent to the originator. You can view the transmission details and the return code on the transmission log, if one is being maintained. Refer to <i>Auditing rule propagation</i> on page 11.17.</p>
Permit rule to be loaded into CSA	<p>Specifying Y in this field is only relevant if Permit rule to be stored in CAF is set to Y. Specify Y to allow remote NC-PASS systems to load a rule into this NC-PASS's CSA as the Active Control Table.</p> <p>If you specify N and a remote NC-PASS transmits a rule to be loaded on this NC-PASS, either all or part of the function will be rejected. You can view the transmission details and the return code on the transmission log, if one is being maintained. Refer to <i>Auditing rule propagation</i> on page 11.17.</p>

Field	Description
Use MHO nodename as userid	<p>Enter Y to specify that when a remote NC-PASS stores a rule on this NC-PASS, the By column on the RULE MAINTENANCE panel (7.1) should show the name of the MHO node that transmitted the rule.</p> <p>Enter N to specify that the By column on the RULE MAINTENANCE panel (7.1) should show the userid of the user that initiated the transmission.</p>

Display fields

Field	Description
MHO Host nodename	<p>The name of the MHO node on this NC-PASS system.</p> <p>This is the name defined on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1) in the MHO Host nodename field.</p>
Status	<p>The current status of the MHO system:</p> <p style="padding-left: 40px;">*ACTIVE* the system is available.</p> <p style="padding-left: 40px;">INACTIVE the system is unavailable.</p> <p style="padding-left: 40px;">PENDING the system in the process of startup or shutdown and is not available.</p>
MHO Symbolic name	<p>The symbolic name, if any, associated with this nodename. This is the name defined on the CROSS SYSTEM COMMUNICATIONS - HOST panel (4.1) in the MHO Symbolic name field.</p>

Function keys

Key	Function
F1	displays help information.
F3	saves any changes made and returns to the previous panel.
F5	displays the MHO TRANSMISSION LOG panel. Refer to <i>Auditing rule propagation</i> on page 11.17.
F12	cancels any changes made and returns to the previous panel.

Auditing rule propagation

If you specify a value between 1 and 999 in the **Transmission log length** field on the REMOTE ADMINISTRATION OPTIONS panel (4.4), NC-PASS will maintain a log of all MHO administration actions in the MHO transmission log, an example of which is shown below:

DATE	TIME	USER	T/F	NODE	FUNCTION	TYPE	NAME	CONFIRM	RC
12/12/1997	12:55:50	TSG0001	To	A01HQ002	STORE	RULE	MRULE	12:56:40	0
12/12/1997	12:55:50	TSG0001	To	A01HQ003	STORE	RULE	MRULE	12:56:42	0
12/12/1997	12:55:50	TSG0001	To	A01HQ004	STORE	RULE	MRULE	12:56:43	0

F1=Help F2=Purge log F3=End F7=Up F8=Down

A log is maintained on each system that specifies the log option.

Viewing the log

You can view this log either by pressing <F5> on the MHO RULE TRANSMISSION panel (7.8.1) or by choosing option 5 from the CROSS SYSTEM COMMUNICATIONS menu (4).

Display fields

Field	Description
Date	The date on which the transmission was requested.
Time	The time at which the transmission was requested.
User	The user who requested the transmission.
T/F	To shows an outgoing transmission. From shows an incoming transmission.
Node	the remote MHO node from or to which the rule was sent.
Function	the administrative function requested. This field will contain either STORE or LOAD.
Type	The type of entity being processed. This field will contain RULE.
Name	The name of the entity being processed.
Confirm	The time at which an acknowledgment of a remote function was received from the remote system.

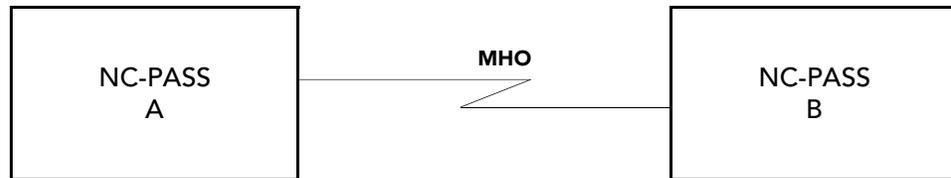
Field	Description
RC	<p>The return code indicates whether the function was successfully processed, as described below:</p> <ul style="list-style-type: none"> 0 Function completed successfully. 4 The function request specified store and load. The receiving system only allows the store function. The rule has been saved successfully, but not loaded. 8 A rule has been propagated to a system that does not allow remote rule administration. 12 Unable to obtain lock on one of the parts of the rule. Some of the data may have been saved. The usual reason for this return code is that an administrator is changing something on the target system. 16 A serious error has occurred. The cause of this should be determined by examining the target systems log for error messages. 20 MHO administration not enabled.

Function keys

Key	Function
F1	displays help information.
F2	purges all entries from the log.
F3	returns to the previous panel.
F7	pages up the log.
F8	pages down the log.

Return codes

The following diagram shows two linked NC-PASS systems.



The following table shows the codes returned to the originating system when the remote system has the settings indicated. The figures in brackets are a reference to the panels where the options are specified:

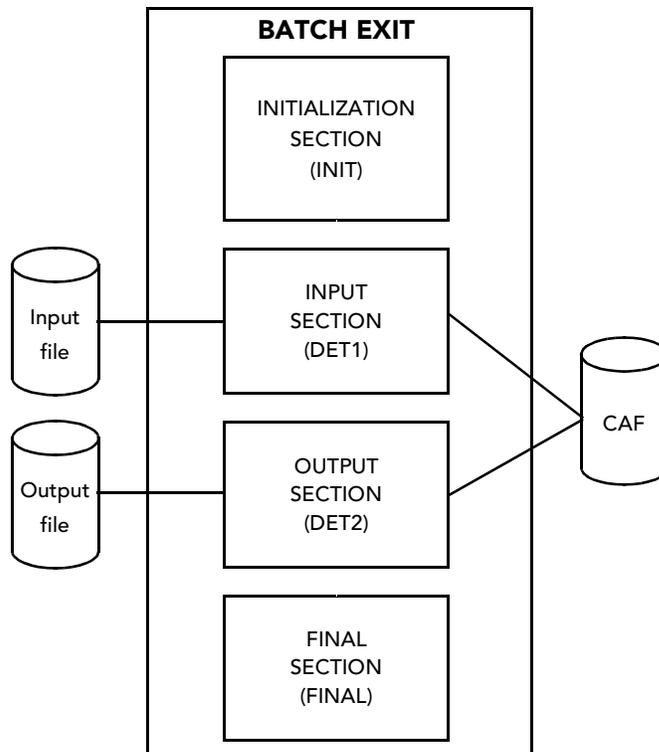
Administrator on NC-PASS A tries to STORE a rule on NC-PASS B	Administrator on NC-PASS A tries to LOAD a rule on NC-PASS B	System option settings on NC-PASS B		
		Allow MHO administration (4.4)	Receive rules over MHO (7.8.2)	Allow rules to be loaded (7.8.2)
20	20	N	Y or N	Y or N
8	8	Y	N	N
0	4	Y	Y	N
0	0	Y	Y	Y

Chapter 12 - Batch administration

Overview	12.2
User exits	12.3
The available functions	12.3
UEXIT variables	12.4
Processing requirements	12.7

Overview

Each batch process has a similar processing structure as shown below:



There are four sections within each exit as follows:

- INIT** This is processed once to set global parameters for the run. Depending on the batch process, this section would be used to:
- specify which function is to be run
 - open input and output files (if required).
- DET1** This is called for each record on the input dataset and transfers information from the input record to the variables used by the function being performed. If there is no input file, this section will be called once only.
- DET2** This is called to process the output from the requested function and allows you to format your output record if required.
- FINAL** This is called once at the end of the run and could be used to close files and produce report totals.

User exits

There are a number of on-line facilities available through the NC-PASS administration panels which allow you to add, change and delete user profiles. These on-line functions are fully described in *Chapter 3 - Controlling user access*.

These processes can also be carried out via batch processing, using exits in the form UEXIT nn .

The available functions

A number of UEXIT nn functions are provided, as described below and on the following pages, and a sample exit for each is provided in the panel library.

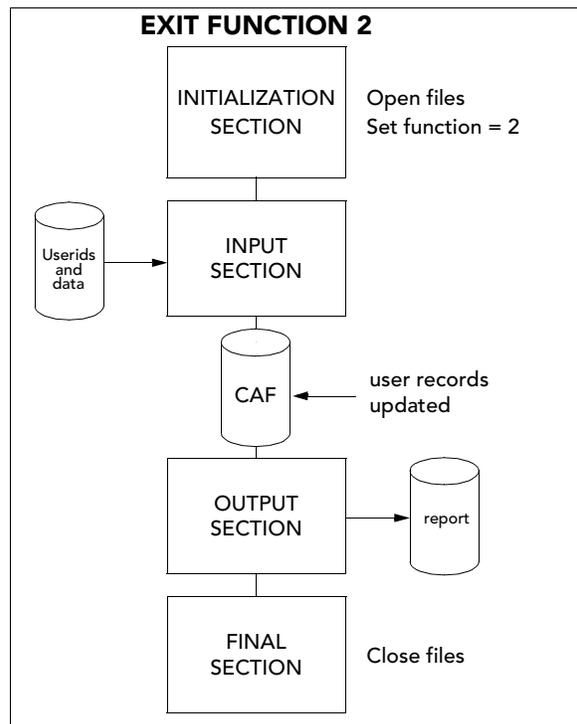
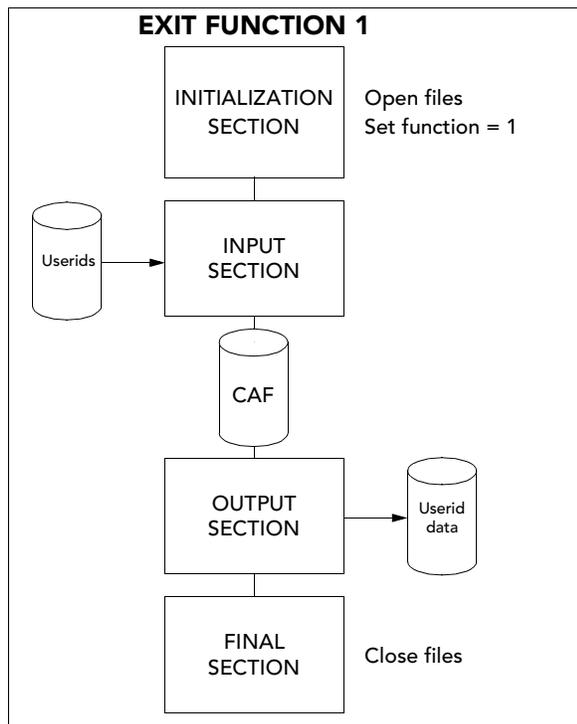
The UEXIT00 master panel documents the four sections of the exit system (as explained in the diagram on page 12.2) and can be used as a base for creating your own versions.

The exits must have names starting with UEXIT, so only the last two digits need to be changed when creating your own exits.

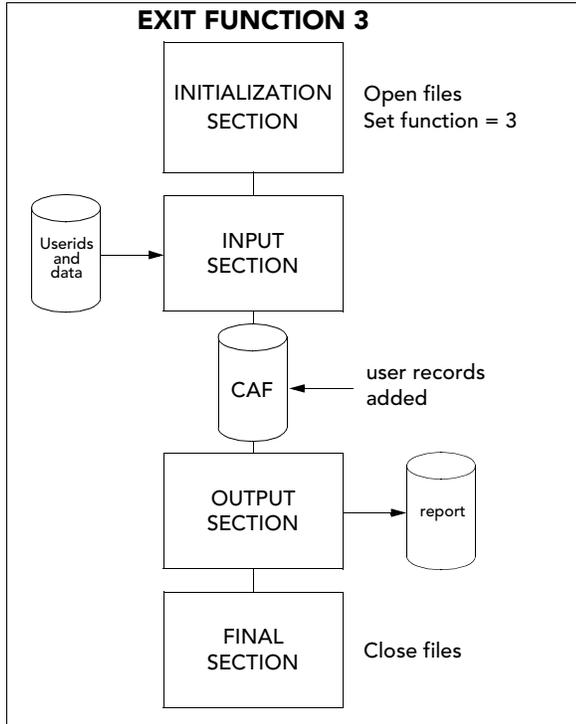
An input file providing the appropriate data must be provided for the exits which must also be changed to accept your PDS names. They must also be modified to accept the parameters set in the INIT sections.

UEXIT function 1 outputs the contents of user profiles.

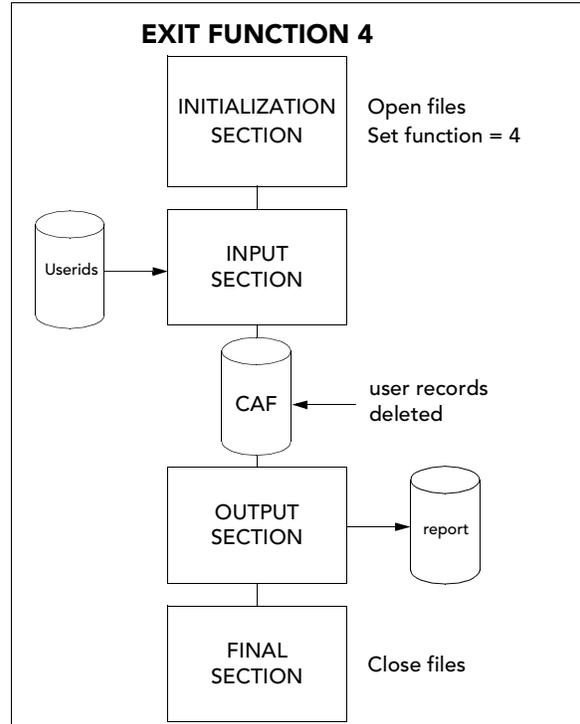
UEXIT function 2 updates user profile records with the data provided. See also *Additional notes for functions 2 and 3* on page 12.5.



UEXIT function 3 adds new user profile records. See also *Additional notes for functions 2 and 3* on page 12.5.



UEXIT function 4 deletes specified user profiles.



UEXIT variables

This section explains the variables used in the four sections described on page 12.2. Each sample exit gives an example of the use of the variables. Your use of the variables will depend on the function chosen.

INIT

Variable	Description	Example of contents
<code>&#uexdsi</code>	Input file name.	'AAAA.BBBB.CCCC(member)' - MVS file NONE - if no input file required Note: access to datasets must be authorized to your job.
<code>&#uexdso</code>	Output file name.	'AAAA.BBBB.CCCC(member)' - MVS file NONE - if no input file required Note: access to datasets must be authorized to your job.
<code>&#uexdao</code>	Append indicator.	Y - to append to existing data N - to overwrite existing data
<code>&#uexdtf</code>	Date format.	1=YYYY/MM/DD, 2=MM/DD/YYYY, 3=DD/MM/YYYY, 4=DDMMYYYY. (The default is 1.)
<code>&#uexfun</code>	A numerical identifier for the batch function to be performed.	A number between 1 and 4 (mandatory.)

DET1

Variable `&#uexin` contains your input record. The following variables must be set for the specified function:

Function	Variable	Must be set to...
1	<code>&#uxiusr</code>	userid or ALL to read all records.
2, 3,4	<code>&#uxiusr</code>	userid.

Additional notes for functions 2 and 3

Function 2 updates existing user profile records. If any of the variables shown below are not set, the corresponding field on the record will remain unchanged.

Function 3 adds new user profile records. The following variables can be used to specify the required data. All fields are fully described in *Profile definition* on page 3.21. If any of the variables are not set, the defaults shown below will be used.

Variable	Description	Contents, if specified	Default.
<code>&#uximu</code>	Model userid	Userid. When adding records, this variable can be used to model the new records on an existing user profile record. The new records will be created with the same fields as defined in the model. Used for function 3 only.	see fields below
<code>&#uxicm1</code>	Comment line 1	Descriptive text.	blank
<code>&#uxicm2</code>	Comment line 2	Descriptive text.	blank
<code>&#uxipv</code>	Password validation	<u>A</u> CF2, <u>I</u> nternal, <u>N</u> one, <u>R</u> ACF, <u>S</u> AC, <u>I</u> OP Secret.	N
<code>&#uxiat</code>	Authority type	<u>A</u> ddministrator, <u>O</u> perator, <u>U</u> ser.	U
<code>&#uxiag</code>	Authority group	<u>A</u> ddministrator, <u>O</u> perator, <u>U</u> ser * (All).	*
<code>&#uxial</code>	Authority level	A number between 1 and 255.	255
<code>&#uximen</code>	Initial menu	The name of the user's primary option menu.	blank
<code>&#uxirtm</code>	Retry maximum	A number between 0 and 99 to specify the maximum number of invalid logon attempts allowed.	0
<code>&#uxinlb</code>	No logon before	A date in the format specified by <code>&#uexdtf</code> .	blank
<code>&#uxinla</code>	No logon after	A date in the format specified by <code>&#uexdtf</code> .	blank
<code>&#uxipcl</code>	Passcode logon	Not applicable for NC-PASS Secure.	N
<code>&#uxibli</code>	Basic lock interval	A number of minutes.	0
<code>&#uxicpd</code>	Change password days	A number of days.	0
<code>&#uxicpl</code>	Change password logons	A number of logons.	0

The following variables relate to connect data definitions. The variables take the format `nameN` where `N` signifies the connect data line and can be between 1 and 9. Refer to *Specifying connection routes* on page 3.26 for more information.

Note: Function 2 (update). If you want to update any connect data field, you must enter data for **all** connect lines since the complete connect data record is updated.

<code>&#uxicdN</code>	Connect data code	N, E, K or M	
<code>&#uxidsN</code>	Connect data destination	Dependent on code above.	
<code>&#uxitmN</code>	Connect data terminal	Terminal id.	*
<code>&#uxidtN</code>	Data passed to appl	Data string.	blank
<code>&#uxiucN</code>	Comment	Descriptive text	blank

The variables listed above will be cleared before the DET2 call; if you want to use them in the output record, store them in your own variable. If you use variables starting with `&@@`, they will be automatically cleared at the end of the FINAL call.

DET2

Variable `&#uxorc` contains the return code for the function, which will contain 0 if the function completed successfully. If it does not contain 0, check that your input variables are not missing or incorrect.

In addition, the following variables are returned for the specified function.

Function	Variable	Content
1	<code>&#uxousr</code> <code>&#uxocm1</code> <code>&#uxocm2</code> <code>&#uxopv</code> <code>&#uxoat</code> <code>&#uxoag</code> <code>&#uxoal</code> <code>&#uxomen</code> <code>&#uxortm</code> <code>&#uxonlb</code> <code>&#uxonla</code> <code>&#uxopcl</code> <code>&#uxobli</code> <code>&#uxocpd</code> <code>&#uxocpl</code>	Userid. Comment line 1. Comment line 2. Password validation. Authority type. Authority group. Authority level. Initial menu. Retry maximum. No logon before. No logon after. Passcode logon. Not applicable for NC-PASS Secure. Basic lock interval. Change password days. Change password logons. The following variables relate to connect data definitions. The variables take the format <i>nameN</i> where <i>N</i> signifies the connect data line and can be between 1 and 9. Refer to <i>Specifying connection routes on page 3.26</i> for more information. <code>&#uxocdN</code> Connect data code. <code>&#uxodsN</code> Connect data destination. <code>&#uxotmN</code> Connect data terminal. <code>&#uxodtN</code> Data passed to appl. <code>&#uxoucN</code> Comment.
2/3/4	.	No additional variables.

Build your output record in variable `&#uexwr1` by concatenating the required fields using SET statements. If you need to output more than one record use variables `&#uexwr2`, `&#uexwr3` etc. Set variable `&#uexwr0` to the total number of records used.

When you want to write the records, set `&#uexwr` to Y before exit.

FINAL

Normally FINAL is executed only once. If you need to call it more than once, set variable `&#uexmor` to Y.

Processing requirements

Batch routines are run separately from NC-PASS but use similar JCL. Ideally the batch job should be run while NC-PASS is shut down, but if this is not possible, and the database is defined with share option 4 or 3, the batch job can be run while NC-PASS is active. In this case, no administration updates should be attempted while the batch job is active.

Variables are supplied to vary the flow. For example, you could have an input record that contained the information for more than one run of the function so that the read of the next record is under your control.

Sample JCL is supplied in the CNTL library in member PSBATCH.

Summary of steps required

-
- | | |
|---------------|--|
| Step 1 | Prepare the input file, if required. This must be a PDS member and can be output from another program (eg RACF) or another UEXIT. |
| Step 2 | Create your UEXIT nn or modify from an existing sample. |
| Step 3 | Update the USER=UEXIT nn parameter in the JCL. Note that the system will allow more than one UEXIT nn in a single run and that they are run in the order of the USER= parameters in the JCL. |
| Step 4 | Run the job. (Refer to processing requirements above). |
-

This page intentionally left blank

Appendix A - VSSE field names and flags

Field names	A.2
Imaginary fields	A.5
Flags	A.7

Field names

The following list provides a description of all network defined field names. Refer to the IBM manual entitled VTAM Customization LY43-0056 for further details.

Those fields that are NOT available at VTAM release 3.3 are marked in the VTAM 3.3 availability column below.

A number of commonly-referenced fields have been given one or more alias names. These alias names can be used in preference to the original name, if required.

Field name	Alias	Description	VTAM 3.3 availability
ADLSSCP		Name of the adjacent SSCP in the direction of the DLU	
AOLSSCP		Name of the adjacent SSCP in the direction of the OLU	
EVHOST		HOSTPU of the host where SME operates	
EVNAMAD		Network name of adjacent network in DLU direction	
EVNAMA0		Network name of adjacent network in OLU direction	
EVNETID	THISNET	NETID of the network where SME operates	
EVSSCP	THISVTAM	SSCPNAME of the host where SME operates	
GDLDCOS		COS name for network on DLU side of GDLNCP	
GDLNCP		Name of gateway NCP in direction of the DLU	
GDL0COS		COS name for network on OLU side of GDLNCP	
GOLDCOS		COS name for network on DLU side of GOLONCP	
GOLOCOS		COS name for network on OLU side of GOLONCP	
GOLONCP		Name of gateway NCP in direction of the OLU	
ILALLUN		ILU RIC - Alias LU name (See ILNETAL field)	No
ILNETAL		ILU RIC - NETID of network where alias LU known	No
ILNETID	LU3NET MENUMET	ILU RIC - Network ID of network containing LU	No
ILNETLU	LU3 MENU	ILU RIC - Network name of the LU (real name)	No
ILUSSCP	LU3VTAM MENUVTAM	ILU RIC - Symbolic name of SSCP controlling LU	No
PHCVR01		PLU HCV (01) - Communication Controller	
PHCVR02		PLU HCV (02) - APPL major node	
PHCVR03		PLU HCV (03) - Local Non-SNA major node	
PHCVR04		PLU HCV (04) - Switched major node	
PHCVR05		PLU HCV (05) - Local SNA major node	
PHCVR06		PLU HCV (06) - CDRM major node	
PHCVR07		PLU HCV (07) - CDRSC major node	
PHCVR08		PLU HCV (08) - CA major node	
PHCVR09		PLU HCV (09) - (Reserved)	
PHCVR10		PLU HCV (10) - CDRM	
PHCVR11		PLU HCV (11) - (Reserved)	
PHCVR12		PLU HCV (12) - GROUP	
PHCVR13		PLU HCV (13) - (Reserved)	
PHCVR 14		PLU HCV (14) - LINE	
PHCVR15		PLU HCV (15) - Direct attachment node	
PHCVR 16		PLU HCV (16) - APPL	

Field name	Alias	Description	VTAM 3.3 availability
PHCVR17		PLU HCV (17) - (Reserved)	
PHCVR18		PLU HCV (18) - PU	
PHCVR19		PLU HCV (19) - (Reserved)	
PHCVR20		PLU HCV (20) - (Reserved)	
PHCVR21		PLU HCV (21) - (Reserved)	
PHCVR22		PLU HCV (22) - LU	
PHCVR23		PLU HCV (23) - Link Station	
PHCVR24		PLU HCV (24) - CDRSC	
PHCVR25		PLU HCV (25) - (Reserved)	
PHCVR26		PLU HCV (26) - (Reserved)	
PHCVR27		PLU HCV (27) - (Reserved)	
PHCVR28		PLU HCV (28) - LAN major node	
PHCVR29		PLU HCV (29) - Packet major node	
PHCVR30		PLU HCV (30) - XCA Major node	No
PLHCVRE		PLU HCV - Count of hierarchy resource entries	
PLALLUN		PLU RIC - Alias LU name (See PLNETAL field)	
PLNETAL		PLU RIC - NETID of network where alias LU known	
PLNETID	APPLNET	PLU RIC - Network ID of network containing LU	
PLNETLU	APPL	PLU RIC - Network name of the LU (real name).	
PLUSSCP	APPLVTAM	PLU RIC - Symbolic name of SSCP controlling LU	
SHCVR01		SLU HCV (01) - Communication Controller	
SHCVR02		SLU HCV (02) - APPL major node	
SHCVR03		SLU HCV (03) - Local Non-SNA major node	
SHCVR04		SLU HCV (04) - Switched major node	
SHCVR05		SLU HCV (05) - Local SNA major node	
SHCVR06		SLU HCV (06) - CDRM major node	
SHCVR07		SLU HCV (07) - CDRSC major node	
SHCVR08		SLU HCV (08) - CA major node	
SHCVR09		SLU HCV (09) - (Reserved)	
SHCVR10		SLU HCV (10) - CDRM	
SHCVR11		SLU HCV (11) - (Reserved)	
SHCVR12		SLU HCV (12) - GROUP	
SHCVR13		SLU HCV (13) - (Reserved)	
SHCVR14		SLU HCV (14) - LINE	
SHCVR15		SLU HCV (15) - Direct attachment node	
SHCVR16		SLU HCV (16) - APPL	
SHCVR17		SLU HCV (17) - (Reserved)	
SHCVR18		SLU HCV (18) - PU	
SHCVR19		SLU HCV (19) - (Reserved)	
SHCVR20		SLU HCV (20) - (Reserved)	
SHCVR21		SLU HCV (21) - (Reserved)	
SHCVR22		SLU HCV (22) - LU	
SHCVR23		SLU HCV (23) - Link Station	
SHCVR24		SLU HCV (24) - CDRSC	
SHCVR25		SLU HCV (25) - (Reserved)	
SHCVR26		SLU HCV (26) - (Reserved)	
SHCVR27		SLU HCV (27) - (Reserved)	
SHCVR28		SLU HCV (28) - LAN major node	
SHCVR29		SLU HCV (29) - Packet major node	
SHCVR30		SLU HCV (30) - XCA Major node	No
SLHCVRE		SLU HCV - Count of hierarchy resource entries	
SLALLUN		SLU RIC - Alias LU name (See SLNETAL field)	

Field name	Alias	Description	VTAM 3.3 availability
SLNETAL		SLU RIC - NETID of network where alias LU known	
SLNETID	TERMNET	SLU RIC - Network ID of network containing LU	
SLNETLU	TERMINAL	SLU RIC - Network name of the LU (real name)	
SLUSSCP	TERMVMTAM	SLU RIC - Symbolic name of SSCP controlling LU	
STNVR01		SLU TNV (1) - Interpret table	No
STNVR02		SLU TNV (2) - Logon mode table	No
STNVR03		SLU TNV (3) - USS table	No

Imaginary fields

The following fields have been coded as imaginary data. These fields represent a logical interpretation of data. Field names beginning with O represent the logical unit from which the data is sent (Originating Logical Unit). This can refer either to the PLU or the SLU depending on the type of session initiation request. Field names beginning with D represent the logical unit to which the data is sent. (Destination Logical Unit). Therefore if the OLU is the PLU for a given session initiation request, the DLU will be the SLU and vice versa.

Those fields that are NOT available at VTAM release 3.3 are marked in the VTAM 3.3 availability column below.

A number of commonly-referenced fields have been given one or more alias names. These alias names can be used in preference to the original name, if required

Field name	Alias	Description	VTAM 3.3 availability
DHCVR01		DLU HCV (01) - Communication Controller	
DHCVR02		DLU HCV (02) - APPL major node	
DHCVR03		DLU HCV (03)- Local Non-SNA major node	
DHCVR04		DLU HCV (04) - Switched major node	
DHCVR05		DLU HCV (05) - Local SNA major node	
DHCVR06		DLU HCV (06) - CDRM major node	
DHCVR07		DLU HCV (07) - CDRSC major node	
DHCVR08		DLU HCV (08) - CA major node	
DHCVR09		DLU HCV (09) - (Reserved)	
DHCVR10		DLU HCV (10) - CDRM	
DHCVR11		DLU HCV (11) - (Reserved)	
DHCVR12		DLU HCV (12)-GROUP	
DHCVR13		DLU HCV (13) - (Reserved)	
DHCVR14		DLU HCV (14) - LINE	
DHCVR15		DLU HCV (15) - Direct attachment node	
DHCVR16		DLU HCV(16)-APPL	
DHCVR17		DLU HCV (17) - (Reserved)	
DHCVR18		DLU HCV (18) - PU	
DHCVR19		DLU HCV (19) - (Reserved)	
DHCVR20		DLU HCV (20) - (Reserved)	
DHCVR21		DLU HCV (21) - (Reserved)	
DHCVR22		DLU HCV (22) - LU	
DHCVR23		DLU HCV (23) - Link Station	
DHCVR24		DLU HCV (24) - CDRSC	
DHCVR25		DLU HCV (25) - (Reserved)	
DHCVR26		DLU HCV (26) - (Reserved)	
DHCVR27		DLU HCV (27) - (Reserved)	
DHCVR28		DLU HCV (28) - LAN major node	
DHCVR29		DLU HCV (29) - Packet major node	
DHCVR30		DLU HCV (30) - XCA Major node	No
DLHCVRE		DLU HCV Count of hierarchy resource entries	
DLALLUN		DLU RIC - Alias LU name (See DLNETAL field)	
DLNETAL		DLU RIC - NETID of network where alias LU known	
DLNETLU	LU2	DLU RIC - Network name of the LU (real name)	
DLNETID	LU2NET	DLU RIC- Network ID of network containing LU	
DLUSSCP	LU2VTAM	DLU RIC - Symbolic name of SSCP controlling LU	

Field name	Alias	Description	VTAM 3.3 availability
OHCVR01		OLU HCV (01) - Communication Controller	
OHCVR02		OLU HCV (02) - APPL major node	
OHCVR03		OLU HCV (03) - Local Non-SNA major node	
OHCVR04		OLU HCV (04) - Switched major node	
OHCVR05		OLU HCV (05) - Local SNA major node	
OHCVR06		OLU HCV (06) - CDRM major node	
OHCVR07		OLU HCV (07) - CDRSC major node	
OHCVR08		OLU HCV (08) - CA major node	
OHCVR09		OLU HCV (09) - (Reserved)	
OHCVR10		OLU HCV (10) - CDRM	
OHCVR11		OLU HCV (11) - (Reserved)	
OHCVR12		OLU HCV (12) - GROUP	
OHCVR13		OLU HCV (13) - (Reserved)	
OHCVR14		OLU HCV (14) - LINE	
OHCVR15		OLU HCV (15) - Direct attachment node	
OHCVR16		OLU HCV (16) - APPL	
OHCVR17		OLU HCV (17) - (Reserved)	
OHCVR18		OLU HCV (18) - PU	
OHCVR19		OLU HCV (19) - (Reserved)	
OHCVR20		OLU HCV (20) - (Reserved)	
OHCVR21		OLU HCV (21) - (Reserved)	
OHCVR22		OLU HCV (22) - LU	
OHCVR23		OLU HCV (23) - Link Station	
OHCVR24		OLU HCV (24) - CDRSC	
OHCVR25		OLU HCV (25) - (Reserved)	
OHCVR26		OLU HCV (26) - (Reserved)	
OHCVR27		OLU HCV (27) - (Reserved)	
OHCVR28		OLU HCV (28) - LAN major node	
OHCVR29		OLU HCV (29) - Packet major node	
OHCVR30		OLU HCV (30) - XCA Major node	No
OLHCVRE		OLU HCV - Count of hierarchy resource entries	
OLALLUN		OLU RIC - Alias LU name (See OLNATAL field)	
OLNETID	LU1NET	OLU RIC - Network ID of network containing LU	
OLNETAL		OLU RIC - NETID of network where alias LU known	
OLNETLU	LU1	OLU RIC - Network name of the LU (real name)	
OLUSSCP	LU1VTAM	OLU RIC - Symbolic name of SSCP controlling LU	

Flags

The following list of single byte flags provides a list of the symbolic names associated with each flag field and a brief description of its purpose. Refer to the IBM manual entitled VTAM Customization LY43-0056 for further details.

Those fields that are NOT available at VTAM release 3.3 are marked in the VTAM 3.3 availability column below.

Flag Field	Description
------------	-------------

DUSEIND	DLU RIC - Usage indicator
---------	---------------------------

Symbolic names	Description
DLNTARG	DLU RIC - resource is not the target (the OLU)
DLNXLAT	DLU RIC - this name has not been translated
DLTARG	DLU RIC - resource is the target (the DLU)
DLXLAT	DLU RIC - this name has been translated

Flag Field	Description
------------	-------------

EXRFUNC	Function code
---------	---------------

Symbolic names	Description
EXOSSA	Function Code - Secondary Session Authorization

Flag Field	Description
------------	-------------

EXRRS11	Related Session Information- byte 1
---------	-------------------------------------

Symbolic names	Description
EX1AUTO	RSI(O) - AUTOLOG session (VARY/LOGON/LOGAPPL)
EX1BAK	RSI(O) - Session is a backup XRF session
EX1DLUN	RSI(O) - DLU real network ID is not assumed
EX DLUY	RSI(O) - DLU real network ID is assumed
EX1NBAK	RSI(O) - Session is not a backup XRF session
EX1OLU	RSI(O) - Third party LU requested the session
EX1PLU	RSI(O) - PLU requested the session (SIMLOG etc)
EX1SLU	RSI(O) - SLU requested the session (USS etc)
EX1SMEN	RSI(O) - Session management exit/takeover not driven
EX1SMET	RSI(O) - Session management exit/takeover driven

Flag Field	Description
------------	-------------

EXRRS12	Related Session Information - byte 2
---------	--------------------------------------

Symbolic names	Description	VTAM 3.3 availability
EX20COSS	RSI(1) - OLU COS substitution has been used	No
EX2SSNO	RSI(1) - Session setup has failed	
EX2SSOK	RSI(1) - Session setup has succeeded	

Flag Field	Description	VTAM 3.3 availability
EXRRSI3	Related Session Information - byte 3	No

Symbolic names	Description	VTAM 3.3 availability
EX3DCOSS	RSI(1) - DLU COS substitution has been used	No

Flag Field	Description	VTAM3.3 availability
IUSEIND	ILU RIC- Usage indicator	No

Symbolic names	Description	VTAM 3.3 availability
ILNXLAT	ILU RIC - This name has not been translated	No
ILXLAT	ILU RIC- This name has been translated	No
ILNTARG	ILU RIC - Resource is not the target (the OLU)	No
ILTARG	ILU RIC - Resource is the target (the DLU)	No

Flag Field	Description
OUSEIND	OLU RIC - Usage indicator

Symbolic names	Description
OLNTARG	OLU RIC - Resource is not the target (the OLU)
OLNXLAT	OLU RIC- This name has not been translated
OLTARG	OLU RIC - Resource is the target (the DLU)
OLXLAT	OLU RIC - This name has been translated

Flag Field	Description
PUSEIND	PLU RIC- Usage indicator

Symbolic names	Description
PLNTARG	PLU RIC - Resource is not the target (the OLU)
PLNXLAT	PLU RIC - This name has not been translated
PLTARG	PLU RIC - Resource is the target (the DLU)
PLXLAT	PLU RIC- This name has been translated

Flag Field	Description
SUSEIND	SLU RIC- Usage indicator

Symbolic names	Description
SLNTARG	SLU RIC - Resource is not the target (the OLU)
SLNXLAT	SLU RIC - This name has not been translated
SLTARG	SLU RIC - Resource is the target (the DLU)
SLXLAT	SLU RIC - This name has been translated

Index

A

ACF2, passwords for user profiles 3.22
ACQUIRE action
 auditing messages from 9.17
 default user profile 2.5
 described 7.15
 introduction 8.3
 protecting sensitive applications 8.3, 8.10
 restrictions 8.21
ACT
 see active control table
actions, VSSE 7.15
 default user profile for ACQUIRE 2.5
active control table
 activating 7.68
 loading 7.68
 loading on remote system 11.3
 replacing with BCT 7.68
administrator
 authority group 3.22
 authority level 3.22
 authority type 3.22
alias names 7.10
ALLOW action
 auditing messages from 9.18
 described 7.15
 filtering audit messages 9.19
 logging audit messages option 7.74
allow MHO administration option 11.5
APPL 7.10
applications
 checking access based on SSCP 8.30
 checking access based on terminal id 8.22
 example rule for protecting 8.4
 preventing access cross domain 8.25
 using VSSE to protect 8.10
 using VSSE to restrict access based on time 8.34
APPLNET 7.12
APPLVTAM 7.11
ARCHIVE FILE CONTROL panel 9.31
archive files
 defining an ESDS for 9.30
 message record layout 9.43
 printing from 9.36
 viewing 9.34
array
 adding a column to 7.44
 adding to a rule 7.35
 changing field order 7.40
 editing 7.37
 editing a column 7.41
 modeling on another 7.35
 moving in a rule 7.36
 overview 7.5
 storing in lookup tables 8.6

auditing
 altering the severity of NC-PASS messages 9.7
 archive file control 9.31
 browsing the message log 9.23
 home node processing 3.59
 message routing 9.4
 overview 9.2
 printing from the message log 9.27
 routing messages according to severity 9.4
 rule propagation 11.17
 SME actions 9.16
 SMF messages 9.34
authority type/group/level
 see administrator
authorization arrays
 see array
AUTHORIZATION CONTROL TABLE CONVERSION
 panel 7.87
AUTOMATIC MESSAGE PROCESSING panel 9.7

B

backup control table
 loading as ACT 7.68
backward compatibility of NC-PASS 7.89
batch processing
 overview 12.2
 processing requirements (users) 12.7
 processing structure 12.2
 UEXITnn functions
 DET1 section 12.5
 DET2 section 12.6
 FINAL section 12.6
 INIT section 12.4
BCT
 see backup control table
BROWSE NC-PASS LOG panel 9.23
browsing the log 9.23
bypass, risk profile keyword 3.8

C

CAF
 record formats 10.5
 report data extraction 10.4
 storing VSSE rule on remote 11.3
central administration file
 see CAF
CKSRDATA 5.5
communication between different versions of NC-PASS 7.88
concurrent NC-PASS systems 2.3
connect data
 CAF record format 10.5
 connecting users to applications 3.26
 storing data on RACF 5.7
CONNECT DEFINITION for USERID panel 3.26
connecting users to applications 3.26
continue logon field, specifying 5.10

- control tables
 - active control table 7.65
 - backout of 7.74
 - backup control table 7.65
 - converting from NC-PASS 1.4 7.83
 - creating 7.19
 - reactivating a backed out table 7.77
 - sending data to other NC-PASS systems 7.69
 - system startup 7.69
 - testing 7.55
 - viewing the outline of 7.31, 7.34
- conversion of NC-PASS 1.4 tables 7.83
 - conversion report 7.86
- CSA
 - example of update request 8.8
 - reusing userid entries 7.80
 - storing userid and related data 7.80
 - timeout period 7.74
 - update requests for userid 7.81
- customization
 - INSTALLATION data field panel display 5.5

D

DATE AND TIME DEFINITIONS panel 6.3

- date display
 - setting format for 2.2
 - year 2000 support 2.2
- date/time definitions
 - CAF record format 10.7
 - creating 6.3
 - end date 6.6
 - modelling on another 6.4
 - samples provided 6.3
 - start date 6.6
 - TIMES field in VSSE 7.13
 - using in risk profiles 3.6, 3.7
 - using in terminal risk profile 3.34
 - using in user risk profile 3.36
 - using in VSSE control table 8.34
 - VSSE field name 7.9
- default action 7.36
- default, risk profile keyword 3.8
- deleting panels from storage 2.9
- deleting user profiles 3.25
- DENY action
 - auditing messages from 9.21
 - described 7.15
 - stopped sessions recovery 7.77
 - stopping a session 7.16
 - stopping sessions option 7.73
- dial-in
 - protecting from unauthorized access 4.3
 - using VSSE to protect 8.28
- DLNETID 7.12
- DLNETLU 7.10
- DLU 7.2
 - list of imaginary fields A.5
- DLUSSCP 7.11
- DOWN command for log browsing 9.24

E

emulators and RACF PassTickets 3.45

- encryption
 - CAF 10.4
 - passwords 3.22
- END command for log browsing 9.24
- escalating terminals/users 3.42
- EVNAMAD 7.12
- EVNAMAO 7.12
- EVNETID 7.12
- EVSSCP 7.11
- EX1AUTO 7.13
- EX1OLU 7.13
- EX1PLU 7.13
- EX1SLU 7.13
- EXIT action 7.15
- EXRRSI1 7.13
- external security database
 - continue logon after error 2.6
 - data validation of NC-PASS data 5.10
 - enabling search of 2.5
 - extracting NC-PASS data from 5.2
 - storing userid profile data in 5.2
 - setting up the system 5.3
- external user profile 5.6
- extracting NC-PASS data from a RACF database 5.8

F

- field names
 - default keywords associated with 5.6
 - storing on an external security database 5.6
- field names, VSSE
 - see VSSE
- filtering SME audit messages 9.19
- FIND command for log browsing 9.24
- flag fields, VSSE 7.9
 - list of A.7
- force, risk profile keyword 3.8

G

GENERAL SYSTEM OPTIONS panel 2.2

- generic names
 - in user risk profiles 3.6
- global options 7.73
- group definitions, VSSE 7.20, 7.52
 - CAF record format 10.6
 - defining group values 7.53

H

home node processing 1.10, 3.47

- audit 3.59
- prerequisites for 3.59
- processing considerations 3.59
- processing overview (TLI) 3.48

I

- ICHP40 5.5
- ICHP422 5.5
- ILNETID 7.12
- ILNETLU 7.10
- ILU 7.2
- ILUSSCP 7.11

imaginary fields
 see *OLU and DLU*
INSTALLATION DATA field
 customization to RACF panel display 5.5
 editing 5.5
 format of entries 5.4
IOP52023 10.2
IOPNSCS 10.2

K

KEYWORD ASSIGNMENT panel 5.14
KEYWORD DEFINITION panel 5.12
keyword definitions, external security database
 changing the keywords for 5.12
 disabling 5.12
 enabling 5.12
 specifying 5.12
keywords, external security database
 assigning 5.14
 defaults associated with field names 5.6
 described 5.4, 5.6
 format of 5.8
 mismatched 5.11
 specifying multiple 5.10
 specifying on RACF database 5.4
keywords, risk profiles 3.8

L

LEFT command for log browsing 9.24
LOAD/RESTORE CONTROL TABLES panel
 description 7.65
 example 7.70
loading an SME Control Table 7.66
lock interval
 specifying in terminal profile 3.19
 specifying in user profile 3.24
 storing data on RACF 5.7
lock, risk profile keyword 3.8
locked terminals
 CAF record format 10.9
 lock interval formula 3.19
 reasons why 3.39
locked users
 lock interval formula 3.24
 reasons why 3.37
log
 browsing 9.23
 NCI 9.28
 printing from 9.27
 routing messages to 9.4
 scroll commands 9.24
 specifying length of 2.3
 writing statistics to 2.14
LOG ON STATISTICS - FULL REPORT panel 10.15
LOG ON STATISTICS - SUMMARY BY DATE panel 10.13
logical units 7.2
logon
 displaying informational messages 2.5
 not allowed before certain date 3.22
 retry maximum 3.22
 statistics 10.12
LOGON DEFAULTS panel 2.5
 continue logon field 5.10
 the search external security database field 5.6

lookup tables (VSSE)
 building 7.81
 example of use 8.8
 exchange of rule information 8.6
 purpose of 7.81
 when used 7.81

lu

 see *logical units*

LU1 7.10
LU1NET 7.12
LU1VTAM 7.11
LU2 7.10
LU2NET 7.12
LU2VTAM 7.11
LU3 7.10
LU3VTAM 7.11

M

MENUNET 7.12
menus
 initial displayed 3.22
MENUVTAM 7.11
MESSAGE ROUTING panel 9.4
messages
 ACQUIRE action 9.17
 ALLOW action 9.19
 auditing facilities 9.2
 automatic processing 9.7
 DENY action 9.21
 destinations of 9.4
 filtering SME audit messages 9.19
 from batch processing
 with NC-PASS active 9.6
 with NC-PASS inactive 9.6
 Netview, entering in user tables 9.3
 printing from the log 9.27
 proprietary security systems 9.38
 record layout
 ESDS 9.43
 SMF 9.42
 routing 9.4
 routing to VSAM ESDS files 9.30
 severity levels 9.4
 text 9.38
 WARN action 9.22
MHO
 CAF record format 10.10
 remote administration via 11.2
 routing messages via 9.37
 transmission log 11.17
model
 creating a date/time definition based on 6.4
 creating a user profile based on 3.20
MSG (TLI keyword)
 FUNCTION=CHECK 3.53
 FUNCTION=LOGON 3.49
multiple keywords, external security database
 examples of using 5.10
 order of matching 5.14
 specifying 5.14

N

NCI
 log control 9.28

NC-PASS
 browsing the log 9.23
 introduction to Authenticator 1.13
 product introduction 1.4
 system shutdown 2.10
 NC-PASS 1.4
 command statement conversion 7.83
 comment lines conversion 7.83
 control statement conversion 7.84
 Network Security Managers 1.2
 NEWPASS (TLI keyword) 3.49
 NEXT action 7.15
 no, risk profile keyword 3.8
 NODE (TLI keyword) 3.49
 node, logon default 2.3
 NON-SWAP startup parameter 2.11
 NPASS (TLI keyword) 3.49
 NULL, symbolic value 7.14

O

OLNETID 7.12
 OLNETLU 7.10
 OLU 7.2
 list of imaginary fields A.5
 OLUSSCP 7.11
 OUTLINE panel 7.49
 OUTPUT (TLI keyword)
 FUNCTION=CHECK 3.53
 FUNCTION=LOGON 3.50

P

panel
 deleting from storage 2.9
 displaying panel number 2.4
 panel/userid toggle 2.4
 PassTicket
 see *RACF PassTickets*
 PASSWORD (TLI keyword) 3.50
 passwords
 for user profiles 3.22
 forcing user to provide 3.8
 specifying change frequency 3.25
 PCT
 see *printer control table*
 PLNETID 7.12
 PLNETLU 7.10
 PLU 7.2
 PLUSSCP 7.11
 printer control table
 described 10.2
 IOP52023 10.2
 IOPNSCS 10.2
 sample code 10.3
 printing
 archived messages 9.36
 from the NC-PASS message log 9.27
 logon statistics 10.12
 reports from administration panels 10.16
 rules 7.34
 user profiles 3.31
 V1.4 authorization table conversion report 7.86
 VTAM printer definitions 2.7
 PROCESS LOCKED TERMINALS panel 3.40
 PROD-MODE startup parameter 2.11

profiles
 described 3.2
 risk 3.5
 specifying terminal 3.18
 specifying user 3.21
 using to verify a user 3.12
 propagating VSSE rules 11.3

R

RACF
 database
 extracting NC-PASS data from 5.8
 INSTALLATION DATA field 5.4
 storing NC-PASS data in 5.4
 using INSTALLATION DATA field 5.5
 PassTicket 3.45
 and emulators 3.45
 configuration 3.45
 PassTickets
 setting on in System Options panel 2.3
 password 3.45
 passwords for user profiles 3.22
 Secured Signon function 3.45
 using to store user risk profile data 5.5
 receiving rules from other systems 11.7
 record formats, CAF 10.5
 REMOTE ADMINISTRATION OPTIONS panel 11.5
 remote administration via MHO 11.2
 report data extraction 10.4
 REPORT PRODUCTION MENU 10.12
 reports
 logon statistics 10.12
 producing from administration panels 10.16
 user profile 3.32
 reset escalated terminals and users 3.43
 restricting access by date and time 6.2
 RETAREA (TLI keyword)
 FUNCTION=CHECK 3.52
 FUNCTION=LOGON 3.49
 RETID (TLI keyword)
 FUNCTION=CHECK 3.53
 FUNCTION=LOGON 3.50
 return codes
 VSSE rule propagation 11.18
 RFIN command for log browsing 9.24
 RIGHT command for log browsing 9.24
 risk profile
 CAF record format 10.8
 combining user and terminal risks 3.6
 date/time definitions in 3.6
 described 3.5
 keyword interpretation 3.8
 storing on RACF 5.5
 terminal
 changing an existing entry 3.33
 creating a new entry 3.33
 example of 3.7
 specifying access routes 3.7
 user
 changing an existing entry 3.35
 creating a new entry 3.35
 example of 3.6
 extracting keywords from 3.6
 routing of messages 9.4
 RULE MAINTENANCE panel 7.33

- rules
 - adding new 7.33, 7.35
 - auditing propagation of 11.17
 - CAF record format 10.6
 - changing 7.33, 7.35
 - default action for 7.36
 - deleting 7.34
 - maximum levels 7.15
 - maximum size 7.15
 - modeling on another 7.33
 - printing 7.34, 7.37
 - example report 7.48
 - sending arrays to other NC-PASSes 8.6
 - storing/loading on remote system 11.3
 - return codes from 11.18
 - viewing the outline of 7.49

S

- SAC, passwords for user profiles 3.22
- SELECT ARCHIVE AND SMF MESSAGES panel 9.34
- sending rules to other systems 11.5
- sensitive application, protecting using ACQUIRE 8.10
- session management exit
 - see SME
- severity level of messages 9.4
- shutting down NC-PASS 2.10
- SLNETID 7.12
- SLNETLU 7.10
- SLU 7.2
- SLUSSCP 7.11
- SME
 - auditing actions 9.16
 - backed out flag 7.77
 - backing out 7.74
 - communication to NC-PASS 7.78
 - Control Tables
 - displaying information about 7.70
 - loading 7.66
 - data passed to by VTAM 7.9
 - enabled flag 7.77
 - enabling 7.73
 - overview 7.5
 - reactivating a backed-out table 7.77
 - stopped sessions recovery 7.77
 - system flag settings 7.77
- SMF
 - message processing using 9.40
 - message record layout 9.42
 - reading and displaying messages from 9.40
 - routing messages to 9.4
 - selecting messages for viewing/printing 9.34
 - writing messages to 9.40
- specifying the use of an external security database 5.6
- statistics
 - displaying system details 2.11
 - logon 10.12
 - writing to the system log 2.14
- stopped sessions 7.77
- storing NC-PASS data on RACF 5.4
- suppressing SME audit messages 9.19
- symbolic names
 - EX1AUTO 7.13
 - EX1OLU 7.13
 - EX1SLU 7.13
 - NULL 7.14
- system date format 2.2

- SYSTEM MONITOR - GENERAL INFORMATION panel 2.11
- SYSTEM MONITOR - LOGGING OPTIONS panel 2.14
- SYSTEM MONITOR - STORAGE USE panel 2.12
- SYSTEM MONITOR - VSM STORAGE panel 2.13
- SYSTEM SHUTDOWN panel 2.10

T

- TDT
 - see *Terminal Definitions Table*
- TERMIN (TLI keyword)
 - FUNCTION=CHECK 3.53
 - FUNCTION=LOGON 3.50
- TERMINAL 7.10
- Terminal Definitions Table
 - defining 3.14
 - defining groups 3.15
 - described 3.3
 - sample TDT 3.14
 - setting variables 3.15
 - statement syntax 3.15
 - GROUP statement 3.16
 - PANEL statement 3.16
 - TERMINAL statement 3.16
 - terminal id not specified in 3.14, 3.15
- terminal idle time 2.3
- terminal profile
 - CAF record format 10.9
 - described 3.3
 - linking to a TDT 3.17
- terminals
 - assigning id to TDT group 3.15
 - defining to NC-PASS 3.14
 - determining the logo panel to be displayed 3.18
 - escalating 3.42
 - imaginary 3.3
 - locked 3.39
 - real 3.3
 - resetting escalated 3.43
 - specifying profiles 3.18
- TERMNET 7.12
- TERMVTAM 7.11
- text messages 9.38
- THISNET 7.12
- THISVTAM 7.11
- time, restricting access by 8.34
- TIMEOUT (TLI keyword)
 - FUNCTION=CHECK 3.53
 - FUNCTION=LOGON 3.50
- TIMES field 7.13
- TOPS
 - passwords for user profiles 3.22
- trace options 2.15
- TRACELEVEL (TLI keyword)
 - FUNCTION=CHECK 3.53
 - FUNCTION=LOGON 3.50
- transaction
 - specifying high risk 3.7
- TXID (TLI keyword) 3.52

U

UEXIT

- processing requirements 12.7
- UEXITnn functions 12.3
- variables 12.4

unlocking users 3.38

UP command for log browsing 9.24

USER PROFILE MAINTENANCE MENU 3.20

user profiles

- CAF record format 10.5
- connection routes 3.26
- creating 3.20
- creating an administrator 3.22
- creating an operator 3.22
- default for modelling 2.3
- default profile for ACQUIRE 2.5
- deleting 3.25
- described 3.4
- listing 3.29
- modelling on another 3.20
- password validation 3.22
- printing 3.31
 - example report 3.32
- risk
 - see risk profile*
- specifying initial menu 3.22

user risk

- storing data on RACF 5.7

USERID (TLI keyword)

- FUNCTION=CHECK 3.52
- FUNCTION=LOGON 3.49

USERID field 7.13

- example of using
 - introduction 8.3
- guidelines for efficient use of 7.82
- propagating arrays containing 7.69, 7.88
- specifying in rules 7.81

userid

- escalating 3.42
- locked 3.37
- resetting escalated 3.43
- specifying as high risk 3.6
- userid/panel toggle 2.4
- using risk profile to protect 4.7

V

validation

- specifying in risk profile 3.6, 3.7, 3.8

verifying a user using risk profiles 3.12

VRM (TLI keyword)

- FUNCTION=CHECK 3.53
- FUNCTION=LOGON 3.50

VSAM ESDS archive files 9.30

VSSE

- actions 7.15
- alias names 7.10
- checking access based on date/time 8.34
- control operator functions 7.76
- field name types 7.9
- field names list A.2
- group definitions 7.20
- introduction to 1.5
- list of flags A.7
- lookup tables 8.6
- lu related fields 7.10
- NC-PASS fields 7.13
- network related data fields 7.12
- overview 7.5
- protecting sensitive applications from dial-in 8.10
- session request related data fields 7.13
- setting global options 7.73
- stopped sessions recovery 7.77
- storing/loading rules on remote systems 11.3
- types of field 7.9
- using to protect dial-in lines 8.28
- VTAM (SSCP) related data fields 7.11

VSSE OPTIONS menu 7.32

VTAM

- introduction to sessions 7.2
- printer definitions 2.7

VTAM PRINTER DEFINITIONS panel 2.7

W

WARN action

- auditing messages from 9.22
- described 7.15

X

XMS

- communication from the SME to NC-PASS 7.79

XMSID (TLI keyword)

- FUNCTION=CHECK 3.52
- FUNCTION=LOGON 3.49

XMSOPT (TLI keyword)

- FUNCTION=CHECK 3.53
- FUNCTION=LOGON 3.51

Y

year 2000, support for 2.2

yes, risk profile keyword 3.8

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 PSA1001.003 - 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

S
e
c
u
r
e

A
d
m
i
n
i
s
t
r
a
t
i
o
n

M
a
n
u
a
l