SECURITRE

Reference Manual

Note: All references to the SECURITRE version in this manual are indicated by *vrs* or *v.r.s.* The current release of SECURITRE is version 4.2.2.

Comments pertaining to this document and the SECURITRE package are encouraged. Please direct all comments to:

Treehouse Software, Inc.
2605 Nicholson Road, Suite 1230
Sewickley, PA 15143
Phone: 724.759.7070
Fax: 724.759.7067
e-mail: tsi@treehouse.com
http://www.treehouse.com

Worldwide marketing of SECURITRE and other products of Treehouse Software, Inc. (TSI) is handled through the Sewickley office.

Last Updated: December 30, 2021

* In this document, CA-ACF2 is referred to as ACF2, and CA-TOP SECRET is referred to as TOP SECRET or TSS.

LIST OF FIGURES

This page intentionally left blank.

SECTION I

INTRODUCTION

I.1 SECURITRE Documentation

The structure of the SECURITRE documentation is intended to make information about the product more convenient to locate and use.

Treehouse Software, Inc. (TSI) provides two manuals for SECURITRE. In order to successfully install and use SECURITRE, both manuals are required.

Administrator Guide
The Administrator Guide provides detailed explanations for installing, setting up, and tailoring SECURITRE to site-specific needs.

The Administrator Guide explains how to install and prepare SECURITRE for use by using a simple, efficient process. It explains installation details for SECURITRE modules and adjustments necessary in RACF, ACF2, and TOP SECRET. It also explains the few primary parameters and modules necessary to get SECURITRE running in a TEST environment, giving several comprehensive examples. Once SECURITRE is operational, it is necessary to view the SECURITRE Reference Manual for information about placing SECURITRE into PRODUCTION, fine tuning, and defining less frequently used parameters.

Reference Manual
The Reference Manual provides detailed reference material about the various SECURITRE functions and features.

The Reference Manual is intended for reference use after the product has been installed and its successful operation has been verified. The Reference Manual lists and describes the items that are typically referenced. Parameters are listed in alphabetical order, and Error Codes are listed in numeric order. There is little introductory discussion in this manual.

The nature of security precludes giving detailed security information or describing security techniques to all except those with a need for the information. Therefore, there is no "User Manual" with SECURITRE. The "users" in this case are end-users and applications programmers. These personnel do not normally need to know if security is in effect or how it is employed. They only need to know that they should report to their management if they receive a security violation message.

Those people with a need for SECURITRE information include:

- The highest level of management to be assured their data and applications are secure
- The Security Administrator, Auditors, and the Security Staff
- The DBA and/or DBA Staff
- The NATURAL Administrator(s)
- The System Programmers and Operations Staff for installation help
- The Applications Analysts and Project Leaders to understand SECURITRE's Application Security features (STRNAT and STRASM)

Additional documentary materials of value to SECURITRE sites are available from TSI free of charge. These include:

- Product Overview
- Fact Sheet

The following sections are presented in this Reference Manual:

- SECURITRE for ADABAS Nucleus
- SECURITRE for NATURAL
- SECURITRE for ADABAS Utilities
- Real-time Monitor
- Internal Application Security Features (STRNAT and STRASM)

I.2 Introduction to SECURITRE

Most IBM (and compatible) mainframe installations rely on one of three major operating System Security Facilities (SSFs) (i.e., RACF, ACF2, or TOP SECRET) to control access to their non-ADABAS data and non-NATURAL applications. These facilities provide centralized security administration for all such applications and datasets available on the computer system.

Centralized control of the security function is essential to promoting the integrity and safety of the computerized applications. ADABAS and NATURAL do not interface directly with these centralized security systems. Instead, ADABAS and NATURAL have their own security mechanisms.

SECURITRE provides an interface that allows all ADABAS/NATURAL related security rules to reside in the SSF, enabling all security data to exist as part of a single rule base. The single rule base provides better security and makes it much easier to manage changes in the security environment.

With SECURITRE in place, the process of controlling access to ADABAS and NATURAL is simplified and centralized. The SSF controls access to ADABAS data and NATURAL environments at all levels, eliminating the need for separate ADABAS and NATURAL security control mechanisms and separate security files and application-based security logic.

A full introduction to the principle of Central Security Management and a more detailed introduction to SECURITRE are presented in the Introduction Section of the Administrator Guide.

SECTION II

SECURITRE FOR ADABAS NUCLEUS

II.1 SECURITRE for ADABAS - Parameters

SECURITRE has been designed to enable the Security Administrator to easily tailor SECURITRE to meet site-specific requirements. Through the use of parameters, a site customizes SECURITRE for ADABAS according to its needs. Tables and full descriptions of these parameters appear later in this section. The two parameter statements (macros) provided include:

```
STRDEF         specifies SECURITRE DEFault settings
STRFNR         specifies SECURITRE file (FNR) overrides
```

STRDEF parameters make it possible for the Security Administrator to specify actions that should be taken by SECURITRE on a global basis. Many of the STRDEF parameters may be overridden at the file level by STRFNR parameters. In most cases, STRDEF makes it possible to define the processing rules to SECURITRE for all the files in a database with only few STRFNR statements for "special case" files.

For Example:

```
STRDEF         Defaults pertaining to site standards, and general file security for
               the database
STRFNR         Exceptions for file 10
STRFNR         Exceptions for files 20-25, 27
STRFNR         Exceptions for file 32
```

```
STRFNR END     This must always be the last STRFNR macro invocation!
```

The specifications of STRDEF and STRFNR statements make up the SECURITRE parameters, or "STRPARMS." **A set of STRPARMS must be generated for use with each database.** These are to be named STP99999, where '99999' refers to the database number in the range 00001-65535. When SECURITRE is run on a particular database, SECURITRE expects to find a 'STRPARMS' module, named appropriately for the database, in the ADABAS Load Library.

II.2 STRDEF Statement

The purpose of the STRDEF statement is to specify default SECURITRE settings. Only one STRDEF statement may be coded for each STRPARMS module.

The reference format for the STRDEF and STRFNR parameters is standard macro assembler format:

- Opcode in column 10
- One or more spaces
- Operands up to column 71, separated by commas
- Continuation symbol (x) in column 72
- Continuation lines start in column 16

In the following figure, the column entitled **STRFNR Override?** indicates (Yes or No) if the STRDEF parameter can be overridden by an STRFNR parameter.

STRDEF Parameter	Function	Valid Values	Default Value	STRFNR Override?
CLASS	Dataset class name	Any value defined to the SSF	DATASET	N
CALLSAF	Indicates if all DB calls are to be sent to the customer's security product or only the first applicable call	FIRST OR ALL	FIRST	Y
CMDLOG	Indicates whether to request command logging in User-Exit-4	ON or OFF	OFF	N
DELIM	Delimiter character in the DSN	any character or null ('')	. (period)	Y
DSNORDR	Order to generate the DSN for File Security	any combination of up to eight of the following: CMD, DBID, FIELD, FILE, GPGM, JOB, NLIB, NODE, NPGM, TERM, TPMON, or TRAN	FILE	Y
DSNPOOL	Number of DSNs to maintain in User-Exit-1 DSN table	1 to 10000	100	N
EX1ALL	Calls STREX1 for documented and undocumented ADABAS commands	ON or OFF	OFF	N
FILEMAX	Specifies the maximum number of files to secure	OLD (255 files) NEW (65535 files)	OLD	N
FLSDEL	Literal to be included in place of FIELD in the DSNORDR during a delete command	any string up to eight characters	DELETE	Y

Figure 1 – STRDEF Parameters
(continued on next page)

(continued from previous page)

STRDEF Parameter	Function	Valid Values	Default Value	STRFNR Override?
FLSPOOL	Number of ADABAS Command-IDs for which SECURITRE may maintain information during Field Level Security processing	0 to 50, must be divisible by 10	20	N
FORCE	Hour to purge user tables	0 to 23 or 99	99 (never purge)	N
LOGVIOL	Specifies which violations (for each file) should be logged by the SSF	ALL or FIRST	ALL	Y
MODE	SECURITRE file protection mode setting	DORMANT, WARN, or FAIL	FAIL	Y
NOIDRED	Action to take when no User-ID is found for a READ command	ACCEPT or REJECT	REJECT	Y
NOIDUPD	Action to take when no User-ID is found for an UPDATE command	ACCEPT or REJECT	REJECT	Y
N2OPREF	DSN Prefix generated for N2O security	any value up to 17 characters	CONTROL.N2O	N
PREFIX	DSN prefix (first part of DSN)	any value up to 17 characters	ADABAS.STR	Y
PRINT	Assembler PRINT directive	GEN or NOGEN	NOGEN	N
PROCCL	Indicates whether USERID table entries should be processed (removed) when an ADABAS CL command is received	ON or OFF	ON	N
PROCEX2	Indicates whether SECURITRE User-Exit-2 should be invoked	ON or OFF	OFF	Y
PURINTT	Seconds user must remain inactive to be purged from internal table	any positive integer value	0	N

Figure 1 – STRDEF Parameters

(continued on next page)

(continued from previous page)

STRDEF Parameter	Function	Valid Values	Default Value	STRFNR Override?
PURINTV	Interval at which inactive users should be purged (in hours)	0, 1, 2, 3, 4, 6, 8, 12, or 24	0 (do not purge)	N
QUALIFY	DSN name qualifier (second part of DSN)	any value up to eight characters or null ('')	PROD	Y
RACHECK	Type of check to be used when calling the SSF (for future use)	RACHECK	RACHECK	N
RTMORDR	Order to generate the DSN to secure the SECURITRE RTM	any combination FUNC and/or DBID	(FUNC, DBID)	N
SECURE	SSF in use at the installation	RACF, ACF2, or TSS	RACF	N
STREX1	Specifies a user-exit to SECURITRE when USERID is unknown	load module name	no default value	N
STREX2	Specifies a user-exit to SECURITRE after an ADABAS command has passed security checks	load module name	no default value	N
STREX3	Specifies a user-exit to SECURITRE when SECURITRE is in an unrecoverable ABEND situation.	load module name	no default value	N
STREX4	Reserved	N/A	N/A	N
STRRTM	DSN prefix generated for the SECURITRE RTM	any value up to 17 characters	CONTROL.STR	N
TERM	Stop or Terminate SECURITRE RTM NATURAL programs	S or T	S	N
TRACE	Specifies if diagnostic trace messages should be produced during execution	ON or OFF	OFF	N
TRACEDD	Defines the DD-name and SYSOUT class for trace messages	(ddname,c)	(STRTRC,H)	N
TRMRTM	DSN prefix generated for the TRIM RTM	any value up to 17 characters	CONTROL.TRM	N
UEXIT11	Specifies a second ADABAS User-Exit-11 to be invoked by SECURITRE	load module name	no default value	N

Figure 1 – STRDEF Parameters

(continued on next page)

(continued from previous page)

STRDEF Parameter	Function	Valid Values	Default Value	STRFNR Override?
USERID	Primary method used to find the User-ID	See description of USERID= below for details.	TSIUEX1G	N
USERID2	Alternate method used to find the User-ID	NONE See description of USERID= below for details	NONE	N
USERS	Number of users to maintain in the internal SECURITRE table	1 to 10000	100	N
USRPOOL	Number of user-to-DSN relationship segments to maintain in the internal SECURITRE table	4 to 20000, must be equally divisible by 4	400	N
UTMODE	Utility Security protection mode setting	DORMANT, WARN, or FAIL	WARN	N
UTORDER	Order to generate the DSN for Utility Security	any combination of UTIL, FUNC, and/or FILE	(UTIL, FUNC, FILE)	N
UTPREF	DSN prefix for ADABAS Utility runs	any value up to 17 characters	ADAUTIL	N

Figure 1 – STRDEF Parameters

II.3 STRDEF Parameters

CALLSAF

Indicates if all DB calls are to be sent to the customer's security product or only the first applicable call. **NOTE**: LOGVIOL=FIRST is *incompatible* with CALLSAF=ALL.

Valid Values:	FIRST or ALL
Default Value:	FIRST
Assigned By:	STRDEF and STRFNR

CLASS

The resource class to be used by SECURITRE when requesting authorization information from the SSF.

Valid Values:	any value defined to the SSF
Default Value:	DATASET
Assigned By:	STRDEF only

CMDLOG

Indicates whether to request command logging in ADABAS User-Exit-4. Since the last User-Exit-4 to be invoked decides whether to log commands, the CMDLOG parameter is useful only if STRUEX4 is the only ADABAS User-Exit-4 installed. CMDLOG has no effect if the User-Exit-4 processing is handled by TRIM.

Valid Values:	ON or OFF
Default Value:	OFF
Assigned By:	STRDEF only

DELIM

The delimiter character to be placed between the PREFIX, QUALIFY, and DSNORDR parameter items when generating a DSN for authorization requests to the SSF when no overriding STRFNR DELIM parameter has been specified for a given file.

Valid Values:	any character or null ('')
Default Value:	. (period)
Assigned By:	STRDEF and STRFNR

DSNORDR The order in which the DSN should be generated after the PREFIX and QUALIFY parameters when no overriding STRFNR DSNORDR parameter has been specified for a given file. SECURITRE will generate the DSN beginning with the PREFIX and QUALIFY parameters, and then add items to the DSN according to the order specified in the DSNORDR parameter. DSNORDR can only be used if SECURITRE obtains the User-ID using method TSIUEX1G because this feature obtains information from the SECURITRE USERINFO area, which is created from the SECURITRE Link-Exit-1. It will not include items that are meaningless in the context of the call. For example, it will not try to include a CICS Transaction-ID if the call does not originate from CICS.

DSNs generated by SECURITRE are limited to 44 characters. When SECURITRE determines that adding an item to the DSN exceeds this limit, it will not include any of the remaining items. Up to eight of the components below may be included, in any order:

CMD The two-character ADABAS command code for this call.

DBID The Database-ID and the file number of the FUSER file being used when a call is made from a NATURAL program. If both the FUSER Database-ID and the file number are less than 256, this item will be formatted as DxxxFyyy, where 'xxx' is the Database-ID and 'yyy' is the FUSER file number. If either the FUSER Database-ID or the file number is greater than 255, this item will be formatted as Dxxxxx.Fyyyyy, where 'xxxxx' is the Database-ID and 'yyyyy' is the FUSER file number. This item will only be included for calls originating from NATURAL.

FIELD The field alias obtained from the FIELDS= parameter in the STRFNR statement. FIELD is only included in the generated DSN when Field Level Security is being checked for a command.

FILE The file number for the file being accessed. The value given the file number consists of the literal 'F' followed by the file number, such as F100 for a file number less than 256 or F00376 for a file number greater than 256. Otherwise, the value given to the file number consists of the file name as assigned in the STRFNR alias NAME parameter, such as PERSONL.

GPGM The non-NATURAL program name. This item will only be included for calls NOT originating from NATURAL.

JOB The MVS Jobname of the job being executed by the user.

DSNORDR (continued from previous page)

<u>NLIB</u>	The NATURAL Library. This item will only be included for calls originating from NATURAL.
<u>NODE</u>	The SMFID of the CPU from which the call originates. If the value given as the SMFID begins with a numeric value, the literal 'N' will be followed by the SMFID. For example, if SMFID=1234 then NODE=N1234, and if SMFID=CPU1 then NODE=CPU1.
<u>NPGM</u>	The NATURAL program name. This item will only be included for calls originating from NATURAL.
<u>TERM</u>	The CICS Terminal-ID. This item will only be included for calls originating from CICS.
<u>TPMON</u>	The TP monitor. Possible values are TSO, STC, CICS, CMS, JOB (for batch), and COMP (COM-PLETE).
<u>TRAN</u>	The CICS Transaction-ID. This item will only be included for calls originating from CICS.
Valid Values:	CMD, DBID, FIELD, FILE, GPGM, JOB, NLIB, NODE, NPGM, TERM, TPMON, or TRAN
Default Value:	FILE
Assigned By:	STRDEF and STRFNR

Note: The DSNORDR parameter may be overridden at the file level in the STRFNR parameters. Therefore, it is possible to set up some files for very strict security requirements, while leaving other files less stringently secured.

DSNPOOL

The maximum number of DSNs to be maintained at a given time in the SECURITRE internal DSN table in User-Exit-1. A higher value will allow more DSNs to be maintained in the DSN table, but will require more storage for User-Exit-1.

Valid Values:	1 to 10000
Default Value:	100
Assigned By:	STRDEF only

EX1ALL

Specifies whether SECURITRE should call STREX1 for every ADABAS command, including unsecured commands, or only for commands where SECURITRE needs to obtain a User-ID.

ON — SECURITRE will call STREX1 for all commands, including unsecured commands.

OFF — SECURITRE will call STREX1 only when it needs to obtain a User-ID.

Valid Values:	ON or OFF
Default Value:	OFF
Assigned By:	STRDEF only

FILEMAX

Specifies the type of parameters that should be generated when the 'STRPARMS' are assembled.

NEW — New style parameters will be generated. This allows for files 1 - 65535 to be specified in the STNFILE. If file numbers greater than 255 are accessed, NEW must be specified.

OLD — The old style parameters will be generated. It allows for files 1 - 255 to be secured. If file numbers greater than 255 are accessed, NEW must be specified.

Valid Values:	NEW or OLD
Default Value:	OLD
Assigned By:	STRDEF only

FLSDEL

The literal to be included in place of FIELD in the DSNORDR when Field Level Security is being checked and the ADABAS command code is E1 or E4 (delete).

Valid Values:	any string up to eight characters
Default Value:	DELETE
Assigned By:	STRDEF and STRFNR

FLSPOOL

The number of ADABAS Command-IDs for which SECURITRE should maintain information during Field Level Security processing. This parameter should equal the average number of CIDs, rounded up to a factor of 10, which will be in use at any given time against a file for which Field Level Security is in effect.

Valid Values:	0 to 50 (must be divisible by 10)
Default Value:	20
Assigned By:	STRDEF only

FORCE

The hour at which SECURITRE should clear the internal tables of all access information. The value '99' indicates to SECURITRE that it should not purge its internal tables at any particular hour. (There are other instances of table purging, described later.)

Valid Values:	0 to 23 or 99
Default Value:	99 (never purge)
Assigned By:	STRDEF only

LOGVIOL

The logging action to be taken when multiple violations are made by a user accessing a DSN and no overriding STRFNR LOGVIOL parameter has been specified for a given file. **NOTE**: LOGVIOL=FIRST is *incompatible* with CALLSAF=ALL.

ALL — SECURITRE will cause the SSF to log all violations by a given user to a given DSN.

FIRST — SECURITRE will cause the SSF to log only the first violation by a given user to a given DSN.

Valid Values:	ALL or FIRST
Default Value:	ALL
Assigned By:	STRDEF and STRFNR

MODE

The level of security to be activated when a file is being accessed and no overriding STRFNR MODE parameter has been specified for a given file.

DORMANT — SECURITRE will not make any security checks and will allow all calls to be processed by ADABAS. In effect, SECURITRE does nothing. DORMANT mode is useful for verifying the correct installation of SECURITRE, and for phasing in SECURITRE control, one or more files at a time.

WARN — SECURITRE will make security checks, cause the SSF to log any violations, and will allow all calls to be processed by ADABAS. WARN mode is provided so that installations can easily migrate to SECURITRE from their existing security arrangement.

FAIL — SECURITRE will make security checks, cause the SSF to log any violations, and prohibit ADABAS from processing unauthorized commands.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	FAIL
Assigned By:	STRDEF and STRFNR

NOIDRED

The action SECURITRE will take when the User-ID for a READ command cannot be found when no overriding STRFNR NOIDRED parameter has been specified for the given file.

ACCEPT — SECURITRE will allow READ commands to be processed when no User-ID is found.

REJECT — SECURITRE will prevent READ commands from being processed when no User-ID is found.

Valid Values:	ACCEPT or REJECT
Default Value:	REJECT
Assigned By:	STRDEF and STRFNR

NOIDUPD

The action SECURITRE will take when the User-ID for an UPDATE command cannot be found when no overriding STRFNR NOIDUPD parameter has been specified for the given file.

ACCEPT — SECURITRE will allow UPDATE commands to be processed when no User-ID is found.

REJECT — SECURITRE will prevent UPDATE commands from being processed when no User-ID is found.

Valid Values:	ACCEPT or REJECT
Default Value:	REJECT
Assigned By:	STRDEF and STRFNR

N2OPREF

Specifies to SECURITRE what literal to use at the beginning of the DSN it generates when requesting authorization from the SSF for a particular user to access N_2O. This parameter is only effective at installations where TSI's N_2O is installed.

Valid Values:	any string up to 17 characters
Default Value:	CONTROL.N2O
Assigned By:	STRDEF only

PREFIX

The first part of the DSN to use when calls are made to the SSF when no overriding STRFNR PREFIX parameter has been specified for a given file.

Valid Values:	any string up to 17 characters
Default Value:	ADABAS.STR
Assigned By:	STRDEF and STRFNR

PRINT

Indicates whether to print the macro expansions of the STRDEF and STRFNR statements when they are assembled.

GEN — Causes macro expansions to be printed in the listing. Using GEN will result in a significantly longer listing.

NOGEN — Suppress macro expansions in the listing.

Valid Values:	GEN or NOGEN
Default Value:	NOGEN
Assigned By:	STRDEF only

PROCCL

Indicates whether or not user table entries should be removed when an ADABAS CL command is received. PROCCL should be set to OFF for databases which process a high number of CL commands, such as databases that are accessed by ADASQL.

Valid Values:	ON or OFF
Default Value:	ON (remove)
Assigned By:	STRDEF only

PROCEX2

Indicates whether or not SECURITRE User-Exit-2 should be invoked after an ADABAS command passes file level and field level security checks.

Valid Values:	ON or OFF
Default Value:	OFF
Assigned By:	STRDEF and STRFNR

PURINTT

The number of seconds that a user must remain inactive before their entries are purged from the internal tables.

Valid Values:	any positive integer value
Default Value:	0
Assigned By:	STRDEF only

PURINTV

The interval, in hours, at which SECURITRE should scan its tables for inactive users and remove these users from its tables. If a value of 0 (zero) is specified, SECURITRE will not purge inactive users from the table.

Valid Values:	0, 1, 2, 3, 4, 6, 8, 12, or 24
Default Value:	0 (do not purge)
Assigned By:	STRDEF only

QUALIFY

The second level of the DSN to be used by SECURITRE when requesting authorization from the SSF when no overriding STRFNR QUALIFY parameter has been specified for a given file.

Valid Values:	any string up to eight characters or null ('')
Default Value:	PROD
Assigned By:	STRDEF and STRFNR

RACHECK

The type of check to be used by SECURITRE when calls are made to the SSF.

Valid Values:	RACHECK
Default Value:	RACHECK
Assigned By:	STRDEF only

RTMORDR Specifies what order the DSN components should be included in the DSN for Real-Time Monitor (RTM) Security. Either or both of the components below may be included, in any order.

DBID The Database-ID. The DSN generated will consist of the STRRTM PREFIX, the literal 'D', followed by the DBID. For example, CONTROL.STR.D007 for a database less than 256 or CONTROL.STR.D00456 for a database greater than 255.

FUNC The RTM function accessed by the user. The DSN generated will consist of this STRRTM PREFIX followed by the FUNC, such as CONTROL.STR.PARM. The values for FUNC are listed in the Real-time Monitor section of this manual.

Valid Values:	FUNC or DBID
Default Value:	(FUNC,DBID)
Assigned By:	STRDEF only

SECURE The System Security Facility in use at the installation.

RACF RACF is in use.

ACF2 ACF2 is in use.

TSS TOP SECRET is in use.

Valid Values:	RACF, ACF2, or TSS
Default Value:	RACF
Assigned By:	STRDEF only

STREX1 The SECURITRE User-Exit-1 to be invoked in the event that SECURITRE cannot determine the USERID issuing the command to ADABAS. The name provided must be the name of the load module for which SECURITRE will issue a LOAD. For more information, refer to the STREX1 User-Exit section of the SECURITRE Administrator Guide.

Valid Values:	a valid load module name
Default Value:	no default value
Assigned By:	STRDEF only

STREX2 The SECURITRE User-Exit-2 to be invoked after a command has passed file level and field level security checks for files with the PROCEX2 parameter set to ON. The name provided must be the name of the load module for which SECURITRE will issue a LOAD. For more information, refer to the STREX2 User-Exit section of the SECURITRE Administrator Guide.

Valid Values:	a valid load module name
Default Value:	no default value
Assigned By:	STRDEF only

STREX3

The SECURITRE User-Exit-3 to be invoked when SECURITRE is in an unrecoverable ABEND situation. The name provided must be the name for the load module for which SECURITRE will issue a LOAD. For more information, refer to the STREX3 user-exit section of the SECURITRE Administrator Guide.

Valid Values:	a valid load module name
Default Value:	no default value
Assigned By:	STRDEF only

STREX4

Reserved for future use.

STRRTM

Specifies to SECURITRE what literal to use at the beginning of the DSN it generates for SECURITRE Real-Time Monitor (RTM) Security.

Valid Values:	any string up to 17 characters
Default Value:	CONTROL.STR
Assigned By:	STRDEF only

TERM

The action to be taken by the SECURITRE RTM NATURAL programs upon their completion.

S	Stop SECURITRE RTM NATURAL programs.
T	Terminate SECURITRE RTM NATURAL programs.
Valid Values:	S or T
Default Value:	S
Assigned By:	STRDEF only

TRACE

Controls the production of diagnostic trace messages written by SECURITRE during execution. Trace messages will be written out to the STRTRC dataset (see. TRACEDD keyword below).

Valid Values:	ON or OFF
Default Value:	OFF
Assigned By:	STRDEF only

TRACEDD

Defines the DD-name and the Sysout class for the diagnostic trace messages. If DD-name is not allocated in the ADABAS start-up JCL, it will be dynamically allocated and assigned to SYSOUT=c, as specified by the second sub-parameter.

Valid Values:	(ddname,class)
Default Value:	(STRTRC,H)
Assigned By:	STRDEF only

TRMRTM

Specifies to SECURITRE what literal to use at the beginning of the DSN it generates when requesting authorization from the SSF for a particular user to access the TRIM Real-Time Monitor (RTM). This parameter is only effective at installations where TSI's TRIM RTM is installed.

Valid Values:	any string up to 17 characters
Default Value:	CONTROL.TRM
Assigned By:	STRDEF only

UEXIT11 The name of a second ADABAS UEX11 to be invoked by SECURITRE (User-Exit-11) after it completes its own processing. The name provided must be the name of the load module that SECURITRE User-Exit-11 will LOAD.

Valid Values:	a valid load module name
Default Value:	no default values
Assigned By:	STRDEF only

USERID The primary method SECURITRE should use to locate the correct SSF User-ID for access authorization purposes. If this method does not locate the User-ID, the method indicated by USERID2 will be used.

TSIUEX1G The ADABAS SSF User-ID will be retrieved from the SECURITRE Link-Exit-1 generated USERINFO Area.

TRIMV4-1 The ADABAS SSF User-ID will be determined from the Additions-3 field in the ADABAS Control Block.

TRIMV4-2 The ADABAS SSF User-ID will be determined from the Additions-4 field in the ADABAS Control Block.

Note: **ALT-1 and** TRIMV5/TRIMV6 are no longer supported,
TSIUEX1G should be used instead of TRIMV5/6.

ALT-2 The ADABAS SSF User-ID will be retrieved from the ADABAS USERINFO area, generated through certain link routines in effect for performance monitors other than TRIM.

CQXAESI The ADABAS SSF User-ID will be retrieved from the area pointed to by CQXAESI

STREX1 The ADABAS SSF User-ID will be obtained from STREX1.

Default Value:	TSIUEX1G
Assigned By:	STRDEF only

USERID2 The method SECURITRE should use to locate the correct SSF User-ID for access authorization purposes if the primary method (USERID) is unable to locate the User-ID.

r

Default Value: NONE
Assigned By: STRDEF only

See description for USERID above for details.

USERS The maximum number of users to be maintained in the SECURITRE internal user table at any given time. The value assigned to USERS is dependent on site requirements. A higher value will allow more users to be maintained in the user table, but it will require more storage for User-Exit-11.

Valid Values: 1 to 10000
Default Value: 100
Assigned By: STRDEF only

USRPOOL

The maximum number of User-to-DSN relationship segments to maintain in the SECURITRE internal table in User-Exit-11. A higher value will allow more relationships to be maintained in the User-to-DSN relationship table but will require more storage for User-Exit-11.

Valid Values:	4 to 20000 (must be divisible by 4)
Default Value:	400
Assigned By:	STRDEF only

UTMODE

The level of security activated when a user attempts to run an ADABAS utility.

<u>DORMANT</u> SECURITRE will not make any security checks and will allow the utility to be executed by ADABAS.

<u>WARN</u> SECURITRE will make security checks, cause the SSF to log any violations, and will allow the utility to be executed by ADABAS.

<u>FAIL</u> SECURITRE will make security checks, cause the SSF to log any violations, and will prevent any unauthorized utilities to be processed by ADABAS.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	WARN
Assigned By:	STRDEF only

UTORDER

The order in which the DSN should be generated after the UTPREF parameter when a call is made to the SSF for Utility Security. Any or all of the components below may be included, in any order.

<u>FILE</u> The file number for the file being accessed, or the file name as assigned in the STRFNR alias NAME parameter, such as PERSONL. The value given to the file number consists of the literal 'F' followed by the file number, such as F100.

Note: If the file number or Database-ID is greater than 255, the value given to the file number will be formatted as 'Fnnnnn,' where 'nnnnn' is the file number (e.g., F00100 or F01234), and the value given to the Database-ID will be formatted as 'Dxxxxx,' where 'xxxxx' is the Database-ID (e.g., D00100 or D01234).

<u>FUNC</u> The utility function accessed by the user.

<u>UTIL</u> The last 3 characters of the utility name, such as ULD, for ADAULD.

For more information about possible values for FUNC and UTIL, refer to the ADABAS Utility Control section of this manual.

Valid Values:	UTIL, FUNC, or FILE
Default Value:	(UTIL,FUNC,FILE)
Assigned By:	STRDEF only

UTPREF The first part of the DSN to use when calls are made to the SSF for Utility Security.

Valid Values:	any string up to 17 characters
Default Value:	ADAUTIL
Assigned By:	STRDEF only

II.4 STRFNR Statement

The purpose of the STRFNR statement is to allow the Security Administrator to specify how SECURITRE is to process specific ADABAS files. When specified, the STRFNR statement parameters override the STRDEF default values for particular files. If there is no STRFNR statement specified for a particular file, the STRDEF default values will be used.

Only one STRFNR statement may be coded related to each file. Each STRFNR statement must contain a FILE parameter and at least one other parameter that applies to the file or files referenced. Unlike STRDEF, multiple STRFNR statements may be coded, as long as no two STRFNR statements reference the same file. STRFNR statements can refer to a single file, multiple files, or a range of files.

Figure 2 lists the STRFNR parameters, their uses, their valid values, and their default values.

STRFNR Parameter	Function	Valid Values	Default Value
CALLSAF	Indicates if all DB calls are to be sent to the customer's security product or only the first applicable call	FIRST or ALL	FIRST (from STRDEF)
DSNORDR	Order to generate the DSN for File Security for the specified file(s)	any combination of up to eight of the following: CMD, DBID, FIELD, FILE, GPGM, JOB, NLIB, NODE, NPGM, TERM, or TRAN	FILE (from STRDEF)
FIELDS	Specifies the ADABAS field names of the fields for which Field Level Security processing should be performed, as well as an alias to be included in the DSN for each of the fields	any number of pairs of 2-character ADABAS field name/8-character alias	no default value
FILE	Specifies to which file or range of files the parameters apply	0 to 65535 or a range	no default value

Figure 2 – STRFNR Parameters

(continued on next page)

(continued from previous page)

STRFNR Parameter	**Function**	**Valid Values**	**Default Value**
FLSDEL	Literal to be included in place of FIELD in the DSNORDR during a delete command	any string of up to eight characters	DELETE (from STRDEF)
FLSMODE	Level of Field Level Security to be activated for this file	DORMANT, WARN, or FAIL	DORMANT
LOGVIOL	Specifies which violations for the specified file(s) should be logged by the SSF	ALL or FIRST	ALL (from STRDEF)
MODE	SECURITRE protection mode setting to be used for the specified file(s)	DORMANT, WARN, or FAIL	FAIL (from STRDEF)
NAME	Specific name to be used for the specified file(s) when calling the SSF	any value up to 17 characters	'F' followed by a 3-digit file number if < 256 or 5-digit if > 255
NOIDRED	Action to take against the specified file(s) when no User-ID is found for a READ command	ACCEPT or REJECT	REJECT (from STRDEF)
NOIDUPD	Action to take against the specified file(s) when no User-ID is found for an UPDATE command	ACCEPT or REJECT	REJECT (from STRDEF)
PREFIX	DSN prefix (first part of DSN) for the specified file(s)	up to 17 characters	ADABAS. STR (from STRDEF)
PROCEX2	Indicates whether SECURITRE User-Exit-2 should be invoked	ON or OFF	OFF (from STRDEF)
QUALIFY	DSN name qualifier (second part of DSN) for the specified file(s)	any value up to eight characters or null ('')	PROD (from STRDEF)
TRACE	Specifies whether or not diagnostic trace messages should be produced during execution	ON or OFF	OFF (from STRDEF)

Figure 2 – STRFNR Parameters

Note: The FIELDS and FLSMODE parameters related to specific file(s), can only be specified as STRFNR parameters, they cannot be specified in STRDEF.

II.5 STRFNR Parameters

CALLSAF Indicates if all DB calls are to be sent to the customer's security product or only the first applicable call. **NOTE**: LOGVIOL=FIRST is *incompatible* with CALLSAF=ALL.

Valid Values:	FIRST or ALL
Default Value:	FIRST
Assigned By:	STRDEF and STRFNR

DELIM The delimiter character to be placed between the PREFIX, QUALIFY, and DSNORDR parameter items when generating a DSN for authorization requests to the SSF for the specified files.

Valid Values:	any character or null ('')
Default Value:	. (period)
Assigned By:	STRDEF and STRFNR

DSNORDR The order in which the DSN should be generated after the PREFIX and QUALIFY parameters for the specified file(s). SECURITRE will stop generating the DSN when it calculates that an additional item will cause the DSN to be longer than 44 characters. Up to eight of the components below may be included in any order.

CMD The two-character ADABAS command code for this call.

DBID The Database-ID and the file number of the FUSER file being used when a call is made from a NATURAL program. If both the FUSER Database-ID and the file number are less than 255, this item will be formatted as DxxxFyyy, where 'xxx' is the Database-ID and 'yyy' is the FUSER file number. If either the FUSER Database-ID or the file number is greater than 255, this item will be formatted as Dxxxxx.Fyyyyyy, where 'xxxxx' is the Database-ID and 'yyyyy' is the FUSER file number. It will only be included for calls originating from NATURAL.

FIELD The field alias obtained from the FIELDS= parameter in the STRFNR statement. FIELD is only included in the generated DSN when Field Level Security is being checked for a command.

FILE The file number for the file being accessed. The value given the file number consists of either the literal 'F' followed by the file number, such as F100 for a file less than 256 or F00376 for a file number greater than 255. Otherwise, the value given to the file number consists of the file name as assigned in the STRFNR alias NAME parameter, such as PERSONL.

GPGM The non-NATURAL program name. This item will only be included for calls NOT originating from NATURAL.

JOB The MVS Jobname of the job being executed by the user.

NLIB The NATURAL Library. This item will only be included for calls originating from NATURAL.

DSNORDR (continued from previous page)

NODE — The SMFID of the CPU from which the call originates. If the value given as the SMFID begins with a numeric value, the literal 'N' will be followed by the SMFID. For example, if SMFID=1234 then NODE=N1234, and if SMFID=CPU1 then NODE=CPU1.

NPGM — The NATURAL program name. This item will only be included for calls originating from NATURAL.

TERM — The CICS Terminal-ID. This item will only be included for calls originating from CICS.

TRAN — The CICS Transaction-ID. This item will only be included for calls originating from CICS.

Valid Values:	CMD, DBID, FIELD, FILE, GPGM, JOB, NLIB, NODE, NPGM, TERM, or TRAN
Default Value:	FILE
Assigned By:	STRDEF and STRFNR

FIELDS — Specifies the names of the ADABAS fields for which Field Level Security processing should be performed, as well as an alias to be included in the DSN for each field. The format of the FIELDS parameter is FIELDS=(aa,alias1,bb,alias2,...,nn, aliasn), where aa, bb, ..., nn specify a 2-character ADABAS field name and alias1, alias2, ..., aliasn specify an alias of up to 8 characters to be used in the DSN.

Valid Values:	any number of pairs of 2-character ADABAS field name/8-character alias
Default Value:	no default value
Assigned By:	STRFNR only

FILE — The file or range of files to which these parameters apply. There is no default setting for this parameter, but an STRFNR statement without a FILE parameter will take effect for all files.

Note: File numbers greater than 255 can not be specified unless FILEMAX=NEW is specified in the STRDEF parameters.

Valid Values:	0 to 65535 or any range within these values
Default Value:	no default value
Assigned By:	STRFNR only

FLSDEL — The literal to be included in place of FIELD in the DSNORDR when Field Level Security is being checked and the ADABAS command code is E1 or E4 (delete).

Valid Values:	any string up to eight characters
Default Value:	DELETE
Assigned By:	STRDEF and STRFNR

FLSMODE The level of Field Level Security activated for this file.

<u>DORMANT</u> SECURITRE will not check Field Level Security for this file.

<u>WARN</u> SECURITRE will check Field Level Security on the fields listed in the FIELDS= parameter for the file as long as file security is allowed for that specific file. This will cause the SSF to log any violations, and will permit access to the file.

<u>FAIL</u> SECURITRE will check Field Level Security on the fields listed in the FIELDS= parameter for the file as long as file security is allowed for that specific file. This will cause the SSF to log any violations, and prohibit the command to be processed if any fields in the Format Buffer are unauthorized.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	DORMANT
Assigned By:	STRFNR only

LOGVIOL The logging action taken when multiple violations are made by a given user accessing the specified file(s).

<u>ALL</u> SECURITRE will cause the SSF to log all violations by a given user to a given DSN.

<u>FIRST</u> SECURITRE will cause the SSF to log only the first violation by a given user to a given DSN.

When a file is in WARN mode, the LOGVIOL is always set to "FIRST" by SECURITRE. **NOTE**: LOGVIOL=FIRST is *incompatible* with CALLSAF=ALL

Valid Values:	ALL or FIRST
Default Value:	ALL
Assigned By:	STRDEF and STRFNR

MODE The level of security, such as file protection mode, to be used for the specified file(s).

<u>DORMANT</u> SECURITRE will not make any security checks, and will allow all calls to be processed by ADABAS. In effect, SECURITRE does nothing. DORMANT mode is useful for verifying the correct installation of SECURITRE, and for phasing in SECURITRE control, one or more files at a time.

<u>WARN</u> SECURITRE will make security checks, cause the SSF to log any violations, and will allow all calls to be processed by ADABAS. WARN mode is provided so that installations can easily migrate to SECURITRE from their existing security arrangement.

MODE (continued from previous page)

FAIL — SECURITRE will make security checks, cause the SSF to log any violations, and prohibit any unauthorized commands from being processed by ADABAS.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	FAIL
Assigned By:	STRDEF and STRFNR

The following chart shows the response code that will be returned by SECURITRE for ADABAS file security with various combinations of SSF and SECURITRE modes:

SSF Mode	SECURITRE Mode	SECURITRE Response Code
DORMANT	WARN	0
DORMANT	FAIL	0
DORMANT	DORMANT	0
WARN	WARN	0 (with warning message from the SSF)
WARN	FAIL	0 (with warning message from the SSF)
WARN	DORMANT	0 (with warning message from the SSF)
FAIL	WARN	0 (with warning message from SECURITRE)
FAIL	FAIL	200
FAIL	DORMANT	0

As shown in the table above, the only way SECURITRE will stop a user operation is to have the SSF system and SECURITRE in FAIL mode. While SECURITRE is installed in a test environment, the site may wish to set SECURITRE in warn mode. However, the SSF should always be in FAIL mode to prevent unwanted access to resources.

Note: Some SSF products will lockout a User-ID after a specified number of failed attempts. Since SECURITRE does not have control over this, the User-ID will be locked out even if SECURITRE is set to WARN or DORMANT mode.

NAME — The file name to use when generating a DSN for the specified file(s). If a name is not provided, the literal 'F' followed by the file number will be used (e.g., F001, F072, F255, or F00300).

Valid Values:	any string up to 17 characters
Default Value:	'F' followed by the 3- or 5-digit file number
Assigned By:	STRFNR only

NOIDRED — The action SECURITRE will take when the User-ID for a READ command cannot be found for the specified file(s).

ACCEPT — SECURITRE will allow READ commands to be processed when no User-ID is found.

REJECT — SECURITRE will prevent READ commands from being processed when no User-ID is found.

Valid Values:	ACCEPT or REJECT
Default Value:	REJECT
Assigned By:	STRDEF and STRFNR

NOIDUPD

The action SECURITRE will take when the User-ID for an UPDATE command cannot be found for the specified file(s).

ACCEPT — SECURITRE will allow UPDATE commands to be processed when no User-ID is found.

REJECT — SECURITRE will prevent UPDATE commands from being processed when no User-ID is found.

Valid Values:	ACCEPT or REJECT
Default Value:	REJECT
Assigned By:	STRDEF and STRFNR

PREFIX

The first part of the DSN to use when calls are made to the SSF for File Security for the specified file(s).

Valid Values:	any string up to 17 characters
Default Value:	ADABAS.STR
Assigned By:	STRDEF and STRFNR

PROCEX2

Indicates whether SECURITRE User-Exit-2 should be invoked after an ADABAS command passes file level and field level security checks.

Valid Values:	ON or OFF
Default Value:	OFF
Assigned By:	STRDEF and STRFNR

QUALIFY

The second level of the DSN to be used by SECURITRE when requesting authorization from the SSF for the specified file(s).

Valid Values:	any string up to eight characters or null (")
Default Value:	PROD
Assigned By:	STRDEF and STRFNR

TRACE

Controls the production of diagnostic trace messages written by SECURITRE during execution. Trace messages will be written to the STRTRC dataset defined using the TRACEDD keyword of STRDEF. When tracing is specified on the file level, trace messages are written only for commands executed against the specified file.

Valid Values:	ON or OFF
Default Value:	OFF
Assigned By:	STRDEF and STRFNR

SECTION III

SECURITRE FOR NATURAL

III.1 SECURITRE for NATURAL - Parameters

Using parameters, a site may customize SECURITRE for NATURAL according to its needs. Tables and full descriptions of these parameters appear later in this section. The parameter statements (macros) that are provided include:

STNPARM provides the site-specific parameters needed to customize SECURITRE for NATURAL.
STNLIB specifies individual library parameters.
STNFILE specifies individual database/file parameters for FDIC, FNAT, and FUSER.
STNDDM specifies individual DDM parameters.
STNFINI indicates the end of parameter specifications.

A set of parameters must include one STNPARM statement as the first statement and one STNFINI statement as the last statement. There may be none, one, or multiples of the other statements, including STNLIB, STNFILE, and STNDDM.

For example:

```
STNPARM      PREFIX='NATURAL',QUALIFY='PROD',...
STNLIB       *DEFAULT,TYPE=PUB,PGMCHK=NO,...
STNLIB       SYSTEM,TYPE=PUB,PGMCHK=NO,...
STNLIB       SYSLIB,TYPE=PUB,PGMCHK=YES,...
STNLIB       PAYROLL,TYPE=PRIV,PGMCHK=YES,...
STNFILE      FDIC,DBID=100,FNR=102
STNFILE      FNAT,DBID=100,FNR=101
STNFILE      FUSER,DBID=100,FNR=100
STNFILE      EMPLOYEE,DBID=101,FNR=001
STNDDM       *DEFAULT,ALIAS=ANYDDM,TYPE=PUB
STNDDM       SALARIES,ALIAS=SALARY,TYPE=PRIV
STNFINI
```

STNLIB and STNDDM defaults (*DEFAULT) will be generated by SECURITRE if they are not provided.

The SECURITRE for NATURAL parameters must be coded in standard macro assembler format:

- Opcode in column 10
- One or more spaces
- Operands up to column 71, separated by commas
- Continuation symbol (x) in column 72
- Continuation lines beginning in column 16

These parameters must be coded, assembled, and link-edited. SECURITRE for NATURAL parameters are statically linked with the NATURAL nucleus. For Batch and TSO, the parameters may be either statically linked with the NATURAL nucleus or dynamically loaded when NATURAL is invoked. The dynamic parameter load option should be used only during SECURITRE for NATURAL testing. The benefit of dynamically loaded parameters is that the database does not need to be recycled to have the new parameters in effect. These parameters may be dynamically loaded through the Real-Time Monitor (RTM). It is recommended that the parameters be statically linked after testing has been completed so that users do not include a parameter dataset in front of the STEPLIB of the NATURAL dataset.

The SECURITRE tape is prepared with a default that forces the parameters to be statically linked. In order to change this default and enable dynamic parameter load, the following zap should be applied to a link-edited copy of module STNA. The vv in the module name must be adjusted to the NATURAL version in use.:

```
NAME STNvvA  STNA
VER  0135   00
REP  0135   FF
```

If STN4nA is zapped for dynamic parameter load, SECURITRE will load the parameter module named STNPNAT. If SECURITRE is unable to load a parameter module with the name STNPNAT, NATURAL ends execution with response code 102.

There are no unusual restrictions on a parameter module name if the parameters are statically linked with the NATURAL nucleus. Additional information can be found on the following table.

III.2 STNPARM Statement

The purpose of the STNPARM statement is to allow the Security Administrator to specify the options in effect for securing the NATURAL environment. The following table lists the STNPARM parameters, their uses, valid values, and their default values.

STNPARM Parameter	Function	Valid Values	Default Value
CLASS	The resource class to be used by SECURITRE for NATURAL when requesting authorization information from the SSF	any class defined to the SSF or null ('')	null ('')
DDMLIT	Literal used for DSNs generated for DDM Security	any value up to eight characters	DDM
DDMMODE	Setting for DDM Security protection mode	DORMANT, WARN, or FAIL	FAIL
DDMORDR	Order in which to generate the DSN for DDM Security	any combination of LIT, LIB, DDM, and/or FDIC	(LIT,LIB,DDM, FDIC)
DELIM	Delimiter character in the DSN	any character or null ('')	. (period)
LGNCHK	RESERVED	N/A	N/A
LGNLIT	Literal for DSNs generated for Logon Security	any value up to eight characters	LGN
LGNMODE	Setting for LOGON Security protection mode	DORMANT, WARN, or FAIL	FAIL
LGNORDR	Order in which to generate the DSN for LOGON Security	any combination of LIT, LIB, and/or FUSER	(LIT,LIB, FUSER)
LGNPRIV	Indicates whether logons to private libraries are allowed	UID, UID+ or NONE	UID+
LGNUNDF	RESERVED	N/A	N/A
NATUEX1	Other NATURAL User-Exit-1 to be invoked by SECURITRE	valid entry point in the NATURAL module	no default value
NSIFDIC	Literal used for DSNs generated for the FDIC file	any value up to eight characters	PROD
NSIFNAT	Literal used for DSNs generated for the FNAT file	any value up to eight characters	PROD
NSIFUSR	Literal used for DSNs generated for the FUSER file	any value up to eight characters	PROD
NSIMODE	Setting for NATURAL Session Initialization Security protection mode	DORMANT, WARN, or FAIL	FAIL

Figure 3 – STNPARM Parameters

(continued on next page)

(continued from previous page)

STNPARM Parameter	Function	Valid Values	Default Value
NSIORDR	Order in which to generate the DSN for NATURAL Session Initialization Security	any combination of LIT and/or FILE	(FILE,LIT)
NULIT	Literal used for DSNs generated by NATURAL Utility security	any value up to eight characters	UTIL
NUMODE	Setting for NATURAL Utility security protection mode	DORMANT, WARN, or FAIL	DORMANT
NUORDR	Order in which to generate the DSN for NATURAL Utility security	any combination of LIT, LIB, UTIL, and/or FUSER	(LIT, LIB, UTIL, FUSER)
PGLITOR	Literal for Program Security (object read)	any value up to eight characters	EXEC
PGLITOW	Literal for Program Security (object write)	any value up to eight characters	STOW
PGLITSR	Literal for Program Security (source read)	any value up to eight characters	READ
PGLITPD	Literal for Program Security (scratch/purge)	any value up to eight characters	DELETE
PGLITSW	Literal for Program Security (source write)	any value up to eight characters	STOW
PGMORDR	Order in which to generate the DSN for Program Security	any combination of LIT, LIB, PGM, and/or FUSER	(LIT,LIB,PGM, FUSER)
PGMTBSZ	Number of program names to store in internal tables	any number between 5 and 999	20
PGWLIT	Literal for Program Write Security	any value up to eight characters	PGMWRT
PGWORDR	Order in which to generate the DSN for program write security	any combination of LIT, LIB, and/or FUSER	LIT, LIB, FUSER
PREFIX	DSN prefix (first part of DSN)	any value up to 17 characters	NAT
PRIVBUF	Reserved	USERDEF	USERDEF
QUALIFY	DSN qualifier (second part of DSN)	any value up to eight characters or null ('')	PROD
RACHECK	Module that issues security calls to the SSF	STN4RCHK STNRCHEK STRACHEK	STRACHEK
RUNLIT	Literal used for DSNs generated for RUN Security	any value up to eight characters	RUN

Figure 3 – STNPARM Parameters

(continued on next page)

(continued from previous page)

STNPARM Parameter	Function	Valid Values	Default Value
RUNORDR	Order in which to generate DSNs for RUN Security	any combination of LIT, LIB, and/or FUSER	(LIT, LIB, FUSER)
SERVER	DBID to which commands will be directed	0 to 65535	255
STEPLIB	Specifies a library besides SYSTEM where NATURAL can obtain programs	any value up to eight characters	SYSTEM
USERBUF	Reserved	N/A	N/A

Figure 3 – STNPARM Parameters

III.3 STNPARM Parameters

CLASS The resource class to be used by SECURITRE for NATURAL when requesting authorization information from the SSF. A null value will cause SECURITRE for NATURAL to use the CLASS assigned in the STRDEF CLASS parameter.

Valid Values: any class defined to the SSF or null ("). (Null indicates that there is no override to the STRDEF CLASS.)
Default Value: null (")
Assigned By: STNPARM and STRDEF

DDMLIT The literal to include in the DSN when SECURITRE sends an authorization request to the SSF for access to a DDM.

Valid Values: any string up to eight characters
Default Value: DDM
Assigned By: STNPARM only

DDMMODE The level of security to be activated when a user attempts to access a DDM.

DORMANT SECURITRE will not make any security checks and will permit the user access to the DDM.

WARN SECURITRE will make security checks, cause the SSF to log any violations, and permit the user access to the DDM.

FAIL SECURITRE will make security checks, cause the SSF to log any violations, and prevent any unauthorized access to the DDM.

Valid Values: DORMANT, WARN, or FAIL
Default Value: FAIL
Assigned By: STNPARM only

DDMORDR The order in which the DSN will be generated, after the PREFIX and QUALIFY parameters, when a call is made to the SSF for DDM Security. Any or all of the components below may be included in any order.

LIT The DDM literal defined in the DDMLIT parameter.

LIB The current library the user is logged on to when attempting to access the DDM.

DDM The DDM name or alias specified in a STNDDM statement.

FDIC The current FDIC file alias for the DDM the user is attempting to access as specified in an STNFILE statement.

Valid Values:	any combination of LIT, LIB, DDM, and/or FDIC
Default Value:	(LIT,LIB,DDM,FDIC)
Assigned By:	STNPARM only

DELIM The delimiter character to be placed between the PREFIX, QUALIFY, and DDMORDR parameter items when generating a DSN for authorization requests to the SSF.

Valid Values:	any character or null (")
Default Value:	. (period)
Assigned By:	STNPARM only

LGNCHK Reserved for future use.

LGNLIT The literal to include in the DSN when SECURITRE sends an authorization request to the SSF for LOGON Security.

Valid Values:	any string up to eight characters
Default Value:	LGN
Assigned By:	STNPARM only

LGNMODE The level of security to be activated when the user attempts to LOGON to a library. The LGNMODE parameter may be overridden at the library level through the use of the STNLIB TYPE parameter.

DORMANT SECURITRE will not make any security checks and will permit the user to logon.

WARN SECURITRE will make security checks, cause the SSF to log any violations, and permit the user to logon.

FAIL SECURITRE will make security checks, cause the SSF to log any violations, and prevent any unauthorized logons.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	FAIL
Assigned By:	STNPARM only

LGNORDR The order in which the DSN will be generated, after the PREFIX and QUALIFY parameters, when a call is made to the SSF for LOGON Security. Any or all of the components below may be included in any order.

LIT The literal defined by the LGNLIT parameter.

LIB The library the user is attempting to logon.

FUSER The current FUSER of the user attempting to logon.

Valid Values: any combination of LIT, LIB, and/or FUSER
Default Value: (LIT,LIB,FUSER)
Assigned By: STNPARM only

LGNPRIV Specifies whether LOGON Security should be bypassed when a user attempts to logon to a library that matches their User-ID exactly (UID) or one that begins with their User-ID (UID+).

UID SECURITRE should bypass security checking if the library name matches the User-ID.

UID+ SECURITRE should bypass security checking if the library name begins with the User-ID.

NONE LOGON Security will always be carried out according to the LGNMODE parameter.

Valid Values: UID, UID+, or NONE
Default Value: UID+
Assigned By: STNPARM only

LGNUNDF Reserved for future use.

NATUEX1 The name of a second NATURAL User-Exit-1 to be invoked by SECURITRE after it completes its own NATURAL User-Exit-1 processing. The name provided must be the name of an entry point in the NATURAL module.

Valid Values: a valid entry point in the NATURAL module
Default Value: no default value
Assigned By: STNPARM only

NSIFDIC The literal to include in the DSN when SECURITRE generates a request to the SSF for access to NATURAL using the FDIC file specified in the NATPARM module during NATURAL Session Initialization.

Valid Values: any string up to eight characters
Default Value: PROD
Assigned By: STNPARM only

NSIFNAT The literal to include in the DSN when SECURITRE generates a request to the SSF for access to NATURAL using the FNAT file specified in the NATPARM module during NATURAL Session Initialization.

Valid Values: any string up to eight characters

Default Value:	PROD
Assigned By:	STNPARM only

NSIFUSR The literal to include in the DSN when SECURITRE generates a request to the SSF for access to NATURAL using the FUSER file specified in the NATPARM module during NATURAL Session Initialization.

Valid Values:	any string up to eight characters
Default Value:	PROD
Assigned By:	STNPARM only

NSIMODE The level of security to be activated during NATURAL Session Initialization time.

DORMANT SECURITRE will not make any security checks and will permit the user to enter the NATURAL environment.

WARN SECURITRE will make security checks, cause the SSF to log any violations, and will permit the user to enter the NATURAL environment.

FAIL SECURITRE will make security checks, cause the SSF to log any violations, and prevent any unauthorized access to the NATURAL environment.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	FAIL
Assigned By:	STNPARM only

NSIORDR The order in which the DSN will be generated, after the PREFIX and QUALIFY parameters, when a call is made to the SSF for NSI Security. Either one or both of the components below may be included, in any order.

FILE The STNFILE alias for the FDIC, FNAT, or FUSER file specified in the NATPARM module. If no alias is available, SECURITRE will generate an alias in the form of DxxxFyyy, where 'xxx' indicates the Database-ID and 'yyy' indicates the file number.

LIT The NSI literal, appropriate to the access being checked as specified in the NSIFDIC, NSIFNAT, and NSIFUSR parameters.

Valid Values:	any combination of FILE and/or LIT
Default Value:	(FILE,LIT)
Assigned By:	STNPARM only

NULIT The literal to include in the DSN generated by SECURITRE when a user attempts to execute a NATURAL Utility.

Valid Values:	any string up to eight characters
Default Value:	UTIL
Assigned By:	STRPARM only

NUMODE The level of security to be activated when the user attempts to execute a NATURAL Utility.

DORMANT SECURITRE will not make any security checks, but it will permit the user to execute all NATURAL Utilities.

WARN SECURITRE will make security checks, cause the SSF to log any violations, and permit the user to execute NATURAL Utilities.

FAIL SECURITRE will make security checks and cause the SSF to log any violations, but it will not permit the user to execute NATURAL Utilities.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	DORMANT
Assigned By:	STRPARM only

NUORDR The order in which the DSN will be generated after the PREFIX and QUALIFY parameters when a call is made to the SSF for NATURAL Utility security. Any or all of the components below may be included, in any order.

LIT The literal defined by the NULIT parameter.

LIB The current library the user is logged on to when attempting to execute the NATURAL Utility.

UTIL The name of the NATURAL Utility the user is attempting to execute.

FUSER The current FUSER of the user attempting to execute the NATURAL Utility.

Valid Values:	any combination of LIT, LIB, UTIL, and/or FUSER
Default Value:	(LIT,LIB,UTIL,FUSER)
Assigned By:	STNPARM only

PGLITOR The literal to include in the DSN generated by SECURITRE when a user attempts to read a program in object form.

Valid Values:	any string up to eight characters
Default Value:	EXEC
Assigned By:	STNPARM only

PGLITOW The literal to include in the DSN generated by SECURITRE when a user attempts to store (CAT) a program in object form.

Valid Values:	any string up to eight characters
Default Value:	STOW
Assigned By:	STNPARM only

PGLITSR The literal to include in the DSN generated by SECURITRE when a user attempts to read a program in source form.

Valid Values:	any string up to eight characters
Default Value:	READ

Assigned By: STNPARM only

PGLITPD The literal to include in the DSN generated by SECURITRE when a user attempts to delete (SCRATCH or PURGE) program source or object.

Valid Values: any string up to eight characters
Default Value: DELETE
Assigned By: STNPARM only

PGLITSW The literal to include in the DSN generated by SECURITRE when a user attempts to store (SAVE) a program in source form.

Valid Values: any character string up to eight characters
Default Value: STOW
Assigned By: STNPARM only

PGMORDR The order in which the DSN will be generated, after the PREFIX and QUALIFY parameters, when a call is made to the SSF for Program Security. Any or all of the components below may be included, in any order.

LIT The program literal, appropriate to the access being checked, as specified in the PGLITOR, PGLITSR, PGLITOW, and PGLITSW parameters.

LIB The library to which the program is being read or written.

PGM The name of the program that is being read or written.

FUSER The current FUSER for the user accessing the program.

Valid Values: any combination of LIT, LIB, PGM, and/or FUSER
Default Value: (LIT,LIB,PGM,FUSER)
Assigned By: STNPARM only

PGMTBSZ The number of program names to be stored internally for each user. A program is added to the internal table after an SSF authorization request has been accepted for an object read (execute). If a program is in the table for the user, SECURITRE will not generate another SSF request for it. The table information for the user is cleared out when the user logs on to another library.

Valid Values: any number between 5 and 999
Default Value: 20
Assigned By: STNPARM only

PGWLIT The literal to include in the DSN when SECURITRE sends an authorization request to the SSF for writing programs in the current library.

Valid Values: any string up to eight characters
Default Value: PGMWRT
Assigned By: STNPARM only

PGWORDR The order in which the DSN will be generated, after the PREFIX and QUALIFY parameters, when a call is made to the SSF for program write security. Any or all of the components below may be included, in any order.

<u>LIT</u> The program write literal defined in the PGWLIT parameter.

<u>LIB</u> The library the user is logging onto.

<u>FUSER</u> The current FUSER for the user.

Valid Values: any combination of LIT, LIB, and/or FUSER
Default Value: (LIT, LIB, FUSER)
Assigned By: STNPARM only

PREFIX The first part of the DSN to use for all SECURITRE for NATURAL SSF calls.

Valid Values: any string up to 17 characters
Default Value: NAT
Assigned By: STNPARM only

PRIVBUF Reserved for future use.

Valid Values: USERDEF
Default Value: USERDEF
Assigned By: STNPARM only

QUALIFY The second level of the DSN generated by SECURITRE for NATURAL when requesting information from the SSF.

Valid Values: any string up to eight characters or null ('')
Default Value: PROD
Assigned By: STNPARM only

RACHECK The module that issues the security check to the SSF.

Valid Values: STN4RCHK (NAT4.1, 4.2) or STRACHEK
Default Value: STRACHEK (version independent)
Assigned By: STNPARM only

RUNLIT The literal to include in the DSN when SECURITRE sends a request to the SSF for RUN Security.

Valid Values: any string up to eight characters
Default Value: RUN
Assigned By: STNPARM only

RUNORDR The order in which the DSN will be generated, after the PREFIX and QUALIFY parameters, when a call is made to the SSF for RUN Security. Any or all of the components below may be included, in any order.

<u>LIT</u>	The literal specified by the RUNLIT parameter.
<u>LIB</u>	The current library for the user issuing the RUN.
<u>FUSER</u>	The current FUSER for the user issuing the RUN.

The name of the program in the work area is irrelevant, since users may assign it the name of a program to which they have access.

Valid Values:	any combination of LIT, LIB, and/or FUSER
Default Value:	(LIT,LIB,FUSER)
Assigned By:	STNPARM only

SERVER A database that is running the SECURITRE for ADABAS User-Exit-1 from an APF-authorized dataset. SECURITRE for NATURAL sends authorization requests to this database, which in turn requests authorization from the SSF. Therefore, the NATURAL module does not have to reside in an APF-authorized dataset. If the value 0 (zero) is used, authorization requests will be directed to the database specified in the ADARUN parameters.

Valid Values:	0 to 65535
Default Value:	255
Assigned By:	STNPARM only

STEPLIB The name of a library where NATURAL can attempt to locate executable programs when they are not found in the current library when no overriding STNLIB STEPLIB parameter has been specified for the specified library.

Valid Values:	any string up to eight characters
Default Value:	SYSTEM
Assigned By:	STNPARM and STNLIB

USERBUF Reserved for future use.

III.4 STNLIB Statement

The SECURITRE library parameters are used to specify unique qualities about each library. The syntax for the library parameters is:

STNLIB library-name,[keyword-parameter=value,]...

Default sets of parameters may be specified by using *DEFAULT as the library name. *DEFAULT may be used in combination with LIBFUSR to specify defaults for specific FUSERs.

SECURITRE scans for matching library parameters starting from the top of the STNLIB list. Therefore, the following rules should be followed when writing STNLIB parameters:

- *DEFAULT libraries should appear at the top of the list.
- Matching library names should appear together for ease of maintenance.
- Blank LIBFUSR parameters must appear at the end of a group of STNLIBs for a library name. If no *DEFAULT/blank LIBFUSR combination is found, SECURITRE will generate one after other *DEFAULTs and before other library parameters.
- To reduce search time, the most commonly used libraries should appear closest to the top of the list.

STNLIB parameters should be coded in the following order:

```
1)   STNLIB *DEFAULT,LIBFUSR=non-blank-FUSERs

2)   STNLIB *DEFAULT           <-generates a blank FUSER

3)   STNLIB lib1,LIBFUSR=FUSER1,...
     STNLIB lib1,LIBFUSR=FUSER2,...
        •
        •
        •
     STNLIB lib1,LIBFUSR=FUSERn,...
     STNLIB lib1,...           <-default for lib1

4)   STNLIB lib2,LIBFUSR=FUSER1,...
     STNLIB lib2,LIBFUSR=FUSER2,...
        •
        •
        •
     STNLIB lib2,LIBFUSR=FUSERn,...
     STNLIB lib2,...           <-default for lib2
```

Separate STNLIB statements for the same library name on different FUSER files may be specified by using the LIBFUSR parameter. Since only one set of SECURITRE for NATURAL parameters may be linked with a NATURAL module, the LIBFUSR parameter allows a site to use the same NATURAL module for multiple FUSERs. However, since more processing is required to identify the correct set of parameters at LOGON time, response time may be slightly affected.

Using the LIBFUSER parameter benefits those who use the same NATURAL module for multiple FUSERs, since it specifies different library parameters for different FUSERs. The value assigned to the LIBFUSR parameter should be a file-alias from the STNFILE parameters. A blank LIBFUSR indicates that this STNLIB statement is the default for the library when a given library/FUSER combination is not found. If LIBFUSR does not appear in an STNLIB statement, it is set to blank.

SECURITRE will select STNLIB parameters based on the following priorities:

1) Match on Library Name and LIBFUSR=FUSER
2) Match on Library Name and blank FUSER
3) STNLIB library = *DEFAULT and LIBFUSR=FUSER
4) STNLIB library = *DEFAULT and LIBFUSR=blank

Note: After SECURITRE has selected the STNLIB parameters for a library, the defaults for the parameters that were not coded in the STNLIB are taken from the selected parameter definitions, not from the *DEFAULT for the library/FUSER.

Information about each of the valid keyword-parameters can be found in Figure 4.

STNLIB Parameter	**Function**	**Valid Values**	**Default Value**
ERRORTA	Specifies *ERROR-TA for this library	a valid NATURAL program	no default value
LGNPRMS	Area passed to STRLOGON after successful LOGON request	any value up to 16 characters	null (")
LIBFUSR	Specifies the FUSER with which these parameters will be used	null (") or file alias from STNFILE	null (")
LT	Override for LT NATPARM while the user is logged on to this library	0 through 2147483647	0
MADIO	Override for MADIO NATPARM while the user is logged on to this library	0, 30 through 32767	0
MAXCL	Override for MAXCL NATPARM while the user is logged on to this library	0, 10 through 32767	0
MT	Override for MT NATPARM while the user is logged on to this library	0 through 86399	0
MODE	Specifies the NATURAL mode for the user (Structured or Reporting) while logged on to this library	STRUCT or REPORT	REPORT
PGMCHK	Specifies the mode for Program Security in this library	DORMANT, WARN, or FAIL	FAIL
PGWRTCK	Specifies the mode for Program Write Security in this library	DORMANT, WARN, or FAIL	DORMANT
PGMTYPE	Types of NATURAL objects affected by program Execution Security	ALL or any combination of PROG, HELP, SUBP, SUBR, and/or MAP	ALL

Figure 4 – STNLIB Parameters

(continued on next page)

(continued from previous page)

STNLIB Parameter	Function	Valid Values	Default Value
PGMWRT	Specifies whether NATURAL objects may be written or deleted while a user is logged on to this library	YES or NO	YES
RDONLY	Specifies whether database updating is disabled while a user is logged onto this library	YES or NO	NO
RUNCHK	Level of RUN Security in this library	DORMANT, WARN, or FAIL	DORMANT
STARTUP	Specifies a default *STARTUP for this library	A NATURAL program name	no default value
STEPLIB	Specifies a library besides SYSTEM where NATURAL can obtain programs while a user is logged on to this library	any string up to eight characters or null (")	null (")
TYPE	Specifies whether SECURITRE will check LOGON Security for this library	PRIV or PUB	PRIV
USRMODE	Specifies whether NATURAL system commands may be executed from this library	YES or NO	YES
XREF	Specifies whether the PREDICT active cross-reference feature is to be used	ON or OFF	OFF

Figure 4 – STNLIB Parameters

III.5 STNLIB Parameters

ERRORTA The *ERROR-TA for this library that is assigned when a user logs on to this library.

Valid Values:	a valid NATURAL program
Default Value:	no default value
Assigned By:	STNLIB only

LGNPRMS A 16-character free-form area that is passed to STRLOGON from STRLGN when a request for LOGON is successful. This area may be used to customize the environment of a library at logon time.

Valid Values:	any string up to 16 characters or null (")
Default Value:	null (")
Assigned By:	STNLIB only

LIBFUSR The library FUSER is used when multiple NATURAL environments are invoked from the same NATURAL module. For example, the FUSER is used if the same NATURAL module is used for both the TEST and PROD environments. Separate STNLIB statements for the same library name in different environments are distinguishable by use of the LIBFUSR parameter.

The value assigned to the LIBFUSR parameter should be a file-alias defined in an STNFILE statement.

Valid Values:	a file-alias defined in an STNFILE statement or null (")
Default Value:	null (")
Assigned By:	STNLIB only

LT A library-level override for the LT NATPARM (the maximum limit on records that may be read in a processing loop). A value of 0 (zero) indicates that no override is to take place, and the default from the installation NATPARM settings or the dynamic NATPARM settings will be used.

Valid Values:	0 through 2147483647
Default Value:	0
Assigned By:	STNLIB only

MADIO A library-level override for the MADIO NATPARM (the limit on ADABAS calls to be made between screen I/Os). A value of 0 (zero) indicates that no override is to take place, and the default from the installation NATPARM settings or the dynamic NATPARM settings will be used.

Valid Values:	0, 30 through 32767
Default Value:	0
Assigned By:	STNLIB only

MAXCL A library-level override for the MAXCL NATPARM (the limit on program calls to be made between screen I/Os). A value of 0 (zero) indicates that no override is to take place, and the default from the installation NATPARM settings or the dynamic NATPARM settings will be used.

Valid Values:	0, 10 through 32767
Default Value:	0
Assigned By:	STNLIB only

MODE A library-level override for the SM NATPARM (structured mode/report mode).

STRUCT	The user is put in structured mode.
REPORT	The user is put in report mode.

Valid Values:	STRUCT or REPORT
Default Value:	REPORT
Assigned By:	STNLIB only

MT A library-level override for the MT NATPARM (the maximum CPU time limit). A value of 0 (zero) indicates that no override is to take place, and the default from the installation NATPARM settings or the dynamic NATPARM settings will be used.

Valid Values:	0 to 86399
Default Value:	0
Assigned By:	STNLIB only

PGMCHK The level of security to be activated when a user attempts to read, save, catalog, or execute a program in this library.

DORMANT	SECURITRE will not make any security checks and will permit the user to complete the action that triggered the security request.
WARN	SECURITRE will make security checks, cause the SSF to log any violations, and permit the user to complete the action that triggered the security request.
FAIL	SECURITRE will make security checks, cause the SSF to log any violations, and will prevent any unauthorized access to the program in this library.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	FAIL
Assigned By:	STNLIB only

PGMTYPE The types of NATURAL objects to be checked for Program Execution Security.

ALL	Check all NATURAL objects. ALL may not be used in combination with any other type.
PROG	Check all NATURAL programs.
HELP	Check all NATURAL help routines.
SUBP	Check all NATURAL subprograms.
SUBR	Check all NATURAL subroutines.
MAP	Check all NATURAL maps.

Valid Values:	ALL or any combination of PROG, HELP, SUBP, SUBR, and/or MAP
Default Value:	ALL
Assigned By:	STNLIB only

PGMWRT Sets the NATURAL parameter SAVECD when a logon is accepted, which specifies whether or not NATURAL objects may be written or deleted. This parameter is ignored if PGWRTCK is FAIL for this library.

YES Sets SAVECD=ON. The user may write and delete NATURAL objects while logged on to this library.

NO Sets SAVECD=OFF. The NATURAL objects may not be written or deleted while a user is logged on to this library.

Note that unless USRMODE is set to NO, PGMWRT may be overridden if the user enters the UPDATE or SAVECD commands.

Valid Values:	YES or NO
Default Value:	YES
Assigned By:	STNLIB only

PGWRTCK The level of security for checking at logon time whether the user may SAVE, CAT, STOW, or PURGE programs in this library.

DORMANT SECURITRE will not check to see whether the user is allowed to SAVE, CAT, STOW, or PURGE programs while logged on to this library. However, the PGMWRT parameter will be used to determine this capability.

WARN SECURITRE will make a security check to see whether the user is allowed to SAVE, CAT, STOW, or PURGE programs while logged on to this library. However, the PGMWRT parameter will be used to determine this capability.

FAIL SECURITRE will make a security check to see whether the user is allowed to SAVE, CAT, STOW, or PURGE programs while logged on to this library. Depending on the answer from the SSF, SECURITRE may or may not allow the user to perform these activities. The result of this program write checking overrides the use of the PGMWRT parameter.

Valid Values:	DORMANT, WARN, or FAIL
Default Value:	DORMANT
Assigned by:	STNLIB only

RDONLY Specifies whether or not a user may update an ADABAS file while logged on to this library.

YES Updates may not take place (equivalent to issuing the NATURAL UPDATE OFF command). A user will **not** be able to update ADABAS data from this library.

NO Updates may take place (equivalent to issuing the NATURAL UPDATE ON command). A user will be able to update ADABAS data from this library.

Note that unless USRMODE is set to NO, RDONLY may be overridden if the user enters the NATURAL UPDATE or SAVECD commands.

Valid Values:	YES or NO

Default Value: NO
Assigned By: STNLIB only

RUNCHK The level of security to be activated for RUN Security in this library.

DORMANT SECURITRE will not make any security checks, but it will permit the user to execute the RUN.

WARN SECURITRE will make security checks, cause the SSF to log any violations, and permit the user to execute the RUN.

FAIL SECURITRE will make security checks, cause the SSF to log any violations, and prevent any unauthorized executions of the RUN.

Valid Values: DORMANT, WARN, or FAIL
Default Value: DORMANT
Assigned By: STNLIB only

STARTUP The default *STARTUP for this library. The STRLOGON front-end to the LOGON process must be used in order for this parameter to be processed.

Valid Values: a NATURAL program name
Default Value: no default value
Assigned By: STNLIB only

STEPLIB The name of a library where NATURAL can attempt to locate executable programs when they are not found in the current library while the user is logged on to this library. When a null value is specified, the default value specified in the STNPARM STEPLIB parameter will be used.

Valid Values: any string up to eight characters or null ('')
Default Value: null ('')
Assigned By: STNPARM and STNLIB

	Function	**Valid Values**	**Default Values**
Step1	Specifies the first alternate library where NATURAL can obtain programs while the user is logged on to this library	any value up to 8 characters or null ('')	no default value
Steps 2-8	Specify the second through the eighth alternate libraries where NATURAL can obtain programs while the user is logged on to these libraries	any value up to 8 characters or null ('')	no default values

Note: All STEPLIB and STEP1/8 definitions have no effect, if LGNMODE=DORMANT is defined in the STNPARM definitions!

TYPE Specifies whether or not SECURITRE should check security when a user logs on to this library.

PRIV SECURITRE will send an authorization request to the SSF when anyone attempts to logon to this library.

PUB No security checking will take place. Anyone may logon to this library.

The TYPE parameter can be used to override the LGNMODE parameter for particular libraries. If LGNMODE is set to FAIL or WARN, individual libraries that have TYPE=PUB will not cause a security check for LOGON Security. However, if LGNMODE is set to DORMANT, setting a library as TYPE=PRIV will not cause SECURITRE to check LOGONs to that library.

Valid Values:	PRIV or PUB
Default Value:	PRIV
Assigned By:	STNLIB only

USRMODE Specifies whether NATURAL system commands may be executed from this library.

YES Commands may be issued from this library (equivalent to the NATURAL command NC=OFF).

NO Commands may not be issued from this library (equivalent to the NATURAL command NC=ON).

Valid Values:	YES or NO
Default Value:	YES
Assigned By:	STNLIB only

XREF Specifies whether the PREDICT XREF feature is to be used while the user is logged on to this library.

OFF No PREDICT Cross-Reference activity is performed.

ON PREDICT Cross Reference is active.

Valid Values:	OFF or ON
Default Value:	OFF
Assigned By:	STNLIB only

III.6 STNFILE Statement

The SECURITRE file parameters are used to specify an alias to be used when referring to a file. The syntax for the file parameter is:

```
STNFILE  file-alias,DBID=nnnnn,FNR=nnnnn
```

STNFILE Parameter	Function	Valid Values	xDefault Value
ALIAS	The name to be used in the DSN that refer to specific files. For example: the NSI DSNs.	any value up to 8 characters	none
DBID	Specifies the DBID for this file	a valid DBID	no default value
FNR	Specifies the file number for this file	a valid file number for the above DBID	no default value

Figure 5 – STNFILE Parameters

III.7 STNFILE Parameters

ALIAS Function.

Valid Values: any string up to 8 characters
Default Value: none
Assigned By: STNFILE only

DBID The database for this Database-ID/file number combination. Use of this parameter is meaningless without an associated FNR parameter.

Valid Values: a valid Database-ID
Default Value: no default value
Assigned By: STNFILE only

FNR The file number for this Database-ID/file number combination. Use of this parameter is meaningless without an associated DBID parameter.

Valid Values: a valid file number
Default Value: no default value
Assigned By: STNFILE only

III.8 STNDDM Statement

The SECURITRE DDM parameters are used to specify unique qualities about each DDM. The syntax for the DDM parameters is

STNDDM DDM-name,[keyword-parameter=value,]...

A default set of DDM parameters may be specified by using *DEFAULT as the DDM name. If *DEFAULT is used, it must appear as the first STNDDM. If no *DEFAULT is provided, SECURITRE will generate one. These default settings will be used for all DDM checks, where the name is not defined via STNDDM.

DDM-name may contain '*' and/or '%' as wildcard(s) to reduce the number of definitions. The '%' stands for any ONE character whereas the '*' represents 1-n characters.

If TYPE=PRIV is set and DDM-name contains wildchar(s), ALIAS= becomes mandatory if DDM-name has wildcard(s). This is also true for the *DEFAULT definition.

The name to be included in the DSN will always be taken from a STNDDM statement. If a STNDDM statement has not been specified for a particular DDM, SECURITRE will take the name from the STNDDM *DEFAULT statement.

Information about each of the valid keyword parameters follows.

STNDDM Parameter	Function	Valid values	Default value
ALIAS	Specifies an alternate name to be used for SSF requests for this DDM	any value up to 17 characters	no default value
TYPE	Specifies whether SECURITRE should check acsess to this DDM (TYPE=PRIV)	PRIV or PUB	PRIV

Figure 6 – STNDDM Parameters

III.9 STNDDM Parameters

ALIAS The name SECURITRE should use when authorization requests are made to the SSF for this DDM. The purpose of an alias name is to shorten the DDM name, so that SSF limitations on dataset name lengths are not exceeded. If no ALIAS= is defined (Default) the DSN for SAF checking will be constructed with the DDM.name.

Valid Values: any string up to 17 characters
Default Value: no default value
Assigned By: STNDDM only

TYPE Indicates to SECURITRE whether or not security should be checked when a user attempts to access this DDM.

PRIV	SECURITRE will send an authorization request to the SSF when anyone attempts to access this DDM.
PUB	No security checking will take place. Anyone may access this DDM.

The TYPE parameter can be used to override the DDMMODE parameter for particular DDMs. For example, DDMMODE can be set to FAIL or WARN, but security will not be checked for a DDM if the TYPE for that DDM is set to PUB. However, if DDMMODE is set to DORMANT, setting a particular DDM TYPE to PRIV will not cause SECURITRE to check access to that DDM.

Valid Values:	PRIV or PUB
Default Value:	PRIV
Assigned By:	STNDDM only

III.10 SECURITRE for NATURAL - Failed Authorization

This section describes the symptoms of a failed authorization request from the SSF for each of the different types of security provided by SECURITRE for NATURAL. In most cases, SECURITRE will replace the NATURAL error message text with the text "SECURITY VIOLATION DETECTED OR INVALID CIPHER CODE." The exceptions to this are:

- LOGON Security: the site specifies how a violation will be handled in STRLOGON.
- DDM Security: when activated within the "LIST FILE" or "LIST FILES" command the normal SYSLIS message will be returned.

NSI Security

In TSO/BATCH, the user will be returned to the environment in use prior to attempt to enter NATURAL. In batch, the step receives a return code 100.

In CICS, the user will receive a NATURAL response code 9987 with the message "SECURITY VIOLATION DETECTED OR INVALID CIPHER CODE".

LOGON Security

If STRLOGON is used as the LOGON program, and the LOGON request is failed, the failure will be handled by the STRLOGON program which is modifiable at the user site, and which will have been renamed to LOGON and put in the SYSTEM library. The STRLOGON provided with SECURITRE displays a screen that allows the user to enter a different library to logon to.

If STRLOGON is not used, and a LOGON request is failed, the user will be returned to the library where the LOGON request was issued with a message saying the logon was successful.

PROGRAM Security

PROGRAM EXECUTE

If a user fails in a request to execute a program, a NAT3200 error code with the message "SECURITY VIOLATION DETECTED OR INVALID CIPHER CODE" will be generated.

PROGRAM SOURCE READ

If a user fails in a request to read program source, a NAT0963 error code with the message "SECURITY VIOLATION DURING PROGRAM EXECUTION" will be generated.

PROGRAM SOURCE WRITE

If a user fails in a request to write program source, a NAT3200 (ADABAS 200: SECURITY VIOLATION) will be generated.

PROGRAM OBJECT WRITE

If a user fails in a request to write program object, a NAT3200 (ADABAS 200: SECURITY VIOLATION) will be generated.

RUN Security

If a user fails in a request to RUN a NATURAL program, a NAT0963 error code with the message "SECURITY VIOLATION DURING PROGRAM EXECUTION" will be generated.

DDM Security

If a user fails in a request to read a DDM from a "LIST FILE" request, a SYSLIS4125 message ("REQUESTED FILE DESCRIPTION NOT AVAILABLE") will be generated.

If a user fails in a request to access a DDM, a NAT0002 error code with the message "SECURITY VIOLATION DETECTED OR INVALID CIPHER CODE" will be generated.

PGWRTCK Security

If a user is not authorized to SAVE/CAT/STOW/PURGE programs while logged on to a library and attempts to perform one of these functions, a NAT0106 error code with the message "SAVE/CA TALOG/STOW/PURGE/UNCATALOG/ SCRATCH not available" will be generated.

Changing the Error Message

The error message "SECURITY VIOLATION DETECTED OR INVALID CIPHER CODE" is obtained from the NATURAL system file. This message may be modified using the NATURAL SYSERR Utility to change message number 3200. For example, if the site has no ciphered files, a more appropriate message is "SECURITRE VIOLATION."

III.11 NATURAL Utility Security

The following NATURAL Utilities will be checked for authorization if the STNPARM parameter NUMODE is WARN or FAIL:

Utility	NATURAL version
SYSDBA	all
SYSDDM	all
SYSERR	all
SYSMAIN	all
*BUS	2.2 or above
*ROUTINES	2.2 or above
SYSBPM	2.2 or above
*SYSFILE	2.2 or above
SYSNCP	2.2 or above
*SYSPROD	2.2 or above
*SYSPROF	2.2 or above
SYSTP	2.2 or above
TEST	2.2 or above
NATLOAD	2.2 or above
NATUNLD	2.2 or above

* Utilities are sub-functions of SYSDBA. They are included on this list since they may also be run outside of SYSDBA.

SECTION IV

SECURITRE FOR ADABAS UTILITIES

IV.1 Introduction to Utility Security

SECURITRE ADABAS Utility Control secures ADABAS Utilities at the database, file, utility, and function levels. Before a user is allowed to execute a utility, SECURITRE generates a DSN containing a utility prefix and any or all of the following: the file alias, the utility name, and the utility function. SECURITRE then sends a request to the SSF to check if the user may access the DSN.

SECURITRE Utility Security will check all ADABAS utility functions for up to 65535 files per utility run. It will also check for ADADBS OPERCOM sub-functions. This section lists these functions and sub-functions and how they will appear in the DSN generated by SECURITRE.

Utility Security Parameters

The Utility Security parameters include UTMODE, UTORDER, and UTPREF. All of these are defined in the STRDEF statement.

IV.2 ADABAS Utility Control

The following list of ADABAS Utilities indicates the items that may appear as part of a SECURITRE DSN for each utility. The presence of any component listed below is dependent on whether that component was specified in the UTORDER parameter in the STRPARMS, and whether or not that value is appropriate for the requested utility.

ADABAS UTILITY		FUNCTION	FUNCTION IN DSN	FILE
ADAACK	ACCHECK	ACCHECK	OPT	
ADACMP	COMPRESS	COMPRESS	OPT	
		DECOMPRESS	DECOMPRE	OPT
ADACDC	----------	-----------	NONE	
ADACNV	----------	CONVERT	CONVERT	
		REVERT	REVERT	
ADADBS	ADD	ADD	NONE	
		ALLOCATE	ALLOCATE	REQD
		CHANGE	CHANGE	REQD
		CVOLSER	CVOLSER	NONE
		DEALLOCATE	DEALLOCA	REQD
		DECREASE	DECREASE	NONE
		DELCP	DELCP	NONE
		DELETE	DELETE	REQD
		DSREUSE	DSREUSE	REQD
		INCREASE	INCREASE	NONE
		ISNREUSE	ISNREUSE	REQD
		MODFCB	MODFCB	REQD
		NEWALTS	NEWALTS	NONE
		NEWFIELD	NEWFIELD	REQD
		OPERCOM*	OPER	OPT
		PRIORITY	PRIORITY	NONE
		RECOVER	RECOVER	NONE
		REFRESH	REFRESH	REQD
		RELEASE	RELEASE	REQD
		RENAME	RENAME	OPT
		RENUMBER	RENUMBER	REQD
		RESETDIB	RESETDIB	NONE
		REUSEDS	REUSEDS	REQD
		REUSEISN	REUSEISN	REQD
		UNCOUPLE	UNCOUPLE	REQD
ADADCK	DSCHECK	DSCHECK	OPT	
ADADEF	DEFINE	DEFINE	NONE	
		NEWWORK	NEWWORK	NONE
		-----------	-----------	NONE
ADAFRM	ASSOFRM	ASSOFRM	NONE	
		ASSORESET	ASSORESE	NONE
		CLOGFRM	CLOGFRM	NONE
		DATAFRM	DATAFRM	NONE
		DATARESET	DATARESE	NONE
		DSIMFRM	DSIMFRM	NONE
		DSIMRESET	DSIMRESE	NONE
		PLOGFRM	PLOGFRM	NONE
		RLOGFRM	RLOGFRM	NONE
		SORTFRM	SORTFRM	NONE
		TEMPFRM	TEMPFRM	NONE
		WORKFRM	WORKFRM	NONE
		WORKRESET	WORKRESE	NONE

Note: There are many sub-functions associated with OPERCOM. T he Security Administrator may want to restrict access to some of them. Therefore, at the function level, OPERCOM rules will be generated as OPER.*, where * r epresents a sub-function from Figure 8 – Sub-function Table for ADABAS V5 OPERCOM Utility.

Figure 7 – Function Table for ADABAS Utilities

(continued on next page)

(continued from previous page)

ADABAS		FUNCTION	
UTILITY	**FUNCTION**	**IN DSN**	**FILE**
ADAICK ACCHECK	ACCHECK	OPT	
	ASSOPRINT	ASSOPRIN	NONE
	BATCH	BATCH	NONE
	DATAPRINT	DATAPRIN	NONE
	DSCHECK	DSCHECK	OPT
	DUMP	DUMP	NONE
	FCBPRINT	FCBPRINT	OPT
	FDTPRINT	FDTPRINT	OPT
	GCBPRINT	GCBPRINT	NONE
	ICHECK	ICHECK	OPT
	INT	INT	NONE
	NIPRINT	NIPRINT	OPT
	NOBATCH	NOBATCH	NONE
	NODUMP	NODUMP	NONE
	NOINT	NOINT	NONE
	RECORD	RECORD	NONE
	UIPRINT	UIPRINT	OPT
ADAINV COUPLE	COUPLE	REQD	
	INVERT	INVERT	REQD
	RELEASE	RELEASE	REQD
	UNCOUPLE	UNCOUPLE	REQD
ADALOD ASSODEV	ASSODEV	REQD	
	LOAD	LOAD	REQD
	UPDATE	UPDATE	REQD
ADAMER ----------	-----------	NONE	
ADANUC ----------	-----------	NONE	
ADAORD REDB	REDB	OPT	
	REF	REF	REQD
	REORASSO	REORASSO	OPT
	REORDATA	REORDATA	OPT
	REORDB	REORDB	OPT
	REORFASSO	REORFASS	REQD
	REORFDATA	REORFDAT	REQD
	REORFILE	REORFILE	REQD
	RESTRUCTUREDB**	RESTRUCT**	OPT
	RESTRUCTUREF**	RESTRUCT**	REQD
	STORE	STORE	OPT
ADAORI ----------	----------	OPT	
ADAPLP PLOGPRI	PLOGPRI	OPT	
	SPLOGPRI	SPLOGPRI	OPT
	WORKPRI	WORKPRI	OPT
ADAPRI ASSOPRI	ASSOPRI	NONE	
	CLOGPRI	CLOGPRI	NONE
	DATAPRI	DATAPRI	NONE
	DSIMPRI	DSIMPRI	NONE
	PLOGPRI	PLOGPRI	NONE
	RLOGPRI	RLOGRI	NONE
	SORTPRI	SORTPRI	NONE
	TEMPPRI	TEMPPRI	NONE
	WORKPRI	WORKPRI	NONE

Figure 7 – Function Table for ADABAS Utilities

(continued on next page)

(continued from previous page)

ADABAS UTILITY	FUNCTION	FUNCTION IN DSN	FILE
ADARAI CHKDB	CHKDB	NONE	
	DISABLE	DISABLE	NONE
	LIST	LIST	NONE
	PREPARE	PREPARE	NONE
	RECOVER	RECOVER	OPT
	REMOVE	REMOVE	NONE
ADAREF AMIRROR	AMIRROR	NONE	
	DMIRROR	DMIRROR	NONE
	DUPLICATE	DUPLICATE	NONE
	NOMIRROR	NOMIRROR	NONE
	WMIRROR	WMIRROR	NONE
	----------	----------	OPT
ADAREP REPORT	REPORT	OPT	
	----------	----------	OPT
ADARES BACKOUT	BACKOUT	OPT	
	CLCOPY	CLCOPY	NONE
	COPY	COPY	NONE
	PLCOPY	PLCOPY	NONE
	REGENERATE	REGENERA	OPT
	REPAIR	REPAIR	OPT
ADASAV DUMP	DUMP	OPT	
	MERGE	MERGE	OPT
	RESTONL	RESTONL	OPT
	RESTORE	RESTORE	OPT
	RESTPLOG	RESTPLOG	OPT
	SAVE	SAVE	OPT
ADASCR CHANGE	CHANGE	NONE	
	DELETE	DELETE	NONE
	INSERT	INSERT	REQD
	PARMDEF	PARMDEF	NONE
	PFIELDS	PFIELDS	REQD
	PFILES	PFILES	NONE
	PPW	PPW	NONE
	PROTECT	PROTECT	REQD
	REMOVE	REMOVE	NONE
	SBYVALUE	SBYVALUE	REQD
ADASEL END	END	NONE	
	SELECT	SELECT	OPT
ADAULD UNLOAD	UNLOAD	REQD	
	----------	----------	REQD
ADAVAL VALIDATE	VALIDATE	REQD	
ADAZAP ----------	----------	NONE	

Note: Since function names are shortened to 8 characters, the ADAORD functions RESTRUCTUREDB and RESTRUCTUREF will result in the same rule element (RESTRUCT). If rules are being generated to include functions for ADAORD, and it is necessary to distinguish between RESTRUCTUREDB and RESTRUCTUREF, it is recommended that the DSNs be generated for the ADABAS-supplied aliases REDB (for RESTRUCTUREDB) and REF (for RESTRUCTUREF). SECURITRE will recognize both the functions through their aliases.

Figure 7 – Function Table for ADABAS Utilities

A sub-function may or may not be associated with a file for the OPERCOM Utility. Where a file is required, the file name from the STRDEF or STRFNR parameters will be included as part of the DSN.

SUB-FUNCTION	FILE Y/N	SUB- FUNCTION	FILE Y/N	SUB-FUNCTION	FILE Y/N
ADAEND	N	DUUQE	N	NOLOGRB	N
CANCEL	N	FEOFCL	N	NOLOGSB	N
DAUQ	N	FEOFPL	N	NOLOGVB	N
DCQ	N	HALT	N	RDUMPST	N
DDIB	N	LOCKF	Y	READONLY	N
DFILES	Y	LOCKU	Y	REVIEWHUBID**	N
DFILUSE	Y	LOCKX	Y	STOPF	Y
DHQA	N	LOGGING	N	STOPI	N
DLOCKF	N	LOGCB	N	STOPU	N
DNC	N	LOGFB	N	SYNCC	N
DNH	N	LOGIB	N	TNAA	N
DNU	N	LOGIO	N	TNAE	N
DPARM	N	LOGRB	N	TNAX	N
DRES	N	LOGSB	N	TT	N
DSTAT	N	LOGVB	N	UNLOCKF	Y
DTH	N	NOLOGGING*	N	UNLOCKU	Y
DUMP	N	NOLOGCB	N	UNLOCKX	Y
DUQ	N	NOLOGFB	N	UTIONLY	N
DUQA	N	NOLOGIB	N		
DUQE	N	NOLOGIO	N		

* NOLOGGING will be shortened to NOLOGGIN in the DSN.
** REVIEWHUBID will be shortened to REVIEWHU in the DSN.

Figure 8 – Sub-Function Table for ADABAS V5 OPERCOM Utility

IV.3 Utility Security Error Messages

In the event that SECURITRE abends an ADABAS Utility run, a message will be printed showing the reason for the ABEND. The messages printed by SECURITRE are listed below along with the possible cause of the ABEND.

ABEND CODE **ERROR MESSAGE PRINTED AND EXPLANATION**

020 **DBID REQUIRED FOR UTILITY EXECUTION**

In order to allow SECURITRE utility control functions to operate, a DBID must be specified in the start-up parameters.

035 **UNABLE TO OPEN DDKARTE**

SECURITRE utility control was unable to open the DDKARTE dataset.

040 **VALID UTILITY FUNCTION NOT FOUND**

SECURITRE utility control detected a utility function that does not appear to be valid. Check the ADARUN cards to see that all utility functions have been specified correctly.

050 **INTERNAL ERROR ON DDCARD DATA**

SECURITRE utility control detected an internal error in the DDCARD data. Check the DDCARD dataset.

055 **PARM CARD ERROR ON DDCARD**

SECURITRE detected an error in the ADARUN parameter cards that were submitted.

056 **CARD MUST START WITH ADARUN**

SECURITRE detected that a utility job card did not contain the ADARUN keyword.

060 **INVALID DATABASE SPECIFIED**

The database specified in the ADARUN cards is not a valid ADABAS database.

150 **PARM CARD ERROR ON DDKARTE**

SECURITRE detected an error in the ADARUN DDKARTE cards.

151 **CARD MUST START WITH UTILITY NAME**

SECURITRE could not find the utility name in the ADARUN card being processed. Check the ADARUN cards for errors.

155 **UTILITY NOT THE SAME AS SPECIFIED WITHIN DDCARD**

The DDKARTE and DDCARD information in the ADARUN parameters does not match. Verify that the correct utility is listed on both the DDCARD and DDKARTE.

165 **INTERNAL ERROR ON DDKARTE DATA**

SECURITRE utility control detected an internal error in the DDCARD data. Check the DDCARD dataset.

170 NO VALID UTILITY FUNCTION DETECTED

The ADARUN card being processed did not specify a valid utility function. Examine the cards for correctness.

175 FILE NUMBER IS REQUIRED FOR THIS UTILITY FUNCTION

The ADARUN cards did not specify which file a utility is operating against. Check the cards for completeness.

180 INVALID UTILITY FUNCTION DETECTED

The ADARUN cards contained an invalid utility function. Verify that the cards are correct.

190 INVALID FILE NUMBER SPECIFIED

The ADARUN cards specified an invalid file number. Verify that the cards are correct.

300 SECURITRE HAS EXPIRED

SECURITRE requires a new expiration date. If the new expiration date zap has not been received, contact TSI.

301 SECURITRE GETMAIN FAILURE OCCURRED FOR RACF, 512 MORE BYTES NEEDED

SECURITRE was unable to GETMAIN the needed memory. Increase the region size by at least 512 bytes.

303 SECURITRE COULD NOT LOCATE THE FILE DEFAULTS (STRPARM)

Ensure that the STRPARM module is available and accessible to SECURITRE.

304 SECURITRE DETECTED INVALID FILE DEFAULTS (STRPARM)

Verify the parameters specified for SECURITRE to ensure that they are coded correctly.

305 SECURITRE DETECTED INVALID FILE DEFAULTS (STRPARM). BAD COND CODE

Verify the parameters specified for SECURITRE to ensure that they are coded correctly.

400 INTERNAL ERROR DETECTED

SECURITRE detected an internal error. Contact TSI.

913 NOT AUTHORIZED FOR THIS UTILITY FUNCTION FOR THIS DATABASE AND FILE SECURITRE WILL ABEND THIS UTILITY

The SSF reported to SECURITRE that the user in question could not execute the requested utility function on the selected database and file. Therefore, the utility job was ABENDed.

This page intentionally left blank.

SECTION V

REAL-TIME MONITOR

V.1 Introduction to the Real-Time Monitor (RTM)

The SECURITRE Real-time Monitor (RTM) provides an on- line view of the current SECURITRE status on any applicable database. With the RTM, the Security Administrator may:

- Display and make modifications to internal SECURITRE tables to keep SECURITRE synchronized with current RACF/ACF2/TOP-SECRET rules.
- Display and modify (reload) certain SECURITRE parameters.
- Reload certain user-exits.
- Start or stop the SECURITRE Trace Facility or modify what is being traced.

V.2 RTM Screen Navigation

Real-Time Monitor (RTM) screen navigation is accomplished through PF-Keys and with screen names. PF1 is always used for the "Help" function. PF3 always means to return to the menu.

The ENTER key is used to execute the selected function on the indicated DBID.

PF12 can be configured so that it performs a NATURAL STOP or a TERMINATE through the use of the "TERM" parameter in the STRDEF statement. STOP will take the user out of the RTM, while remaining in NATURAL. TERMINATE will take the user out of NATURAL, in effect preventing the user from performing other functions within NATURAL.

The screen name is displayed at the bottom right of most screens. The screen name can be entered on the direct command line of each screen to transfer control from one screen to another. Pressing ENTER causes the screen transfer to take place and the RTM immediately displays the new screen.

For example, while on the Display SECURITRE Parms "PARM" screen, one may immediately transfer control to the Reload SECURITRE Parms "RPRM" screen by entering "RPRM" on the direct command line and pressing ENTER. A list of the available RTM modules/screen names is provided on the following page.

V.3 RTM Screen Names

RTM programs are executable by entering the screen name in the Screen-ID field at the top of the screen. While many NATURAL modules make up the RTM, only the following modules are directly executable by entering the valid name in the Screen-ID field:

SCREEN NAME	SCREEN FUNCTION
MENU	Main Menu
FRC1	Force One User From the Tables
FRCA	Force All Users From the Tables
PARM	Display SECURITRE parms
REXT	Reload User-Exit(s)
RPRM	Reload SECURITRE parms
TRAC	SECURITRE Trace Facility
TRIM	Invoke the TRIM Real-Time Monitor (if installed)
NPRM	Display SECURITRE/NATURAL parms
TBLS	Display Current Table Sizes
STOP	Terminate the Real-time Monitor

Figure 9 – RTM Screen Names

V.4 RTM Security

The RTM functions are secured by SECURITRE. Some of the functions described in the next section may not be available to all users. The security administrator defines what functions each user can access via SSF rules. If a function is not available, a rule must be changed/added to the SSF before access will be granted by SECURITRE. Refer to **Section V.2 – RTM Security** in the SECURITRE Administrator Manual for more information on RTM security.

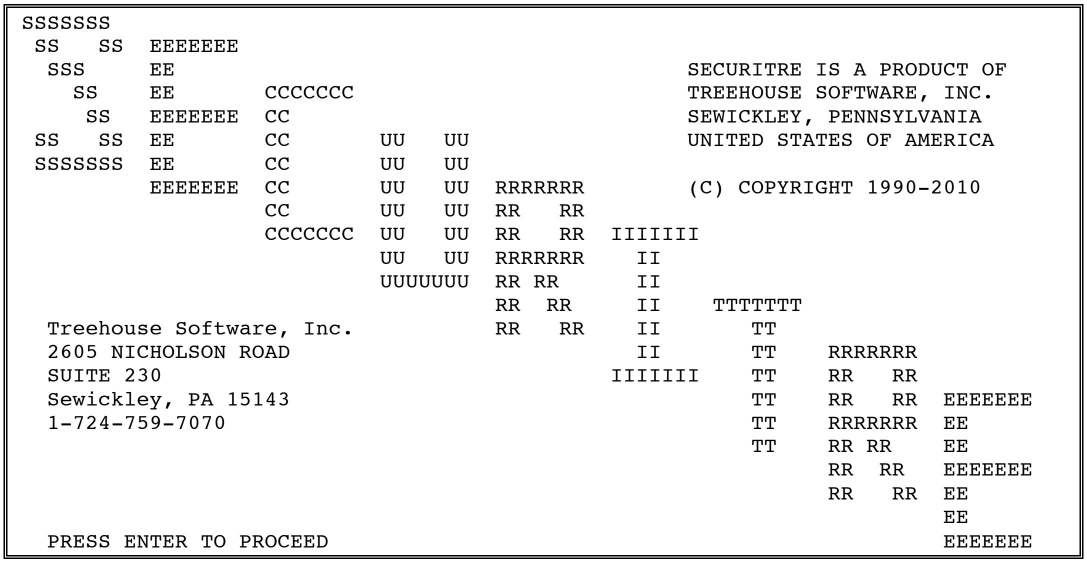
V.5 RTM Screen Functions

Although others may use the RTM, for illustration purposes assume that the Security Administrator is the user.

Standard procedures at the user's site are used to first invoke NATURAL. Then the Security Administrator logs onto "STRLIB" or whichever library the RTM was installed onto and executes the "MENU" Program.

```
LOGON STRLIB
MENU
```

The following screen is displayed:

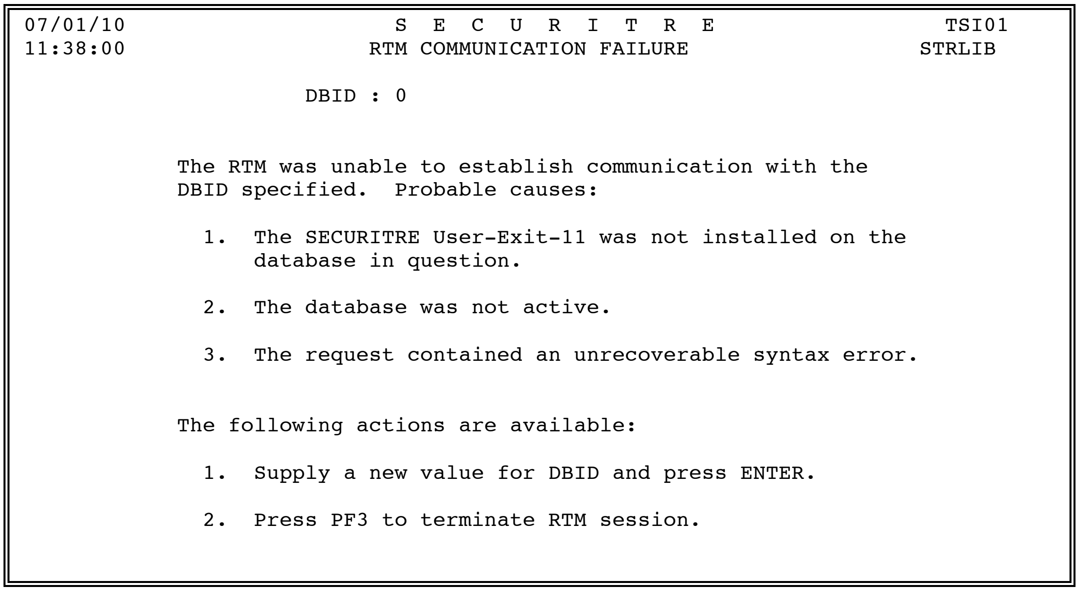


```
SSSSSSS
 SS    SS EEEEEEE
  SSS     EE                                        SECURITRE IS A PRODUCT OF
    SS    EE       CCCCCCC                          TREEHOUSE SOFTWARE, INC.
     SS   EEEEEEE  CC                               SEWICKLEY, PENNSYLVANIA
 SS    SS EE       CC       UU   UU                 UNITED STATES OF AMERICA
 SSSSSSS  EE       CC       UU   UU
          EEEEEEE  CC       UU   UU  RRRRRRR        (C) COPYRIGHT 1990-2010
                   CC       UU   UU  RR   RR
                   CCCCCCC  UU   UU  RR   RR  IIIIIII
                            UU   UU  RRRRRRR    II
                            UUUUUUU  RR RR      II
                                     RR  RR     II    TTTTTTT
  Treehouse Software, Inc.           RR   RR    II       TT
  2605 NICHOLSON ROAD                           II       TT    RRRRRRR
  SUITE 230                                   IIIIIII    TT    RR   RR
  Sewickley, PA 15143                                    TT    RR   RR  EEEEEEE
  1-724-759-7070                                         TT    RRRRRRR  EE
                                                         TT    RR RR    EE
                                                               RR  RR   EEEEEEE
                                                               RR   RR  EE
                                                                        EE
  PRESS ENTER TO PROCEED                                                EEEEEEE
```

The "Authorized" line on this screen may authorize use:

- For limited trial
- By licensee only
- By a particular licensee, by name

If SECURITRE detects a problem communicating with its User-Exit-11, the screen below is displayed and describes the probable causes of the failure and the possible corrective actions.

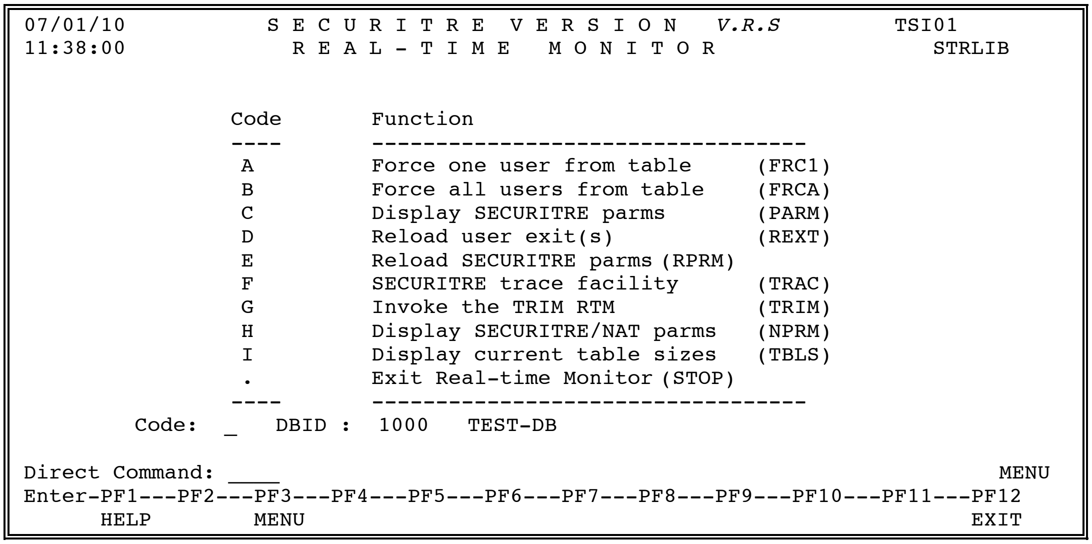


```
07/01/10                    S  E  C  U  R  I  T  R  E                TSI01
11:38:00                   RTM COMMUNICATION FAILURE                STRLIB

                      DBID : 0


             The RTM was unable to establish communication with the
             DBID specified.  Probable causes:

               1.  The SECURITRE User-Exit-11 was not installed on the
                   database in question.

               2.  The database was not active.

               3.  The request contained an unrecoverable syntax error.


             The following actions are available:

               1.  Supply a new value for DBID and press ENTER.

               2.  Press PF3 to terminate RTM session.
```

To attempt to examine another database, the Security Administrator must input the new DBID number and press ENTER. To exit the SECURITRE RTM, the Security Administrator would press PF3.

In some cases, this screen will list a "probable cause" (e.g., "UEX11 installed, UEX4 not installed"). One common message is "REASON UNKNOWN, usually ADABAS RESPONSE: 0" indicates that SECURITRE cannot find a User-ID for this user or that the user does not have RTM security. If there is no default DBID specified in the module MENU, the default DBID will be the same as the database where the FUSER is located (shown by the SYSPROF command). If SECURITRE's User-Exit-11 is not installed on the default database, the user will have to enter a different DBID on the screen.

Once ENTER is pressed, the following Main Menu screen is displayed:



```
07/01/10           S E C U R I T R E  V E R S I O N   V.R.S         TSI01
11:38:00             R E A L - T I M E   M O N I T O R                 STRLIB


                Code       Function
                ----       ----------------------------------
                 A         Force one user from table     (FRC1)
                 B         Force all users from table    (FRCA)
                 C         Display SECURITRE parms       (PARM)
                 D         Reload user exit(s)           (REXT)
                 E         Reload SECURITRE parms (RPRM)
                 F         SECURITRE trace facility      (TRAC)
                 G         Invoke the TRIM RTM           (TRIM)
                 H         Display SECURITRE/NAT parms   (NPRM)
                 I         Display current table sizes   (TBLS)
                 .         Exit Real-time Monitor (STOP)
                ----       ----------------------------------
         Code:  _   DBID :  1000   TEST-DB

Direct Command: ____                                                        MENU
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP        MENU                                                    EXIT
```

The date and time are displayed at the top left of every screen. The User-ID and current library are displayed at the top right of every screen. The screen name appears at the bottom right of most screens.

PF1 will always display help for the current screen.

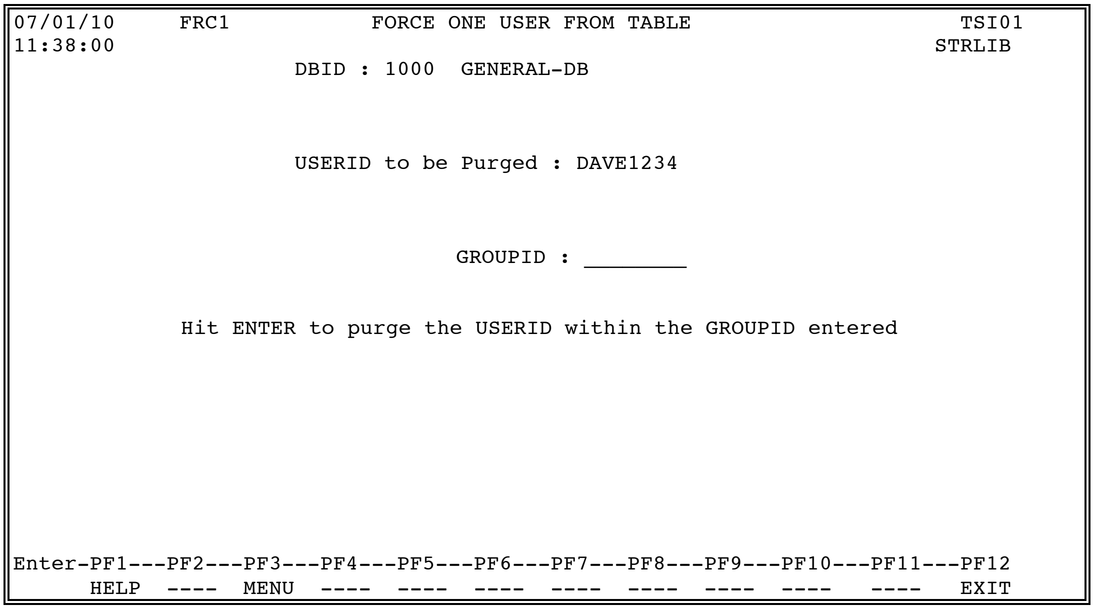
PF3 will always return to this menu screen.

On most screens, the Security Administrator may press PF12 to discontinue monitoring.

V.5.1 Force One User from the Table

SECURITRE provides the ability to perform synchronization with the SSF at timed intervals as specified in the "STRPARM" module. For more information about FORCE, PURINTT, PURINTV parameters, refer to **Section II.3 – STRDEF Parameters**. The synchronization allows SECURITRE to adjust to any changes in a user's security rules within the SSF in a reasonable period of time. Using the RTM function "FRC1", the Security Administrator can force a user from the SECURITRE internal tables causing an immediate synchronization between SECURITRE and the SSF for the specified user.

To force a particular user from the SECURITRE internal tables, enter the appropriate SSF User-ID on the following screen:



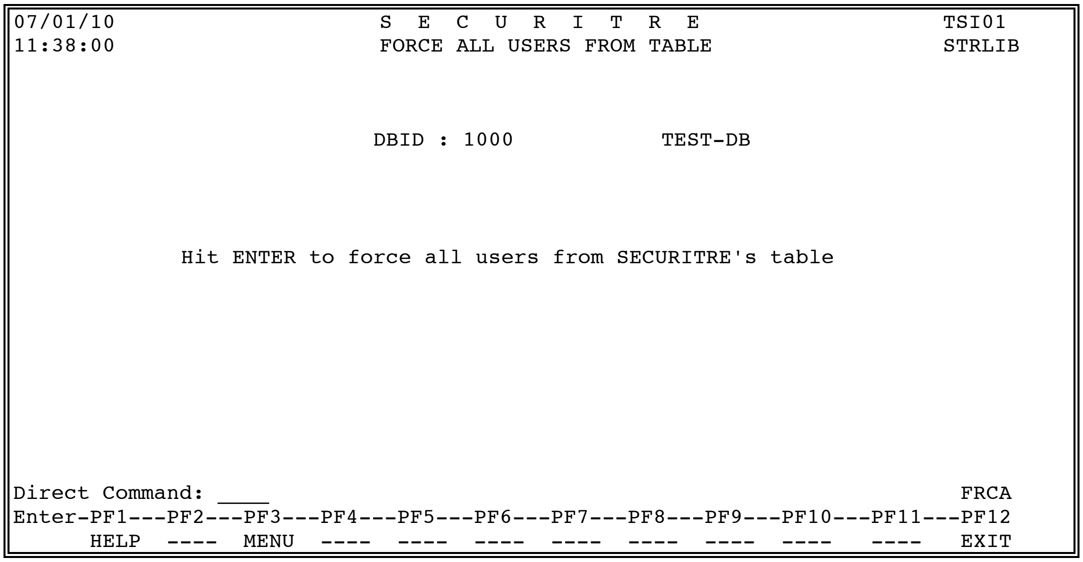
```
07/01/10     FRC1           FORCE ONE USER FROM TABLE                    TSI01
11:38:00                                                                STRLIB
                      DBID : 1000  GENERAL-DB



                      USERID to be Purged : DAVE1234



                                  GROUPID : ________


             Hit ENTER to purge the USERID within the GROUPID entered








Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

The SECURITRE table entry for User-ID "DAVE1234" will be removed when ENTER is pressed. The next ADABAS access by "DAVE1234" will result in SECURITRE retrieving the current access information for DAVE1234 for that file from the SSF on the user's next call to ADABAS.

V.5.2 Force All Users from the Table

When changes are made to SSF rules affecting hundreds of users, removing the individual users from the SECURITRE internal tables might be time-consuming or error-prone. For this reason, SECURITRE makes it possible to use the RTM to remove all users from the internal tables. This ensures that any changes in SSF rules will be synchronized with SECURITRE actions.

To remove all the users from the SECURITRE internal tables, enter the appropriate Database-ID on the following screen:



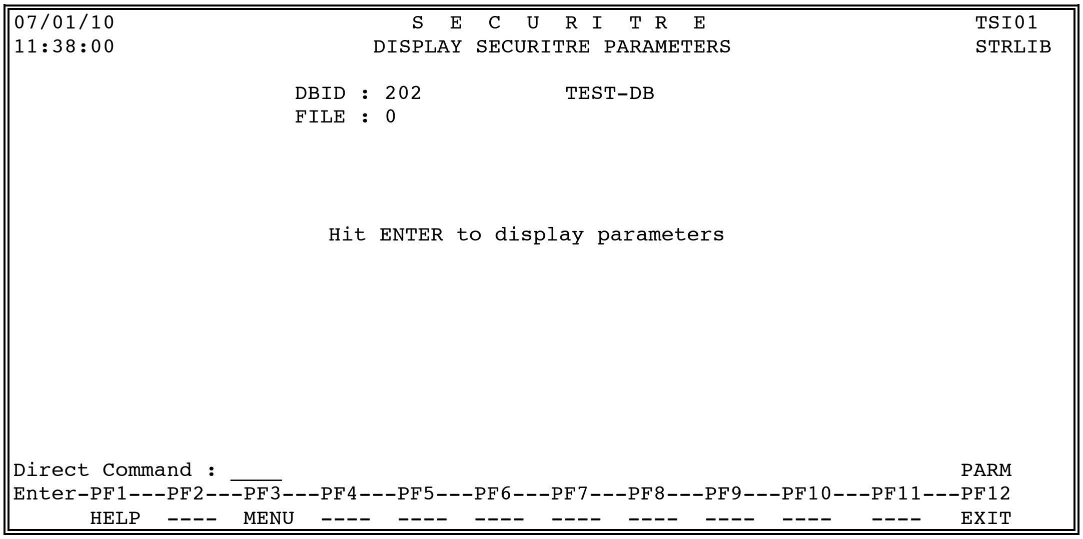
```
07/01/10                    S  E  C  U  R  I  T  R  E                 TSI01
11:38:00                    FORCE ALL USERS FROM TABLE                STRLIB



                           DBID : 1000           TEST-DB




             Hit ENTER to force all users from SECURITRE's table









Direct Command: ____                                                   FRCA
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

In the example above, all users will be forced from the tables maintained by SECURITRE in its User-Exit-1 on DBID number 1000, the "PAYROLL-DATABASE" database.

V.5.3 Display SECURITRE Parameters

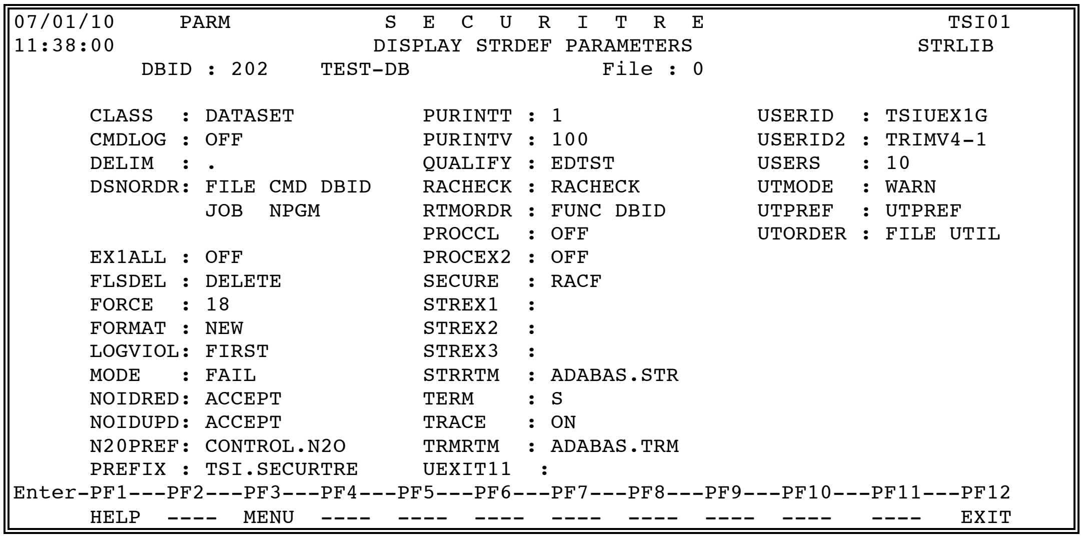
The Security Administrator may wish to determine if SECURITRE has been configured as desired.

In order to display the STRDEF parameters in effect for database 202, the Security Administrator would enter "202" in the DBID field on the following screen:



```
07/01/10                       S  E  C  U  R I  T R  E                     TSI01
11:38:00                    DISPLAY SECURITRE PARAMETERS                   STRLIB

                      DBID : 202           TEST-DB
                      FILE : 0





                         Hit ENTER to display parameters









Direct Command : ____                                                     PARM
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

Once ENTER is pressed, the STRDEF parameters active on database 202 are displayed as shown on the following screen:

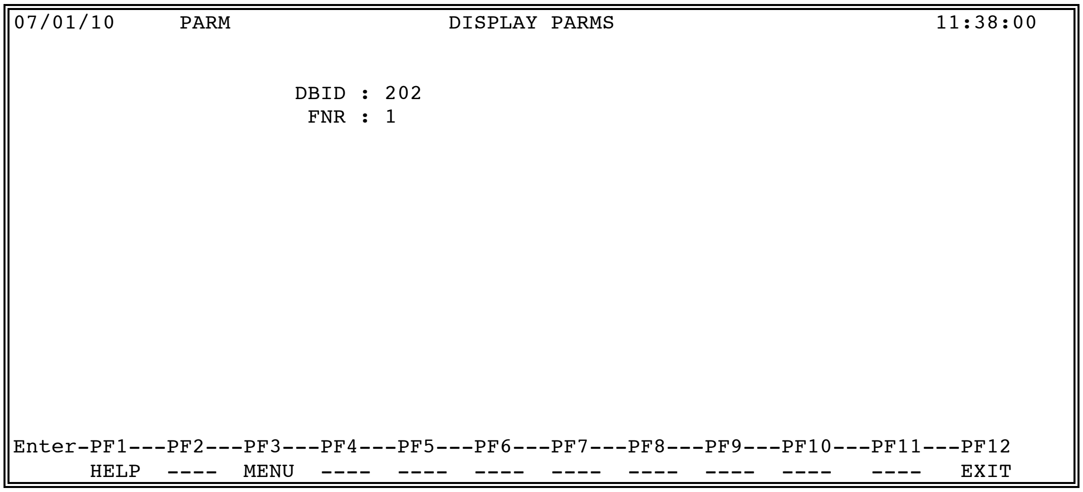


```
07/01/10     PARM           S  E  C  U  R  I  T  R  E                TSI01
11:38:00                    DISPLAY STRDEF PARAMETERS              STRLIB
          DBID : 202    TEST-DB              File : 0

      CLASS  : DATASET          PURINTT : 1                USERID  : TSIUEX1G
      CMDLOG : OFF              PURINTV : 100              USERID2 : TRIMV4-1
      DELIM  : .                QUALIFY : EDTST            USERS   : 10
      DSNORDR: FILE CMD DBID    RACHECK : RACHECK          UTMODE  : WARN
               JOB  NPGM        RTMORDR : FUNC DBID        UTPREF  : UTPREF
                                PROCCL  : OFF              UTORDER : FILE UTIL
      EX1ALL : OFF              PROCEX2 : OFF
      FLSDEL : DELETE           SECURE  : RACF
      FORCE  : 18               STREX1  :
      FORMAT : NEW              STREX2  :
      LOGVIOL: FIRST            STREX3  :
      MODE   : FAIL             STRRTM  : ADABAS.STR
      NOIDRED: ACCEPT           TERM    : S
      NOIDUPD: ACCEPT           TRACE   : ON
      N20PREF: CONTROL.N2O      TRMRTM  : ADABAS.TRM
      PREFIX : TSI.SECURTRE     UEXIT11  :
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

This display includes all STRDEF parameters in effect on database 202, except for those that control table size, which may be seen using the TBLS function. For example, it can be seen that SECURITRE will purge the SECURITRE internal tables at 6:00 p.m. (18:00).

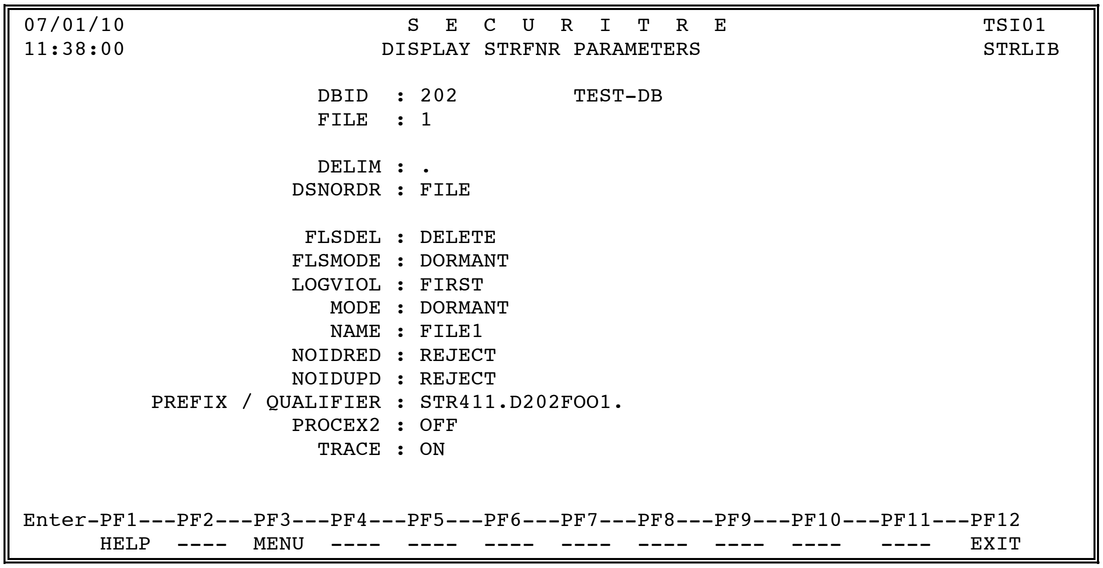
Several STRDEF parameters may be overridden at the file level. For example, file 1 may have been set to DORMANT mode in one of the STRFNR statements.

To see the STRFNR overrides, the Security Administrator would enter "1" in the FNR field on the "PARM" screen, as shown on the following screen:



```
07/01/10     PARM                DISPLAY PARMS                          11:38:00


                      DBID : 202
                       FNR : 1
















Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

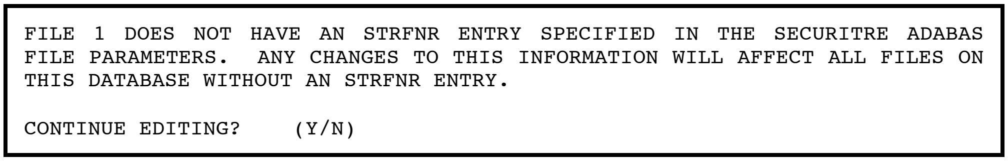
When ENTER is pressed, the STRFNR override parameters in effect for database 202, file number 1 will be displayed as shown on the following screen:



```
07/01/10                     S  E  C  U  R  I  T  R  E                     TSI01
11:38:00                   DISPLAY STRFNR PARAMETERS                       STRLIB

                       DBID  : 202         TEST-DB
                       FILE  : 1

                       DELIM : .
                     DSNORDR : FILE

                      FLSDEL : DELETE
                     FLSMODE : DORMANT
                     LOGVIOL : FIRST
                        MODE : DORMANT
                        NAME : FILE1
                     NOIDRED : REJECT
                     NOIDUPD : REJECT
          PREFIX / QUALIFIER : STR411.D202FOO1.
                     PROCEX2 : OFF
                       TRACE : ON


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

All of the displayed STRFNR parameters, with the exception of PREFIX / QUALIFIER, may be updated by typing the new values over the existing values and hitting ENTER. To avoid updating these values, press PF 3. If updated, the new values will be in effect until the parameters are reloaded using RPRM or until the database is brought down.

If FILEMAX=NEW is specified and the file number entered in the FILE field does not have an STRFNR definition in the 'STRPARMS', the following window will be displayed.



```
FILE 1 DOES NOT HAVE AN STRFNR ENTRY SPECIFIED IN THE SECURITRE ADABAS
FILE PARAMETERS.  ANY CHANGES TO THIS INFORMATION WILL AFFECT ALL FILES ON
THIS DATABASE WITHOUT AN STRFNR ENTRY.

CONTINUE EDITING?    (Y/N)
```

This indicates that the default parameters defined by STRDEF are in effect for this file. Entering 'N' at this prompt will allow the user to view the parameters, but they may not change them. The message '*** BROWSE MODE *** DEFAULT PARAMETERS DISPLAYED' is displayed at the bottom of the screen to indicate that editing is not allowed.

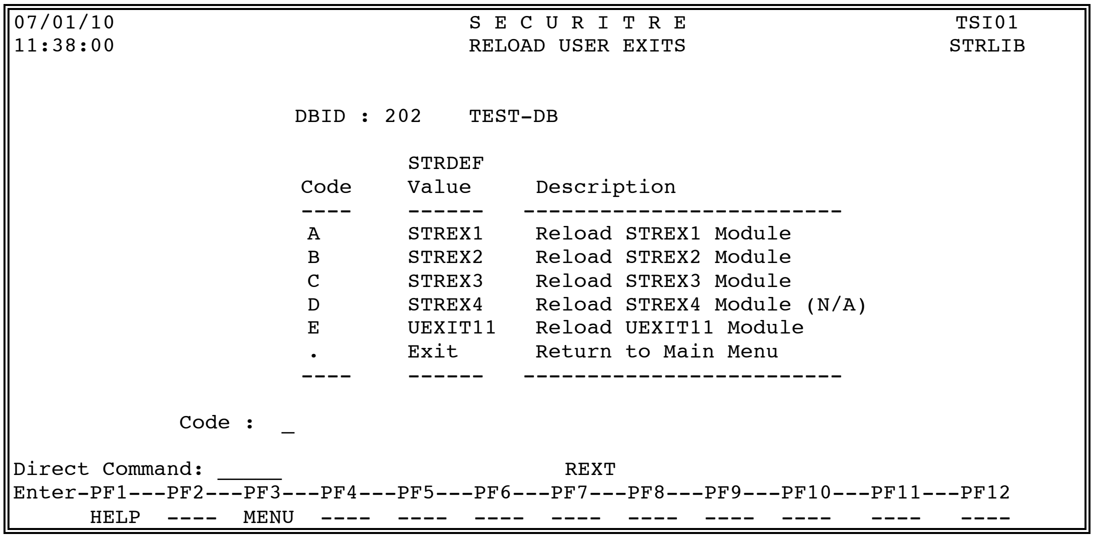
Entering 'Y' at this prompt will allow the user to change all of the parameters except the NAME and PREFIX/QUALIFIER fields. The message '***EDIT MODE*** DEFAULT PARAMETERS DISPLAYED' is displayed at the bottom of the screen to indicate that editing is allowed.

Note: Changes to the default parameters will affect **ALL** files that do not have an STRFNR specification in the 'STRPARMS'.

V.5.4 Reload User-Exits

When changes are made to a particular SECURITRE User-Exit or to another User-Exit-11 in effect for a particular database, the Security Administrator may reload these exits using the RTM.

Assume that TRIM's User-Exit-11 is specified in the UEXIT11 parameter of STRDEF in the "STRPARMS" (refer to Section II.3 STRDEF Parameters). If the database administrator applies a zap supplied by TSI to Securitre's User-Exit-11 parameter, the database would normally have to be bounced to load the new user edit. However, this can be done while the database is up using the SECURITRE RTM. This is accomplished by entering "REXT" or pressing "D" on the Main Menu, then entering the appropriate DBID and the letter "E" for the number of the exit to be reloaded on the following screen:



```
07/01/10                           S E C U R I T R E                     TSI01
11:38:00                           RELOAD USER EXITS                     STRLIB


                      DBID : 202    TEST-DB

                               STRDEF
                       Code    Value     Description
                       ----    ------   -------------------------
                        A      STREX1    Reload STREX1 Module
                        B      STREX2    Reload STREX2 Module
                        C      STREX3    Reload STREX3 Module
                        D      STREX4    Reload STREX4 Module (N/A)
                        E      UEXIT11   Reload UEXIT11 Module
                        .      Exit      Return to Main Menu
                       ----    ------   -------------------------

              Code :  _

Direct Command: _____                      REXT
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   ----
```

When ENTER is pressed, SECURITRE will reload the update User-Exit-11. In the example above, Securitre's User-Exit-11 with the new zap will be re-loaded. The following modules can be reloaded dynamically using the SECURITRE RTM 'REXT' function:

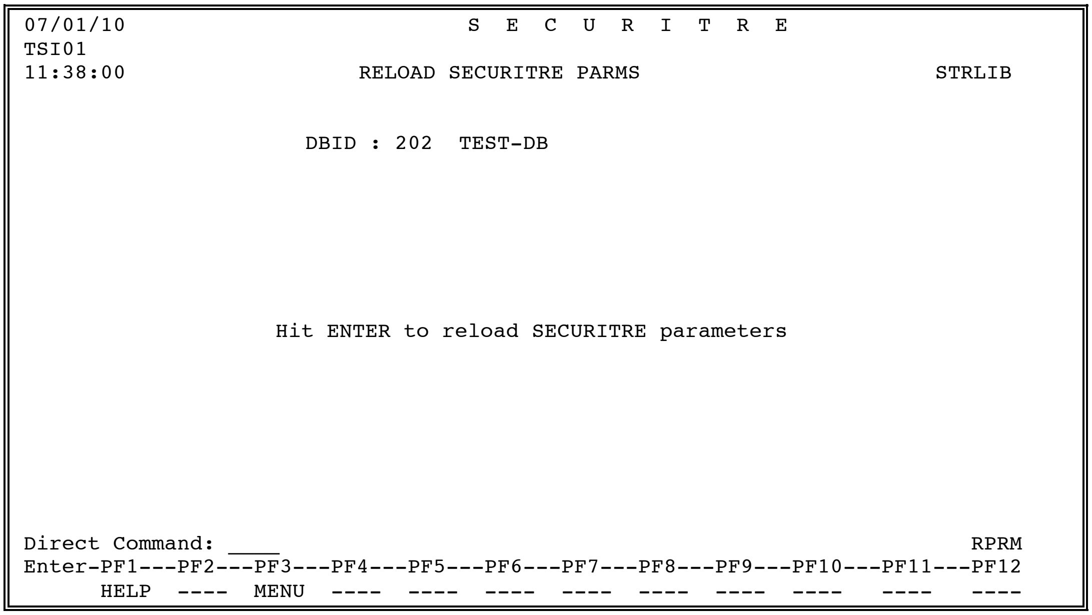
STRDEF Parameter	Description
STREX1	The module defined as SECURITRE's User-Exit-11. This is not the STRUEX11 module.
STREX2	The module defined as SECURITRE's User-Exit-2.
STREX3	The module defined as SECURITRE's User-Exit-3.
STREX4	The module defined as SECURITRE's User-Exit-4.
UEXIT11	The module defined as the second ADABAS User-Exit-11 to call after SECURITRE has finished processing the command.

For more information on the STRDEF parameters STREX1, STREX2, STREX3, STREX4, and UEXIT11, refer to **Section II.3 - STRDEF Parameters**.

V.5.5 Reload SECURITRE Parameters

To refresh the SECURITRE parameters for a particular database without bringing the database down and up, the Security Administrator would prepare a modified STRPARM module and reload the SECURITRE parameters by entering "RPRM" or pressing "E" on the Main Menu.

To reload the parameters, the DBID must be entered on the following screen and the ENTER key pressed.



```
07/01/10                          S E C U R I T R E
TSI01
11:38:00                  RELOAD SECURITRE PARMS                       STRLIB


                      DBID : 202  TEST-DB







                    Hit ENTER to reload SECURITRE parameters








Direct Command: ____                                                     RPRM
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   ----
```

Once ENTER is pressed, SECURITRE will reload its parameter settings for the specified database. This can be verified by re-displaying the parameters for that database.

After the reload parameter processing, SECURITRE will use the new parameter settings to control access to the given database. The following individual parameter settings are **not** adjusted by a reload of the SECURITRE "STRPARM" module:

DSNPOOL

This parameter controls the size of the DSN table to be GETMAINed by SECURITRE. All GETMAIN requests are issued during startup only. Changes to the DSNPOOL parameter will become effective only after the database is brought down and up.

FLSPOOL

This parameter controls the size of the table used to maintain CID information for Field Level Security processing. Changes to the FLSPOOL parameter will become effective only after the database is brought down and up.

USRPOOL

This parameter controls the size of the user / DSN relationship table to be GETMAINed by SECURITRE. All GETMAIN requests are issued during startup only. Changes to the USRPOOL parameter will become effective only after the database is brought down and up.

USERS

This parameter controls the size of the user table to be GETMAINed by SECURITRE. All GETMAIN requests are issued during startup only. Changes to the USER parameter will only become effective after the database is brought down and up.

STREX1-4

User-Exits to SECURITRE are not re-loaded during a reload of the SECURITRE parameters. To obtain a fresh copy of the SECURITRE user-exits, use the "REXT" function.

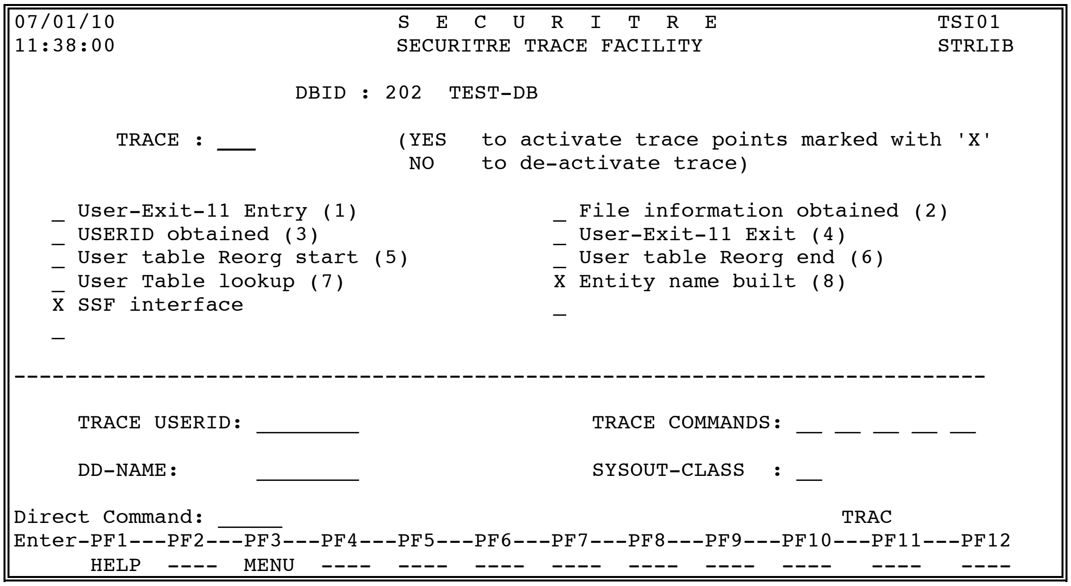
UEXIT11

Other ADABAS User-Exit-11 programs are not re-loaded during a reload of the SECURITRE parameters. To obtain a fresh copy of another ADABAS User-Exit-11 program, use the REXT function.

V.5.6 Trace Facility

If a problem should develop with SECURITRE, TSI's support personnel will want to help the customer solve it as rapidly as possible. A Trace Facility has been implemented within SECURITRE to produce diagnostic trace messages that will enable TSI support personnel to more easily determine the source of the customer's problem.

The Trace Facility can significantly increase the overhead associated with ADABAS. Therefore, it is recommended that the Trace Facility should only be activated while testing SECURITRE or when a problem arises.



```
07/01/10                      S  E  C  U  R  I  T  R  E                 TSI01
11:38:00                      SECURITRE TRACE FACILITY                  STRLIB

                      DBID : 202  TEST-DB

        TRACE : ___           (YES   to activate trace points marked with 'X'
                               NO    to de-activate trace)

   _ User-Exit-11 Entry (1)              _ File information obtained (2)
   _ USERID obtained (3)                 _ User-Exit-11 Exit (4)
   _ User table Reorg start (5)          _ User table Reorg end (6)
   _ User Table lookup (7)               X Entity name built (8)
   X SSF interface                       _
   _
----------------------------------------------------------------------------

     TRACE USERID: ________               TRACE COMMANDS: __ __ __ __ __

     DD-NAME:      ________               SYSOUT-CLASS  : __

Direct Command: _____                                            TRAC
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   ----
```

To activate specific trace point(s), enter "X" next to the desired trace point(s) and enter YES in the TRACE field. To turn off all trace points, enter NO in the TRACE field.

To limit trace information to a specific User-ID, enter the User-ID in the TRACE USERID field. You may specify a group of User.IDs (all same prefix) by terminating the search argument ends with an asterisk.

To limit trace information to a specific set of ADABAS commands, enter the commands in the TRACE COMMANDS field.

Since tracing is also limited to files that have the TRACE parameter set to ON, it may be necessary to use the PARM function to update the TRACE parameter. When using the PARM function, tracing can be turned off for only one file at a time.

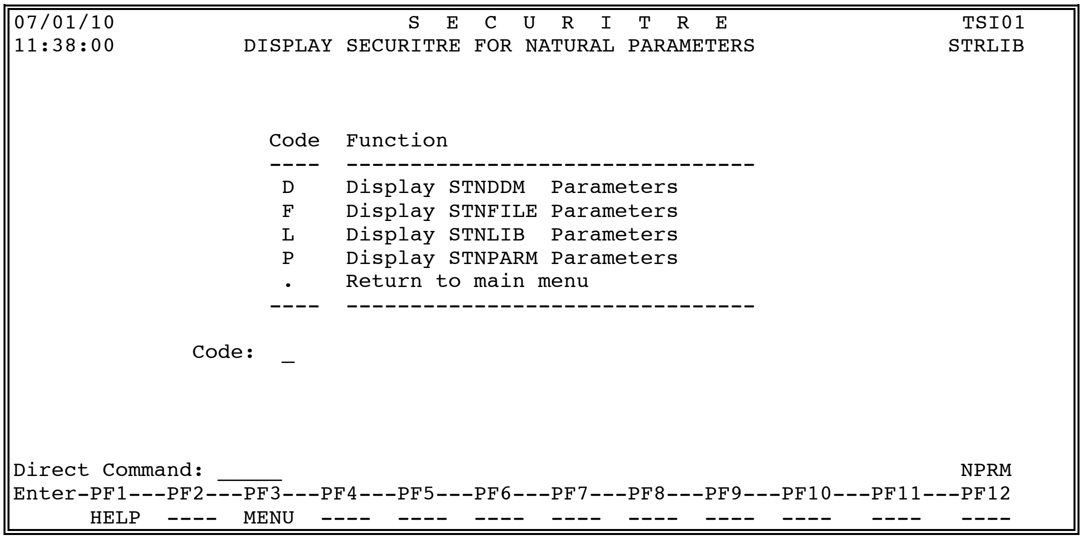
When turning the TRACE off for a file, it is more efficient to turn it off by using the PARM function or by reloading the parameters using the RPRM function than to simply enter NO in the TRACE field in the TRAC facility.

To direct the trace output data to a specific DD-name, enter the requested value in the DD-NAME field. If this DD-name is not allocated in the start-up JCL of ADABAS it will be dynamically allocated and assigned to SYSOUT.
SYSOUT-CLASS has only effect if DD-name is not defined in the start-up JCL. A dynamically allocated trace output file will be closed if tracing is turned off..

Any changes to DD-NAME and/or SYSOUT CLASS will only become effective at the next OPEN to the trace output file. You have to turn trace off (NO) and on (YES) again.

V.5.7 <u>Display SECURITRE/NATURAL Parameters</u>

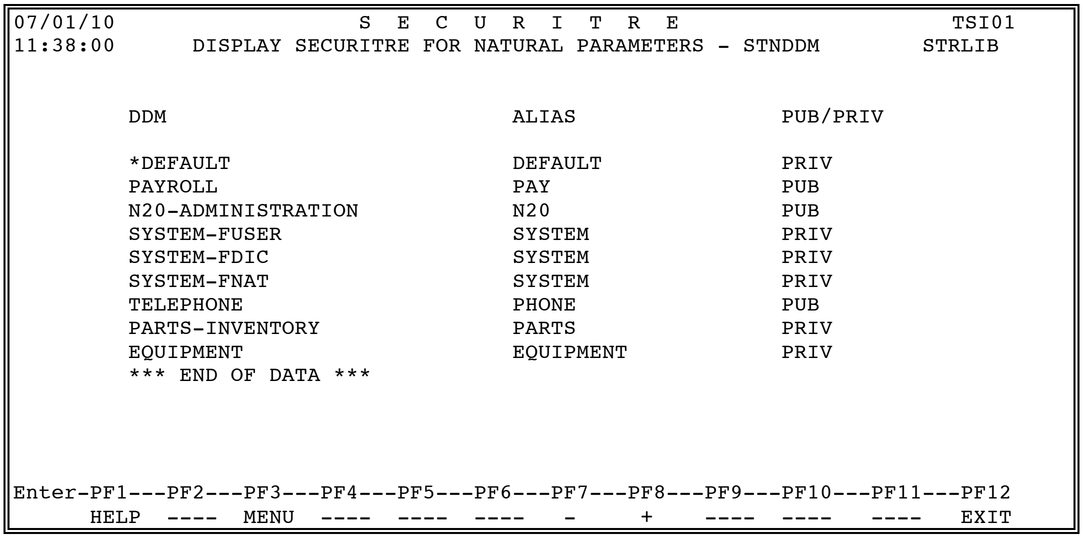
To display the current SECURITRE for NATURAL parameter settings, the Security Administrator should either enter "NPRM" or press "H" on the Main Menu. Then, the following screen is displayed:



```
07/01/10                      S  E  C  U  R  I  T  R  E                    TSI01
11:38:00          DISPLAY SECURITRE FOR NATURAL PARAMETERS                STRLIB



                    Code  Function
                    ----  --------------------------------
                     D    Display STNDDM  Parameters
                     F    Display STNFILE Parameters
                     L    Display STNLIB  Parameters
                     P    Display STNPARM Parameters
                     .    Return to main menu
                    ----  --------------------------------

              Code:  _




Direct Command: _____                                                     NPRM
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   ----
```

By entering the appropriate code, any of the four types of SECURITRE for NATURAL parameters (STNPARM, STNLIB, STNDDM, or STNFILE) may be displayed. Entering a "." or pressing PF3 returns to the Main Menu.

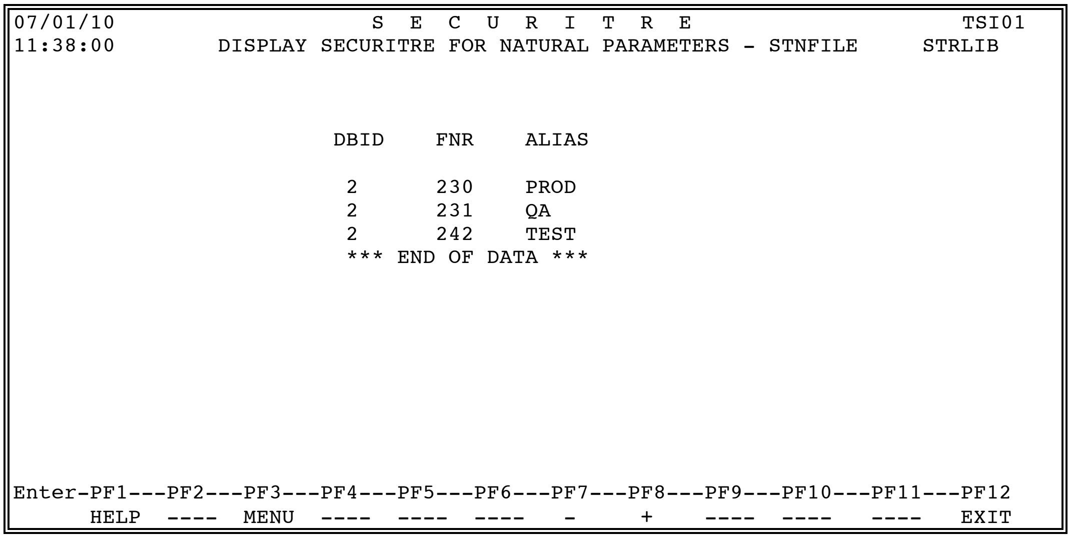
When item "D" is selected to display the STNDDM parameters, the following screen is displayed:



```
07/01/10                  S  E  C  U  R  I  T  R  E                       TSI01
11:38:00      DISPLAY SECURITRE FOR NATURAL PARAMETERS - STNDDM        STRLIB


         DDM                            ALIAS               PUB/PRIV

         *DEFAULT                       DEFAULT             PRIV
         PAYROLL                        PAY                 PUB
         N20-ADMINISTRATION             N20                 PUB
         SYSTEM-FUSER                   SYSTEM              PRIV
         SYSTEM-FDIC                    SYSTEM              PRIV
         SYSTEM-FNAT                    SYSTEM              PRIV
         TELEPHONE                      PHONE               PUB
         PARTS-INVENTORY                PARTS               PRIV
         EQUIPMENT                      EQUIPMENT           PRIV
         *** END OF DATA ***




Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----   -     +    ----  ----   ----   EXIT
```

The STNDDM parameters are displayed in the order in which they are listed in the parameter dataset. Up to 13 STNDDM statements will be displayed on each screen. PF8 may be used to scroll forward in the list if more than one page of data is available. PF7 may be used to scroll backward.

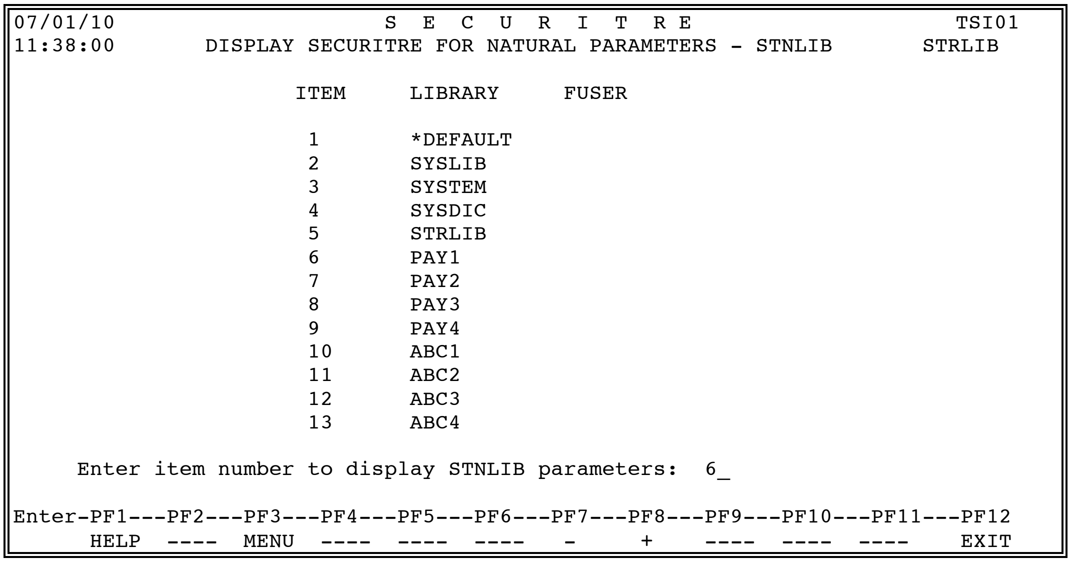
The STNFILE parameters may be displayed by entering "F" on the NPRM menu.



```
07/01/10                   S  E  C  U  R  I  T  R  E                    TSI01
11:38:00        DISPLAY SECURITRE FOR NATURAL PARAMETERS - STNFILE     STRLIB



                         DBID    FNR    ALIAS

                          2      230    PROD
                          2      231    QA
                          2      242    TEST
                          *** END OF DATA ***









Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----   -     +    ----  ----   ----   EXIT
```

The STNFILE parameters are displayed in the order in which they are listed in the parameter dataset. Up to 13 STNFILE statements will be displayed on each screen. PF8 m ay be used to scroll forward in the list if more than one page of data is available. PF7 may be used to scroll backward.

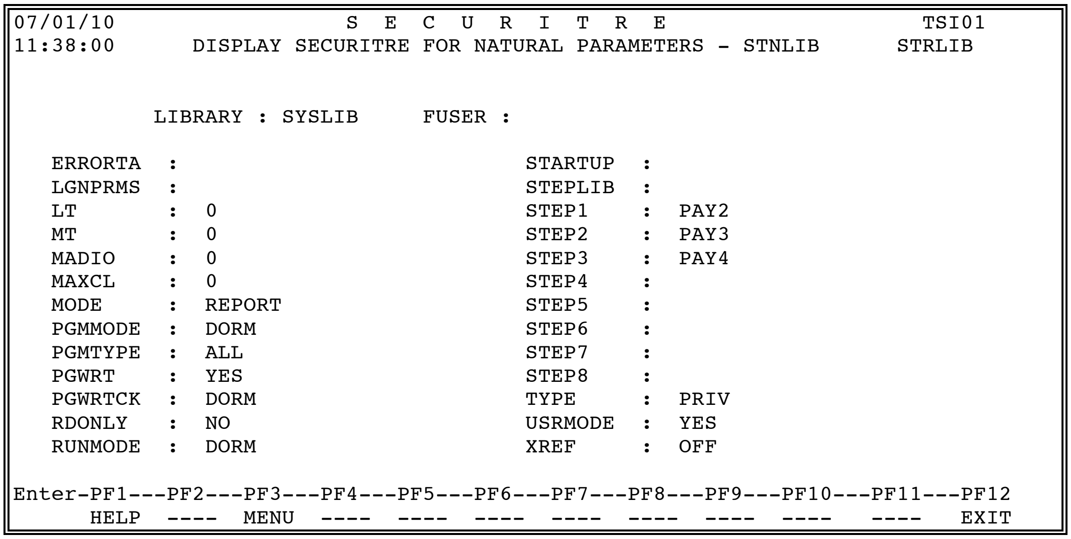
The STNLIB parameters may be displayed by entering "L" on the NPRM menu.



```
07/01/10                    S  E  C  U  R  I  T  R E                   TSI01
11:38:00       DISPLAY SECURITRE FOR NATURAL PARAMETERS - STNLIB       STRLIB

                      ITEM     LIBRARY     FUSER

                       1       *DEFAULT
                       2       SYSLIB
                       3       SYSTEM
                       4       SYSDIC
                       5       STRLIB
                       6       PAY1
                       7       PAY2
                       8       PAY3
                       9       PAY4
                       10      ABC1
                       11      ABC2
                       12      ABC3
                       13      ABC4

     Enter item number to display STNLIB parameters:  6_

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----   -     +    ----  ----  ----    EXIT
```

The STNLIB parameters are di splayed in the order in which they are listed in the parameter dataset. Up to 13 STNFILE statements will be displayed on each screen. PF8 m ay be used to scroll forward in the list if more than one page of data is available. PF7 may be used to scroll backward.

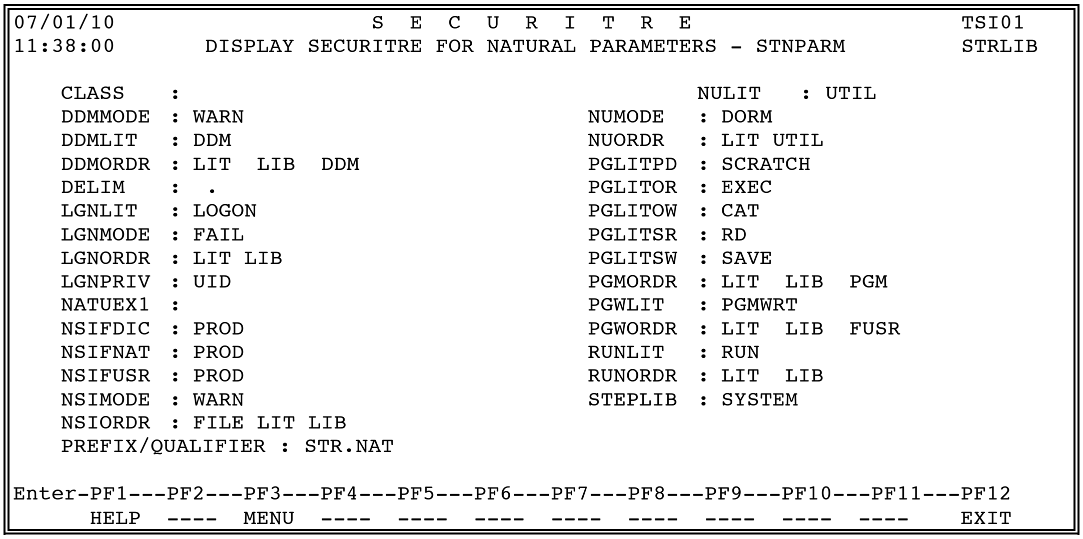
To display all the parameters for a particular STNLIB statement, enter the number of the statement at the prompt on the bottom of the screen, and press ENTER. The following screen will be displayed:



```
07/01/10                  S  E  C  U  R  I  T  R  E                    TSI01
11:38:00      DISPLAY SECURITRE FOR NATURAL PARAMETERS - STNLIB      STRLIB


          LIBRARY : SYSLIB     FUSER :

   ERRORTA  :                           STARTUP  :
   LGNPRMS  :                           STEPLIB  :
   LT       :  0                        STEP1    :  PAY2
   MT       :  0                        STEP2    :  PAY3
   MADIO    :  0                        STEP3    :  PAY4
   MAXCL    :  0                        STEP4    :
   MODE     :  REPORT                   STEP5    :
   PGMMODE  :  DORM                     STEP6    :
   PGMTYPE  :  ALL                      STEP7    :
   PGWRT    :  YES                      STEP8    :
   PGWRTCK  :  DORM                     TYPE     :  PRIV
   RDONLY   :  NO                       USRMODE  :  YES
   RUNMODE  :  DORM                     XREF     :  OFF

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

To return to the STNLIB statement list, press PF3. To return to the Main Menu from the STNLIB statement list, press PF3.

When item "P" is selected to display the STNPARM parameters, the following screen is displayed:

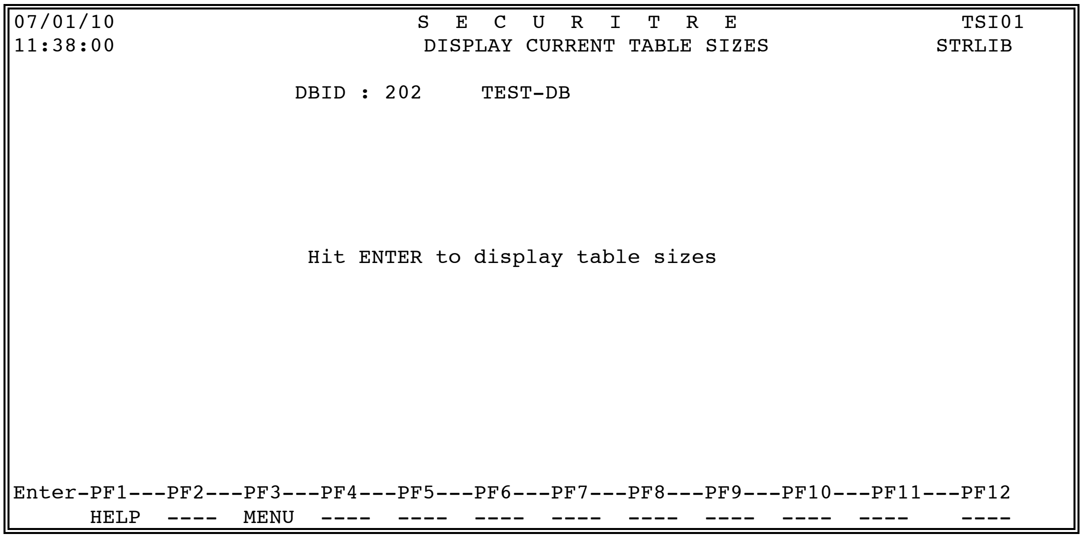


```
07/01/10                   S  E  C  U  R  I  T  R  E                       TSI01
11:38:00       DISPLAY SECURITRE FOR NATURAL PARAMETERS - STNPARM         STRLIB

    CLASS    :                                    NULIT    : UTIL
    DDMMODE  : WARN                       NUMODE   : DORM
    DDMLIT   : DDM                        NUORDR   : LIT UTIL
    DDMORDR  : LIT  LIB  DDM              PGLITPD  : SCRATCH
    DELIM    :  .                         PGLITOR  : EXEC
    LGNLIT   : LOGON                      PGLITOW  : CAT
    LGNMODE  : FAIL                       PGLITSR  : RD
    LGNORDR  : LIT LIB                    PGLITSW  : SAVE
    LGNPRIV  : UID                        PGMORDR  : LIT  LIB  PGM
    NATUEX1  :                            PGWLIT   : PGMWRT
    NSIFDIC  : PROD                       PGWORDR  : LIT  LIB  FUSR
    NSIFNAT  : PROD                       RUNLIT   : RUN
    NSIFUSR  : PROD                       RUNORDR  : LIT  LIB
    NSIMODE  : WARN                       STEPLIB  : SYSTEM
    NSIORDR  : FILE LIT LIB
    PREFIX/QUALIFIER : STR.NAT

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----  ----    EXIT
```

V.5.8 Display Current Table Sizes

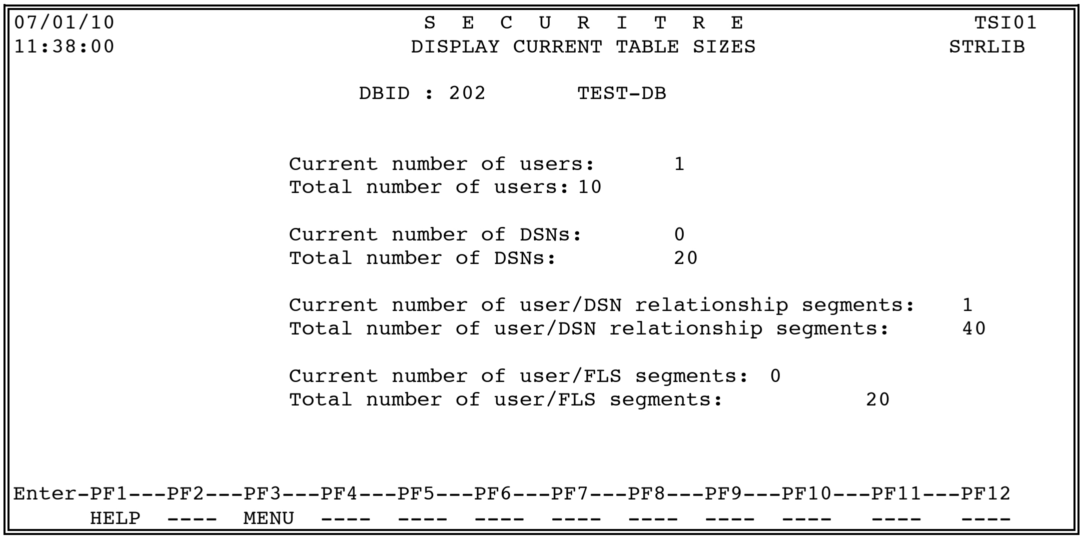
The Security Administrator may want to display the table sizes allocated by the STRDEF parameters for a database. The table size can be displayed for the User, DSN, User-to-DSN relationship, and Field Level Security tables.

In order to display the table sizes in effect for database 202, the Security Administrator would enter "202" in the DBID field on the following screen:



```
07/01/10                       S  E  C  U  R  I  T  R  E                 TSI01
11:38:00                        DISPLAY CURRENT TABLE SIZES            STRLIB

                      DBID : 202     TEST-DB







                       Hit ENTER to display table sizes









Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----  ----    ----
```

Once ENTER is pressed, the table sizes allocated for database 202 are displayed as shown on the following screen:

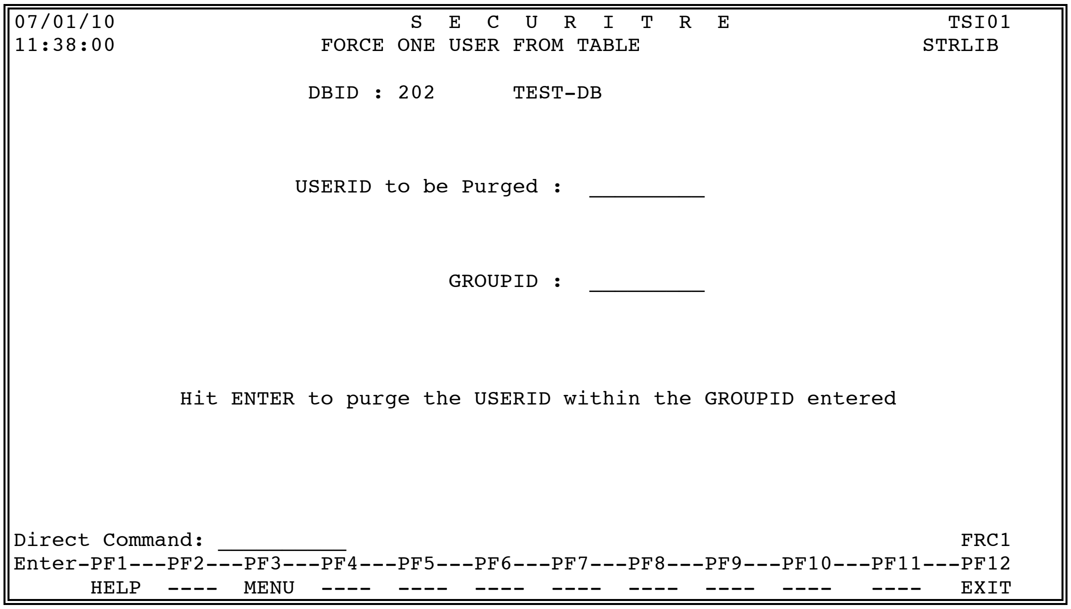


```
07/01/10                        S  E  C  U  R  I  T  R  E                 TSI01
11:38:00                       DISPLAY CURRENT TABLE SIZES               STRLIB

                           DBID : 202       TEST-DB


                      Current number of users:      1
                      Total number of users: 10

                      Current number of DSNs:       0
                      Total number of DSNs:         20

                      Current number of user/DSN relationship segments:   1
                      Total number of user/DSN relationship segments:     40

                      Current number of user/FLS segments:  0
                      Total number of user/FLS segments:           20



Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   ----
```

The display includes the current and maximum table sizes. For instance, in the example above, the User Table has space for 10 users, but there is currently only 1 user in the table.

V.5.9 **Help Screens**

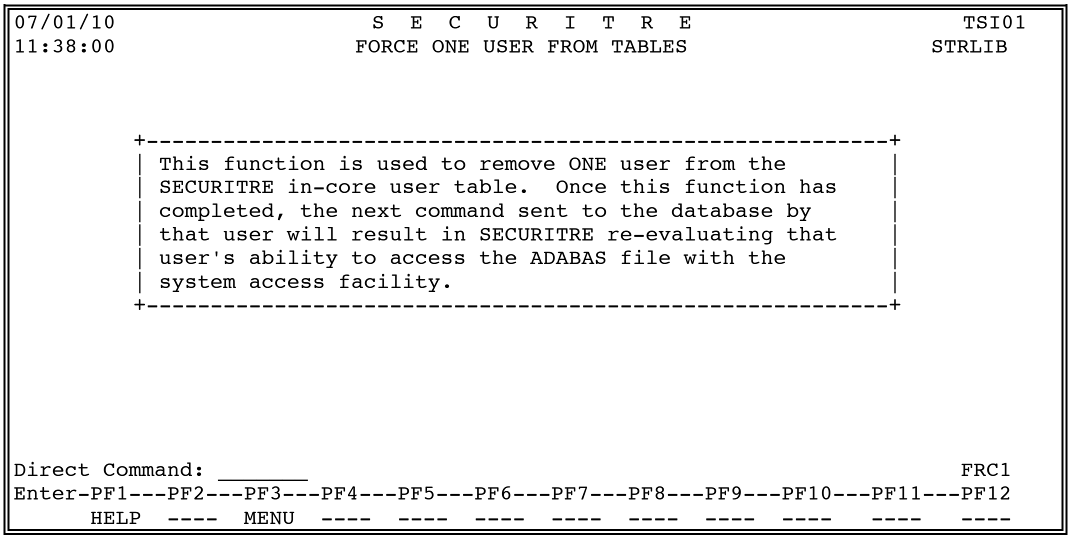
SECURITRE includes help screens for all RTM functions. These are viewed by navigating to the appropriate screen and pressing the PF1 key. For instance, to view the help screen for the "Force One User From the Tables" function, the Security Administrator would either enter "FRC1" or press "A" on the Main Menu. The following screen is displayed:



```
07/01/10                       S E C U R I T R E                      TSI01
11:38:00                    FORCE ONE USER FROM TABLE                STRLIB

                           DBID : 202      TEST-DB


                          USERID to be Purged :  _________


                                      GROUPID :  _________



                 Hit ENTER to purge the USERID within the GROUPID entered




Direct Command: __________                                             FRC1
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   EXIT
```

If there is some question as to the meaning of this "FRC1" function, the user may press PF1 to invoke the SECURITRE HELP screen.

To get help for this function, the Security Administrator would press PF1. The following help screen is displayed if PF1 is pressed while on the "FRC1" screen:



```
07/01/10                    S E C U R I T R E                          TSI01
11:38:00                       FORCE ONE USER FROM TABLES             STRLIB


         +-----------------------------------------------------------+
         | This function is used to remove ONE user from the         |
         | SECURITRE in-core user table.  Once this function has     |
         | completed, the next command sent to the database by       |
         | that user will result in SECURITRE re-evaluating that     |
         | user's ability to access the ADABAS file with the         |
         | system access facility.                                   |
         +-----------------------------------------------------------+






Direct Command: _______                                                FRC1
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12
      HELP  ----  MENU  ----  ----  ----  ----  ----  ----  ----   ----   ----
```

By pressing ENTER, SECURITRE will return to the previously displayed screen.

This page intentionally left blank.

SECTION VI

INTERNAL APPLICATION SECURITY FEATURES (STRNAT AND STRASM)

VI.1 STRNAT Calling Parameters

A description of the function of STRNAT and an example of STRNAT usage are presented in ***Section VII - Internal Application Security Features (STRNAT and STRASM)*** in the ***Administrator Guide***.

The calling parameters for the STRNAT interface are illustrated in the following NATURAL DEFINE DATA code:

```
DEFINE DATA
      LOCAL
      01   ENTITY                    (A44)          /* DSN TO BE CHECKED
      01   ACCESS-TYPE               (A1)           /* R=READ, U=UPDATE
      01   SSF-CLASS                 (A8)           /* VALID SSF CLASS
      01   ACCESS-ALLOWED            (L)            /* ACCESS ALLOWED
      01   COMMUNICATION-OK          (L)            /* DATABASE ACTIVE
      01   OTHER                     (A50)          /* OTHER PARAMETERS
      01   REDEFINE OTHER
           02  MESSAGE               (A25)
           02  LOG-VIOL              (A1)
```

The calling sequence for STRNAT is:

```
CALLNAT 'STRNAT' USING
   ENTITY
   ACCESS-TYPE
   SSF-CLASS
   ACCESS-ALLOWED
   COMMUNICATION-OK
   OTHER
```

VI.2 STRASM Calling Parameters

A description of the function of STRASM and an example of STRASM usage are presented in ***Section VII - Internal Application Security Features (STRNAT and STRASM)*** in the ***Administrator Guide***.

The calling parameters for the STRASM interface are illustrated in the following COBOL code:

```
01   ENTITY                    PIC X(44).
01   ACCESS-TYPE               PIC X.
01   SSF-CLASS                 PIC X(8).
01   ACCESS-ALLOWED            PIC X.
01   COMMUNICATION-OK          PIC X.
01   OTHER.
     02  MESSAGE               PIC X(25).
     02  LOG-VIOL              PIC X.

 ENTITY                        DSN TO BE CHECKED
 ACCESS-TYPE                   R=READ, U=UPDATE
 SSF-CLASS                     VALID SSF CLASS
 ACCESS-ALLOWED                ACCESS ALLOWED   ('Y' or 'N')
 COMMUNICATION-OK              DATABASE ACTIVE  ('Y' or 'N')
 OTHER                         ERROR MESSAGE, LOG VIOLATION
                               INDICATOR ('Y' OR 'N')
```

The calling sequence for STRASM is:

```
CALL 'STRASM' USING ENTITY, ACCESS-TYPE, SSF-CLASS,
     ACCESS-ALLOWED, COMMUNICATION-OK, OTHER.
```

Treehouse
SOFTWARE

2605 Nicholson Road, Suite 1230
Sewickley, PA 15143

Phone: (724) 759-7070
Fax: (724) 759-7067

Email: tsi@treehouse.com
Web site: www.treehouse.com