CA Top Secret® for z/OS

Report and Tracking Guide

r15

Ninth Edition

CA Technologies Product References

This documentation set references the following CA products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Common Services for z/OS (CA Common Services)
- CA Distributed Security Integration Server for z/OS (CA DSI Server)
- CA LDAP Server for z/OS (CA LDAP Server)
- CA Top Secret® for z/OS (CA Top Secret)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- TSSUTIL Report Selection Criteria (see page 27)—Added a description for new option TERSE, which bypasses the process of populating the Department, Division, and Zone columns with ACID names. This process avoids additional I/O processing and helps shorten the report running time.

The following documentation updates were made in the previous release of this documentation:

- How to Generate Sample Report 1 (Inactive ACIDs) (see page 154)—Presented steps for how to generate the report; modified the maximum value for INACTIVE option in the report.

The following documentation updates were made in a previous release of this documentation:

- NOECHO Selection Criteria Option—Suppress Echoed Input (see page 40)—Added this section to describe a new TSSUTIL report formatting option that suppresses echoed input parameter content.
- NOTITLE Selection Criteria Option—Suppress All Title Lines and Pagination (see page 41)—Added this section to describe a new TSSUTIL report formatting option that suppresses all title lines and pagination in the main body of the TSSUTIL report and suppresses the legend that normally follows the report.
- ONETITLE Selection Criteria Option—Use One Full Title Block (see page 41)—Added this section to describe new TSSUTIL report formatting option that prints one full title block at the beginning of the TSSUTIL report and suppresses all later pagination and title blocks.
- Sample TSSAUDIT Listing of Changes (see page 123)
  - Added CMDE to the list of values for the TYPE category of displayed information. CMDE indicates the issuance of a TSS command with a type 71 RACF ENF signal.
  - Described how the product handles a TSS command that contains UID(?) or GID(?) and a possible RANGE specification.
- TSSCFILE Utility—Moved this chapter to the new *CA Top Secret TSSCFILE Utility Guide*.

The following changes were made in the previous release of this documentation:

- TSSCFILE Utility—Formatted Record Types—Updated information for record ID 2021.

- Output from MODIFY(STATUS(CIART))—Deleted the record ID 9753 section, which contained obsolete information.
- TSS MODIFY(STATUS(CIART))—Deleted the record ID 9753 section, which contained obsolete information.

Contents

Chapter 1: TSSUTIL Utility

This section contains the following topics:

How to Report and Archive Security-Related Activity

The TSSUTIL batch utility processes security-related activity that is recorded in SMF data sets and the CA Top Secret Audit/Tracking File. You can use TSSUTIL to perform the following activities:

- Produce reports about activity.
- Archive activity.

In a single execution of TSSUTIL, you can generate multiple different reports based on the same SMF or Audit/Tracking File input data.

To use TSSUTIL to archive and report on security-related activity:

1. Ensure that you have authority to use TSSUTIL (see page 18).
2. Configure logging options (see page 16) to ensure that relevant security information is available for archiving and reporting.
3. Assemble JCL for the TSSUTIL job. JCL includes the following components:
   - DD statements (see page 22) (if using SMF input)
   - Verbs (see page 25) (EXTRACT to archive security incidents and REPORT to report on incidents)
   - Selection criteria (see page 27) (to select types of incidents to process)
4. Submit the JCL to execute TSSUTIL.

   CA Top Secret extracts data or produces reports according to your specifications.

Using the TSSUTIL Utility

The following considerations affect the TSSUTIL utility:

- Reports are produced with events in the order found in the SMF or Audit/Tracking Files. No sorting is performed. For SMF data sets, the order is normally chronological. When the input is the CA Top Secret audit tracking file, the records are in order from the beginning of the files. If the file has wrapped or if an audit file switch has occurred, the report may not be in chronological order. Use the CA SORT or DFSORT utilities to create an input file sorted by date. For information, see the section TSSUTIL JCL.
- Report and tracking depends greatly upon the correct specification of logging options. The LOG control option lets you request the type of events to be logged, specify where logging information is recorded, and choose where violation notification is to be made.
- The following logging options are required to record the related security information for later reporting via TSSUTIL:

  ```
  LOG(INIT,...) requests logging of all job/session initiations and terminations.
  LOG(SMF,...) requests SMF recording of selected events.
  LOG(ACCESS,...)
  requests logging of all resource access.
  ```
- Logging options can be set globally by the LOG control option or by facility using the LOG suboption of the FACILITY control option.
- Security violations are always reported in the EVENT(AUDIT) report. To obtain audited events other than security violations, you must run the EVENT(AUDIT) report and have events being audited for resources or user activity via one of the following:

  ```
  TSS ADDTO(acid) AUDIT
  TSS PERMIT(acid) resclass(resource) ACTION(AUDIT)
  TSS ADDTO(AUDIT) resclass(resourcename)
  TSS MODIFY FACILITY(facilityname=AUDIT)
  ```
- The Audit/Tracking Files should be backed up using the TSSARCHI job provided in CAI.CAKOJCL0. This job uses the EXTRACT keyword to retrieve all the events recorded in the atf(s) and places them on tape using the DCB attributes RECFM=VB and LRECL=465.
- The EXTRACT function will produce either the SMFOUT, XTROUT file, or both depending on the situation. See the explanation of the EXTRACT keyword for a description of these files.

- For z/OS 1.9 and above, SMF data may be sent to the LOGGER services controlling the write of SMF data in LOGSTREAM structures. SMF data will not be recorded in the usual SYS1.MANx data sets. The TSSRPTST utility is able to read the data when:
  - The LOGR services are active on the system with the definitions that contains the SMF data.
  - A LOGR subsystem is active on the system
  - An IEFSSNxx member is defined and activated at IPL time with the definition:

    ```
    SUBSYS SUBNAME(LOGR) INITRTN(IXGSSINT)
    ```

  The RECxxxxx DD used to read the data has the format:

  ```
  //RECxxxxx DD  DSN=IFASMF.DATA.LOGSTRM,DISP=SHR,
  //          SUBSYS=(LOGR,IFASEXIT,subsys-options1,subsys-options2)
  ```

  Description of SUBSYS options-1 includes:

  ```
  [FROM={({[yyyy/ddd][,hh:mm[:ss]]}) | OLDEST}]
  [TO={({[yyyy/ddd][,hh:mm[:ss]]}) | YOUNGEST}]
   [,DURATION=(nnnn,HOURS)]
   [,VIEW={ACTIVE|ALL|INACTIVE}]
   [,GMT|LOCAL]
  ```

  The subsys-options1 parameters used by the IBM IFASEXIT are the same as those used by the IFBSEXIT. For information on the parameters for IFBSEXIT, see IBM's *MVS Diagnosis: Tools and Service Aids*.

Authority and Scope

To use TSSUTIL, an ACID must possess REPORT authority. This administrative authority might be given by anyone who has REPORT authority by entering the following command.

```
TSS ADMIN(acid) ACID(REPORT)
                RESOURCES(REPORT)
```

A user with no administrative authority may use TSSUTIL if given USE access to entity “TSSUTILITY.TSSUTIL” in the CASECAUT resource class. This access may be granted by an administrator using the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSUTIL) ACCESS(USE)
```

You can only extract those incidents that are generated for ACIDs within the scope of your authority. The scopes are as follows:

SCA

Every event

LSCA

Every event within the LSCAs scope

ZCA

Entire zone or specific divisions, departments or ACIDs within the zone

VCA

Entire division or specific departments or ACIDs within the division

DCA

Entire department or specific ACIDs within the department

USER

Himself

Note: When using EVENT(VIOL) or EVENT(AUDIT) VCAs and DCAs are allowed to view VIOL and AUDIT events for owned resources even if the subject acid is not within their scope. VCAs using EVENT (VIOL|AUDIT) and specifying a department will get resources within that department's scope. For more details about EVENT, see TSSUTIL Report Selection Criteria.

TSSUTIL JCL

TSSUTIL works against sequential SMF data or the Audit/Tracking File. We suggest that you select the Audit/Tracking File instead of SMF data. While SMF requires one or more pre-processing "dump" steps, the Audit/Tracking File is a direct-access file providing immediate access. The Audit/Tracking File also allows use of TSSTRACK to monitor security events online (in real-time), which SMF data does not. JCL for using TSSUTIL in batch is outlined below.

JCL for TSSUTIL Using TSS AUDIT File Input

```
//REPORT         JOB
//REPORT         EXEC          PGM=TSSUTIL
//*
//*                            INPUT SMF OR AUDIT/TRACKING FILE
//*
//SMFIN          DD            DSN=name.of.atf,DISP=SHR
//SMFIN1         DD            DSN=name.of.atf2,DISP=SHR] optional
//*
//*                            REPORT OUTPUT
//*
//UTILOUT        DD            SYSOUT=*
//*
//*                            SELECTION CRITERIA
//*
//UTILIN         DD            *
  options
/*
//SYSPRINT       DD            SYSOUT=*
//SYSUDUMP       DD            SYSOUT=*
//*
//*                            OPTIONAL DD STATEMENTS
//*
//SMFOUT           DD                DSN=name.of.abstract.dataset,
//                                   DISP=(,CATLG,DELETE),
//                                   VOL=SER=volser,SPACE=(space-values),
//
DCB=(LRECL=465,BLKSIZE=file-blocksize,RECFM=VB)
//XTROUT           DD                DSN=name.of.abstract.dataset,
//                                   DISP=(,CATLG,DELETE),
//                                   VOL=SER=volser,SPACE=(space-values),
//                                   DCB=(LRECL=27994,BLKSIZE=27998,RECFM=VB)
//EARLOUT        DD            DSN=output-file-name,UNIT=unit-name,
                               DISP=(NEW,KEEP),
//                             VOL=SER=volser,SPACE=(space-values),
//                             DCB=BLKSIZE=file-blocksize
```

JCL for Wrapped or Switched Audit File

If the audit file is switched or wrapped, use the following JCL to produce a report sorted by date:

```
//MASTERU  JOB  (118300000),'MASTER UTIL',CLASS=A,MSGCLASS=X,
//  NOTIFY=MASTER,TIME=1440
//*
//*  STEP 1
//*
//UTIL     EXEC PGM=TSSUTIL,REGION=2M
//UTILOUT  DD  SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SMFIN        DD    DISP=SHR,DSN=USER.TEST.AUDIT
//SMFIN1       DD    DISP=SHR,DSN=USER.TEST.AUDIT2
//SMFOUT   DD DSN=USER.TEST.EXTRACT.AUDIT,
//    SPACE=(TRK,(15,1),RLSE),DCB=(RECFM=VB,LRECL=465,BLKSIZE=11160),
//    UNIT=SYSDA,VOL=SER=XXXXXX, DISP=(NEW,CATLG,DELETE)
//UTILIN   DD  *
 EXTRACT EVENT(ALL) END
//*
//*  STEP 2
//*
//JS10     EXEC PGM=SORT
//SYSOUT   DD  SYSOUT=*
//SORTIN       DD    DISP=SHR,DSN=USER.TEST.EXTRACT.AUDIT
//SORTOUT  DD DSN=USER.TEST.AUDIT.SORTED,
//    SPACE=(TRK,(15,1),RLSE),DCB=(RECFM=VB,LRECL=465,BLKSIZE=11160),
//    UNIT=SYSDA,VOL=SER=XXXXXX,DISP=(NEW,CATLG,DELETE)
//SYSIN    DD  *
        SORT FIELDS=(92,3,PD,A,96,4,CH,A)
//*
//*  STEP 3
//*
//UTIL     EXEC PGM=TSSUTIL,REGION=2M
//UTILOUT  DD  SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SMFIN        DD    DISP=SHR,DSN=USER.TEST.AUDIT.SORTED
//UTILIN   DD  *
 REPORT EVENT(ALL) END
//
```

Step 1 extracts the audit records from two audit files to create a single audit file. Step 2 sorts the single audit file by date and time. Step 3 uses the sorted file as input for the TSSUTIL report run.

JCL for TSSUTIL Using SMF Input

```
//REPORT        JOB
//********      dump              vsam type-80 data first
//MAN           EXEC              PGM=IFASMFDP
//DUMPIN        DD                DSN=SYS1.MANX,DISP=SHR
//SMFOUT        DD                DSN=&&SMF.,DISP=(,PASS),
//                                SPACE=(CYL,10),UNIT=disk
//SYSPRINT      DD                SYSOUT=*
//SYSIN         DD                *
    LSNAME(IFASMF.XE15.TSSLOG)
    OUTDD(SMFOUT,TYPE(80))
/*
//MANY          EXEC PGM=IFASMFDP
//DUMPIN        DD                DSN=SYS1.MANY,DISP=SHR
//SMFOUT        DD                DSN=&&SMF.,DISP=(MOD,PASS)
//SYSPRINT      DD                SYSOUT=*
//SYSIN         DD *
    INDD(DUMPIN,OPTIONS(DUMP))
    OUTDD(SMFOUT,TYPE(80))
/*
//REPORT        EXEC              PGM=TSSUTIL,PARM='options list'
//UTILOUT       DD                SYSOUT=*
//SMFIN         DD                DSN=&&SMF.,DISP=OLD,DCB=(BFTEK=A)
[//SMFIN1       DD                DSN=&&SMF.,DISP=OLD,DCB=(BFTEK=A)]
                                  optional
[//SMFOUT      DD                DSN=extract.smf.data set,DISP=SHR]
                                  optional
[//XTROUT        DD                    DSN=extract.smf.data set,DISP=SHR]
                                       optional
//UTIILIN       DD *
   options...
/*
```

TSSUTIL DD Statements

SMFIN

Defines an input data set to TSSUTIL. SMFIN can represent any of the following:

- An Audit/Tracking file as illustrated by the first JCL example.
- An SMFOUT EXTRACT file.
- A backup copy of the SMF data from tape.

Notes:

- SMF extract files can be concatenated.
- TSS AUDIT files can be concatenated.
- SMF and AUDIT files should not be mixed in the same execution of TSSUTIL.
- When SMF files are used for SMFIN, DCB=BFTEK=A is required.

SMFIN1

Defines an additional DD statement for SMF or AUDIT file input to the utility. If the data in SMFIN is SMF (or AUDIT, respectively), SMFIN1 is expected to be the same type of data. When SMF files are used for SMFIN1, DCB=BFTEK=A is required.

SMFOUT

Defines an output data set used only for EXTRACT. It is an optional DD statement, and the data set characteristics must be RECFM=VB, LRECL=465.

UTILIN

Defines input containing selection criteria options. These options can also be specified in the 'options list' of the PARM field in the EXEC statement. EXEC parameters override UTILIN options; in fact, UTILIN is ignored when EXEC parameters are coded.

UTILOUT

Defines an output data set for the formatted report of security incidents based on selection criteria. If UTILOUT is being routed to a PDS, the PDS must be defined with LRECL=133. If you are running at or above genlevel 9301, the blocksize can be a multiple of 133, TSSUTIL will honor what is coded in the UTILOUT DD statement. If you are running below genlevel 9301, the BLKSIZE is hardcoded as 2660 and any other valued specified in the UTILOUT DD statement is ignored. Also, be sure to include a member name with the data set.

For sequential data sets, if you create a new data set (DISP=NEW), TSSUTIL makes LRECL=133 regardless of what you specify in the DCB information on the UTILOUT DD statement. The blocksize will default to 23408 unless you override it in the DCB information on the UTILOUT DD statement.

To route the output to an existing sequential data set, it must have LRECL=133 and the blocksize must be a multiple of 133 (if at or above genlevel 9301), otherwise, an SO13 abend will occur.

EARLOUT

Generates Easy Access Report Language CA-Earl®) formatted record types that can be used as input to produce customized reports.

- output-file-name-The data set name of the file.
- unit-name-Assigns the I/O device for the output media. Any output media compatible with the sequential access method (such as tape or disk) can be used.
- volser-The volume serial number of the volume on which the file will reside.
- space-values-If a disk device is chosen for output, assign disk for the output file. Omit this parameter if a tape device if used.
- file-blocksize-Choose a blocksize to make the most efficient use of the output media chosen. The value chosen must be an integral multiple of 456, the file record length.

XTROUT

Defines an output data set used only for EXTRACT. It is an optional DD statement and the data set characteristics must be as follows: RECFM=VB,LRECL=27994,BLKSIZE=27998. This DD statement may be required if the site is using OPTIONS(32) to write USS records to the audit tracking file. In that case, some output records may exceed the defined LRECL of 465 for the SMFOUT file.

Notes:

- IFASMFDP (the SMF DUMP program) is used to convert VSAMSMF files to a sequential SMF data set.
- TSSUTIL cannot execute if the TSS address space is not active.
- If you are using VBS format SMF data, and DCB=BFTEK=A is not coded, you might get a system 0C4 abend.

Formatted Record Types

The following formatted record types give the offsets and full lengths for each record that can be used to generate CA Earl reports from TSSUTIL output.

```
 3    7     5       DATE (PACKED YYDDDF)
 8    13    6       TIME OF DAY (HHMMSS)
 14   21    8       ACID NAME
 22   29    8       DEPARTMENT NAME
 30   37    8       DIVISION NAME
 38   45    8       ZONE NAME
 46   53    8       JOB NAME
 54   61    8       TERMINAL ID
 62   62    1       TYPE (S=STC,J=JOB,....)
 63   69    7       JOB NUMBER
 70   77    8       FACILITY NAME
 78   81    4       USER'S MODE
 82   83    2       RETURN CODE
 84   86    3       DETAIL REASON CODE
 87   94    8       AUDIT INDICATOR
 95   102   8       BYPASS INDICATOR
103   110   8       SUSPENSION INDICATOR
111   114   4       SYSID
115   130   16      SPARE
                    START OF VARIABLE DATA

ID:         "IN     ="  USER INITIATION
131   162   32          NAME OF USER

ID:         "RE OR DS  ="  RESOURCE VALIDATION
131   138   8       RESOURCE CLASS
139   146   8       REQUESTED ACCESS1
147   154   8       REQUESTED ACCESS2
155   162   8       REQUESTED ACCESS3
163   170   8       ALLOWED ACCESS1
171   178   8       ALLOWED ACCESS2
179   186   8       ALLOWED ACCESS3
187   194   8       PROGRAM IN CONTROL
195   197   3       CALLING SVC IN DECIMAL

ID:         "RE     ="  RESOURCE VALIDATION (NON-DATASET)
201   456   256         RESOURCE NAME

ID:         "DS     ="  RESOURCE VALIDATION (DATASET)
201   244   44          DATASET NAME
245   250   6           VOLUME SERIAL

ID:         "MD     ="  PARAMETER FILE/MODIFY OPTIONS
131   386   256         PARM/MODIFY OPTION
```

```
ID:        “LG      =“  INSTALLATION LOGGING
131   174   44           INSTALLATION DEFINED
ID:        "TR      ="  USER TERMINATION
131   162   32           NAME OF USER
```

For record id types RE and DS, the requested/allowed access level fields will contain the character equivalent of the hex representation for the access level. If more than one access level is represented by the hex value, starting with the highest level, the requested/allowed access level fields will all be filled in starting with field REQUESTED/ALLOWED ACCESS LEVEL1.

TSSUTIL Verbs

Begin a control statement with a verb that indicates whether to create reports or extract data for archival. Control statements can span multiple lines.

If a control statement spans multiple lines, you can specify +,-, or * characters between options, which allows you to embed in-line comments or provide a visual indication of places where JCL statements occupy more than one line. TSSUTIL ignores any content from the specified character through the end of a current line.

Important! You cannot specify the characters in the middle of parameter lists that span multiple lines.

You can specify the following TSSUTIL verbs:

REPORT *option*,*option*,…

Produces a formatted report of security incidents based on specified selection criteria options (one line per event or two lines per event if you specify LONG).

EXTRACT *option*,*option*,…

Selects records (based on specified selection criteria options) and archives the records to the SMFOUT file, the XTROUT file, or both for later processing.

A report of selected records is also produced (if the LIST control option has been specified). Any audit record that exceeds LRECL=465 is truncated (triggering an RC=04).

If you extract to both SMFOUT and XTROUT files, long records are truncated in the SMFOUT file but are written in their entirety in the XTROUT file.

END

Separates multiple reports by indicating the end of a selection request. Additional REPORT or EXTRACT requests might follow.

Important! You cannot specify a +, -, or * character (or any comments) after the END verb.

Note: If both REPORT and EXTRACT are omitted, REPORT is assumed.

Example: Embed Comments Between Control Statement Options

This example shows how to use the - character to include comments between control statement options:

```
REPORT DATE(TODAY) - Report only today's events
       EVENT(VIOL) - Report only violations
       LONG - Report is to be produced in long format
END
```

The comments enable the administrator to provide notes about reporting activity. TSSUTIL ignores the content from the specified character (-) through the end of each line.

Example: Include a Visual Indication of a Multiple-Line JCL Statement

This example specifies the following REPORT statement:

```
REPORT EVENT(VIOL) DATE(-14,-00) TIME(080000,160000)       -
DEPARTMENT(DEPT1,DEPT2,DEPT3) RES('SAMPRES') LONG END
REPORT EVENT(ACCESS) DATE(-14,-00) RES('SAMPRES') END
```

The specified statement produces reports about the following activity:

- All security violations against SAMPRES that occurred during the last 14 days, between 8 a.m. and 4 p.m., by all users in departments DEPT1, DEPT2, and DEPT3.
- All access attempts against SAMPRES in the last 14 days.

The first line of the statement uses a character (-) as a visual indicator that the statement spans multiple lines.

More information:

TSSUTIL Report Selection Criteria (see page 27)

TSSUTIL Report Selection Criteria

Selection criteria options determine the types of incidents to process. You can specify any option, but each option can be specified only once. For example, the following specification is valid:

```
DEPARTMENT(XYZ,ABC)
```

The following specification is *not* valid:

```
DEPARTMENT(XYZ) DEPARTMENT(ABC)
```

To be valid for processing, all selection criteria must be met within each SMF or Audit/Tracking File record.

Note: Abbreviated forms, if any, appear under the full names of the selection criteria in the boxed areas.

Every selection criteria option that has a parameter list can span multiple lines; however, the following restrictions apply:

- Although you can split the parameter list across lines, you *cannot* split a parameter across lines (except for the RESOURCE option).

  Example: The following RESOURCE option specification splits a parameter across lines and is valid:

  ```
  RESOURCE(SAMPLE.RESOURCE.NAME.THAT.IS.LONG.ENOUGH.SUCH.THAT.IT.
  SPANS.MULTIPLE.LINES,
  ABC)
  ```

  Example: The following DEPARTMENT option specification attempts to split a parameter across lines and is *not* valid:

  ```
  DEPARTMENT(XY
  Z,ABC)
  ```

  Example: The following DEPARTMENT option specification splits the parameter list across lines and is valid:

  ```
  DEPARTMENT(XYZ,
  ABC)
  ```

- A continuation character (+,-,*) cannot appear inside parameter lists unless the character is a valid character for the entity name or the prefix indicator.

The list of selection criteria is as follows:

- ACCESS
- ACCESSOR

- CLASS
- DATASET
- DATE
- DEPARTMENT
- DIVISION
- DRC
- EVENT
- EXCLACID
- EXCLJOB
- FACILITY
- HISTORY
- JOBID
- JOBNAME
- LINECNT
- LIST
- LONG
- MODE
- NOLEGEND
- PROGRAM
- RESCLASS
- RESOURCE
- SYSID
- TERSE
- TERMINAL
- TERSE
- TIME
- TITLE
- UNDEF
- VOLUME
- ZONE

More information:

TSSUTIL Verbs (see page 25)

ACCESS

Selects a level of access to data set, volume, CICS, UR1, UR2, and FIELD requests. Only those incidents whose access matches the requested access level is selected. A maximum of eight levels can be specified.

```
ACCESS(level,level,...,(resclass))
```

level

Used to select incidents with matching requested access level.

resclass|dataset

Access level names given are defined in the RDT for the resource class name given. If resource class is not given, DATASET is used as the default. Specifying a resource class name is optional.

ACCESSOR

Selects records produced by jobs or sessions running under a specific ACID. A maximum of eight ACIDs can be specified.

```
ACCESSOR(acid,acid*,*,...)
ACID
A
```

acid

A specific ACID name. If you specify more than one, separate them with commas.

acid*

An ACID prefix. All ACIDs that begin with the given prefix is selected.

Selects undefined ACIDs including *MISSING*, *UNDEF*, and *BYPASS*.

ACID(*) might only be used by an SCA.

CLASS

Selects records that refer to a specific resource class.

CLASS(*type*)

Replace *type* with one of the following single-character codes:

a CA-IDMS SUBSCHEM.

b AllFusion™ CA-IDMS® AREA

c Adabas database

d IMS DBD

e JESINPUT

f IBM Facility

g TSO account number

h TSO authority

i TSO procedure name

j TSO performance group

k VAX file

I VAX device

m VM IUCV

n VM VMCF

o TSAF

p JESPOOL

q JESJOBS

r OPERCMDS

s CICS CEMT SPI

t DEVICES (for VTAM 3.2)

u CA REPORT

v CA TAPE

w SMESSAGE (TSO/E)

x VTAMAPPL (VTAM 3.2)

y CAADMIN

z CAVAPPL

' SYSCONS

A Application

B Audited job submission

C Mode by user

D Data set

E CICS DCT

F CICS FCT

G Authentication call

H TOTAL file

I ACID xe03type

J CICS JCT

K Terminal unlock

L Terminal lock

M UR1

N UR2

O TSS control options

P Program

Q CICS PPT

R Database field

S DL/1 PST

T Terminal

U Abstract

V Tape volume

W DASD volume

X Transaction

Y USERn

Z CICS TST

1 Change propagation

2 CA jobname

3 CA panel

4 DUFXTR

5 DUFUPD

6 User logging

7 VM MDISK

8 VM CP CMD

9 VM diagnose

0 VM network

* Reserved

VM RDR

% Logging DB2 resources

$ VM DCSS

@ VM dial

+ Logging installation exit call

= CACMD

- CA Scheduler

? Extract

< Operation commands

> Owned transactions

. Data set

/ Dasdvold

´´ Tapevolt

! CA Station

& Recipid

: Reserved

¢ VMANAPPL

¦ UNVEDIT

\ UNVRPRT

~ UNVPGM

, CPU

| SDSF userclass

} VM Machine

{ IMBGROUP

` PROPCNTL

_ Librarian resource CALIBMEM

; Librarian resource CACCFMEM

¬ Librarian resource CACCFDSN

(SMS management class

) SMS storage class

Note: Class O records only display when specifically requested, and they can only be requested by the SCA and MSCA.

DATASET

Selects records that refer to any of the specified data set prefixes. A maximum of eight data set prefixes can be specified.

```
DATASET(dsnprx,...)
DSN
D
```

dsnprx

A data set prefix. All records that refer to data set(s) matching the prefix(es) are selected. If you specify more than one prefix, separate them with commas.

DATE Selection Criteria Option

Use the DATE selection criteria option to select records by using dates or date ranges. This option has the following format:

DATE(*yyddd*|*yyddd*,*yyddd*|*-nn*|*-nn*,*-nn*|TODAY)

DATE(*yyddd*|*yyddd*,*yyddd*|*-nn*|*-nn*,*-nn*|TODAY)

Selects records based on a date or range of dates. Omitting DATE lists *all* changes made from the beginning date of the recovery file.

Note: Specifying DATE and TIME concurrently displays only records that are within *both* the date range and time range.

DATE(*yyddd*[,*yyddd*])

Specifies a specific date or range of dates (in Julian format) from which to select records. Specifying only one date selects records that are produced from that date through the current date. Specifying two dates creates a range that selects records that are produced between the specified dates.

To select records that are produced on a single day, specify the same value for both *yyddd* entries.

DATE(*-nn*)

Specifies a value from -00 to -99, which subtracts the specified number of days from the current date (to create a start date). This specification produces a report that includes records from the start date through the current date.

Example: Specify DATE(-01) to use yesterday as a start date and produce a report that includes records from yesterday through today.

DATE(*-nn,-nn*)

Specifies a set of values (each value between -00 to -99) to select records that are produced on the two relative dates and produced during the time between the dates.

Example: Specify DATE(-60,-40) to select all records that were produced between 60 days ago and 40 days ago.

DATE(TODAY)

Specifies to select records from today.

DEPARTMENT

Selects one or more departments for which Security Records are selected. A maximum of eight Department ACIDs can be specified. TSSUTIL reports only on users that are in a DEPARTMENT when the audit record is created.

```
DEPARTMENT(dept,...)
```

dept

Specifies the department name.

DIVISION Selection Criteria Option

Use the DIVISION selection criteria option to select one or more divisions for which security records are selected. This option has the following format:

```
DIVISION(division,...)
```

division

Specifies the division ACID name. You can specify a maximum of eight division ACIDs.

DRC

Selects all records that are flagged with the specified error code(s).

```
DRC(code,... |IN|DS|VL|RS|PW)
```

code

Specifies a detailed error reason code in hexadecimal format: 00 through FF-up to a maximum of 32 total DRCs.

IN

Selects all initiation violation codes. 01 - 1D, 46, and 64

DS

Selects all data set violation codes. 65 - 72

VL

Selects all volume violation codes. 73 - 81

RS

Selects all resource violations. 42, 5F - 63, and 82 - 101

PW

Selects all password and OID violations. 07 - 0F

EVENT

Selects one or more of the incidents to be chosen.

```
EVENT(ALL|ACCESS,JOBS,INIT,TERM,VIOL,AUDIT,AUDTA)
```

ALL

Selects all events except TSS control options. See keyword CLASS type O for details. ALL is the default.

Note: ALL is mutually exclusive with all other options.

ACCESS

Selects resource and facility accesses.

JOBS

Selects job/session initiations and terminations.

INIT

Selects only job/session initiations.

TERM

Selects only job/session terminations.

VIOL

Selects resource and facility access and password violations.

AUDIT

Selects audited incidents.

AUDTA

Displays OK+A events and prevents OK+B events from displaying.

AUDTB

Displays OK+B events and prevents OK+A events from displaying.

Note: VIOL and AUDIT allow extended scope checking for DCAs and VCAs. A DRC of '09', '77', '01', '1B', and '1C' will always be audited with the AUDIT/AUDTA option.

EXCLJOB

Use to exclude a job record from the report output. A maximum of eight job names can be specified.

```
EXCLJOB(jobname,jobname*,…)
```

jobname

Indicates the name of the job record to exclude from the report output.

jobname*

Indicates a job name or job name prefix. All job names that start with the supplied prefix are selected.

EXCLACID

Use to exclude an ACID record from the report output. A maximum of eight acids can be specified.

```
EXCLACID(acid,acid*,…)
```

acid

Indicates the ACID record to exclude from the report output.

acid*

Indicates an acid or acid prefix. All acids that start with the supplied prefix are selected.

FACILITY

Selects records produced by jobs or sessions using one or more specific system facilities.

```
FACILITY(ALL|fac,...)
FAC
F
```

ALL

Includes all facilities. The default is ALL.

fac

A system facility defined to CA Top Secret: BATCH, STC, TSO, IMS, CICS, NCCF, CA-Roscoe®, WYLBUR, or any installation-defined facility.

HISTORY

When used with the ACID keyword, selects ACIDs that have been deleted from the Security File. For example, if ACID USER10 has been deleted, the following statement would report on the events USER10 created:

```
REPORT EVENT (ALL) ACID(USER10) HISTORY
```

```
HISTORY
```

Note: This keyword can only be used by an SCA or the MSCA.

JOBID

Selects records with specific job IDs. A maximum of eight job IDs can be specified.

```
JOBID(jobid1,jobid*,…)
```

jobid1

Specifies a job ID.

jobid*

Specifies a job ID or job ID prefix. All job IDs that start with the supplied prefix are selected.

JOBNAME

Selects records produced by specific jobs or online sessions. A maximum of eight jobnames can be specified.

```
JOBNAME(jobname, job*,...)
JOB
J
```

jobname

Specifies a jobname or online userid.

job*

Specifies a jobname or TSO userid prefix. All jobnames that start with the supplied prefix is selected.

LINECNT(nn)

Changes the default line count of 53 information lines for the report listing.

```
LINECNT(nn)
```

nn

Specifies the new line count, in the range 10 to 99.

LIST

Requests the simultaneous production of a report listing when used with the EXTRACT verb.

```
LIST
```

LONG

Requests the long format (two lines per event) of a report.

```
LONG
```

MODE

Selects all events that were recorded while the user was in the specified mode.

```
MODE(DORMANT|WARN|IMPL|FAIL)
```

NOECHO Selection Criteria Option—Suppress Echoed Input

Use the NOECHO selection criteria option to suppress echoed input parameters and the preceding title line (unless CA Top Secret detects a parameter syntax error or compatibility error). If an error is detected, CA Top Secret prints the parameter echo title, all input parameters, and all error messages in order.

"Echoed" content in the output represents a visual copy of your specified input, which allows you to quickly review the input specifications for accuracy. However, suppressing the echoed content lets you run TSSUTIL output directly into another program (without having to skip the echoed content).

This option has the following format:

```
NOECHO
```

NOLEGEND

Suppresses generation of legend at the bottom of all reports in current job execution.

```
NOLEGEND
```

NOTITLE Selection Criteria Option—Suppress All Title Lines and Pagination

Use the NOTITLE selection criteria option to suppress all title lines and pagination in the main body of the TSSUTIL report. The option also suppresses the legend that normally follows the TSSUTIL report.

Important! This option is incompatible with ONETITLE.

This option has the following format:

```
NOTITLE
```

More information:

ONETITLE Selection Criteria Option—Use One Full Title Block (see page 41)

ONETITLE Selection Criteria Option—Use One Full Title Block

Use the ONETITLE selection criteria option to print one full title block at the beginning of the TSSUTIL report and suppress all later pagination and title blocks.

Important! This option is incompatible with NOTITLE.

This option has the following format:

```
ONETITLE
```

More information:

NOTITLE Selection Criteria Option—Suppress All Title Lines and Pagination (see page 41)

PROGRAM

Selects records with specific program names. A maximum of eight program names can be specified.

```
PROGRAM(PROGRAM1,PROG*,…)
```

program1

Specifies a program name.

prog*

Specifies a program name or program name prefix. All program names that start with the supplied prefix are selected.

RESCLASS

Selects any resource class defined in the RDT.

```
RESCLASS(resource class name)
```

resource class name

Any resource that has been predefined or dynamically defined to the RDT.

RESOURCE Selection Criteria Option

Use the RESOURCE selection criteria option to select records that refer to all resource prefixes or a specific resource name. You can specify up to eight resource prefixes or specific resource names. Use commas to separate multiple prefixes or names.

Note: You can use the RESOURCE and RESCLASS options together to select a specific type of resource.

This option has the following format:

```
RESOURCE(prefix,'name',...)
```

prefix

Specifies a prefix (up to eight characters) for an online or RJE terminal, command, program, application, or user-defined resource. Specifying a prefix selects all records that refer to resources matching the prefix.

'name'

Specifies a specific resource entity name (up to 255 characters) for an online or RJE terminal, command, program, application, or user-defined resource. Specifying a name selects all records that refer to resources matching the name.

Note: You must enclose the name within single quotation marks.

Specific resource names can span multiple lines. For a long resource name, ensure that the name is enclosed in single quotation marks before starting any new name or prefix.

Important! If resource name spans multiple lines, do not exceed column 72 on a line before continuing the name on the next line. TSSUTIL ignores any content in columns 73 through 80.

SYSID

Selects records produced on a specific system or CPU. Use SYSID to select records from an SMF file in which SMF records from multiple systems have been merged.

```
SYSID(smfid)
```

smfid

The four-character SMF-id of the required system.

TERMINAL

Selects all events associated with a specific terminal or reader. This includes all events, not only initiations.

```
TERMINAL(termprx,...)
TERM
T
```

Termprx

A prefix for an online terminal or RJE reader.

New Topic (382)

(Applicable with EARLOUT option) Bypasses the process of populating the Department, Division, and Zone columns of a CA Earl report with ACID names. This process avoids the I/O processing that is associated with producing these names, which helps shorten the report running time.

TERSE

TIME Selection Criteria Option

Use the TIME selection criteria option to select records by using a specific time or a time period. This option has the following format:

TIME(*hhmmss*|*hhmmss*,*hhmmss*)

TIME(*hhmmss*[,*hhmmss*])

Selects records that are produced at a specific time or during a specific time period (up to but not including 24 hours). Specifying only one time selects the records that are produced from that time through the end of the 24-hour period. Specifying two times selects all records that are produced between those times. Omitting TIME lists all changes that are made in a 24-hour period (000000 to 235959).)

Note: Specifying DATE and TIME concurrently displays only records that are within *both* the date range and time range.

To select records that are produced at a specific time, specify the same value for both *hhmmss* entries.

Example: Specify TIME(181500,181500) to select records that are produced at 6:15 p.m.

Important! You *cannot* produce a single report that spans days. For example, to select all records produced between 6:00 p.m. yesterday and 6:00 a.m. today, you must produce multiple reports by using the following specification:

```
TIME(180000) DATE(-01,-01)
TIME(000000,060000) DATE(TODAY)
```

TITLE

Provides up to 39 characters to replace the characters “CA Top Secret“ on the report title line.

TITLE(text...)

UNDEF

Indicates whether events with undefined (*UNDEF*) or missing (*MISSING) ACIDs are selected.

```
UNDEF(INC|EXC)
```

INC

Includes undefined or missing ACID events. The default is UNDEF(INC).

EXC

Excludes undefined or missing ACID events.

VOLUME

Selects records that refer to any of the specified prefixes.

```
VOLUME(volprx,...)
VOL
V
```

volprx

A volume prefix. All records that refer to any volume matching the prefix are selected. If you specify more than one prefix, separate each of them with commas.

ZONE Selection Criteria Option

Use the ZONE selection criteria option to select one or more zones for which security records are selected. This option has the following format:

```
ZONE(zone,...)
```

zone

Specifies the zone ACID name. You can specify a maximum of eight zone ACIDs.

TSSUTIL Selection Criteria Examples

Example: Produce Two Reports without Legends

This example produces two reports without legends: the first, a total violation report; the second, audit entries

```
NOLEGEND
REPORT EVENT(VIOL) END
REPORT EVENT(AUDIT) END
```

Example: Select all TSO Data Set Violations from Yesterday and Today

This example selects all TSO data set violations that occurred yesterday and today:

```
DATE(-01) DRC(DS) FACILITY(TSO)
```

Example: Select All Events Logged on a Specific Date for Specific Jobs

This example selects all events logged on April 26, 1999 for jobs FINBUD01 and FINBUD02:

```
J(FINBUD01,FINBUD02) DATE(99426,99426) EVENT(ALL)
```

Example: Select all Violations in a Department

This example selects all violations by all users in the Finance Department (If submitted by a VCA or DCA, violations against all resources owned in the Finance Department as well as by users in the Finance Department):

```
DEPARTMENT(FINANCE) EVENT(VIOL)
```

Select all Violations Against volumes with Specific Prefixes

This example selects all violations against volumes with the prefix WORK by users B1010, B1020, B1030:

```
A(B1010,B1020,B1030) V(WORK) EVENT(VIOL)
```

Example: Select All Jobs Submitted from a Specific Terminal

This example selects all jobs submitted from terminal R15.RD1:

```
RES(R15.RD1) RESCLASS(TERMINAL) EVENT(INIT)
```

Example: Select All Updates Against a Data Set from a Specific CPU

This example selects all updates against SYS1.SPFPARMS from the CPU SYS3:

```
SYSID(SYS3) EVENT(ACCESS) DSNAME(SYS1.SPFPARMS) ACCESS(UPDATE)
```

Example: Select All Test CICS Transactions with Violations, with Two Lines Per Incident

This example selects all test CICS transactions with violations so that the report generates two lines per security incident:

```
RESCLASS(OTRAN) FACILITY(CICSTEST) EVENT(VIOL) LONG
```

Example: Select Illegal Access Attempts for a Specific Time Period

This example selects illegal CPU SYS2 access attempts for the second shift:

```
EVENT(VIOL) RES(CPU.SYS2) TIME(160000,235959)
```

Example: Select All IMS Production Signon Password Violations

This example selects all IMS production sign-on password violations:

```
DRC(PW) F(IMSPROD)
```

Example: Select all Undefined Batch Jobs

This example selects all batch jobs that are undefined:

```
FACILITY(BATCH) ACID(*)
```

Example: Select All Operator Authentication Failures

This example select all operator authentication failures:

```
EVENT(ALL) JOB(PROD*)
```

Example: Select Violations Against Payroll Files

This example selects CICS production and test violations against payroll files:

```
EVENT(VIOL) RES(PAY) FACILITY(CICSPROD,CICSTEST)
```

Example: Select All Unsuccessful Terminal Unlocks

This example selects all unsuccessful terminal unlocks:

```
RESCLASS(TERMINAL)
```

Example: Select Specific Audited Terminals

This example selects specific audited terminals:

```
EVENT(AUDIT) TERMINAL(188,189,18A)
```

Example: Select All Uses of Selected System Utilities

This example selects all uses of selected system utilities:

```
EVENT(ALL) RES(IMASPZAP,IEHPROGM,IEHINITT)
```

TSSUTIL Report Description

If the REPORT option is used, the TSSUTIL report function produces a fixed-format report whose content is determined by the selection criteria. One report line is generated for each security incident unless the LONG selection criterion, which generates two report lines, is used. A final summary shows retrieval statistics, and if NOLEGEND is not specified, two legends are produced at the end of each report to describe the various areas and codes.

The title line of each report page indicates the sequence number of the report being produced, as several reports can be produced with one run of the utility. A subtitle, controlled by the TITLE option, can be used to identify different reports or to provide a company or department name.

Following are sample reports and legends of the TSSUTIL batch utility executed with the specified selection criteria. Field descriptions follow the sample reports.

Report Using EVENT(ALL) DATE(TODAY)

The following information is displayed on the report.

DATE

The date when the related incident was recorded. The format of the date is controlled by the DATE control option specified at CA Top Secret initialization. The default is month/day/year. This can vary if using European, military, or other date format. Selection criterion is DATE.

TIME

Time of day when the incident was recorded. The report is, for the most part, time-sequenced; however, this is controlled by the SMF logging function of MVS. TSSUTIL does not sort the incidents, so some events might be out of sequence. You might also notice that blocks of events will have the same time stamp-especially true for online violations. CA-Roscoe, CICS, IMS and other online facilities record incidents indirectly to SMF. The CA Top Secret address space does the actual logging every 15 to 300 seconds (based on the time value set by the TIMER control option). Selection criterion is TIME.

SYSID

The SMF identification of the CPU that logged the event. Selection criterion is SYSID.

ACCESSOR

The ACID that was in effect for the user. ACIDs that begin with an asterisk '*' are special to CA Top Secret:

- *BYPASS*-Indicates that the user is bypassing security.
- *MISSING*-Indicates that the ACID was not supplied on a job card.
- *UNDEF*-Indicates an undefined user.
- Selection criterion is ACID.

JOBNAME

The name of a batch job, the procedure name of a started task (STC), or the userid of an online user. The jobname is usually the same for a TSO user. The jobname for the online region will appear with that of an online user ACID. Selection criterion is JOBNAME.

FFM

Represents two data items: FACILITY ID and MODE. The facility being used is represented by one or two characters. The most common facility codes are:

- B=BATCH
- C=CICSPROD
- K=CICSTEST
- I=IMSPROD
- R=CA-ROSCOE
- S=STARTED TASK
- T=TSO
- V=VM

FACILITY codes for other facilities can be obtained by entering:
`F TSS,FACILITY(fac) at the console.`

The mode of the user is represented by the last single character that shows:

- D=DORMANT
- W=WARN
- I=IMPL
- F=FAIL

For example, TW shows a TSO user in WARN mode. Selection criteria are FACILITY and MODE.

VC

Represents a consecutive accumulation of violations for the duration of the session or job. It is displayed only with violation entries.

PROGRAM

Shows the name of the program in control at the time the security incident was recorded. Common program names are:

- IEFIIC-Batch initiator
- IKJEFLC-TSO LOGON
- IMASPZAP-Superzap
- ISPTASK-SPF

A program name will not always be present, especially if the event was recorded through an online data base system such as CICS or IMS. Selection criterion is RESOURCE. (Select RESOURCE only if you are looking for explicitly owned program usage.)

R-ACCESS

Displays the access level requested for a resource request. The label is determined from the RDT access level definition. If the ACID access level is not an exact match with the bit value for an RDT access-level, the binary access level is placed into the report preceded by an asterisk.

Note: A requested access of FETCH appears as READ in MVS.

A-ACCESS

Displays the access level from the ACID "best fit" permission. The label for the access level is determined from the RDT access level definition. If the ACID access level is not an exact match with the bit value for an RDT access-level, the binary access levelis placed into the report preceded by an asterisk.

SRC/DRC

Shows the return code presented to the system (caller) and the associated detailed error reason code. This indicates whether the access was successful or was failed. If it was successful, one of the following codes will display.

- OK-Indicates that the request was successful.
- OK+A-Indicates a successfully audited incident.
- OK+B-Indicates a successfully bypassed access.
- OK+P-Indicates that data set access is allowed as a result of ACTION(password) being on the rule that granted the access.

Otherwise, the return and detail codes are shown in the format ***rr***-**dd**, where rr is the return code and dd is the detailed error reason code. For example, *30*-0F indicates a terminal or reader violation during initiation; *08*-65 indicates a data set is not accessible. The selection criteria is EVENT(VIOL,AUDIT) to get all violations and audit entries and DRC to get only the specific violations as explained by the detailed error reason codes.

Return codes and the Detailed Error Reason Codes are documented in this manual as well as in the CA Top Secret *Messages and Codes*.

SEC

Shows the MVS, vendor or customer security driver requesting security validation. This is represented by a three-character mnemonic or by a hexadecimal value for the SVC in control. The following codes will appear:

- ADA-Database
- BLP-BLP
- CAT-Catalog management
- CRE-Create data set
- DES-Data encryption
- EOV-End of volume
- FAP-Fetch access protection
- FEV-FEOV
- HSM-HSM
- INC-RACINITC
- INI-Job/STC/session initiation
- INY-RACINITY
- LCF-Command/program
- LKD-"AC=1"
- LST-IMS/CICS initiation
- OPJ-Open-J
- OPN-Open
- REN-Rename-DSNAME
- SCR-Delete-DSNAME
- SUB-Submit
- TMS-Tape management
- TRM-Termination
- USS-UNIX System Services
- VSM-VSAM-Catalog management
- XX-SVC number in hex

RESOURCE

Shows a one character code and up to a 248 character resource name. For initiations, the name of the user will appear via the NAME= keyword. For job submissions, the name of the job and associated ACID will appear. For data set access, the volume serial number and data set name will usually both appear. The class code is one of the following:

```
a = CA_IDMS SUBSCHEMA       U = Abstract
b = CA-IDMS AREA            V = Tape volume
c = Adabas database         W = DASD volume
d = IMS DBD                 X = Transaction
e = JESINPUT                Y = USERn
f = IBM Facility            Z = CICS TST
g = TSO account number      1 = Change propagation
h = TSO authority           2 = CA jobname
i = TSO procedure name      3 = CA panel
j = TSO performance group   4 = DUFXTR
k = VAX file                5 = DUFUPD
l = VAX device              6 = User logging
m = VM IUCV                 7 = VM MDISK
n = VM VMCF                 8 = VM CP CMD
o = TSAF                    9 = VM diagnose
p = JESPOOL                 0 = VM network
q = JESJOBS                 * = Reserved
r = OPERCMDS                # = VM RDR
s = CICS CEMT SPI           % = Logging DB2 resources
t = DEVICES (for VTAM 3.2)  $ = VM DCSS
u = CA REPORT               @ = VM dial
v = CA TAPE                 + = Logging installation exit call
w = SMESSAGE (TSO/E)        = = CACMD
x = VTAMAPPL (VTAM 3.2)     - = Ca Scheduler
y = CAADMIN                 ? = Extract
z = CAVAPPL                 < = Operator commands
' = SYSCONS                 > = Owned transactions
A = Application             . = Data set
B = Audited job submission  / = Dasdvold
C = Mode by user            “ = Tapevolt
D = Data set                ! = CA Station
E = CICS DCT                & = Recipid
F = CICS FCT                : = Reserved
G = Authentication call     ¢ = VMANAPPL
H = TOTAL File              ¦ = UNVEDIT
I = ACID xe03type           7 = UNVRPRT
J = CICS JCT                ~ = UNVPGM
K = Terminal unlock         , = CPU
L = Terminal lock           | = SDSF userclass
M = UR1                     } = VM Machine
N = UR2                     { = IMBGROUP
O = TSS control options     ` = PROPCNTL
P = Program                 _ = Librarian resource CALIBMEM
```

```
Q = CICS PPT                ; = Librarian resource CACCFMEM
R = Database field          ¬ = Librarian resource CACCFDSN
S = DL/1 PST                ( = SMS management class
T = Terminal                ) = SMS storage class
```

The selection criteria are:

- DATASET-For data sets
- VOLUME-For volumes
- RESOURCE-For other resources
- RESCLASS-For specific class
- OPERCMDS-For operator commands

JOBID

Shows the JES2 job number. The job number might be preceded by one of the following codes:

- J-Job
- S-Started task
- T-TSO

TERMINAL

Shows the terminal for an online user or the reader through which a batch job was submitted (JES2 only). Jobs submitted through the internal reader are listed as INTRDR. For users accessing the system via TCP/IP, the IP address is reported in this field as an eight-byte hexadecimal value. For example, access from IP address 111.222.33.123 would be reported as 6FDE217B, where:

- 6F = 111
- DE = 222
- 21 = 33
- 7B = 123

The selection criteria is TERMINAL.

DATE AND TIME RANGES OF AUDIT FILES(S)

Shows the beginning and end of the time range included in the Audit Tracking File(s). This helps the security administrator determine what information is included in the report. If the Audit Tracking File(s) is empty, the STARTING and ENDING fields will contain XX/XX/XX and 99:99:99.

Report Using EVENT(ALL) DATE(-01) LONG

The following information is displayed on the report:

DATE

The date when the related incident was recorded. The format of the date is controlled by the DATE control option specified at CA Top Secret initialization. The default is month/day/year. This can vary if using European, military, or other date format. Selection criterion is DATE.

TIME

Time of day when the incident was recorded. The report is, for the most, part time-sequenced; however, this is controlled by the SMF logging function of MVS. TSSUTIL does not sort the incidents, so some events might be out of sequence. You might also notice that blocks of events will have the same time stamp-especially true for online violations. CA-ROSCOE, CICS, IMS and other online facilities record incidents indirectly to SMF. The CA Top Secret address space does the actual logging every 15 to 300 seconds (based on the time value set by the TIMER control option). Selection criterion is TIME.

SYSID

The SMF identification of the CPU that logged the event. Selection criterion is SYSID.

ACESSOR

The ACID that was in effect for the user. ACIDs that begin with an asterisk '*' are special to CA Top Secret.

- *BYPASS*—Indicates that the user is bypassing security.
- *UNDEF*—Indicates an undefined user.
- *MISSING*—Indicates that the ACID was not supplied on a job card.

Selection criterion is ACID.

JOBNAME

The name of a batch job, the procedure name of a started task (STC), or the userid of an online user. The jobname is usually the same for a TSO user. The jobname for the online region will appear with that of an online user ACID. Selection criterion is JOBNAME.

FACILITY

Shows the facility being used. The most common facilities are:

- BATCH
- CICSPROD
- CICSTEST
- IMSPROD
- ROSCOE
- STC
- TSO
- VM

MODE

Shows the mode of the user. Valid modes are:

- DORM
- FAIL
- IMPL
- WARN

VC

Represents a consecutive accumulation of violations for duration of the session or job. It is displayed only with violation entries.

PROGRAM

Shows the name of the program in control at the time the security incident was recorded. Common program names are:

- IEFIIC—Batch initiator
- IKJEFLC—TSO logon
- IMASPZAP—Superzap
- ISPTASK—SPF

A program name will not always be present, especially if the event was recorded through an online data base system such as CICS or IMS. Selection criterion is RESOURCE. (Select RESOURCE only if you are looking for explicitly owned program usage.)

R-ACCESS

Shows the requested access level as defined in the RDT for the current resource (usually data set, volume, or CICS file).

If an access mask does not uniquely define an access level, the access mask is displayed preceded by an asterisk. In this case; the access mask displayed represents more than one access level.

Note: A requested access of FETCH will appear as READ in MVS.

If the requested access is ALTER, then the TSS PERMIT command requires an access level of ALL.

A-ACCESS

Shows the allowed access level as defined in the RDT for the current resource. Indicates how the resource (usually data set, volume, or CICS file) was accessed by the user of job.

If an access mask does not uniquely define an access level, the access mask is displayed preceded by an asterisk. In this case; the access mask displayed represents more than one access level.

SRC/DRC

Shows the return code presented to the system (caller) and the associated detailed error reason code. This indicates whether the access was successful or failed. If it was successful, one of the following codes will display.

- OK—Indicates that the request was successful.
- OK+A—Indicates a successfully audited incident.
- OK+B—Indicates a successfully bypassed access.
- OK+P—Indicates a successfully issued password.

Otherwise, the return and detail codes are shown in the format ***rr***-**dd**, where rr is the return code and dd is the detailed error reason code. For example, *30*-0F indicates a terminal or reader violation during initiation; *08*-65 indicates a data set is not accessible.

The selection criteria is EVENT(VIOL,AUDIT) to get all violations and audit entries, and DRC to get only the specific violations as explained by the detailed error reason codes.

Return codes and the Detailed Error Reason Codes are documented in this manual, as well as in the CA Top Secret *Messages and Codes.*

SEC

Shows the MVS, vendor or customer security driver requesting security validation. This is represented by a three-character mnemonic or by a hexadecimal value for the SVC in control. The following codes will appear:

- ADA—Database
- BLP—BLP
- CAT—Catalog management
- CRE—Create data set
- DES—Data encryption
- EOV—End of volume
- FAP—Fetch access protection
- FEV—FEOV
- HSM—HSM
- INC—RACINITC
- INI—Job/STC/session initiation
- INY—RACINITY
- LCF—Command/program
- LKD—”AC=1”
- LST—IMS/CICS initiation
- OPJ—Open-J
- OPN—Open
- PGM—Attach, link or load request
- REN—Rename-DSNAME
- SCR—Delete-DSNAME
- SUB—Submit
- TMS—Tape management
- TRM—Termination
- USS—UNIX System Services
- VSM—VSAM-Catalog management
- XX—SVC number in hex

JOBID

Shows the JES2 job number. The job number can be preceded by one of the following codes:

- J—Job
- S—Started task
- T—TSO

TERMINAL

Shows the terminal for an online user or the reader through which a batch job was submitted (JES2 only). Jobs submitted from the internal reader are listed as INTRDR. Selection criterion is TERMINAL.

RESOURCE

Shows the eight-character resource type and up to a 248-character resource name. The resource varies greatly and does not always appear.

For initiations, the name of the user will appear.

For job submissions, the name of the job and associated ACID will appear.

For data set access, the volume serial number and data set name will both appear. The selection criteria are:

- DATASET—For data sets
- VOLUME—For volumes
- RESOURCE—For other resources
- RESCLASS—For specific class
- OPERCMDS—For operator commands

ORIGINAL RESOURCE CLASS

Displays the original eight-character resource class before it was translated during the security check to the resource class displayed in the prior line. This line is displayed only:

- On a type=LONG audit report
- If a resource class translation has been performed

```
ORIGINAL RESOURCE CLASS:  xxxxxxxx
```

DATE AND TIME RANGES OF AUDIT FILES(S)

Shows the beginning and end of the time range included in the Audit Tracking File(s). This helps the security administrator determine what information is included in the report. If the Audit Tracking File(s) is empty, the STARTING and ENDING fields will contain XX/XX/XX and 99:99:99.

Security/Activity Report Legend

The Security/Activity Report Legend provides information on the data areas found on the TSSUTIL report.

The following information appears on the Security/Violation Report Legend:

DATE

The date on which the incident occurred (not sorted)

TIME

The time at which the event occurred

SYSI

System Identification (SMF ID)

ACCESSOR

The accessor security identification (ACID)

JOBNAME

The batch jobname, STC procname, or online userid

FF

Type of Facility

- B=BATCH
- C=CICSPROD
- I=IMSPROD
- K=CICSTEST
- R=ROSCOE
- S=STARTED TASK
- T=TSO
- V=VM
- M= Mode
- D=DORMANT
- F=FAIL
- I=IMPL
- W=WARN

VC

The number of violations accumulated by JOB/SESSION.

PROGRAM

The name of the program in control during the security call.

R-ACCESS

The requested access level. An access mask is shown preceded by an '*' if the access mask represents more than one access level name.

A-ACCESS

The allowed access level. An access mask is shown preceded by an '*' if the access mask represents more than one access level name.

SRC/DRC

Security reason code, detailed reason code:

- 00=OK
- +A=AUDIT
- B=BYPASS
- +P=PW

For resource access:

- 04 OR 08 = ACCESS DENIED

For job initiation:

- 08=PASSWORD IS INCORRECT
- 0C=PASSWORD EXPIRED
- 10=NEW PASSWORD INVALID
- 18=FAILED INST/EXIT
- 1C=ACCESS NOT AUTHORIZED
- 20=SECURITY DORMANT
- 28=OPER-ID CARD REQUIRED
- 2C=BAD OPER-ID CARD
- 30=TERMINAL UNAUTHORIZED
- 34=UNAUTH APPLICATN

Detailed Error Reason Codes are described on the next page of the report.

SEC

System driver issuing security check:

- ADA=DATABASE
- BLP=BLP
- CAT=CVOL/CATLG-MNGT
- CRE=CREATE-DSNAME

- DES=DATA ENCRYPT
- EOV=END-VOL/OPN
- FAP=FETCH ACCESS PROTECTION
- FEV=FEOV
- HSM=HSM
- INC=RACINITC
- INI=JOB/STC/SESSION START
- INY=RACINITY
- LCF=CMD/PGM
- LKD="AC=1"
- LST=IMS/CICS INITIATION
- OPJ=OPEN-J
- OPN=OPEN
- REN=RENAME-DSNAME
- SCR=DELETE-DSNAME
- SUB=SUBMIT
- TMS=TAPE MANAGEMENT
- TRM=TERMINATION
- USS=UNIX System Services
- VFX=RACROUTE REQ=VERIFYX
- VSM=VSAM-CATLG-MNGT
- XX=SVC NUMBER IN HEX

RESOURCE

The type and name of the accessed resource.

a = CA_IDMS SUBSCHEMA	U = Abstract
b = CA-IDMS AREA	V = Tape volume
c = Adabas database	W = DASD volume
d = IMS DBD	X = Transaction
e = JESINPUT	Y = USERn
f = IBM Facility	Z = CICS TST
g = TSO account number	1 = Change propagation
h = TSO authority	2 = CA jobname
i = TSO procedure name	3 = CA panel
j = TSO performance group	4 = DUFXTR
k = VAX file	5 = DUFUPD
l = VAX device	6 = User logging
m = VM IUCV	7 = VM MDISK
n = VM VMCF	8 = VM CP CMD
o = TSAF	9 = VM diagnose
p = JESPOOL	0 = VM network
q = JESJOBS	* = Reserved
r = OPERCMDS	# = VM RDR
s = CICS CEMT SPI	% = Logging DB2 resources
t = DEVICES (for VTAM 3.2)	$ = VM DCSS
u = CA REPORT	@ = VM dial
v = CA TAPE	+ = Logging installation exit call
w = SMESSAGE (TSO/E)	= = CACMD
x = VTAMAPPL (VTAM 3.2)	- = Ca Scheduler
y = CAADMIN	? = Extract
z = CAVAPPL	< = Operation commands
' = SYSCONS	> = Owned transactions
A = Application	. = Data set
B = Audited job submission	/ = Dasdvold
C = Mode by user	“ = Tapevolt
D = Data set	! = CA Station
E = CICS DCT	& = Recipid
F = CICS FCT	: = Reserved
G = Authentication call	¢ = VMANAPPL
H = TOTAL File	¦ = UNVEDIT
I = ACID xe03type	7 = UNVRPRT
J = CICS JCT	~ = UNVPGM
K = Terminal unlock	, = CPU
L = Terminal lock	| = SDSF userclass
M = UR1	} = VM Machine
N = UR2	{ = IMBGROUP
O = TSS control options	` = PROPCNTL
P = Program	_ = Librarian resource CALIBMEM
Q = CICS PPT	; = Librarian resource CACCFMEM
R = Database field	¬ = Librarian resource CACCFDSN

```
S = DL/1 PST                ( = SMS management class
T = Terminal                ) = SMS storage class
```

JOBID

The JES2 job number:

- S=STC
- J=JOB
- T=TSO

TERMINAL

The online terminal name or JES2 Reader or remote.

Detailed Violation Error Reason Code Legend

The Detailed Violation Error Reason Code Legend provides an explanation of all codes in hexadecimal format that appear in the SRC/DRC column of the report.

The following Detailed Reason Codes appear on the TSSUTIL report. For a complete description of these codes, see the *Messages and Codes Guide*.

Codes	Description
01	ACID suspended
02	Failed by site exit
03	ACID missing
04	Facility deactivated
05	ACID expired
06	System facility not authorized
07	Password missing
08	TSO password supplied at logon
09	Password incorrect
0A	Password expired, new password not supplied
0B	New password invalid
0C	CA Top Secret inactive-end of day
0D	Operator ID card required
0E	Operator ID card invalid
0F	New password reverify failed

Codes	Description
10	Cancelled-excessive violations
11	STC undefined
13	Locked-too many violations
14	ACID already signed on
15	Illegal ACID ID
16	Remote job entry terminal not authorized for submission
17	Cross-memory failure
18	Suspended user on holidays
19	NOATS
1A	Terminal or reader is not an authorized source
1B	Password violation threshold exceeded
1C	ACID inactive too long
1D	Voice/image rejection
1E	Internal interfacing error
1F	No authority for function
20	Internal interfacing error
21	Internal system error
22	TSS command failure
23	Unknown facility
24	Integrity error
25	Init error
26	Integrity error
2C	Insufficient CSA storage
41	Invalid volser
46	ACID not defined
47	ACID already exists
4C	Invalid resource name/length
4D	Error during backup
4E	(INST)DATA not present
51	Volume not found

Codes	Description
52	Volume not owned
53	Volume not owned
54	Volume already defined
55	Volume already defined
56	Vol prefix not owned
57	DSNAME/prefix not defined
58	DSNAME/prefix already defined
59	Prefix owned
5A	Resource already defined
5B	Resource not found
5C	Resource not owned
64	TSS is inactive
65	DSNAME inaccessible
66	X-AUTH'D data set access not granted
67	Access denied for globally restricted data set
68	Fetch denied
69	Cannot delete-erase disallowed
6A	Illegal data set access through non-privileged program/filepool
6B	Illegal data set access through unauthorized TASK/LIBRARY/SFS file
6C	Fetch violation
6D	Data set access failed by installation exit
6E	Data set accessed at illegal time
6F	Data set accessed on unauthorized day
70	Data set accessed through unauthorized facility
73	Volume access denied by exit
74	BLP access unauthorized
75	Volume not owned
77	Cross-authorized volume accessed at unauthorized level
78	Cannot create data sets on this volume
79	System error during validation

Codes	Description
7A	Attempted to access entire volume without specification of data set name
7E	Volume access not allowed on this day
7F	Volume access denied by time
80	Volume accessed through unauthorized facility
81	Volume accessed by unpriviledged program
88	Resource access denied
8C	IMS XACTN required password
8E	IMS XACTN password bad
90	Resource access denied by installation exit
91	Resource denied this day
92	Resource denied this time
93	Terminal locked
94	Unlock failed bad password
95	Resource access by unpriviledged program
96	Resource access by unauthorized facility
97	Unauth resource access level
98	Terminal locked-excessive violations
99	JOB/ACID security bypass
9A	Submit failed-unauthorized facility
9B	Submit failed-bad program
9C	Submit failed by exit
9D	Submit failed unauthorized ACID
9E	No LCF authority
9F	Unauth program execution attempt
A0	Facility access not allowed at this time
A1	Facility access denied by day

To customize reporting without TSSUTIL, see the SMF Type 80 Record Layout section.

TSSUTIL Abend and Return Codes

Abend Codes

Code	Description
1600	Failure to open file SYSPRINT

This is the only abend code. All other abend codes have been replaced by an error message issued to SYSPRINT with a final return code of 8.

Return Codes

Code	Description
RC=0	All reports processed successfully
RC=4	One or more reports with no incidents found matching selection criteria. For the EXTRACT function, only the SMFOUT file was supplied in the JCL and at least one record written to the file was truncated. In this case the XTROUT file should be added to the JCL to contain the longer records.
RC=8	An error has been found and an error message was issued to file SYSPRINT. The execution is terminated.

SMF Type 80 Record Layout

The following layout is for the SMF type 80 record. If you want to customize reporting rather than use TSSUTIL, you can review the layout of the SMF type 80 record shown next. For an ALT-ACID audit entry, the jobname may appear immediately after the eight-character ACID of the audit record that is produced.

SMF Type 80 Record Layout			
SMF80FLG	DS	X	X'02'VS2
SMF80RTY	DS	X	80 DECIMAL
SMF80TME	DS	XL4	TIME
SMF80DTE	DS	CL4	DATE

SMF Type 80 Record Layout			
SMF80SID	DS	CL4	SYSTEM ID
SMF80DES	DS	XL2	DESCRIPTOR FLAGS
SMF80EVT	DS	X	EVENT CODE:
$S80INIT	EQU	1	JOB INITIATION
$S80AUTH	EQU	2	AUTHORIZATION CHECK
$S80CMD	EQU	50	AUTH COMMAND
$S80PSWD	EQU	51	PASSWORD CHANGE
$S80COPT	EQU	52	TSS CONTROL OPTIONS
$S80AVO	EQU	55	AVO REQUEST
$S80VOL	EQU	56	VOLUME UPDATE
$S80NVOL	EQU	57	TAPEMNGT ADD VOLUME
$S80DVOL	EQU	58	TAPEMNGT DELETE VOLUME
$S80DUF	EQU	59	DYNAMIC (INSTDATA) UPDATE
$S80ABND	EQU	60	USER ABEND IN CA Top Secret
$S80XDIS	EQU	61	EXIT DISABLED
$S80STSS	EQU	62	START CA Top Secret ADDRESS SPACE
$S80PTSS	EQU	63	STOP CA Top Secret ADDRESS SPACE
$S80STCA	EQU	64	STC OPERATOR ACCOUNTABILITY
$S80STAT	EQU	65	STATISTICS DUMP
*			
SMF80EVQ	DS	X	EVENT CODE QUALIFIER
SMF80USR	DS	CL8	ACCESSOR ID
	DS	XL2	
	DS	XL2	
	DS	XL2	
	DS	XL2	
SMF80REL	DS	CL2	OFFSET TO 1ST EXTENSION
SMF80CNT	DS	XL2	# OF EXTENSION SECTIONS
SMF80ATH	DS	X	AUTHORITY

SMF Type 80 Record Layout			
	DS	X	
	DS	X	
	DS	X	
SMF80TRM	DS	CL8	TERMINAL ID
SMF80JBN	DS	CL8	JOBNAME
SMF80RST	DS	XL4	READER TIME
SMF80RSD	DS	XL4	READER DATE
SMF80UID	DS	CL8	SMF USERID
SMF80VER	DS	X	RACF VERSION
LSMF80	EQU	*-SMF80	
SMF80REX	DSECT		
SMF80DTP	DS	X	DATA TYPE:
$S80XCMD	EQU	103	IMAGE OF CA Top Secret COMMAND
$S80XSRI	EQU	104	SRIPL/PW/AVO
$S80XOPT	EQU	105	IMAGE OF CA Top Secret OPTIONS
$S80XFLG	EQU	109	COPY OF FLOG
$S80XHDR	EQU	255	AUDIT/FILE HEADER RECORD
$S80XEND	EQU	0	AUDIT/FILE WRAPPER
SMF80DLN	DS	X	LENGTH OF DATA IN EXT SECTION
SMF80DTA	DS	0X	VARIABLE DATA SECTION
*			
	DS	A	RESERVED
	DS	X	RESERVED
	DS	X	RESERVED
FLIND2	DS	X	AUDIT REASON INDICATOR:
$FLI2ACT	EQU	X'80'	ACTION AUDIT
$FLI2RSC	EQU	X'40'	RESOURCE AUDIT
$FLI2USR	EQU	X'20'	USER AUDIT
$FLI2FAC	EQU	X'10'	FACILITY AUDIT
*			

SMF Type 80 Record Layout			
	DS	X	RESERVED
	DS	X	RESERVED
FLFLAGS	DS	X	LOGGING INDICATORS:
$LOGVIOL	EQU	X'80'	VIOLATION
$LOGFORC	EQU	X'40'	FORCED LOG-OUT
$LOGFAIL	EQU	X'20'	TRUE FAILURE
$LOGAUDT	EQU	X'10'	AUDITED EVENT
*			
FLDATE	DS	XL3	DATE (PACKED YYDDDF)
	DS	X	RESERVED
FLTIME	DS	XL4	TIME OF DAY (HHMMSSTH)
FLRACC	DS	XL2	REQUESTED ACCESS
FLAACC	DS	XL2	ALLOWED ACCESS
FLRETCOD	DS	X	RETURN CODE
FLDETLRC	DS	X	DETAIL REASON CODE
FLJOBTYP	DS	X	FACILITY
FLSVC	DS	X	CALLING SVC
FLCLASS	DS	X	RESOURCE CLASS:
$ARAPPL	EQU	C'A'	APPLICATION
$ARSUBM	EQU	C'B'	SUBMIT ACID
$RRCHANG	EQU	C'C'	SECURITY FILE CHANGE
$ARDSN	EQU	C'D'	DSNAME PREFIX
$ARDCT	EQU	C'E'	CICS DCT
$ARFCT	EQU	C'F'	CICS FCT
$ARJCT	EQU	C'J'	CICS JCT
$ARTSS	EQU	C'O'	TSS OPTIONS
$ARPGM	EQU	C'P'	PROGRAM
$ARTERM	EQU	C'T'	TERMINAL
$ARVOL	EQU	C'V'	TAPE VOLUME
$ARDASDV	EQU	C'W'	DASD VOLUME

SMF Type 80 Record Layout			
$ARXACTN	EQU	C'X'	TRANSACTION
*			
FLMODE	DS	X	USER'S MODE:
$DORM	EQU	X'80'	DORMANT MODE
$WARN	EQU	X'40'	WARN MODE
$FAIL	EQU	X'20'	FAIL MODE
$IMPL	EQU	X'30'	IMPL MODE
*			
FLJOBNUM	DS	XL2	JOBNUMBER (JES FORMAT)
FLNVIOL	DS	X	VIOLATION COUNT (FOR SESSION)
	DS	XL2	RESERVED
	DS	XL2	RESERVED
FLACID	DS	CL8	ACID NAME
FLJOB	DS	CL8	JOB NAME
FLVOLSER	DS	CL6	VOLUME SERIAL
	DS	CL2	RESERVED
FLPGM	DS	CL8	PROGRAM IN CONTROL
FLRES	DS	CL44	RESOURCE NAME
FLIND1	DS	X	INDICATORS:
$FLBYPSS	EQU	X'80'	USER IS BYPASSING SEC'Y
$FLNOTIF	EQU	X'40'	ACTION(NOTIFY)
$FLSUSP	EQU	X'20'	SUSPEND ACID
$FLFRAK	EQU	X'10'	FRACHECK-INITIATED LOG
$FLRENMO	EQU	X'04'	RENAME OLD DSNAME DATA
$FLRENMN	EQU	X'02'	RENAME NEW DSNAME DATA
$FLRENM	EQU	$FLRENMO+ $FLRENMN	RENAME OLD AND NEW
$FLVSAM	EQU	X'01'	VSAM CATALOG DATA
*			
FLINDEV	DS	CL8	INPUT DEVICE (TERMINAL/READER)

SMF Type 80 Record Layout			
FLATTR1	DS	XL1	USER ATTRIBUTES:
$AMULTPW	EQU	X'80'	PASSWORD PER FACILITY
$ATSOMPW	EQU	X'40'	MULTIPLE TSO UADS PASSWORDS
$ANOADSP	EQU	X'20'	DONT USE ADSP (INIT)
$ANOPWC	EQU	X'10'	USER CANNOT CHANGE PASSWORD
$AAUDIT	EQU	X'08'	AUDIT THIS ACID
$AOID	EQU	X'04'	OIDCARD REQUIRED
$ATRACE	EQU	X'02'	TRACE THIS USER
$ANOSUBK	EQU	X'01'	CAN SUBMIT ANY ACID
*			
FLATTR2	DS	XL1	USER ATTRIBUTES:
$A14LIB	EQU	X'80'	PRIV LIB(S) PRESENT IN A/REC
$AERROR	EQU	X'40'	ACT/REC ON FILE IS IN ERROR
$ASUSPND	EQU	X'20'	ACID IS SUSPENDED
$ANORESK	EQU	X'10'	NO RESOURCE CHECKING
$ANOVOLK	EQU	X'08'	NO VOLUME CHECKING
$ANODSNK	EQU	X'04'	NO DATASET CHECKING
$ANOLCFK	EQU	X'02'	NO LCF CHECKING
*			
FLATTR3	DS	XL1	USER ATTRIBUTES:
$AMRO	EQU	X'80'	MRO-SECURITY RECORDS IN CSA
$ASHRPRF	EQU	X'40'	SHARED COMMON PROFILES
$ACON	EQU	X'20'	CONSOLE AUTHORITY
$AGAP	EQU	X'10'	GLOBALLY ADMINISTRABLE PROFILE
$ADUFXTR	EQU	X'08'	DUF EXTRACT
$ADUFUPD	EQU	X'04'	DUF UPDATE
$ASUSPUN	EQU	X'02'	SUSPEND UNTIL IN EFFECT
$ANOVMMD	EQU	X'01'	NO MINI DISK CHECKING
*			

SMF Type 80 Record Layout			
	DS	X	RESERVED
FLRTME	DS	XL3	READER START TIME
FLRDTE	DS	XL3	READER START DATE

Chapter 2: TSSTRACK Utility

This section contains the following topics:

About the TSSTRACK Utility

TSSTRACK allows administrators and auditors to monitor security-related events in real time for one or more systems. Information is obtained from the CA Top Secret Audit/Tracking File, providing you with a complete, up-to-date display of violations and other audited events. A single terminal can be used to monitor activity on all systems using CA Top Secret and a common Audit/Tracking File.

As distributed, this utility is executable under TSO and CICS. TSSTRACK can be used at both 3270 terminals with 80 or 132 character widths or non-3270 terminals under TSO. Only 3270 terminals are supported under CICS. TSSTRACK supports up to 30 CPUs.

TSSTRACK is designed primarily for continuous monitoring of security-related events. If you wish to extract information about particular events, execute the batch TSSUTIL program. You cannot run TSSTRACK from RACF/SAC compatibility mode.

Using the TSSTRACK Utility

The following considerations affect the TSSTRACK utility:

- Security related events are displayed in chronological order as found in the Audit/Tracking File(s). No sorting is performed.
- Report and tracking depends greatly upon the correct specification of logging options. The LOG option lets you request the type of events to be logged; specify where logging information is recorded; and choose where violation notification is to be made.
- The following logging options are required to obtain security information:
  - LOG(INIT,...) requests logging of all job/session initiations and terminations.
  - LOG(SMF,...) requests SMF recording in addition to logging on the Audit Tracking File.
- Each facility can be separately monitored.
- To obtain audited events, you must be auditing resources and/or user activity.
- The security authority under which TSSTRACK is executed.

Authority and Scope

To use TSSTRACK, you must be defined as a security administrator (SCA, LSCA, ZCA, VCA or DCA) or the MSCA and have the following administrative authority:

```
TSS ADMIN(acid) ACID(REPORT,AUDIT)
                RESOURCES(REPORT,AUDIT)
```

A user with no administrative authority may use TSSTRACK if given USE access to entity TSSUTILITY.TSSTRACK in the CASECAUT resource class. This access may be granted by an administrator using the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSTRACK) ACCESS(USE)
```

Only those events associated with ACIDs within your scope are tracked. For example, a divisional administrator receives information only about events involving ACIDs in her division. (The scope of authority is determined by the assigned ACID type when you were defined to CA Top Secret.)

Allocating the Audit/Tracking Files

TSSTRACK accesses the product AUDIT files (DDNAME AUDIT and optional AUDIT2) to format information about your system in TSO or CICS. In order to access these files, CA Top Secret must have these files pre-allocated.

The sample CLIST TSSTRACK in the next section can be invoked from READY or from TSO/ISPF. The CLIST allocates the AUDIT files, invokes the utility, and then frees the files. See the section “Invoking TSSTRACK under TSO or ISPF.” The TSO user ACID or the CICS ACID must have, at least, READ access for the Audit/Tracking File(s), and must always be allocated with a disposition of SHR.

Allocation for CICS can take place using standard FCT RDO or MDO. The Audit/Tracking Files under CICS can be dynamically allocated using the ADYN transaction, if installed. No FCT entries are required for the Audit/Tracking files if allocated with the ADYN transaction. However, the AUDIT (and AUDIT2) DD JCL statements must be added to the JCL for the CICS Region. TSSTRACK in CICS is invoked through the TSS command transaction.

Invoking TSSTRACK under TSO or ISPF

The following CLIST can be used as a model to invoke TSSTRACK under TSO:

```
TSSTRACK CLIST
    PROC 00 OPTION
    FREE DDN(AUDIT,AUDIT2)
    ALLOC DDNAME(AUDIT) DSNAME ('dsname of first ATF') SHR
    ALLOC DDNAME(AUDIT2) DSNAME('dsname of second ATF') SHR
    TSSTRACK '&OPTION.'
    FREE DDN(AUDIT,AUDIT2)
    EXIT
```

(For sites which do not employ AUDIT2, that allocation might be omitted.) You will need to make the CLIST available to the SYSPROC allocation for users who will need to invoke the utility. The CLIST has the capacity to take a single option as a parameter. If more than one option needs to be specified, the CLIST should be invoked without operands, and the program will prompt for options.

After entering your options, the security-related information is continuously displayed. The INTERVAL selection criterion will specify how frequently the Audit/Tracking File is to be checked for new events. New selection criteria values can be entered at any time by pressing the PA1 key on 3270 terminals or the BREAK key on non-3270 terminals. (Remote 3270 terminals in SNA environments might need to use the ATTN key.) This interrupts the tracking information display, and the input prompt is reissued. You can then enter the desired selection criteria. To return to the tracking information display, press the Enter key.

If DATE or TIME is specified after displaying the requested tracking information, TSSTRACK will display the “option” prompt when the current date and time is reached in the Audit/Tracking file after the Enter key is pressed.

TSSTRACK is terminated by interrupting the tracking information display as described above, then entering the STOP or END selection criteria.

Invoking TSSTRACK Using CICS

TSSTRACK in CICS is executed from the TSS command transaction. TSSTRACK can be invoked in two modes:

Continuous Mode

In this mode, TSSTRACK is invoked for a fixed time period. TSSTRACK refreshes its output automatically without input from the terminal operator. For example:

```
TSS TRACK=ON,FOR=(#minutes)
```

Interactive Mode

In this mode, TSS TRACK=ON is invoked without the FOR operand. Operation options and session termination are based on terminal input.

Note: Program function and attention keys operate differently in CICS than they do in TSO.

CICS Users in Interactive Mode

To invoke TSSTRACK in interactive mode under CICS, enter:

```
TSS TRACK=ON\{,option\}
```

In the interactive mode, you must press the Enter key to update the screen. TSSTRACK does not continuously display the security-related information as in TSO or as in the continuous mode in CICS.

New selection criteria values can be entered at any time by pressing the PF3 or PF15 key. This causes an interruption of the tracking information display and the input prompt is reissued. You can then enter the desired selection criteria where the cursor is positioned.

TSSTRACK is terminated by interrupting the tracking information display as described above, then entering the STOP or END selection criteria.

CICS Users in Continuous Mode

To invoke TSSTRACK in continuous mode under CICS for a period of “hh” hours and “mm” minutes, enter:

```
TSS TRACK=ON,FOR(hh:mm)
```

To designate only a specified number of minutes for the FOR keyword, omit the colon. For example, if you only want to run TSSTRACK for 15 minutes you would enter:

```
TSS TRACK=ON,FOR(15)
```

This command invokes TSSTRACK continuously for 15 minutes and refreshes the display automatically as data becomes available. The data display continues for the specified 15-minute time interval or until interrupted with BREAK/ATTENTION or PA1.

When additional options are required, invoke TSSTRACK without options. The utility will prompt tracking criteria.

In continuous mode, TSSTRACK takes over the terminal for the time specified when TSSTRACK was invoked. Once the Enter key is pressed, security-related information is continuously displayed. The INTERVAL selection criterion will specify how frequently the Audit/Tracking File is to be checked for new events. In order to interrupt TSSTRACK in this mode, or stop it before the specified time has expired, enter the following from another terminal:

```
TSS TRACK=OFF,TERM=(ALL|terminal,...)
```

This allows the user to stop processing TSSTRACK from all terminals, or only specified terminals. After an interrupt, the option entry screen is displayed. You can enter new options for additional display or terminate the session with END.

Entering Options in TSSTRACK

TSSTRACK options only pertain to TSSTRACK and should not be confused with Security File Control Options which set system-wide defaults and are stored in the Parameter File. If there are no options passed to TSSTRACK when it is invoked, the following prompt is displayed:

TSSTRACK Options Prompt

```
CA Top Secret SECURITY VERSION 5.2  ONLINE TRACKING mm/dd/yy hh:mm:ss

AVAILABLE OPTIONS ARE:  DATE(YYDDD!TODAY!-##) TIME(HHMM) SYSID(????)
   SIDCOL(#)  EVENT(ALL|VIOL,AUDIT,AUDTA,AUDTB,JOBS)  FACILITY(ALL|???,...)|F(...)
   ACID(????????)|A(????????) DRC(??,??,...)|DRC  INTERVAL(##) LINES(##)
   WIDTH(##) SCROLL(##|YES|NO) SIGNAL(ON|OFF) HOLD|RESUME CURRENT HELP
   HARDCOPY(?|OFF)|HARDC(?,##) LOCK|UNLOCK  STOP|END

TSS8192A ENTER TSSTRACK SELECTION CRITERIA/OPTIONS
```

Notes:

- The pound signs (#) and question marks (?) indicate that values must be supplied with an associated option.
- The maximum number of characters (including spaces) that can be entered for criteria options is 100.

Types of Security Events to Interrogate

TSSTRACK reads Audit/Tracking files (ATFs) to obtain information about security events for the administrator. Use this utility to interrogate:

- Live security events against the current audit file
- Historical security events against ATFs no longer in use.

Security Events

To track ongoing security events, assure that neither AUDIT nor AUDIT2 files are allocated when TSSTRACK is invoked. TSSTRACK determines which file is receiving events and allocates the correct file name and data set name dynamically. Determining which is the live file is made complex by the possibility that a switch (for example from AUDIT to AUDIT2) may take place during the administrator's query. TSSTRACK dynamically allocates the AUDIT files based on data set names available in internal CA Top Secret control blocks

Historical Data

If you use TSSTRACK to report historical Audit/Tracking data the files must be pre-allocated. The mechanism for this depends on whether you are in the TSO or CICS environments. If you use TSSTRACK for historical purposes, supply DATE and TIME operands within the range of data provided on your pre-allocated ATF files for your requests.

Installation

The installation SAMPJCL(TSSTRACK) member contains a CLIST you can use. To invoke the CLIST, copy it into one of your user CLIST libraries. The CLIST may be employed from ISPF or from READY mode. An ISPF Panel is also available in TSSISPF(TSS@PRIM) to invoke TSSTRACK and other utilities.

TSSTRACK CLIST

The installation SAMPJCL(TSSTRACK) member contains a CLIST you can use. To invoke the CLIST, copy it into one of your user CLIST libraries. The CLIST may be employed from ISPF or from READY mode.

The TSSTRACK CLIST has the following parameters:

HIST(N|Y)

Indicates that TSSTRACK is (Y) or is not (N) being employed to interpret historical data. HIST(N) is the default and indicates that the current audit/tracking file will be allocated dynamically

AUDIT()

Indicates that historical data set name for the AUDIT allocation. This has no effect when HIST(N)

AUDIT2('*NONE*') AUDIT2('audit2.dsn')

Indicates that:

- Only one AUDIT file is to be used for historical purposes ('*NONE*'): in this case, the AUDIT dataset name will be used for AUDIT2 as well.
- A second data set name will be allocated for historical TSSTRACK analysis

This parameter has no effect when HIST(N).

OPTION('option1,...')

Indicates a list of options for TSSTRACK to be invoked immediately without prompting. The default for this option is INTERVAL(10), which requests a refresh of data after 10 seconds.

TSS@PRIM ISPF Panel

An ISPF panel is also available in TSSISPF(TSS@PRIM) to invoke TSSTRACK and other utilities. You can copy the TSSISPFM(TSS@PRIM) panel into your ISPF Panel Library allocation and modify your system ISR@PRIM to invoke TSS@PRIM.

Refreshing the Display

After entering your options the security-related information is continuously displayed. The INTERVAL selection criterion specifies how frequently the Audit/Tracking File is checked for new events.

To enter new selection criteria, press the:

- PA1 key on 3270 terminals
- BREAK key on non-3270 terminals. (Remote 3270 terminals in SNA environments might need to use the ATTN key.)

This interrupts the tracking information display and reissues the input prompt. You can then enter the new options or END to terminate the TSSTRACK session.

DATE and TIME Options

You can enter TSSTRACK DATE and TIME options with the following limitations:

- When reviewing historical audit/tracking data always use the DATE and TIME options consistent with the range of events in the allocated AUDIT and AUDIT2 files.
- When reviewing activities in the current ATF, use DATE and TIME options consistent with the events on the file. TSSTRACK attempts to find events beginning with the specified date and time and displays events from that time through currently logged events.

Invoking TSSTRACK Using CICS

TSSTRACK should be used with caution under CICS. TSSTRACK is not designed for use in CICS by more than one user simultaneously.

Do not use TSSTRACK for historical purposes under CICS. For the most predictable results with TSSTRACK set the AUDIT and AUDIT2 files FCT entries to CLOSED and DISABLED prior to execution of TSSTRACK. The current TSS audit/tracking file is dynamically allocated by TSSTRACK when invoked for this purpose.

There is no new transaction or program required to invoke TSSTRACK in CICS, because TSSTRACK is invoked from within the TSS command/transaction. If you have already installed the TSS command/transaction (for instance using SAMPJCL(TSSCSD)), then TSSTRACK has already been installed.

TSSTRACK can be invoked in two modes:

Continuous Mode

In this mode, TSSTRACK is invoked for a fixed time period. TSSTRACK refreshes its output automatically without input from the terminal operator. For example:

```
TSS TRACK=ON,FOR=(#minutes)
```

Interactive Mode

In this mode, TSS TRACK=ON is invoked without the FOR operand. Operation options and session termination are based on terminal input.

Note: Program function and attention keys operate differently in CICS than they do in TSO.

Continuous Mode

To invoke TSSTRACK in continuous mode use the FOR option:

```
TSS TRACK=ON,FOR(mm)
```

This command invokes TSSTRACK continuously for *mm* minutes and refreshes the display automatically as data becomes available.

The data display continues for the specified FOR time interval or until interrupted with BREAK/ATTENTION or PA1.

After an interrupt the option entry screen is displayed. You can enter new options for additional display or terminate the session with END.

Interactive Mode

To invoke TSSTRACK in interactive mode leave the FOR option out of the command:

```
TSS TRACK=ON
```

When invoked without FOR, TSSTRACK waits for the terminal operator to press ENTER before proceeding to the next display.

Use PF3 or PF15 to terminate the display of audit data and display the option entry screen. You can enter additional options or use END to terminate the session.

TSSTRACK Options

The selection criteria are listed alphabetically below, with brief descriptions and the defaults, if any. All selection criteria are discussed in detail after the alphabetical listing.

Note: Once set, the ACID, LINES, WIDTH, FACILITY, HARDCOPY, EVENT, SIDCOL, SIGNAL, and SYSID options will remain in effect for the duration of the TSSTRACK session.

You can enter the DATE and TIME options with the following limitations:

- When reviewing historical audit/tracking data always use the DATE and TIME options consistent with the range of events in the allocated AUDIT and AUDIT2 files.
- When reviewing activities in the current ATF, use DATE and TIME options consistent with the events on the file. TSSTRACK attempts to find events beginning with the specified date and time and displays events from that time through currently logged events.

TSSTRACK options only pertain to TSSTRACK and should not be confused with Security File Control Options, which set system-wide defaults and are stored in the Parameter File. If there are no options passed to TSSTRACK when it is invoked, a prompt appears, displaying available options and allowing you to enter options. Pound signs (#) and question marks (?) indicate that values must be supplied with an associated option. The maximum number of characters (including spaces) that can be entered for criteria options is 100.

ACID

Specifies an ACID for the tracking information display.

CURRENT

Forces TSSTRACK to display information for the current date and time. This is the default if no other Selection Criterion is specified when TSSTRACK is first invoked.

DATE

Specifies the starting date for the tracking information display. The default is TODAY.

DRC

Requests information about the detailed error reason codes used in the tracking display.

END

Terminates TSSTRACK.

EVENT

Specifies the type of security-related events for which tracking information is to be displayed. The default is AUDIT,VIOL.

FACILITY

Specifies the facilities for which tracking information is to be displayed.

HARDCOPY

Specifies whether hardcopy of the tracking information displayed is to be produced. The default is OFF.

HELP

Requests summary information about the abbreviations used in the tracking information display.

HOLD

Temporarily freezes the tracking information display.

INTERVAL

Specifies how often TSSTRACK is to check the Audit/Tracking File for new events. The default is 15 seconds.

LINES

Specifies the maximum number of lines that may be used on the 3270 terminal screen.

LOCK

Locks the terminal while TSSTRACK is running.

RESUME

Resumes normal TSSTRACK processing after the pause forced by the HOLD parameter.

SCROLL

Specifies whether the tracking information display on a terminal is to be paged forward automatically, as necessary, to create space for new display lines. The default value is YES for 3270s; NO for non-3270s.

SIDCOL

Specifies the column of the SMF-ID from which the one-character system identifier is taken for the TSSTRACK Information Display.

SIGNAL

Specifies whether the audible alarm is to be sounded when information about a new event is written to the terminal, if so equipped. The default is ON.

STOP

Terminates TSSTRACK.

SYSID

Specifies the SMF identifier of the CPU for which tracking information is to be displayed.

TIME

Specifies the starting time for the tracking information display.

UNLOCK

Unlocks the terminal after the password is entered.

WIDTH

Specifies the maximum number of columns that may be used on the 3270 terminal screen.

All selection criteria are described in detail below using the following syntax conventions:

UPPERCASE	**Option must appear as shown.**
lowercase	Option must be supplied.
ellipsis	Additional options can be supplied.
[ ]	Brackets indicate an option not required.

|	Vertical bar indicates that only one of the options can be supplied.

Note: Abbreviated forms, if any, will appear under the full name of the selection criteria in the boxed areas.

ACID

Specifies an ACID for tracking information display.

```
ACID(acid)
A
```

acid

Specifies an ACID to be monitored. The default is null. Once used the ACID specification remains for the duration of the TSSTRACK session.

To reset the ACID enter:

```
ACID( )
```

CURRENT

Forces TSSTRACK to display event information using the current date and time. This is the default if date and/or time was not specified when TSSTRACK was first invoked.

```
CURRENT
```

DATE

Specifies the starting date for the tracking information display. All events logged from this date through the current date are displayed. If DATE is omitted, a default of TODAY and the current time are used.

```
DATE(-nnn|yyddd|TODAY)
```

-nnn

Specifies the number in days subtracted from the current date which calculates the starting date for the tracking information display. This number 'nnn' may be an integer from 0 to 365. Specifying 0 generates the same result as specifying TODAY.

yyddd

Specifies the Julian date to be used as the starting date for the tracking information display.

TODAY

Specifies that the current date is to be used as the starting date for the tracking information display.

Note: Specifying the DATE selection criteria sets the SCROLL control option value to NO, unless SCROLL is specified after the DATE selection criteria. After displaying the requested tracking information, TSSTRACK will display the “option” prompt when the current date and time are reached in the Audit/Tracking file after the Enter key is pressed.

DRC

Displays “help” description of DRC codes. If included with additional operands to be used in selection of events from the AUDIT file, the additional operands will be ignored, regardless of their positional placement in the request. DRC codes may be supplied with the request in hexadecimal format. The syntax of a DRC request is:

```
DRC[(x1,x2)]
```

Notice that DRC may be issued with or without an explicit list of codes. If DRC is requested without operands, the user will be prompted for codes by the following message:

TSS8193A ENTER LIST OF DETAIL REASON CODES, SEPARATED BY COMMAS

The user then responds with:

```
01,67,6D
```

This is completely equivalent to specifying:

```
DRC(01,67,6D)
```

The results of either query will display the following information:

```
01-Acid has been suspended
67-Global dataset access denied
6D-Dataset access failed by installation exit
```

Note: DRC requests will not edit the ATF input for the DRC codes selected.

END

Terminates TSSTRACK.

```
END
```

When END is entered, the following message is issued:

```
ONLINE TRACKING TERMINATED
```

Note: No other selection criteria should be entered with END. This selection criterion cannot be used in continuous mode under CICS.

EVENT

Specifies the type of security-related events for which tracking information is to be displayed.

```
EVENT(ALL|VIOL,AUDIT,AUDTA,AUDTB,JOBS)
```

ALL

Information is to be displayed for all types of security-related events.

EVENT

Specifies security-related event(s) for which information is to be displayed. This may be one or more of the following:

- AUDIT-Audited events are to be displayed.
- JOBS-Job initiations and terminations being tracked are to be displayed.
- VIOL-Security violations are to be displayed.
- AUDTA-Displays OK+A events and prevents OK+B events from being displayed.
- AUDTB-Displays OK+B events and prevents OK+A events from being displayed.

If more than one event is specified, the types of events should be separated by commas. If EVENT is omitted, a default of AUDIT, VIOL is used.

Note: The EVENT selection criterion can be used in conjunction with the FACILITY and SYSID selection criteria to monitor very specific types of events.

FACILITY

Specifies the facilities for which tracking information is to be displayed. If FACILITY is omitted, a default of ALL is used.

```
FACILITY(ALL|facility,...)
FAC
F
```

ALL

Information is to be displayed for all facilities. FACILITY(ALL) is also used to reset the FACILITY option prior to the termination of the TSSTRACK session.

facility

Specifies facility or facilities for which information is to be displayed. May be any facility defined in the site's Systems Facilities Matrix or one of the default facility names provided by CA Top Secret.

The CICS and IMS Facilities Matrix entries usually refer only to the production versions, not test versions.

Note: The FACILITY selection criterion can be used with the EVENT and SYSID selection criteria to monitor very specific types of events.

HARDCOPY

Specifies whether hardcopy of the tracking information display is to be produced. With no operand, hardcopy is produced and directed to SYSOUT class A. If HARDCOPY is omitted, a default of OFF is used.

```
HARDCOPY(OFF, class[,#lines]) [(OFF)]
```

OFF

Existing hardcopy SYSOUT file is to be printed, if any exists.

class

Hardcopy is to be produced and associated with the indicated SYSOUT class. May be any SYSOUT class name.

#lines

The optional maximum number of lines per page for the hardcopy output. If specified, headings are produced for the hardcopy output. By default, no headings are produced if SCROLL(YES) was specified.

Specifying HARDCOPY(class) results in the dynamic allocation of a SYSOUT file for hardcopy of the tracking information display. This file is closed and directed to the indicated SYSOUT class when TSSTRACK terminates. The SYSOUT file can be closed and printed while TSSTRACK is executing in one of two ways:

- If HARDCOPY(OFF) is specified, the existing SYSOUT file is closed and directed to its SYSOUT class for printing; no new SYSOUT file is allocated.
- If HARDCOPY(class) is specified, the existing SYSOUT file is closed and directed to its SYSOUT class for printing. In addition, a new SYSOUT file is dynamically allocated.

HELP

Requests summary information about the abbreviations used in the tracking information display.

```
HELP
```

No other selection criteria should be entered with HELP.

Information is displayed concerning the following:

- Resource class code
- Facility codes
- Mode codes
- Access codes
- Security drivers

To obtain information about the detailed error reason codes used in the tracking information display, use the DRC selection criterion.

HOLD

Temporarily freezes the tracking information display.

```
HOLD
```

No other selection criteria should be entered with HOLD. To return to the tracking information display in TSO, press the PA1 key; in CICS interactive mode, press the PF3 or PF15 key. In either case, then enter RESUME. In continuous mode under CICS, you cannot use this selection criterion.

HOLD is valid only at 3270 terminals. It is ignored if entered from a non-3270 terminal.

Note: The HOLD option is not VALID if the SCROLL control option has been set to no.

INTERVAL

Specifies how many seconds the Audit/Tracking File is to be checked for new events. If INTERVAL is omitted, a default of 15 is used.

```
INTERVAL(nnn)
```

nnn

Interval (in seconds) that TSSTRACK is to wait before examining the Audit/Tracking File for new events. May be an integer between 01 and 600.

LINES

Specifies the number of lines to be displayed on your terminal screen. If LINES is omitted, TSSTRACK uses the maximum number of lines available on the terminal screen.

```
LINES(nn)
```

nn

Maximum number of lines that may be used on your terminal screen. May be an integer between 10 and 48.

LOCK

Locks the terminal while TSSTRACK is running.

```
LOCK
```

If you terminate TSSTRACK, use TSS UNLOCK to unlock the terminal. In TSO and CICS interactive mode, you can also enter the UNLOCK selection criterion before terminating TSSTRACK to unlock the terminal.

RESUME

Allows TSSTRACK processing to continue after a pause caused by the HOLD parameter.

```
RESUME
```

Note: If desired, other selection criteria can be entered with RESUME. RESUME is valid only at 3270 terminals under TSO, and in interactive mode under CICS. It is ignored if entered from a non-3270 terminal.

SCROLL

Specifies whether output is to be paged forward as necessary to accommodate new tracking information. If SCROLL is omitted, a default of YES is used for 3270 terminals; NO for non-3270 terminals.

```
SCROLL(NO|YES|##)
```

NO

Display is to be paged forward only when the ENTER key is pressed.

Due to the overhead involved with SCROLL(NO) in CICS, it is recommended that you use YES.

YES

Display is to be paged forward automatically when there is no more space on the screen for the new output.

In CICS interactive mode, YES will page forward when the ENTER key is pressed.

##

Display is to be paged forward automatically when there is no more space on the screen for the new output line. After scrolling forward, TSSTRACK will wait before scrolling to the next screen.

SIDCOL

Specifies the column of the SMF-ID from which the one-character CPU identifier is taken for the TSSTRACK display.

```
SIDCOL(#)
```

#

The SMF ID column number. The default is 4. For example, if the SMF-ID is “XAE1” and SIDCOL(4), TSSTRACK will display “1”. If SIDCOL(2) was specified, TSSTRACK would display “A.”

SIGNAL

Specifies whether the audible alarm is to be sounded each time information about a new event is written to the terminal. If SIGNAL is omitted, a default of ON is used.

```
SIGNAL(OFF|ON)
```

OFF

The audible alarm feature is to be suppressed.

ON

The audible alarm is to be sounded each time information about a new event is written to the terminal.

Note: The SIGNAL selection criterion is ignored when entered from terminals not equipped with the audible alarm feature.

STOP

Terminates TSSTRACK.

```
STOP[(hhmm)]
```

hhmm

Under TSO only, specifies the time when TSSTRACK is to terminate. If the time is less than the current time, TSSTRACK will stop at that time on the next day.

When STOP is entered or when the STOP time is reached, the following message is issued:

```
ONLINE TRACKING TERMINATED
```

Note: No other selection criteria should be entered with STOP if no STOP time is specified. This selection criterion cannot be used in continuous mode under CICS.

SYSID

Specifies the SMF identifier of the system for which tracking information is to be displayed. If SYSID is omitted, tracking information is displayed for all systems.

```
SYSID(smfid)
```

smfid

SMF identifier of system for which tracking information is to be displayed.

TIME

Specifies the starting time for the tracking information display.

```
TIME(hhmm)
```

hhmm

Starting time (in hours and minutes) for the tracking information display.

If TIME is omitted, the current time is used as the starting time if the DATE selection criterion has not been specified. If DATE has been specified, the starting time is 12 a.m. on the date specified.

Note: Specifying the TIME selection criteria sets the SCROLL control option value to NO, unless SCROLL is specified after the TIME selection criteria.

UNLOCK

Unlocks the terminal after the password is entered.

```
UNLOCK
```

Message TSS8176A, requesting a password, is issued.

WIDTH

Specifies the maximum number of columns that may be used on the 3270 screen. If WIDTH is omitted, a default of 80 is used.

```
WIDTH(nnn)
```

nnn

Maximum number of columns that may be used. May be an integer between 80 and 132.

TSSTRACK Report Description

The examples below illustrate various ways that TSSTRACK can be used.

- Provide tracking information for all security events logged from 5 p.m. until the current time is reached. When the current time is reached, the TSSTRACK selection criteria/control options prompt is displayed. The display is to be positioned to the first event logged during this period and is to be scrolled forward only when the Enter key is pressed. Hardcopy of the display should be produced and routed to SYSOUT class A when TSSTRACK terminates.

  ```
  TIME(1700) SCROLL(NO) HARDCOPY
  ```

- Provide tracking information for all security violations logged in the last two days on System 033E. The display should be positioned to start with the first event logged during this period and should be scrolled forward only when the Enter key is pressed. No hardcopy is to be produced.

  ```
  DATE(-2) SYSID(033E) EVENT(VIOL) SCROLL(NO)
  ```

- Provide tracking information for all TSO events logged from the current date and time until TSSTRACK terminates or alternate selection criteria are entered. The Audit/Tracking File should be examined every 60 seconds for new events.

  ```
  EVENT(ALL) FACILITY(TSO) INTERVAL(60)
  ```

TSSTRACK Report

The following fields are displayed in the output of TSSTRACK.

dd/mm/yy

Date on which tracked events shown occurred (line two of heading). Heading line 1 contains the current date and time to the right.

One-character system identifier. Taken from the CPUs SMF-ID on which the event occurred. See SIDCOL option.

An asterisk (*) in column 2 of the display line indicates a new event.

TIME

Time at which tracked event occurred.

VC

Accumulated violation count since start of session for ACID associated with tracked event.

JOB/USR

Name of batch job, started task, or user responsible for tracked event.

FFM

A one- or two-character identifier for the facility (FF) and a one-character identifier for the security mode (M) involved. Facility codes are:

- B=BATCH
- C=CICSPROD
- I=IMSPROD
- K=CICSTEST
- N=NCCF
- S=STC
- T=TSO
- V=VM
- X=IMSTEST
- Security modes are:
- D=DORMANT
- F=FAIL
- I=IMP
- W=WARN

ACIDNAME

Name of ACID associated with user or job responsible for tracked event.

RDR/TERM

JES reader or online terminal associated with tracked event.

DRC

Detailed error reason code or one of the following:

- OK-Incident was logged without violation
- OKA-Incident was audited without violation
- OKB-Incident was audited because of security bypass

Information about the detailed error reason code can be obtained by using the DRC selection criterion. An asterisk in column two of the display line indicates a new event.

R/ACCESS/A

Access level requested (R) and allowed (A). TSSTRACK attempts to find an exact match between the requested/allowed access level with the bit-map access level label supplied for the RDT definition of the requested resource. If no matching label is found, the binary access level is placed into the report, preceded by an asterisk. If a matching label is found, the first four characters of the RDT access-level label are reported, unless the access label is one of these standard access levels:

- ALOG=AUTOLOG
- ALTR=ALTER
- BRWS=BROWSE
- CREI=CREATEIN
- CRTB=CRETAB
- CRTE=CREATE
- CRTS=CRETS
- CTRL=CONTROL
- DELT=DELETE
- LOGN=LOGON
- IMGC=IMAGCOPY
- INDX=INDEX
- INSR=INSERT
- NSHR=NOSHR
- PKAD=PACKADM
- RCVR=RECOVDB
- SCRT=SCRATCH
- SLCT=SELECT
- SRGL=SURROGATE
- UPDT=UPDATE

SEC

Security driver identifier:

- ADA=DATABASE
- BLP=OPEN-TAPE-BLP
- CAT=CATALOG-MANAGEMENT
- CRE=CREATE-DSN
- DES=DATA-ENCRYPTION
- EOV=OPEN-EOV
- FAP=FETCH-ACCESS-PROTECTION
- FEV=FORCE-EOV
- HSM=IBM/HSM
- INC=RACINITC
- INI=JOB/STC/SESSION START
- INY=RACINITY
- LCF=TRANSACTION
- LST=IMS/CICS-INITIATION
- OPJ=OPEN-TYPE-J
- OPN=OPEN
- REN=RENAME-DSN
- SCR=DELETE-DSN
- SUB=SUBMIT
- TMS=TAPE-MANAGEMENT
- TRM=JOB/STC/SESSION TERMINATION
- USS=UNIX SYSTEM SERVICES
- VSM=VSAM
- ??=HEXADECIMAL-SVC-NUMBER.

PROGRAM

Name of program in control when tracked event took place.

RES/CLS/NAME

A resource class code, followed by the resource name. The first four characters of the resource class are used as the resource class code, with the following exceptions:

- APCL=APPCLU
- APPL=APPL
- CCCM=CACCFMEM
- CCFD=CACCFDSN
- DBD =DBD
- DSN =DATASET
- DB2 =DB2
- D2BF=DB2BUFFP
- D2DB=DB2DBASE
- D2PL=DB2PLAN
- D2ST=DB2STOGP
- D2SY=DB2SYS
- D2TB=DB2TABLE
- D2TS=DB2TABSP
- FLD =FIELD
- PNL =PANEL
- SMSG=SMESSAGE
- SUB =ALT-ACID
- TSOG=TSOPRFG
- TSOT=TSOAUTH
- TST =TST
- VOL =VOLUME
- VXFI=VXFILE
- VTAP=VTAMAPPL
- VXDV=VXDEVICE
- USRL=USERLOG
- WRTR=WRITER
- XACT=TRANSACTION

On an 80 character screen, *BELOW* appears in the RES/CLS/NAME column indicating that the remaining resource information is displayed in the next line.

ORIGINAL RESOURCE CLASS

Displays the original eight-character resource class before it was translated during the security check to the resource class displayed in the prior line. This line is displayed only:

- On a type=LONG audit report
- If a resource class translation has been performed

Altering CPU Identifiers Used in Tracking Display

By default, the CPU identifier used in the TSSTRACK Information Display is obtained from the last character of the CPU's SMF identifier. The SIDCOL option lets you specify another column from which to obtain the CPU identifier. If this is not acceptable, your site may supply its own identifiers by zapping CSECT TSSTRAKT in the TSSTRAK0 module.

TSSTRAKT consists of 100 five-byte constants in the form:

xxyyyyyyyy

xx

The tracking information display identifier for the CPU.

yyyyyyyy

The SMF identifier of the CPU.

Note: Both xx and yyyyyyyy are in hexadecimal format.

An optional APAR is available in the FIXLIB data set of the maintenance tape. This APAR contains ASIS VER and REP statements for altering how TSSTRACK reports the CPU SMF identifier.

00	4040404040	
00	xxyyyyyyyy	replacement ID for 1st CPU
05	4040404040	
05	xxyyyyyyyy	replacement ID for 2nd CPU
0A	4040404040	
0A	xxyyyyyyyy	replacement ID for 3rd CPU
0F	4040404040	
0F	xxyyyyyyyy	replacement ID for 4th CPU
14	4040404040	
14	xxyyyyyyyy	replacement ID for 5th CPU

19	4040404040	
19	xxyyyyyyyy	replacement ID for 6th CPU
1E	4040404040	
1E	xxyyyyyyyy	replacement ID for 7th CPU
23	4040404040	
23	xxyyyyyyyy	replacement ID for 8th CPU

Error messages and abend codes can be found in the *Messages and* Codes guide.

TSSTRACK Return Codes

The program Return Code is placed in register 15 at termination; when TSSTRACK is executed under TSO, this value is available through the &LASTCC variable.

Code	Description
0	Execution successful
4	Undefined user, CA Top Secret inactive, Audit File(s) empty
8	User has insufficient authority
12	TSSTRACK Initialization error
16	Unable to open Audit data set
20	No records found in Audit data set
24	I/O error accessing Audit data set
28	Audit data set not formatted by TSSMAINT
32	Insufficient storage for internal buffers
36	Unable to establish TSO attention exit

Chapter 3: TSSAUDIT Utility

This section contains the following topics:

How to Monitor Security File Changes and Other Sensitive Data

The TSSAUDIT batch utility allows an auditor to monitor changes to the CA Top Secret security file and monitor other sensitive MVS data. The type of security information depends on the control statements that you specify.

For example, you can use TSSAUDIT to perform the following tasks:

- List security information about modules in Authorized Program Facility (APF) libraries.
- List all changes to ACIDs or list changes during a range of dates or times.
- List MVS information about site-written Supervisor Calls (SVCs), the Program Properties Table (PPT), and Terminal Monitor Program (TMP) authorized program lists.
- List security file information about one or more ACIDs (including attributes and privileges).

To use TSSAUDIT to monitor security file changes and monitor other sensitive data:

1. Ensure that you have authority to use TSSAUDIT (see page 108).
2. Assemble JCL for the TSSAUDIT job (see page 109).

   JCL includes the following components:

   - DD statements
   - Control statements
3. Submit the JCL to execute TSSAUDIT.

   TSSAUDIT provides output based on your specifications.

More information:

Sample Control Statements (see page 118)
Sample TSSAUDIT Listings (see page 119)

Authority (TSSAUDIT)

The following authorities are required for TSSAUDIT control statements:

APF

Requires PROGRAM(REPORT) administrative authority and must be executed by an SCA type ACID.

CHANGES

Requires ACID(REPORT) and RESOURCE(REPORT) authority.

MVS

Requires PROGRAM(REPORT) administrative authority and must be executed by an SCA type ACID.

PRIVILEGES

Requires ACID(REPORT,AUDIT) and RESOURCE(REPORT) authorities.

A user with none of the above administrative authorities may use TSSAUDIT if given USE access to entity TSSUTILITY.TSSAUDIT in the CASECAUT resource class.This access is granted by an administrator using the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSAUDIT) ACCESS(USE)
```

TSSAUDIT JCL

JCL for using TSSAUDIT in batch is outlined below. Sample listings for TSSAUDIT appear at the end of this chapter.

```
//STEP1        EXEC PGM=TSSAUDIT[,PARM='control statement(s)'
//AUDITOUT     DD SYSOUT=*
//RECOVERY     DD DSN=name.of.recovery.file,DISP=SHR
//ddname       DD DSN=name.of.apf.file,DISP=SHR
//AUDITIN      DD *
   TSSAUDIT control statement(s)
/*
```

The use of each of the above DD statements is described next.

AUDITIN

Defines an input data set containing TSSAUDIT control statements. This data set is normally included in the input stream, but can also be a sequential data set or member of a PDS. The following DCB attributes are set by TSSAUDIT and cannot be changed: DSORG=PS and LRECL=80. Block size may be any multiple of 80.

AUDITOUT

Defines an output data set containing messages issued by TSSAUDIT. This data set can be assigned to a printer, tape volume, or DASD volume. The following DCB attributes are set by TSSAUDIT and cannot be changed: DSORG=PS, RECFM=FBA, LRECL=133, and BLKSIZE=1330.

ddname

Defines an input data set to be processed as specified in one or more APF control statements. No DCB attributes should be specified. This DD statement is required only when the APF control statement is specified with the DDNAME operand. Multiple data sets may be concatenated.

RECOVERY

Defines an input data set containing the CA Top Secret recovery file. DCB attributes should not be specified. This DD statement is required only when the CHANGES control statement is specified.

Control statements can be entered in the PARM field of the EXEC statement and/or as input in the AUDITIN DD statement.

If the AUDITIN data set is not used, its DD statement must be specified as follows:

```
//AUDITIN  DD DUMMY
```

Control statements in the AUDITIN data set must begin in column 1.

APF

Lists information about one or more load modules residing in authorized libraries.

CHANGES

Lists changes made to the CA Top Secret Security File. Only changes made by an administrator within the scope of the ACID running the utility are reported.

MVS

Lists information about site-written SVCs, the Program Properties Table (PPT), and the Terminal Monitor Program's authorized program lists.

PRIVILEGES

Lists Security File information about one or more ACIDs. Only privileges for ACIDs within the scope of the ACID running the utility are reported.

APF Control Statement

The APF control statement generates a two-part report that displays:

- A list of data sets contained in:
  - SYS1.LPALIST
  - Live dynamic APF list
  - Live dynamic LLA list

  The data sets in these lists can be located on the specified volumes. Data sets whose volumes do not exist or that cannot be located on the volume will be omitted from consideration.
- A list of authorized programs (AC=1) within each reported partitioned data set (PDS) in the above list. Although the program will tolerate PDS/E's, it does not support member lists for such libraries.

The APF control statement may take any of the following formats:

APF

TSSAUDIT searches modules on SYSI1.LPALIB (by default) as well as any libraries in the current dynamic-APF list.

APF DDNAME(xx)

TSSAUDIT searches modules in the library specified by the filename specified in the DDNAME operand. The DDNAME for this specification is expected to reference a PDS of RECFM=U, containing load modules.

APF PARMLIB

TSSAUDIT searches modules from libraries specified in the local SYS1.PARMLIB members (IEAAPFnn and LNKLSTnn)

APF PARMLIB DDNAME(xx)

TSSAUDIT searches modules from libraries specified in a specific PARMLIB (not necessarily the one in use where the utility is being executed). The DDNAME for this specification is expected to reference a fixed length 80-character record partitioned data set.

The following is the APF control statement syntax:

```
APF <DDNAME=xx> <{PARMLIB          }> <DUMPALL|STRING(charstrg)|ZAPPED>
                <{MEMBER(*|module)}>
```

Use the following operands with this syntax:

DDNAME

If PARMLIB is specified, it refers to a copy of SYS1.PARMLIB to be searched for static LPALSTxx members and LNKLSTxx members. The data sets provided in these static lists will then be searched for load modules and reported for their audit characteristics. This file is expected to be an 80-character length partitioned data set.

If PARMLIB is not specified, it refers to a load library (a partitioned data set of RECFM=U) to be searched and reported on specifically.

PARMLIB

Specifies the list of data sets to be searched for load modules is to be taken from the current SYS1.PARMLIB (when no DDNAME is specified) or from a copy of another system's SYS1.PARMLIB (when DDNAME is specified and references the parmlib to be searched). PARMLIB is mutually exclusive with MEMBER.

MEMBER

Specifies all modules are to be searched (*) or a specific module is to be searched. MEMBER is mutually exclusive with PARMLIB.

DUMPALL

All CSECTS in each module are to be listed in the report.

STRING

Only modules containing the specified character string (“charstrg”) are to be reported in the second part of the report. The character string must consist of alphanumeric characters and must not be enclosed in apostrophes or quotes.

ZAPPED

Only modules whose IDR count is greater than zero will be listed.

CHANGES Control Statement

Use the CHANGES control statement to list changes made to the CA Top Secret security file.

Note: You can list only changes that are within your scope. For example, a VCA can list changes for his or her division and all departments within his or her division.

This control statement has the following format:

```
            [CA(acid)]
CHANGES     [DATE(yyddd|yyddd,yyddd|-nn|-nn,-nn|TODAY)]
            [TIME(hhmmss|hhmmss,hhmmss)]
            [STRING(string)]
```

CA(*acid*)

Lists only security file changes that were made by the control ACID that you specify. Omitting this entry lists *all* changes.

DATE(*yyddd*|*yyddd*,*yyddd*|*-nn*|*-nn*,*-nn*|TODAY)

Selects records based on a date or range of dates. Omitting DATE lists *all* changes made from the beginning date of the recovery file.

Note: Specifying DATE and TIME concurrently displays only records that are within *both* the date range and time range.

DATE(*yyddd*[,*yyddd*])

Specifies a specific date or range of dates (in Julian format) from which to select records. Specifying only one date selects records that are produced from that date through the current date. Specifying two dates creates a range that selects records that are produced between the specified dates.

To select records that are produced on a single day, specify the same value for both *yyddd* entries.

DATE(*-nn*)

Specifies a value from -00 to -99, which subtracts the specified number of days from the current date (to create a start date). This specification produces a report that includes records from the start date through the current date.

Example: Specify DATE(-01) to use yesterday as a start date and produce a report that includes records from yesterday through today.

DATE(*-nn*,*-nn*)

Specifies a set of values (each value between -00 to -99) to select records that are produced on the two relative dates and produced during the time between the dates.

Example: Specify DATE(-60,-40) to select all records that were produced between 60 days ago and 40 days ago.

DATE(TODAY)

Specifies to select records from today.

TIME(*hhmmss*[,*hhmmss*])

Selects records that are produced at a specific time or during a specific time period (up to but not including 24 hours). Specifying only one time selects the records that are produced from that time through the end of the 24-hour period. Specifying two times selects all records that are produced between those times. Omitting TIME lists all changes that are made in a 24-hour period (000000 to 235959).)

Note: Specifying DATE and TIME concurrently displays only records that are within *both* the date range and time range.

To select records that are produced at a specific time, specify the same value for both *hhmmss* entries.

Example: Specify TIME(181500,181500) to select records that are produced at 6:15 p.m.

Important! You *cannot* produce a single report that spans days. For example, to select all records produced between 6:00 p.m. yesterday and 6:00 a.m. today, you must produce multiple reports by using the following specification:

```
TIME(180000) DATE(-01,-01)
TIME(000000,060000) DATE(TODAY)
```

STRING(*string*)

Lists only the changes that contain the specified string entries.

Because TSSAUDIT reads the entire CA Top Secret recovery file into memory when the CHANGES control statement is specified, you might need to increase the REGION size. Insufficient storage is indicated by a U2719 abend.

Example: Report Changes Based on a Specific Time

This example generates a report on all security file changes that were made at 8:00 a.m. and later (within a 24-hour period) for all days on and after the date that the recovery file started:

```
CHANGES TIME(080000)
```

Example: Report Changes Based on a Time Period

This example generates a report on all security file changes that were made from 8:00 a.m. to 4:00 p.m. for all days on and after the date that the recovery file started:

```
CHANGES TIME(080000,160000)
```

Example: Report Changes Based on a Date in the Past

This example produces a report on all security file changes that occurred yesterday:

```
CHANGES DATE(-01,-01)
```

Example: Report Changes Based on a Specific Date

This example produces a report on all security file changes that occurred on May 4, 2012:

```
CHANGES DATE(12124,12124)
```

Example: Report Changes Based on a Date Range

This example produces a report on all security file changes that occurred between 14 days ago and 7 days ago.

Note: You can also specify two specific dates in Julian format.

```
CHANGES DATE(-14,-07)
```

MVS Control Statement

Lists information about site-written Supervisor Calls (SVCs), the Program Properties Table (PPT), and the Terminal Monitor Program's (TMP) authorized program lists.

```
MVS
```

There are no operands for this control statement.

The MVS option is only valid when issued by an SCA or an MSCA.

PRIVILEGES Control Statement

Lists Security File information about one or more ACIDs.

```
PRIVILEGES [SHORT]
```

SHORT

Information is listed only for those ACIDs that have administrative authority or any of the following attributes or privileges:

Abbreviation	Attribute
ASUS/SUSP	Administrative SUSPEND/SUSPEND ACID

Abbreviation	Attribute
AUD	AUDIT attribute
CONS	CONSOLE attribute
DUFU	DUFUPD attribute
DUFX	DUFXTR attribute
GAP	GAP attribute on profile
LDS	LDS Attribute
MRO	MRO attribute
MPW	MULTIPW attribute
NADS	NOADSP attribute
NATS	NOATS attribute
NDSN	NODSNCHK privilege
NLCF	NOLCFCHK privilege
NPWC	NOPWCHG attribute
NRES	NORESCHK privilege
NSUB	NOSUBCHK privilege
NSUS	NOSUSPEND privilege
NVMD	NOVMDCHK privilege
NVOL	NOVOLCHK privilege
OID	OIDCARD attribute
PSUS	Password SUSPEND
REST	RSTDACC attribute
TMPW	TSOMPW attribute
TRA	TRACE attribute
VSUS	Violation SUSPEND
XSUS	Installation Exit SUSPEND

In the listing produced by the PRIVILEGES control statement, underlining of attributes indicates that the attributes are in a profile to which the specified ACID is attached. If the PRIVILEGES control statement is specified, you must be the MSCA or have the following administrative authority:

```
TSS ADMIN (Auditor's acid)
          ACID(REPORT,AUDIT)
          RESOURCES(REPORT,AUDIT)
```

Sample Control Statements

- All Security File changes made in the past five days by the ACID named PAYROLL are listed.

```
//STEP1          EXECPGM=TSSAUDIT
//AUDITOUT   DD      SYSOUT=*
//RECOVERY   DD      DSN=TOP.SECRET.RECOVERY,DISP=SHR
//AUDITIN    DD      *
  CHANGES CA(PAYROLL) DATE(-05)
/*
```

- All Security File changes that included the string “CICS” are listed. Note that the CHANGES control statement is specified in the PARM field. Because no control statements are included in the AUDITIN data set, it is allocated as DUMMY.

```
//STEP1          EXECPGM=TSSAUDIT,
//           PARM='CHANGES STRING(CICS)'
//AUDITOUT   DD      SYSOUT=*
//RECOVERY   DD      DSN=TOP.SECRET.RECOVERY,DISP=SHR
//AUDITIN    DD      DUMMY
```

  Note that the recovery file is a wrap-around file and that historical data requested could have been overlaid. It is important to assure that your recovery file is sufficiently large, and your backup procedures are sufficiently robust, to assure that recovery data is never lost. It is the administrator's responsibility to assure that requested data for reporting is present on the RECOVERY file specified.

- Control statements are included in both the PARM field and the AUDITIN data set. The CHANGES control statement in the PARM field requests that all Security File changes made on the current date by the ACID named CORP are to be listed. The APF control statement in the AUDITIN data set requests that all modules in the data set identified by the DDNAME operand be searched for the string “ZAP”. All records found with that string are to be listed. The search is to include all control sections within each module.

```
//STEP1          EXECPGM=TSSAUDIT,
//           PARM='CHANGES CA(CORP)'
//AUDITOUT   DD      SYSOUT=*
//RECOVERY   DD      DSN=TOP.SECRET.RECOVERY,DISP=SHR
//LPALIB     DD      DSN=SYS1.LPALIB,DISP=SHR
//AUDITIN    DD      *
  APF DDNAME(LPALIB) MEMBER(*) STRING(ZAP) DUMPALL
/*
```

- The APF control statement requests that all modules in the data set identified by the DDNAME operand that have had zaps applied to them be listed.

```
//STEP1          EXECPGM=TSSAUDIT
//AUDITOUT   DD      SYSOUT=*
//LINKLIB    DD      DSN=SYS2.LINKLIB,DISP=SHR
//AUDITIN    DD      *
  APF DDNAME(LINKLIB) ZAPPED
/*
```

Error messages and abend codes for TSSAUDIT can be found in the CA Top Secret *Messages and Codes.*

Sample TSSAUDIT Listings

The following pages contain sample output listings of TSSAUDIT using various control statements. The samples consist of:

- Two listings of modules residing in an APF library.
- A listing of changes.
- Three listings produced when using MVS control statements.
- A listing of Privileges and Attributes.

Samples in an APF Library

```
APF DDNAME(ddname) MEMBER(*) ZAPPED
INCOMING PARAMETER ===>      APF DDNAME(APFLIB) MEMBER(*) ZAPPED
SECURITY V9.0              AUDIT UTILITY          10/30/06   08:50:07    PAGE 002

                                                                 -------------
-APF AUDIT FOR LIBRARY: SYS1.LINKLIB                                VOLUME: MV22 B

MEMBER   AC1   1ST-CSECT  LINKDATE  ZAPCOUNT                      PRINTABLE DATA
=======  ===   =========  ========  == ========================================

$SPCPUID       $SPCPUID    03/06/00   1  F.KRUER    3/85... SPCPUIDIS  LOADED BY SPSYSCPU
  S1071215  YES  S1071215  08/20/00   3  MIT S1071215SP 2.1.52USE  R MOD08/20/8711.44
CAJ2107100CAJ 21071SP 2.1.508/20/8711.44 C0
  S2471215  YES  S2471215  08/20/00   3  MIT S2471215SP 2.1.52USE  R MOD08/20/8711.41
CAJ2X47100CAJ 2X471SP 2.1.508/20/8711.41 C0
  S2671215  YES  S2671215  08/20/00   3  MIT S2671215SP 2.1.52USE  R MOD08/20/8711.42
CAJ2X67100CAJ 2X671SP 2.1.508/20/8711.42 D
  S2771215  YES  S2771215  08/20/00   3  MIT S2771215SP 2.1.52USE  R MOD08/20/8711.43
CAJ2X77100CAJ 2X771SP 2.1.508/20/8711.43 C0
                                    TSS8126E MEMBER NOT FOUND
```

The following information is displayed on the report.

MEMBER

Lists name of the specific PDS member. (If "*" is used the names for all the members are listed.) If MEMBER operand is not specified, all modules flagged with AC1 is listed in this column.

AC1

If YES, indicates that the particular member was linked with SETCODE AC(1).

1ST-CSECT

Lists the name of the first control section (CSECT). When DUMPALL is specified, the remaining CSECT names are also included.

LINKDATE

Lists the date on which the module was last link-edited.

ZAPCOUNT

The number of superzaps applied to the module.

PRINTABLE DATA

Displays the first 80 bytes of printable data. This should be examined to detect peculiarities. When the STRING option is specified, only those entries with printable data matching the string are listed.

APF DDNAME(ddname) PARMLIB

```
INCOMING PARAMETER ===>    APF DDNAME(PARMLIB) PARMLIB
V9.0     AUDIT UTILITY  10/30/06   09:04:19   PAGE 002
-  ----- LISTING OF APF LIBRARIES TO BE SEARCHED ----

   ORIGIN               VOLSER    LIBRARY
   ======    ========================================

   PARMLIB(IEAAPFLQ)    MVSPP0    ISF.V2R2.MVS217.R3380K.LOAD
   PARMLIB(IEAAPFLQ)    MVSPP0    ISP.V2R3M0.ISPLOAD0
   PARMLIB(IEAAPFLQ)    MVSPP0    ISR.V2R3M0.ISRLOAD0
   PARMLIB(IEAAPFLQ)    MVSPP0    SYS2.SDSF21.LINKLIB
   PARMLIB(IEAAPFLQ)    MVSPP0    SYS2.SYSPROG.LINKLIB
   PARMLIB(IEAAPFLQ)    MV217A    SYS1.CMDLIB
   PARMLIB(IEAAPFLQ)    MV217A    SYS1.LINKLIB
   PARMLIB(IEAAPFLQ)    MV217A    SYS1.LPALIB
   PARMLIB(IEAAPFLQ)    MV217A    SYS1.SVCLIB
   PARMLIB(IEAAPFLQ)    MV217A    SYS1.VTAMLIB
   PARMLIB(IEAAPFLQ)    MV217A    SYS2.LPALIB
   PARMLIB(IEAAPFLQ)    MV217B    SYS1.CMDLIB
   RMLIB(IEAAPFLQ)      MV217B    SYS1.LINKLIB
   PARMLIB(IEAAPFLQ)    MV217B    SYS1.LPALIB
   PARMLIB(IEAAPFLQ)    MV217B    SYS1.SVCLIB
   PARMLIB(IEAAPFLQ)    MV217B    SYS1.VTAMLIB
   PARMLIB(IEAAPFLQ)    MV217B    SYS2.LPALIB
   PARMLIB(IEAAPFLQ)    MVSPP0    SYS3.VTAMLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.CMDLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.LINKLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.MLPALIB
   PARMLIB(IEAAPFLQ)    MVSCAT    SYS2.MVSSYS.LPALIB
   PARMLIB(IEAAPFLQ)    MVSCAT    SYS2.MVSSYS.LINKLIB
   PARMLIB(IEAAPFLQ)    MVSSYS    SYS2.NCPLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.NCPLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.PPLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.SSPLIB
   PARMLIB(IEAAPFLQ)    MVXE14    SYS2.TSS.SSA.LOAD
   PARMLIB(IEAAPFLQ)    MVXE14    QUEEL01.TEST.LOAD
   PARMLIB(IEAAPFLQ)    MVXE14    SYS2.XDC15.LOAD
   PARMLIB(IEAAPFLQ)    MVXE14    SYS2.MVSXE14.LINKLIB
   PARMLIB(IEAAPFLQ)    MVSLIB    SYS2.VTAMLIB
   PARMLIB(IEAAPFLQ)    MVSSYS    USER.LINKLIB
   PARMLIB(IEAAPFLQ)    MVSSYS    USER.MLPALIB
   PARMLIB(IEAAPFLQ)    MVXE14    CAI.CAILIB
   PARMLIB(IEAAPFLQ)    XXXXXX    XXXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXX
   PARMLIB(IEAAPFLQ)    ZZZZZZ    ZZZZZZZZ.ZZZZZZZZ.ZZZZZZZZ.ZZZZZZZZ.ZZZZZZZ
   PARMLIB(IEAAPFMI)    IMSRES    IMS130X.RESLIB
```

```
PARMLIB(IEAAPFMI)    IMSRES    IMS130X.MATRIXA
PARMLIB(IEAAPFMI)    IMSRES    IMS130X.MATRIXB
PARMLIB(IEAAPFMI)    IMSRES    IMS130X.MODBLKSA
PARMLIB(IEAAPFMI)    IMSRES    IMS130X.MODBLKSB
PARMLIB(IEAAPFMI)    CICRES    CICS161A.LOADLIB1
PARMLIB(IEAAPFMI)    IMSRES    IMS130A.RESLIB
PARMLIB(IEAAPFMI)    IMSRES    IMS130A.MATRIXA
PARMLIB(IEAAPFMI)    IMSRES    IMS130A.MATRIXB
PARMLIB(IEAAPFMI)    IMSRES    IMS130A.MODBLKSA
PARMLIB(IEAAPFMI)    IMSRES    IMS130A.MODBLKSB
PARMLIB(IEAAPFMI)    MV136A    SYS1.VTAMLIB
PARMLIB(IEAAPFMI)    MV136A    SYS1.CMDLIB
```

Note: When using PARMLIB, another list follows giving all programs associated with each specified library.

The following information is displayed:

ORIGIN

Lists where the library was found.

VOLSER

Lists the volume serial number of the specified library.

LIBRARY

Lists the specific APF-authorized library.

If the APF control statement is specified, you must be the MSCA and have READ access for the data set(s) specified in the ddname DD statement.

Sample TSSAUDIT Listing of Changes

A sample listing of changes is as follows:

```
CHANGES CA(acid) DATE(-nn)
V9.0          AUDIT UTILITY                        10/30/02   08:03:36     PAGE 001
+                                                 _____________

  INCOMING PARAMETER ===>      CHANGES CA(KORDI01) DATE(-01)
V9.0          AUDIT UTILITY                        10/30/00   08:03:36     PAGE 002
+                                                 _____________
-             ----- LISTING OF CHANGES TO SECURITY FILE -----

CHANGER    DATE     TIME   SYSID TYPE                      COMMAND/IMAGE
======= ======== ======== ===== ==== ==================================

KORDI01 02/14/14 10:23:46 XE14 CMND TSS CREATE(TEDMON) DEPT(QADEPT1) TYPE(USER) NAME('TED MON')
KORDI01 02/14/14 10:24:42 XE14 CMND TSS ADD(MASTER) DSN(PAY)
KORDI01 02/14/14 10:25:12 XE14 CMND TSS PER(TEDMON) DSN(PAY.MSTR) LIB(SYS1.UTY) PRI(PAY60)
KORDI01 02/14/14 10:30:11 XE14 CMND TSS REVOKE(TEDMON) DSN(PAY.MSTR)
KORDI01 02/14/14 10:31:48 XE14 CMND TSS ADD(MASTER) DSN(SYS9.)
KORDI01 02/14/14 10:32:31 XE14 CMND TSS PER(TEDMON) LIB(SYS9.UTY) DSN(PAY.MSTR) PRI(PAY60)
KORDI01 02/14/14 10:33:55 XE14 CMND TSS REM(MASTER) DSN(SYS9.)
KORDI01 02/14/14 10:34:55 XE14 CMND TSS REV(TEDMON) DSN(PAY.MSTR)
KORDI01 02/14/14 10:35:46 XE14 CMND TSS ADD(MASTER) DSN(SYS9.)
KORDI01 02/14/14 10:36:31 XE14 CMND TSS PER(TEDMON) DSN(PAY.MSTR) LIB('SYS9.UTY') PRI(PAY60)
ADMSCA1 02/14/14 12:32:24 XE14 CMNE TSS ADD(TEDMON) SUSPEND
ADMSCA1 02/14/14 12:32:24 XE14 CMNE TSS REM(M129MG) PROFILE(SYS01P)
KORDI01 02/14/14 07:57:49 XE14 PW   TSS REP(BOBBY01) PASSWORD(????????)

-                                                ALL CHANGES WITHIN SCOPE LISTED

                                                     TSS COMMAND CHANGES = 00010
                                                        PASSWORD CHANGES = 00001
                                                         DYNAMIC UPDATES = 00000
```

The listing displays the following information:

CHANGER

Lists the ACID of the administrator who made the change.

DATE

Lists the date on which the change was made. (Date information appears in the form specified in the CA Top Secret DATE startup option.)

TIME

Lists the time at which the change was made.

SYSID

Lists the SMF identifier of the CPU on which the change was made.

TYPE

Indicates the type of change that occurred:

CMDE

Indicates that a TSS command was issued with a type 71 RACF ENF signal.

CMND

Indicates that a TSS command was issued.

PW

Indicates that a password change occurred.

COMMAND/IMAGE

Lists the TSS command—including comments—used to make the change or a simulated TSS command for PW, AVO, DUF. You can use comments on CA Top Secret administrative commands to strategically document the reason for security files changes.

A TSS command can contain UID(?) or GID(?), which instructs the product to automatically assign a USS UID or GID. In this situation, the following processing occurs:

- Instead of including the ? value in the command that appears to the recovery file record, the product includes the assigned UID or GID value. For example, TSS ADD(JONATHAN) UID(256) appears in the record instead of TSS ADD(JONATHAN) UID(?).
- If the original command contained a RANGE specification, the product removes the specification from the command that appears in the recovery file but writes a copy of the original command to the recovery file as a comment statement (for example, /*TSS ADD(Rachael) UID(?) RANGE(1000,5000) */).

Note: For complete information about using the UID and GID keywords in your TSS command syntax, see the *CA Top Secret Command Reference Guide*.

If the CHANGES control statement is specified, you must have READ access authority for the CA Top Secret recovery file. In addition, if you are not the MSCA, you must have the following administrative authority:

```
TSS ADMIN(auditor_acid) ACID(REPORT) RESOURCES(REPORT)
```

Samples Using MVS Control Statements

Three listings are produced when using the MVS control statement:

- Inventory of user SVCs.
- Contents of Program Properties Table.
- Contents of TMP Command and Program Tables.

```
INCOMING PARAMETER ===>      MVS

SECURITY V9.0            AUDIT UTILITY             10/30/02   09:27:26    PAGE 002
+
                                                    _____________
-                                            ----- MVS AUDIT FOR CPU XE14 -----
                                          INVENTORY OF USER SVC'S ON THIS SYSTEM
                                          ======================================
          SVC NUMBER   APF AUTH'Y                  PRINTABLE DATA
          ----------   ----------   ------------------------------------------
          203                   0YIPLSVC2.008/09/8523.48SOFTWARE DEVELOPED AND WRI
          223                   00IEFQB585 85105 JBB22200000000000 0 PATCH AREA IE
          224                   0FKIGC0022D1.003/24/8612.07SOFTWARE WRITTEN BY FRE
          227                   00IEFJDSNA 81.260 K KKKKKKKK00KMS0000. 0IGG0203Y.M
          241                   00SYSRUTR09/06/8415.21KJJ KJDCKJHCKJQB.CB 0BB BJKK
          252                   0NAKAKAKK00IEBCOPY
          253                   0IGC0025C08/10/8500.38 ATTACH IEBCOPY SVC 0/0 K800
```

The following information is displayed:

SVC NUMBER

Lists the interrupt number associated with each site-written SVC.

APF AUTH'Y

Lists whether SVC has APF authority which indicates potential to bypass security.

PRINTABLE DATA

Lists up to 40 bytes of printable data. (Consecutive blanks are compressed in the listing.)

Contents of Program Properties Table

The following information is displayed:

PROGRAM

Lists the PPT name.

SECURITY BYPASS

Determines whether the PPT has security bypass.

OTHER ATTRIBUTES

Lists other attributes such as storage keys, and so on. The listing for the Program Properties Table (PPT) includes the program name, whether the PPT has security bypass, and other attributes such as storage keys, and so on.

Contents of TMP Command and Program Tables

The listing for the Terminal Monitor Program (TMP) includes a list of commands followed by the program name.

Sample Listing of Privileges and Attributes

```
INCOMING PARAMETER ===> PRIVILEGES SHORT
9.0                     AUDIT UTILITY                  10/30/02   11:06:08     PAGE 002
                        ----- CROSS-REFERENCE OF PRIVILEGES AND ATTRIBUTES -----
ACIDNAME TYPE                                          ATTRIBUTES & PRIVILEGES
======== ==== ================================================================================

AUDDCA1  DCA  SUSP AUD  CONS DUFU DUFX  -   MRO  MPW  NADS NATS NDSN NLCF NPWC NRES NSUB NSUS NVMD
NVOL  -   LDS  TRA  TMPW
STRTE01P PROF  -   -   -   -   -  GAP  -   -   -   -   -   -   -   -   -   -   -   -  LDS  -   -
AUDUSR1  USER SUSP AUD  CONS DUFU DUFX  -    -    -   NADS NATS NDSN NLCF NPWC NRES NSUB NSUS NVMD
NVOL  -   LDS  TRA   -
AUDVCA1  VCA  ASUS AUD  CONS DUFU DUFX  -    -    -   NADS NATS NDSN NLCF NPWC NRES NSUB NSUS NVMD
NVOL  -   LDS  TRA   -
AUDZCA1  ZCA  SUSP AUD  CONS DUFU DUFX  -    -    -   NADS NATS NDSN NLCF NPWC NRES NSUB NSUS NVMD
NVOL  -   LDS  TRA   -
CARLX08  USER  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
CARMA01  SCA   -   -  CONS  -   -   -   -   -   -  NDSN  -   -  NRES  -   -   -   -   -   -   -  *ADMIN
CAS9    USER  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  NSUS  -   -   -   -   -   -
CCFADM   SCA   -   -  CONS  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -
CHAGE02  SCA   -  AUD   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
CICSAOR  USER  -   -   -   -   -   -   -   -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICSTOR  USER  -   -   -   -   -   -   -   -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -  LDS  -   -
CICSUSR  SCA   -   -  CONS  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
CICSU64  USER  -   -   -   -   -   -  MRO  -   -   -   -   -  NPWC  -   -   -   -   -   -   -   -   -
CICS21A  USER  -   -   -   -   -   -  MRO  -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICS21T  USER  -   -   -   -   -   -  MRO  -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICS32A  USER  -   -   -   -   -   -   -   -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICS32T  USER  -   -   -   -   -   -   -   -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICS33A  USER  -   -   -   -   -   -  MRO  -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICS33T  USER  -   -   -   -   -   -  MRO  -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CICS41A  USER  -   -   -   -   -   -  MRO  -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -  LDS  -   -
CICS41T  USER  -   -   -   -   -   -  MRO  -   -   -  NDSN NLCF  -  NRES NSUB  -   -  NVOL  -   -   -   -
CN01    USER  -  AUD   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -
CN02    USER  -  AUD   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -
CN03    USER  -  AUD   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -
CN04    USER  -  AUD   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -
COBVIS1  USER  -   -   -   -   -   -   -   -   -   -  NDSN NLCF  -  NRES  -   -   -  NVOL  -   -   -   -
CPFTEST  SCA   -   -  CONS  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  LDS  -   -  *ADMIN
DAIRO01  SCA   -   -  CONS  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
DB2SCA1  SCA   -   -  CONS  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
DB2US13  USER  -   -   -   -   -   -   -   -   -   -  NDSN  -   -   -   -   -   -   -   -   -   -   -
DB2US14  USER  -   -   -   -   -   -   -   -   -   -  NDSN  -   -   -   -   -   -   -   -   -   -   -
DORDA01  SCA   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
DORDA02  SCA   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  LDS  -   -
DUNAN01  USER  -  AUD  CONS  -   -   -   -   -   -   -  NDSN  -   -  NRES  -   -   -   -   -   -   -   -
DUTILT1  SCA   -   -  CONS  -   -   -   -   -   -   -  NDSN  -   -  NRES NSUB  -   -  NVOL  -   -   -   -  *ADMIN
HINJO01  USER  -  AUD  CONS  -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -  *ADMIN
```

The following information appears:

ACIDNAME

Lists security information for the specified ACID.

TYPE

Lists the type of ACID record.

ATTRIBUTES & PRIVILEGES

Lists any of the above-mentioned attributes that the ACID might have. If the ACID has administrative authority, *ADMIN* will appear in the last column.

Chapter 4: TSSCHART Utility

This section contains the following topics:

About the TSSCHART Utility

TSSCHART builds a tree structure of the full CA Top Secret Security File in memory consisting of control blocks representing divisions, departments, profiles, and users. This tree structure is then filtered, depending on user parameters. These parameters, which reside in the SYSIN DD file, are completely in free format and can come from a data set of any LRECL size. The tree structure is also automatically filtered according to the administrator's scope; that is, an administrator may only chart those ACIDs within his scope of authority. After the tree structure is appropriately filtered, TSSCHART "walks through" the tree, and uses the Security File to print more detailed information.

Authority and Scope (TSSCHART)

The administrator must have RESOURCE(REPORT) or ACID(REPORT) authority to run TSSCHART.

Users with no administrative authority may use TSSCHART if given USE access to entity TSSUTILITY.TSSCHART in the CASECAUT resource class. An administrator can grant this access by using the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSCHART) ACCESS(USE)
```

TSSCHART Required JCL

Required JCL for TSSCHART is as follows:

```
//TSSCHART        JOB
/*JOBPARM K=0
//CHART           EXEC     PGM=TSSCHART,REGION=0M
//SYSPRINT        DD       SYSOUT=*
//SYSIN           DD *
(options)
/*
```

SYSPRINT is the DD statement that is associated with the output for TSSCHART. SYSIN is the DD statement containing the control statements that customize the scope of TSSCHART.

Note: Specifying K=0 in the JOBPARM instructs JES to ignore line counts. Omitting K=0 distorts the continuity of the vertical chart lines; therefore, you should always specify K=0.

TSSCHART Keywords

The following principal keywords are used with TSSCHART:

- CHART
- RESOURCE
- ZONE or XZONE
- DIV or XDIV
- DEPT or XDEPT
- PROF or XPROF
- USER or XUSER
- LAYOUT
- PAGE

The optional parameters for each keyword can be separated by commas or spaces—for example, CHART(ACIDS,RESOURCE,VCA) or CHART(ACIDS RESOURCE VCA).

If the optional parameters for a keyword exceed the length of the line, end the line with a parenthesis. Begin the next line with the keyword followed by the remainder of the parameters in parentheses. An example follows:

```
DIV(div,div,div,div,.....................)
DIV(div,*EJECT*)
```

This rule applies to all keywords with multiple optional parameters that might exceed the length of the line.

Note: For information about TSSCHART error messages and abend codes, see the *Messages and Codes.*

CHART Keyword—Determine Chart Contents

The CHART keyword determines the data to include in the chart.

This keyword has the following format:

```
CHART(ACIDS,RESOURCE,STATS,SCA,LSCA,ZCA,VCA,DCA)
```

ACIDS

Includes the zone, division, department, profile, group, and user names in the chart. If supplied, profiles, groups, and users print in list format. This value is the default.

RESOURCE

Includes resource ownership elements on the chart (resources owned by the zone, division, department, profile, groups, and users). If you specify ACIDS with RESOURCE, the product omits resources owned by profiles, groups, and users, and the product prints the information in list format. If you do not specify ACIDS, profile, group, and user information—including owned resources—prints in box format.

STATS

Includes Security File statistics (for example, record sizes) with each block on the chart.

SCA

Includes resources owned by the MSCA and the SCAs on the chart. This parameter implies CHART(RESOURCE).

LSCA

Includes resources owned by the MSCA and the LSCAs on the chart. This parameter implies CHART(RESOURCE).

ZCA

Includes resources owned by zonal administrators on the chart. This parameter implies CHART(RESOURCE).

VCA

Includes resources owned by divisional administrators on the chart. This parameter implies CHART(RESOURCE).

DCA

Includes resources owned by departmental administrators on the chart. This parameter implies CHART(RESOURCE).

Example: List ACIDs and Show Records Sizes and Page Ejects

In this example, an MSCA needs a listing of all ACIDs in the Security File as well as resource ownership. In addition, the MSCA wants to know the size of the ACID records on the Security File and page ejects on new divisions.

```
CHART(ACIDS,RESOURCE,SCA,LSCA,ZCA,VCA,DCA,STATS)
DIV(*EJECT*)
```

Example: List ACIDs, List Record Sizes, and Request Separate Pages for New Divisions

In this example, an SCA only wants a chart of all ACIDs in the Security File accompanied by the record size of the ACID. The entry requests separate pages for each new division.

```
CHART(ACIDS,STATS)
DIV(*EJECT*)
```

Example: Chart All Departments Not Belonging to Divisions

In this example, an SCA needs to chart all departments not belonging to divisions:

```
CHART(ACIDS)
XDEPT(*DIV*)
```

Example: List Data Sets and Volumes Within a Division

In this example, a VCA wants to obtain a listing of data sets and volumes within his division:

```
CHART(RESOURCE)
RESOURCE(DATASET,VOLUME)
```

Example: Create a Chart with Users from Specific Departments

In this example, a VCA needs a chart containing only users in specific departments to which they belong:

```
CHART(ACIDS)
PROF(*NONE*)
DEPT(SYSTEMS)
```

Example: List Specific Divisions and Departments; List ACID and Resource Information; and Set Up Page Ejects

In this example, an SCA wants to list a particular division and the department(s) attached to it. He also needs all ACIDs and owned resources, who owns the resources, and the size of the ACID records of the Security File. A page eject will occur when a division is to be charted.

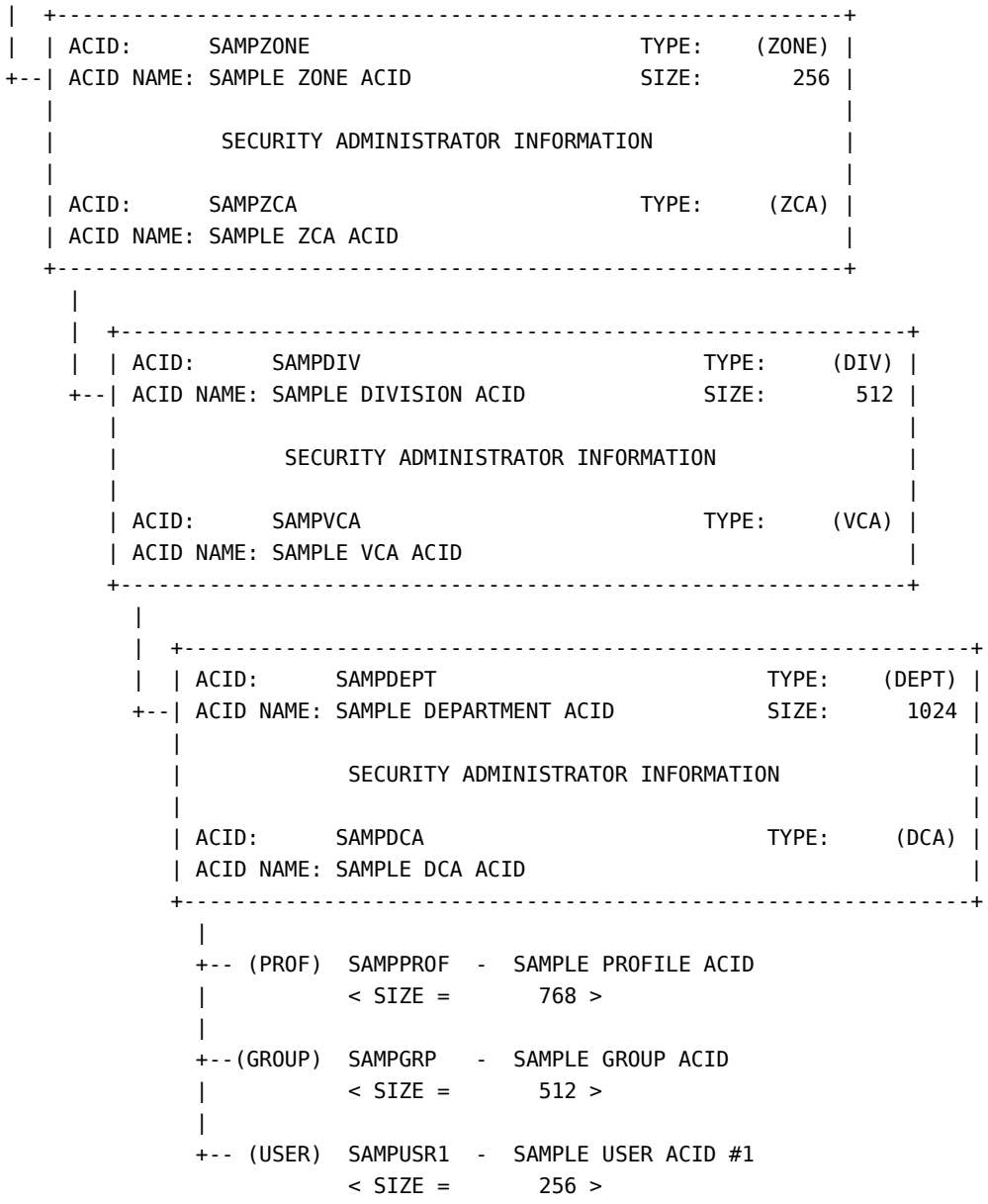
```
CHART(ACIDS,RESOURCE,VCA,DCA,STATS)
RESOURCE(ALL)
DIVISIOM(DEVLDIV *EJECT*)
DEPT(*DIV*)
```

Example: Generate List Form for Profile, Group, and User ACIDs

In this example, an SCA wants to see the ACIDs and ACID names of all records in the security file. He also wants to see record size statistics and format the output for printing in portrait layout on 8½x11in. paper.

```
CHART(ACIDS,STATS)
LAYOUT(PO)
```

After the SCA submits this JCL, the product produces the following output:



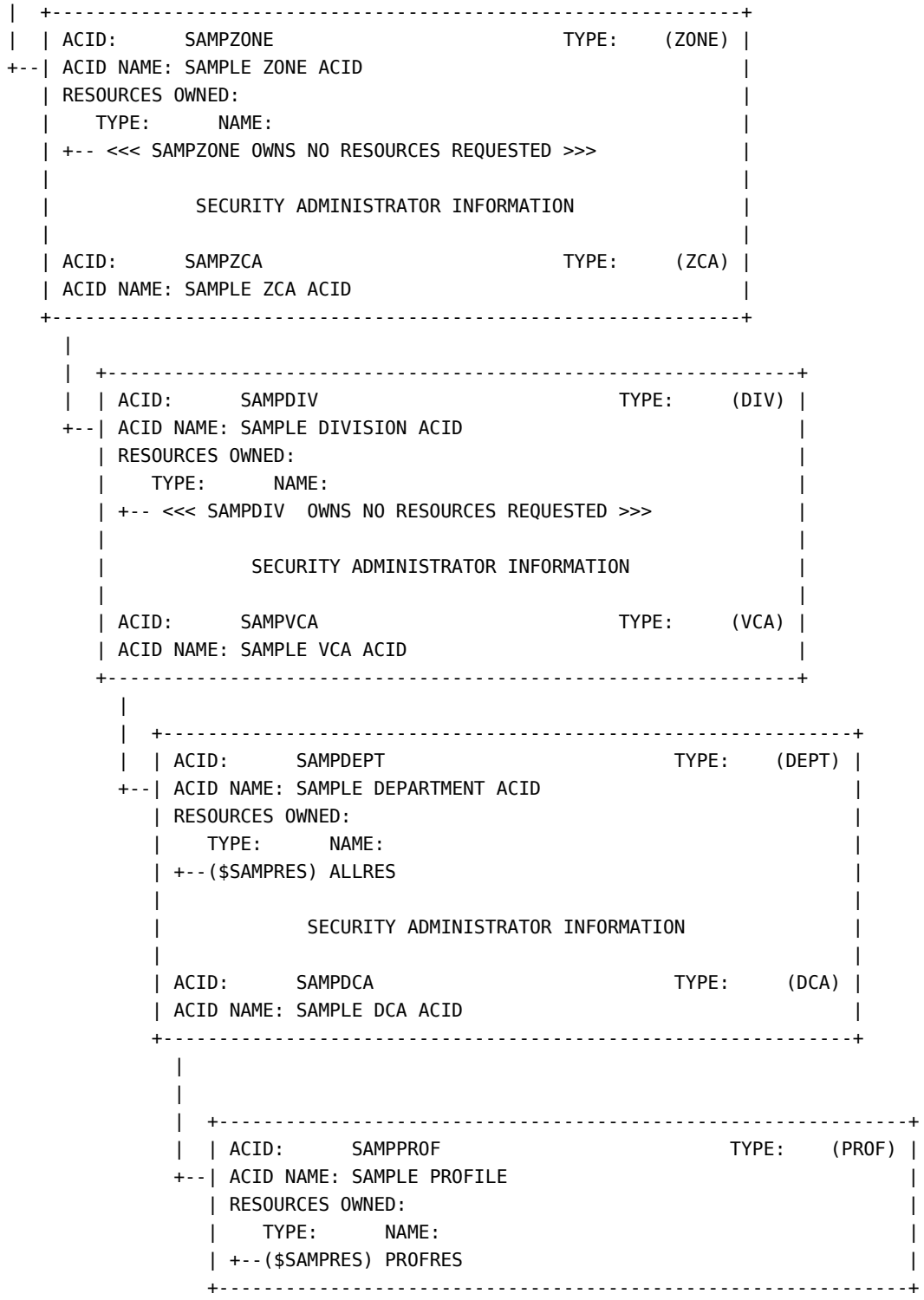
The PROF, GROUP, and USER ACIDs are listed rather than being contained in a box like the ZONE, DIV, and DEPT ACIDs. Also, the record size of the ACID is shown if CHART(STATS) is supplied. The CHART(ACIDS) keyword always produces PROF, GROUP, and USER ACIDs in this format.

Example: Generate Box Form for Profile, Group, and User ACIDs

In this example, an MSCA needs a listing of all ACIDs in the Security File as well as resource ownership for ZONE, DIV, DEPT, PROF, GROUP, and USER ACIDs:

```
CHART(RESOURCE,STATS)
```

After the MSCA submits this JCL, the product produces the following output:



The PROF ACID is contained in a box like the ZONE, DIV, and DEPT ACIDs. Also, each box for the ACIDs has its owned resources listed or an appropriate message if the ACID does not own any resources. If CHART(ACIDS) is not supplied, PROF, GROUP, and USER ACIDs always print in this format.

RESOURCE Keyword—Specify Class Resources for the Resource Chart

The RESOURCE keyword specifies the class resources to include on the resource chart.

This keyword has the following format:

```
          [  (ABSTRACT,APPLICATION,CICS,DATASET,  ]
RESOURCE  [  FIELD,GENERAL,IDMS,IMS,PROGRAM,     ]
          [  TERMINAL,TSO,VM,VOLUME,ALL)         ]
```

Note: In addition to the following parameters, you can also supply user-defined resources in the Resource Descriptor Table (RDT) as parameters to the RESOURCE keyword.

ABSTRACT

Includes abstract resources on the chart.

APPLICATION

Includes applications on the chart.

CICS

Includes CICS resources (DCT, FCT, PPT,...).

DATASET

Includes DSNAME resources.

FIELD

Includes user-defined fields.

GENERAL

Includes UR1, UR2 resources.

IDMS

Includes CA-IDMS subschemas and areas.

IMS

Includes IMS PSB and DBD resources.

PROGRAM

Includes program resources.

SMS

Includes all SMS resources.

TERMINAL

Includes terminal resources.

TSO

Includes all TSO resources.

VM

Includes all VM resources.

VOLUME

Includes volume resources.

ALL

Includes all of the above classes of resources.

If you use CHART(RESOURCE), the default is RESOURCE(ALL); otherwise, the default is RESOURCE(NONE).

PAGE Keyword—Specify Page Size

Specifies the page size for TSSCHART. This specification is useful for printing charts on non-standard size pages, because blocks will not cross page boundaries.

This keyword has the following format:

PAGE(*nn*)

nn

Specifies the page size, which can be from 01 to 99 lines per page. The default value is 66.

ZONE or XZONE Keyword—Include or Exclude Zones

The ZONE and XZONE keywords let you specify zones to include (ZONE) or exclude (XZONE) from the chart. XZONE is treated hierarchically. After a zone has been excluded, you cannot report on divisions, departments, users, or profiles that fall within the excluded zone. The acid types that can use this keyword are LSCA, SCA, and MSCA.

This keyword has the following format:

```
ZONE | XZONE(zone,...,*ALL*,*NONE*,*EJECT*)
```

zone

Includes or excludes any valid specified zone names.

ALL

Includes or excludes all zones.

NONE

Includes or excludes no zones.

EJECT

Causes a page eject at each new zone.

Note: *EJECT* must be the last item in the list or the only item.

The default is ZONE(*ALL*) or XZONE(*NONE*).

DIV or XDIV Keyword—Include or Exclude Divisions

The DIV or XDIV keyword specifies divisions to include or exclude from the chart. XDIV is treated hierarchically. After a division has been excluded, you cannot report on departments, users, or profiles that fall within the excluded division. The acid types that can use this keyword are: ZCA, LSCA, SCA, and MSCA.

This keyword has the following format:

```
DIV | XDIV(div,...,*ALL*,*NONE*,*REG*,*EJECT*)
```

div

Includes or excludes any valid specified division names.

ALL

Includes or excludes all divisions.

NONE

Includes or excludes no divisions.

REG

Includes or excludes those divisions belonging to zones.

EJECT

Causes a page eject at each new division.

EJECT must be the last item in the list or the only item.

The default is DIV(*ALL*) or XDIV(*NONE*).

Example: List ACIDs and Show Records Sizes and Page Ejects

In this example, an MSCA needs a listing of all ACIDs in the Security File as well as resource ownership. In addition, the MSCA wants to know the size of the ACID records on the Security File and page ejects on new divisions.

```
CHART(ACIDS,RESOURCE,SCA,LSCA,ZCA,VCA,DCA,STATS)
DIV(*EJECT*)
```

Example: List ACIDs, List Record Sizes, and Request Separate Pages for New Divisions

In this example, an SCA only wants a chart of all ACIDs in the Security File accompanied by the record size of the ACID. The entry requests separate pages for each new division.

```
CHART(ACIDS,STATS)
DIV(*EJECT*)
```

DEPT or XDEPT Keyword—Include or Exclude Departments

Specifies those departments to include (DEPT) or exclude (XDEPT) from the chart. XDEPT is treated hierarchically. After a department has been excluded, you cannot then report on users or profiles that fall within the excluded department. The acid types that can use this keyword are: VCA, ZCA, LSCA, SCA, and MSCA.

This keyword has the following format:

```
DEPT | XDEPT(dept,...,*ALL*,*NONE*,*DIV*,*EJECT*)
```

dept

Includes or excludes any valid specified department names.

ALL

Includes or excludes all departments.

NONE

Includes or excludes no departments.

DIV

Includes or excludes only those departments belonging to divisions.

EJECT

Causes a page eject at each new department.

Note: *EJECT* must be the last item in the list or the only item.

The default is DEPT(*ALL*) or XDEPT(*NONE*).

PROF or XPROF Keyword—Include or Exclude Profiles

The PROF and XPROF keywords specify profiles to include (PROF) or exclude (XPROF) from the chart.

The keyword specification has the following format:

```
PROF | XPROF(prof,...,*ALL*,*NONE*)
```

prof

Includes or excludes any valid specified profile names.

ALL

Includes or excludes all profiles.

NONE

Includes or excludes no profiles.

The default is PROF(*ALL*) or XPROF(*NONE*).

USER or XUSER Keyword—Include or Exclude User-Level ACIDs

The USER and XUSER keywords specify user-level ACIDs to include or exclude from the chart.

This keyword has the following format:

```
USER|XUSER(acid,...,*ALL*,*NONE*,*ONLY*)
```

acid

Includes or excludes any valid specified user-level ACID names.

ALL

Includes or excludes all users.

NONE

Includes or excludes no users.

ONLY

Shows only USER ACIDs. You can combine this parameter with *ALL* to see all USER ACIDs in the security file. You can also include a list of ACIDs to see specific users. You can use ZONE, DIV, DEPT, and PROF keywords to filter user ACIDs by ZONE, DIV, DEPT, or PROF.

Note: *ONLY* must be the last item in the list or the only item.

The default is USER(*ALL*) or XUSER(*NONE*).

Example: Show Only the SAMPUSER ACID

In this example, an administrator wants to see only the SAMPUSER ACID, including its owned resources and record size. To do, the administrator specifies the following option in the JCL:

```
CHART(resources,stats)
USER(SAMPUSER,*ONLY*)
```

This specification produces the following output:

```
+-------------------------------------------------------------+
| ACID:      SAMPUSER                          TYPE:    (PROF) |
| ACID NAME: SAMPUSER SAMPLE PROFILE                          |
| RESOURCES OWNED:                                            |
|    TYPE:      NAME:                                         |
| +--($SAMPRES) PROFRES                                       |
+-------------------------------------------------------------+
```

LAYOUT Keyword—Specify Page Layout

The LAYOUT keyword specifies the page layout for TSSCHART. This functionality is useful when printing the output of TSSCHART on standard 8½x11inch paper.

This keyword has the following format:

```
LAYOUT(LS|PO)
```

LS

Specifies to format output for landscape print on 11x8½ inch paper. When this value is supplied, the default for PAGE is 66.

PO

Specifies to format the output for portrait print on 8½x11inch paper. When this value is supplied, the default for PAGE is 66.

If LAYOUT is not supplied, the default is LAYOUT(PO).

Example: Format Output for Landscape Printing

This example formats output for landscape print on 11x8½ inch paper.

```
CHART(ACIDS,STATS)
LAYOUT(LS)
```

More information:

PAGE Keyword—Specify Page Size (see page 140)

TSSCHART Sample Executions

An MSCA needs a listing of all ACIDs in the Security File as well as resource ownership. In addition, he wants to know the size of the ACID records on the Security File and may also like page ejects on new divisions.

```
CHART(ACIDS,RESOURCE,SCA,LSCA,ZCA,VCA,DCA,STATS)
DIV(*EJECT*)
```

An SCA only wants a chart of all ACIDs in the Security File accompanied by the ACID record size. Separate pages are requested for each new division.

```
CHART(ACIDS,STATS)
DIV(*EJECT*)
```

An SCA needs to chart all departments not belonging to divisions.

```
CHART(ACIDS)
XDEPT(*DIV*)
```

A VCA decides to obtain a listing of data sets and volumes within his division.

```
CHART(RESOURCE)
RESOURCE(DATASET,VOLUME)
```

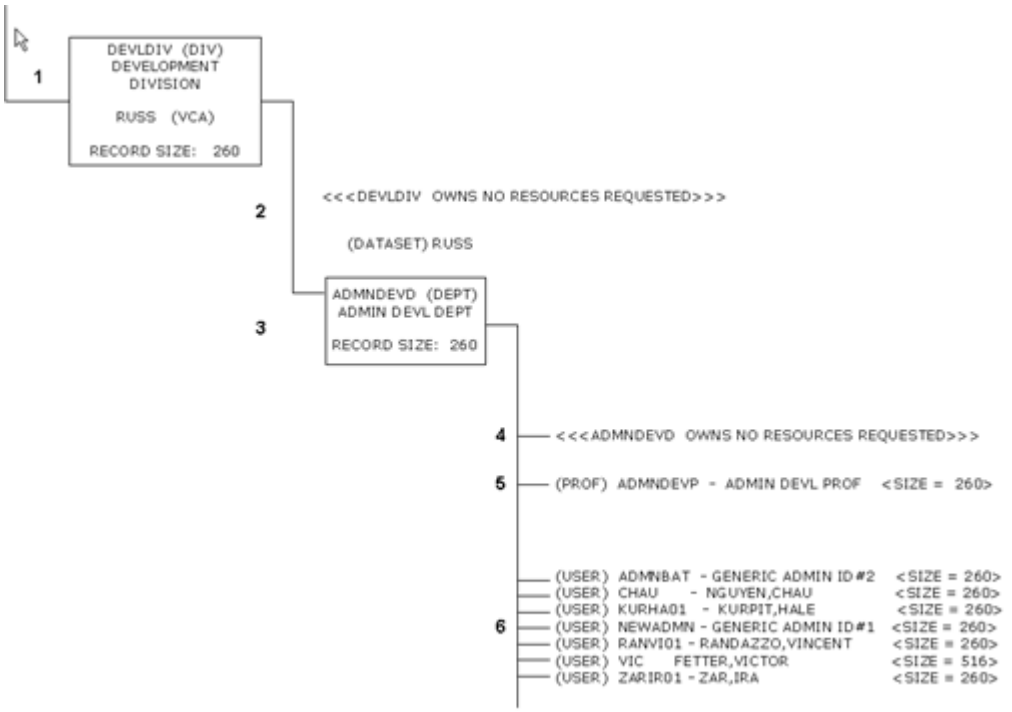
A VCA needs a chart containing only users in specific departments to which they belong.

```
CHART(ACIDS)
PROF(*NONE*)
DEPT(SYSTEMS)
```

An SCA wishes to list a particular division and the department(s) attached to it. He also needs all ACIDs and owned resources, who owns the resources, and the size of the ACID records of the Security File. A page eject will occur when a division is to be charted.

```
CHART(ACIDS,RESOURCE,VCA,DCA,STATS)
RESOURCE(ALL)
DIVISIOM(DEVLDIV *EJECT*)
DEPT(*DIV*)
```

This last sample will contain the actual output on the following page, with a description of the specific blocks on the tree structure.



The following information displays:

1. Division ACID, name of division, VCA ACID, and record size.
2. Resources owned by division as well as resources owned by VCA.
3. Department ACID, name of department, and record size.
4. Resources owned by department. Notice that TSSCHART informs you if no resources are owned that you requested.
5. Profile ACIDs, names of profiles, and record sizes.
6. User ACIDs, names of ACIDs, and record sizes.

Chapter 5: TSSCPR Utility

This section contains the following topics:

About the TSSCPR Utility

The TSSCPR utility is a batch utility that gives the user the ability to produce customized reports extracted from the CPF Recovery File.

Authority and Scope

All scope and administrative authority restrictions are honored by this utility, thereby preventing unauthorized access to the CPF Recovery File.

TSSCPR can only be issued by the MSCA or by an SCA, otherwise the following message is issued:

```
TSS8081E MUST BE MSCA OR SCA
```

To execute the TSSCPR utility, an SCA must have or be given the following administrative access:

```
TSS ADMIN(acid) ACID(REPORT) RESOURCE(REPORT) DATA(authority level(s))
```

JCL Requirements

To execute TSSCPR, use the following JCL

```
//TSSCPR          JOB
//XTRACT          EXEC    PGM=TSSCPR
//CPFOUT          DD      DSN=dsname,UNIT=????,VOL=SER=????????
//                DISP=(,CATLG,DELETE),SPACE=(TRK,(15,15),RLSE),
//                DCB=(RECFM=FB,LRECL=4500,BLKSIZE=22500)
//CPFFILE         DD      DSN=cpf.recovery.file.name, DISP=SHR
```

The following is a description of the DD statements used with TSSCPR:

DD Statement	Description
CPFOUT	Contains formatted records of information extracted from the CPF Recovery File.
CPFFILE	Contains the CPF Recovery File.

The following DCB defaults are used with TSSCPR:

DD Statement	Description
DDNAME	DCB Defaults
CPFOUT	DSORG=PS, LRECL=4500, BLKSIZE=22500, RECFM=FB

The record layout for TSSCPR is as follows:

Field Position	Description
1 to 8	Internal Flags
9 to 16	Command Destination
17 to 20	Internal Flags
21 to 24	Record ID 'TCPL'
25 to 43	Internal Control Fields
44 to 51	ACID name
52 to 148	Internal Control Fields
149 to 158	Date of Command
159 to 404	Internal Control Fields

Field Position	Description
405 to 406	Command Length
407 to 408	Internal Flags
409 to 844	Command Buffer

Only the Command Destination, ACID Name and Command Buffer fields can be displayed.

For information on using the TSSREPORT3 facility to produce an CA-Earl® report from TSSCPR output, see the chapter “Using CA-EARL”

Chapter 6: Using CA Earl

This section contains the following topics:

CA Earl Utilities

You may use three utilities as input for customized reports using CA Earl: TSSREPORT, TSSREPORT2, and TSSREPORT3. TSSREPORT applies the capabilities of CA Earl, an easy-to-use report language, to the output of the TSSCFILE utility to provide formatted summaries of CA Top Secret data.

Using the Utilities

Eleven sample reports are provided on the tape and described in this chapter. The default parameters shown enable you to run the samples as given. Optional parameters help you to tailor the reports exactly to fit your needs. These reports can also be customized through the use of TSSCFILE and CA-Earl statements. For example, this command limits the report output to selected user ACIDs within the personnel department.

```
TSS LIST(ACIDS) DEPARTMENT(PERSONNEL)
                TYPE(USER)
```

TSSREPORT2, on the other hand, takes the output from the TSSUTIL utility to produce flat file (straight sequential disk) output for use with CA-Earl, as long as the user includes the optional EarlOUT DD statement in the execution JCL.

TSSREPORT3 takes the output from the TSSCPR utility to produce a single report depicting the contents of the CPF Recovery File.

CA-Earl documentation is supplied with your CA Top Secret manuals. See the appropriate guide for information on using CA-Earl.

See the chapter “TSSCFILE” for details on the use of TSSCFILE, and the chapter “TSSUTIL Utility” for details on the use of TSSUTIL. See “TSSCPR Utility” chapter for details on the use of TSSCPR.

Authority and Scope

CA Top Secret administrative authority is required to execute these reports. To execute the TSSREPORT, TSSREPORT2, and TSSREPORT3 utilities you must have the following administrative authorities required for TSSCFILE, TSSUTIL, and TSSCPR.

```
TSS ADMIN(acid) ACID(REPORT)
                RESOURCE(REPORT)
                DATA(authority level(s))
```

Note: In addition, only the MSCA or an SCA can issue the TSSCPR utility.

TSSREPORT Utility

CA-Earl and the output of the TSSCFILE utility provide formatted summaries of CA Top Secret data. This expanded reporting function gives you the capability to generate additional administrative summary reports.

TSSREPORT JCL

The following JCL resides in the CAI.TSS.CAIJCL file on the distribution tape:

```
//Earl        EXEC PGM=Earl,REGION=4096K
//EarlLIB      DD DISP=SHR,DSN=&USERLIB.
//EarlOBJ      DD UNIT=&UNIT.,SPACE=(3200,(50,4),RLSE)
//SYSUT1       DD UNIT=&UNIT.,SPACE=(3200,(15,4),RLSE)
//SYSUT2       DD UNIT=&UNIT.,SPACE=(3200,(4,4))
//SYSUT3       DD UNIT=&UNIT.,SPACE=(3200,(4,4))
//SYSUT4       DD UNIT=&UNIT.,SPACE=(3200,(10,4),RLSE)
//SYSUT5       DD UNIT=&UNIT.,SPACE=(3200,(70,4),RLSE)
//SYSUT6       DD UNIT=&UNIT.,SPACE=(3200,(15,1),RLSE)
//SORTIN       DD UNIT=&UNIT.,SPACE=(3200,(70,4),RLSE)
//SORTOUT      DD UNIT=&UNIT.,SPACE=(3200,(70,4),RLSE)
//WORK1        DD UNIT=&UNIT.,SPACE=(3200,(300,200))
//SORTWK01     DD UNIT=&UNIT.,SPACE=(3200,(70,4))
//SORTWK02     DD UNIT=&UNIT.,SPACE=(3200,(70,4))
//SORTWK03     DD UNIT=&UNIT.,SPACE=(3200,(70,4))
//SYSUDUMP     DD &SYSOUT=*.
//SYSPRINT     DD &SYSOUT=*.
//SYSOUT       DD &SYSOUT=*.
//SYSIN        DD DISP=SHR,DSN=&USERLIB. (&REPORT).
               PEND
```

EarlLIB

Defines the CA Earl macro library. This source statement library is referenced by the COPY statement within the user's CA-Earl source program.

EarlOBJ

Defines the file on which the CA Earl text file is stored.

SORTIN

Defines the temporary hit file, which contains only the fields from the input records, which are needed to produce the final printed reports. If required to sort the hit file, SORTIN defines the input file to the stand-alone sort invoked by CA Earl.

SORTOUT

Defines the temporary output file from the stand-alone sort.

WORK1

Defines the SRAM (Sort Reentrant Access Method) file.

SORTWK01

Used with SORTWK02 and SORTWK03, defines the temporary work files for the stand-alone sort.

TSSCFILE

The name of your TSSCFILE OUT file. You must run TSSCFILE before running TSSREPORT. See the topic JCL Requirements in the chapter “TSSCFILE Utility” for the JCL needed to run that utility.

You can generate reports by putting the TSSCFILE output (OUT DD) in a permanent data set and using this data set to run multiple CA-Earl reports. This saves time by allowing you to run many reports from the same data.

You can also run TSSCFILE and write the output to a temporary data set. Use this temporary data set as input for your TSSREPORT JCL.

SYSIN

The input control statement. Put the name of the report you wish to run after the name of your source library: TSSEarl1, TSSEarl2, or whichever report you want, up to 7.

Note: PARM= in the JCL refers to the input parameters as defined in the next section.

Report Selection Criteria

Reports 1 through 7 are described in the following pages. Input parameters, if any, appear in the boxes and are followed by definitions of both required and optional parameters. The headers that appear on each report output follow the respective report sample.

The DATE format for reports 1, 2, and 3 is MM/DD/YY. This can be modified with the CA-Earl installation options.

Note: See the topic Command Syntax in the chapter “TSSUTIL Utility” for a list of syntax conventions to be used in these reports.

How to Generate Sample Report 1 (Inactive ACIDs)

This sample report lists all ACIDs that are inactive. An ACID is considered “inactive” and is denied access to the system after a specified amount of time that was predetermined with the INACTIVE control option. The ACIDs in this report would get suspended during the next signon attempt.

To generate the report:

1. Run TSSCFILE:

```
TSS LIST(acids) DATA(ALL,PASS)
```

2. Execute TSSREPORT JCL (see page 153) that includes the following information:

   - The following PARM entry:

     PARM='INACTIVE(*nnn*)'

     nnn

     Specifies a number that matches the site-selected INACTIVE control option parameter, which is any number from 0 through 999.

   - A TSSCFILE DD statement that points to the output file produced by the TSSCFILE job

   The generated report shows the following information:

   ACID

   Lists the inactive ACIDs.

   NAME

   Lists the user name associated with each ACID.

   DATE INACTIVE

   Lists the date that the product denied the ACID access to the system.

   Example: A user's last logon was January 1, 2014, and the user's password expired on February 1. If *nnn* is 30, the inactive date would be reported as March 2 (30 days after the password expired).

   Note: A 1980 date under DATE INACTIVE means that the user's password had been assigned the EXP parameter (to expire immediately).

If your site does not use the default date (mm/dd/yy) in CA Top Secret, you encounter a U3000 abend. To use the alternate date format, edit the TSSEARL1 job with the following statements:

```
DEF S_EXP_MO = S_EXPO_ 3 - 4 N
DEF S_EXP_DA = S_EXPO_ 1 - 2 N
DEF EXP_MO = R3000XPD 1 - 2 N
DEF EXP_MO = R3000XPD 4 - 5 N
```

See the comments in member TSSEARL1 contained in CAI.SAMPJCL.

Sample Report 2 - Expired ACIDs

Lists all ACIDs that are expired.

PARM=

There are no input parameters for this report.

ACID

Lists the expired ACIDs.

NAME

Lists the user's name associated with each ACID.

DATE EXPIRED

Lists the date each ACID expired.

Sample Report 3 - Suspended ACIDs

Lists all ACIDs that are suspended.

PARM=

There are no input parameters for this report.

ACID

Lists the suspended ACIDs.

PROFILE INDICATOR

A **P** in this column means that the listed ACID is a profile ACID.

NAME

Lists the name associated with each listed ACID.

DATE RESUME

Output appears here only if the ACID in question has been temporarily suspended. This is the date it will resume after the temporary suspension.

Sample Report 4 - ACID Names

Lists ACIDs in alphabetical order by name. The following parameters may be used to specify the order in which the user wants the ACIDs sorted. One and only one of the first four parameters must be specified; the delimiter and A or D are optional.

```
PARM='FIRST|LAST|Pnn|Cnn[,delimiter][,A|,D]
```

FIRST

This parameter sorts by first name, starting with the first nonblank character in the name field.

LAST

This parameter sorts by last name, starting with the first character following the last delimiter found, or, if no delimiters are found, starts with column 1.

Pnn

This parameter sorts by nnth positional subfield. The subfield to be sorted starts with the first character after the (nn-1)th delimiter and ends with the next delimiter or the last character in the name field, whichever occurs first. If a subfield specified is outside the range of fields found on a name being sorted, the following error message is generated:

SUBFIELD nn WAS NOT FOUND IN THE NAME FIELD

Cnn

This parameter sorts by the entire name field, beginning with column nn (with nn equaling a number 1 through 20), and ending with the last character in the name field.

delimiter

This parameter is optional. It cannot be used if **Cnn** was used. The delimiter is the one-byte character indicating a separation between positional subfields within the ACID name (such as a comma, blank, or hyphen). Default is a blank.

A

This parameter is a default. It sorts in ascending alphabetical order (EBCDIC collating sequence). If this parameter is selected, a report is also generated in descending order, with the note: “Descending order report not selected for this run”. Conversely, a request for descending order will result in the additional ascending-order report and note.

D

This parameter sorts in descending alphabetical order. If not specified, the default is A.

Note: Remember to enter your parameters exactly as shown in the example. Even if the delimiter you select is a comma, you must still use a comma before this delimiter, as shown next.

```
PARM='P8,,,D'
```

The report title indicates which options were selected, and which delimiter, if any, is used.

```
VERSION 9.0 ADMINISTRATIVE REPORT UTILITY                    PAGE   1
```

```
JUL 23 02           REPORT 4:  REPORT OF ACID NAMES
SORTED ON LAST NAME
IN ASCENDING ORDER, USING ' ' AS A DELIMITER
------------------------------------------------------------------------
NAME                                    ACID
------------------------------------------------------------------------
FROPH01 DIV #1                          FROPHV1
FROPH01 DIV #2                          FROPHV2
FROPH01 DIV #3                          FROPHV3
FROPH01 DEPT A                          FROV1DA
FROV1DA USER A                          1DAUSRA
FROV1DA USER A                          1DBUSRA
FROPH01 DEPT B                          FROV1DB
FROV1DA USER B                          1DBUSRB
FROV1DA USER B                          1DAUSRB
FROV1DA USER C                          1DBUSRC
FROV1DA USER C                          1DAUSRC
FROV1DA USER D                          1DAUSRD
FROV1DA USER D                          1DBUSRD
FROV1DA USER E                          1DAUSRE
FROV1DA USER E                          1DBUSRE
FROV1DA USER F                          1DAUSRF
FROV1DA USER F                          1DBUSRF
VCA FOR DIV FROPHV1                     FROVC11
VCA FOR DIV FROPHV2                     FROVC21
VCA FOR DIV FROPHV3                     FROVC31
VCA FOR DIV FROPHV3                     FROVC32
DCA FOR DEPT FROV1DA                    FRODC1A1
DCA FOR DEPT FROV1DA                    FRODC1A2
DCA FOR DEPT FROV1DB                    FRODC1B1
FROV1DA USER G                          1DAUSRG
FROV1DA USER G                          1DBUSRG
FROV1DA USER H                          1DAUSRH
FROV1DA USER H                          1DBUSRH
FROV1DA USER I                          1DAUSRI
FROV1DA USER I                          1DBUSRI
FROV1DA USER J                          1DAUSRJ
FROV1DA USER J                          1DBUSRJ
DEPT FROV1DA PROF                       FRO1AP1
DEPT FROV1DB PROF                       FRO1BP1
DEPT FROV1DB PROF                       FRO1BP3
DEPT FROV1DB PROF                       FRO1BP2
DEPT FROV1DA PROF                       FRO1AP3
DEPT FROV1DA PROF                       FRO1AP2
END OF REPORT
```

NAME

Lists the given names in the order specified.

ACID

Lists the ACID associated with each name.

Sample Report 5 - List of ACIDs

Lists ACIDs in alphabetical order by selected positions within the ACID.

```
PARM='[Scc][,Ecc][,A|,D]
```

Scc

This parameter sorts by starting column position within the ACID. Select column 1 through 8. This parameter is optional. Default is S1.

Ecc

This optional parameter sorts by ending column position within the ACID. The default is E8. Select column 1 through 8, but the number must be greater than or equal to **Scc.** If an Ecc is specified that is less than Scc, the job will terminate execution and the following message will appear in place of the report:

INVALID PARAMETER-NO REPORT PRODUCED

A

This is the default parameter. This parameter sorts in ascending alphabetical order (EBCDIC collating sequence). If this parameter is selected, a report is also generated in descending order, with the note: “Descending order report not selected for this run.” Conversely, a request for descending order will result in the additional ascending-order report and note.

D

This parameter sorts in descending alphabetical order. If not specified, the default is **A.**

The report title indicates whether ascending or descending order was selected, and which starting and ending column positions were selected for the sort.

ACID

Lists the ACIDs in the order specified.

NAME

Lists the given name for the ACIDs being listed.

Sample Report 6 - Who Has Attributes

Lists ACIDs that have the attribute specified.

```
PARM='[attribute]'
```

attribute

The attribute is any CA Top Secret attribute that may be assigned to a user or profile ACID.

ACID

Lists the ACIDs that have the attribute.

PI

A **P** under this header indicates that the ACID is a profile ACID.

NAME

Lists the given name for the ACIDs being listed.

ATTRIBUTES

Refers to the attribute specified.

An asterisk appears before each BYPASS attribute: NODSNCHK, NOVOLCHK, NOLCFCHK, NOSUBCHK, NORESCHK.

When an ACID having the attribute requested is found, all of that ACID's attributes (BYPASS or non-BYPASS) is shown. If no PARM was specified, all ACIDs having any attribute is shown.

Sample Report 7 - Who Has Administrative Authorities

Lists ACIDs that have administrative authorities, and their scope of authority.

```
PARM=
```

There are no input parameters for this report.

ACID

Lists the ACIDs.

TYPE

Lists each ACID type: MASTER, CENTRAL, LSCA, ZONE C/A, DIVISION C/A, DEPARTMENT C/A, PROFILE or USER.

SCOPE OF AUTHORITY

Lists scope of authority with the format
`ACIDNAME(scope)`

If the TYPE is MASTER or CENTRAL, the scope is ALL.

AUTHORITY

Authority type is one of the following: FACILITY, ACID, LIST DATA, MISC1, MISC9, RESOURCE, or a predetermined specific resource class name, such as DATASET.

The ACID's authority levels are listed after Authority Type. See the chapter “Using the FDT Record” in the *Command Functions Guide* for information about authority levels.

ACCESS

After authority level:XAUTH, “access” indicates the access levels the ACID may use to cross-authorize (PERMIT) users to the corresponding resource after authority type. The TSS command for TSSCFILE for this particular report is:
`TSS LIST(acids) DATA(ALL)`

TSSREPORT2 Utility

TSSREPORT2 uses the output from the TSSUTIL utility to produce flat file (straight sequential disk) output for use with CA-Earl, if you include the optional EarlOUT DD statement in the execution JCL.

TSSREPORT2 JCL

The JCL is found in the CAI.SAMPJCL file on the distribution tape.

```
//REPORT      JOB
//Earl        EXEC PGM=Earl,REGION=4096K
//EarlLIB      DD DISP=SHR,DSN=your.source.library
//EarlOBJ      DD UNIT=unit,SPACE=(3200,(50,4),RLSE)
//SYSUT1       DD UNIT=unit,SPACE=(3200,(15,4),RLSE)
//SYSUT2       DD UNIT=unit,SPACE=(3200,(4,4))
//SYSUT3       DD UNIT=unit,SPACE=(3200,(4,4))
//SYSUT4       DD UNIT=unit,SPACE=(3200,(10,4),RLSE)
//SYSUT5       DD UNIT=unit,SPACE=(3200,(70,4),RLSE)
//SYSUT6       DD UNIT=unit,SPACE=(3200,(15,1),RLSE)
//SORTIN       DD UNIT=unit,SPACE=(3200,(70,4),RLSE)
//SORTOUT      DD UNIT=unit,SPACE=(3200,(70,4),RLSE)
//WORK1        DD UNIT=unit,SPACE=(3200,(300,200))
//SORTWK01     DD UNIT=unit,SPACE=(3200,(70,4))
//SORTWK02     DD UNIT=unit,SPACE=(3200,(70,4))
//SORTWK03     DD UNIT=unit,SPACE=(3200,(70,4))
//SYSUDUMP     DD SYSOUT=*
//SYSPRINT     DD SYSOUT=*
//SYSOUT       DD SYSOUT=*
//TSSUTI       DD DSN=name.of.tssutil
//SYSIN        DD DISP=SHR,DSN=your.source.library(TSSEarlA|B|C|D)
```

EarlLIB

Defines the CA-Earl macro library. This source statement library is referenced by the COPY statement within the user's CA-Earl source program.

EarlOBJ

Defines the file on which the CA-Earl text file is stored.

SORTIN

Defines the temporary hit file, which contains only the fields from the input records, which are needed to produce the final printed reports. If required to sort the hit file, SORTIN defines the input file to the stand-alone sort invoked by CA-Earl.

SORTOUT

Defines the temporary output file from the stand-alone sort.

WORK1

Defines the SRAM (Sort Reentrant Access Method) file.

SORTWK01

Used with SORTWK02 and SORTWK03, defines the temporary work files for the stand-alone sort.

TSSUTI

The name of your TSSUTIL OUT file. You must run TSSUTIL before running TSSREPORT2. See TSSUTIL JCL in the chapter “USSUTIL Utility” for the JCL needed to run that utility.

You can generate reports by putting the TSSUTIL output (OUT DD) in a permanent data set and using this data set to run multiple CA-Earl reports. This saves time by allowing you to run many reports from the same data.

You can also run TSSUTIL and write the output to a temporary data set. Use this temporary data set as input for your TSSREPORT2 JCL.

SYSIN

The input control statement. Put the name of the report you wish to run after the name of your source library: TSSEarlA, TSSEarlB, TSSEarlC or TSSEarlD for whichever report you select.

Note: PARM= in the JCL refers to the input parameters as defined in the next section.

TSSREPORT2 Selection Criteria

Reports A through D are described in the following pages. Input parameters, if any, appear in the boxes and are followed by definitions of both required and optional parameters. The headers that appear on each report output follow the respective report sample.

The DATE format for each report is MM/DD/YY. This can be modified with the CA-Earl installation options.

Note: See the topic Command Syntax in the chapter “TSSUTIL Utility” for a list of syntax conventions to be used in these reports.

Sample Report A - Data Set Violations

Generates a list of all violations against data sets. This list is sorted by ACID and indicates the number of violations per data set.

PARM=

There are no input parameters for this report.

```
VERSION 9.0 ADMINISTRATION REPORT UTILITY2
12/07/02   REPORT A: REPORT OF DATASET and NUMBER OF VIOLATIONS    PAGE 1

-------------------------------------------------------------------------
           ACID           DATASET NAME                   NO. OF VIOLATION
-------------------------------------------------------------------------

           USER001        AUDT001.CLIST                              4
           USER001        SYS1.BRODCAST                              1
           USER001        SYS1.MACLIB                                1
                                                                  ------
           USER001                                                   6
                                                                  ------
           USER002        AUDT001.CLIST                              1
                                                                  ------
           USER002                                                   1
                                                                  ------
                                                                  ------
                                                                     7
GRAND TOTAL                                                       ------
```

ACID

Lists the ACID responsible for the data set violation.

DATASET NAME

Lists the name of the data set the user attempted to access.

NO. OF VIOLATIONS

Lists the number of violations against each data set.

For TSSUTIL report selection criteria, select EVENT(VIOL).

Sample Report B - Requested vs. Allowed Access

Lists all access violations against each data set and indicates which ACID requested access, what type of access was requested and what access level was allowed for that ACID. This list is sorted according to data set name.

```
PARM=
```

There are no input parameters for this report.

DATE

Indicates the date when the ACID attempted to access the data set.

TIME

Indicates the time at which access was attempted.

DATASET NAME

Indicates which data set the ACID attempted to access.

ACID

Indicates the ACID which incurred the violation.

REQ ACCESS

Indicates what access level the ACID requested to the data set.

ALLOWED ACCESS

Indicates the actual level at which the ACID is allowed to access the data set.

For TSSUTIL report selection criteria, specify EVENT(VIOL).

Sample Report C - Password Violations

Lists all ACIDs that have received password violations.

PARM=

There are no input parameters for this report.

```
VERSION 9.0 ADMINISTRATION REPORT UTILITY2
23/07/02    REPORT C: REPORT OF PASSWORD VIOLATIONS                    PAGE 1

------------------------------------------------------------------------------
            DATE        TIME          ACID          TSSTEXT
------------------------------------------------------------------------------

            94162       15:17:47      USER001       PASSWORD INCORRECT
            94162       15:17:33      USER001       PASSWORD INCORRECT
            94162       15:17:03      USER001       PASSWORD INCORRECT
            94162       15:16:49      USER001       PASSWORD INCORRECT
            94162       15:19:23      USER002       PASSWORD INCORRECT
            94162       15:19:12      USER002       PASSWORD INCORRECT
END OF REPORT
```

DATE

Lists the date that the violation occurred.

TIME

Lists the time that the violation occurred.

ACID

Indicates which ACID incurred the violation.

TSSTEXT

Details, in plain language rather than in DRC code numbers, the type of password violation which occurred.

For TSSUTIL report selection criteria, specify EVENT(VIOL).

Sample Report D - Terminal Violations

Generates a list of all terminal violations. The type of violation is explained in text, not by DRC code.

PARM=

There are no input parameters for this report.

```
VERSION 9.0 ADMINISTRATION REPORT UTILITY2
23/07/02      REPORT D: REPORT OF TERMINAL VIOLATIONS      PAGE 1

------------------------------------------------------------------
   DATE   TIME         TERM ID               TSSTEXT
------------------------------------------------------------------

   94162  15:17:47     K18L4258              PASSWORD INCORRECT
   94162  15:17:33     K18L4258              PASSWORD INCORRECT
   94162  15:17:03     K18L4258              PASSWORD INCORRECT
   94162  15:16:49     K18L4258              PASSWORD INCORRECT
   94162  15:19:23     A29LP021              PASSWORD INCORRECT
   94162  15:19:32     A29LP021              PASSWORD INCORRECT
   94164  12:58:29     INTRDR                SYSTEM FACILITY NOT AUTHORIZED
   94164  12:58:49     INTRDR                ACID NOT DEFINED

END OF REPORT
```

DATE

Indicates the date on which the violation occurred.

TIME

Indicates the time that the violation occurred.

TERM ID

Indicates the terminal at which the violation occurred.

TSSTEXT

Details the type of violation that occurred.

For TSSUTIL report selection criteria, specify

EVENT(VIOL)RESOURCE(TERMINAL)

TSSREPORT3 Utility

TSSREPORT3 takes the output from the TSSCPR utility to produce a single report depicting the contents of the CPF Recovery File.

TSSREPORT3 JCL

The JCL is found in CAI.SAMPJCL on the distribution tape.

```
//REPORT        JOB
//Earl          EXEC PGM=Earl,REGION=4096K
//EarlLIB         DD DISP=SHR,DSN=your.source.library
//EarlOBJ         DD  UNIT=unit,SPACE=(3200,(50,4),RLSE)
//SYSUT1          DD  UNIT=unit,SPACE=(3200,(15,4),RLSE)
//SYSUT2          DD  UNIT=unit,SPACE=(3200,(4,4))
//SYSUT3          DD  UNIT=unit,SPACE=(3200,(4,4))
//SYSUT4          DD  UNIT=unit,SPACE=(3200,(10,4),RLSE)
//SYSUT5          DD  UNIT=unit,SPACE=(3200,(70,4),RLSE)
//SYSUT6          DD  UNIT=unit,SPACE=(3200,(15,1),RLSE)
//SORTIN          DD  UNIT=unit,SPACE=(3200,(70,4),RLSE)
//SORTOUT         DD  UNIT=unit,SPACE=(3200,(70,4),RLSE)
//WORK1           DD  UNIT=unit,SPACE=(3200,(300,200))
//SORTWK01        DD  UNIT=unit,SPACE=(3200,(70,4))
//SORTWK02        DD  UNIT=unit,SPACE=(3200,(70,4))
//SORTWK03        DD  UNIT=unit,SPACE=(3200,(70,4))
//SYSUDUMP        DD  SYSOUT=*
//SYSPRINT        DD  SYSOUT=*
//SYSOUT          DD  SYSOUT=*
//TSSCPFR         DD  DSN=name.of.tsscpr
//SYSIN           DD  DISP=SHR,DSN=your.source.library(TSSEarlE)
```

EarlLIB

Defines the CA-Earl macro library. This source statement library is referenced by the COPY statement within the user's CA-Earl source program.

EarlOBJ

Defines the file on which the CA-Earl text file is stored.

SORTIN

Defines the temporary hit file, which contains only the fields from the input records, which are needed to produce the final printed reports. If required to sort the hit file, SORTIN defines the input file to the stand-alone sort invoked by CA-Earl.

SORTOUT

Defines the temporary output file from the stand-alone sort.

WORK1

Defines the SRAM (Sort Reentrant Access Method) file.

SORTWK01

Used with SORTWK02 and SORTWK03, defines the temporary work files for the stand-alone sort.

TSSCPFR

The name of your CPFOUT file. You must run TSSCPR before running TSSREPORT3. See the chapter “TSSCPR Utility” for the JCL needed to run that utility.

You can generate reports by putting the TSSCPR output **(OUT DD)** in a permanent data set and using this data set to run multiple CA-Earl reports. This saves time by allowing you to run many reports from the same data.

You can also run TSSCPR and write the output to a temporary data set. Use this temporary data set as input for your TSSREPORT3 JCL.

SYSIN

The input control statement. Put the name of the report you wish to run (in this case TSSEarlE) after the name of your source library.

Note: TSSREPORT3 produces a preformatted report depicting the entire contents of the CPF Recovery File. There are no additional parameters or selection criteria that can be specified.

Sample Report E CPF Recovery File

This report produces a list of the contents of the CPF Recovery File.

PARM=

There are no input parameters for this report.

```
07/07/02    Sample /MVS Report 3                      PAGE       1
                                                  CPF Recovery File

_____________________________________________________________________
CMD   ACID   Cmd buffer in 80 byte segments                    Count
Dest_____________________________________________________________

XE56  USER01  TSS LIST(USER01) DATA(NAMES) TARGET(*) WAIT(N)

XE56  MASTER  TSS REP(TWFRED) PASS(?)

XE56  MASTER  TSS REP(USERJM) PASS(?)

XE56  MASTER  TSS ADD(RJDEV1) PASS(?)

XE56  MASTER  TSS LIST(RJDEV1) DATA(ALL) TARGET(*)

XE56  MASTER  TSS REP(KELDEV) PASS(?)

XE56  AUDVAC  TSS CREATE(AUDIT01) TYPE(USER)
                  NAME('John Smith') DEPT(AUDEPT) PASSWORD(?)

XE56  AUDVAC  TSS CREATE(AUDIT02) TYPE(USER) NAME('Charles Browne')
                  DEPT(AUDEPT) PASSWORD(?) VXAUFGROUP(GROUP1)
                  VXACCOUNT(ACCT1) VXGNAME(GROUP1)

XE56  RDBRRN  TSS LIST(RDT) RESCLASS(JOBNAME)
```

Note: Passwords are printed as question marks (?) and not revealed.

CMD Dest

Indicates the node to which the command was propagated.

ACID

Indicates the ACID issuing the command.

Cmd buffer

Displays the syntax of the command that was issued, in 80 character segments

Count

Indicates both the total number of commands issued to each node and, at the end of the report, the total number of commands issued.

Chapter 7: TSSRPTST Utility

This section contains the following topics:

About the TSSRPTST Utility

The batch utility program, TSSRPTST, processes and displays the output that was sent to SMF by the SAF SECTRACE command.

Using the TSSRPTST Utility

To run the TSSRPTST report, you must have already run the SAF SECTRACE operator command and set the output destination to SMF. With few exceptions, CA Top Secret processes all MVS SAF security requests by default. The SAF Trace report enables you to display the monitored RACROUTE parameter list passed by requests for SAF services. This report also displays additional environmental information, such as job name, user ID, and the program issuing the SAF call. For more information about using the SAF SECTRACE command, see the *Troubleshooting Guide.*

For z/OS 1.9 and above, SMF data may be sent to the LOGGER services controlling the write of the SMF data in LOGSTREAM structures. SMF data is not recorded in the usual SYS1.MANx data sets.

The TSSRPTST utility is able to read the data under when:

- The LOGR services is active on the system with the definitions that contain the SMF data
- The LOGR subsystem is active on the system
- An IEFSSNxx member is defined and activated at IPL with the definition:

  ```
  SUBSYS SUBNAME(LOGR) INITRTN(IXGSSINT)
  ```

The RECxxxxx DD used to read the data has the format:

```
//RECxxxxx DD  DSN=IFASMF.DATA.LOGSTRM,DISP=SHR,
//          SUBSYS=(LOGR,IFASEXIT,subsys-options1,subsys-options2)
```

Description of SUBSYS options-1 includes:

```
[FROM={({[yyyy/ddd][,hh:mm[:ss]]}) | OLDEST}]
[TO={({[yyyy/ddd][,hh:mm[:ss]]}) | YOUNGEST}]
 [,DURATION=(nnnn,HOURS)]
 [,VIEW={ACTIVE|ALL|INACTIVE}]
 [,GMT|LOCAL]
```

The subsys-options1 parameters used by the IBM IFASEXIT are the same than those used by the IFBSEXIT. For information on the parameters for IFBSEXIT, see IBM's *MVS Diagnosis: Tools and Service Aids*.

Authority and Scope

CA Top Secret performs authorization checking to determine whether the person submitting the TSSRPTST job is authorized to view or manipulate the input SMF data.

TSSRPTST JCL

The following sample JCL, or a user-written substitute for the job stream, can be used to run the TSSRPTST report.

```
//REPORTS JOB 1,'TSSRPTST REPORTS',MSGCLASS=A,CLASS=A
//*******************************************************************
//*
//*  THIS JOB MAY BE USED TO PRODUCE A COPY OF TSSRPTST REPORT
//*
//*******************************************************************
//*
//*
//*****************************
//* TSSRPTST REPORT GENERATOR
//*****************************
//REPORT  EXEC PGM=TSSRPTST
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//RECMAN1 DD DSN=IFASMF.XE15.SMFLOG,DISP=SHR,
// SUBSYS=(LOGR,IFASEXIT)
//SYSIN    DD *
```

Input and Output Files for SAF Trace Report Generator

This section gives the ddname and description of the input and output files.

RECxxxxx

These are the input files containing SMF records that your site collects and maintains. The CA Top Secret report generators use these files for input. These files must have DDnames beginning with the characters REC. For example:

```
//RECMAN1  DD DSN=SYS1.MAN1,DISP=SHR
//RECMAN2  DD DSN=SYS1.MAN2,DISP=SHR
```

SYSIN

A file that lets you specify parameters to TSSRPTST report generator. Specify parameters by using the PARM field of a JCL EXEC statement. The SYSIN file enables you to specify a set of parameters that exceeds 100 characters. The JCL PARM parameter is explained in this chapter in the section on parameters.

The SYSIN file is defined in one of the following formats:

- F or FB-The last eight characters of each record are assumed to be a sequence number and are ignored.
- VB-The first eight characters are assumed to be the sequence field and are ignored.

You can create a SYSIN file like the following one by using the TSO EDIT command:

```
TITLE(DATA SET LOGGING RECORD)
JOBMASK(TSG-)
SDATE(91170)
EDATE(91189)
```

All records in the SYSIN file are assumed to be an extension of the JCL EXEC statement PARM field. Any parameter value specified in a record is continued in the next record in the file. A dash (-) as the last non-blank character of a record indicates a continuation in the next record. The contents of the next record are concatenated to the preceding record at the position of the dash. The dash itself is omitted.

SYSPRINT

A file that specifies where the report output is sent. Output is directed to a printer or to a listing data set. The record format is VBA. Specification of the BLKSIZE parameter is optional; the default is 3665.

Report generator output is generally 80 characters wide for most reports. This width permits convenient report browsing on an 80-character display screen. However, some reports have a wider format for use with printer-directed output. To find out the maximum record length for each format, refer to the explanation of each report generator.

SYSPRINT is referred to as OUTPUT LIST NAME on the ISPF report generator panels.

SMF Input Records for SAF Trace Report Generator

SMF record number 231 identifies the input records for the CA Top Secret SAF Trace Report generator.

For z/OS 1.9 and above, SMF data may be sent to the LOGGER services controlling the write of the SMF data in LOGSTREAM structures.SMF data is not recorded in the usual SYS1.MANx data sets.

The TSSRPTST utility is able to read the data when:

- The LOGR services is active on the system with the definitions that contain the SMF data.
- The LOGR subsystem is active on the system
- An IEFSSNxx member is defined and activated at IPL with the definition:

```
SUBSYS SUBNAME(LOGR) INITRTN(IXGSSINT)
```

The RECxxxxx DD used to read the data has the format:

```
//RECxxxxx DD  DSN=IFASMF.DATA.LOGSTRM,DISP=SHR,
//          SUBSYS=(LOGR,IFASEXIT,subsys-options1,subsys-options2)
```

Description of SUBSYS options-1 includes:

```
[FROM={({[yyyy/ddd][,hh:mm[:ss]]}) | OLDEST}]
[TO={({[yyyy/ddd][,hh:mm[:ss]]}) | YOUNGEST}]
 [,DURATION=(nnnn,HOURS)]
 [,VIEW={ACTIVE|ALL|INACTIVE}]
 [,GMT|LOCAL]
```

TSSRPTST Parameters

Specify parameters for TSSRPTST report generator using the following methods:

- Use the PARM parameter of the EXEC statement in the JCL. For example:

```
//STLOGS  EXEC PGM=TSSRPTST,REGION=128K,
//        PARM=('TITLE(SAF TRACE LOGGING RECORDS)',
//       'SDATE(91170)','EDATE(91174)')
```

- Use the SYSIN file. Supply a SYSIN DD statement and control record file as previously explained in the topic Input and Output Files for SAF Trace Report Generator.

```
//STLOGS  EXEC PGM=TSSRPTST,REGION=128K
//SYSIN    DD DSN=ADMIN.WORK.PARMS(ST),DISP=SHR
```

  If you specify a particular parameter more than once, the last specified value for the parameter is used. For example, if you specify:

  PARM=('SDATE(91001)','EDATE(91005)','SDATE(91002)')

The SDATE parameter uses a value of 91002.

To represent a literal string of text delimited by single quotes as part of an EXEC PARM, use two single quotes. For example:

```
PARM=('IF(PREFIX NE ''********'')')
```

Selection Criteria

The selection criteria used in generating the SAF Trace reports are listed below, with brief descriptions. All selection criteria are described in detail after the listing.

JOBMASK

Limits records appearing on the report to those for the job indicated by the job name mask.

TITLE

Specifies a character string added to other title information at the top of the report. This character string can be up to 35 characters in length.

LINECNT

The LINECNT (linecount) parameter specifies the number of output lines to be printed on a page.

SDATE

Specifies the start date of the report in Julian date format.

EDATE

Specifies the ending Julian date from which report information is selected.

STIME

Specifies the start time for the interval from which SMF records are selected.

ETIME

Specifies the end time for the interval from which SMF records are selected.

DETAIL

Specifies the report is to include all the information available for each logging event.

POSTLOG

Requests records created after security validation has completed.

PRELOG

Requests records created before security validation has occurred.

TRACEID

Specifies an eight-character trace ID.

JOBMASK

Specifies that records appearing on the report are to be limited to those for the job indicated by the job name mask.

```
JOBMASK(********|jobmask,...)
```

****

Specifies all jobs are to appear on the report.

jobmask

Indicates jobs are to be limited to those meeting the masking criteria. Use commas or spaces to separate multiple masks.

TITLE

Specifies a character string added to other title information at the top of the report.

```
TITLE(string)
```

string

This character string can be up to 35 characters in length. If you do not specify this parameter, the report generator uses the first 35 characters in the PARM field of the EXEC statement. If this character string is longer than 35 characters, the first 35 characters are used.

LINECNT

Specifies the number of output lines (line count) to be printed on a page.

```
LINECNT(60|nnnnn)
```

nnnnn

Specifies the number of output lines to be printed on a page. To prevent splitting of information, CA Top Secret report generators that issue multiple line reports check to see whether a complete report item will fit on a page. The maximum number of output lines per page is limited only by the physical constraints of the output media being used, or to 99,999 lines.

SDATE

Specifies the beginning Julian date from which report information is to be selected.

SDATE(00000|yyddd)

yyddd

Specifies the date in Julian date format (last two digits of the year and the sequential number of the day). Any input SMF records generated before the SDATE value are ignored.

Default: 00000, all available records

EDATE

Specifies the ending Julian date for the selected report information.

EDATE(:hp5.99365:ehp5.|yyddd)

yyddd

Specifies the ending Julian date. When combined with the SDATE parameter, this parameter creates a window for report content. The default, 99365, specifies up to the time the job is run.

STIME

Specifies the beginning-of-time interval from which SMF records are selected. This time is based on a 24-hour clock.

STIME(0000|hhmm)

hhmm

Specifies the time at which reporting on the selected SMF records is to begin. This time is based on a 24-hour Any SMF records generated before this specified time of day are ignored. The selection of records begins at the STIME specified for each date in the SDATE/EDATE range.

Default: 0000, midnight

ETIME

Specifies the end-of-time interval from which SMF records are selected. This time is based on a 24-hour clock.

ETIME(2359|hhmm)

hhmm

Specifies the time at which reporting on the selected SMF records is to end. Any SMF records generated after this specified time of day are ignored.

Default: 2359, one minute before midnight.

DETAIL

Specifies that the external data structures identified in the RACROUTE parameter list definition are displayed following the RACROUTE parameters. These external data structures are shown in both hexadecimal and EBCDIC formats.

POSTLOG

Requests records created after security validation has completed. These records contain the return and reason codes from the security call as well as the modified data structures.

PRELOG

Requests records created before security validation has occurred. These records contain the return and reason codes from the security call as well as the modified data structures.

TRACEID

Specifies an eight-character trace identifier.

TRACEID(********|traceid)

****

(Default) Specifies all trace identifiers.

traceid

Specifies a trace ID. Masking can be used with trace IDs.

Sample TSSRPTST Output

TSSRPTST formats and reports SAF SECTRACE output written to the System Management Facility (SMF). SMF is the only SAF SECTRACE output destination where output is guaranteed because SMF is the only destination that can be written to in any mode.

```
TSS UTILITY LIBRARY - TSSRPTST - SAF TRACE REPORT PAGE 59
DATE 06/29/00 (94.180) TIME 14.09 TRACEID(SECOFF)

  SMFID= VEGA      TOD= 14:09:12.57    TRACEID= SCOFF       USERID= USER01

  JOBNAME= USER01  ASID= 001C / 002F   PGM= IKJEFF04        CURR RB= SVC0

  SFR/RFR= 0/0:0   MODE= TASK          APF= AUT  HORIZED    LOCKS= NONE


  RACROUTE REQUEST=AUTH,MSGSP=0,WORKA=,ATTR=READ,CLASS='DATASET',
         DDNAME='SYS00014',DSTYPE=N,
         ENTITY=('USER01,SPFTEMP0.CNTL',NONE),FILESEQ=0,
         GENERIC=ASIS,LOG=ASIS,RACFIND=NO,RELEASE=1.8,STATUS=NONE,
         TAPELBL=STD
```

The TSSRPTST report always produces entries formatted like the sample above.

The TSSRPTST report produces additional information in the entries when the DETAIL parameter is specified, as shown in the following sample.

```
TSS UTILITY LIBRARY - TSSRPTST - SAF TRACE REPORT PAGE 59
DATE 06/29/00 (94.180) TIME 14.09 TRACEID(SECOFF),DETAIL

 SMFID= VEGA      TOD= 14:09:23.35      TRACED= SECOFF        USERID= USER01

 JOBNAME= INIT    ASID= 000F / 003C     PGM= IEFIB600         CURR RB= IEFIB


 SFR/RFR= 0/0:0   MODE= TASK             APF= AUTH  ORIZED     LOCKS= NONE

RACROUTE REQUEST=VERIFY,MSGSP=0,WORK=,ACTINFO=,ENCRYPT=YES,
         ENVIR=CREATE,JOBNAME='USER01A',LOG=ASIS,PASSCHK=YES,
         PGMNAME='MYPROGRAM',RELEASE=1.8,SMC=YES,STAT=ASIS
ACTINFO  DATA AREA FOLLOWS
00024485 +000 0105E2E2 C402E600 00000000 00000000 *..USER01........*
00024495 +010 00000000 00000000 00000000 00000000 *................*
000244A5 +020 00000000 00000000 00000000 00000000 *................*
000244B5 +030 00000000 00000000 00000000 00000000 *................*
000244C5 +040 00000000 00000000 00000000 00000000 *................*
```

Following the TSSRPTST output fields, the external data structures identified by the RACROUTE parameter list are displayed in both hexadecimal and EBCDIC formats.

The following fields appear on the TSSRPTST report.

SMFID

Shows the SMF CPU identifier of the executing CPU.

TOD

Shows the time of day when the SAF request was issued.

TRACEID

Lists the SAF SECTRACE event identifier. The TRACEID is the ID set in the SAF SECTRACE command.

USERID

Shows the user ID active in the address space when the SAF event was traced.

JOBNAME

Identifies the name of the job for which the SAF request was issued.

ASID

Indicates the home address space identifier in which the SAF request was issued and, if applicable, the primary address space identifier in which the code for the task is executed.

PGM

Shows the program that issued the SAF request. This field specifies the program name of the newest PRB on the active RB chain. If no PRB exists on the active RB chain when a monitored event occurs, the name used for the RB field is also used for PROGRAM.

CURR RB

Shows the program name associated with the current request block (RB) under which the call was made. This field specifies the program request block (PRB) name in which the security event must occur. When an event occurs directly under a PRB, the name of the program specified in that block is used to match what you specify in this field. If an event occurs under a supervisor call request block (SVRB), the RB name is assigned SVCnnn, where nnn is the decimal SVC number. If this RB is the only RB on the active RB chain under an SVRB, the interrupt code (SVC number) cannot be determined. Therefore, another RB name is assigned. If the program manager indicator is set, the assigned RB name is *PMSVRB*. If the indicator is not set, the RB name is *SYSTEM*. If the security event occurs under the control of a service request block (SRB), the assigned RB name is *SRB*.

SFR/RFR

Shows the SAF return code and the security system's return and reason codes (n:n) from the SAF event. These values are available only on TRACE=POST requests. See the IBM publication External Security Interface (RACROUTE) Macro Reference for MVS and VM for information about these return and reason codes.

MODE

Shows the operating mode of the address space. There are two different indicators for mode. MODE=TASK indicates that the SAF request was made from a task mode requester. MODE=SRB indicates that the request was made from a SAF mode requester.

APF

Indicates whether the requestor was APF-authorized.

LOCKS

Indicates the locks that were held in the address space at the time the SAF event was traced.

RACROUTE REQUEST

Shows the external data structures identified in the RACROUTE parameter list.

Chapter 8: TSSOERPT Utility

This section contains the following topics:

About TSSOERPT

The batch utility program, TSSOERPT, processes security-related activity recorded in SMF data sets to monitor user activity in an OpenEdition MVS/Unix System Services for z/OS (USS) environment. CA Top Secret logs security events under this environment to SMF using standard CA Top Secret SMF type 231 records. By default, log records are written for any security event that denies the ACID access to a USS function or resource. These records can assist you in determining the UID and GID of the ACID involved in the attempted access. The TSSOERPT utility uses type 231 SMF records. In order to get output for this report, you must be logging type 231 records to SMF.

For sites with specific reporting requirements for activity in a USS environment, use the following members provided in TSSOPMAT to produce customized reports on USS:

- S231DESC—Describes how to use the next three members
- S231ASSM—Sample BAL source to map the SMF Type 231 records
- TSSSMFOX—Mapping macro for the SMF Type 231 record extension
- SMF80—Mapping macro for the SMF Type 231(and 80) base record

Using the TSSOERPT Utility

For z/OS 1.9 and above, SMF data may be sent to the LOGGER services controlling the write of SMF data in LOGSTREAM structures. SMF data will not be recorded in the usual SYS1.MANx data sets. The TSSRPTST utility is able to read the data when:

- The LOGR services are active on the system with the definitions that contains the SMF data.
- A LOGR subsystem is active on the system
- An IEFSSNxx member is defined and activated at IPL time with the definition:

  ```
  SUBSYS SUBNAME(LOGR) INITRTN(IXGSSINT)
  ```

  The RECxxxxx DD used to read the data has the format:

  ```
  //RECxxxxx DD  DSN=IFASMF.DATA.LOGSTRM,DISP=SHR,
  //          SUBSYS=(LOGR,IFASEXIT,subsys-options1,subsys-options2)
  ```

  Description of SUBSYS options-1 includes:

  ```
  [FROM={({[yyyy/ddd][,hh:mm[:ss]]}) | OLDEST}]
  [TO={({[yyyy/ddd][,hh:mm[:ss]]}) | YOUNGEST}]
   [,DURATION=(nnnn,HOURS)]
   [,VIEW={ACTIVE|ALL|INACTIVE}]
   [,GMT|LOCAL]
  ```

The subsys-options1 parameters used by the IBM IFASEXIT are the same as those used by the IFBSEXIT. For information on the parameters for IFBSEXIT, see IBM's *MVS Diagnosis: Tools and Service Aids*.

Logging Successful Events

Turning on user logging or audit options in an HFS file can cause logging to occur even when access is allowed.

Adding TRACE to an acid causes all the acid's activity (including USS events) to be recorded in SMF. Use the following command to log all activity for an acid:

```
TSS ADDTO(acid)TRACE
```

The owner of a USS file can set the user audit attribute of the file using the chaudit USS command. Each attributes is set based on the access being attempted to the file. If AUDIT attributes or flags are turned on in a file for the type of file access requested, the access is logged by writing an SMF record.

Running the Report Using JCL

The TSSOERPT report uses CA Top Secret report JCL. For example:

```
//TSSOERPT JOB 1,'USS RPT',MSGCLASS=A,TYPRUN=HOLD
//*
//REPORT EXEC PGM=TSSOERPT,PARM='TITLE(USS EVENTS)'
//*
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//RECMAN1 DD DSN=IFASMF.XE15.TSSLOG,DISP=SHR,
//SUBSYS=(LOGR,IFASEXIT)
//SYSIN    DD *
  DETAIL
/*
//
```

TSSOERPT JCL Parameters

The TSSOERPT JCL parameters are specified using the PARM= keyword on the exec statement or in the SYSIN dataset. The SUMMARY, DETAIL, LINECNT, and TITLE parameters control report formatting. The UID, GID, USER, GROUP, SERVICE, ERROR, INCLUDE, EXCLUDE, JOBMASK, SDATE, EDATE, STIME, and ETIME parameters select which events are included in the report.

EDATE(169365|cyyddd)

Specifies the ending Julian date from which report information is selected, where c is required and specifies the century. Enter 1 for years greater than (>) 2000 or 0 for years less than (<) 2000. When combined with the SDATE parameter, this parameter creates a window for report content. The defaults for SDATE and EDATE process all available records.

ERROR

Specifying ERROR restricts the output of the report to include only entries for services that end with a SAF RC greater than zero. This helps produce a report that is easier to read when attempting to resolve a USS setup problem. If ERROR is not specified.

Default: Report on all SMF records that are written.

ETIME(2359|hhmm)

Specifies the end-of-time interval from which SMF records are selected based on a 24-hour clock. SMF records generated after this specified time of day are ignored. The selection of records begins at the STIME specified for each date in the SDATE/EDATE range and ends on each date at the ETIME given. The defaults for STIME and ETIME process all available records.

EXCLUDE(service1,service2, …,servicen)

Specifies the SAF callable services to be omitted from the report. Services specified in EXCLUDE can be masked with a dash (-) and multiple services can be specified. For information on these services, see the IBM z/OS Security Server (RACF) Callable Services guide.

If SERVICE, INCLUDE and EXCLUDE are not specified.

Default: All services.

Note: This parameter is mutually exclusive with the SERVICE parameter.

GID(value)

Specifies the USS GID you intend to collect security information for. This field is not maskable.

Range: 0 to 2,147,483,647.

Default: All GID values.

GROUP(groupname)

Specifies the group for which you want USS security information collected. This field is maskable.

Default: All groups.

INCLUDE(service1, service2,…,servicen)

Specifies the SAF callable services for which you want security information collected. Services specified in INCLUDE can be masked with a dash (**-**) and multiple services can be specified.

For information, see the IBM z/OS Security Server (RACF) Callable Services guide.

Default: All services.

Note: This parameter is mutually exclusive with the SERVICE parameter.

JOBMASK(******|jobmask1,...,jobmask8)**

Specifies that records appearing on the report are limited to those for the jobs indicated by the job name mask. Use commas or spaces to separate multiple job name masks. Up to 8 job masks can be specified.

Default: All jobs.

LINECNT(60|nnnnn)

The LINECNT parameter specifies the number of output lines to be printed on a page. The maximum number of output lines per page is limited only by the physical constraints of the output media used, or to 99,999 lines.

Default: 60 lines per page.

PRINTER|TERMINAL

Specifying TERMINAL produces report output formatted for an 80 character per line display. Specifying PRINTER produces report output formatted for 133 character per line printed output.

Default: TERMINAL.

SDATE(000000|cyyddd)

Specifies the beginning Julian date from which report information is selected, where c is required and specifies the century. Enter 1 for years greater than (>) 2000 or 0 for years less than (<) 2000. Any input SMF records generated before the SDATE value are ignored.

SERVICE(service)

Specifies the name of the SAF callable service for which you want security information collected. For information, see the IBM z/OS *Security Server (RACF) Callable Services* guide.

Default: All services.

Note: The SERVICE parameter is mutually exclusive with the INCLUDE and the EXCLUDE parameter.

STIME(000000|hhmm)

Specifies the beginning-of-time interval from which SMF records are selected based on a 24-hour clock. SMF records generated before this time are ignored. The selection of records begins at the STIME specified for each date in the SDATE/EDATE range and ends on each date at the ETIME given.

Default: Process all available records.

SUMMARY|DETAIL

Specifying SUMMARY produces a three-line entry for each event logged. Specifying DETAIL produces report entries that include all the information available for each logging event.

Default: SUMMARY.

TITLE(string)

Specifies a one to 35 character string added to other title information at the top of the report. If this character string is longer than 35 characters, an error message is issued.

Default: USS Event Log.

UID(value)

Specifies the USS UID for which you intend to collect security information. Acceptable numeric values range from zero to 2,147,483,647. This field is not maskable.

Default: All UID values.

USER(acid)

Specifies the acid for which you want USS security information collected. This field is maskable and it is case sensitive.

Default: All acids.

Sample Output

This TSSOERPT report shows the logging of security events in a USS environment:

```
Mainframe Security - z/OS USS Event Log       - PAGE    1
 DATE 03/04/05 (06.007) TIME 12.34

      SERVICE      USERID    GROUP        UID         GID    SAF  RC   RSN
        DATE          TIME    JOBNAME   SOURCE   SYSID   CPU   SECLABEL

   R_writepriv      USER01  OMVSGRP       8888888       44444   4    4    0
   01/07/05  05.007   12.23.26 USER01                    CPU1
   Failed - Write-Down by user is not active on this system.
    Function: Query

   getGMAP          USER01  OMVSGRP       8888888       44444   0    0    0
   01/07/05  05.007   12.24.27 USER01                    CPU1
   Successful - Logging active by Trace/Audit options
    UID/GID value:            0
    Map name:      ZEROGRP      Search by GID/UID

   ck_access        USER01  OMVSGRP       8888888       44444   8    8    4
   01/07/05  05.007   12.24.31 USER01                    CPU1
   Failed - User not authorized to access file
    Function: chdir               User Type: Local
    Requested Access: Search
    Name flag:     Use CRED_name_flag to determine pathname
    Pathname: dev
    Filename: dev
    File Permissions: Owner: rwx Group: --- Other: r--
    Owning UID:           0   Owning GID:          10
    Volume  : TSO02A  File Identifier:   208505000000000003
    File Audit Options:
    User    : Read Failure  Write Failure  Exec/Search Failure
    Auditor : Read Failure  Write Failure  Exec/Search Failure
```

Sample Output with MLS Security Active

```
   ck_access        USER01  OMVSGRP        8888888          10   0    0    0
   01/07/05  05.007   12.56.44 USER01                   CPU1   SYSLOW
   Successful - Logging active by Trace/Audit options
    Function: open  User Type: Local
    Requested Access: Read
    Name flag: Use CRED_name_flag to determine pathname
    Pathname: /usr/file2
    Filename: file2
    File Permissions: Owner: rw- Group: r-- Other: r--
    Owning UID:          0     Owning GID:           0   SECLABEL: BCD
```

```
Volume  : TSO01S  File Identifier:   00010E000000230000
File Audit Options:
User    : Read Failure  Write Failure  Exec/Search Failure
Auditor : Read None     Write None     Exec/Search None
```

TSSOERPT Field Descriptions

All entries in the TSSOERPT report contain the fields described below in the first three lines of the entry. If DETAIL is specified, entries for some services include additional information.

SERVICE

The type of service requested.

USERID

The acid of the user the request was made for.

GROUP

The GROUP the user is associated with.

UID

The z/OS UNIX UID number of the user.

GID

The z/OS UNIX GID number of the user.

SAF

The SAF return code. For all services:

- 0-Successful completion
- 4-CA Top Secret not active
- 8-Request denied. See explanation line

RC

The CA Top Secret return code. For all services:

- 0-Successful completion
- 8-Request denied. See explanation line

RSN

The SAF reason code.

DATE

The Julian and Gregorian date when the access was attempted.

TIME

The time of day when the access attempt occurred.

JOBNAME

The name of the job under which the access was attempted.

USER-SECLABEL

The 8-byte session seclabel.

FSP-SECLABEL

The 8-byte file or directory seclabel. For information on implementing MLS on a system using CA Top Secret, see the Multilevel Security Planning Guide.

CPU

The SMF name of the CPU that validated the request.

EXPLANATION LINE

An explanation of the return and reason codes for this call. States if the request failed or succeeded and provides a brief explanation of the disposition. Failed request messages are customized to reflect the reason for the failure. Successful requests resemble:

```
Successful - Logging active by Trace/Audit options
```

Service Field Values

This section describes the possible values for the SERVICE, INCLUDE, and EXCLUDE fields of the TSSOERPT report. These values are case-sensitive.

Note: Additional information that appears on the report when the DETAIL option is specified is a function of the call.

ck_access

Determines if a user has the requested access (READ, WRITE, EXECUTE, or SEARCH) to the specified file or directory.

ck_file_owner

Checks if a current process is a superuser or the owner of the specified file. A process could be the owner of a file if the effective UID is equal to the file owner's UID.

ck_IPC_access

Determines whether the current process has the requested access to the interprocess communication (IPC) key or identifier whose IPC security packet (IISP) is passed.

ck_owner_2_files

Checks whether the calling process is a superuser or is the owner of the file/directory, or directory/directory entry pair represented by input FSP1 and FSP2. A process is the owner of the file if the processes effective UID is equal to the file's owner UID.

ck_priv

Determines if the calling process is a superuser.

ck_process_owner

Checks to see if the calling process is the owner of a process being called.

clear_setid

Clears temporary access given to a file or directory. (Resets the S_ISUID, S_ISGID, and S_ISVTX bits in the file's or directory's access permissions to zero. For information, see the IBM *z/OS UNIX System* Services *User's Guide.*

deleteUSP

Indicates that the user's access to USS terminated.

getGMAP

Indicates that a call was made to determine the GID for a groupname or the groupname for a GID.

get_uid_gid_supg

Gets the real, effective, and saved UIDs and GIDs, and the supplemental groups from the USP.

getUMAP

Indicates that a call was made to determine the UID for a username or the username for a UID.

initACEE

Provides an interface for creating and managing security contexts created through the pthread_security_np service.

initUSP

Indicates initial user access to USS.

- Home-The home directory of the user at initial access to USS.
- Program-The name of the program for the indicated user at initial access to USS.

makeFSP

Seen when a file or directory is created.

- File Type-The file type of the file for which the FSP is being created. Tells whether a file is a directory, a regular file, or one of several special types of files.
- File Permissions-The file access permissions to be assigned to the indicated file. These are displayed in the fields named Owner, Group, and Other. Values for the fields are r for READ, w for WRITE, x for EXECUTE, and s for SEARCH.

makeISP

Builds an IISP in the area provided by the caller.

make_root_fsp

Indicates that a new file system is being initialized in a new PDSE/x data set.

query_file_opts

Indicates that file security options were queried to determine the settings.

query_sys_opts

Indicates that system security options were queried to determine the settings.

R_admin

Allows applications to pass an CA Top Secret command buffer used to update the CA Top Secret secfile.

R_audit

A record cut in addition to a security service record. The record supplies additional information about the file being audited.

R_cacheserv

Indicates a call was made for cache services. A cache is stored in a data space and contains security relevant information. The cache functions are:

- START-Start a new cache.
- ADD-Add a record to the new cache.
- END-End cache creation.
- FETCH-Fetch a record from the cache.
- DELETE-Delete the cache.

R_chaudit

Indicates that a file's Audit Options have been changed.

- User Audit Options-Indicates what type of user access to this file should be audited.
- Auditor Audit Options-Indicates what type of auditor access to this file should be audited.

R_chmod

Indicates a file's permissions (mode) have changed.

- File Type-The file type of the file whose permissions are being changed. It indicates if a file is a directory, a regular file or one of several special types of files.
- File Permissions-The file access permissions assigned to the indicated file. These are displayed in the fields named Owner, Group, and Other. Values for the fields are r for READ, w for WRITE, x for EXECUTE, and s for SEARCH.

R_chown

Changes a file's owning UID and GID to a new value.

- UID To Be Set-The UID number the file's owning UID is being set to.
- GID To Be Set-The GID number the file's owning GID is being set to.

R_datalib

Implements OCSF data library support, which provides access to digital certificates connected to a keyring.

- Function-The specific R_datalib function being invoked, such as DataGetFirst or DataGetNext.
- Userid-The userid the KEYRING profile record belongs to or blanks if the KEYRING profile record is owned by the issuer of the request.
- Ring Name-The ring name of the KEYRING profile record.

R_dceauth

Enables an application server to check a user's authority to access a CA Top Secret defined resource. Used only for the USS kernel on behalf of an application server.

R_dceinfo

Retrieves or sets fields in the DCE USER profile record.

R_dcekey

Enables USS DCE to retrieve or set a DCE password (key).

R_dceruid

Enables USS DCE to determine the user ID of the client from the string forms of the client's DCE UUID pair.

- Function-The specific function being processed (“Return RACF userid” or “Return DCE UUID”).
- Userid-The CA Top Secret acid.
- Principal-The string form of the principal DCE UUID.

R_exec

Changes the effective and saved UID or GID or both.

- Set UID-Change made to UID.
- Set GID-Change made to GID.

R_fork

Indicates a call was made to get the security information for a forked process.

R_getGroups

Indicates a call was made to determine what groups the current process or user belongs to.

R_getgroupsbynam

Indicates that a call was made to determine the groups to which a specific userid belongs.

R_IPC_ctl

Performs functions based on a function code.

R_kerbinfo

Retrieves or sets SecureWay Security Server Network Authentication Service fields. The service returns principal or realm information and updates the count of invalid attempts at accessing the SecureWay Security Server Network Authentication Service. The invalid key count is also cleared upon successful access to the service.

R_ptrace

Indicates that a check was made to see if a calling process can ptrace a target process it is calling.

R_PKIServ

Allows applications to request the generation retrieval and administration of V3 X.509 digital certificates.

R_proxyserv

Allows applications to invoke the LDAP component of the Security Server for z/OS to obtain data which resides in an LDAP directory.

R_setegid

Changes the effective GID to a different GID

- GID To Be Set-The GID to be set as the effective GID
- Real GID-The actual GID of this user
- Effective GID-The GID under which this user's accesses are being validated
- Saved GID-Internally used GID

R_seteuid

Changes the effective UID to a different UID.

- UID To Be Set-The UID to be set as the effective UID
- Real UID-The actual UID of this user
- Effective UID-The UID under which this user's accesses are being validated
- Saved UID-Internally used UID

R_setfacl

Indicates a call was made to create or modify an Access Control List.

- Operation-The type of operation performed; Add, Modify, or Delete.
- ACL Type-The type of ACL affected; Access, Directory Model, or File Model.
- UID/GID-The UID or GID for this ACL entry.
- Permissions-The octal value of the file permissions specified for this user or group. If PERM-DEL the ACL entry for the specified UID/GID is deleted.

R_setfsecl

Changes the security label in the FSP

R_setgid

Changes the real, effective, and saved GIDs to a different GID.

- GID To Be Set-The GID to be set as the current GID
- Real GID-The actual GID of this user
- Effective GID-The GID under which this user's accesses are being validated
- Saved GID-Internally used GID

R_setuid

Changes the real, effective and saved UID to a different UID.

- UID To Be Set-The UID that is to be set as the current UID.
- Real UID-The actual UID of this user or process.
- Effective UID-The UID under which this user's accesses are being validated.
- Saved UID-Internally used UID

R_ticketserv

This service enables application servers to parse or extract principal names from a GSS-API context token. This enables an application server to determine the client principal who originated an application-specific request when the request includes a GSS-API context token.

R_umask

Change of permissions that a program sets in a new file or directory when it creates a new file or directory.

R_usermap

Enables z/OS application servers to determine the application user identity associated with an CA Top Secret acid, or to determine the CA Top Secret acid associated with an application user identity or digital certificate. Currently, the only supported applications are Lotus Notes for z/OS and Novell Directory Services and SecureWay Server Network Authentication Server.

R_writepriv

Sets, resets, or queries the setting of the write-down privilege in the ACEE. When MLS is active, the following fields are captured on the TSSOERPT report:

Security Credentials and File Security Packets

Many log entries show additional information about the request. The information is contained internally as Security Credentials (CRED) and File Security Packets (FSP). This information is common to many calls and can appear in the following fields on the TSSOERPT report if it is available:

FUNCTION

Specifies the function attempted for a file or directory, for example OPEN and SEARCH.

PATHNAME

Specifies the full pathname of a file or directory, including the file or directory name itself. There could be two pathnames specified if the call involved more than one file or directory.

FILENAME

Specifies the name of a file or directory. In the case of a ck_access, this field names the part of the path currently being validated for access (If the path is *aa/bb/cc* three separate ck_access calls are seen: the first with filename *aa,* the second with filename *bb,* and the third with filename *cc*). There can also be two filenames specified if the call involved more than one file or directory.

FILE PERMISSIONS

Specifies the access permissions for the file's owning UID (owner), the file's owning GID (group), and all others attempting access (other).

OWNING UID

Specifies the UID of the owner of the file or directory. If the real UID of a user or process attempting access to this file matches the owning UID, access is granted according to the owner file permissions.

OWNING GID

Specifies the GID of the owner of the file or directory. If the real GID of a user or process attempting access to this file matches the owning GID, access is granted according to the group file permissions. If the process or user does not have the owning GID as its primary GID, but has a supplemental group that matches the owning GID, access is also determined by the group file permissions.

Note: If the GID or UID do not match the owner's GID or UID, the other file permissions are used to determine access.

VOLUME

Specifies the volume on which the file system that contains the file resides.

FILE IDENTIFIER

In some cases pathname or filename are not indicated in a call. In this occurs, access is validated using the file identifier. To determine the path and filename for this call, find the last previous call with the same file identifier. The pathname and filename for that call are the same as for the call in question.

FILE AUDIT OPTIONS

The file audit options are:

- U-Indicates the type of file access that should be logged for a user. For example, if the report shows “Read Failure, Write All, Exec/Search None,” all failed READ attempts, all WRITEs, but no EXECs or SEARCHes are logged to SMF for the user.
- Auditor-Indicates the type of file access that should be logged for an auditor. For example, if the report shows “Read Failure, Write All, Exec/Search None,” all failed READ attempts, all WRITEs, but no EXECs or SEARCHes are logged to SMF for the auditor.

Chapter 9: TSSPROT Utility

This section contains the following topics:

About the TSSPROT Utility

The TSSPROT utility is used to secure (or unsecure) MVS data sets, generally in an SU-32 (non-SAF) environment. Both VSAM and non-VSAM data sets can be processed. A secured data set is one that has a RACF security indicator turned on. This indicator is recognized by the MVS Standard Security Interface and its drivers.

Note: If your system operates under an MVS Alwayscall environment this process is not required.

TSSPROT JCL Requirements

To execute TSSPROT, use the following JCL:

```
//JOBNAME          JOB
//TSSPROT          EXEC          PGM=TSSPROT
//PROTOUT          DD            SYSOUT=*
//PROTIN           DD *
  (control statements)
/*
```

Only the MSCA can use this utility. TSSPROT should ideally be run on an idle system, when no data sets are currently open. If TSSPROT secures a data set that is open, the DSCB security indicator may be reset when the data set is closed. The report will indicate that the data set was protected. To avoid this situation, execute TSSPROT with no jobs active. No indication is provided that a data set was not processed.

Error messages and abend codes can be found in the *Messages and Codes Guide.*

TSSPROT Keywords

The following keywords can be used with the TSSPROT PROTECT and UNPROTECT verbs:

- DSNPRX
- MSS
- PASSWORD
- SIM
- UNIT
- USERCAT
- VOLUME

Use PROTECT or UNPROTECT to begin coding options. You can code more than one statement but CA Top Secret processes each one separately. The following operands apply to the TSSPROT keywords:

```
                [ Dsnprx(dsn,...)          ]
                [ MSS                      ]
                [ PASSWORD(IGNORE)         ]
                [          (PROTECT)       ]
                [ SIM                      ]
                [ UNIT                     ]
{Protect  }     [ USERCAT({AIX         }) ]
{Unprotect}     [         ({CLUSTER    }) ]
                [         ({DATA       }) ]
                [         ({GDG        }) ]
                [         ({INDEX      }) ]
                [         ({PATH       }) ]
                [         ({SPACE      }) ]
                [         ({USERCATALOG}) ]
                [ Volume                   ]
```

In the syntax, verbs and keywords can be entered in free format, separated by spaces. A verb must be the first operand per request. A request is considered one statement. To continue a statement, supply a dash (-) at the end of the last operand, then continue from position one of the next statement. For example:

```
P CAT(CATALOG.VSYSA01)  DSN('GCC.TCTTT11.RESLIB') -
VOL(PROD)
```

PROTECT

Requests that TSSPROT secure the data sets identified by keywords. PROTECT with no keywords protects all non-VSAM data sets on all accessible volumes. (The keywords are described in the next section.)

UNPROTECT

Requests that TSSPROT remove its protection (turn off the MVS protection indicator) from data sets identified by the keywords. UNPROTECT with no keywords removes protection from all non-VSAM data sets on all accessible volumes.

Note: This utility will only (un)protect data sets and volumes that are accessible to the caller. Only the MSCA can use this utility.

To get VSAM protection, the catalog itself must be protected via TSSPROT. MVS does not properly recognize individual data set protection if the associated catalog is not secured.

The following keywords identify the data sets to be processed by TSSPROT to dynamically allocate selected volumes.

DSNPRX

Identifies a data set for processing.

```
P DSNPRX(datasetname)
```

datasetname

A list of up to 20 full data set names or data set prefixes. TSSPROT processes the single data set or all data sets that match the prefix. A specific data set is supplied within single quotes.

MSS

Indicates that the (un)protect operation is carried out against a specific mass storage volume. The VOLUME keyword must specify a specific volume and not a volume prefix. The UNIT value should refer to your MSS volume.

```
P MSS
```

PASSWORD

Requests the type of processing to be performed for data sets that are password protected through the operating system. When a password-protected data set is protected, it loses its MVS password protection and gains CA Top Secret protection. Therefore, these data sets should only be secured when about to run in FAIL or IMPLEMENT mode.

```
P PASSWORD(IGNORE|PROTECT)
```

PROTECT

CA Top Secret will control password-protected data sets.

IGNORE

(Default) Data sets will retain their MVS passwords.

SIM

Requests that no changes be made to the selected DSCBs and VSAM catalogs for testing or auditing purposes. When you specify this option, the operation will proceed but no processing is performed. A simulated report is generated.

```
P SIM
```

UNIT

Is the unit name used by TSSPROT to limit processing to selected volumes.

```
P UNIT(name)
```

name

The unit name. The default is SYSALLDA.

USERCAT

Indicates a target catalog for processing.

```
P USERCAT(catalogname)
```

catalogname

The catalog name. The following are valid for processing:

- AIX
- CLUSTER
- DATA
- GDG
- INDEX
- PATH
- SPACE
- USERCATALOG

If a USERCATALOG is processed, all valid entries in the USERCATALOG is processed. If a CLUSTER is processed, all VSAMDSETs (system-generated names) associated with the CLUSTER is processed. Only one VSAM catalog may be processed with each execution of TSSPROT.

Note: To protect a catalog or a user catalog, it must be protected as a data set and the PROTECT statement must include a CAT reference to the catalog or user catalog.

VOLUME

Identifies a volume for processing.

```
P VOLUME(volser)
```

vol

A full volume serial or volume prefix. TSSPROT processes the single volume or all volumes that match the prefix. If you omit the VOLUME option, TSSPROT selects all resident volumes for processing.

TSSPROT Examples

The following are examples of PROTECT requests.

PROTECT D(SMPPROD) VOL(TSO) UNIT(3380)

```
97.192         TOP SECRET SECURITY              DATASET PROTECTION UTILITY (V5.1)  PAGE   1
PROTECT D(SMPPROD) VOL(TSO) UNIT(3380)
97.192         TOP SECRET SECURITY              DATASET PROTECTION UTILITY (V5.1)  PAGE   2

                PROCESSING VOLUME:  TSO38B
  SMPPROD.TSS.TSSCFILE                                    PROTECTED
  SMPPROD.TSS.EARLOUT                                     PROTECTED

97.192         TOP SECRET SECURITY              DATASET PROTECTION UTILITY (V5.1)  PAGE   3

                  PROCESSING VOLUME:  TSO38A
  SMPPROD.SDSF.OUTPUT                                     PROTECTED
  SMPPROD.TSS44.CNTL                                      PROTECTED
  SMPPROD.TSS43.CNTL                                      PROTECTED
  SMPPROD.CICSV330.CNTL                                   PROTECTED
  SMPPROD.XE38.CNTL                                       PROTECTED
  SMPPROD.USER.CATALOG                                                IGNORED - VSAM DATA
  SMPPROD.USER.CATALOG.CATINDEX                                       IGNORED - VSAM DATA
  SMPPROD.SPUFI.INPUT                                     PROTECTED
```

PROTECT PASSWORD(PROTECT) VOL(MVXE38)

```
PROTECT PASSWORD(PROTECT) VOL(MVXE38)
97.192     TOP SECRET SECURITY  DATASET PROTECTION UTILITY (V5.1)  PAGE   6

             PROCESSING VOLUME:  MVXE38
SYS1.VTOCIX.MVXE38                     PROTECTED
ICF.VMVXE38                                 IGNORED - VSAM DATA
SYS1.VVDS.VMVXE38                           IGNORED - VSAM DATA
ICF.VMVXE38.CATINDEX                        IGNORED - VSAM DATA
VTAM.LOCAL.VTAMLST                     PROTECTED
TSSJHB.ISPF.ISPPROF                    PROTECTED
TSSMVS.CAI.P9409.CAICICS               PROTECTED
SYS95082.T124525.RA000.ROS60.R0000109          IGNORED - TEMPORARY DATASET
SYS1.STGINDEX.DATA                             IGNORED - VSAM DATA
SYS1.STGINDEX.INDEX                            IGNORED - VSAM DATA
SYS1.MAN1.DATA                                 IGNORED - VSAM DATA
SYS1.MAN2.DATA                                 IGNORED - VSAM DATA
SYS1.MAN3.DATA                                 IGNORED - VSAM DATA
SYS2.LEVEL1.CICS33A.LOADLIB            PROTECTED
LIBR.DUNLA01.TEST41                    PROTECTED
     .              .
     .              .
     .              .
     .              .
ISF.HASPINDX                           PROTECTED
ROBIA03.ISPF.ISPPROF                   PROTECTED
SYS2.ADAM.CLIST                        PROTECTED
```

PROTECT CAT(ICF.VMVXE38)

```
97.192        TOP SECRET SECURITY            DATASET PROTECTION UTILITY (V5.1)              PAGE
17
  PROTECT CAT(ICF.VMVXE38)
    0000000000000000000000000000000000000000000000                                    ENTITY NOT
FOUND
    ICF.VMVXE38                                          PROTECTED
    ICF.VMVXE38.CATINDEX                                 PROTECTED
    DABAD01.CICS.KSDS                                    PROTECTED
    DABAD01.CICS.KSD.DATA                                PROTECTED
    DABAD01.CICS.IDX.INDEX                               PROTECTED
    DABAD01.VSAM                                         PROTECTED
    DABAD01.VSAM.KSD.DATA                                PROTECTED
    DABAD01.VSAM.IDX.INDEX                               PROTECTED
    PAGE.VMVXE38.COMMON2                                 PROTECTED
    PAGE.VMVXE38.COMMON2.DATA                            PROTECTED
    PAGE.VMVXE38.LOCAL3                                  PROTECTED
    .                 .
    .                 .
    .                 .
    .                 .
    SYS2.LEVEL1.V211.DFHTEMP                             PROTECTED
    SYS2.LEVEL1.V211.DFHTEMP.DATA
```

PROTECT SIM

```
 97.192        TOP SECRET SECURITY            DATASET PROTECTION UTILITY (V5.1)             PAGE
20
 PROTECT SIM
 97.192        TOP SECRET SECURITY            DATASET PROTECTION UTILITY (V5.1)             PAGE
21

                  PROCESSING VOLUME:  MV136A
    SYS1.VTOCIX.MV136M                                      PROTECTED
    IPO1.LEVEL89A                                           PROTECTED
    SYS1.VSCOBLIB                                           PROTECTED
    IPOPPS.LINKLIB                                          PROTECTED
    IPOUSER.PROCLIB                                         PROTECTED
    IPOUSER.LINKLIB                                         PROTECTED
    SYS1.LINKLIB                                            PROTECTED
    SYS1.PLILINK                                            PROTECTED
    SYS1.CMDLIB                                             PROTECTED
    SYS1.LOGREC                                             PROTECTED
    SYS1.PROCLIB                                            PROTECTED
    SYS1.PARMLIB                                            PROTECTED
    SYS1.BRODCAST
    SYS1.UADS
    SYS1.MACLIB
    SYS1.IMAGELIB                                           PROTECTED
    ANDMA02.MACLIB.ASM                                      PROTECTED
    SKOJE02.CV.V1L092DV.CNTL                                PROTECTED
    SKOJE02.CV.V1L092XX.CNTL                                PROTECTED
    .                 .
    .                 .
    .                 .
    .                 .
    SKOJE02.CVD.V1L0R430.MAC                                PROTECTED
    SKOJE02.CVD.V1L0R430.OBJECT                             PROTECTED


                                          ***  NO DATASETS PROCESSED  ***
 97.192        TOP SECRET SECURITY           DATASET PROTECTION UTILITY (V5.1)             PAGE
355
```

Chapter 10: LDS Recovery

This section contains the following topics:

About LDS Recovery

The LDS recovery report (LDSRPT), lists all LDS requests stored in the LDS Recovery File. LDS recovery retrieves records containing information pertaining to administrative commands that ADD, REPLACE, and DELETE ACID fields as well as password changes that are eligible for LDS processing. There are no REPORT parameters for this program.

Note: Only a person with SCA or AUDIT privileges is eligible to run the LDSRPT report.

Sample JCL

The following is sample JCL to run the LDSRPT report:

```
//LDSRPT        EXEC    PGM=CAS4LRPT
//STEPLIB       DD      DSN=CAI.CAILIB,DISP=SHR
//LDSRCVR       DD      DSN=CALDAP.LDSRCVR,DISP-SHR
//SYSPRINT      DD      SYSOUT=*
```

Sample Report Output

The report title displays the date and time the report was generated. The report summary displays the total number of LDS recovery records on the LDS Recovery File. The following is a sample of the LDSRPT report output:

```
04.182) TIME 12.33  -  Security LDS Recovery Report         -  PAGE     1
Date    Time    LDAP Node ID    User     LDS Recovery Data

2004121 153451  LDAP.LISLE2     LDSETA2  INS LID(LDSETA2 ) OBJECTCLASS(TSSLID), ADD Name(1534       ),
ADD objectclass(AC
2004121 153451  LDAP.LISLE2      LDSETA2      F2LID)
2004121 154026  LDAP.LISLE2      LDSETA2  DEL LID(LDSETA2 ) OBJECTCLASS(TSSLID)
2004121 160905  LDAP.LISLE2     LDSETA1  MOD LID(LDSETA1 ) OBJECTCLASS(TSSLID), REP Name(1608       )
2004121 162455  LDAP.LISLE2     LDSETA3  MOD LID(LDSETA3 ) OBJECTCLASS(TSSLID), REP Name(1624       )
2004121 162936  LDAP.LISLE2     LDSETA2  INS LID(LDSETA2 ) OBJECTCLASS(TSSLID), ADD Name(THIRD      ),
ADD objectclass(AC
2004121 162936  LDAP.LISLE2      LDSETA2      F2LID)
DATE 06/30/04 (04.182) TIME 12.33  -  CA Top Secret Security LDS Recovery Report         -  PAGE     2

  -  Total number of LDS records processed is  05
```

Field Descriptions

Date

The date the LDS recovery record was stored on the LDS Recovery File.

Time

The time the LDS recovery record was stored on the LDS Recovery File.

LDAP Node ID

The LDAP Node Record ID of the LDAP server that the LDS request was originally transmitted.

User

The user's logonid of the LDS request that was updated by the CA Top Secret administrator.

LDS Recovery Data

The type of LDS request, including the list of LDAP attribute names and values to be transmitted to the LDAP server. To protect password based attribute data values from disclosure, password values are displayed as “SUPPRESSED” in this report.

Chapter 11: Certificate Utility

This section contains the following topics:

About the Certificate Utility

Use the Certificate Utility to display the certificate hierarchy in your database. Optionally, it will display each certificate, its signing certificate, the certificates that it has signed, and all of the information provided with the CHKCERT and LIST commands. Execution of SAFCRRPT requires a region size of 1500K.

You can tailor the output to display certificates:

- For a specified user
- For a specified key ring
- That have not expired
- That have a key in ICSF
- That are currently trusted
- That will expire within a specified number of days

If you are having a problem setting up SSL for an application, run the utility against the key ring to identify problems in the set up.

Authorization

If the certificates are *not* obtained from a key ring, update access to IRR.DIGTCERT.LIST in the IBMFAC class is required to run the report.

If the certificates are from a key ring, the utility uses the R_datalib callable service. R_datalib requires READ access to the IRR.DIGTCERT.LISTRING resource in the IBMFAC class when the key ring is owned by the caller of the utility.

If the key ring is *not* owned by the caller of the utility, or the key ring is owned by CERTAUTH or SITE, UPDATE access is required to the IRR.DIGTCERT.LISTRING resource.

Sample Certificate Utility JCL

The following is sample JCL to run the certificate utility. This JCL is found in the CAI.CAKOJCL0 file on the distribution tape. The member name is CERTUTIL:

```
//SAFRPTCR   EXEC PGM=SAFCRRPT,PARM='TITLE(Certificate detailed report)'
//STEPLIB    DD   DISP=SHR,DSN=CAI.CAKOLINK
//SYSUDUMP   DD   SYSOUT=*
//SYSPRINT   DD   SYSOUT=*
//SYSIN      DD   *
Recordid(CERT-) detail EXT
```

Sample Output - Summary

```
Mainframe Security - SAFCRRPT - Certificate Utility    - PAGE    3
DATE 03/14/06 (06.073) TIME 10.18

Record id - CERTAUTH.AUTO014           Signed by:  None - Self-Signed
            Signer of -     CERTAUTH.AUTO013
Record id - CERTAUTH.BOB               Signed by:  None - Self-Signed
Record id - CERTAUTH.CLIFFTA           Signed by:  None - Self-Signed
Record id - CERTAUTH.DSACA             Signed by:  None - Self-Signed
         Signer of -   BOB.DSA2048      CARLA01.DSA2048  CARLA01.DSA512
                       CARLA01.DSA768   CARLA01.RSA512   CARLA01.RSA768
                       DSATEST.DSA1024  DSATEST.DSA2048  DSATEST.DSA512
                       KERMIT.DSA       KERMIT.RSA
Record id - CERTAUTH.EDDIEABC          Signed by:  None - Self-Signed
Record id - CERTAUTH.HAWKS01           Signed by:  None - Self-Signed
Record id - CERTAUTH.HAWKS02           Signed by:  None - Self-Signed
Record id - CERTAUTH.HAWKS03           Signed by:  None - No Record Found
Record id - CERTAUTH.HEROS             Signed by:  None - No Record Found
Record id - CERTAUTH.ICSFCA            Signed by:  None - Self-Signed
         Signer of -   CARLA01.ICSFCA  IMWEBSRV.ICSFSSL  IMWEBSRV.SSLICSF
                       STANLEY.ICSFCA
Record id - CERTAUTH.ICSF01            Signed by:  None - Self-Signed
Record id - CERTAUTH.LOCALCA           Signed by:  None - Self-Signed
         Signer of -   CARLA01.T2048    GENC002A.AUTO001  GENC002A.AUTO002
                       GENC002A.AUTO003 GENC002A.AUTO004  IMWEBSRV.SERVER
                       TIMOTHY.DEE      WEBSRV
Record id - CERTAUTH.MAJORLG           Signed by:  None - Self-Signed
         Signer of -    CERTAUTH.AL       CERTAUTH.NL
```

Sample Report Output - Detail

```
Mainframe Security - SAFCRRPT - Certificate Utility    - PAGE   11
DATE 03/14/06 (06.073) TIME 10.18

Record id - CERTAUTH.AL               Signed by:  CERTAUTH.MAJORLG
            Label           American League CA
            Serial #  -     05
            Issuer  DN -    CN=Major League Baseball Certificate Authority.
                            OU=Used for testing PKCS 12 CA certificate insert
                            processing.O=MLB Commissioners Office.C=US
            Subject DN -    CN=American League Certificate Authority.O=Major
                            League Baseball.C=US
            Active Date     2004/11/30
            Expire Date     2015/12/20
            Pub Key Size    1024  RSA
            Public Key      0000  30819F30 0D06092A 864886F7 0D010101
                            0010  05000381 8D003081 89028181 00D7F4B8
                            0020  BCA5B3B0 D33F5575 C7EF5F48 9ABC4C77
                            0030  5F46257B 13C3A9A7 B497F422 EFDD8B44
                            0040  9F756234 76D70DFC 2A6B3FE6 40532234
                            0050  0147CC94 4DB0ABD4 732729B4 9E8FBD44
                            0060  F7DAFB00 33ED254D EB0A6334 8FD0ECEB
                            0070  4374317C D4CBB1AE B7C6FD08 0412785B
                            0080  0A751C69 3BF4DC66 C2CBA8F1 093BAE10
                            0090  3604CC15 66CF8A5D 2EF9038A 03020301
                            00A0  0001
                            Signer of -     CERTAUTH.ACENTRAL CERTAUTH.ALWEST

Record id - CERTAUTH.LOCALCA          Signed by:  None - Self-Signed
            Label           Local CA
            Serial #  -     0000000000
            Issuer  DN -    CN=CA-TSS Certificate Authority.OU=CA-AC
                            F2 Development.OU=OS390 Development.O=Computer
                            Associates
                            Subject DN -    CN=CA-TSS Certificate Authority.OU=CA-AC
                            F2 Development.OU=OS390 Development.O=Computer Associates
            Active Date     2001/09/05
            Expire Date     2002/09/05
            Pvt Key Size    512  RSA
            Public Key      0000  305C300D 06092A86 4886F70D 01010105
                            0010  00034B00 30480241 00E3E055 322F34F9
                            0020  18099F1C 05D0EB3E 4011AD5B 8BE8CCC2
                            0030  54E83564 5DB02E6F 682D9A23 49C62077
                            0040  0ACFABAF C9847E4D 3646062B 4B1C249D
                            0050  44072EC6 577F98D4 AE020301 0001
                            Signer of -      CARLA01.T2048     GENC002A.AUTO001
                            GENC002A.AUTO002 GENC002A.AUTO003  GENC002A.AUTO004
                            IMWEBSRV.SERVER  TIMOTHY.DEE       WEBSRV
```

Sample Report Output - Detail Ext

```
User - JONATHAN Digicert - Sweet4      Signed by:  CERTAUTH.AUTH01
          Label           Sweet4
          Serial #  -     01
          Issuer  DN -    CN=AUTH01.T=Auth 01 signer
          Subject DN -    CN=Sweet4.T=Little Boy
          Active Date     2010/03/26
          Expire Date     2011/03/26
          Pub Key Size    1024  RSA
          Algorithm       sha-1WithRSAEncryption
          Trusted         Yes
          Cert Length     025F
          Extensions      X509v3 Key Usage
                            DOCSIGN (40)
                          Netscape Comment
                            Generated by CA SAF Certificate Management Facili
                          X509v3 Authority Key Identifier
                            931222BCCD024D24CCA1D57216F69BA90735F2B6
                          X509v3 Subject Key Identifier
                            2F4B6E8E64AC5F3CF493E57691B2FCBCE141E9F1
          Public Key      0000  30819F30 0D06092A 864886F7 0D010101
                          0010  05000381 8D003081 89028181 00CDC14D
                          0020  737C5704 52049344 7D0135C9 5EFE3456
                          0030  16FC6BF4 22A366AE 703B9E8B CBE2FF7F
                          0040  4F3DF663 7B699695 03FF11D4 40A0E6FC
                          0050  0D5DF167 C63450DC 92409A9A 07FEE89C
                          0060  96B6518A BA84921C DC276E9B AFE610AC
                          0070  E7147F29 E3622D6E EB8A0E1A ADDD8946
                          0080  42EF2D62 C6354DE7 FCC1C009 E212E899
                          0090  BF49032C E60B5C21 C69639DB 9D020301
                          00A0  0001
```

Sample Output - Totals

```
CA Mainframe Security     - 'r15 example of totals for Cert Utility Rpt'
DATE 11/22/10 (10.326) TIME 13.58
          Total Certificates             80
          CA Certificates                00
          Site Certificates              00
          User Certificates              80
          Expired Certificates           00
          Inactive Certificates          00
          ICSF Certificates              00
          PCICC Certificates             00
          Self-signed certificates       80
          RSA certificates               80
          DSA certificates               00
          ECC certificates               00
          Trusted Certificates           80
          High Trust Certificates        00
```

Sample Output “Signed by:” Field Definition

Each certificate record displayed in both the summary and detail reports includes a field to display the record ID of the CA Top Secret defined certificate used to sign the current certificate. This field is preceded by the “Signed by:” constant. Based on the results of the search performed by the utility, this field contains one of three possible values:

- The actual name of the signing certificate if found in the security file.
- “None – Self-signed”. There is no signing certificate because the current certificate is self-signed.
- “None – No Record Found”. The current certificate is signed by another certificate, but the signing certificate could not be found in the security file. This can happen when the certificate was signed by an external certificate authority (CA) before it was added to CA Top Secret, or if the signing certificate has been deleted from the security file.

Certificate Utility Parameters

The input parameters can be specified in the PARM field or SYSIN data set. When parameters conflict, the last parameter entered will be used (USER and RECORDID).

TITLE (*ccccccccc*)

Specifies a character string used as the title at the top of the report. If you do not specify this parameter, the title is 'SAFCRRPT - Certificate Utility'. If this string is longer than 35 characters, the report generator uses only the first 35 characters as the title.

Range: 1 to 35

LINECNT(60|*nnnn*)

Specifies the number of output lines to print on a page.

Maximum: The physical constraints of the output media used or 99,999 lines.

USER (*userid*|*userid mask*)

All certificates for the specified user(s) are displayed. When specified with the RINGNAME parameter, the user field cannot be masked.

Default: The caller's userid.

DETAIL|SUMMARY

DETAIL

Specifies that the label, serial number, subject's distinguished name, issuer's distinguished name, validity dates, public key, PKDS label (if one exists), private key size and type are displayed.

SUMMARY

Specifies that the record id of the displayed record, the record id of the signing certificate and the record ids of the certificates that this certificate signed are displayed.

Default: Summary.

DUMP

Adds a hexadecimal dump of the certificate to the display. Dump is ignored if DETAIL is not specified.

EXT

Adds a list of the extensions in the certificate to the display. EXT is ignored if DETAIL is not specified. If the utility cannot identify the name of the extension in the certificate, the OID of the extension is displayed.

Extension values are also displayed. If the format of the extension can be identified, a meaningful description of the settings within the extension is displayed. If the format of the extension cannot be identified, a hexadecimal dump of the extension contents along with a character representation will be displayed.

RINGNAME(*ring name*)

Displays certificates from a specific key ring. The utility uses the R_datalib callable service to retrieve the certificates from the key ring. When RINGNAME is specified, the USER parameter cannot be masked.

Note: The RINGNAME value is the same as the CA Top Secret LABLRING value of the up to 237-character label name of the keyring where the certificates reside.

RECORDID(*record id mask*)

Specifies the record id of the certificate(s) to be displayed. RECORDID cannot be used with the RINGNAME parameter.

TRUST|NOTRUST

Specifies that only certificates that have either TRUST or NOTRUST status are displayed.

ICSF

Specifies that only certificates that have the public or private key saved in ICSF are displayed.

PCICC

Specifies that only certificates that have the public or private key saved in saved in ICSF using the PCICC keyword are displayed.

EDAYS(*expire days*)

Specifies that only certificates that expire within the specified number of days are displayed.

Range: 1 to 365

RSA

Specifies that only certificates that use the RSA algorithm to create the public-private key pair are displayed.

DSA

Specifies that only certificates that use the DSA algorithm to create the public-private key pair are displayed.

FIELDS(*subparameter1,subparameter2,...*)

Limits the information returned by the report. The subparameters are as follows:

LABEL

Display certificate label.

SERIAL

Display serial #.

ISSUER

Display Issuer DN.

SUBJECT

Display Subject DN.

ACTIVE

Display Active Date.

EXPIRE

Display Expire Date.

KEYSIZE

Display key size.

PUBLIC

Display public key.

PKDS

Display PKDS label.

SIGNOF

Display the certificates that this certificate has signed.

SIGALG

Displays the signature algorithm used to create the signature.

TRUST

Displays an indication of whether the certificate is trusted or not.

CERTLEN

Displays the length of the certificate.

If the FIELDS parameter is specified and no subparameters are listed an error message is displayed. If SUMMARY is specified after the FIELDS parameter, the FIELDS parameter is ignored. If SUMMARY is specified before the FIELDS parameter, the SUMMARY parameter is ignored. If more than one FIELDS parameter is specified, only the last FIELDS parameter is acknowledged.

FIELDS Parameter Considerations

If the FIELDS parameter is specified and no sub-parameters are listed an error message will be displayed. If SUMMARY is specified after the FIELDS parameter, the FIELDS parameter will be ignored. If SUMMARY is specified before the FIELDS parameter, the SUMMARY parameter will be ignored. If more than one FIELDS parameter is specified, only the last FIELDS parameter will be acknowledged.

The FIELDS parameter can be specified on the PARM= of the EXEC within the JCL as well as via the SYSIN parameter.

Examples: FIELDS parameter

In this example the FIELDS parameter is specified on the PARM= of the EXEC, without any other parameters. Each element of the list separated by a comma:

```
//SAFRPTCR EXEC PGM=SAFCRRPT,
// PARM=(FIELDS(LABEL,SERIAL,ISSUER,SUBJECT,ACTIVE,EXPIRE,
// KEYSIZE,PUBLIC,PKDS,SIGNOF))
```

In this example the FIELDS parameter is specified on the PARM= of the EXEC with other parameters, the other parameters are enclosed in single quotes, such as ‘RECORDID(-)’:

```
//SAFRPTCR EXEC PGM=SAFCRRPT,
// PARM=('RECORDID(-)',
// FIELDS(ACTIVE,EXPIRE,KEYSIZE,PUBLIC,PKDS,SIGNOF,LABEL,
// SERIAL,ISSUER,SUBJECT))
```

In this example the FIELDS parameter is specified within the SYSIN of the JCL. In the case that the parameter extends to several lines each element of the list separated by a single space:

```
//SYSIN DD *
FIELDS(ISSUER SUBJECT ACTIVE EXPIRE KEYSIZE PUBLIC PKDS SIGNOF LABEL
SERIAL)
RECORDID(-)
/*
```

Chapter 12: TSSRPTSG Statistics Report

To monitor and assist in determining and identifying potential security issues and problems, CA Top Secret gathers statistics for the:

- Sysplex Coupling Facility
- Cache Facility
- Command Propagation Facility (CPF)
- CMDSTATS
- Workload
- IOSTATS
- SAF RACROUTE requests
- SECCACHE Facility

The statistics are logged to SMF using the standard CA Top Secret SMF record.

This section contains the following topics:

Running the Report Using JCL

TSSRPTSG uses standard CA Top Secret report JCL for batch submission. For example:

```
//TSSRPTSG JOB 1,'STATS RPT',MSGCLASS=A
//*
//REPORT EXEC PGM=TSSRPTSG
//*
//RECMAN1 DD DSN=IFASMF.XE15.SMFLOG,DISP=SHR,
//SUBSYS=(LOGR,IFASEXIT)
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
INCLUDE(-)
//
```

The report will also accept input via PARM=:

```
//TSSRPTSG JOB 1,'STATSRPT',MSGCLASS=A,
//*
//REPORT  EXEC  PGM=TSSRPTSG,PARM=('INCLUDE(-)',
//  'EXCLUDE(CACHE,COMMAND),LINECNT(20)')
//RECMAN1    DD  DSN=SYS1.MAN1,DISP=SHR
//SYSPRINT   DD  SYSOUT=*
//SYSUDUMP   DD  SYSOUT=*
//SYSIN      DD  DUMMY
//
```

TSSRPTSG JCL Parameters

For each of the following parameters (with the exception of PRINTER|TERMINAL):

- Enclose the input in parenthesis
- Separate multiple features with commas

Example: JCL parameter syntax

This example shows the INCLUDE parameter with three features specified:

```
INCLUDE(CACHE,SYSPLEX,RACROUTE)
```

TSSRPTSG JCL Parameter List

Function(*feature*)

Specifies the name of the security feature statistics are reported for. Possible values for this field are shown in the section 'Feature Field Values'. Only one feature

value can be specified for the Function keyword.

Example:

```
Function(SYSPLEX)
```

Note: This parameter is mutually exclusive with the INCLUDE and the EXCLUDE parameters.

INCLUDE(feature1,feature2,…)

Specifies the name of the security feature or features statistics are reported for. Features specified can be masked with a dash (-), for example INCLUDE(C-). Possible values for this field are shown in the section 'Feature Field Values'.

Example:

```
INCLUDE(RACROUTE,IOSTATS)
```

Note: This parameter is mutually exclusive with the FUNCTION parameter.

EXCLUDE(feature,feature2,…)

Specifies multiple security features to be omitted from the report. Features specified can be masked with a dash (-), for example EXCLUDE(RAC-).

Possible values for this field are shown in the section 'Feature Field Values'.

Example:

```
EXCLUDE(SYSPLEX)
```

Note: This parameter is mutually exclusive with the FUNCTION parameter.

LINECNT(value)

Specifies the number of lines printed per page. Specify numeric values for this parameter.

Example:

```
LINECNT(20)
```

Default: 60

TITLE(value)

Specifies a one to 35 character string that is part of the report's page header. If the character string is longer than 35 characters an error message is issued.

Example:

```
TITLE(TEST REPORT - APRIL 2006)
```

Default: CA Statistics Log

SDATE(value)

Specifies the beginning date from which records should be selected for the report. Valid input is numeric values in yyddd format.

Example:

```
SDATE(06031)
```

Default: 00000

EDATE(value)

Specifies the ending date records should be selected for the report. Valid input is numeric values in yyddd format.

Example:

```
EDATE(06100)
```

Default: 99365

STIME(value)

Specifies the beginning time from which records should be selected for the report. Valid input is numeric values in hhmm format.

Example:

```
STIME(0900)
```

Default: 0000

ETIME(value)

Specifies the ending time for which records should be selected for the report. Valid input is numeric values in hhmm format.

Example:

```
ETIME(1700)
```

Default: 2359

PRINTER|TERMINAL

Specify:

- PRINTER-The report produces a report format designed for output to a 133-column line printer.
- TERMINAL-The Report uses the default format designed to fit a limited width display terminal.

Feature Field Values

Possible values for the FUNCTION, INCLUDE, and EXCLUDE fields of the TSSRPTSG report are:

CACHE

Returns the statistics collected from the CACHE Facility. The following statistics are returned:

- Total maximum size of the CACHE
- Total size of the CACHE in use
- Total number of calls received in CACHE
- Total number of calls satisfied in CACHE
- Total number of times CACHE cleared

CPF

Return the statistics collected from the Command Propagation Facility. The following statistics are returned for each node:

- Total number of inbound command requests
- Total number of outbound command requests
- Total number of inbound password requests
- Total number of outbound password requests
- Total number of returned outbound requests

RACROUTE

Returns the SAF RACROUTE request statistics. The following statistics are returned:

- Total number of REQUEST= AUTH
- Total number of REQUEST= FASTAUTH
- Total number of REQUEST= LIST
- Total number of REQUEST= DEFINE
- Total number of REQUEST= VERIFY
- Total number of REQUEST= EXTRACT
- Total number of REQUEST= DIRAUTH
- Total number of REQUEST= TOKENMAP
- Total number of REQUEST= VERIFYX
- Total number of REQUEST= TOKENXTR
- Total number of REQUEST= TOKENBLD
- Total number of REQUEST= EXTRACT (BRANCH)

- Total number of REQUEST= AUDIT
- Total number of REQUEST= STAT
- Total number of REQUEST= SIGNON
- Total number of REQUEST= TOKENMAP (Cross memory MODE)
- Total number of REQUEST= EXTRACT (Cross memory MODE)

SYSPLEX

Returns the statistics collected from the Sysplex Coupling Facility. The following statistics are returned:

- Total number of writes
- Total number of reads
- Total number of deletes
- Total number of messages sent
- Total number of messages retrieved

COMMAND

Returns the statistics collected from commands entered in CA Top Secret. The following statistics are returned:

- Total number of CREATE commands issued
- Total number of DELETE commands issued
- Total number of ADD commands issued
- Total number of REPLACE command issued
- Total number of RENAME commands issued
- Total number of REMOVE commands issued
- Total number of PERMIT commands issued
- Total number of REVOKE commands issued
- Total number of WHOOWNS commands issued
- Total number of WHOHAS commands issued
- Total number of LIST commands issued
- Total number of HELP commands issued
- Total number of LOCK commands issued
- Total number of UNLOCK commands issued
- Total number of WHOAMI commands issued
- Total number of MODIFY commands issued
- Total number of ADMIN commands issued

- Total number of DEADMNIN commands issued
- Total number of MOVE commands issued
- Total number of REFRESH commands issued
- Total number of GENCERT commands issued
- Total number of GENREQ commands issued
- Total number of EXPORT commands issued
- Total number of CHKCERT commands issued
- Total number of MLWRITE commands issued
- Total number of REKEY commands issued
- Total number of ROLLOVER commands issued

WORKLOAD

Returns the statistics collected from the use of Command Processor Subtasks within CA Top Secret Security. The following statistics are returned:

- Total number of commands issued
- Command Processor Subtask 1 (percent use)
- Command Processor Subtask 2 (percent use)
- Command Processor Subtask 3 (percent use)
- Command Processor Subtask 4 (percent use)
- Command Processor Subtask 5 (percent use)
- Command Processor Subtask 6 (percent use)
- Command Processor Subtask 7 (percent use)
- Command Processor Subtask 8 (percent use)
- Command Processor Subtask 9 (percent use)
- Command Processor Subtask 10 (percent use)

IOSTATS

Returns the statistics collected from Input/Output activity within CA Top Secret Security. The following statistics are returned:

- Number of RACINITS
- Number of SRI Calls
- Total RACINITS,RACHECKS,RACDEFS,RACLISTS
- Number of Violations
- Number of EXEC intercepts
- Number of SMF Records Dumped

- Number of Security File Changes
- Number of Security File Changes Dumped
- Number of Audit Records Written
- Number of Reads to the Security File
- Number of Writes to the Security File
- Number of Waits High Water Mark
- Number of RCBs in WAIT Queue
- Number of Lock I/Os issued
- Number of Failed lock I/Os

SECCACHE

Returns the statistics collected from the SECCACHE facility. The following statistics are returned:

- Maximum size of cache data area
- Size of cache data area in use
- Percentage of cache data area in use
- Maximum number of index entries
- Number of index entries in use
- Percentage of index entries in use
- Number of successful ADD requests
- Number of successful DELETE requests
- Total number of GET requests
- Number of satisfied GET requests
- Percentage of GET requests satisfied
- Number of SHARE enqueue waits
- Number of EXCLUSIVE enqueue waits
- Number of data area alloc failures
- Number of index area alloc failures
- Lowest security record size in cache
- Highest security record size in cache
- Average security record size in cache
- Record expiration interval in hours
- Threshold full warning level

Chapter 13: TSSCFILX Utility

Use the TSSCFILX utility to query TSSCFILE data without creating additional security file overhead. TSSCFILX does not require multiple TSS administrative authorities. TSSCFILX uses output from TSSCFILE as input to process TSS LIST commands exclusively, it does not list SDT or NDT records. You must have MSCA or SCA authority to use this utility.

This section contains the following topics:

Sample JCL

Use the following JCL to run the TSSCFILX utility:

```
//RODER01X  JOB ACCT,TSSCFILX,CLASS=A,MSGCLASS=X,NOTIFY=RODER01
//*-------------------------------------------------------------
//*  THIS IS A SAMPLE JOB USED TO EXECUTE THE TSSCFILX UTILITY.
//*
//*  BEFORE SUBMITTING THIS JOB, MAKE THE FOLLOWING ADJUSTMENTS:
//*
//*   1. STEPLIB - SPECIFY THE LIBRARY WHERE THE UTILITY IS LOCATED.
//*
//*   2. CFILEIN - SPECIFY THE INPUT TSSCFILE DATASET
//*
//*   3. OUT - SPECIFY A DATASET WHERE THE OUTPUT FROM THE UTILITY
//*      WILL BE STORED
//*
//*-------------------------------------------------------------
//S1    EXEC PGM=TSSCFILX,REGION=4M
//STEPLIB DD DISP=SHR,DSN=TSS.CAI.CAILIB
//CFILEIN DD DISP=SHR,DSN=TSS.TSSCFILE.INPUT
//OUT     DD DSN=TSS.OUTPUT.TSSCFILX,
//           DISP=(NEW,CATLG,DELETE),
//           SPACE=(CYL,(1,1),RLSE),UNIT=SYSDA,
//           DCB=(RECFM=FB,LRECL=300,BLKSIZE=0)
//PRINT   DD SYSOUT=*
//IN        DD *
TSS LIST(ACIDS) TYPE(ZCA)
```

STEPLIB

Specifies the library where the utility is stored

CFILEIN

Specifies the input file for TSSCFILX. This is usually an output file saved from TSSCFILE.

OUT

Specifies a file where the TSSCFILX output is stored.

Sample Data

Below is a sample TSSCFILE input:

```
000001     0001                          TSS LIST(ACIDS) TYPE(SCA)
000002     0100      MASTER    SC        MASTER SECURITY
000003     0200      MASTER    SC        MASTER      8448
000004     3700      MASTER    SC        *ALL*
000005     0500      MASTER    SC        07/20/0608/07/0715:5400:00
000006  Q  0700      MASTER    SC
000007     0800      MASTER    SC        NODSNCHKNOVOLCHK        NOSUBCHKNORESCHK
000008     0900      MASTER    SC        08/07/0714:12XE11BATCH   00306
000009     0100      ADMIN1    SC        SCA
000010     0200      ADMIN1    SC        CENTRAL      768
000011     3700      ADMIN1    SC        BATCH
000012     3700      ADMIN1    SC        TSO
000013     0500      ADMIN1    SC        01/30/0701/30/0716:3215:32
000014     0900      ADMIN1    SC        01/30/0715:33XE11TSO     00001
000015     0100      CLEANID   SC        CLEANUP
000016     0200      CLEANID   SC        CENTRAL     1792
000017     3700      CLEANID   SC        *ALL*
000018     0500      CLEANID   SC        01/11/0706/29/0712:2312:25
000019     0600   C  CLEANID   SC        SYSPROF
000020     0600      CLEANID   SC        CLNPRO1
000021     0650      CLEANID   SC        OMVSGRP
000022  Q  0700      CLEANID   SC                            NOPWCHG
000023     0800      CLEANID   SC        NODSNCHKNOVOLCHKNOLCFCHKNOSUBCHKNORESCHK
000024     0900      CLEANID   SC        06/29/0712:08XE11TSO     00009
000025     0100      CLEANID1  SC        CLEANUP
000026     0200      CLEANID1  SC        CENTRAL      768
000027     3700      CLEANID1  SC        *ALL*
000028     0500      CLEANID1  SC        01/11/0701/11/0712:3112:31
000029     0600      CLEANID1  SC        SYSPROF
000030     0650      CLEANID1  SC        OMVSGRP
000031  Q  0700      CLEANID1  SC                            NOPWCHG
000032     0800      CLEANID1  SC        NODSNCHKNOVOLCHKNOLCFCHKNOSUBCHKNORESCHK
000033     0100      CLEANID2  SC        CLEANUP
000034     0200      CLEANID2  SC        CENTRAL      768
000035     3700      CLEANID2  SC        *ALL*
000036     0500      CLEANID2  SC        01/11/0701/11/0711:4311:43
000037     0600      CLEANID2  SC        SYSPROF
000038     0650      CLEANID2  SC        OMVSGRP
000039  Q  0700      CLEANID2  SC                            NOPWCHG
000040     0800      CLEANID2  SC
000041     0100      CLEAN2    SC        CLEANUP
000042     0200      CLEAN2    SC        CENTRAL     1792
000043     3700      CLEAN2    SC        *ALL*
000044     0500      CLEAN2    SC        01/11/0701/23/0717:5912:50
000045     0600   C  CLEAN2    SC        SYSPROF
```

```
000046     0600      CLEAN2    SC      CLNPRO1
000047     0650      CLEAN2    SC      OMVSGRP
000048  Q  0700      CLEAN2    SC                                NOPWCHG
000049     0800      CLEAN2    SC
000050     0900      CLEAN2    SC      01/23/0717:51XE11TSO     00002
000051     0100      HARDE10   SC      HOTP SCA
000052     0200      HARDE10   SC      CENTRAL     1792
000053     3700      HARDE10   SC      *ALL*
000054     0500      HARDE10   SC      07/20/0607/24/0714:4700:00
000055     0650   C  HARDE10   SC      OMVSGRP
000056     0650      HARDE10   SC      TTY
000057  Q  0700      HARDE10   SC                     AUDIT   NOPWCHG
000058     0800      HARDE10   SC             NOVOLCHKNOLCFCHKNOSUBCHK
000059     0900      HARDE10   SC      07/26/0709:09XE11TSO     00046
000060     0100      JOE1      SC      JOE
000061     0200      JOE1      SC      CENTRAL      768
000062     3700      JOE1      SC      *ALL*
000063     0500      JOE1      SC      12/10/0601/24/0711:1300:00
000064     0600   C  JOE1      SC      SYSPROF
000065     0600   C  JOE1      SC      PROCPROF
000066     0600   C  JOE1      SC      TSOPROF
000067     0600      JOE1      SC      TSSPROF
000068     0650   C  JOE1      SC      OMVSGRP
000069     0650      JOE1      SC      TTY
000070  Q  0700      JOE1      SC
000071     0800      JOE1      SC      NODSNCHKNOVOLCHK         NOSUBCHKNORESCHK
000072     1100      JOE1      SC      NEVER*ALL*
000073     0100      KAUGE01   SC      HOTP SCA
000074     0200      KAUGE01   SC      CENTRAL     2048
000075     3700      KAUGE01   SC      *ALL*
000076     0500      KAUGE01   SC      07/20/0606/29/0709:3500:00
000077     0600      KAUGE01   SC      SYSPROF
000078     0650      KAUGE01   SC      OMVSGRP
000079  Q  0700      KAUGE01   SC                                NOPWCHG
000080     0800      KAUGE01   SC      NODSNCHKNOVOLCHKNOLCFCHKNOSUBCHKNORESCHK
000081     0900      KAUGE01   SC      08/07/0714:07XE11TSO     00043
000082     0100      MASTERL   SC      MASTERL
000083     0200      MASTERL   SC      CENTRAL      768
000084     3700      MASTERL   SC      *ALL*
000085     0500      MASTERL   SC      02/05/0707/25/0708:4700:00
000086     0600      MASTERL   SC      SYSPROF
000087     0650   C  MASTERL   SC      OMVSGRP
000088     0650      MASTERL   SC      TTY
000089  Q  0700      MASTERL   SC                                NOPWCHG
000090     0800      MASTERL   SC             NOVOLCHKNOLCFCHKNOSUBCHK
000091     0900      MASTERL   SC      07/25/0708:46XE11TSO     00001
000092     0100      MASTER1   SC      MASTER
000093     0200      MASTER1   SC      CENTRAL      512
000094     3700      MASTER1   SC      *ALL*
```

```
000095     0500      MASTER1   SC      07/20/0607/09/0715:5500:00
```

Below is a sample TSSCFILX output:

```
0001                        TSS LIST(ALL)
0100      *ALL*             GLOBAL-RESOURCES
0200      *ALL*             GLOBAL      4352
0500      *ALL*             06/14/0608/08/0718:0800:00

0001                        TSS LIST(RDT)
0100      *RDT*             RESOURCE DEFINITIONS
0200      *RDT*             GLOBAL     61440

0001                        TSS LIST(FDT)
0100      *FDT*             FIELD DEFINITIONS
0200      *FDT*             GLOBAL     14332

0001                        TSS LIST(STC)
0100      *STC*             STARTED-TASKS
0200      *STC*             GLOBAL      4608
0500      *STC*             06/14/0608/01/0718:0500:00

0001                        TSS LIST(AUDIT)
0100      *AUDIT*           RESOURCE-AUDITING
0200      *AUDIT*           GLOBAL       256
0500      *AUDIT*           06/14/0608/01/0723:0200:00

0001                        TSS LIST(MASTER1) DATA(ACIDS)
0100      MASTER1   SC      MASTER SECURITY
2800   C  MASTER1   SC      ACF2DEPTD ACLDEPT D APPCDIV V APPLDEPTD
2800   C  MASTER1   SC      ARMFR01 SCAUDZONE1Z AUDZONE2Z AUDZONE3Z
2800   C  MASTER1   SC      BC10507 D BC66DEP D BC66099 LCBECKI03 SC
2800   C  MASTER1   SC      BOERO02 SCBOSDEPT D BOSDE01 SCBOSDE02 SC
2800   C  MASTER1   SC      BOSDIV  SCBOSDIVV V BOSLSCA LCBOSSCA  SC
2800   C  MASTER1   SC      BOSZONE Z BRERO04 SCBURBE02 SCCICSDEPTD
2800   C  MASTER1   SC      CICSDIV V CICSUSR SCCICS01  V CICTH01 SC
2800   C  MASTER1   SC      CPFDIV  V CPFSCA1 SCDB2DEPT D DB2SCA1 SC
2800   C  MASTER1   SC      DEARO03 SCDENDEPT D DENDIV  V DEPTBIGID
2800   C  MASTER1   SC      DEPTGAT D DEPTR12 D DMDEPT  D DOUMA02 SC
2800   C  MASTER1   SC      DOUMA02DD DUNAN01 SCEAQNDEP1D EAQNDIV1V
2800   C  MASTER1   SC      EAQNZON1Z EMOBR01 SCEMOTSTD D ENFDEPT D
2800   C  MASTER1   SC      ESPNZON1Z EXMNDPT D FILEDEPTD FJADEPT2D
2800   C  MASTER1   SC      FJADEPT3D FJADEPT4D FJADEPT7D FJADIV  V
2800   C  MASTER1   SC      FJADIV2 V GSSDEPT D HARBEDPTD HARBE01 SC
2800   C  MASTER1   SC      HARBE01DD HARBE1BDD HARBE1D1D HARBE1D2D
2800   C  MASTER1   SC      HARMI01 SCHFSDEPT D HOLNO01 SCIDMSDPT D
2800   C  MASTER1   SC      IVPDPT  D JTKDIV  V KALDA01 SCKNUJO01 SC
2800   C  MASTER1   SC      KOTPA01 SCKRACCID SCKRBDEPT D KUTILT1 SC
2800   C  MASTER1   SC      LABDEPT D LDAPDEPTD LDSSCA  SCLDSZONE Z
2800   C  MASTER1   SC      LOTUSDPTD LQDIV   V LQZONE  Z LUGBR01 SC
2800   C  MASTER1   SC      LV1DEPT D MASKDIV V MCCRA01 SCMIXCDEPTD
```

```
2800   C  MASTER1   SC      MLSDEPT D MOVEDPT D MOVEZNE Z MULDE03 SC
2800   C  MASTER1   SC      MULDE05 SCMULTDEPTD NEMODEPTD NESTDEPTD
2800   C  MASTER1   SC      OMEGDEPTD OMVSDEPTD OMVSSCA SCPAMDPT  D
2800   C  MASTER1   SC      PDSDEPT D PEAST02 SCPHRSDPT D PORJO01 SC
2800   C  MASTER1   SC      QAIMSZONZ QAJESDEPD QASCA   SCQA60DEP D
2800   C  MASTER1   SC      QO31DEP1D QO35DEPTD QO40DEP1D QUEEL01 SC
2800   C  MASTER1   SC      QUEEL01DD QUEEL02 SCRACF1   SCRDTDEPT D
2800   C  MASTER1   SC      REIPA02 SCRESDEPT D RMBDEPT1D ROSDIV  V
2800   C  MASTER1   SC      ROSSCA  SCROZMI02 SCSETGID  D STCDEPT D
2800   C  MASTER1   SC      STRTE01 SCSTRTE01ZZ STRTH01 SCSYSADM  SC
2800   C  MASTER1   SC      SYSDEPT D TCSFJA  SCTDGMAH  SCTEDLSCA LC
2800   C  MASTER1   SC      TESTDEP D TESTDEPTD TESTJT  D TEST00  SC
2800   C  MASTER1   SC      TEST002 SCTSODEPT D TSSCSCA SCTSSDEPT D
2800   C  MASTER1   SC      TSSSCA  SCTSTMOVE LCVENODEPTD VENODIV V
2800   C  MASTER1   SC      VENOZONEZ VERDIV  V VERI01  SCVMDEPT  D
2800   C  MASTER1   SC      VMQM    V VPAS123 SCWASDEPT D WOLRO02 SC
2800      MASTER1   SC      XE14SCA SC
```

Chapter 14: IDMAP Cleanup Utility (TSSCHKDN)

This section contains the following topics:

About the TSSCHKDN Utility

TSSCHKDN is a batch utility that identifies invalid distinguished names (DNs) for CA Top Secret IDMAP users implementing secondary distinguished names. Use this utility to more efficiently identify IDMAPDN values in IDMAP records that are invalid for z/OS 1.13.

JCL Requirements

Use following sample JCL or a user-written substitute for the job stream to run the TSSIDMAP report.

```
//REPORTS JOB 1,'TSSCHKDN REPORTS',MSGCLASS=A,CLASS=A
//*********************************************************************
//*                                                                   *
//*  CREATE THE A REPORT OF INVALID DISTINGUISHED NAMES               *
//*                                                                   *
//*********************************************************************
//*
//*
//IDMAP    EXEC  PGM=TSSCHKDN
//MAINTOUT DD  SYSOUT=A
//SYSPRINT DD SYSOUT=*
//*SYSPRINT DD  DISP=SHR,DSN=KAUGE01.IDMAP.REPORT
/*
```

SYSPRINT

Specifies where report output is sent. Output is directed to a printer or to the listed data set. The record format is VBA. You can optionally specify the BLKSIZE parameter; the default for this parameter is 3665. For most reports, report generator output is 80 characters wide. This width enables convenient report browsing on an 80-character display screen. However, some reports have a wider format for use with printer-directed output. To determine the maximum record length for each format, refer to the explanation of each report generator.

Sample TSSCHKDN Output

```
IDMAP Records That are Invalid Because of the IDMAPDN z/OS 1.13 Normalization
--------------------------------------------------------------------------------
ACCESSORID = RMAPTUA   IDMAP = TESTMAB1
IDMAPDN    = =UID=DaveR,CN=Dave Reddy,OU=qa,O=CaACF2,C=US

ACCESSORID = RMAPTUA   IDMAP = TESTMAB2
IDMAPDN    = ,UID=DaveR,CN=Dave Reddy,OU=qa,O=CaACF2,C=US

ACCESSORID = RMAPTUA   IDMAP = TESTMAB3
IDMAPDN    = ;UID=DaveR,CN=Dave Reddy,OU=qa,O=CaACF2,C=US

ACCESSORID = RMAPTUB   IDMAP = TESTMAB4
IDMAPDN    = UID=Da+eR,CN=Dave Reddy,OU=Dev,O=CaACF2,C=US
```

This report displays the following information:

ACCESSORID

Identifies the ACID that has that IDMAP record on it.

IDMAP

Identifies a unique 8-byte record identifier.

IDMAPDN

Identifies the invalid distinguished name (DN).

Return codes

The following return codes are associated with this utility:

0

Report executed successfully

4

No IDMAP Table

8

Internal Error

997

No SAFIVT

998

CA Top Secret is not active

999

Output file cannot open

Index

M

N

O

P

R

S

T

U

V

W