CA Top Secret® for z/VM

Troubleshooting Guide

r12

Contact CA Technologies

Contact CA Support

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

- 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

Provide Feedback

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

If you would like 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.

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This guide is intended for CA Top Secret for z/VM administrators who are charged with the maintenance of CA Top Secret, or for any security administrator, operator, auditor, or programmer who must diagnose and resolve CA Top Secret related problems.

This guide enables security administrators to:

- Verify that a problem actually exists, categorize the problem, and eliminate obvious causes
- Diagnose and resolve specific problem categories by providing step-by-step procedures or checklists for each category
- Conduct clear, streamlined discussions with CA Top Secret Technical Support by providing guidelines on when to call technical support, and what information to provide to the CA Top Secret support analyst.

Obviously, this guide alone will not solve all of your CA Top Secret problems. It can, however, show you how to use your CA Top Secret documentation and product features to make your troubleshooting procedures more effective and efficient. Hopefully, it will allow you to solve many problems on your own.

If you must take advantage of CA Top Secret support, this guide provides the necessary checklists and job aids which enable you to get the most out of your conference with the support analyst. Incidentally, these checklists and job aids assist CA Top Secret Technical Support in helping you resolve your problems quickly and efficiently.

Note: CA Top Secret has built a reputation as the best VM security product because it is easy to customize, administer, and use. Since this guide is written explicitly to simplify users' tasks, you can help make CA Top Secret even better by offering your feedback on the practical usage of this guide. Your help is greatly appreciated.

CA Top Secret Approach to Troubleshooting

CA Top Secret contains features and utilities which allow a basic troubleshooting approach to be incorporated into a simple three-phase procedure:

- Phase 1 - Verify and categorize the problem.
- Phase 2 - Perform diagnostic or checkout procedure(s) to determine the cause of the problem. If a resolution is found, implement it and then test it. If it works, your problems are solved.
- Phase 3 (optional) - Organize diagnostic information, and call Technical Support for assistance with diagnosis and resolution of the problem.

An explanation of each phase is documented within this guide.

Contents of This Guide

The following explains how this guide supports each troubleshooting phase.

Phase 1: Problem Identification

To begin your diagnostic effort, answer the following questions: “Is this problem really a problem, what type of problem is it, and where do I go for help?”

Phase 1 assists you by providing:

- A simple procedure for categorizing problems. The supported general categories are:
  - Abends
  - Customization
  - Facility Authorization
  - Logging of Events
  - Message Production/Suppression
  - Resource Authorization
- Directions and references to other CA Top Secret guides and utilities which allow you to diagnose and resolve the problem.

Phase 2: Diagnostic Procedures

Once you verify that there is indeed a problem and are able to isolate it to one of the supported categories (listed above), you may refer to the appropriate diagnostic procedure or checklist which is provided for each general category.

Each procedure is designed to either allow you to determine the cause and resolution of the problem yourself, or to assemble as much information as you can about the problem. This enables you to make effective use of any discussions you may have with CA Top Secret Technical Support.

Phase 3: CA Technical Support

This phase provides a checklist of items and information which greatly facilitate discussions with the CA Top Secret support analyst. This is actually the easiest phase of your investigation since you have assembled most of this data as part of prior troubleshooting phases.

Phase 3 also describes how the CA Technical Support Center is organized, and how your call is processed.

Appendix Information

The Phase 2 procedures often direct you to one or more of the following troubleshooting appendixes:

- "Diagnostic Tools"
- "Diagnostic Tools"
- "Message Display/Suppresion Algorithm"
- "SAFTRACE"

Chapter 2: Phase 1 - Problem Identification

This section contains the following topics:

Steps

To identify a problem, follow these steps:

1. Determine nature of the problem.
2. Attempt to recreate the problem on the system. Did the problem reoccur?
   - If YES, go to step 3.
   - If NO, go to step 5.
3. Did the system display a CA Top Secret message, DRC code, or other abend code?
   - If YES, refer to the *Messages and Codes Guide* to determine the cause of the problem. Take the corrective action which corresponds to the message or code. Then, go to step 7.
   - If NO, go to step 4.
4. If the problem does not correspond to one of the categories listed below, or appears to be caused by CA Top Secret internals, go directly to the Phase 3 in this guide. The listed categories are general categories only. If you cannot locate an exact category in the list, try to apply basic troubleshooting principles of a related category before contacting the CA Top Secret Support Center.
5. Has maintenance been applied to CA Top Secret for VM or CP since the initial problem was reported?
   - If YES, Isolate the changes made. Then, go to step 6.
   - If NO, go to step 7.
6. Does the maintenance explain/justify the problem?
   - If YES, stop.
   - If NO, go to step 7.
7. Before proceeding to Phase 2, review the CA Top Secret security validation algorithm to ensure that the problem is not due to a misunderstanding of how CA Top Secret works.

The CA Top Secret algorithm takes the following factors into consideration when processing a request to access a resource.

Ownership vs. Authorization

Ownership overrides authorization. If CA Top Secret finds two CA Top Secret entries, one giving ownership of a resource to an ACID and the other giving authorization, ownership prevails, allowing the ACID total access.

Order of Search

CA Top Secret searches the security records in the following order:

- ACID's Security Record
- Profile(s) attached to the ACID
- The ALL Record

Best Match Criteria

When more than one relevant PERMIT is encountered in a security validation search, CA Top Secret employs the "best match" criteria. "Best match" refers to the closeness of the matchup between the resource identifier in the PERMIT and the resource identifier for which access is requested. Generic prefixing and masking are often the culprits responsible for (un)authorized access discrepancies.

AUTH Control Option

The AUTH control option governs whether or not CA Top Secret merges the results of the security record search.

MODE Control Option

The mode setting specifies the level of security at which validation will be performed. Mode options range from DORMANT to FAIL. CA Top Secret uses this setting to determine the response to security validation requests.

Volume vs. Data Set Authorization

When determining access to a particular DASD data set, CA Top Secret must evaluate both volume and data set access authorizations. Volume level checking can optionally be bypassed. However, in situations where both volume and data set level checking is done, CA Top Secret performs volume-level checking first. Thus, a request to access a data set can be granted or failed strictly on the basis of the user's volume access authorization.

Based on the CA Top Secret security validation algorithm, does a problem still exist?

- If YES, go to Phase 2.
- NO, review the CA Top Secret documentation and examine your existing security definitions. Remember that CA Top Secret offers customer assistance in the form of education classes and on-site security consulting.

Chapter 3: Phase 2 - Diagnostic Procedures

This section contains the following topics:

Categories

Phase 2 of the troubleshooting procedure describes the steps that may be taken to diagnose the root of your problem. The procedures in Phase 2 are broken down by categories. (Prior to reaching this phase you must place your problem into a specific category.) To locate the proper procedure, find the exact category heading or the heading that most closely resembles the type of problem you are experiencing. The general categories are:

Problem	Procedure
Abends	Abends
Customization	Customization
Facility Access	Access Incorrectly Allowed Sign-on Passwords Not Being Checked CPU Restriction Not Honored Access Incorrectly Denied
Logging	CA Top Secret Not Logging Violations CA Top Secret Not Logging Access or Initiations
Messages	Users Not Receiving CA Top Secret Messages Console Not Receiving CA Top Secret Messages
Resource Access	Access Incorrectly Denied

Abends

If the CA Top Secret virtual machine abends or if CP abends in a CA Top Secret routine, gather the following information:

- Unload the spool file dump to disk using DUMPLOAD.
- If possible, provide a copy of the system operator's console log from 15 minutes before and 5 minutes after the abend occurred. Hardcopy is preferred.
- If CA Top Secret message TSS0999E indicated the abend, record the text of the message, including all register and offset information which follow the message.
- Copy all other CA Top Secret messages that appear in the order in which they occur.
- Refer to the Phase 3 procedure for a checklist of general information required by Technical Support, and for instructions on how to call Technical Support.

Customization

Customization problems can stem from any one of the two supported CA Top Secret customization techniques, namely,

- The Installation Exit
- The Application Interface
- RACROUTE (ESM) Security Interface

Problems usually occur within the parameter lists that are passed to CA Top Secret by the customized code. There are a number of tools that can be used for diagnostics:

- Information Feedback Areas containing DRCs and messages
- CA Top Secret Messages and IBM Messages
- Traces containing DRCs (see the "Diagnostic Trace" appendix)
- Dumps

Tips and Checkpoints

Customization code can get tricky at times. This chapter outlines those little things that can easily be overlooked when developing the customization code and can lead to problems. Locate the customization facility you are using and check that the listed items have been incorporated into your customization code.

Installation Exit

- The TSSINS text file has been incorporated into the server machine nucleus. The nucleus load map for the server machine is contained in a file called TSSNUC MAP on the CAIMAINT virtual machine 291 disk for test installation, 391 disk for production.
- The EXIT control option is ON. TSS MODIFY(STATUS) lists the status of EXIT.
- To test your installation exit code you can set up debug code which executes the exit only for a particular ACID, virtual machine, etc. These fields are in the parameter list passed to the exit.
- Ensure the server machine has been restarted by TSS MODIFY(RESTART) to bring in the copy of the exit.

Application Interface

- All the necessary Request Record fields are supplied.
- Samples of the Application Interface can be found in the *Implementation Guide*.

Customization Troubleshooting - General Procedure

The general procedure that can be used to troubleshoot customization problems follows.

STEP 1

Write down all message numbers and text displayed by CA Top Secret or VM. Refer to the *Messages and Codes Guide* to determine the meaning of the CA Top Secret messages and the appropriate action that must be taken to correct the problem.

Did the messages expose the problem?

- If YES, go to STEP 3
- If NO, go to STEP 2

STEP 2

Turn on the CA Top Secret TRACE:

```
TSS MODIFY(SECTRACE(ACT,USER))

TSS ADD(acid) TRACE
```

Retry request and examine the TRACE information. The TRACE shows the information that is passed to CA Top Secret along with DRCs and other valuable diagnostic information. Appendix B explains how to read the CA Top Secret TRACE.

Did the TRACE expose the problem?

- If YES, go to STEP 3
- If NO, go to STEP 4

STEP 3

Implement the solution to the problem and retest the customization code.

Was the problem resolved?

- If YES, stop
- If NO, go to STEP 4

STEP 4

Gather all pertinent information. Go to Phase 3 for instructions on how to call Technical Support.

Facility Access

This chapter is comprised of the following procedures:

- Access Incorrectly Allowed
- Sign-on Passwords Not Being Checked
- CPU Restrictions Not Honored
- Access Incorrectly Denied

These procedures assume that the reader is familiar with the TSS LIST and TSS MODIFY commands and with the FACILITY, LOG, and MODE control options.

Facility Access Incorrectly Allowed

STEP 1

Determine if the user or profile has been explicitly granted access to the facility.

```
TSS LIST(acid) DATA(BASIC,PROF)
```

Does the facility in question appear within the user or profile ACID's Security Record?

- If YES, TSS REMOVE the facility from the Security Record or remove the profile from the user. Go to STEP 8
- If NO, go to STEP 2

STEP 2

Determine the security mode for the facility (or site) and for the user or profile ACID.

For Facility, enter:

```
TSS MODIFY('FAC(fac)')
```

For ACID(s), enter:

```
TSS LIST(acid) DATA(XAUTH,PROF)
```

Is the user or profile ACID or the facility in either DORMANT or WARN mode?

- If YES, DORMANT mode allows access without security checking. WARN mode may also allow access, but CA Top Secret sends messages to the user's terminal. Consider using the TSS PERMIT command to move the user to a more restrictive security mode (IMPL or FAIL), or set WARNPW for the FACILITY control option. This prohibits a user from accessing a facility unless explicitly authorized.

  Go to STEP 3 if WARN mode. Go to STEP 7 if DORMANT.
- If NO, go to STEP 4.

STEP 3

List the logging options to determine if warning messages are issued to the user. Ask the user to enter TSS WHOAMI at the terminal.

Is MSG displayed in the LOG field of the WHOAMI response?

- If YES, Take administrative action. Go to STEP 8.

  Go to STEP 3 if WARN mode. Go to STEP 7 if DORMANT.
- If NO, The MSG option is not specified, therefore no messages are sent to the user. Review LOG control options. Go to STEP 8.

STEP 4

Determine if the user possesses the NORESCHK attribute:

```
TSS LIST(acid) DATA(BAS,PROF)
```

Does the user or profile possess the NORESCHK attribute?

- If YES, TSS REMOVE the NORESCHK attribute from the ACID
- If NO, Go to STEP 5

STEP 5

Determine if user is allowed to bypass security by locating BYPASS message on the STATUS response:

```
TSS MODIFY('STATUS')
```

Does the user's ACID or jobname appear in this list?

- If YES, you must reset BYPASS, TSS MODIFY('BYPASS(RESET)').

  Go to STEP 8.
- If NO, Go to STEP 6.

STEP 6

Determine if the DRC control option is set to NOVIOL for the returned DRC code:

```
TSS MODIFY('DRC(drc#)')
```

Is the DRC set to NOVIOL?

- See the *Control Options Guide* to reset the DRC NOVIOL attribute. Go to STEP 8.
- Go to STEP 7.

STEP 7

Activate the diagnostic trace for the user. Refer to ADD-TRACE in the *Command Functions Guide* for instructions and to the SECTRACE parameter in the *Control Options Guide*.

Did trace records appear?

- If YES, see the "Diagnostic Trace" appendix for instructions on how to interpret trace information. Go to STEP 8.
- If NO, Go to STEP 10.

STEP 8

Implement the solution to the problem if this has not been done.

- If YES, and if a solution has been determined, go to STEP 9.
- If NO, and if no solution has been determined, go to STEP 10.

STEP 9

Attempt to sign on to the facility in question using the ACID in question.

Was access denied?

- If YES, STOP.
- If NO, go to STEP 10.

STEP 10

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

Sign-on Passwords not being Checked

STEP 1

Determine user's or profile's security mode.

```
TSS LIST(acid) DATA(XAUTH,PROF)
 TSS WHOHAS MODE(DORM or WARN)
```

Is user or profile ACID in either DORMANT or WARN mode?

- If YES, consider that DORMANT mode may allow access without security checking. WARN mode may also allow access, but CA Top Secret sends messages to the user's terminal. Consider using the TSS PERMIT command to move the user to a more restrictive security mode (IMPL or FAIL). This prohibits a user from accessing a facility unless explicitly authorized. Or assign the DORMPW or WARNPW attribute to the facility:

  ```
  TSS MODIFY ('FAC(fac=DORMPW)')
  ```

  or

  TSS MODIFY('FAC(fac=WARNPW)').

  This forces defined users and jobs to enter their correct passwords while in WARN mode.

  If user is in WARN, go to STEP 4. If in DORMANT, go to STEP 8.
- If NO, go to STEP 2.

STEP 2

Determine the facility's mode and attributes.

```
TSS MODIFY('FAC(fac)')
```

Is facility in WARN MODE with the NOWARNPW attribute?

- If YES, consider that WARN mode, in combination with NOWARNPW, allows a user to bypass password security checking. Consider using the TSS PERMIT command to move the user to a more restrictive security mode, IMPL or FAIL. This prohibits a user from accessing a facility unless explicitly authorized. Or assign the WARNPW attribute to the facility and TSS MODIFY('FAC(fac= WARNPW)'). This forces defined users and jobs to enter their correct passwords while in WARN mode.
- If NO, go to STEP 3.

STEP 3

Is facility in DORMANT mode with the NODORMPW attribute?

- If YES, consider that DORMANT mode, in combination with NODORMPW, allows a user to bypass password security checking. Consider using the TSS PERMIT command to move the user to a more restrictive security mode, IMPL or FAIL. This prohibits a user from accessing a facility unless explicitly authorized. Or assign the DORMPW attribute to the facility and TSS MODIFY('FAC(fac=DORMPW)'). This forces defined users and jobs to enter their correct passwords while in DORMANT mode. Go to STEP 7.
- If NO, go to STEP 5.

STEP 4

List the user's logging options to determine if warning messages are logged. Ask the user to enter TSS WHOAMI at the terminal.

Is MSG displayed in the LOG field of the WHOAMI response?

- If YES, take administrative action. Go to STEP 7.
- If NO, since LOG options are not specified, therefore no messages are sent to the user. Review LOG control options. Go to STEP 7.

STEP 5

Determine if user is allowed to bypass security by locating the BYPASS message on the STATUS response:

```
TSS MODIFY('STATUS')
```

Does the user's ACID appear in this list?

- If YES, TSS REMOVE the applicable bypass attribute from the user's ACID. Go to STEP 7.
- If NO, go to STEP 6.

STEP 6

Activate the diagnostic trace for the user. Refer to ADD-TRACE in the *Command Functions Guide* for instructions and to the SECTRACE parameter in the *Control Options Guide*.

Did trace records appear?

- If YES, see the "Diagnostic Trace" appendix for instructions on how to interpret trace information. Go to STEP 7.
- If NO, go to step 9.

STEP 7

Implement the solution to the problem if this has not been done.

- If a solution has been determined, go to STEP 8.
- If no solution has been determined, go to STEP 9.

STEP 8

Attempt to sign on to the facility in question using the ACID and an invalid password.

Was access denied?

- If YES, STOP.
- If NO, go to step 9.

STEP 9

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

CPU Restrictions not Honored

STEP 1

Determine if the CPU restriction exists for the user(s) and CPU in question:

```
TSS LIST(acid) DATA(XAUTH,PROF)
 TSS LIST(ALL) DATA(XAUTH)
```

Note: Examine rules for time of day, day of week, and program restrictions, along with any ACTIONS which may be in the PERMITs for the CPU.

Do permissions exist which allow the user to access the CPU?

- If YES, TSS REVOKE the permissions, or TSS PERMIT the user access to the CPU with ACTION(FAIL,DENY). Go to STEP 9.
- If NO, go to step 2.

STEP 2

Ensure that the CPU is owned.

```
TSS WHOOWNS CPU(cpu)
```

Is the CPU owned?

- If YES, go to step 3.
- If NO, refer to TSS ADD - CPU in the *Command Functions Guide*. If resource is not owned, CA Top Secret cannot restrict access. Go to STEP 9.

Note: If the DEFPROT attribute is attached to a particular resource class, then the resource class is protected by default, even if it is not owned. To determine whether DEFPROT is attached enter:

```
TSS LIST(RDT) RESCLASS(CPU).
```

STEP 3

Determine the security mode for the facility (or site) and for the user or profile ACID(s).

For Facility, enter:

```
TSS MODIFY('FAC(fac)')
```

For ACID(s), enter:

```
TSS LIST(acid) DATA(XAUTH,PROF)
```

Is the ACID(s) or the facility in either DORMANT or WARN mode?

- If YES, consider that DORMANT mode may allow access without security checking. WARN mode may also allow access, but CA Top Secret sends messages to the user's terminal. Consider using the TSS PERMIT command to move the user to a more restrictive security mode (IMPL or FAIL). This prohibits a user from accessing a facility unless explicitly authorized. Go to STEP 4 if WARN mode. Go to STEP 10 if DORMANT.
- If NO, go to step 4.

STEP 4

List the user's logging options to determine if warning messages are logged. Ask the user to enter TSS WHOAMI at the terminal.

Is MSG displayed in the LOG field of the WHOAMI response?

- If YES, go to step 5.
- If NO, since LOG options are not specified, no messages are sent to the user. Review LOG control options. Go to STEP 9.

STEP 5

Determine if the ACID possesses the NORESCHK attribute:

```
TSS LIST(acid) DATA(BAS,PROF)
```

Does ACID possess the NORESCHK attribute?

- If YES, then enter:

  ```
  TSS REMOVE(acid) NORESCHK
  ```

  And go to STEP 9.
- If NO, go to STEP 6.

STEP 6

Determine if the DRC control option is set to NOVIOL for the returned DRC:

```
TSS MODIFY ('DRC(drc#)')
```

Is the DRC set to NOVIOL?

- If YES, See the *Control Options Guide* to reset the DRC. Go to STEP 9.
- If NO, go to STEP 7.

STEP 7

Determine if user is allowed to bypass security by locating the BYPASS message on the STATUS response:

```
TSS MODIFY('STATUS')
```

Does the user's ACID appear in this list?

- If YES, TSS REMOVE the applicable bypass attribute from the user's ACID. Go to STEP 9.
- If NO, go to STEP 8.

STEP 8

Activate the diagnostic trace for the user. Refer to ADD-TRACE in the *Command Functions Guide* for instructions and to the SECTRACE parameter in the *Control Options Guide*.

Did trace records appear?

- If YES, see the "Diagnostic Trace" appendix for instructions on how to interpret trace information. Go to STEP 9.
- If NO, go to STEP 10.

STEP 9

Has the solution to the problem been implemented?

- If YES, go to STEP 10.
- If NO, go STEP 11.

STEP 10

Attempt to sign on to the facility in question using the ACID in question.

Was access denied?

- If YES, STOP.
- If NO, go STEP 11.

STEP 11

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

Facility Access Incorrectly Denied

STEP 1

Is there a Detailed Violation Reason code (DRC) displayed with the violation?

- If YES, refer to "Detailed Reason Codes" in the *Messages and Codes Guide* to determine if the correct authorizations have been made to ensure access. Go to STEP 2.
- If NO, go STEP 3.

STEP 2

Was the problem resolved during STEP 1?

- If YES, go to STEP 5.
- If NO, go STEP 3.

STEP 3

Determine the facilities the user is allowed to access via ADD or PERMIT authorizations:

TSS LIST(*acid*) DATA(BASIC,PROF)

Do authorizations exist which permit the user to access the facility?

- If YES, go to STEP 4.
- If NO, TSS ADD the facility to the user's ACID. Go to STEP 5.

STEP 4

Activate the diagnostic trace for the user. Refer to ADD-TRACE in the *Command Functions Guide* for instructions and to the SECTRACE parameter in the *Control Options Guide*.

Did trace records appear?

- If YES, see the "Diagnostic Trace" appendix for instructions on how to interpret trace information. Go to STEP 5.
- If NO, go to STEP 7.

STEP 5

Has the solution to the problem been implemented?

- If YES, go to STEP 6.
- If NO, implement the solution to the problem.

STEP 6

Attempt to sign on to the facility in question using the ACID in question.

Was access allowed?

- If YES, STOP.
- If NO, go to STEP 7.

STEP 7

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

Logging of Events

Whether or not security events are properly logged is a function of the LOG option which can be issued globally or by facility. Facility logging overrides the global LOG option.

Although the following procedure provides basic checks which must be made to ensure that the LOG options are set correctly, the actual settings for the LOG option vary from site to site, and from facility to facility. Refer to the *Planning Guide* and the LOG control option in the *Control Options Guide* to ensure the proper implementation and use of the LOG control option.

These procedures assume that the reader can use TSSUTIL to obtain logging reports. Refer to the *Reporting Guide* if unfamiliar with this utility.

CA Top Secret Not Logging Violations

STEP 1

Is AUDIT attribute turned on for the facility?

Enter:

```
TSS MODIFY('STATUS') or TSS MODIFY('FAC(facility)')
```

Is the site or facility in DORMANT mode?

- If YES, consider that CA Top Secret does not perform logging in DORMANT mode. Upgrade mode of user or facility if logging is desired. Go to STEP 4.
- If NO, go to STEP 2.

STEP 2

Examine the DRC control option setting: TSS MODIFY('DRC(drc#)')

Is DRC set to NOVIOL?

- If YES, Reset the DRC NOVIOL setting. Enter:

  ```
  TSS MODIFY ('DRC(drc#,VIOL)')
  ```

  Go to STEP 4.
- If NO, go to STEP 3.

STEP 3

Examine the directory entry for the server machine.

Is there a LINK or MDISK with write access entry for a disk at virtual address X'300'?

- If YES, go to STEP 5.
- If NO, refer to the *Getting Started* on how to create the Audit/Tracking File. Go to STEP 4.

STEP 4

Simulate a violation to the facility in question using the ACID in question.

Was the violation logged?

- If YES, STOP.
- If NO, go to STEP 5.

STEP 5

Enter TSS MODIFY(SYSOUT) and examine the server machine console log.

Are there I/O error messages against the Audit File (TSS0917, TSS0918)?

- If YES, perform DASD diagnostics to determine if there are errors on the pack. Reformat or restore the minidisk if errors are found.
- If NO, go to STEP 6.

STEP 6

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

CA Top Secret Not Logging Access or Initiations

STEP 1

Is AUDIT attribute turned on for the facility?

Enter:

```
TSS MODIFY('STATUS') or TSS MODIFY('FAC(facility)')
```

Is the site or facility in DORMANT mode?

- If YES, consider that CA Top Secret does not perform logging in DORMANT mode. Upgrade the mode of the user or facility if logging is required. Go to STEP 3.
- If NO, go to STEP 2.

STEP 2

Are ACCESS or INIT specified as suboptions of the LOG control option?

- If YES, go to STEP 4.
- If NO, refer to the LOG or FACILITY control options in the *Control Options Guide* on how to enter ACCESS or INIT suboptions. Go to STEP 3.

STEP 3

Simulate the access and initiation attempt using the ACID in question.

Was the access or initiation logged?

- If YES, STOP.
- If NO, go to STEP 5.

STEP 4

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call CA Technical Support.

Messages

The behavior of CA Top Secret Messages is controlled by the MSG suboption of the FACILITY or LOG control option.

Users not Receiving CA Top Secret Messages

STEP 1

Enter:

```
TSS MODIFY('STATUS')
 or
TSS LIST(acid) DATA(XAUTH,PROF)
```

Is the site, facility, profile, or user in DORMANT mode?

- If YES, consider that CA Top Secret does not perform logging in DORMANT mode. Consider upgrading the mode of the user or facility if logging is desired. Go to STEP 4.
- If NO, go to STEP 2.

STEP 2

Determine if the MSG suboption of the LOG control option is specified:

Have the user enter TSS WHOAMI **or** enter:

```
TSS MODIFY('FAC(facility)')
```

Is MSG specified?

- If YES, go to STEP 3.
- If NO, refer to LOG or FACILITY in the *Control Options Guide*, and enter the MSG suboption. Go to STEP 4.

STEP 3

CA Top Secret may suppress messages due to entries made via the MSG control option. Refer to the *Control Options Guide* for instructions on how to check the characteristics of messages via the MSG control option.

Are messages suppressed unnecessarily?

- If YES, Make the appropriate entries for the MSG control option. Go to STEP 4.
- If NO, go to STEP 5.

STEP 4

Perform access and initiation attempts using the ACID in question.

Were messages received?

- If YES, STOP.
- If NO, go to STEP 5.

STEP 5

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

Console not Receiving CA Top Secret Messages

STEP 1

Enter:

```
TSS MODIFY('STATUS')
 TSS MODIFY('FAC(CONSOLE'))
```

Is the site or facility in DORMANT mode?

- If YES, consider that CA Top Secret does not perform logging in DORMANT mode. Upgrade the security mode if logging is required. Go to STEP 4.
- If NO, go to STEP 2.

STEP 2

Determine if the OPER suboption of the LOG control option is specified.

Is OPER specified?

- If YES, go to STEP 3.
- If NO, refer to LOG or FACILITY in the *Control Options Guide* and enter the OPER suboption. Go to STEP 5.

STEP 3

CA Top Secret may suppress certain messages due to entries made via the MSG control option (such as NOOPER). Refer to the *Control Options Guide* for instructions on how to check the characteristics of messages via the MSG control option.

Are messages suppressed unnecessarily?

- If YES, make the appropriate entries for the MSG control option. Go to STEP 4.
- If NO, go to STEP 5.

STEP 4

Perform access and initiation attempts using the ACID in question.

Were messages received?

- If YES, STOP.
- If NO, go to STEP 5.

STEP 5

Gather all information obtained during previous steps. Go to Phase 3 for instructions on how to call Technical Support.

Resource Access Problems

This procedure provides instructions on how to diagnose access authorization problems for:

- Minidisks
- Data Sets
- Volumes
- Other ownable resources

CA Top Secret uses an access algorithm to determine whether or not to grant a user the access that they requested to the resource. This algorithm is reviewed in Chapter 2. A thorough understanding of the algorithm, and the control options and commands which affect the algorithm, are prerequisites to the effective use of the following procedures and guidelines.

Use of the TSS LIST command function is a prerequisite skill. Refer to the *Command Functions Guide* for complete details.

Resource Access Incorrectly Denied

STEP 1

Determine the user's and facility's mode.

Enter:

```
TSS LIST(acid) DATA(XAUTH,PROF)
     TSS MODIFY('FAC(facility)')
```

Does the user or attached profile have a more restrictive mode than the facility?

Example: User is permitted to FAIL mode but the facility is in WARN mode.

- If YES, permit the user to a less explicit mode (or remove the permitted mode) or permit the user explicit access to the resource. Go to STEP 6.
- If NO, go to STEP 2.

STEP 2

Determine if the resource is protected by ownership.

Enter:

```
TSS WHOOWNS resource(resource name)
```

Is the resource owned (possibly by a generic prefix)?

- If YES, the user explicit access to the resource. Go to STEP 5.
- If NO, if the resource is a minidisk or data set, go to STEP 3.

STEP 3

Determine if default protection is in effect for IMPLement or WARN modes (Default protection is automatic for minidisks and data sets in FAIL mode).

Enter:

```
TSS LIST(RDT) RESCLASS(resource)
```

Is the DEFPROT attribute attached to the resource?

- If YES, permit the user explicit access to the resource. Go to STEP 5.
- If NO, go to STEP 4.

STEP 4

Activate the diagnostic trace for the user. Refer to TSS-ADD trace in the Command Functions Guide and the SECTRACE parameter in the Control Options Guide.

Did trace records appear?

- If YES, see the "Diagnostic Trace" appendix for instructions on how to interpret trace information. Go to STEP 5.
- If NO, go to STEP 6.

STEP 5

Log on to VM with the userid or supply the ACID= parameter on the logon command line and attempt to access the resource.

Was the access to the resource now granted?

- If YES, STOP.
- If NO, go to STEP 6.

STEP 6

Obtain all information gathered in the previous steps. Go to Phase 3 for instructions on how to contact CA Technical Support.

Resource Access Incorrectly Allowed

STEP 1

Determine the user's and facility's mode.

Enter:

```
TSS LIST(acid) DATA(XAUTH,PROF)
     TSS MODIFY(FAC(facility))
```

Does the user or attached profile have a less restrictive mode than the facility?

Example: User is permitted to DORM mode but the facility is in IMPL mode.

- If YES, permit the user a more explicit mode or remove the permitted mode. Go to STEP 5.
- If NO, go to STEP 2.

STEP 2

Determine if the resource is authorized to the user.

Enter:

```
TSS WHOHAS resource(resource name)
```

Is the user ACID or attached profile(s) listed as authorized?

- If YES, go to STEP 3.
- If NO, go to STEP 4.

STEP 3

Does the listed permit allow access either through an authorized access level or absence of ACTION(DENY)?

- If YES, Provide a more explicit permit with either ACCESS(NONE) or ACTION(DENY). Go to STEP 5.
- If NO, go to STEP 4.

STEP 4

Activate the diagnostic trace for the user. Refer to TSS-ADD trace in the Command Functions Guide and the SECTRACE parameter in the Control Options Guide.

Did trace records appear?

- If YES, see the “Diagnostic Trace” appendix for instructions on how to interpret trace information. Go to STEP 5.
- If NO, go to STEP 6.

STEP 5

Log on to VM with the userid or supply the ACID= parameter on the logon command line and attempt to access the resource.

Was access to the resource still granted?

- If YES, go to STEP 6.
- If NO, STOP.

STEP 6

Obtain all information gathered in the previous steps. Go to Phase 3 for instructions on how to contact CA Technical Support.

Chapter 4: Phase 3 - CA-Technical Support

This section contains the following topics:

Pre-Call Preparation

Before contacting Technical Support, it is recommended that you attempt to use the applicable Phase 2 diagnostic procedure. If your problem is not solved by the procedure, then you must prepare the necessary information prior to placing your call.

Required Information

Prior to calling CA Top Secret support, obtain the following:

- All information obtained from the Phase 2 diagnostic process, including violation codes, message numbers, TRACE results, operator console log from the time of the error, TSS LIST results, and everything else you know about the problem
- The current CA Top Secret maintenance level as obtained through the VERSION control option for both the CP level and service machine's level of maintenance
- A list of all zaps applied to CA Top Secret as obtained through the APAR STATUS function of CAIMAINT
- Maintenance levels of the software environment
- Any information regarding special exits or customization strategies
- Any information about when the specific problem started and what changes occurred in your system

Enhancing Communication with Technical Support

Please have all required information available If a dump is available, the system programmer should process it to disk using DUMPLOAD. Then the dump can either be sent on tape (use either TAPE DUMP or VMFPLC2 DUMP), or the dump can be sent immediately via FTP after contacting Support.

Note: When using FTP, be sure to specify BINARY F 4096 before sending. See Using Anonymous FTP to Send Documentation for more information.

Contacting Technical Support

CA provides 24-hour support, 365 days a year. If you need technical assistance with your CA product, there are four ways to obtain it:

- During normal business hours, call the support number for the product with which you are having a problem, and you will be connected with a support representative. If a technician is not available, your call will be logged and a technician will return your call as soon as possible.

  If you are calling with a severity one problem and do not get a technician immediately, the receptionist will ask you if you would like to stay on hold until a technician is available. The support number for the CA VM products is 908-874-9605. (The individual support numbers are listed in the Product Support Directory,located at http://support.cai.com.)

- A toll free number 1-800-645-3042 is also available to you for support calls. Calls logged there will be returned in a timely fashion. This number is also to be used to request after-hours emergency support for all products. If you are calling from outside of North America or if the 800 number is not accessible to you please contact your local CA Support Center.

- If you wish to contact the center through FAX, you may do so using the following number: 908-874-9178.

  Note: Only your local CA Technical Support Center can provide native language assistance. Please use English when contacting any North American center.

- CA-Total Client Care (CA-TCC) provides internet access to the CA centralized client support database at http://support.cai.com. This includes access to Program Temporary Fixes (PTFs), PIBs, and PMLs for all environments, and direct problem reporting and tracking capabilities.

There are two kinds of technical support available: primary and emergency. Primary service is provided for all CA products during normal business hours. Emergency service is available after primary service hours for severity one problems only.

When contacting technical support, have the following information available:

- Your site ID (a six digit ID which uniquely identifies your site). This number can be found on the labels of most mailings received from CA, or may be obtained from your account manager.
- The product name, release number, operating system and genlevel
- Your name, telephone number, and extension (if any)
- Your company name
- The severity code—This is a number from one to four that you assign to the problem. Use the following guidelines when determining the severity of the problem:

  1—A “system down” or inoperative condition

2—A suspected high-impact condition associated with the product

3—A question concerning product performance or an intermittent low-impact condition associated with a product

4—A question concerning general product utilization or implementation

- Any documentation that may help in resolving the problem, including dumps, compiler listings, etc.

Refer to the Product Support Directory for the individual primary service support numbers for each of your CA products. For severity one calls during emergency service hours, you should always call 1-800-645-3042 so that a technician on call can be paged to return your call.

Note: Requests for services such as: orders for documentation, maintenance tapes, requests for products, information about education, on-site assistance, or requests for new features or design changes to CA Top Secret may be directed to your Regional Account Representative.

Level One Support

The level one support team handles problems as follows:

- If the problem appears to be caused by CA Top Secret internals, the technician determines if corrective maintenance tapes have been distributed. If the maintenance tapes have been distributed, the analyst asks the customer to apply the maintenance. If no fix exists, the problem is escalated to the level two support team for further examination.
- If the problem appears to be caused by customer setup, then the technician attempts to help the customer diagnose and resolve the error. The technician asks many of the same questions that were asked by the Phase 2 procedures.
- Before escalating a problem to level two support, the level one technician ensures that the customer has prepared information as documented in this guide.
- If a client calls asking for the status of a case, any technician can offer assistance provided the client has a contact number. The customer should specify that he or she merely wants the status of a particular case.

Level Two Support

The level two support team is responsible for the following type of request:

Locate the internal errors and provide a fix. These fixes are later incorporated into the standard maintenance tapes. If the level two technician is unable to locate the internal error, or if the error requires major modifications, the request is referred to management for review by development.

Mailing Diagnostic Information

Diagnostic information, such as trace records, system logs, etc., may be mailed to the following address:

Note: Your CA Top Secret customer number and representative must be clearly marked on the package.

```
CA, Inc.
                PCS Desk
          Route 206 & Orchard Road
   Princeton, New Jersey 08543-0008 USA
  case number, representative name
```

Note that this address is appropriate for documentation (hard copy) only.

VM dumps must be either TAPE DUMP or VMFPLC2 DUMPs of the processed dump file created by DUMPLOAD. Under no circumstances should you send a SPTAPE dump of the unformatted spool file.

Please mark the following information on the tape's external label:

- Contact number associated with diagnostic materials
- Names of files on the tape.
- Release of operating system on which material was produced (for example, VM/ESA 2.4.0). Maintenance level of operating system (for example, 9903).
- Return address if the tape needs to be returned to your data center.

Note: A cover letter should accompany the tape information. Call your CA Technical Support Representative for a copy of the letter and send it with the tape information to:

```
CA, Inc.
      1 CA Plaza
       Islandia, NY 11788-7000
  Attn: PCS Desk
```

Materials that are not in the proper form delay problem resolution.

Using Anonymous FTP to Send Documentation

As an alternative to mail or dialing into a client site, documentation can be exchanged with support using anonymous FTP. To do this you must have FTP client software running at your site and must not be prevented by a firewall or company policy to connect to the CA FTP server. To use this facility, the technical support person at CA must set up a private directory for the data. A directory will be created with a format similar to the following, sftp://supportftp.ca.com/xxxxxxx/yyyyyyyy-01/files_from_customer, where xxxxxxx is the site ID yyyyyyy is the issue number.

Once the directory is created you can send data by connecting to server MF.CAI.COM. Log on using your support.ca.com userid and password.

A typical dialog follows:

```
ftp supportftp.ca.com
EZA1450I IBM FTP CS V1R10
EZA1466I FTP: using TCPIP01
EZA1554I Connecting to: supportftp.ca.com 141.202.253.54 port: 21.
220 usilfs60 FTP server (SecureTransport 4.8.1) ready.
EZA1459I NAME (supportftp.ca.com:USER01):
USER01@ca.com                                <----- online_userid
  EZA1701I >>> USER USER01@ca.com
  331 Password required for USER01@ca.com.
  EZA1789I PASSWORD:
 ********                                     <----- online_password
  EZA1701I >>> PASS
  230 Virtual user USER01@ca.com logged in.
  EZA1460I Command:
 cd /0143445/19115730-01/files_from_ca
  EZA1701I >>> CWD /0143445/19115730-01/files_from_ca
  250 CWD command successful.
  EZA1460I Command:
 binary f 4096
  EZA1542I Usage: BINARY
  EZA1460I Command:

 put 'dataset.name' dump                    <--- sends data from your system to CA
 Binary Transfer complete
 QUIT
 Goodbye
```

A full explanation of FTP commands are documented with your FTP client software.

Chapter 5: Using the TSSFAR Utility

This section contains the following topics:

TSSFAR Tasks

The CA Top Secret File Analysis Routine (TSSFAR) allows security administrators to review the permissions and assignments that are recorded in the Security File. The type of security information displayed by TSSFAR depends upon the control statements selected. Each control statement is discussed in detail following a discussion of the JCL necessary to execute TSSFAR.

TSSFAR can be used to perform the following tasks:

- Provide a cross reference of ALRB block keys with the ARLBs in the block and verify the count against what is in the header block map.
- Review mismatched ARLB chains.
- Review connections between ACIDs and PROFILEs.
- Review connections between owned and owning ACIDs.
- Review resource ownership between ACIDs and resources.

CAUTION! The file upon which TSSFAR executes will be continuously accessed for the duration of the job. Therefore, running TSSFAR against the Security File could cause significant degradation to system performance. Because of this, we strongly recommend that TSSFAR always run against a Backup File. Only run TSSFAR at the direction of the CA Top Secret support staff.

TSSFAR JCL

The following sample JCL can be used to run TSSFAR.

```
//TSSJOB ACID=MASTER,PASSWORD=USOPEN
//EXEC PGM=TSSFAR
KEY=C2C9C7C2E4C3D2E2
PRIMARY
ACIDCHAN
HEADER
ARLBMAP
ALLOC
ACIDLINK
RESINDEX
WHOHAS(resource owning ACID)
 /*
```

Control Statements

The selection criteria used in generating TSSFAR reports are listed below. They are described on the following pages. Mandatory control statements are:

- KEY
- PRIMARY or BACKUP

Option control statements are:

- ACIDCHAN
- ACIDLINK
- ALLOC
- ARLBMAP
- HEADER
- RESINDEX
- WHOHAS (resource owning ACID)

Mandatory Control Statements

This section describes the mandatory control statements.

KEY=

Displays customer encryption key in either 16 byte hexadecimal or 8 EBCDIC characters. The KEY control statement is mandatory.

KEY=*hhhhhhhhhhhhhhhh*|:hp5.'*cccccc*':ehp5.

PRIMARY or BACKUP

You must specify which Security File, either the Primary or the Backup, that TSSFAR will search. The control statement PRIMARY causes TSSFAR to search the Primary Security File; the control statement BACKUP causes TSSFAR to search the Backup Security File.

Optional Control Statements

This section describes the optional control statements.

ACIDCHAN

ACIDCHAN runs the ALLOC function and then uses the ACID index and chase ARLB chains to build a second allocated ACID map. While chasing the chains, TSSFAR will confirm the actual number of chained ARLBs against what the ACID had listed in its FACTREC. ACIDCHAN then lists any ARLBs that are chained but empty. If these match the ARLB numbers reported as key errors in the ALLOC function, the allocation maps are correct.

All FACTREC header ARLB counts match actual chains - This message shows that the value found as the number of ARLBs in the FACTREC header matches the number of ARLBs chained together for all ACIDs.

Note: There will be a discrepancy of 12 in the total number of ACIDs reported in your system by TSSFAR compared to a TSS LIST command. This is due to TSSFAR having eight User ACIDs that are reserved and four Department ACIDs that are dynamically built.

ACIDCHAN provides additional analysis of the contents as follows:

- The number of ACID index entries allocated and used.
- The number of ACID index blocks allocated and used.
- The next and last available ACID number.
- Recommended CA Top Secret cache size.
- Recommended XES structure size.

ACIDLINK

ACIDLINK reviews all ACIDs for connections to other ACIDs. If a connection exists, ACIDLINK verifies whether it should exist. If an ACID shows a profile attached, ACIDLINK verifies that the profile reflects the same information.

ALLOC

Prints a cross reference of all ARLB block keys and the actual ARLBs in the block. ALLOC also verifies the number of ARLBs against what is in the header block map.

This routine assumes that if an ARLB is allocated, it should have something in it. Exceptions exist if an ARLB is chained and the first byte was used to add an x'00' to end an XE. This makes the key appear to be wrong because the key is allocated but the ARLB is empty. These cases can be resolved using the ACIDCHAN function.

ARLBMAP

Prints the ARLB allocation map from the header record.

HEADER

Prints the first 256 bytes of the header record.

RESINDEX

RESINDEX verifies that all resource ownership indexes match the owning ACID.

WHOHAS (Resource Owning ACID)

WHOHAS (resource owning ACID) lists PERMITS to all resources owned by the specified ACID.

Sample TSSFAR Output

A sample TSSFAR output is printed below.

```
KEY=
PRIMARY
HEADER
ARLBMAP
ALLOC
ACIDCHAN
ACIDLINK
RESINDEX
WHOHAS(FJADEPT)
   ******* HEADER   *******

          +000000  C8C4D940 00001800 000016B8 F88DCF5D  E73B600F ED864B51 F61EB78F
C2709644  * HDR ........8..)X.-..f..6...B.o.
          +000020  F7306C1C 48E52F93 14808000 48E52F93  CBA33F60 00000000 00001027
0098240F  * 7.%..V.l.....V.l.t.-.........q..
          +000040  11001335 00000000 00000000 00000000  00000052 00000014 00000004
00000001  * ............................
          +000060  000001C2 00001480 00000000 00000000  00000018 00000180 00000180
00000180  * ...B........................
          +000080  000000AF 0000001E 0000000A 00000070  00000008 00000074 00000236
0000006F  * ............................?
          +0000A0  0000001D 00000073 00000008 00000235  000016B5 00007AFF 00004A4A
000005FF  * ....................:.........
          +0000C0  00000000 0001339D 0001EBFF 00000180  00230010 00100100 00000000
00000000  * ............................
          +0000E0  C2C1C3D2 E4D74040 439B95A0 28068EEE  FA000000 00000000 00000000
00000000  * BACKUP  ..n...................

   ******* ARLB MAP *******

          +000000  00000000 00000000 00000000 00000000  00010000 00000000 00000000
00000000  * ............................
          +000020  00000000 00000000 00050001 00000200  00000200 00000000 00000000
00020000  * ............................
          +000040  00000000 00000002 00000102 01040100  00000200 01000000 00000200
00000100  * ............................
          +000060  00000000 00000000 01010009 03020500  00000000 00000000 00000004
00000000  * ............................
          +000080  08050000 00000605 02030307 01020001  01040300 00020303 010B0000
000B0A18  * ............................
          +0000A0  0003060B 000B0003 00001809 01000B00  07180000 00000000 18181818
18181818  * ............................
          +0000C0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ............................
          +0000E0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ............................
          +000100  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ............................
          +000120  18181818 18181818 18181818 18181818  18181818 18181818 18181818
```

```
18181818   * ............................
           +000140  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000160  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000180  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +0001A0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +0001C0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +0001E0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000200  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000220  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000240  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000260  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +000280  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +0002A0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +0002C0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
           +0002E0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818   * ............................
```

```
            C A - T O P   S E C R E T  V e r s i o n  1.6 -- Security File Analysis
Utility                        mm/yy/dd

          +000300  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +000320  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +000340  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +000360  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +000380  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +0003A0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +0003C0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +0003E0  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +000400  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................
          +000420  18181818 18181818 18181818 18181818  18181818 18181818 18181818
18181818  * ..............................

 *** Allocation Map Validation Begins ***

 RBA 00567 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00005 KEY/ARLB
mismatches: 00000

 RBA 00569 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00005 KEY/ARLB
mismatches: 00000

 RBA 00570 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00008 KEY/ARLB
mismatches: 00000

 RBA 00580 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00002 KEY/ARLB
mismatches: 00000

 RBA 00588 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00003 KEY/ARLB
mismatches: 00000

 RBA 00596 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00597 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00598 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000
```

```
 RBA 00599 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00600 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00601 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00602 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00603 RESULTS:  HEADER FREE ARLBS: 00000 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000

 RBA 00609 RESULTS:  HEADER FREE ARLBS: 00001 KEY/ARLB Matched free: 00012 KEY/ARLB
mismatches: 00000

 RBA 00715 RESULTS:  HEADER FREE ARLBS: 00002 KEY/ARLB Matched free: 00013 KEY/ARLB
mismatches: 00000

 RBA 00733 RESULTS:  HEADER FREE ARLBS: 00003 KEY/ARLB Matched free: 00024 KEY/ARLB
mismatches: 00000
```

```
            C A - T O P   S E C R E T  V e r s i o n   1.6  --  Security File Analysis
Utility                         mm/yy/dd

 *** ACID Chain Validation Begins ***

 All FACTREC header ARLB counts match actual chains

 ACID:  RBA 00719   ARLB 0003672      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003673      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003674      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003675      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003676      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003677      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003678      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003679      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003680      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003681      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003682      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003683      Key: USED      Chain: FREE
 ACID:  RBA 00719   ARLB 0003684      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003912      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003913      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003914      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003915      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003916      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003917      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003918      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003919      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003920      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003921      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003922      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003923      Key: USED      Chain: FREE
 ACID:  RBA 00729   ARLB 0003924      Key: USED      Chain: FREE


 Acid index entries allocated:     31,487  Acid index entries defined:      1,900

 Next available acid number:       19,018  Last available acid number:     31,487

 Acid blocks allocated:             5,248  Acid blocks used:                  173


 Recommended TSS cache size:          1033K

 Recommended XES structure size:      4236K
```

```
            C A - T O P   S E C R E T  V e r s i o n   1.6  --  Security File Analysis
Utility                         mm/yy/dd

 Active Acid count:     1,888  Average size:       477 bytes

              SCAs:         81
             LSCAs:         16
             ZONEs:         20
              ZCAs:          4
              DIVs:         48
              VCAs:         92
             DEPTs:        185
              DCAs:         30
             USERs:        817
             PROFs:        579
            GROUPs:         16

 *** ACID Chain Validation Ends ***


 *** Acid Link Validation Begins ***

 ACID RPGDCA1  claims Profile RPGP1    but the Profile doesn't claim the ACID
 ACID RPGDCA1  claims Profile RPGP2    but the Profile doesn't claim the ACID

 Profile FJAP1    claims ACID SYSOPR   but the  ACID doesn't claim the Profile
 Profile HARBE1P1 claims ACID HARBPROF but the  ACID doesn't claim the Profile
 ACID RPGD1    claims to be owner of HARBE07  but he denies it
 ACID TCSMSCA  claims to be owner of KOTPA01  but he denies it
 ACID TCSMSCA  claims to be owner of ZONECA   but he denies it

 *** Acid Link Validation Ends ***


 *** Resource Index Validation Begins

 ACID IJMDEPT1 denies owning RIE  rescode(D0) resource IJMUSER1
 ACID CICSDEPT denies owning RIE  rescode(C6) resource FILER

      7,680 RIE  Type Entries allocated      4,862 RIE   Type Resources defined

 ACID TCSWKS   denies owning PIE  rescode(C4) resource A1234567.B1234567.C1234567
 ACID ELLPH01  denies owning PIE  rescode(E1) resource DLF2.TEST.P001092.D15699V1
 ACID PASJE01  denies owning PIE  rescode(E1) resource DLF2.TEST.P001093.D15699V1
 ACID ELLPH01  denies owning PIE  rescode(E1) resource DLF2.TEST.P001091.D15699V1
 ACID PASJE01  denies owning PIE  rescode(C4) resource PASJE06.PASJE03.PASJE02.PA
```

```
            C A - T O P   S E C R E T   V e r s i o n   1.6  --  Security File Analysis
Utility                          mm/yy/dd

 ACID ACCTDP   denies owning PIE  rescode(C4) resource REIPA02.SMS.DATA
 ACID TOPDINV  denies owning PIE  rescode(C4) resource TOP.INVEST.MASTER.WITH.CRU
 ACID RPGP25   denies owning PIE  rescode(9B) resource ZZZZZZZZ.BBBBBBBB.CCCCCCCC

     78,750 PIE  Type Entries allocated      2,553 PIE   Type Resources defined

 ACID BUTJO04  denies owning VPIE volume G

        384 VPIE Type Entries allocated         27 VPIE  Type Resources defined

 ACID TOPDSFT  denies owning VIE  volume TOPMVS
 ACID VOLDEPT  denies owning VIE  volume TSS001
 ACID TOPDSFT  denies owning VIE  volume TOPTSO
 ACID TOPDSFT  denies owning VIE  volume TOPWK2
 ACID HZSP1S   denies owning VIE  volume TSS002
 ACID CICSDIV  denies owning VIE  volume TED
 ACID TOPDSFT  denies owning VIE  volume TOPPAG
 ACID TOPDSFT  denies owning VIE  volume TOPUSR
 ACID TOPDSFT  denies owning VIE  volume TOPWK3
 ACID TOPDSFT  denies owning VIE  volume TOPIPL
 ACID TOPDSFT  denies owning VIE  volume TOPWK1
 ACID MDADEPT  denies owning VIE  volume TIM001
 ACID TOPDSFT  denies owning VIE  volume TOPRES

      1,536 VIE  Type Entries allocated        202 VIE   Type Resources defined

 *** Resource Index Validation Ends

 WHOHAS information for ACID: FJADEPT
 NRNP5     DATASET   HH.+++++++P
    ACCESS(READ)

 NRNP5     DATASET   HH.PY+++++P
    ACCESS(NONE)

 ROSCOE    IBMGROUP  ARCCATGP

 DINERO    DATASET   HH.+++++++X
    ACCESS(UPDATE)

 DINERO    DATASET   HH.LO+++++X
    ACCESS(READ)

 VENTURE   DATASET   HH.+++++++X
    ACCESS(ALL)
```

```
            C A - T O P   S E C R E T   V e r s i o n   1.6  --  Security File Analysis
Utility                          mm/yy/dd

 VENTURE    DATASET   HH.LO+++++X
    ACCESS(READ)

 TCSLFM     DB2       DSNR.SSS

 FOXYD      DB2       DSNR.SSSS.BATCH

 FOXYD      DB2       DSNR.DB2E.BAT

 *ALL*      DATASET   'FRANKS.TEST.DSN'
    ACCESS(READ)

 SYSADM     DB2       DSNR.DSN.BATCH

 TDGRPG     OPCCLASS  AD
    ACCESS(READ)

 TCSFJA     ARANK     BINKY
    ACCESS(READ)
    ACTION(FAIL)

 TCSFJA     DB2       DSNR.SSSS.BATCH

 TCSFJA     ARANK     L2U
    ACCESS(READ)

 TDGRPG     DATASET   DB2SYS
    ACCESS(CREATE)

 MCCRA01    DATASET   DSNTEST.RENAME
    ACCESS(ALL)
    ACTION(FAIL)

 DB2ACID    DATASET   DB2
    ACCESS(ALL)

 DB2ACID    DATASET   DSN
    ACCESS(ALL)

 *ALL*      DB2       DSNR.DB2T.
    ACTION(AUDIT)

 MATGA01    OTRAN     FLOG
    ACCESS(ALL)
```

```
                C A - T O P   S E C R E T   V e r s i o n   1.6  --  Security File Analysis
Utility                              mm/yy/dd
 HARBE30   TSOPROC   $HARBE03

 HARBE30   TSOPROC   $HARB350

 ACCTUS3   TSOPROC   $TSO(G)

 ACCTUS2   TSOPROC   $TSOAC(G)

 ACCTUS5   TSOPROC   $TSOAC

 DABAD01   TSOPROC   $DABDB2(G)

 DABAD01   TSOPROC   $DABXDC(G)

 DABAD01   TSOPROC   $DB2510(G)

 *ALL*     TSOPROC   $DABDB2

 ADAM01    TSOPROC   $DABDB2

 *ALL*     TSOPROC   $DB2510

 *ALL*     TSOPROC   $

 BERLA02   TSOPROC   $BERLA02

 WHOHAS info list complete
 ***File Analysis Complete***
```

Appendix A: Diagnostic Tools

This section contains the following topics:

List of Tools

TSS LIST

Lists ACID information including that contained in attached profiles. It can also list global (ALL) authorizations related to the accessed resource. Refer to the Command Functions Guide.

TSS WHOHAS

Lists the ACIDs which have access to the resource specified in the command. Refer to the Command Functions Guide.

TSSUTIL program

Used to obtain event reports. Refer to the Reporting Guide.

TSS WHOAMI

Describes a logged on user's security environment and important controls such as bypass attributes, log and message display options, and user's mode. Useful for "on-the-spot" debugging. Refer to the Command Functions Guide.

MODE

The mode of the actual event, not always the user's or facility's mode. You must know the actual mode, be it facility, user, or event level. The only sure way of knowing the mode of a security event is through a trace. Refer to the Control Options Guide.

Authorization Algorithm

Basic understanding of the algorithm is mandatory for definition of proper authorizations. Refer to the General Concepts Guide.

AUTH control option

Incorrect setting or changing of AUTH dramatically affects whether CA Top Secret grants access to a resource. Refer to the Control Options Guide.

LOG control option

LOG and FACILITY(LOG=) control CA Top Secret violation recording and message display. Refer to the Control Options Guide.

Message Algorithm

Explains when and why messages are displayed or suppressed. Appendix C describes the algorithm.

MSG control option

Controls message characteristics, such as when they are to be suppressed. Refer to the Control Options Guide for details.

TRACE

The diagnostic trace can be employed to provide event-related details that cannot be uncovered by other tools. Appendix B explains how to interpret trace information. See TRACE in the ADD/REMOVE chapter of the Command Functions Guide and SECTRACE or FACILITY in the Control Options Guide for instructions on how to apply the trace.

STATUS control option

Status of various control options and understanding of how they relate to or affect the behavior of Trust CA Top Secret Security. Refer to the Control Options Guide for details.

FACILITY control option

Attributes and status of facility controls. Refer to the Control Options Guide for details.

DRC control option

Controls or displays violation attributes, especially if your site has changed the effect of some violations. See DRC in the Control Options Guide, and DRC in the Messages and Codes Guide.

DUMP control option

Generates internal control block dump. Appendix D documents how to interpret the output. See also DUMP in the Control Options Guide.

CAIMAINT

To obtain a maintenance level, and optional and special zap status.

Appendix B: Diagnostic Trace

This section contains the following topics:

Using Trace

The CA Top Secret trace is used to diagnose access problems. It is activated via any one of several control options specified through the TSS MODIFY command in combination with the TSS ADDTO commands:

Trace Level	Activation
SYSTEM-WIDE	SECTRACE(ALL)
FACILITY-WIDE	FACILITY(VM=TRACE)
GROUP OF USERS	TSS ADDTO(profile) TRACE
SPECIFIC USER	TSS ADDTO(user) TRACE

Note: The SECTRACE parameter does not apply to SFS resource access.

Trace Destinations

Trace records can go up to the user's terminal, operator's console, or both. The trace provides abundant information: two or three lines per event.

Trace Messages

What follows is a sample trace message and a table which explains what each term in the message indicates.

Trace messages begin with:

```
TSS-?
```

The “?” indicates the type of trace record, as shown below. A trace for a single event comprises one to three trace messages with the headers shown below:

- TSS-?-trace data .....
- TSS-1 trace data .....
- TSS-2 trace data .....
- TSS-5 trace data .....

Trace Formats

The following trace record is always produced during a trace:

```
TSS-c U/cccccccc A/cccccccc T/cccccccc M/c RC/xxxxxx
      VF/xxxxxxxx SF/xxxxxxxx OC/xxxxxxxx
```

TSS-c

The c is one of four values:

- I—Session initiation
- T—Session termination
- R—Resource validation
- F—Resource validation by CP fast-path

U/ccc..c

The name of the virtual machine

A/ccc..c

The ACID under which the virtual machine is running

T/ccc..c

The terminal at which the user is logged on or “DISC”

M/c

The mode of the user:

- D—DORMANT
- W—WARN
- F—FAIL
- I—IMPLEMENTATION

RC/xxx..x

The return code:

- Byte 1: Return Code
- Byte 2: Detail error Reason Code (DRC)
- Byte 3: Flags for the DRC as set by the DRC control option
- X'80' = Reserved
- X'40' = "
- X'20' = "
- X'10' = Password type violation
- X'08' = This DRC is also audited

- X'04' = Fail in all modes
- X'02' = Fail in WARN mode
- X'01' = Not a violation, do not log unless audited

VF/xxx..x

Security flags (Part 1)

- Byte 1:
  - X'80' = AUTOLOG request
  - X'40' = ACID= specified on logon or autolog
  - X'20' = Reserved
  - X'10' = User is system operator
  - X'08' = Random new password requested
  - X'04' = Non-IBM or indirect ACI call
  - X'02' = Reserved
  - X'01' = AUTOLOG directory password has been verified
- Byte 2:
  - X'80' = User has supplied at least one invalid password
  - X'40' = Virtual machine is disconnected
  - X'20' = DOWN option has been used
  - X'10' = TSS MODIFY
  - X'08' = Virtual machine is running on surrogate ACID
  - X'04' = User is TSS locked
  - X'02' = Re-init of user to refresh Security Record
  - X'01' = User is surrogating self
- Byte 3:
  - X'80' = Access violation detected by CP fast-path
  - X'40' = Log an Audit Record
  - X'20' = Reserved
  - X'10' = "
  - X'08' = "
  - X'04' = "
  - X'02' = "
  - X'01' = "
- Byte 4:

- X'80' = ACID has been suspended
- X'40' = Resource authorized with VMPRIV
- X'20' = Virtual machine to be forced
- X'10' = Data set authorization based on volume
- X'08' = Reserved
- X'04' = "
- X'02' = "
- X'01' = "

SF/xxx..x

Security flags (Part 2)

- Byte 1:
  - X'80' = Modifying attributes of current VM
  - X'40' = Shared portion of RACVT modified
  - X'20' = TSSVMI call
  - X'10' = Audit this call
  - X'08' = TSSSEC resource audit test
  - X'04' = CP TRANSFER
  - X'02' = VMUSER present on CP command
  - X'01' = CP command has privileged and non-privileged forms
- Byte 2:
  - X'80' = Password was changed
  - X'40' = Random password generated
  - X'20' = Password validated
  - X'10' = Skip password validation
  - X'08' = Forced logon
  - X'04' = Reconnect logon
  - X'02' = New password required
  - X'01' = Autolog logon
- Byte 3:
  - X'80' = VMMACHine needs to be validated
  - X'40' = Force default protection on resource
  - X'20' = Volume access check for DSN
  - X'10' = Resource is defined

- X'08' = Password verification request
- X'04' = Reserved
- X'02' = "
- X'01' = "

- Byte 4:
  - X'80' = Violation has occured
  - X'40' = Suppress logging
  - X'20' = Force failure
  - X'10' = Audit entry
  - X'08' = Send a message to operator
  - X'04' = Issue the message in DORMANT mode
  - X'02' = Password violation for defined user
  - X'01' = Reserved

OC/xxxxxxxx

The original resource class if translation was performed.

For resource validation, an additional trace record is produced:

```
TSS-1 RT/x RD/xxxx AC/xxxxxxxx AT/xxxx AL/xxxxxxxxxxxxxx
      RN/ccccccccccccc
```

RT/x

Resource type.

RD/xxxx

Resource flags from RDT.

- Byte 1:
  - X'80' = Resource supports access levels
  - X'40' = Resource supports libraries
  - X'20' = Resource supports PRIVPGM
  - X'10' = Call resource exit for this resource
  - X'08' = Resource supports VMUSER
  - X'04' = Resource is protected by default
  - X'02' = Resource supports 44 character names
  - X'01' = Validate the resource using AUTH(MERGE)
- Byte 2:
  - X'80' = Fake RDT entry (internal use)

- X'40' = Built in resource indicator
- X'20' = Use AUTH(ALLMERGE)
- X'10' = VAX remote resource
- X'08' = Does not prefix by default
- X'04' = PIE type resource
- X'02' = Allow access by default
- X'01' = Maskable RIE

AC/xxxxxxxx

Requested (byte 1) and allowed (byte 2) access to resource

- The meanings of these flags vary from resource type to resource type. A list of these values for a specific resource may by found by listing the required RDT entry:

```
TSS LIS(RDT) RESCL(resource-class)
```

AT/xxxx

ACTION associated with permit

- X'8000' = Treat authorization in FAIL mode
- X'4000' = Process as privileged CP command/diagnose
- X'2000' = Audit this access
- X'1000' = Invoke installation exit
- X'0800' = Issue message TSS0400I to operator
- X'0400' = Reserved
- X'0200' = Prompt for link password (minidisk only)
- = Base data set access on volume access (O/S volume only)
- = Deny access (resource only)
- X'01' = Reverify password (MVS resource only)

AL/xxx..x

Algorithm details

- Byte 1: High length of resource found
- Byte 2: Algorithm detail
  - X'00' = Resource access allowed
  - X'04' = Resource not defined
  - X'08' = Resource access denied
  - X'0C' = Resource access denied with ACCESS(NONE)

- Byte 3: How resource is authorized
  - X'80' = Owned by ACID or connected profile
  - X'40' = Permitted to ACID or connected profile
  - X'00' = No authorization exists
- Byte 4: Which profile for resource
  - X'00' = Permitted to/owned by ACID
  - X'01'-X'FC' = Relative profile
  - X'FF' = ALL Record
- Byte 5: Rule within user/profile ACID record
- Byte 6: Which profile for volume (O/S data set only)
- Byte 7: Rule within profile for volume (O/S data set only)

RN/ccc..c

Resource name

- If the resource being validated also supports the VMUSER attribute, a third trace record is provided:

```
TSS-2  VH/x  VU/cccccccc
```

VH/x

High length of VMUSER

VU/ccc..c

Name of VMUSER being validated

```
TSS-5  fieldname/pf  fieldname/pf  fieldname/pf  fieldname/pf  fieldname/pf
fieldname/pf
```

Fieldname

Name of field to be extracted

pf

Relative security record from which the field was extracted:

- 00 = User record
- 01-FE = Profile 1-254
- FF = Default value supplied
- NF = Field not found

Example Diagnostic Traces and Meanings

Trace Example 1

Problem:

USER01 is running in IMPLEMENT mode and has an explicit permit to link any of USER02's minidisks in the form:

```
TSS PER(USER01) VMMD(USER02) ACC(READ)
```

However, when a link to USER02's 191 disk is issued, the attempt is failed by CA Top Secret. The following trace records are produced:

```
TSS-R U/USER01 A/USER01 T/GRAF0081 M/I RC/086640
      VF/00000000 SF/00000000
TSS-1 RT/7 RD/8100 AC/400000000 AT/0000 AL/090C4002040000
      RN/USER02.0191
```

From the trace, it can be seen that the user is being failed by CA Top Secret: Return code=8, DRC=66 (insufficient access).

Solution:

An examination of the access flags (AC/) shows that USER01 is requesting read access (byte 1=40); however, the allowed access has been found to be none (byte 2=00). This occurs in spite of the permit that was done with an ACC(READ).

An examination of the algorithm flags (AL/) indicates that the permit which was used in determining access was not the one in the ACID record, but the fourth permit (byte 5=4) in the second profile (byte 4=02) attached to this user. A TSS LIST of this profile shows that there is indeed an explicit permit to USER02.0191 with ACC(NONE).

This still leaves the problem as to why the permit in the ACID record was ignored. Under normal AUTH(OVERRIDE) processing, CA Top Secret would have matched on the permit in the user ACID and stopped. The answer lies in the RDT (RD/) flags. The first byte of the RDT flags indicates the following:

x'80' shows that the resource supports access levels

x'01' indicates that the resource has the MERGE attribute associated with it.

With the MERGE attribute, CA Top Secret takes the best fit (longest prefix) from the combination of the user ACID record and all attached profiles.

Trace Example 2

Problem:

USER01 has a SOURCE(GRAF009) associated with USER01's ACID but can still log on from any terminal. A list of USER01's ACID and attached profiles show no other SOURCE restrictions. The following trace record is produced when USER01 logs on:

```
TSS-I U/USER01 A/USER01 T/GRAF0081 M/I RC/001AC1 VF/00000000
      SF/00000080
```

Solution:

A review of the RC/DRC flags (RC/) shows that while the user is getting a violation (byte 2=1A, invalid source), the return code (byte 1) is zero. The DRC flags (byte 3) indicate the cause of the problem. The x'C0' is irrelevant, however the x'01' indicates the DRC has the NOVIOL attribute. With the NOVIOL attribute, the violation is ignored.

Appendix C: Message Display/Suppression Algorithm

The checks that are made to determine whether or not the user or security console receive a message are documented in the following flowchart:

Appendix D: SAFTRACE

The SAFTRACE control option controls the display of RACROUTE calls coming to the security server via the RACROUTE macro.

SAFTRACE Control Option

Format:	Entry Method:
SAFTRACE(*function*,*option*... [,*option*... [,*option*...]])	Parameter File/MODIFY

function

Is one of the following:

- SET—Define a new SAFTRACE entry
- MODIFY—Alter an already defined SAFTRACE entry
- ENABLE—Enable a currently disabled SAFTRACE entry
- DISABLE—Disable a currently enabled SAFTRACE entry
- DELETE—Remove a currently defined SAFTRACE entry
- DISPLAY—Display a specific entry or all currently defined SAFTRACE entries

option

Is one of the following:

- ID=xxxxxxxx—A user defined name for this SAFTRACE entry
- ID=ALL—Function applies to ALL existing SAFTRACE entries
- DEST=UserID to receive trace information.
- DISABLE—New SAFTRACE is to be disabled after definition
- USERID=—Limit SAFTRACE output to use of this ACEE
- VMUSERID=—Limit SAFTRACE output to calls from this virtual machine
- RETCODE=—Limit SAFTRACE output to this return code
- RSNCODE=—Limit SAFTRACE output to this reason code
- MATCHLIM=—After 1 to 255 matches, disable this SAFTRACE
- TRACE=BEFORE—Show the RACROUTE macro at ESM entry
- TRACE=AFTER—Show the RACROUTE macro and return codes at ESM exit
- TRACE=ALL—Show both before and after

The table below shows which options are valid for which functions.

Note: Some form of id= is required for all functions.

	SET	ENABLE	MODIFY	DISABLE	DELETE	DISPLAY
id=ALL		X	X	X	X	X
id=xxxxxxx	X	X	X	X	X	X
DEST=	X		X			
DISABLE	X		X			
USERID=	X		X			

	SET	ENABLE	MODIFY	DISABLE	DELETE	DISPLAY
VMUSERID=	X		X			
RETCODE=	X		X			
RSNCODE=	X		X			
MATCHLIM=	X		X			
TRACE=	X		X			

Example

To set a SAFTRACE to show all RACROUTE calls with resulting reason codes for machine SFSSERV, enter the following:

```
TSS MODI(SAFTRACE(SET,ID=TRACE1,TRACE=AFTER,VMUSERID=SFSSERV))
```

Note: The results of a SAFTRACE(DISPLAY,...) are returned to the issuer of the command. If DEST= is used, the actual traces, as they occur, will go to the CA Top Secret service machine console and the userID specified in the DEST= parameter. If DEST= is not specified, the trace info will only go to the service machine console. To see those traces as they occur you must set active the secondary console support for the service machine.