CA Top Secret® for z/OS

Message Reference Guide

r15

Tenth Edition

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the “Documentation”), is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 changes have been made since the last release of this documentation:

- Added or revised messages TSS9150I, TSS9920I, TSS9921I, TSS9922I, TSS9923I, TSS9924I, TSS9925I, TSS9926I, TSS9927I, TSS9951I, TSS9952I, TSS9953I, TSS9954I, TSS9955I.

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

- Added or revised the following messages:
  - TSS0415E—INVALID SITRAN FACILITY (see page 79)
  - TSS1366W—SECCACHE Data | Index area is nnn% full (see page 138)
  - TSS1629I—Unable to send IBM ENF Signal for command (see page 192)
  - TSS7111E—NEW PASSWORD | PASSWORD PHRASE CHANGE INVALID - reason (see page 264)
  - TSS9198I—Inactive interval exceeds max value and was set to 999 days (see page 435)
  - TSS9998I—TSF BUFFER FULL - WRITE TO CHORUS ENDED NO RECORD SENT TO TSF - BUFFER FULL (see page 552)

Contents

Chapter 1: TSS Messages 9

TSS0100 to TSS0199 9
TSS0200E to TSS0299E 10
TSS0300I to TSS0399E 46
TSS0400E to TSS0599E 75
TSS0600E to TSS0965E 108
TSS1000E to TSS1628E 118
TSS2000I to TSS2069E 193
TSS5587E to TSS5858E 203
TSS6000I to TSS6099I 204
TSS6100E to TSS6301I 238
TSS7000I to TSS7054I 250
TSS7100E to TSS7199A 259
TSS7200E to TSS7299I 283
TSS7450I to TSS7802I 300
TSS8001E to TSS8085E 304
TSS8110I to TSS8199E 315
TSS8324E to TSS8399I 334
TSS8400I to TSS8601A 353
TSS8700E to TSS8860E 357
TSS9000I to TSS9099I 366
TSS9101W to TSS9198I 401
TSS9203I to TSS9301I 435
TSS9400E to TSS9499I 454
TSS9500I to TSS9599E 464
TSS9601E to TSS9692E 487
TSS9700E to TSS9769E 494
TSS9800E to TSS9999E 513
TSSC001E to TSSC105I 553

Chapter 2: Messages for SAF SECTRACE Reporter 563

TSS41022 to TSS9C000 563

Chapter 3: CAS20 – CAS4 Messages 573

CAS20 System Authorization Facility (SAF) Messages 573
    Security Initialization Routine 575

CAS21 SECTRACE Routine....601
CAS22 SAF Common Service Routines....635
CAS23 LDS Journal Messages....671
CAS23 SAF HFS Security....679
CAS24 R_cacheserv SAF Callable Service....687
SAFCRINT....695
SAFCRENC....696
SAFCRMAN....702
CAS25 z/OS USS Logging Report and Statistics Gathering Report....704
CAS3 Common Record-Level Protection Routines....712
CAS40 PDS Member-Level Protection Messages....775
Diagnostic Messages....784
CAS41 Compliance Information Analysis Report Messages....789

Chapter 4: TSSPAN Administration Panel Messages 799

Chapter 5: CIA Unload Utility Messages 803

Chapter 6: Detailed Reason Codes 815

Reserved DRCs....815
Conventions....816
Detailed Reason: Codes....816
DRC To Message Cross-Reference....857

Chapter 7: CASECCFS Codes 865

Codes....865

Chapter 8: CIA0101E - CIA0199E Messages 869

CIA0101E CIA Real-Time Initialization Routines....869
CIA0201E - CIA0249E Messages....871
CIA0300I CIA Processing Component Messages....891
CIA0400 Series Messages....911
CIA0500 Series Messages....931
CIA0800 Series Messages....934
CIA0900 Series Messages....944

Chapter 9: Abend Codes 947

TSSMNGR4 (TSS Address Space) ABEND Codes....947

TSSPROT ABEND Codes 951
TSSMAINT ABEND Codes 951
TSSCNV43 ABEND Codes 952
TSSUTIL ABEND Codes 959
TSSRECVR ABEND Codes 960
TSSTRACK ABEND Codes 960
TSSAUDIT ABEND Codes 961
TSSCHART ABEND Codes 961
TSSXTEND Abend Codes 962
TSSFAR ABEND Codes 964
TSSENQ ABEND Code 965
CICS Abend Codes 965
CA C Runtime ABEND Code 967

Chapter 1: TSS Messages

CA Top Secret violation and warning messages appear only if the LOG/MSG Control Option is in effect.

TSS0100 to TSS0199

TSS0130E

Cannot use new password with password phrase logon

Reason:

A user has tried to log on with a password phrase and replace it with a new password. A password phrase can be replaced with a new password phase only.

Action:

Retry the log on using correct syntax.

TSS0131E

Cannot use new password phase with password logon

Reason:

A user has tried to log on with a password and replace it with a password phrase. A password can be replaced with a password only.

Action:

Retry the log on using correct syntax.

TSS0163I

Password phrase Will Expire on mm/dd/yy

Reason:

The current password phrase is nearing the date it will expire on.

Action:

Reset the password phrase before the specified date.

TSS0164I

Password phrase use is disabled

Reason:

A user has tried to log on with a password phrase but this feature is not enabled in the control file.

Action:

Retry the log on using a password instead of a password phrase.

TSS0200E to TSS0299E

TSS0200E

TSS COMMAND ENVIRONMENT ERROR

Reason:

The TSS command cannot be initiated due to an MVS environment error. Two common reasons for an MVS environment error are insufficient storage for the LOAD under TSO and the TSS command is contained in a non-APF authorized step library.

Action:

You should increase your TSO logon region size and ensure that the CA Top Secret load library is in the APF list (parmlib member IEAAPFnn). If a steplib is used, ensure that all other data sets included in the steplib concatenation are also APF authorized.

TSS0201E

CA TOP SECRET IS NOT ACTIVE

Reason:

TSS commands cannot be processed if the CA Top Secret address space is inactive.

Action:

Determine why the CA Top Secret address space has not been initialized. To start CA Top Secret, use the START TSS command.

TSS0202E

YOU ARE NOT AUTHORIZED TO USE THE TSS COMMAND

Reason:

An undefined user attempted to issue a TSS command.

Action:

No action required.

TSS0203E

YOU ARE NOT AUTHORIZED FOR THIS TSS FUNCTION

Reason:

You do not have authority to use the entered CA Top Secret function.

Another possible reason for this message is with the use of an invalid parameter on the create statement as when a DCA or VCA incorrectly specifies the Department or Division on the create statement.

Action:

No action required.

TSS0204E

FUNCTION KEYWORD MISSING OR INVALID

Reason:

An invalid function was entered for a TSS command.

Action:

See the *Command Functions Guide*.

TSS0204I

CREATE,DELETE,ADD,REPLACE,RENAME,REMOVE,PERMIT,REVOKE,WHOOWNS, WHOHAS,HELP,LIST,LOCK,UNLOCK,WHOAMI,MODIFY,ADMIN,DEADMIN,MOVE

Reason:

The TSS HELP command was issued. A list of valid TSS HELP keywords was provided.

Action:

For a complete explanation of the functions, see the *Command Functions* Guide.

TSS0205E

YOU DO NOT YOURSELF HAVE THIS AUTHORITY

Reason:

An administrator must possess an authority before he can grant/remove that authority to/from another user.

Action:

No action required.

TSS0206E

TYPE = function

Reason:

Displays the function for which a user does not have authority.

Action:

No action required.

TSS0207E

INSUFFICIENT AUTHORITY FOR FUNCTION

Reason:

The user does not have authority to use the entered function.

Action:

No action required.

TSS0208E

TYPE = function, AUTHORITY = authority

Reason:

Displays the specific function and the authority level at which the user is not authorized. See message TSS0207E. You should note that authority to administer a specific resource class overrides authority to administer the general RESOURCE class.

Action:

No action required.

TSS0209E

ERROR ATTEMPTING TO PROMPT

Reason:

CA Top Secret was unable to perform a terminal prompt.

Action:

Check the TSO profile to be sure that it is set to PROMPT and not NOPROMPT. If the problem still exists, contact CA Technical Support.

TSS0210E

INVALID ACCESS KEYWORD

Reason:

An unrecognizable ACCESS level was specified, or the specified ACCESS level is not valid for the resource type.

Action:

For the correct access levels, see the ACCESS keyword in the *Command* Functions *Guide*.

For installation-defined resources, the ACCESS level must match one of the ACLST levels listed in the TSS ADDTO(RDT) command that added the resource.

TSS0211E

ACCESSOR-ID MISSING OR INVALID

Reason:

An CA Top Secret function was specified without the ACID operand.

Action:

Reenter the function in the correct format.

TSS0212E

INVALID DATA LIST KEYWORD

Reason:

An invalid option was specified for the DATA keyword of the LIST function.

Action:

Reenter the LIST function using a valid DATA keyword.

TSS0213E

INVALID DAYS KEYWORD

Reason:

An invalid option was specified for the DAYS or CALENDAR keyword of the PERMIT function.

Cannot specify both DAYS and CALENDER on a PERMIT function.

Action:

Reenter the PERMIT function using a valid DAYS keyword.

TSS0214E

INVALID DATASET NAME/PREFIX

Reason:

A data set or data set prefix was incorrectly specified. The:

- Incorrect data set masking (valid only for PERMIT & REVOKE) was used,
- Entry contains invalid characters,
- Entry is too short, or
- LIBRARY keyword is not specified correctly.

Action:

Correct the data set format and reenter the request.

TSS0215E

INVALID EXPIRATION

Reason:

The expiration date in a FOR or UNTIL keyword parameter is incorrect. Both FOR and UNTIL were specified for a single ACID or resource, or an incorrect keyword was used with an ADD or REMOVE of SUSPEND.

Action:

Enter the date in the format specified by the DATE control option, or use the appropriate SUSPEND or SUSPEND FOR/UNTIL keywords.

TSS0216E

FACILITY KEYWORD MISSING OR INVALID

Reason:

An invalid facility name was specified for the FACILITY keyword. There are three other possible reasons:

FACILITY keyword of the COMMANDS or XCOMMANDS function is missing or invalid, or,

The MASTFAC value is incorrect, or,

The Facility parameter of the LOCKTIME or SITRAN keywords is incorrect.

Action:

Determine if the facility was specified correctly. If it was, ensure the facility is properly defined to CA Top Secret (see the Implementation guides).

TSS0217E

INVALID FOR KEYWORD DAYS COUNT

Reason:

The number of days specified by the FOR keyword exceeds the maximum of 255 days.

Action:

Correct the number of days and reenter the command.

TSS0218E

INVALID LCF COMMAND

Reason:

A command or transaction specified on the COMMANDS or XCOMMANDS function contains more than 8 characters or invalid characters.

Action:

Correct the command or transaction specification and reenter the function.

TSS0219E

DATASET MASKING NOT ALLOWED FOR LIBRARIES

Reason:

Data set masking cannot be used in the LIBRARIES keyword to specify program libraries. However, full data set names can be specified by entering them in quotation marks.

Action:

You may specify full data set names by entering them in quotation marks.

TSS0220E

INVALID ACTION KEYWORD

Reason:

One of the following has occurred:

The type of ACTION selected in your command is invalid. For a corrective action, see number 1 below.

2. The type of ACTION selected in your command cannot be used with this resource. For a corrective action, see number 2 below.

Action:

1. Assure that the ACTION in your command is valid. For details, see "PERMIT/REVOKE" in the *Command Functions Guide*.

2. Assure that the ACTION selected is compatible with the resource. For example, ACTION(REVERIFY) can only be used with OTRAN.

TSS0221E

OWNER'S NAME REQUIRED.

Reason:

When creating an ACID, you did not enter the NAME keyword. The NAME keyword is used for identification and reporting and must be entered when using the CREATE function.

Action:

Reenter the TSS CREATE command including the NAME keyword parameter.

TSS0222E

RESOURCE LENGTH INVALID FOR FUNCTION

Reason:

A prefix resource longer than 26 bytes, or a general resource longer than 8 bytes was specified for the ADDTO, REMOVE, or WHOOWNS functions. Longer resources are only valid for PERMIT, REVOKE, and WHOHAS functions.

Action:

Correct the resource name and reenter the function command.

TSS0223E

PROFILE CANNOT HAVE PROFILES

Reason:

Users can be defined to as many as 254 Profiles. Profiles, however, cannot be added to other Profiles.

Action:

See the explanation of a PROFILE in the *User Guide*.

TSS0224E

PASSWORD KEYWORD REQUIRED

Reason:

The PASSWORD keyword was not specified for a CREATE of a new ACID, or the ADDTO of a facility for an ACID having multiple passwords.

Action:

Reenter the command including the PASSWORD parameter.

TSS0225E

TSO TEST COMMAND INVALID FOR "COMMAND" LIST

Reason:

When restricting an ACID to execute only certain TSO commands, you cannot specify the TEST command. With the TEST command, ACIDs can invoke commands that are normally unavailable to them.

Action:

Remove TEST from the list and reenter the function command.

TSS0226E

REQUEST FAILED BY INSTALLATION EXIT

Reason:

An installation exit written by your own installation has failed the request.

Action:

Contact your Central Security Group to determine the function of the exit.

TSS0227E

INVALID VOLUME SERIAL

Reason:

The volume specification either:

- Contains less than 2 characters,
- Contains more than 6 characters, or
- Contains invalid characters.

Action:

Correct the volume serial specification and reenter the function.

TSS0228E

INVALID VOLUME ATTRIBUTES

Reason:

The attributes of a volume are incorrectly specified. Typical causes are invalid attribute combinations, such as both D (DASD) and T (TAPE) being specified.

Action:

See the *Command Functions Guide* for the correct format of specifying VOLUME attributes.

TSS0229E

INVALID TIMES VALUES

Reason:

The TIMES or TIMEREC keyword contains invalid hour specifications. The hours of permitted access to a resource must be represented as two numerical values from 00 to 24. Both the starting and the ending hours must be entered.

Cannot specify both TIMES and TIMEREC on a PERMIT function

Action:

See the TSS PERMIT command function in the *Command Functions Guide* for the correct TIMES format, and re-issue the command.

TSS0230E

AT LEAST 1 RESOURCE OR FACILITY KEYWORD REQUIRED

Reason:

The PERMIT, REVOKE, WHOOWNS or WHOHAS functions require that a resource keyword--that is, VOLUMES or PROGRAMS--is specified.

Action:

See the appropriate chapter in the *Command Functions Guide* for the correct resource or facility, and re-issue the command.

TSS0231E

ONLY 1 RESOURCE OR FACILITY MAY BE SPECIFIED

Reason:

The WHOOWNS or WHOHAS function was specified with more than one resource.

Action:

Reenter the function, specifying one resource at a time.

TSS0232E

PROCNAME MISSING FOR 'STC' FACILITY

Reason:

When modifying the Started Task table, you did not supply the PROCNAME.

Action:

Reenter the TSS ADDTO/REMOVE(STC) specifying the PROCNAME keyword.

TSS0233E

INVALID CICS SCTYKEY

Reason:

A CICS security key greater than 64 was specified. Valid security keys are 0-64.

Action:

Enter a valid key.

TSS0234E

INVALID TIME ZONE

Reason:

An invalid time zone displacement was specified. Valid time zones are -12 to 12.

Action:

See the *Command Functions Guide* for a complete explanation of the TZONE keyword parameter (used with the ADDTO or CREATE function).

TSS0235E

INVALID CICS OPCLASS

Reason:

A CICS operator class greater than 24 was specified. Valid classes are 0-24.

Action:

Enter a valid class.

TSS0236E

INVALID CICS OPPRTY

Reason:

A CICS operator priority greater than 255 was specified. Valid priority is 0-255.

Action:

Enter the proper priority.

TSS0237E

INVALID LOCK TIME TERMINAL

Reason:

A terminal lock time greater than 120 minutes was specified. Valid lock times are 0-120 minutes.

Action:

Reenter the terminal lock time with a valid minute specification.

TSS0238E

USER CLASS NAME MISSING OR INVALID

Reason:

An invalid user class was specified for UR1 or UR2. The user class must be a single character or digit.

Action:

See the *Command Functions Guide* for a complete description of UR1 and UR2.

TSS0239E

INVALID or MISSING ADMINISTRATION AUTHORITY

Reason:

A specified administration authority is invalid or unknown.

Action:

See the *Command Functions Guide* for valid ADMIN/DEADMIN authorities.

TSS0240E

INVALID RESOURCE NAME

Reason:

A resource name or resource name prefix was incorrectly specified. Either masking was used incorrectly, the entry contained invalid characters, the entry was too short, or the minimum match length exceeded the MAXPERMIT(...) setting for the resource class.

Action:

Specify the resource name such that:

- It has a minimum length of 2 characters
- The minimum match length does not exceed the MAXPERMIT(...) setting for the resource class.
- Masking characters are used correctly. For information, see the *User Guide*.

TSS0241E

INVALID DIAGNOSE RESOURCE

Reason:

An invalid diagnose response was specified. Valid diagnose resources are hexadecimal values ranging from 0 to FFFF.

Action:

No action required.

TSS0242E

UNKNOWN KEYWORD

Reason:

The command processor could not recognize the entered keyword

Action:

Reenter the TSS command, using the correct spelling of the keyword.

TSS0243E

INVALID SUBFIELD DATA

Reason:

The format of the subfield did not conform to the format as required by the keyword.

Action:

Reenter the TSS command, using correct subfield format

TSS0244E

INVALID SUBFIELD LENGTH FOR KEYWORD - xxxxxxxx

Reason:

The contents of a subfield of the keyword exceed the maximum length permitted for that keyword. In the case of a resource class, the maximum length is determined by the MAXPERMIT(...) setting for the resource class, except where the resource class has the ATTR(MASK) attribute, in which case the maximum length is forced to 255 characters.

Action:

Reenter the TSS command, specifying an appropriate subfield length.

TSS0245E

INVALID INTEGER VALUE

Reason:

The text of the subfield was not 0-9 characters.

Action:

Reenter the TSS command, using integer characters.

TSS0246E

SUBFIELD CONTAINS INVALID CHARACTER(S)

Reason:

The text of the subfield as required by the keyword should have been one of the following but was not:

- ALPHABETIC
- ALPHANUMERICS
- NUMERIC

Action:

Reenter the TSS command, using the characters required by the keyword.

TSS0247E

DUPLICATE KEYWORD SPECIFICATION

Reason:

The same keyword was entered more than once.

Action:

Reenter the TSS command, using each keyword only once.

TSS0248E

REQUIRED SUBFIELD MISSING FOR KEYWORD keyword

Reason:

You need a subfield for this keyword.

Action:

Reenter the TSS command, with the appropriate subfield.

TSS0249E

STATEMENT CONTAINS UNBALANCED PARENTHESIS

Reason:

The TSS command is missing one of its parentheses.

Action:

Reenter the TSS command, including both parentheses.

TSS0250E

INVALID HEX VALUE

Reason:

The text of the subfield was not 0-9 or A-F characters.

Action:

Reenter the TSS command, using valid hex characters.

TSS0251E

KEYWORD <keyword> DOES NOT SUPPORT SUBFIELDS

Reason:

A subfield was entered for a keyword that does not require a subfield.

Action:

Reenter the TSS command, using valid syntax.

TSS0252E

KEYWORD NOT DISCERNIBLE keyword

Reason:

An abbreviated form of a keyword was specified, however, it was too short to identify one full keyword name. For example, if you use “PA” as a password, TSS cannot discern whether it stands for PAssword or PAnel.

Action:

Reenter the TSS command using a valid keyword.

TSS0253E

NOTHING TO REFRESH. ACID/JOBNAME NOT FOUND.

Reason:

While attempting to execute a REFRESH command, one of the following has been sensed:

- There has been no change to the ACID in the REFRESH command, so there is nothing to refresh.
- There is no active address space where the ACID of the REFRESH is active which matches the JOBNAME operand specified. This is an informational message.

Action:

Assure that changes to the ACID have been completed before issuing the REFRESH command. Assure that the ACID and JOBNAME specified in the command are correctly spelled.

TSS0254I

REFRESH ALREADY IN PROGRESS. RETRY LATER.

Reason:

A previously issued TSS REFRESH command for this ACID has not yet completed processing.

Action:

Allow previous command to complete before re-issuing the command.

TSS0255I

JOBNAME xxxxxxxx LOGICALLY SWAPPED. REFRESH NOT POSSIBLE. TRY LATER.

Reason:

While attempting to execute a REFRESH command, a job or system task was encountered in a logically swapped out state. This condition prevents CA Top Secret from determining whether the ACID of the REFRESH was present in the job, and prevents refresh of ACIDs where the condition is sensed. Processing continues to refresh ACIDs in address spaces relevant to and accessible by the command process.

Action:

The user must determine whether the jobname “xxxxxxxx” is relevant to the REFRESH command issued. If the jobname is not relevant, no further action is required. If the jobname is relevant, the job needs to be swapped into active memory before the command can be repeated successfully for that job.

TSS0256E

INVALID SUBFIELD LENGTH FOR KEYWORD - PROFINTERVAL

Reason:

The PROFINTERVAL value is not within the supported range.

Action:

Correct the interval value and retry.

TSS0257E

PRIVPGM INVALID FOR THIS RESOURCE CLASS

Reason:

PRIVPGM was entered as a keyword on a TSS PERMIT command and PRIVPGM is not valid for the resource class being permitted.

Action:

Remove the PRIVPGM keyword from the PERMIT or if it is a user-defined resource class, add the PRIVPGM attribute to the RDT entry for resource class and reissue TSS PERMIT.

TSS0258E

MISSING OR INVALID LINKID VALUE

Reason:

The linkid value specified was missing or invalid.

Action:

Correct the linkid specified.

TSS0259E

INVALID CONVSEC VALUE

Reason:

An incorrect value was specified for Conversation Security

Action:

Specify a maximum of eight characters.

TSS0260E

INVALID INTERVAL VALUE

Reason:

An incorrect or too high of a value was specified.

Action:

Specify a value that does not exceed 99999.

TSS0261E

MORE THAN 5 ACIDS

Reason:

A maximum of 5 acids can be specified in a single TSS command; however, the TSS command can be repeated an unlimited amount of times.

Action:

Reenter the TSS command, specifying 5 or less acids per command entry.

TSS0262E

ACID IS ASUSPENDED

Reason:

A TSS REMOVE(SUSPEND) command was issued for an ACID that was administratively suspended.

Action:

Issue the TSS REMOVE(ASUSPEND) command.

TSS0263E

MORE THAN 8 DATASETS OR LIBRARIES

Reason:

A maximum of 8 data sets or libraries can be specified in a single TSS command; however, the TSS command can be repeated an unlimited amount of times.

Action:

Reenter the TSS command specifying 8 or less data sets or libraries per command entry.

TSS0264E

MORE THAN 30 ENTRIES IN LIST

Reason:

A maximum of 30 commands can be specified in a LCF list of a single TSS command; however, the TSS command can be repeated an unlimited amount of times.

Action:

Reenter the TSS command, specifying 30 or less commands in the LCF list per command entry.

TSS0265E

LDAP NODE NAME NOT DEFINED IN *NDT*

Reason:

The LDAPDEST field contained an undefined LDAPNODE name.

Action:

Ensure all LDAPDEST names are defined as LDAPNODE's on the NDT.

TSS0266E

MORE THAN 8 PRIVILEGED PROGRAMS

Reason:

A maximum of 8 privileged programs can be specified in a single TSS command; however, the command can be repeated an unlimited amount of times.

Action:

Reenter the TSS command, specifying 8 or less privileged programs per command entry.

TSS0267E

MORE THAN 5 PROFILES

Reason:

A maximum of 5 profiles can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 5 or less profiles per command entry.

TSS0269E

MORE THAN 30 VOLUMES

Reason:

A maximum of 30 volumes can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 30 or less volumes per command entry.

TSS0270E

MORE THAN 5 SYSIDs

Reason:

A maximum of 5 SYSIDs can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 5 or less SYSIDs per command entry.

TSS0271E

MORE THAN 5 JOB SOURCES

Reason:

A maximum of 5 job sources can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 5 or less job sources per command entry.

TSS0272E

MORE THAN 5 USER DATA ELEMENTS

Reason:

A maximum of 5 user data elements can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 5 or less user data elements per command entry.

TSS0273E

MORE THAN 5 RESOURCE ELEMENTS

Reason:

A maximum of 5 resource elements can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 5 or less resource elements per command entry.

TSS0274E

MORE THAN 8 MISC1 AUTHORITIES

Reason:

A maximum of 8 MISC1 AUTHORITIES can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 8 or less MISC1 AUTHORITIES per command entry.

TSS0275E

MORE THAN 8 MISC9 AUTHORITIES

Reason:

A maximum of 8 MISC9 AUTHORITIES can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 8 or less MISC9 AUTHORITIES per command entry.

TSS0276E

MORE THAN 8 RESOURCE AUTHORITIES

Reason:

A maximum of 8 resource authorities can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command specifying 8 or less resource authorities per command entry.

TSS0277E

MORE THAN 8 MINIDISKS

Reason:

A maximum of 8 minidisks can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action:

Reenter the TSS command, specifying 8 or less minidisks per command entry.

TSS0278E

MORE THAN 20 ACCESS LEVELS

Reason:

You exceeded the 20-access-level limit for this resource.

Action:

Reenter the TSS command, specifying 20 or fewer access levels.

TSS0279E

RESCLASS MISSING, INVALID, OR RESERVED

Reason:

A TSS RDT command was entered and the RESCLASS parameter was missing, more than 8 characters, or already being used in the RDT record.

When adding a new RESCLASS name, be sure that it does not match the first four characters of any existing resource class name.

Action:

Reenter the TSS command, using a valid resource class.

TSS0280E

RESCODE MISSING, INVALID, OR RESERVED

Reason:

- In CA Top Secret 5.2, RESCODE is not required: CA Top Secret will assign the next unused value eligible for user assignment. If all available RESCODE values have already been assigned, this message indicates that the only available RESCODE values are reserved for CA Top Secret system defined resources.
- You have entered a hexadecimal value for RESCODE which contains:

  more than 3 hexadecimal digits (nibbles)

  an invalid character for a hexadecimal number

  a hexadecimal value which is ineligible for a user-defined resource

Action:

- If all eligible user RESCODE values have been exhausted, you will have to determine if assigned user RESCLASSes are all actively being used. If you find a RESCLASS that can be deleted, you will have to revoke existing permissions and remove existing ownership relations for the related resources. Such a resource may then be removed from the RDT, and its associated RESCODE will be available for the new resource class you require.
- If an invalid RESCODE value has been supplied, re-enter the command with a valid RESCODE value. The available values of RESCODE eligible for user assignment are:

  001 - 03F (RIE)

  101 - 13F (PIE)

  101 - 13F (PIE)

For an explanation of the differences between RIE and PIE resource classes, see the *User Guide*.

TSS0281E

INVALID ACLST/DEFACC VALUE

Reason:

A TSS RDT command was entered with the ACLST and/or DEFACC parameter that was formatted incorrectly. One of the following caused the error:

- The access level name was greater than 8.
- The access level name was entered without a hex value and that name did not match one of the system-supplied access level names.
- More than 4 characters were entered as a hex value.
- Non-hex characters were entered as an access level.
- The hex value was entered in parenthesis.

Action:

Reenter the TSS command with a valid ACLST or DEFACC. The format of elements must be acclvlnm=hhhh or acclvlnm, where acclvlnm equals a one to eight access level name consisting of alphanumeric or national characters and hhhh equals a one to four hexadecimal access level mask. Entries formatted as acclvlnm(hhhh) are not acceptable. For further details see the *Command* Functions *Guide*.

TSS0282E

DEFACC ENTRY MUST MATCH ACLST ENTRY

Reason:

The TSS RDT command you entered had an ACLST and/or DEFACC parameter. One of the following caused the error:

- If ACLST and DEFACC were entered, the name and hex value of DEFACC does not match an ACLST entry.
- If only ACLST was entered, none of the ACLST hex values match the DEFACC in the RDT.
- If only DEFACC was entered, its hex value does not match any of the ACLST values in the RDT.

Action:

Reenter the TSS command with a valid ACLST/DEFACC.

TSS0283E

RESOURCE OWNED WITHIN RESCLASS, CANNOT BE REMOVED

Reason:

A TSS REMOVE(RDT) command was entered but resources had been defined under the RESCLASS to be removed.

Action:

Determine what resources are owned under this RESCLASS by issuing TSS WHOOWNS resclass(*), removing ownership, and reentering the TSS REMOVE(RDT) command.

TSS0284E

ONLY 'ATTR(EXIT,DEFPROT,MERGE,ALLMERGE,GENERIC,MASK)' VALID WHEN UPDATING A STATIC RDT ENTRY

Reason:

Only the specified attributes may be modified for a system defined (static) RDT entry.

Action:

If you truly must alter an attribute (other than in the message) for a static RDT entry, you will have to contact support. To otherwise alter the behavior for a system-defined resource, consider modifying the installation exit (TSSINSTX) at the RESOURCE entry point; modify the RDT entry so that the EXIT attribute is activated.

TSS0285E

INVALID PRIVPGM NAME

Reason:

A TSS command was entered with the PRIVPGM keyword but the PRIVPGM name had more than 8 characters or an '(' was entered but not followed by 'G)' for GENERIC. Example: PRIVPGM(G) is correct.

Action:

Reenter the TSS command, using a valid PRIVPGM.

TSS0286E

INVALID VMUSER NAME

Reason:

A TSS command was entered with the VMUSER keyword, but the VMUSER name had more than 8 characters or an '(' that was not followed by a 'G)' for generic. Example: PGM(G) is correct.

Action:

Reenter the TSS command, using a valid VMUSER.

TSS0287E

ACTION DENY IS INVALID; RESOURCE HAS ACCESS LEVEL

Reason:

You entered a TSS PERMIT ACTION(DENY) but the resource supports the ACCESS keyword.

Action:

To prohibit the use of a resource which supports access levels, ACCESS(NONE) should be used.

TSS0288E

MORE THAN 30 RESOURCE CLASSES

Reason:

You entered a TSS LIST(RDT) RESCL() command, but the RESCLASS keyword had more than 30 classes in the list.

Action:

Reenter the TSS command, specifying 30 or fewer RESCLASSes.

TSS0289E

INVALID TERMINAL OR OPERATOR ID CARD

Reason:

The OIDCARD keyword was specified, but either the terminal from which the command was entered does not have an operator id card reader, or either VTAM or TCAM encountered a permanent I/O error while reading the operator id card. Note that this keyword may not be specified if the TSS command is being used in batch.

Action:

No action required.

TSS0291E

FUNCTION INVALID IN THIS ENVIRONMENT

Reason:

The LOCK, UNLOCK, and WHOAMI functions are not valid from the console.

Action:

No action required.

TSS0292E

TSS COMMAND ABENDED PROCESSING THIS REQUEST

Reason:

The TSS command subtask abended while processing your request.

Action:

Notify your system support staff.

TSS0293E

INVALID VALUE FOR KEYWORD cccccccc

Reason:

The value of the keyword shown is incorrect.

Action:

See the *Command Functions Guide* for acceptable value(s).

TSS0294E

MORE THAN nn xxxxxxxxxx

Reason:

The keyword shown only accepts nn operands

Action:

Reenter the command with no more than nn operands. You may enter the command more than once, if needed.

TSS0295E

INVALID MAXLEN VALUE OR FIELD ENTERED IS TOO LONG

Reason:

If ADDTO/REPLACE to RDT: The value entered for MAXLEN in ADD(RDT) must be in the range 1 to 255.

For RIE resource class, MAXLEN must be at least 1.

For PIE resource class, MAXLEN must be at least 2.

For further explanation of the RIE and PIE types of resource classes, see the *User Guide*.

The MAXLEN keyword cannot be used with REPLACE(RDT).

If ADDTO/REPLACE to FDT: The value entered for MAXLEN must be in the range 1 to 32767. The total of all MAXLENs dynamically added to the FDT must not exceed 32767.

If ADDTO/REPLACE to ACID: The user has attempted to add or replace the value for a field whose FDTNAME MAXLEN has been exceeded.

Action:

If ADDTO to RDT: Replace the value of MAXLEN with a valid value.

IF REPLACE to RDT: Reenter the command without the MAXLEN keyword.

If ADDTO/REPLACE to FDT: If the total of all dynamically defined FDTNAME entries has exceeded 32767, determine if all fields are still actively being used. Remove any unused field values from associated ACIDs. Then remove the associated FDTNAME from FDT. After removing unused fields from the FDT, reattempt the ADDTO or REPLACE command with the new FDTNAME entry. Otherwise, replace the value of MAXLEN with a valid value.

If ADDTO/REPLACE to ACID: Reattempt to add a smaller field which does not exceed the associated FDTNAME MAXLEN. If possible replace the MAXLEN parameter in the associated FDTNAME to accommodate the larger field requirements. Then reattempt to add a value for the field which does not exceed the new MAXLEN.

TSS0296E

RESERVED SEGMENT NAME

Reason:

When adding or changing the SEGMENT associated with an FDT entry the given segment name is reserved by the system.

Action:

Chose another SEGMENT name and re-enter the command.

TSS0297A

SPECIFY YOUR PASSWORD

Reason:

Your signon password is required to perform the service you have requested, typically to unlock a terminal.

Action:

Type your signon password. Press the ENTER key.

TSS0297E

SCOPE ACID MUST BE TYPE LSCA OR ZONE

Reason:

An attempt was made to assign a scope to an LSCA and one or more of the ACIDs identified in the SCOPE keyword was not a ZONE or an LSCA.

Action:

Reenter the command using a valid ZONE or LSCA in the SCOPE keyword.

TSS0298A

INSERT OPERATOR ID CARD

Reason:

TSS must read the data from the OIDCARD for later verification when the ACID attempts to sign on to a facility.

Action:

Insert the ACID's operator ID card into the reader.

TSS0298E

RECURSIVE SCOPING ATTEMPTED

Reason:

An attempt was made to give scope of ACID1 to ACID2, but ACID2 already has scope over ACID1.

Action:

No action required.

TSS0299E

keyword KEYWORD ILLEGAL FOR FUNCTION

Reason:

The named keyword is invalid for the entered function.

Action:

For a list of valid function keywords enter: TSS HELP

TSS0300I to TSS0399E

TSS0300I

TSS function FUNCTION SUCCESSFUL

Reason:

The listed CA Top Secret function has successfully completed.

Action:

No action required.

TSS0301I

TSS function FUNCTION FAILED, RETURN CODE = XX

Reason:

The listed CA Top Secret function has failed. This message will always be preceded by a detailed message explaining the reason for the failure. The following codes and messages apply:

- **4** Syntax error, such as invalid access
- **8** Functional error, such as data set not found
- **16** Unexpected error occurred, message TSS0390E will also display

Action:

No action required.

TSS0302I

***WARNING* THIS ACCESSOR-ID RECORD IS DAMAGED**

Reason:

The TSS command attempted to modify a security record and found that it contained invalid data.

Action:

Contact CA Technical Support.

TSS0303I

AcidName(xxxxxxxx) Type(xxxx) Mode(xxxx) Facility(xxxxxxxx) Terminal(xxxxxxxx) SystemID(xxxxxxxx) Log(xxx) INSTDATA(xxxxxxxx) BYPASSING(xxxxx)

Reason:

This message displays information about an ACID in response to a TSS WHOAMI command.

Action:

Informational message, no action necessary.

TSS0305E

FDTNAME MISSING, INVALID, OR RESERVED

Reason:

A TSS FDT command was entered and the FDTNAME parameter was missing, more than 8 characters, or already being used in the FDT record.

Action:

Reenter the TSS command, using a valid field name.

TSS0306E

FDTCODE IS NOT DEFINED

Reason:

The FDTCODE specified in the TSS command is not defined in the Field Descriptor Table (FDT).

Action:

Reenter the TSS command, specifying a valid FDTCODE.

TSS0307E

FDTCODE MISSING, INVALID, OR RESERVED

Reason:

The TSS ADDTO(FDT) command that you just entered was invalid. Possible causes include: a missing FDTCODE, an FDTCODE with more than 2 characters, invalid hex characters, or the FDTCODE has already been used.

Action:

Reenter the TSS command, using a valid FDTCODE.

TSS0308E

ONLY USER DEFINED FDT ENTRIES CAN BE UPDATED

Reason:

The field name in your TSS REPLACE(FDT) command represents a system supplied field. No attributes of system-supplied fields may be modified dynamically.

Action:

If changes are required to a system supplied field, contact CA Top Secret Support. If additional user-supplied information is required, consider defining your own user-defined field in the FDT (which you can manipulate and extract separately.)

TSS0310E

DATASET/PREFIX SECURITY FILE SEGMENT IS FULL

Reason:

No new data sets or data set prefixes can be created until the Security File is extended.

Action:

To extend the Security File, use the CA Top Secret utility, TSSXTEND.

TSS0311E

VOLUME SECURITY FILE SEGMENT IS FULL

Reason:

No new volumes or volume prefixes can be added until the Security File is extended.

Action:

To extend the Security File, use the CA Top Secret utility, TSSXTEND.

TSS0312E

ACCESSOR-ID SECURITY FILE SEGMENT IS FULL

Reason:

No new ACID's can be created until the Security File is enlarged.

Action:

To extend the Security File, use the CA Top Secret utility TSSXTEND.

TSS0313E

PERMANENT I/O ERROR UPDATING THE SECURITY FILE

Reason:

A permanent hardware I/O error was encountered by CA Top Secret while updating the Security File. The system console operator will be informed of the problem.

Action:

When the Security File becomes available, verify the results of the last entered command. If the problem is not hardware related, contact CA Technical Support.

TSS0314E

ACID DOES NOT EXIST

Reason:

The ACID specified on a function or in the ACID keyword has not been CREATED.

Action:

Create a new ACID or specify an existing one.

TSS0315E

ACID ALREADY EXISTS

Reason:

The ACID being CREATED already exists in the Security File.

Action:

If you wish to create an ACID other than the existing one, you must specify a new acid name.

TSS0316E

VOLUME NOT FOUND IN SECURITY FILE

Reason:

The specified volume has not been ADDed to the Security File.

Action:

Use the TSS ADDTO function if you wish to add the volume to the CA Top Secret Security File. See the *Command Functions Guide* for the correct format of the ADD function.

TSS0317E

DATASET/PREFIX NOT FOUND IN SECURITY FILE

Reason:

The specified data set or data set prefix has not been ADDed to the Security File.

Action:

The data set/prefix must be added to an existing ACID via the TSS ADDTO function.

TSS0318E

RESOURCE NOT FOUND IN SECURITY FILE

Reason:

The specified resource has not been ADDed to the Security File.

Action:

The resource must be added to an existing ACID via the TSS ADDTO function.

TSS0319E

INVALID SPECIFICATION FOR KEYWORD 'keyword'

Reason:

The specified keyword did not contain a valid value for the command entered.

Action:

Reenter command with a valid parameter for the specified keyword.

TSS0320E

SPECIFIED UID/GID ALREADY IN USE BY acid

Reason:

This message indicates an error with the value supplied for the UID, GID or HOMEUID keywords. The supplied value is already in use by another ACID, or the named-ACID already has a value set. Use the TSS LIST command function and list the ACID shown in the message to determine which one of these conditions has caused the error.

Action:

Give this user a different, unique, UID/GID number or remove this number from the listed ACID prior to adding to this ACID.

TSS0321E

INVALID ACID TYPE FOR THIS UID/GID

Reason:

The administrator has tried to add a GID value to a non-TYPE(GROUP) acid or has tried to add a UID value to an ACID that is not a USER, DCA, VCA, ZCA, LSCA, or SCA.

Action:

No action required.

TSS0322E

INVALID KEYWORD WITH THIS ACID TYPE

Reason:

The administrator has attempted to add a resource or field to an ACID that cannot have that information added to it.

Action:

Ensure that the target ACID is the correct one and only add valid information to the ACID.

TSS0323E

RESOURCE SECURITY FILE SEGMENT IS FULL

Reason:

New resources cannot be added to the Security File until the file is enlarged.

Action:

Enlarge the Security File using the TSSXTEND utility.

TSS0324E

ADMINISTRATOR'S ACID DOES NOT EXIST ON TARGET NODE

Reason:

A TSS command has been sent to another node using CPF, but the ACID for the administrator issuing the command does not exist on the remote system.

Action:

You must get your ACID defined on the remote system prior to directing any administration commands to that node.

TSS0325E

BAD RANGE FOR UID/GID

Reason:

One of the following scenarios occurred:

- The low value is greater than the high value.
- The low value is less than 1.
- A RANGE was entered when a value for the UID/GID was also entered on the same command line.

Action:

If you are specifying a number, leave off the keyword range. If not, reenter the command with the range in which the first value is a positive number that is less than the second number.

TSS0326E

UID/GID NOT AVAILABLE IN RANGE

Reason:

One of the following scenarios occurred:

- There were not any UIDs or GIDs available in the table within the range specified on the command line.
- No range was given and there were not any UIDs or GIDs available in the default range.

Action:

Alter the range in the defaults or on the command line and reenter the command.

TSS0327E

KEYSMSTR missing record

Reason:

A command was entered that required the use of a specific record that isn't yet defined on KEYSMSTR.

Action:

Define the missing record on KEYSMSTR. See KEYSMSTR keyword in Command *Functions Guide* for more details.

TSS0329E

DELETE COMMAND INVALID FOR DELEGATE ACID

Reason:

The DELETE command is not valid for the DELEGATE ACID.

Action:

Specify the ADD or MODIFY commands which are valid for the ACID.

TSS0330E

DELETE COMMAND INVALID FOR DATACLAS ACID

Reason:

The DELETE command is not valid for the DATACLAS ACID.

Action:

Specify the ADD or REMOVE commands which are valid for the ACID.

TSS0331E

DELETE COMMAND INVALID FOR SIGVER ACID

Reason:

The DELETE command is not valid for the SIGVER ACID.

Action:

Specify the ADD or REMOVE commands that are valid for the ACID.

TSS0335E

ATTRIBUTE NOT MODIFIABLE FOR THIS FDT ENTRY

Reason:

For FDT fields, CA Top Secret supports pre-defined fields and user-defined fields. Users cannot alter pre-defined fields, except when the attributes NOXTRPRP and XTRPRP are not defined.

This message can display for two reasons:

- You specified the attribute NOXTRPRP or XTRPRP for a pre-defined field that already includes a pre-defined setting for these attributes. If CA has pre-defined this attribute, you cannot alter it.
- You tried to specify attributes for a user-defined field (for example, MIXED, NONDISP) on a pre-defined field.

Action:

For the first case, you cannot change this attribute in this scenario.

For the second case, re-enter the command and specify the correct attributes for a user-defined field.

TSS0336E

CONFLICTING FDT ATTRIBUTES SPECIFIED

Reason:

You specified both NOXTRPRP and XTRPRP attributes. You can only select one of these two attributes.

Action:

If you *do not want* the results of an extract/replace call from this field to be sent to the recovery file and propagated to other systems, choose NOXTRPRP.

If you *want* the results of an extract/replace call from this field to be sent to the recovery file and propagated to other systems, choose XTRPRP.

TSS0340E

DATASET/PREFIX NOT OWNED WITHIN SCOPE

Reason:

The data set or data set prefix specified in an ADDTO request is already owned by an ACID in another department or division.

Action:

To grant an ACID access to the data set/prefix, use the TSS PERMIT function.

TSS0341E

ACID SPECIFIED IS INVALID FOR CROSS-AUTHORIZATION

Reason:

A TSS PERMIT(USERA) ACID(USERB) was issued with USERB as a type PROFILE.

Action:

Reissue the command with one of the following ACID types for USERB: USER, DCA, VCA, ZCA, LSCA, SCA, or MSCA.

TSS0342E

DATASET/PREFIX NOT FOUND IN SECURITY RECORD

Reason:

The data set or data set prefix specified in a REMOVE or REVOKE request was not found in the ACID's Security Record, so it cannot be removed or revoked from that ACID.

Action:

No action required.

TSS0343E

VOLUME IS NOT OWNED WITHIN SCOPE

Reason:

The volume specified in an ADD request is already owned by an ACID in another department or division.

Action:

To grant access to the volume, use the TSS PERMIT function.

TSS0345E

VOLUME NOT FOUND IN SECURITY RECORD

Reason:

The volume specified in a REMOVE or REVOKE request was not found in the ACID's Security Record, so it cannot be removed or revoked from that ACID.

Action:

No action required.

TSS0346E

PROFILE/GROUP NOT FOUND

Reason:

- The profile or group specified in an ADDTO, REMOVE or REVOKE request was not found.
- The group specified in an ADDTO, REPLACE, or REMOVE request for the keyword LNXENTS was not found on the acid.

Action:

No action required.

TSS0347E

NAMED ENTRY NOT FOUND IN RECORD

Reason:

The linkid specified was not found or the entry specified with this linkid was not found.

Action:

Ensure the linkid exists or that the entry is there.

TSS0350E

RESOURCE IS NOT OWNED WITHIN SCOPE

Reason:

The resource you have attempted to administer is already owned by an ACID which is outside your administrative scope.

The resource you have attempted to manipulate can only be administered by MSCA.

Action:

To grant access to the resource, use the TSS PERMIT function.

You must sign on as the MSCA to perform the necessary administration.

TSS0351E

SPECIFY 'UNDERCUT' TO TRANSFER OWNERSHIP

Reason:

An attempt was made to ADDTO a resource to an ACID; however, the resource is already owned.

Action:

If transfer of ownership is intended, you must specify the UNDERCUT keyword with the ADDTO function.

TSS0352E

ACID NOT OWNED WITH SCOPE

Reason:

The ACID whose Security Record you wish to modify is not within your scope of authority.

Action:

Determine the department or division responsible for the ACID Security Record. Notify the responsible Security Administrator.

If the ACID was an SCA or LSCA and the command was ADMIN, DEADMIN, or CREATE only the MSCA has authority over an SCA or LSCA for these functions. Notify the MSCA to issue the command.

TSS0353E

USER ALREADY ATTACHED TO PROFILE/GROUP

Reason:

An attempt was made to ADDTO a PROFILE or GROUP to an ACID that already has a profile or group associated with it.

Action:

No action required.

TSS0354E

INVALID SPECIFICATION OF PROFILE

Reason:

An attempt was made to ADDTO a profile to a department, division, another profile or to a valid ACID that already has that profile.

Action:

Profiles can be added to the following Acid types only: USER, SCA, VCA, DCA. If you are attempting to define a profile, you must use the TSS CREATE function.

TSS0355E

STARTED TASK PROCEDURE NOT FOUND

Reason:

The PROCNAME specified in a REMOVE(STC) request was not found in the Started Task table.

Action:

No action required.

TSS0356E

SECURITY RECORD ENQ/DEQ FAILED

Reason:

Before processing a security record, the TSS command attempts to ENQ on the security record. This ENQ attempt has failed.

Action:

This message is usually an indication of a system-wide problem. Notify your system support staff.

TSS0357E

PROFILE NOT OWNED WITHIN SCOPE

Reason:

A PROFILE which is not within your scope of authority or that is not Globally Administrable (GAP keyword) was specified in an ADDTO request.

Action:

No action required.

TSS0358E

FUNCTION INVALID FOR "ALL" FACILITY

Reason:

An invalid function was specified when administering the "ALL" record.

Action:

No action required.

TSS0359E

STORAGE GETMAIN FAILED

Reason:

Insufficient storage was available for the entered TSS command. Your region size is too small or there is a shortage of common storage.

Action:

Contact CA Technical Support.

TSS0360E

ACCESSOR-ID ALREADY OWNS THE RESOURCE

Reason:

An attempt was made to PERMIT a resource to an ACID; however, the ACID already owns that resource. By definition, the owner ACID already possesses full access to the resource.

Action:

No action required.

TSS0361E

ATTEMPT TO ADD MORE THAN 254 PROFILES TO ACID

Reason:

An ACID can be assigned a maximum of 254 Profiles.

Action:

No action required.

TSS0362E

ACCESSOR-ID IS THE OWNER OF THE RESOURCE

Reason:

Resources that are owned by an ACID cannot be REVOKEd from that ACID.

Action:

To remove the ACID's access to the owned resource, use the REMOVE function.

TSS0363E

DIVISION SPECIFICATION MISSING OR INVALID

Reason:

There are two possible reasons:

The DIVISION keyword specified an invalid DIVISION name.

An attempt was made to CREATE a VCA and the DIVISION keyword was omitted.

Action:

Specify the correct keyword.

TSS0364E

DEPARTMENT SPECIFICATION MISSING OR INVALID

Reason:

There are two possible reasons:

The DEPARTMENT keyword specified an invalid DEPARTMENT name.

An attempt was made to CREATE a DCA and the DEPARTMENT keyword was omitted.

Action:

Specify the correct keyword.

TSS0365E

FUNCTION INVALID FOR “STC” FACILITY

Reason:

An invalid function was specified when administering the STARTED TASK(STC) record. Only ADDTO and REMOVE functions are valid.

Action:

No action required.

TSS0367E

RESOURCE HAS BEEN PERMITTED TO ANOTHER ACID

Reason:

An attempt was made to REMOVE a resource; however, the resource has been permitted to another ACID.

Action:

To successfully execute the REMOVE command, all permissions to the resource must be removed. If this message is received when deleting an acid, enter:

```
TSS WHOHAS ACID(acid)
```

acid

Specifies the acid being deleted.

If the acid is permitted to another acid, revoke the permit.

If the acid is *not* permitted to another acid, determine if the acid owns any resources. Enter:

```
TSS LIST(acid) DATA(RESOURCE)
```

If yes, transfer this ownership to another acid. Enter:

```
TSS ADD(dept) resclass(resname) UNDERCUT
```

TSS0368E

LSCA/ZONE/DIV/DEPT/PROFILE STILL HAS CONNECTED ACIDS

Reason:

An attempt was made to DELETE a Department, Division, Zone or Profile. CA Top Secret has failed the request because there are still ACIDs connected to it.

Action:

Before DELETE can be executed on a Zone, Division Department or Profile record, all ACID assignments/connections must be removed. Use the TSS LIST command to display the ACIDs that are connected.

TSS0369E

ADMIN INVALID FOR ZONE, DIV, DEPT, PROFILE, OR GROUP

Reason:

Administration authority cannot be granted to any ACID other than a user, Administrator, or the “ALL” record.

Action:

No action required.

TSS0370E

OIDCARD DATA NOT FOUND IN SECURITY RECORD

Reason:

The operator id card of an ACID was not found in the Security Record when a REMOVE request was specified.

Action:

No action required.

TSS0371E

LCF COMMAND NOT FOUND IN SECURITY RECORD

Reason:

The command specified in a REMOVE request was not found in the ACID's LCF list.

Action:

No action required.

TSS0372E

FUNCTION INVALID FOR “AUDIT” FACILITY

Reason:

An invalid function was specified for the “AUDIT” facility. The only valid functions are ADDTO and REMOVE.

Action:

No action required.

TSS0374E

ZONE SPECIFICATION MISSING OR INVALID

Reason:

There are two possible reasons for this message:

- The ZONE keyword specified an invalid ZONE name.
- An attempt was made to CREATE a ZCA, and the ZONE keyword was omitted.

Action:

Reenter the command using a valid ZONE ACID.

TSS0375E

PERMITTED ACID NOT FOUND IN SECURITY RECORD

Reason:

The acid specified in the ACID keyword of a REVOKE request was not found in the Security Record.

Action:

No action required.

TSS0376E

PASSWORD INVALID FOR ZONE, DIV, DEPT OR PROFILE

Reason:

A password may only be given to a user or an administrator.

Action:

Reenter the command excluding the PASSWORD parameter.

TSS0377E

ADMIN AUTHORITY NOT FOUND IN SECURITY RECORD

Reason:

The administration authority specified in a DEADMIN request did not exist.

During a CREATE(acid) USING(acid) command, the administrator issuing the command does not have an administrative authority that is present on the model acid.

Action:

No action is required.

Compare the administrative authority of the model acid and the administrator issuing the command. Make necessary changes.

TSS0378E

FACILITY INVALID FOR DIVISION OR DEPARTMENT

Reason:

Division, department, group, and zone ACIDs cannot access a system facility; therefore, the FACILITY keyword cannot be used for these ACIDs.

Action:

No action is required.

TSS0379E

PERMIT AND REVOKE INVALID FOR ZONE, DIV, DEPT or GROUP

Reason:

A resource cannot be PERMITed or REVOKEd from a DEPARTMENT, DIVISION, ZONE, or GROUP.

Action:

No action required.

TSS0380E

SOURCE NOT FOUND IN SECURITY RECORD

Reason:

The source specified in a REMOVE request was not found in the ACID's Security Record.

Action:

No action required.

TSS0381E

INSTDATA NOT FOUND IN SECURITY RECORD

Reason:

A request was made to REMOVE installation data from an ACID's Security Record; however, the ACID's Security Record did not contain installation data.

Action:

No action required.

TSS0382E

USER FIELD NOT FOUND IN SECURITY RECORD

Reason:

The user resource specified in a REMOVE request was not found in the ACID's Security Record.

Action:

No action required.

TSS0383E

RESOURCE ELEMENT NOT FOUND

Reason:

The general field specified in a REMOVE request was not found in the ACID's Security Record.

Action:

No action required.

TSS0384E

RESOURCE NOT FOUND IN SECURITY RECORD

Reason:

A CICS resource--such as FCT or PPT--specified in a REMOVE or REVOKE request was not found in the ACID's Security Record.

Action:

No action required.

TSS0385E

DATASET/PREFIX ALREADY OWNED, USE PERMIT

Reason:

An attempt was made to ADD a resource to an ACID. This message resulted because another ACID already owns the resource at a generically higher level (a shorter prefix).

Action:

To grant access to the resource, use the “PERMIT” function. To transfer ownership, use the “ADDTO” function with the UNDERCUT parameter. The resource prefix must be at least as generically high as the prefix that is currently owned.

TSS0386E

VOLUME ALREADY OWNED, USE PERMIT

Reason:

See message TSS0385E

Action:

No action required.

TSS0387E

RESOURCE ALREADY OWNED, USE PERMIT

Reason:

See message TSS0385E

Action:

No action required.

TSS0389E

FUNCTION INVALID WHEN USED WITH RDT/FDT

Reason:

A TSS RDT/FDT command was entered, but the function was not ADDTO, REMOVE FROM, REPLACE, DELETE, or LIST.

Action:

Reenter the TSS command using the correct function.

TSS0390E

UNEXPECTED ERROR, CODE = xxx

Reason:

CA Top Secret encountered a situation that logically should never occur.

Action:

The code XXX can be looked up in the Detailed Reason: Codes section of this manual. If the code is 079, the problem is simply that the specified ACID security record is full. See message TSS0473E for more information. For all other codes, collect dumps and/or trace logs produced by error. Contact CA Technical Support.

TSS0391E

ADMIN ACID MUST BE TYPE LSCA

Reason:

A TSS ADMIN(acid) SCOPE command was issued and the target of the command was not an LSCA.

Action:

Reenter the command using a valid LSCA ACID.

TSS0391I

MERGE DELETED RESOURCE XXXXXXXX

Reason:

A TSS DELETE(RDT) was issued, and the indicated user defined resource class has been deleted from the RDT.

Action:

Informational message only.

TSS0392E

MERGE FAILED - COULD NOT DELETE RESCLASS XXXXXXXX

Reason:

A TSS DELETE(RDT) was issued, and resources were found to be defined for the indicated user-defined resource class. The RDT may not be deleted until all user-defined resources have been removed.

Action:

Remove all references to the user defined resources.

TSS0393E

RESOWNER ACID DOES NOT EXIST

Reason:

An attempt was made to ADDTO a RESOWNER to a data set for SMS, but the ACID indicated in the RESOWNER parameter was not a valid ACID.

Action:

Re-enter the command using a valid ACID.

TSS0394E

RESOWNER ACID TYPE IS INVALID

Reason:

The ACID indicated by the RESOWNER parameter is not an SCA, VCA, DCA, or USER ACID.

Action:

Reissue the command, specifying a valid ACID.

TSS0395E

RESOWNER ACID IS NOT IN SCOPE

Reason:

The ACID indicated by the RESOWNER parameter does not fall within your administrative scope.

Action:

Specify an ACID which falls within your scope, or have an administrator with the proper authority assign the RESOWNER.

TSS0396E

USING ACID DOES NOT EXIST

Reason:

In the USING parameter of CREATE, you specified an ACID which does not exist.

Action:

Reissue the command, specifying a valid ACID.

TSS0397E

TYPE SPECIFIED DOES NOT MATCH USING ACID

Reason:

The type of ACID you specified in the using parameter of a TSS CREATE was incompatible with the acid type indicated by the TYPE keyword. For example, TSS CREATE(USER01) TY(USER) USING(DEPT01) is incorrect because DEPT01 is a department-type ACID, not a USER ACID.

Action:

Re-issue the command, specifying a valid ACID, or excluding the TYPE parameter.

TSS0398E

INVALID BEFORE/AFTER KEYWORD

Reason:

Both the BEFORE keyword and AFTER keyword were specified on the ADD of a profile. The BEFORE and AFTER keywords cannot be specified together in one command.

Action:

Reissue the command, specifying the BEFORE or AFTER keyword, not both.

TSS0399E

BEFORE/AFTER PROFILE DOES NOT EXIST

Reason:

The profile specified by the BEFORE or AFTER keyword was not a valid PROFILE.

Action:

Reissue the command, specifying a valid PROFILE ACID.

TSS0400E to TSS0599E

TSS0400E

BEFORE/AFTER PROFILE NOT ATTACHED TO ACID

Reason:

The PROFILE ACID specified by the BEFORE or AFTER keyword was not connected to the USER ACID.

Action:

Reissue the command, specifying a valid PROFILE ACID.

TSS0401E

INVALID TYPE

Reason:

The TYPE parameter of a MOVE function is incompatible with the type of ACID being moved. See the *Command Functions Guide* for a list of valid types which may be specified on a MOVE.

Action:

Reissue the command, omitting the TYPE keyword, or specifying a valid ACID type.

TSS0402E

INVALID TSO DATA - KEYWORD=

Reason:

The text of the data specified on the indicated TSO UADS command keyword is invalid.

Action:

See the *Command Functions Guide* for a description of valid values for the indicated keyword.

TSS0403E

CPF INACTIVE; COMMAND WILL NOT BE EXECUTED OR LOGGED

Reason:

An attempt was made to route a TSS command to a remote node through the TARGET keyword. However, the Command Propagation Facility (CPF) of CA Top Secret is not active.

Action:

Issue a TSS MODIFY(STATUS) to find the current status of CPF. See the CPF chapter in the *Command Functions Guide*

TSS0404E

MORE THAN 254 REMOTES TARGETED; REQUEST IGNORED

Reason:

The TARGET keyword was specified on a TSS command and contained a list of more than 254 target nodes.

Action:

If you intend to route a TSS command to more than 254 nodes, the command will have to be issued more than once with less than 254 TARGET nodes specified each time. Otherwise, enter the correct number of TARGET nodes.

TSS0405E

NO REMOTES TARGETED

Reason:

The WAIT keyword was specified on a TSS command and the TARGET keyword was omitted, or no default nodes were indicated by the CPFTGT control option.

Action:

Omit the WAIT keyword from the command and include the TARGET keyword with the WAIT command, or establish default TARGETs through the CPFTGT control option.

TSS0406E

INVALID VALUE FOR WAIT KEYWORD

Reason:

The WAIT keyword of the TSS command did not contain a value of Y (Yes) or N (No).

Action:

Re-specify the value for the WAIT keyword, or omit the keyword and allow the command to take the default indicated by the CPFMSGS control option.

TSS0407E

CPF SUBTASK HAS ABENDED

Reason:

An error occurred attempting to route a command to or from a remote node.

Action:

Contact CA Technical Support.

TSS0408E

RESCLASS AND RESCODE ARE MUTUALLY EXCLUSIVE FOR LIST FUNCTION

Reason:

Both the RESCLASS and RESCODE keywords were specified on a LIST(RDT) command. Only one keyword may be used.

Action:

Reissue the command, specifying the RESCLASS or RESCODE.

TSS0409E

RESCODE IS NOT DEFINED

Reason:

The RESCODE specified in the TSS command is not defined in the Resource Descriptor Table (RDT).

Action:

Re-enter the command, specifying a valid RESCODE.

TSS0410E

MORE THAN 8 MISC2 AUTHORITIES

Reason:

A TSS ADMIN/DEADMIN command for MISC2 authorities was attempted, and the list of authorities contained more than 8 entries.

Action:

Examine the syntax of the command entered, as there are only three unique values for MISC2.

TSS0412E

ATTR(LIB) IS INVALID FOR THIS RESOURCE CLASS

Reason:

The LIB keyword is valid only for the DATASET resource class.

Action:

If you are attempting to add or replace the characteristics of a resource class in the RDT, re-enter the command without ATTR(LIB).

If you are attempting to permit an ACID to a resource, re-enter the command without the LIB restriction. PRIVPGM may be specified without the LIB keyword.

TSS0413E

RESOURCE ALREADY DEFINED TO PERMITTEE

Reason:

A PERMIT with ACTION(ADMIN) was issued against the owner of the resource.

Action:

The owner of a resource automatically has administrative authority over the resource, and a PERMIT with ACTION(ADMIN) is not allowed.

TSS0414E

EXTENDED ADMINISTRATION DOES NOT SUPPORT MASKING

Reason:

Extended administration (ACTION(ADMIN)) does not support the use of masking characters in the resource name.

Action:

Re-enter the command, omitting the masking character in the resource name.

TSS0415E

INVALID SITRAN FACILITY

Reason:

The facility that was specified in the command does not exist.

Action:

Re-enter the command with the correct spelling of the facility, or define the facility before issuing the command.

TSS0418I

NO HELP AVAILABLE

Reason:

You issued a TSS HELP command for an operand that is not supported in CA Top Secret help.

Action:

No action necessary.

TSS0419E

INVALID REMOTE NODE IN TARGET LIST

Reason:

The remote node identified in target list is not defined in the CPFNODES control option.

Action:

Add desired target to CPFNODES in parmfile.

TSS0420E

INCONSISTENT VALUES IN DATA KEYWORD

Reason:

Keywords entered for the DATA parameter conflict with one another.

Action:

Reenter the command with one or the other DATA keyword.

TSS0421E

FUNCTION INVALID WHEN USED WITH APPCLU

Reason:

An attempt was made to RENAME, PERMIT, REVOKE, ADMIN or DEADMIN APPCLU ACID.

Action:

Retry command using one of the valid TSS command functions (i.e., ADDTO, REMOVE, or REPLACE).

TSS0422E

PASSWORD VERIFICATION FAILED AT REMOTE NODE

Reason:

ACID updated his password and during the propagation of that new password, CPF discovered that the ACID's old password on the local node did not match his current password on the remote node. This could indicate that there are two different ACIDs with the same ACID name on two or more different nodes. Password change does not take effect on the remote node.

Action:

No action required. This message is issued to the CPF SPOOL data set of the remote node.

TSS0423I

FROM: cpfnode

Reason:

This message is issued immediately before a display of messages received from a remote node in response to a synchronous (WAIT(y)) command previously sent to that node.

Action:

No action required.

TSS0424I

ACID aaaaaaaa FOR PROCNAME bbbbbbbb REPLACED WITH ACID cccccccc

Reason:

This is an informational message indicating that a TSS ADDTO was done to the STC record for a procname that already exists; however, the ACID parameter was different than the ACID associated with the procname. The current ACID is replaced with the new ACID.

aaaaaaaa = the old ACID

bbbbbbbb = the procname

cccccccc = the new ACID

Action:

No action required.

TSS0425E

SCOPE ACID MUST BE TYPE LSCA OR ZONE

Reason:

An attempt was made to assign a scope to an LSCA and one or more of the ACIDs identified in the SCOPE keyword was not a ZONE or an LSCA.

Action:

Reenter the command using a valid ZONE or LSCA for the SCOPE.

TSS0426E

ADMIN ACID MUST BE TYPE LSCA

Reason:

A TSS ADMIN(ACID) SCOPE command was issued and the target of the command was not an LSCA.

Action:

Reenter the command using a valid LSCA ACID.

TSS0427E

INVALID KEYWORD FOR THIS RESOURCE: xxxxxxxx

Reason:

The displayed keyword (xxxxxxxx) cannot be used for the given resource.

Action:

Correct the command and re-issue it.

TSS0428E

INVALID RESOURCE TYPE FOR ATTRIBUTE: xxxxxxxx

Reason:

The displayed attribute (xxxxxxxx) cannot be used with the given resource type.

Action:

Correct the command and re-issue it.

TSS0429E

SCOPED PROFILES ARE FOR ZCA, VCA, OR DCA ONLY

Reason:

An attempt was made to add profile scopes to an invalid ACID type.

Action:

None.

TSS0430I

CPF INITIALIZING;COMMAND WILL EXECUTE ON LOCAL NODE ONLY.

Reason:

CPF(ON) has been specified, but CCI is not available or not fully initialized. Until CCI completes initialization, commands entered on the local node will execute only on that node, and will not be propagated. The command also will not be logged to the CPF Recovery File.

Action:

Check to determine that CCI has completed initialization (CPF status shows ON, and not INIT) before issuing any commands intended for remote nodes.

TSS0431E

YOU MUST SPECIFY AN SDT RECORD TYPE WITH THIS COMMAND

Reason:

To list SDT data, you must specify the record type that you want to list.

Action:

Include a record type in your command syntax, and reissue the command.

TSS0432E

REQUIRED KEYWORD MISSING OR INVALID: xxxxxxxx

Reason:

Administrator has entered an ADDTO or REPLACE command that requires the specified (xxxxxxxx) field to be included with correct syntax.

Action:

Re-issue the command correcting or supplying the needed keyword.

TSS0433E

FUNCTION INVALID FOR SDT FACILITY

Reason:

An attempt was made to CREATE an ACID named SDT, or to rename another ACID to SDT. These functions are no longer valid because CA Top Secret 5.1 uses SDT (Static Definition Table) as a reserved ACID name.

Action:

Select another acidname for the CREATE or RENAME function.

TSS0434W

UPDATE STC RECORD FOR PROC procname

Reason:

An ACID has been deleted which was associated with a PROCNAME in the STC record. This invalidates the PROCNAME in the STC record. Any further invocating of the PROCNAME is assigned to a default ACID. This is your only warning.

Action:

Immediately copy all of the PROCNAMEs this message was issued for. If the PROCNAME is no longer used, remove it from the STC record. To correctly assign an ACID to the PROCNAME, replace the PROCNAME in the STC with a new valid ACID.

If you do not assigned another ACID to this PROCNAME, any attempt to start this PROCNAME results in the message:

TSS7145W Accessor ID not defined to Security

TSS0436E

SHORTER RESOURCE PREFIX ALREADY EXISTS IN THE AUDIT RECORD

Reason:

A TSS ADD(AUDIT) DSN(xxxx) command is issued where the resource name already exists at a shorter length in the AUDIT record. The command is properly failed.

Action:

The resource is already owned. Issue a PERMIT command as needed.

TSS0441E

INVALID DIGITAL CERTIFICATE NAME

Reason:

The name specified with the DIGICERT keyword is invalid or missing.

Action:

Reissue the command with a valid name. Reissue the command with a valid name. Note that, if this message is received after a GENREQ command, the GENREQ command does not create a certificate. Use the GENCERT command to create a certificate.

TSS0442I

TRUST AND NOTRUST ARE MUTUALLY EXCLUSIVE

Reason:

Both the TRUST and NOTRUST keywords were specified on an ADD or REPLACE DIGICERT command. Only one keyword may be used.

Action:

Reissue the command, specifying TRUST or NOTRUST.

TSS0443E

DIGITAL CERTIFICATE NOT FOUND

Reason:

The digital certificate name specified with the DIGICERT keyword could not be found in the user's ACID record.

Action:

Reissue the command with the name of an existing certificate.

TSS0444I

REPLACE COMMAND RESULTS IN EXPIRE DATE BEFORE START DATE

Reason:

Administrator issued a REPLACE command for a digital certificate and specified a new FOR or START keyword resulting in a bad date. On a replace, if the START date is not specified then the FOR date will be calculated using the current day's date.

Action:

Correct the command. If necessary include both START and FOR keywords to get the desired results.

TSS0446E

INVALID CERTIFICATE KEYRING NAME

Reason:

The KEYRING keyword was specified without a keyring name or the name entered is not a valid 8-byte name.

Action:

Reissue the command with KEYRING(xxxxxxxx).

TSS0447E

CERTIFICATE NAME ALREADY EXISTS

Reason:

You are attempting to add a certificate to an acid that already has a certificate by that name.

Action:

Reissue DIGICERT(xxxxxxxx) with a different name.

TSS0448E

CERTIFICATE KEYRING ALREADY EXISTS

Reason:

You are attempting to add a keyring to an acid that already has a keyring by that name.

Action:

Reissue KEYRING(xxxxxxxx) with a different name.

TSS0449E

CERTIFICATE KEYRING NOT FOUND

Reason:

You must add the KEYRING to an acid before attempting to ADD RINGDATA for perform any other function against the KEYRING.

Action:

Issue TSS ADDTO(acid) KEYRING(xxxxxxxx) before performing any other functions.

TSS0450E

INVALID USAGE SPECIFIED

Reason:

You specified an incorrect operand for the USAGE keyword.

Action:

Issue TSS ADDTO(acid) KEYRING(xxxxxxxx) USAGE(xxxxxxxx) with PERSONEL, CERTSITE, OR CERTAUTH specified as the type of usage for the KEYRING being updated.

TSS0451E

INVALID CERTIFICATE NAME FILTER

Reason:

The CERTMAP keyword was specified without a record ID or the MULTIID acid was specified without specifying the CERTMAP keyword.

Action:

Reissue the command with CERTMAP(rrrrrrrr).

TSS0452E

INVALID CRITERIA MAP

Reason:

The CRITERIA keyword was specified and neither SDNFILTR or IDNFILTR was specified or the format of the CRITERIA data was invalid.

Action:

Reissue the command with one or both filter keywords.

TSS0453E

INVALID CERTIFICATE NAME FILTER DATA

Reason:

An invalid identifier was found in the SNDFILTR or IDNFILTR data field.

Action:

Reissue the command with correct certificate identifiers. See the CA Top Secret *Cookbook* for information on correct identifiers.

TSS0454E

MULTIID AND CRITERIA MUST BOTH BE SPECIFIED

Reason:

ACID(MULTIID) was specified and the CRITERIA keyword was not or the CRITERIA keyword was specified and the acid name was not MULTIID.

Action:

Reissue the command specifying both ACID(MULTIID) and CRITERIA on the same command.

TSS0455E

CERTIFICATE LABEL ALREADY EXISTS

Reason:

You are attempting to add a label to an acid that already has a label by that name.

Action:

Reissue LABLCERT(xxxxxxxx) with a different name.

TSS0456E

CERTIFICATE KEYRING LABEL ALREADY EXISTS

Reason:

You are attempting to add a label to a keyring that already has a label by that name.

Action:

Reissue LABLRING(xxxxxxxx) with a different name.

TSS0457E

CERTIFICATE LABEL NOT FOUND

Reason:

You specified a LABLCERT keyword that does not exist for the acid.

Action:

Issue TSS ADDTO(acid) LABLCERT(xxxxxxx) before performing any other functions against that certificate label.

TSS0458E

CERTIFICATE KEYRING LABEL NOT FOUND

Reason:

You must add the LABLRING to the acid with the KEYRING before attempting to add RINGDATA information or perform any other function against that LABLRING.

Action:

Issue TSS ADDTO(acid) KEYRING(xxxxxxxx) LABLRING(xxxxxxx) before performing any other functions.

TSS0459E

MUST SPECIFY SIGNWITH

Reason:

A certificate without a private key was being created or the DCDSN keyword was included on a TSS GENCERT command. In either situation the SIGNWITH keyword must be specified.

Action:

Issue TSS GENCERT with the SIGNWITH keyword included.

TSS0460E

INVALID FORMAT

Reason:

Invalid format was specified on the TSS EXPORT command.

Action:

Valid formats are CERTDER or CERTB64. The default is CERTB64.

TSS0461E

INVALID SUBJECTSDN DATA

Reason:

SUBJECTDN data was entered without one of the correct prefixes. All SUBJECTDS data must be prefixed by one of the predefined codes.

Action:

Reissue the SUBJECTDN keyword with the correct syntax. See the CA Top Secret *Cookbook* for a list of the correct codes.

TSS0462E

INVALID KEYWORD SPECIFIED FOR FUNCTION

Reason:

A TSS REMOVE(acid) CERTMAP(rrrrrrrr) command was issued with another parameter specified or SDNFILTR or IDNFILTR was specified on a TSS REPLACE command.

Action:

Reissue the REMOVE command with only the CERTMAP keyword. If the SDNFILTR or IDNFILTR keywords need to be replaced on the acid the CERTMAP keyword must be removed and then added again.

TSS0463E

AT LEAST 1 KEYWORD MUST BE SPECIFIED WITH ADD

Reason:

A TSS ADDTO(acid) command was entered with no keywords.

Action:

Reissue the command with at least one keyword specified.

TSS0464E

YOU MUST SPECIFY KEYWORD DIGICERT

Reason:

You issued a CA Top Secret command that requires the DIGICERT keyword.

Action:

Reissue the command including the DIGICERT(xxxxxxxx) keyword.

TSS0465E

YOU MUST SPECIFY KEYWORD KEYRING

Reason:

You issued a CA Top Secret command that requires the KEYRING keyword.

Action:

Reissue the command including the KEYRING(xxxxxxxx) keyword.

TSS0466E

YOU MUST SPECIFY KEYWORD CERTMAP

Reason:

You issued a CA Top Secret command that requires the CERTMAP keyword.

Action:

Reissue the command including the CERTMAP(xxxxxxxx) keyword.

TSS0467E

YOU MUST SPECIFY KEYWORD CRITMAP

Reason:

You issued a CA Top Secret command that requires the CERTMAP keyword.

Action:

Reissue the command including the CRITMAP(xxxxxxxx) keyword.

TSS0468I

STATIC DATA TABLE (SDT) IS FULL

Reason:

The SDT Record holds data for digital certificates, keyrings, CNF, Calendar, RLP, SLP, and Timerec records. An attempt was made to update the SDT with one of these record types. However, the SDT storage area was exceeded.

Action:

Expand the number of SDT blocks on your security file as follows:

Run TSSMAINT to backup the security file.

Run TSSMAINT to create a new security file with SDTBLOCKS=99.

Run TSSXTEND to copy the existing security file to the new security file created in step 2.

TSS0469E

INVALID CNFUVAR DATA

Reason:

The CNFUVAR data is not in the correct format. A variable and its data must be separated by an equal sign (=) and each set of variable and data must be separated by a period.

Action:

Correct the syntax and reissue the command.

TSS0470E

CERTIFICATE NOT FOUND FOR SPECIFIED SIGNWITH

Reason:

The SIGNWITH keyword specified a certificate that does not exist.

Action:

Correct the syntax and reissue the command.

TSS0471E

CERTIFICATE NOT FOUND FOR SPECIFIED SERIAL/ISSUERDN

Reason:

The SERIALNUM or ISSUERDN keyword was issued for a certificate that does not exist.

Action:

Correct the syntax and reissue the command.

TSS0472E

INVALID PRIVATE KEY SIZE

Reason:

There is no info in our write-up about the KEYSIZE(key-size) keyword.

Action:

Correct the syntax and reissue the command.

TSS0473E

MAX SIZE OF ACID xxxxxxxx HAS BEEN EXCEEDED

Reason:

The ownership keywords and permissions associated with this ACID have exceeded the capacity of CA Top Secret to absorb additional security specifications from your latest command.

Action:

If this is a hierarchy ACID (for example, DEPARTMENT, DIVISION, or ZONE), you may need to provide an additional hierarchy ACID at the same level to accommodate new ownerships. However, you may also find that you can reduce the number of ownerships required by owning a higher level prefix instead of owning many individual resources or lower-level multiply qualified resource prefixes.

If this is a PROFILE ACID, consider granting permission at a lower-level prefix instead of using multiple lower-level permissions. You may also decide to split this profile into more carefully tailored and individualized profiles of more manageable size.

If this is a USER ACID, consider the possibility of granting permissions to individual PROFILE ACIDs instead of to individual users. PROFILE ACIDs are cached in central shared storage, and will reduce system overhead by reducing security file I/O requests. Individual ACID permissions and keywords should be used to override information stored in more general profiles shared by large numbers of users.

TSS0474E

INVALID OR MISSING KERBNAME

Reason:

An attempt was made to ADD a Kerberos segment and the keyword KERBNAME was not specified or had an invalid value.

Action:

Reissue TSS command with a valid KERBNAME value. See the *User Guide* for details on keyword KERBNAME.

TSS0475E

REALM RECORD ALREADY EXISTS

Reason:

An attempt was made to ADD a Kerberos REALM record to the SDT and one by that name already exists.

The REALM record name must be uniquely specified.

Action:

Reissue TSS command choosing a unique name for REALM keyword.

TSS0476E

REALM RECORD NOT FOUND

Reason:

An attempt was made to REMOVE or REPLACE a Kerberos REALM SDT record and the record cannot be found.

Action:

Recheck value specified for REALM name, and reissue TSS command.

TSS0477E

MISSING OR INVALID REALM

Reason:

An attempt was made to ADD a Kerberos REALM record to the SDT, however the keyword REALM was not specified or incorrectly specified. You must specified valid REALM label when creating a REALM record to the SDT.

Action:

Reissue TSS command specifying valid REALM label name.

TSS0478E

INVALID OR MISSING KERBPASS

Reason:

An attempt was made to ADD a Kerberos REALM record to the SDT and the keyword KERBPASS was not specified or had an invalid value. The KERBPASS is used in building the Kerberos Key for the Realm.

Action:

Reissue TSS command with a valid KERBPASS value. See the *User Guide* for details on keyword KERBPASS.

TSS0479E

MUST SPECIFY MINTKTLF, DEFTKTLF, AND MAXTKTLF ALL TOGETHER

Reason:

An attempt was made to ADD a Kerberos LOCAL REALM record to the SDT with ticket life values, and only one or two values were specified. However, to complete the definition, all three values must be set.

Action:

Reissue TSS command specifying all three-ticket life values.

TSS0480E

MISSING OR INVALID KERBLINK

Reason:

An attempt was made to ADD or REMOVE a Kerberos foreign KERBLINK SDT record and the keyword KERBLINK was not specified or was invalid.

Action:

Reissue TSS command specifying valid KERBLINK value.

TSS0481E

KERBLINK RECORD NOT FOUND

Reason:

An attempt was made to REPLACE or REMOVE a Kerberos KERBLINK record from the SDT, however the KERBLINK record was not found.

Action:

Reissue TSS command specifying valid KERBLINK name.

TSS0482E

DEFAULT REALM (KERBDFLT) NOT DEFINED

Reason:

An attempt was made to process a Kerberos (principal) segment and the required SDT local REALM record (KERBDFLT) was not found.

Action:

Define a Local REALM record to the SDT, then reissue TSS command to add the principal.

TSS0483E

MINTKTLF VALUE MUST NOT EXCEED DEFTKTLF

Reason:

An attempt was made to ADD or REPLACE ticket life values for the Local REALM, and found that the minimum ticket life (MINTKTLF) specified was greater then the value in DEFTKTLF (the default ticket life).

Action:

Reissue TSS command choosing a MINTKTLF equal to or less than DEFTKTLF.

TSS0484E

DEFTKTLF VALUE MUST NOT EXCEED MAXTKTLF

Reason:

An attempt was made to ADD or REPLACE ticket life values for the Local REALM, and found that the default ticket life (DEFTKTLF) specified was greater than the value in MAXTKTLF (the maximum ticket life).

Action:

Reissue TSS command choosing a DEFTKTLF equal to or less than MAXTKTLF.

TSS0485E

KERBLINK RECORD ALREADY EXISTS

Reason:

An attempt was made to ADD a Kerberos segment (principal user) and a SDT KERBLINK record already exists for this user. The user already has a Kerberos segment, or the name previous chosen for a foreign KERBLINK conflicts with this users name.

Action:

Check (TSS LIST) to see if user already is defined as a Kerberos principal and has a Kerberos segment. If not, display the KERBLINK SDT record and see if the name for that foreign link could be renamed. If so, removed the KERBLINK SDT record and re-add specifying another name.

TSS0486E

INVALID OR MISSING LINKNAME

Reason:

An attempt was made to ADD a Kerberos foreign Kerberos link and the keyword LINKNAME was not specified or has an invalid value specified.

Action:

Reissue TSS command with a valid LINKNAME value. See the *User Guide* for details on keyword LINKNAME.

TSS0487E

CANNOT REMOVE, KERBLINK IS ATTACHED TO A LOCAL PRINCIPAL

Reason:

An attempt was made to REMOVE a Kerberos KERBLINK record from the SDT. However this record is already attached to a user who has been defined as a Kerberos principal user. The KERBLINK name is part of that definition.

Action:

To remove this KERBLINK record, you must do so by removing the Kerberos segment from the user.

TSS0488E

MISSING REALMNAME

Reason:

An attempt was made to ADD a Kerberos REALM record and the keyword REALMNAME was not specified.

Action:

Reissue command with a REALMNAME value.

TSS0489E

KERB SEGMENT ALREADY EXISTS

Reason:

An attempt was made to ADD or REPLACE the KERBNAME but the value duplicates the value on another ACID.

Action:

Use a new value for the KERBNAME on the ACID. Alternatively, list the SDT KERBLINK table to determine the ACID which currently employs that KERBNAME value; alter or remove the KERBNAME on that ACID.

TSS0490E

CANNOT ADD SEGMENT, A KERBLINK RECORD OF THE SAME NAME (xxxxxxxx) ALREADY EXISTS

Reason:

An attempt was made to ADD a Kerberos segment to a user, however the user's acid name already matches a KERBLINK record of the same name, the existing KERBLINK record was previously defined as a foreign KERBLINK record.

Action:

Need to rename the existing KERBLINK, and then reissue TSS command to add the Kerberos segment.

TSS0491E

ALTNAME CONTAINS AN INVALID KEYWORD - keyword

Reason:

The GENCERT command found a syntax error within the ALTNAME keyword specification. The keyword in error is displayed at the end of the message text.

Action:

The command ends. Re-enter the command with the correct syntax.

Module:

TSSAUTH1

TSS0492E

ALTNAME CONTAINS AN INVALID VALUE IN KEYWORD -

Reason:

The GENCERT command found a syntax error within the ALTNAME keyword specification. The value specified is in error and displayed at the end of the message text.

Action:

The command ends. Re-enter the command with the correct syntax.

Module:

TSSAUTH1

TSS0493E

ALTNAME CONTAINS DUPLICATE KEYWORD - keyword

Reason:

The GENCERT command found a duplicate keyword within the ALTNAME keyword specification. The keyword specified is in error and displayed at the end of the message text.

Action:

The command ends. Re-enter the command with the correct syntax.

Module:

TSSAUTH1

TSS0494E

ALTNAME CONTAINS A VALUE TOO LONG IN KEYWORD -

Reason:

The GENCERT command found a value too long within the ALTNAME keyword specification. The keyword specified is in error and displayed at the end of the message text.

Action:

The command ends. Re-enter the command with the correct syntax.

Module:

TSSAUTH1

TSS0495E

ALTNAME CONTAINS MISSING DATA FOR KEYWORD - keyword

Reason:

The GENCERT command found a null data within the ALTNAME keyword specification. The keyword specified is in error and displayed at the end of the message text.

Action:

The command ends. Re-enter the command with the correct syntax.

Module

TSSAUTH1

TSS0496E

MISSING OR INVALID KEYUSAGE

Reason:

The GENCERT command found a null or invalid data for keyword KEYUSAGE.

Valid values are: HANDSHAKE, DATAENCRYPT, DOCSIGN, and CERTSIGN.

Action:

The command ends. Re-enter the command with the correct syntax.

Module:

TSSAUTH1

TSS0497E

INVALID SITHWITH - USER CERTIFICATE CANNOT SIGN CERTAUTH/SITE CERTICATE

Reason:

The GENCERT command found the certificate specified in the SITHWITH keyword is not authorized to sign a CERTAUTH or CERTSITE certificate.

Action:

The command ends. Re-enter the command with the correct SITHWITH certificate.

Module:

TSSAUTH1

TSS0498E

SIGNWITH CERTIFICATE IS NOT TRUSTED. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

When generating a new certificate, the trust status for the new certificate comes from the signing certificate. The SIGNWITH certificate specified is not trusted so the newly generated certificate is also not trusted. All self-signed certificates are generated with a status of TRUST.

Action:

None. The certificate was created but the status was set to NOTRUST.

TSS0499E

INVALID SIGNWITH - CERTIFICATE HAS NO PRIVATE KEY

Reason:

The GENCERT command requires a certificate that contains a private key. A private key is not available for this certificate specified in the SITHWITH keyword.

Action:

The command ends. Re-enter the command using a certificate that has a private key.

Module:

TSSAUTH1

TSS0501E

INVALID SIGNWITH – USER CERTIFICATE CANNOT BE USED TO SIGN ANOTHER USER'S CERTIFICATE

Reason:

When SIGNWITH specifies a user acid, the acid name must be the same as specified on the GENCERT or RENEW command.

Action:

Reissue the command with the correct SIGNWITH certificate.

TSS0521E

TSS0521E ERROR ENCOUNTERED DURING PASSWORD ENCRYPTION

Reason:

When attempting to update a user password, an error occurred during password encryption processing.

Action:

Contact CA technical support.

TSS0522E

TSS0522E ERROR ENCOUNTERED DURING PASSWORD PHRASE ENCRYPTION

Reason:

When attempting to update a user password phrase, an error occurred during password phrase encryption processing.

Action:

Contact CA technical support.

TSS0597E

TSS0597E DATA CLASSIFICATION variable

Reason:

An error has occurred during an administration attempt of the DATACLAS records. See the variable portion of the error message for specific problem

Action:

Correct the syntax of the command and re-issue it.

TSS0598E

DATA CLASSIFICATION COMMAND ENVIRONMENT ERROR

Reason:

The DATACLAS record can only be processed when the VSAM_DIGICERT feature is active.

Action:

Define a VSAM file to be used with CA Top Secret. Initialize a new security file with TSSMAINT and specify INITVSAM=DIGICERT. For more information, see the *Installation Guide*.

TSS0599E

CA Top Secret ENVIRONMENT ERROR

Reason:

The CA Top Secret address space was not available.

Action:

Retry when CA Top Secret is available.

TSS0600E to TSS0965E

TSS0600E

USER NOT DEFINED TO CA Top Secret

Reason:

Data was requested on an ACID which does not exist.

Action:

Define the ACID to CA Top Secret or verify that the ACID has been specified correctly.

TSS0610E

SIGVER COMMAND ENVIRONMENT ERROR

Reason:

The SIGVER record is only supported with a VSAM security file.

Action:

Do not use SIGVER related commands with a non-VSAM security file.

TSS0611E

SIGVER command – *error condition*

Reason:

The specified SIGVER command failed due to the reported error condition.

Action:

Correct the error condition and re-issue the command if necessary.

TSS0920E

R_admin Internal error. Rsn= nn

Reason:

An internal error occurred while processing an R_admin service request. The reason code (nn) identifies the cause of the error.

Action:

Contact CA Top Secret support.

Module:

TSSOEADM

TSS0935E

Error retrieving SignWith certificate label = *uuuuuuuu*

Reason:

An attempt to retrieve a certificate authority certificate that is needed to sign a completed certificate request failed. *uuuuuuuu* shows the label for the certificate.

Action:

Use the TSS LIST command to verify that the certificate with the specified label exists. If the certificate exists, contact CA technical support.

TSS0936E

Increment serial number error RC = xx

Reason:

An error occurred while incrementing the serial number for a signwith certificate.

Action:

Contact TSS support.

TSS0937E

Error inserting certificate with label = *uuuuuuuu*

Reason:

An attempt to add a certificate to the TSS database failed. *uuuuuuuu* shows the label for the certificate. Contact CA technical support.

Action:

Use the TSS LIST command to verify that the certificate with the specified label exists. If the certificate exists, contact TSS support.

TSS0938E

Error retrieving certificate with label = *uuuuuuuu*

Reason:

An attempt to retrieve a certificate for information failed. *uuuuuuuu* shows the label for the certificate. Contact CA technical support.

Action:

Use the TSS LIST command to verify that the certificate with the specified label exists. If the certificate exists, contact CA technical support.

TSS0940I

DUPLICATE CERTIFICATE DETECTED - *uuuuuuuu*

Reason:

An attempt was made to ADD a Digital Certificate that has already been added to the CA Top Secret file. Where *uuuuuuuu* shows the ACID name for the current user.

Action:

Issue the TSS command CHEKCERT with the certificate data set (DCDSN) as input. The CHECKCERT will display some details about the certificate itself, and what TSS ACID has it.

TSS0941I

CERTIFICATE DATA SET *rrrrrrrr* ERROR

Reason:

An attempt was made to process the DCDSN (Digital Certificate data set) and an allocation error occurred. The *rrrrrrrr* shows the data set name in question.

Action:

Determine if the data set name specified within the DCDSN parameter is correct. Re-issue the TSS command with the correct DCDSN specification.

TSS0942I

INVALID CERTIFICATE DATA

Reason:

An attempt was made to process the DCDSN (Digital Certificate data set) and TSS detected invalid key information.

Action:

Issue the TSS command CHKCERT with the certificate data set (DCDSN) as input. The CHKCERT will display some details about the certificate itself, and what TSS ACID has it. Make sure the certificate specified in DCDSN is valid.

TSS0943I

GENCERT FUNCTION NOT INSTALLED

Reason:

The component required to make GENCERT fully functional has not been installed.

Action:

Verify that the SAF FMIDs are installed properly. If there are no installation errors, please contact CA Technical Support.

TSS0944I

GENREQ FUNCTION NOT INSTALLED

Reason:

The component required to make GENREQ fully functional has not been installed.

Action:

Verify that the SAF FMIDs are installed properly. If there are no installation errors, please contact CA Technical Support.

TSS0945I

INVALID OR MISSING PASSWORD - PKCSPASS

Reason:

An attempt was made to process a password protected PKCS #12 Digital Certificate. The password specified in the PKCSPASS parameter is incorrect or not specified.

Action:

Supply the correct password in PKCSPASS that matches the specified DCDSN certificate.

TSS0946I

INPUT DCDSN CONTAINS PKCS#10 REQUEST

Reason:

The TSS CHKCERT command will not work on a dataset that contains a PKCS#10 certificate request. CHKCERT only works on a dataset that contains a PKCS#12 certificate.

Action:

Supply a dataset that contains a PKCS#12 certificate.

TSS0947E

DUPLICATE LABLPKDS DETECTED

Reason:

If processing the GENCERT, REKEY or ADD command, LABLPKDS was specified and the label name that was specified already exists for PKDS labels.

Action:

Specify another LABLPKDS label value.

TSS0948E

SAFCRCSF ICSF failure

Reason:

An attempt to add a certificate key to ICSF failed.

Action:

Contact CA technical support.

TSS0949E

SPECIFIED PRIVATE KEY DOES NOT MATCH EXISTING PRIVATE KEY

Reason:

The certificate being added already exists but the private key of the certificate does not match the private key in the existing certificate.

Action:

The certificate is not updated. Correct the error with the certificate and retry the function.

TSS0950I

UNSUPPORTED SIGNATURE ALOGRITHM – ADDING CERTIFICATE WITH NOTRUST

Reason:

The algorithm used to create the signature of a certificate being inserted is not supported. The certificate is added with NOTRUST status.

Action:

Since the signature could not be verified, there is a potential that the certificate could have been modified before it was inserted. If you can be sure that the signature has been verified by other means, set the status to TRUST to allow the certificate to be used. Contact CA Top Secret Support as there may be current support for the signature algorithm.

TSS0956E

UNLOCK PROCESS OF PASSWORD CHANGE FAILED - INVALID PASSWORD

Reason:

The password you entered was incorrect. The password will not change.

Action:

Replace your password again. Enter the correct old password when prompted.

TSS0960E

SHARED PROFILE TABLE IS FULL - jobname

Reason:

During a signon, the profile sharing table used by this region was found to be full. The signon continues but profiles needed by this user will be privately obtained and not eligible for sharing by other users of the region. When users of a region do not share profiles, region storage is often adversely impacted.

Action:

Report this message to security personnel. The size of the shared profile table used by this region may need adjustment. See the PRFT facility option in the *Control Options Guide* for more information.

TSS0961W

SIGNON FASTPATH UNAVAILABLE RC=xx

Reason:

During signon to a region supporting profile sharing, it was detected that CA Top Secret signon fastpath logic was temporarily unavailable due to system workloads. The current signon continues but without the benefit of signon fastpath performance.

Action:

Intermittent issuance of the message, especially during peak periods, does not signify a problem. When available, CA Top Secret employs ESA AR-mode service facilities to improve signon performance for regions using profile sharing. If these services are frequently unavailable, consider disabling profile sharing for the affected regions.

TSS0962E

MAXUSER EXCEEDED - XREF TABLE FULL - F(facility) J(jobname)

Reason:

The XREF in-core signon table for the multi-user address space *jobname* is exhausted. ACEE information is stored for the individual terminal session only and is not stored in the XREF table. Features like SIGN(S) cannot be enforced for such locally signed on ACEEs. In IMS, this can lead to additional signons in dependent regions.

Action:

Increase the MASTFAC facility MAXUSER parameter appropriate to the number of simultaneous end-users who will be signed on to the address space. Although MAXUSER may be modified at any time for a FACILITY, the address space *jobname* must be recycled for the new parameter to take effect.

TSS0963I

SHARED PROFILE TABLE > nn% FULL - JOB jjjjjjj (sssssss)

Reason:

The shared profile table is a storage area reserved in CA Top Secret multi-user address spaces to store TYPE=PROFILE acids at signon as a common pool for the address space. This message is displayed when the profile table reaches 65%, 70%, and 80% of capacity.

Administrators can use the control option SHRPROF(*jjjjjjjj*) to display statistics for this table in a specified jobname.

nn% is the percentage of allocated storage in use by profiles signed on to the designated multi-user address space *jjjjjjjj*. *ssssssss* designates whether the profile table is stored in PRIVATE or COMMON areas of storage.

Action:

When the shared profile percentage reaches 100%, the address space must read new profiles into the private SECREC for newly signed on users. This causes additional security file I/O during signon and may reduce the efficiency of CA Top Secret for this address space. To increase the profile table size modify the region ACID MASTFAC facility parameter PRFT.

For information on the FACILITY parameter, see the *Control Options Guide*. Increasing the size of the PRIVATE profile table may require an increase the region size for the multi user address space. Increasing the size of a COMMON profile table require a reconfiguration of the size of your MVS CSA.

TSS0964I

NO SHARED PROFILE TABLE FOR JOB *jjjjjjjj*

Reason:

The shared profile table for JOBNAME *jjjjjjjj* could not be located. This message may be issued in response to the control option SHRPROF(*jjjjjjjj*) when:

- The job or stc name *jjjjjjjj* is no longer actively executing.
- The job or stc name *jjjjjjjj* has a region acid with a MASTFAC which indicates it is a single user address space (SUAS). Only a multi-user address space (MUAS) can possess a shared profile table.
- No ACID has signed on to the address space with an attached profile.

Action:

Assure that the jobname referenced by the SHRPROF control option has the appropriate prerequisite conditions for a shared profile table to be allocated.

TSS0965E

KEYUSAGE INDICATES ONLY KEYAGREE – CANNOT ADD CERTIFICATE UNDER CERTAUTH

Reason:

The certificate being added contains a key usage value of keyAgreement with no other values specified. This prevents the certificate from being used for signing and verification. The certificate cannot be added under the CERTAUTH userid.

Action:

Obtain a certificate that can be used as a CA Technologies certificate or add the current certificate under a different user.

TSS1000E to TSS1628E

TSS1000E

INSUFFICIENT MEMORY.

Reason:

TSSCHART was unable to acquire a sufficient amount of memory for its work area.

Action:

No action required.

TSS1001E

UNABLE TO IDENTIFY MASTER SCA.

Reason:

TSSCHART was unable to obtain information about the Master Security Administrator from the CA Top Secret address space.

Action:

No action required.

TSS1002E

SECURITY FILE IS EMPTY.

Reason:

TSSCHART found no departments, divisions or alternate SCA's in the Security File--that is, there is no information present on the Security File to chart.

Action:

No action required.

TSS1003E

CA Top Secret IS UNAVAILABLE AT THIS TIME.

Reason:

The CA Top Secret address space was not currently active when TSSCHART was run. CA Top Secret is required to obtain Security File information during the charting process.

Action:

Rerun when CA Top Secret is active.

TSS1004E

CA Top Secret CROSS MEMORY COMMUNICATIONS FAILURE

Reason:

This message is issued by TSSCHART when it is unable to service a request (TSS is down, MVS system service failure, and so forth).

Action:

Restart CA Top Secret if it is down. If this does not work or if the error is not caused by CA Top Secret, review other dumps occurring at the same time and contact the appropriate vendor.

TSS1005E

INSUFFICIENT AUTHORITY FOR TSSCHART.

Reason:

The following administration authorities were not found:

ACID(REPORT) and RESOURCE(REPORT) .

Action:

Obtain proper administrative authorities and rerun.

TSS1006E

"SYSPRINT" DD STATEMENT MISSING.

Reason:

The SYSPRINT DD-statement was not present. All charting information is sent to the SYSPRINT file.

Action:

Correct JCL and resubmit.

TSS1007E

"SYSIN" DD STATEMENT MISSING.

Reason:

The SYSIN DD-statement was not present. All charting keywords are read from the SYSIN file.

Action:

Correct JCL and resubmit.

TSS1008E

KEYWORD keyword - INSUFFICIENT AUTHORITY.

Reason:

One of the following was encountered:

- CHART(ACID) was specified without the administrator having ACID(REPORT) authority; or
- CHART(RESOURCE) was specified without the administrator having RESOURCE(REPORT) authority.

Action:

No action required.

TSS1009E

KEYWORD keyword - INVALID SUBFIELD VALUE.

Reason:

An invalid subfield value was specified for the indicated keyword.

Action:

Correct subfield value and resubmit.

TSS1010E

KEYWORD keyword - ALREADY SPECIFIED.

Reason:

Duplicate CHART or RESOURCE keywords were encountered.

Action:

Delete duplicate keyword and resubmit.

TSS1011E

KEYWORD keyword - CONFLICTING PARAMETER.

Reason:

One of the following was encountered:

- DIVISION and XDIVISION were both specified
- DEPARTMENT and XDEPARTMENT were both specified
- PROFILE and XPROFILE were both specified
- USER and XUSER were both specified.

Action:

Correct keywords and parameters and resubmit.

TSS1012E

ACID acid IS NOT WITHIN YOUR SCOPE.

Reason:

The specified acid is not within your scope of authority. Only those acids within your scope may be charted.

Action:

No action required.

TSS1013E

ACID acid IS UNKNOWN/UNDEFINED TO CA Top Secret.

Reason:

The specified acid has not been defined to CA Top Secret. (The acid has not been created.)

Action:

No action required.

TSS1014E

ACID acid - PARAMETER/TYPE MISMATCH

Reason:

The specified acid type did not match the type of acid expected for that keyword. (A department acid was specified in the DIVISION or XDIVISION keyword.)

Action:

No action required.

TSS1015E

MISSING/INVALID SECURITY ENVIRONMENT

Reason:

TSSCHART has found that no security environment has been established for this administrator.

Action:

No action required.

TSS1016E

CA Top Secret/TSSCHART VERSION MISMATCH

Reason:

Different versions of CA Top Secret and TSSCHART are incompatible.

Action:

No action required.

TSS1017E

UNKNOWN ACID CHAIN DETECTED - X=xx,P=pppppp,T=tt,C=cccccc (DRC=dd)

Reason:

This message is issued by TSSCHART when it fails for building ACID's tree structure because the invalid or broken chains of ACID records are detected.

Where:

xx: Entry Identifier on Security File

pppppp: Parent ACID Number

tt: ACID Type

cccccc: Child ACID Number in the bucket of Parent ACID

dd: Detailed Return Code

Action:

Contact CA Top Secret technical support and provide the message number and diagnostic DUMP information of U0998.

TSS1047E

TSSCHART MUST EXECUTE APF-AUTHORIZED

Reason:

TSSCHART must be executed from an APF authorized library.

Action:

Ensure TSSCHART is in an APF authorized library and rerun.

TSS1301I

CACHE HAS BEEN CLEARED

Reason:

A CACHE(CLEAR) command was issued or the CACHE threshold value was exceeded and the CACHE was cleared.

Action:

No action is required, you may wish to increase the CACHE threshold if CACHE is cleared too often.

TSS1302I

CACHE COMMAND FAILED

Reason:

An error has occurred during the processing of the CACHE command.

Action:

Enter a TSS MODIFY CACHE(nnnn) command to start CACHE.

TSS1303I

CACHE IS OFF

Reason:

You issued the TSS MODIFY CACHE(STATUS) command when CACHE was not active.

Action:

Enter a TSS MODIFY CACHE(nnnn) command to start CACHE.

TSS1304I

------ CACHE STATISTICS -----

TSS1305I

MAXSIZE (nnnnnnnnnK) SIZE (nnnnnnnnnK)

TSS1306I

CALLS (nnnnnnnnn) SATISFIED (nnnnnnnnn)

TSS1307I

CLEARED (nnnnnnnnn)

Reason:

These messages provide statistics on how much cache is used and how efficient CACHE is in avoiding extra I/O.

MAXSIZE

Maximum number of kilobytes used by CACHE as the storage threshold.

SIZE

Current amount of storage used. If CACHE overflows, it is automatically cleared and starts to fill again.

CALLS

Number of calls made to CACHE.

SATISFIED

Number of calls satisfied in CACHE.

CLEARED

How many times CACHE was cleared for the life of the CA Top Secret address space. Clear is also automatically performed whenever a cache request is issued that would cause the CURRENT SIZE to exceed the MAXSIZE.

Action:

No action necessary.

TSS1308

INVALID REFRESH REQUEST

Reason:

An invalid REFRESH option was entered.

Action:

Enter a correct option and reissue the REFRESH command.

TSS1308I to TSS1322I

```
TSS1308I  ------- STATISTICS BY COMMAND -------

TSS1309I CREATE(000000000) DELETE        (000000000)

TSS1310I ADD               (000000000) REPLACE     (000000000)

TSS1311I RENAME            (000000000) REMOVE      (000000000)

TSS1312I PERMIT            (000000000) REVOKE      (000000000)

TSS1313I WHOOWNS           (000000000) WHOHAS      (000000000)

TSS1314I LIST      (000000000) HELP          (000000000)

TSS1315I LOCK      (000000000) UNLOCK        (000000000)

TSS1316I WHOAMI            (000000000) MODIFY      (000000000)

TSS1317I ADMIN             (000000000) DEADMIN     (000000000)

TSS1318I MOVE    (000000000) REFRESH       (000000000)

TSS1319I GENCERT           (000000000) GENREQ      (000000000)

TSS1320I EXPORT            (000000000) CHKCERT     (000000000)

TSS1321I MLWRITE           (000000000) REKEY       (000000000)
```

TSS1322I

ROLLOVER (000000000)

Reason:

These messages provide statistics on how many times each command was issued successfully.

CREATE

Number of CREATE commands issued.

DELETE

Number of DELETE commands issued.

ADD

Number of ADD commands issued.

REPLACE

Number of REPLACE commands issued.

RENAME

Number of RENAME commands issued.

REMOVE

Number of REMOVE commands issued.

PERMIT

Number of PERMIT commands issued.

REVOKE

Number of REVOKE commands issued.

WHOOWNS

Number of WHOOWNS commands issued.

WHOHAS

Number of WHOHAS commands issued.

LIST

Number of LIST commands issued.

HELP

Number of HELP commands issued.

LOCK

Number of LOCK commands issued.

UNLOCK

Number of UNLOCK commands issued.

WHOAMI

Number of WHOAMI commands issued.

MODIFY

Number of MODIFY commands issued.

ADMIN

Number of ADMIN commands issued.

DEADMIN

Number of DEADMIN commands issued.

MOVE

Number of MOVE commands issued.

REFRESH

Number of REFRESH commands issued.

GENCERT

Number of GENCERT commands issued.

GENREQ

Number of GENREQ commands issued.

EXPORT

Number of EXPORT commands issued.

CHKCERT

Number of CHKCERT commands issued.

MLWRITE

Number of MLWRITE commands issued.

REKEY

Number of REKEY command issued.

ROLLOVER

Number of ROLLOVER commands issued.

Action:

No action necessary.

Note: Command Processor Statistics are only displayed when STATG(ON) is specified. For information on the STATG control option see the *Control Options Guide*.

TSS1323I to TSS1328I

TSS1323I ------ CPF STATISTICS ----------

TSS1324I INBD CMDS PROCESSED	**(000000000)**	**XE15**
TSS1325I INBD PSWD PROCESSED	**(000000000)**	**XE15**
TSS1326I OUTB CMDS PROCESSED	**(000000000)**	**XE15**
TSS1327I OUTB PSWD PROCESSED	**(000000000)**	**XE15**
TSS1328I RETURNED OUTB REQUESTS	**(000000000)**	**XE15**
TSS1324I INBD CMDS PROCESSED	**(000000000)**	**XE11**
TSS1325I INBD PSWD PROCESSED	**(000000000)**	**XE11**
TSS1326I OUTB CMDS PROCESSED	**(000000000)**	**XE11**
TSS1327I OUTB PSWD PROCESSED	**(000000000)**	**XE11**
TSS1328I RETURNED OUTB REQUESTS	**(000000000)**	**XE11**

Reason:

These messages provide statistics on commands issued using CPF. Statistics are listed by node.

INBOUND COMMAND REQUESTS

Number of inbound command requests for a particular node.

INBOUND PASSWORD REQUESTS

Number of inbound password requests for a particular node.

OUTBOUND COMMAND REQUESTS

Number of outbound command requests for a particular node.

OUTBOUND PASSWORD REQUEST

Number of outbound password requests for a particular node.

RETURNED OUTBOUND REQUESTS

Number of rejected commands for a particular node.

Action:

No action necessary.

Note: The CPF Statistics are only displayed when STATG(ON) is specified and CPF is active. For information on the STATG control option, see the *Control Options Guide*.

TSS1309

SAF MODULES REFRESH FAILED

Reason:

The module supplied was invalid for one of the following reasons:

- CA-SAF modules are missing from your CA Top Secret CAILIB or CAILPA.
- An invalid SAF module was entered for individual refresh.

Action:

Contact your Systems Programmer to have the missing modules loaded, or enter a valid SAF module name.

TSS1320E

ADD FAILED. NEW PDS TABLE TOO SMALL

Reason:

While processing a PDSPROT control option statement, an internal table was exceeded. Most likely, an excessive number of PDSPROT statements have been issued.

Action:

Check the number of statements being issued and, if the problem is not apparent, contact CA Technical Support. Execute CAS4STAT.

TSS1321E

REMOVE FAILED. ENTRY NOT FOUND.

Reason:

The data set name, volser, and class combination specified on a PDSPROT(REM...) statement could not be matched against any active PDSPROT entry. The remove function failed.

Action:

Ensure that the PDS data set name and volser have not been reassigned to a different resource class, or removed previously by another user.

TSS1322E

PDSPROT INTERNAL ERROR

Reason:

While processing a PDSPROT statement, an internal control block or module was unexpectedly missing.

Action:

Verify that CA security system initialization messages were seen when the system was IPL'ed. In particular, check that versions of ICHSEC00 or ICHSEC05 provided by CA exist in the active LPA. Contact CA Technical Support for further assistance.

TSS1323E

STORAGE OBTAIN FAILED. PDSPROT ROUTINE.

Reason:

Insufficient storage was available to process a PDSPROT control option statement. The statement is not processed.

Action:

Check storage resources for shortages. If none are found or if the problem persists, contact CA Technical Support. Execute CAS4STAT.

TSS1324E

STORAGE RELEASE FAILED. PDSPROT ROUTINE.

Reason:

An attempt to release storage during the processing of a PDSPROT control option has failed. CA Top Secret will continue.

Action:

This error should be reported to CA Technical Support.

TSS1325E

ADD FAILED. PDSPROT NOT VALID ON SYS1.IMAGELIB

Reason:

PDS protection is inappropriate for SYS1.IMAGELIB. Although colloquially, entries in the data set are referenced as “members,” the data set is not a partitioned data set and is not accessed according to any access method which CA Top Secret would detect as partitioned data set I/O.

Action:

Only data set protection is available on SYS1.IMAGELIB.

TSS1326E

PDSPROT DATA SET NAME EXCEEDS 44 CHARACTERS

Reason:

The PDSPROT data set name exceeds 44 characters, which is the maximum number of characters allowed for a data set name.

Action:

Re-enter the command using a valid data set name.

TSS1350I

SECCACHE QUIESCING AFTER TWICE THE TIMER INTERVAL

Reason:

CA Top Secret is shutting down. The actual shutdown occurs after the TIMER control option cycle has expired twice.

Action:

No action is required. You can enter a SECCACHE(STATUS) command to see when the SECCACHE has been disabled.

TSS1351I

SECCACHE CLEAR SUCCESSFUL

Reason:

A SECCACHE(CLEAR) command was issued and at least one cache entry was cleared.

Action:

No action is required. You can enter a SECCACHE(STATUS) command to see how much data or index area storage was recovered.

TSS1352E

SECCACHE COMMAND FAILED

Reason:

A SECCACHE command was issued to initialize security record cache processing, but one or more input parameters failed a validation check.

Action:

Review the SECCACHE command, and correct any invalid input.

Note: For information about the SECCACHE option, see the *Control Options Guide*.

TSS1353I

SECCACHE IS OFF

Reason:

A SECCACHE(OFF) command was issued to deactivate security record cache processing, or a SECCACHE(CLEAR) or SECCACHE(STATUS) command was issued and the cache was inactive.

Action:

No action is required. Enter a SECCACHE(SIZE=nn,…) command to activate the security record cache process.

TSS1354I—TSS1361I

TSS1354I ---------- SECCACHE STATISTICS ----------

TSS1355I Data Size nnnnnnnnnn In Use nnnnnnnnnn
% Used nnn

TSS1356I Index Size nnnnnnnnnn In Use nnnnnnnnnn
% Used nnn

TSS1357I SHR Wait nnnnnnnnnn EXCL Wait nnnnnnnnnn

TSS1358I Gets nnnnnnnnnn Satisfied nnnnnnnnnn
% Found nnn

TSS1359I Adds nnnnnnnnnn Deletes nnnnnnnnnn
Exp Hrs nnn

TSS1360I NOSPACE nnnnnnnnnn NOINDEX nnnnnnnnnn
Warn % nnn

TSS1361I Low Rcd nnnnnnnnnn High Rcd nnnnnnnnnn
Avg Rcd nnnnnnnnnn

Reason:

These messages provide statistics on how much of the security record cache is used and how efficient it is in improving overall system performance.

Data Size

Maximum number of bytes allocated to the cache.

In Use

Current number of data area bytes in use.

% Used

The percentage of data area bytes in use.

Index Size

Maximum number of index entries allocated to the cache.

In Use

Current number of index entries in use.

% Used

The percentage of index entries in use.

SHR Wait

The number of times cache processing had to wait for a shared enqueue.

EXCL Wait

The number of times cache processing had to wait for an exclusive enqueue.

Gets

Number of get requests made to the cache process.

Satisfied

Number of get requests satisfied by the cache process.

% Found

The percentage of records found on a get request.

Adds

Number of successful add/replace requests.

Deletes

Number of successful delete requests.

Exp Hrs

Number of hours before a cached record is eligible to expire.

NOSPACE

Number of data area allocation requests failing due to no available space.

NOINDEX

Number of index entry allocation requests failing due to no available space.

Warn %

Threshold full level to trigger console warning messages.

Low Rcd

The lowest security record size found in the cache.

High Rcd

The highest security record size found in the cache.

Avg Rcd

The average security record size found in the cache.

TSS1365I

SECCACHE ALREADY ACTIVE

Reason:

A SECCACHE command was issued to initialize security record cache processing but the cache was already active.

Action:

No action is required. A SECCACHE(OFF) command must be entered before the cache can be re-initialized with new parameters.

TSS1366W

SECCACHE Data | Index area is *nnn*% full

Reason:

The data area or index area of the cache reached the *percentage full* threshold (*nnn*%). Sufficient space cannot be recovered automatically to lower the area below the warning level. The security record cache remains active, and records continue to be added until the data area or index area becomes 100% full.

Action:

Attempt to recover space by issuing the following command with an expiration level that is less than the level entered during cache initialization:

`SECCACHE(CLEAR,EXP=`*`hhh`*`)`

hhh

Attempts to recover cache space by deleting existing records that have expired based on the time interval that you specify in hours (*hhh*). This input specification overrides the expiration interval supplied at cache initialization.

Example: Specifying CLEAR,EXP=2 attempts space recovery by deleting records that have expired after 2 hours.

Note: Specifying EXP=0 deletes records based on the expiration interval specified at cache initialization. For example, if you specified EXP=1 at cache initialization and then subsequently specify CLEAR,EXP=0, the product deletes existing records that have expired based on the original 1 setting. To view the expiration level established during initialization, issue the SECCACHE(STATUS) command.

TSS1367I

SECCACHE CLEAR FOUND NO ELIGIBLE ENTRIES

Reason:

A SECCACHE(CLEAR) command was issued to recover space, but no record entries were found to match the input criteria, and no space was recovered.

Action:

No action is required. You can change the input criteria and re-issue the SECCACHE(CLEAR) command to attempt to recover space. For information, see the *Control Options Guide*.

TSS1368I

SECCACHE DATA SPACE CANNOT BE OBTAINED

Reason:

A SECCACHE command was issued to initialize security record cache processing but the data space where the cache is stored could not be obtained. There is either not enough virtual storage defined to meet the requested size, or the number of active SCOPE=COMMON data spaces has exceeded the system setting.

Action:

Ensure that sufficient virtual storage is available to allocate to the data space based on the size requested. You may have to increase the value specified for the MAXCAD parameter within the IEASYSxx member of PARMLIB by one.

TSS1369I

SECCACHE DATA SPACE SERVICES NOT AVAILABLE

Reason:

A SECCACHE command was issued to initialize security record cache processing but the data space services modules could not be found.

Action:

This is an internal error. Contact CA support for assistance.

TSS1401E

SECLABEL|SECLEVEL|CATEGORY|Resource entry not found.

Reason:

An administrative command was issued for the MLS record and the specified entry was not found.

Action:

Reissue the command with the proper entry name or define the entry specified.

TSS1402E

SECLABEL can not be removed - in use'

Reason:

An administrator attempted to remove a SECLABEL that was assigned to one or more resources.

Action:

Remove the SECLABEL from all resources and then reissue the command to remove the SECLABEL.

TSS1403E

Specified SECLEVEL|CATEGORY|SECLABEL is not defined

Reason:

An administrator attempted to add a SECLABEL and the specified SECLEVEL or CATEGORY was not defined. Or an administrator attempted to add a SECLABEL to a resource and the SECLABEL was not defined.

Action:

Define the SECLEVEL, CATEGORY or SECLABEL and reissue the original command.

TSS1405E

Category name already exists

Reason:

An administrator attempted to add a CATEGORY when a specified CATEGORY already exists.

Action:

Reissue the command with a different category name.

TSS1405E

Invalid number of resources specified

Reason:

An administrator attempted to add a SECLABEL to a resource but 0 or more than 1 resource was specified.

Action:

Reissue the command and specify a single resource class and entity name.

TSS1407E

MLS Security is not active

Reason:

A user attempted a function that requires MLS security to be active.

Action:

Reissue the command or execute the function when MLS security is active.

TSS1408

MLWRITE command not available

Reason:

A user issued the MLWRITE command but the MLWRITE(YES) global option is active.

Action:

The command is unnecessary in this environment.

TSS1409I

Write-Down for user is ENABLED|DISABLED

Reason:

The MLWRITE command was issued and the write-down status for the user is displayed.

Action:

No action is required.

TSS1410E

YOU MUST SPECIFY AN MLS RECORD TYPE

Reason:

An Administrator has entered TSS LIST(MLS) only; this command also requires a record type to identify which type to list.

Action:

Re-issue the command giving a record type. Valid record types with the MLS ACID are: SECLEVEL, CATEGORY, SECLABEL, DATA, RESOURCE, or resclass. For more information on the LIST MLS command, see the CA Top Secret *Security for z/OS Multilevel Security Planning Guide*.

TSS1411E

CPFSYSID/CPFNODE ALREADY EXISTS. USE REPLACE

Reason:

An administrator attempted to add a CPFSYSID or CPFNODE and the name specified an existing entry.

Action:

Use the TSS REPLACE command to change options for a CPFSYSID or CPFNODE.

TSS1500E

INVALID SUBJECTDSN LENGTH - TOO LARGE

Reason:

The GENCERT command found a value too long within the SUBJEDSN keyword specification. The keyword specified is in error and displayed at the end of the message text.

Action:

The command ends. Re-enter the command with the correct syntax.

Module:

TSSAUTH1

TSS1501E

NO PRIVATE KEY EXISTS FOR CERTIFICATE

Reason:

The GENREQ command requires a certificate that contains a private key. A private key is not available for this certificate.

Action:

The command ends. Re-enter the command using a certificate that has a private key.

Module:

TSSAUTH1

TSS1502E

CERTAUTH/SITE CANNOT HAVE A KEYRING

Reason:

An attempt was made to ADD a Keyring to acid CERTAUTH or CERTSITE. These acid types cannot have Key rings.

Action:

The command ends. Re-enter the command using a acid other then CERTAUTH or CERTSITE.

Module:

TSSAUTH1

TSS1503E

INVALID CERTIFICATE RENEWAL - CERTIFICATE IN DCDSN DOES NOT MATCH CURRENT CERTIFICATE

Reason:

An attempt was made to renew (REP) a certificate, however the certificate to be renewed did not match the subject's DN, issuer's DN, serial# or public key.

Action:

The command ends. Re-enter the command using matching certificate.

Module:

TSSAUTH1

TSS1504E

MISSING SIGNWITH CERTIFICATE

Reason:

An error occurred retrieving the certificate specified in the SIGNWITH parameter.

Action:

Verify that the certificate exists and that the issuer of the command has proper authority to access the certificate. .

Module:

TSSAUTH1

TSS1501W

NO PRIVATE KEY EXITS FOR CERTIFICATE - ICSF OPTION INVALID

Reason:

(ICSF option only.) A TDD add(*user01*) digicert(*xxxxx*) DCDSN(*xxxx*) ICSF command has been issued but the private key is missing.

Action:

If there is no private key, remove the ICSF keyword and reissue the command.

TSS1505E

PKCS #12 CERTIFICATE WAS REQUESTED - PKCSPASS REQUIRED

Reason:

An EXPORT request was made for a PKCS #12 certificate. PKCS #12 certificates require encryption. The PASSWORD keyword must be supplied with a password that can be used to encrypt the private key and certificates within the PKCS #12 certificate package.

Action:

Re-enter the command specifying a password.

Module:

TSSAUTH1

TSS1506E

XREF TSSACID field name too long

Reason:

The TSSACID field name of the NDT LDAPNODE XREF sub-field, is too long.

Action:

Correct and re-issue the command.

TSS1507E

XREF TSSACID field name is invalid

Reason:

The TSSACID field name of the NDT LDAPNODE XREF sub-field is not a valid ACID field name.

Action:

Correct and re-issue the command.

TSS1508E

XREF field type is invalid

Reason:

The output field type of the NDT LDAPNODE XREF sub-field, is not a valid field type.

Action:

Correct and re-issue the command.

TSS1509E

XREF field format is invalid

Reason:

The output field format of the NDT LDAPNODE XREF sub-field, is not a valid field format.

Action:

Correct and re-issue the command.

TSS1510E

XREF attribute length is invalid

Reason:

The output field length of the NDT LDAPNODE XREF sub-field, is not a valid field length.

Action:

Correct and re-issue the command.

TSS1511E

ADMPSWD or APPLNAME must be specified

Reason:

The ADMDN keyword of an NDT LDAPNODE ADD/REP command, should be accompanied by the ADMPSWD keyword or the APPLNAME keyword.

Action:

Correct and re-issue the command.

TSS1512E

LDAPNODE mandatory keyword missing

Reason:

At least one mandatory keyword is missing when adding a new NDT LDAPNODE definition.

Action:

Correct and re-issue the command.

TSS1513E

LDAPNODE name is undefined

Reason:

The node name specified on an NDT LDAPNODE REP command is undefined.

Action:

Correct and re-issue the command.

This message also displays if LINUXNODE, CPFNODE, and CPFSYSID are not defined.

TSS1514E

Unable to access SAF LDAP node table

Reason:

An error occurred when trying to access the SAF in-core LDAP node table.

Action:

Contact CA Technical Support.

TSS1515E

LDAP OUTBOUND PROCESSING FAILURE

Reason:

An error occurred when processing an LDAP outbound request.

Action:

Contact CA Technical Support.

TSS1516E

(G)ENERIC OPTION NOT SUPPORTED FOR RESOURCE

Reason:

You have incorrectly used the “G” (Generic prefixing indicator) on a command.

Action:

See the *User Guide* for more information about using the (G)eneric indicator.

TSS1517E

CPFSYSID cannot be removed when node entries still exit

Reason:

CPFSYSID can not be removed from the NDT record as long as node entries still exist for the specified CPFSYSID.

Action:

Remove all CPFNODE entries then remove the CPFSYSID.

TSS1518E

CPFNODE not allowed when adding new CPFSYSID definition

Reason:

CPFNODE cannot be added to a CPFSYSID which did not previously exist.

Action:

Create the CPFSYSID entry on the NDT record, then add CPFNODE definitions.

TSS1519E

Invalid Use of Generic Option

Reason:

The resource class already has the GENERIC attribute in the RDT. Permitting or adding a resource in this resource class with the (G) qualifier is superfluous. In the case of pseudo-resources (for example, LCF TRANS, XTRANS, CMD or XCMD), which are considered generic by default, this message may also occur.

Action:

Correct and re-issue the command.

TSS1520E

At least one keyword should be specified

Reason:

At least one keyword should be specified on an NDT LDAPNODE ADD/REP command.

Action:

Correct and re-issue the command.

TSS1521E

XREF field entry does not exist

Reason:

No matching XREF entry was found for an NDT LDAPNODE REM command.

Action:

Correct and re-issue the command.

TSS1522E

Last XREF field can not be removed

Reason:

The last and only XREF entry of an NDT LDAPNODE, can not be removed.

Action:

Correct and re-issue the command.

TSS1523E

ADMPSWD & APPLNAME are mutually exclusive

Reason:

The ADMPSWD and APPLNAME keywords of an NDT LDAPNODE ADD/REP command are mutually exclusive.

Action:

Correct and re-issue the command.

TSS1524E

MUST SPECIFY DATE ALONG WITH TIME

Reason:

A GENCERT request was made and NATIME or NBTIME was specified without supplying NADATE or NBDATE.

Action:

Re-enter the command specifying a NADATE or NBDATE.

Module:

TSSAUTH1

TSS1525E

CERTIFICATE ALREADY EXISTS WITH THIS SERIAL/ISSUERDN

Reason:

A GENCERT request was made but could not generation a new certificate because the same serial#/Issuer's distinguish name already exists in TSS.

Action:

Re-enter the command specifying a different subject distinguish name in order make the certificate's serial#/distinguish name unique.

Module:

TSSAUTH1

TSS1526E

INVALID NATIME SPECIFIED

Reason:

A GENCERT request was made but the NATIME was missing or invalid.

Action:

Re-enter the command specifying the correct time. For example: NATIME(11:15:00)

Module:

TSSAUTH1

TSS1527E

INVALID NBTIME SPECIFIED

Reason:

A GENCERT request was made but the NBTIME was missing or invalid.

Action:

Re-enter the command specifying the correct time. For example: NBTIME(10:15:00)

Module:

TSSAUTH1

TSS1528E ONLY ACID=CERTAUTH CAN HAVE HITRUST STATUS

Reason:

An attempt was made to ADD a Digital Certificate to a user ACID with the keyword of HITRUST. The HITRUST status is reserved for the CERTAUTH user id only.

Action:

If HITRUST option is desired, you must add the certificate to the CERTAUTH user id.

TSS1529E

MISSING KERBUSER

Reason:

An attempt was made to ADD a foreign principal KERBLINK but KERBUSER was not included in the command.

Action:

Re-issue the command with KERBUSER correctly specified.

TSS1530E

KERBSEGM RECORD NOT FOUND

Reason:

An attempt to remove the KERBNAME from an ACID could not be performed because the corresponding SDT entry was missing. The SDT KERBSEGM could be missing because the KERBNAME has already been removed, or because the KERBNAME specified in the REMOVE command does not correspond to the KERBNAME in the ACID and the SDT.

Action:

Perform the command TSS LIST(acid) SEGMENT(KERB) to determine the actual KERBNAME stored on the ACID. Verify that the KERBNAME is missing or that the KERBNAME does not correspond to the value in the REMOVE command. If already removed, there is no action which needs to be taken. If the KERBNAME in your command was incorrect, alter your command to use the correct value for KERBNAME.

TSS1531E

LINKNAME ALREADY EXISTS

Reason:

An attempt was made to ADD a KERBLINK entry, however the LINKNAME already exists in TSS.

Action:

Choose another name for LINKNAME and reenter the command.

TSS1532E

UNDERCUT FAILED - NOT ENOUGH SPACE IN ACID RECx

Reason:

During UNDERCUT processing when resources are being transferred from one ACID to another, it has been determined that the target ACID record does not have enough space to contain all the resources being transferred.

Action:

Remove some other resources from the target ACID and retry the UNDERCUT command.

TSS1533E

CANNOT EXPORT DUE TO PRIVATE KEY IN ICSF

Reason:

An attempt was made to EXPORT a Digital Certificate that has its private key in ICSF storage facility. There is no function of ICSF to extract the key for this process.

Action:

You could export the certificate without the private key using format (CERTDER or CERTB64). If the private key is desired, you must first remove the certificate then re-generate or re-add the certificate without specifying the ICSF option.

TSS1534E

PCICC AND DCDSN ARE MUTUALLY EXCLUSIVE FOR THIS FUNCTION

Reason:

An attempt was made to ADD or GENCERT a certificate using both PCICC and DCDSN keywords. The PCICC keyword implies generating a certificate private/public key pair using the PCICC feature. However, the DCDSN keyword implies a PKCS#10 certificate request that already contains a public key as input. Hence, these keywords are mutually exclusive.

Action:

Decide whether the certificate is to be generated using PCICC or by a PKCS#10 certificate request as input.

TSS1535E

PCICC AND ICSF ARE MUTUALLY EXCLUSIVE FOR THIS FUNCTION

Reason:

An attempt was made to ADD or GENCERT a certificate using both PCICC and ICSF keywords. The PCICC keyword implies generating a certificate private/public key pair using the PCICC feature. However, the ICSF keyword implies generating a certificate that uses software and not PCICC.

or

A RENEW command was issued for a certificate in which the original certificate was in ICSF format and PCICC was specified on the command (or conversely).

Action:

Decide whether the certificate is to be generated using PCICC or by using ICSF software.

TSS1536E

LDS INACTIVE; COMMAND WILL NOT BE EXECUTED OR LOGGED

Reason:

An attempt was made to issue a TSS REM(*LDSRECV) command to remove records from the LDS recovery file. However, the LDS subtask of CA Top Secret is not active.

Action:

Issue a TSS MODIFY(STATUS) to find the current status of LDS. See the LDAP chapter in the *Command Functions Guide.*

TSS1537I

***LDSRECV COMMAND SCHEDULED**

Reason:

A TSS REMOVE(*LDSRECV) command was issued and is schedule to be processed by the LDS service subtask.

Action:

None

TSS1538E LDAPINST Field entry does not exist

Reason:

When trying to REMOVE and LDAPINST entry from a NDT LFDAPNODE record, the Attribute Name provided did not match any of the existing LDAPINST attribute names already defined on the LDAPNODE record.

Action:

Correct the LDAPINST attribute name and retry.

TSS1539E

ROLLOVER NOT DONE - CERTIFICATES HAVE THE SAME LABLCERT

TSS1539E

ROLLOVER NOT DONE - DIGICERT HAS NO PRIVATE KEY

TSS1539E

ROLLOVER NOT DONE - NEWDIGIC HAS NO PRIVATE KEY

TSS1539E

ROLLOVER NOT DONE - NEWDIGIC WAS USED IN SIGNING ANOTHER

TSS1539E

ROLLOVER NOT DONE - WAS PERFORMED ALREADY FOR NEWDIGIC

Reason:

You are attempting to ROLLOVER one certificate to another that contains the same 32-byte label (LABLCERT) name for the certificate being rolled over.

Action:

Verify the NEWDIGIC id specified. Use the LIST and CHKCERT commands to help verify that the records are the ones you intended to specify. The FORCER operand can be used to bypass this test and will allow the ROLLOVER to complete.

TSS1541E

LABLPKDS VALUE IS INVALID

Reason:

If processing the GENCERT, REKEY, or ADD command, LABLPKDS(*) was specified and the LABLCERT that was specified does not conform to the rules for PKDS labels. If processing the REKEY command, LABLPKDS(*) was specified and the LABLCERT specified does not conform to the rules for PKDS labels. PKDS labels may consist of alphanumeric and national characters (@, #, $) and periods. However, only alphabetic or national characters may be the first position in the label.

Action:

Specify a valid LABLPKDS field or specify a LABLCERT field that conforms to the rules for the LABLPKDS field.

TSS1542E

MISSING LABLCERT

Reason:

If processing the GENCERT, REKEY, or ADD command, LABLPKDS(*) was specified and the LABLCERT parameter was not supplied in the command.

Action:

Specify a LABLCERT field, making certain it conforms to the rules for the LABLPKDS field.

TSS1544E

MUTUALLY EXCLUSIVE KEYWORDS SPECIFIED - aaaaaaaa/bbbbbbbb

Reason:

The fields specified in the message text are mutually exclusive and cannot both be set.

Action:

Specify one field or the other, but not both.

Module:

TSSAUTH1

TSS1545E

NISTECC or BPECC was specified but input certificate is not NISTECC or BPECC

Reason:

An attempt to REKEY a certificate was unsuccessful because the private key of the original certificate (DIGICERT) was not BPECC/NISTECC and BPECC or NISTECC was specified for the new key.

Action:

Reissue the REKEY command without the BPECC/NISTECC keyword.

Module:

TSSAUTH1

TSS1545E

DSA and ICSF ARE MUTUALLY EXCLUSIVE FOR THIS FUNCTION

Reason:

An attempt was made to GENCERT or REKEY a certificate using both DSA and ICSF keywords. The DSA keyword implies generating a certificate private/public key pair using the DSA feature. The ICSF keyword implies generating a certificate using software.

Action:

Decide whether the certificate is to be generated using DSA or by using ICSF software.

TSS1546E

Unable to generate Kerberos key for ACID with *NOPW*

Reason:

CA Top Secret requires a substantive user password to generate Kerberos encryption keys. An ACID with PASSWORD(NOPW) cannot accept the KERBNAME operand. An ACID with the KERBNAME operand cannot accept an administered PASSWORD(NOPW).

Action:

For any ACID intended for Kerberos processing, correct the password to contain substantial text. (Not NOPW, which bypasses password processing.)

TSS1547E

DSA and DATAENCRYPT ARE MUTUALLY EXCLUSIVE FOR THIS FUNCTION

Reason:

An attempt was made to GENCERT or REKEY a certificate using both DSA and DATAENCRYPT keywords. The DSA keyword implies generating a certificate private/public key pair using the DSA feature. The DATAENCRYPT keyword implies generating a certificate using software.

Action:

Decide whether the certificate is to be generated using DSA or by using DATAENCRYPT software.

TSS1548I

Password not Changed FAC(facility)

Reason:

A TYPE=USER ACID attempted to alter several facility-specific passwords in a single command for the current acid:

`TSS ADD(acid) FACILITY(fac1,fac2,...) PASSWORD(password) MULTIPW`

The password change was inappropriate for one of the facilities in the command.

Action:

Remove the facility indicated by the message.

TSS1549E

Facility Password not Found FAC(facility)

Reason:

An TYPE=USER ACID attempted to alter a MULTIPW facility-password but the facility specified does not have a password and is covered by the ALL-facility password. Only an administrator has permission to create a new facility specific password where none previously existed

Action:

Consult with your local administrator to make arrangements to create a facility-specific password. Otherwise, alter the ALL-facility password to make changes to the password for the specified facility.

TSS1550E

MISSING ICSF or PCICC KEYWORD

Reason:

If processing the GENCERT, REKEY, or ADD command, LABLPKDS(value) was specified and the ICSF or PCICC keyword was not supplied in the command.

Action:

Specify ICSF or PCICC keyword along with LABLCERT field.

TSS1551E

RECORDS ARE IN VSAM, USE LIST(ACIDS) INSTEAD

Reason:

When using the VSAM option to store digital certificate and certificate keyrings, the LIST(SDT) is no longer valid because the records reside now in VSAM and not the SDT.

Action:

Specify TSS LIST(ACIDS) KEYRING(ALL) or DIGICERT(ALL).

TSS1552E

RECORDS ARE IN SDT, USE LIST(SDT) INSTEAD

Reason:

The LIST(ACIDS) DIGICERT or KEYRING is only valid when using the VSAM option to store digital certificates and keyrings in VSAM data set. These records reside in the SDT.

Action:

Specify TSS LIST(SDT) KEYRING(ALL) or DIGICERT(ALL).

TSS1553I

ICSF NOT ACTIVE

Reason:

An administrator issued a TSS P11TOKEN command, but the ICSF cryptography services were not available.

Action:

Start the ICSF cryptography services and reissue the command.

TSS1554E

TOKEN NOT DEFINED TO ICSF

Reason:

An administrator issued a TSS P11TOKEN command and the LABLCTKN parameter specified a token name that was not defined to ICSF.

Action:

Reissue the command with the correct token name or define the token to ICSF.

TSS1555E

ICSF SERVICES ERROR

Reason:

An administrator issued a TSS P11TOKEN command and command processing terminated because there was an ICSF services error.

Action:

Contact CA Technical Support.

TSS1556E

Certificate in PKCS 11 token cannot be deleted - *error*

Reason:

You are attempting to delete a certificate but there are objects in the certificate that do not exist in the CA Top Secret database.

error

Description of error. For example, the certificate does not exist in CA Top Secret or the private key does not exist in CA Top Secret.

Action:

Verify that the certificate selected can be safely removed. Specify FORCE on the delete or import the objects into CA Top Secret. Retry the delete.

TSS1558E

Error returned from ICSF services. ICSF RC= rc - RSN = rsn

Reason:

An error was returned from ICSF services when processing a certificate request.

Action:

To determine the cause of the error, check the IBM *ICSF Application Programmer's Guide* for information on return code (rc) and reason code (rsn). Correct the error and retry the command.

TSS1559E

P11TOKEN SECURITY ENVIRONMENT ERROR

Reason:

An administrator issued a TSS P11TOKEN command, and an error occurred checking the administrator's authority to the CRYPTOZ resources.

Action:

Contact CA Technical Support.

TSS1560E

Input certificate contains non-RSA public key. Public key cannot be added to ICSF

Reason:

The input certificate contains an invalid public key.

Action:

Verify that the public key is a valid key. If the public key is valid, contact CA Support. If the public key is not valid, specify an input certificate with a valid public key and retry the command.

TSS1561E

Invalid or missing PKDS label. Public key cannot be added to ICSF

Reason:

The PKDS label of the certificate is invalid or missing.

Action:

Specify a valid PKDS label (LABLPKDS) and retry the command.

TSS1562E

Key size of certificate requires PCI Cryptographic Coprocessor. Specify PCICC instead of ICSF

Reason:

You specified a key size that is too large or cannot be used with ICSF, and must be used with PCICC.

Action:

Verify that you have a PCICC coprocessor installed and active, specify PCICC instead of ICSF, and retry the command.

TSS1563E

Old password must be specified when PWVERIFY(YES) is in effect

Reason:

Control option PWVERIFY(YES) is in effect and a user attempted to change their password without providing the old password.

Action:

Specify PASSWORD(oldpswd/newpswd) on the self change password command.

TSS1564E

Old password is not allowed in the context it was specified.

Reason:

Old password was specified for re-verification on a self password change command, in conjunction with other password related keywords which are not allowed when Old password is specified.

Action:

Specify "PASSWORD(oldpswd/newpswd)" without any other password subfields.

TSS1565E

When SECCACHE active change is not allowed for attribute: attribute_name

Reason:

Certain RDT attributes have an impact on how permissions are built into user security records, so it is not allowed to modify these attributes while the SECCACHE facility is active.

Action:

Turn off SECCACHE and retry the RDT modification command.

TSS1566E

Entry count exceeds capacity of field URL

Reason:

Multiple URL field will accept up to 3 URL's.

Action:

Reduce is the number of URL's on LDAPNODE to three or less.

TSS1567E

Action leaves field URL incompletely specified.

Reason:

There must be at least 1 URL in the node.

Action:

Leave at least 1 URL on each LDAPNODE.

TSS1568E

Feature not supported by Security File - CODEPAGE

Reason:

This security file does not support Code pages.

Action:

To use this feature, you must have a R12 and above extended file.

TSS1569E

Feature not supported by Security File - MULTIPLE URLs.

Reason:

This security file does not support multiple URL's.

Action:

To use this feature you must have a R12 extended file.

TSS1570E

NO DELEGATE RECORD FOUND

Reason:

An attempt was made to remove a resource from the DELEGATE record, but the delegate resource was not found.

Action:

Perform a TSS LIST(delegate) command and review delegate resources.

Module

TSSAUTDG

TSS1571E

DELEGATE RECORD ALREADY EXISTS

Reason:

An attempt was made to add a resource to the DELEGATE record and the delegate resource was already found.

Action:

Perform a TSS LIST(delegate) command and review delegate resources.

Module

TSSAUTDG

TSS1572E

Feature not supported by Security File - UNICODE.

Reason:

This security file does not support multiple UNICODE.

Action:

To use this feature you must have an r12 extended file.

TSS1573E

XREF Enclose character is invalid.

Reason:

You have entered an invalid EncloseCharacter for XREF. Valid enclose characters are 'SQ' for single quotes and 'DQ' for double quotes.

Action:

Enter the correct enclose character.

TSS1573E

ATTR SHORT INVALID - MAXPERMIT > 8

Reason:

ATTR(SHORT) is valid only when MAXLEN is 8.

Action:

Use ATTR(LONG), which is equivalent to MAXLEN(44).

TSS1573I

THE CERTIFICATE digicert SIGNER NOT FOUND. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert) but the signing certificate could not be located in CA Top Secret. For the status of a certificate being added to be set with TRUST status, one of the criteria for a non-self signed certificate is that the signer must be within the CA Top Secret data base. The certificate is added as NOTRUST and an informational message is issued.

Action:

To ascribe TRUST to this certificate, locate the signing certificate and add to CA Top Secret, and issue TSS REPLACE command with TRUST keyword.

Module:

TSSAUTCR

TSS1574I

THE CERTIFICATE digicert SIGNER NOT CA. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the signing certificate for the certificate does not reside within the CERTAUTH (CA) ACID. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the signer resides in the CERTAUTH user ID. The certificate is added as NOTRUST and an informational message is issued.

Action:

To ascribe TRUST to this certificate, locate the signing certificate and add to CA Top Secret, and issue TSS REPLACE command with TRUST keyword.

Module:

TSSAUTCR

TSS1575I

THE CERTIFICATE digicert SIGNER NOT TRUSTED. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the signing certificate for the certificate has a NOTRUST status. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the signer has the status of TRUST. The certificate is added as NOTRUST and an informational message is issued.

Action:

To ascribe TRUST to this certificate, update the signing certificate with TRUST status using the TSS REPLACE command.

Module:

TSSAUTCR

TSS1576I

THE CERTIFICATE digicert SIGNER EXPIRED. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the validity date range of the signing certificate being added did not fall within the validity date range. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the signer has not expired. The certificate is added as NOTRUST and an informational message is issued.

Action:

Update the certificate signer by certificate renewal process with valid dates.

Module:

TSSAUTCR

TSS1577I

THE CERTIFICATE digicert SIGNER INVALID. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the validity 'before' date range of the signing certificate being added did not fall within the validity date range. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the signer has a valid start or before date. The certificate is added as NOTRUST and an informational message is issued.

Action:

Update the certificate signer by certificate renewal process with valid dates.

Module:

TSSAUTCR

TSS1578I

THE CERTIFICATE digicert IS INVALID. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the validity 'before' date range of the signing certificate being added did not fall within the validity date range. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the signer has a valid start or before date. The certificate is added as NOTRUST and an informational message is issued.

Action:

Update the certificate signer by certificate renewal process with valid dates.

Module:

TSSAUTCR

TSS1579I

THE CERTIFICATE digicert CA EXPIRED. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the validity date range of the signing CA certificate being added did not fall within the validity date range. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the CA signer has not expired. The certificate is added as NOTRUST and an informational message is issued.

Action:

Update the certificate signer by certificate renewal process with valid dates.

Module:

TSSAUTCR

TSS1579E

CERTIFICATE ALREADY DEFINED TO CA TOP SECRET

Reason:

A TSS P11TOKEN IMPORT command was issued and the digital certificate to be imported to the security file already exists in the file.

Action:

Correct the command.

TSS1580E

KEYWORD IDMAP IS MISSING OR INVALID

Reason:

The IDMAP identify is either missing or invalid and this keyword is require for administrating IDMAP records.

Action:

Reenter TSS command and specify correct IDMAP value.

Module:

TSSAUTH1

TSS1580I

THE CERTIFICATE digicert IS EXPIRED. ADDING CERTIFICATE WITH NOTRUST STATUS

Reason:

An attempt was made to add a certificate (as specified in digicert), but the validity date range of the certificate being added did not fall within the validity date range. For the status of a certificate being added to be set with TRUST status, one of the criteria is that the certificate is not expired. The certificate is added as NOTRUST and an informational message is issued.

Action:

Update the certificate by certificate renewal process with valid dates.

Module:

TSSAUTCR

TSS1581E

Maximum # of CFPNODE entries exceeded for a single CPFSYSID

Reason:

You have exceeded the maximum amount of storage for the CPFNODES for a single CPFSYSID; the value cannot exceed 32767, which allows for 200 CPFNODE entries. The new node is not added.

Action:

Reenter the command, adjusting the input values so you do not exceed 32767.

TSS1582E

YOUR MUST SPECIFY KEYWORD IDMAPDN

Reason:

This message appears when you are adding an IDMAP record and the keyword IDMAPDN is missing. You must specify the IDMAP Distinguished Name using the keyword IDMAPDN when administering IDMAP records to TSS.

Action:

Enter the keyword IDMAPDN with the TSS ADD(acid) IDMAP command.

Module:

TSSAUTH1

TSS1583E

IDMAP NOT FOUND

Reason:

The IDMAP record was not found.

Action:

Reenter the TSS command and specify the correct IDMAP value.

Action:

Enter the correct keyword IDMAP.

Module:

TSSAUTH1

TSS1584E

YOU MUST SPECIFY KEYWORD IDMAP

Reason:

IDMAPRN, IDMAPDN, or IDLABEL keyword was entered, but the associated keyword IDMAP was missing.

Action:

Specify a unique IDMAP value.

Module:

TSSAUTH1

TSS1585E

IDMAP ALREADY EXISTS

Reason:

During the adding of an IDMAP record, the value specified in IDMAP was already found in the TSS security file.

Action:

Enter a unique IDMAP value.

Module:

TSSAUTH1

TSS1586E

IDMAPDN/IDMAPRN ALREADY EXISTS

Reason:

During the adding or replacing of an IDMAP record, the value specified in IDMAPDN, IDMAPRN, or both was already found in the IDMAP records.

Action:

Enter a unique IDMAPDN and/or IDMAPRN value.

Module:

TSSAUTID

TSS1587E

IDLABEL AREADY EXISTS FOR THIS USERID

Reason:

During the adding or replacing of an IDMAP record, the value specified in IDLABEL was already found for this USERID within the IDMAP records.

Action:

Enter a unique IDLABEL value.

Module:

TSSAUTID

TSS1588E

LABLPKDS AND FROMICSF ARE MUTUALLY EXCLUSIVE

Reason:

Both the LABLPKDS and FROMICSF keywords were specified on a GENCERT command. Only one keyword may be used.

Action:

Reissue the command, specifying the LABLPKDS or FROMICSF.

TSS1589E

MORE THAN 12 SYMXCERT VALUES

Reason:

A TSS PERMIT command for SYMXCERT labels was attempted, and the list of labels contained more than 12 entries.

Action:

Examine the syntax of the command entered because you may only specify 12 labels.

TSS1590E

MORE THAN 12 SYMXKEYS VALUES

Reason:

A TSS PERMIT command for SYMXCERT labels was attempted, and the list of labels contained more than 12 entries.

Action:

Examine the syntax of the command entered because you may only specify 12 labels.

TSS1591E

ACTION(ADMIN) invalid for resource type ACID

Reason:

ACTION(ADMIN) is invalid on a PERMIT if ACID(acidname) is specified.

Action:

No action required.

TSS1592E

YOU MUST SPECIFY KEYWORD IDMAPRN

Reason:

During the adding of an IDMAP record, the keyword IDMAPRN is missing. You must specify the IDMAP Registry Name using the keyword IDMAPRN when administering IDMAP records to TSS.

Action:

Enter the keyword IDMAPRN with the TSS ADD(acid) IDMAP command.

Module:

TSSAUTH1

TSS1593E

KEYWORD INTO IS MISSING OR INVALID

Reason:

On a LIST, DELETE or MODEL command the keyword ARCHIVE was specified, however the INTO keyword was missing or invalid.

Action:

Reenter the command with a valid INTO keyword.

Module:

TSSAUTH1

TSS1594I

ARCHIVE FUNCTION SUCCESSFUL

Reason:

On a LIST or DELETE command the keyword ARCHIVE was specified, and the archive function executed successfully.

Action:

None.

Module:

TSSAUTAR

TSS1595E

ARCHIVE FUNCTION FAILED IN TSS*xxxxxx*

Reason:

Keyword ARCHIVE was specified on a LIST or DELETE command, but the archive function failed.

TSS*xxxxxx*

Identifies the module where the error occurred.

Action:

Contact CA Top Secret Support.

Module:

TSSAUTAR

TSS1596E

Invalid IDMAP data Rsn = xxxxxxxx

Reason:

An invalid IDMAP data value was detected.

Action:

Contact CA Top Secret support.

Module:

TSSAUTID

TSS1597E

UTF8 Conversion Error, RC=ccc RSN=rrr

Reason:

The IBM conversion service CUNSCSMA returned a data field conversion error.

Action:

Contact CA Top Secret support.

Module:

TSSAUTID

TSS1598E

ARCHIVE AFILE PROCESSING FAILED – REASON CODE = nn

Reason:

On a LIST or DELETE command the keyword ARCHIVE was specified, and the archive function failed. The following reason codes may apply:

- 04—No list output buffer generated
- 08—No address found for module TSSCFJ
- 12—Storage obtain failed
- 16—No command output buffer generated
- 20—Empty buffer found for command file

Action:

Contact CA Top Secret support.

Module:

TSSAUTAR

TSS1599E

Cannot overwrite existing LABLPKDS with RENEW command

Reason:

An attempt was made to RENEW a certificate using a LABLPKDS keyword. However, the certificate being renewed already has a LABLPKDS.

Action:

To change the LABLPKDS value, generate a new certificate. To renew the certificate without changing the LABLPKDS value, issue the RENEW command without the LABLPKDS keyword.

TSS1600E

KEYWORD ARCHIVE IS MISSING

Reason:

On a LIST or DELETE command the keyword INTO was specified, however the ARCHIVE keyword was missing.

Action:

Reenter the command and specify both the ARCHIVE and INTO keywords.

Module:

TSSAUTH1

TSS1601E

KEYWORD USING IS MISSING

Reason:

On a MODEL or COMPARE command the keyword USING was not specified.

Action:

Reenter the command, specifying the USING keyword.

Module:

TSSAUTH1

TSS1602E

KEYWORD ACID IS MISSING

Reason:

On a MODEL command the keyword ACID was not specified.

Action:

Reenter the command using the ACID keyword.

Module:

TSSAUTH1

TSS1603E

THE INTO DATASET MUST BE A PDS - REASON CODE = 12

Reason:

On a MODEL or LIST command LIST with the ARCHIVE keyword, the specified INTO dataset was not a PDS format dataset or the member name was not valid. The member name may not start with a number.

Action:

Reenter the command, specifying an INTO dataset that is in PDS format and verifying that the member name is valid.

Module:

TSSAINTO

TSS1604E

OUT OF SPACE - PDS TOO SMALL

Reason:

On a MODEL or LIST command with the ARCHIVE keyword, the dataset specified in the INTO keyword was too small and a D37 abend occurred.

Action:

Ensure that the dataset specified in the INTO keyword is large enough and reenter the command.

Module:

TSSAINTO

TSS1606E

COMPARE ACOMP PROCESSING FAILED - REASON CODE = nn

Reason:

The COMPARE command failed. Possible reason codes:

- 1 Bad RACVT
- 2 First ACID buffer failed
- 3 Second ACID buffer failed
- 4 Bad Getmain for ACID 1
- 5 Bad Getmain for ACID 2

Action:

Informational message, none.

Module:

TSSACOMP

TSS1607E

INVALID ACID TYPE FOR COMPARE

Reason:

For the COMPARE command, an acid type other than user was specified.

Action:

Reenter the command and specify a acid type of user.

Module:

TSSAUTH1

TSS1608E

ACID VALUE FOR KEYWORD USING MISSING

Reason:

On a COMPARE command, an acid value was not specified for the USING keyword.

Action:

Reenter the command and specify an acid value for the USING keyword.

Module:

TSSAUTH1

TSS1609E

UNABLE TO UPDATE VSAM FILE - DRC=XX

Reason:

CA Top Secret was unable to update the VSAM file for the command issued.

Action:

Due to the number of Detailed Reason Code possibilities and their dynamic nature, contact CA Technical Support to resolve the issue.

TSS1610E

Not Authorized to use NOPW keyword

Reason:

The user is not authorized to set a NOPW password value.

Action:

To set a password as NOPW you must have UPDATE access to entity TSSCMD.USER.*cmd*.NOPW in the CASECAUT resource class.

cmd

Specifies the command being issued.

Limits: CREATE, ADDTO, or REPLACE

TSS1611E

DUPLICATE VALUES NOT ALLOWED FOR COMPARE AND USING ACIDS

Reason:

On a COMPARE command, the acids specified for COMPARE and USING were the same.

Action:

Reenter the COMPARE command and specify different acids for COMPARE and USING.

Module:

TSSAUTH1

TSS1612E

INVALID VALUE FOR KEYWORD SIGNALG

Reason:

An attempt to GENCERT or REKEY a certificate was unsuccessful due to an invalid value specified in keyword SIGNALG or SIGNALG(SHA256) was specified along with DSA keyword. SHA256 is not valid for DSA.

Action:

Reissue the command with correct value for keyword SIGNALG. Valid values are SHA1 and SHA256 for non-DSA and SHA1 for DSA.

Module:

TSSAUTH1

TSS1613E

ICSF or PCICC was specified but input certificate is NISTECC or BPECC

Reason:

An attempt to REKEY a certificate was unsuccessful because the private key of the original certificate (DIGICERT) was not BPECC/NISTECC and BPECC or NISTECC was specified for the new key.

Action:

Reissue REKEY without the BPECC/NISTECC keyword.

Module:

TSSAUTH1

TSS1614E

CANNOT DOWNGRADE PRIVATE KEY FROM ECC

Reason:

An attempt to REKEY a certificate was unsuccessful because the private key of the original certificate (DIGICERT) was BPECC/NISTECC and DSA was specified for the new key.

Action:

Reissue the REKEY command without the DSA keyword.

Module:

TSSAUTH1

TSS1615E

Not Authorized to set MSCA password

Reason:

The user is not authorized to set a new password value for the MSCA.

Action:

To set a password for the MSCA an SCA must have UPDATE access to entity TSSCMD.USER.cmd.MSCAPW in the CASECAUT resource class , where ‘cmd' is ADDTO or REPLACE.

TSS1616E

SIGNALG CANNOT BE USED WHEN NISTECC OR BPECC IS SPECIFIED

Reason:

An attempt to GENCERT a certificate was unsuccessful because the keyword NISTECC or BPECC was specified, and these keywords are not compatible with the SIGNALG keyword.

Action:

Do *one* of the following:

- Reissue the GENCERT command without the BPECC/NISTECC keyword.
- Remove SIGNALG and reissue the GENCERT command with one of the ECC options.

Module:

TSSAUTH1

TSS1617E

BPECC and DATAENCRYPT CANNOT BE SPECIFIED TOGETHER

NISTECC and DATAENCRYPT CANNOT BE SPECIFIED TOGETHER

Reason:

The fields specified in the message are mutually exclusive and cannot be used together. For information about why these fields cannot be used together, see the *Command Functions Guide*.

Action:

Specify one field or the other, but not both.

Module:

TSSAUTH1

TSS1618E

ACF0A213 Input certificate contains non-RSA public key. Public key cannot be added to ICSF

Reason:

The public key is not an RSA public key. Only RSA public keys can be added to ICSF.

Action:

Verify the certificate being inserted is an RSA certificate. If it is, contact CA Support at http://supportconnect.ca.com. If the public key is not valid, specify an input certificate with an RSA public key and retry the command.

Module:

TSSAUTTK

TSS1619E

THE IDMAP DISTINGUISHED NAME IS INVALID AND MUST BE CORRECTED

Reason:

The distinguished name of the IDMAP record is incorrect. For z/OS Release 1.13 and higher, CA Top Secret normalizes the distinguished name of an exiting IDMAP record when the record is being updated.

Action:

Change the distinguished name to a valid value and rerun the command.

Module:

TSSAUTID

TSS1620I

Certificate has a private key that cannot be inserted – Certificate inserted without the private key

Reason:

You attempted to insert a private key that CA Top Secret does not support. CA Top Secret allows only RSA, DSA, NISTECC, and BPECC private keys to be added into its database. The certificate was inserted without the private key.

Action:

None. This message is informational.

TSS1621W

{ORG|USER} ACID (*acid_name*) has reached 80% of maximum allowed size

Reason:

The record size of the ACID has reached 80% of the maximum allowable size.

acid_name

Specifies the name of the ACID.

Action:

Monitor the size of the ACID to ensure that the ACID does not exceed the maximum size. For an organizational ACID, review resources that are owned by the ACID and consider transferring ownerships to other organizational ACIDs. For a user ACID, review resource permissions and consider using profiles, which let you group together users who can share access authorizations for protected resources.

Note: For more information about using profiles, see the *CA Top Secret User Guide*.

TSS1622E

***acid_name* IS A SPECIAL ACID THAT IS NOT ALLOWED WITH COMPARE**

Reason:

Special ACIDs (such as an ALL, STC, FDT, or RDT record) are not allowed in the TSS COMPARE command. CA Top Secret discontinues the comparison.

Action:

No action is required.

Module:

TSSACOMP

TSS1623E

ARCHIVE SORT PROCESSING FAILED

Reason:

An internal error occurred during TSS ARCHIVE command processing. Possible causes are as follows:

- The REGION size on the CA Top Secret startup procedure is too small.
- An abend occurred.
- After a restart, CA Top Secret now points to a different security file.

Action:

Make adjustments—for example, adjusting the startup procedure REGION size—if you can diagnose the problem. If the problem persists, contact CA Support.

Module:

TSSACOPY

TSS1624I

CERTIFICATE *cccccccc* HAS BEEN ADDED TO USER *uuuuuuuu*

Reason:

A digital certificate with identifier *cccccccc* has been added to the specified user.

Action:

No action is required.

TSS1625I

Uuuuuuuu* CERTIFICATE *ccccccc* HAS BEEN PLACED IN *dataset

Reason:

During a successful EXPORT request, a digital certificate was placed in the specified data set.

Action:

No action is required.

TSS1626W

{PKCS#12|PKCS#7} EXPORT PACKAGE WAS CREATED BUT WAS INCOMPLETE

Reason:

One of the signing certificates was expired or not installed as a CERTAUTH certificate. A PKCS #12|PKCS#7 certificate package contains the end-entity certificate and all signing certificates in the hierarchy (including the self-signed root certificate).

Action:

If you require a complete PKCS #12|PKCS#7 certificate package, make sure all signing certificates are installed under CERAUTH and are not expired, then re-enter the command.

TSS1627E

CLOSE ERROR ON PDS - RETURN CODE B14

Reason:

On a MODEL or LIST command with the ARCHIVE keyword, the data set specified in the INTO keyword had a close error.

Action:

Ensure that the data set was defined correctly. For example, you can review the record length or block size, or you can verify that the data set is defined as a PDS.

Review the accompanying WTO console message to obtain the B14-*xx* return code, then see the IBM *z/OS MVS System Messages* guide for more information about the return code.

Module:

TSSAINTO

TSS1628I

Cannot REMOVE – Certificate has been GENREQed

Reason:

You attempted to remove a certificate that was previously the source of a GENREQ command. If the certificate is deleted, the private key associated with the GENREQ data set is no longer available.

Action:

Specify the following command to force the removal the certificate from the user:

```
TSS REMOVE(u) DIGICERT(d) FORCE
```

TSS1629I

Unable to send IBM ENF Signal for command

Reason:

An ENF type 71 signal that was issued during TSS command execution failed to complete. The product sends this signal to notify an application about a particular change that a security administrator made to the security record of an ACID. The application can then take action (for example, immediately refresh the security record in a CICS remote region).

Action:

Contact CA Support if the problem persists.

Module:

TSSAUTH2

TSS2000I to TSS2069E

TSS2000I

CA Top Secret MSTR INITIALIZATION IN PROGRESS

Reason:

This is an informational message indicating that Master Scheduler Initialization has begun.

Action:

No action required.

TSS2001I

CA Top Secret MSTR INITIALIZATION COMPLETE

Reason:

This is an informational message indicating that Master Scheduler Initialization has completed.

Action:

No action required.

TSS2002I

CA Top Secret MSTR SAF INITIALIZATION VERIFIED

Reason:

This is an informational message indicating that SAF initialization was verified.

Action:

No action required.

TSS2003I

CA Top Secret MSTR SAF REPLACEMENT SUCCESSFUL

Reason:

The SAF interface has been properly installed.

Action:

No action required.

TSS2004I

CA Top Secret MSTR SAF INSTALLATION SUCCESSFUL

Reason:

The CA Top Secret SAF interface has been properly installed.

Action:

No action required.

TSS2020E

CA TSS MSTR INITIALIZATION FAILURE

Reason:

One or more errors have occurred during Master Scheduler Initialization.

Action:

Check other messages to determine the problem. An IPL, other actions, or both may be necessary.

TSS2021E

CA TSS MSTR IPL IS REQUIRED TO CORRECT ERRORS

Reason:

An error occurred that can only be corrected by a system IPL.

Action:

Check other messages to determine cause of problem. An IPL is necessary.

TSS2022E

CA TSS MSTR TERMINATED WITH USER 2000-nn ABEND

Reason:

An error occurred during Master Scheduler Initialization.

Action:

Check other messages to determine cause of problem. The ABEND reason code 'nn' will match the last two characters of the matching error message. For example, if the user ABEND code reason is '34', then a TSS2034E message will also be issued with other problem related information. An IPL may be necessary.

TSS2023E

CA Top Secret MSTR TERMINATED BY SYSTEM xxx-nnnn ABEND

Reason:

An error occurred during Master Scheduler Initialization.

Action:

Check other messages to determine cause of problem. An IPL may be necessary.

TSS2024W

CA Top Secret MSTR INITIALIZATION COMPLETED WITH ERROR(S)

Reason:

An error has occurred during Master Scheduler Initialization.

Action:

Check other messages to determine the cause of problem. An IPL will not be required, however may still be advised.

TSS2025I

CA TSS MSTR COMPLETE SDUMP TAKEN

Reason:

An error occurred during MSI processing resulting in an SDUMP.

Action:

Check other messages to determine the cause of the problem. Dump analysis may be required.

TSS2026I

CA Top Secret MSTR PARTIAL SDUMP TAKEN

Reason:

An SDUMP has been taken, due to errors during Master Scheduler Initialization.

Action:

Check other messages to determine cause of problem. Dump analysis may be required.

TSS2027I

CA Top Secret MSTR SDUMP FAILED - NO DUMP TAKEN

Reason:

A SDUMP was attempted, but no dump data sets were available.

Action:

Check other messages to determine cause of problem.

TSS2030E

CA TSS MSTR TSSMSI00 NOT AUTHORIZED

Reason:

TSSMSI00 was invoked in an unauthorized fashion.

Action:

Relink TSSMSI00 with AC(1) specified, and IPL.

TSS2031E

CA TSS MSTR module WORK AREA GETMAIN FAILED

Reason:

A work area GETMAIN failed during Master Scheduler Initialization.

Action:

Check other related messages, correct the error, and IPL.

TSS2032E

(NO MESSAGE)

Reason:

An error occurred during WTO processing, during Master Scheduler Initialization.

Action:

Check any other related messages, correct the error and IPL.

TSS2033E

CA Top Secret MSTR UNABLE TO ESTABLISH ESTAE - RC nn-nn

Reason:

An error occurred in ESTAE processing, during Master Scheduler Initialization.

Action:

Check any other related messages, correct the error.

TSS2034E

CA Top Secret MSTR NOT INVOKED BY MASTER SCHEDULER

Reason:

TSSMSI00 has been improperly invoked, for example as a started task. TSSMSI00 is intended to be invoked by IEEMB860 (Master Scheduler Initialization) in ASID 1 only.

Action:

No action required.

TSS2035E

CA Top Secret MSTR MODULE TSSFRVT LOAD FAILED - RC nn-nn

Reason:

Module TSSSFRVT is not in the LINKLST, or has invalid attributes.

Action:

Reinstall module TSSSFRVT and IPL.

TSS2036E

CA Top Secret MSTR MODULE TSSSFRVT CORRUPTED OR INVALID

Reason:

Module TSSSFRVT has been corrupted or failed other checking.

Action:

Reinstall module TSSSFRVT and IPL.

TSS2037E

CA Top Secret MSTR SAFV GETMAIN FIELD - RC nn

Reason:

Module TSSMSI00 was unable to obtain sufficient CSA for the SAF vector table.

Action:

Check for other messages. An IPL will be necessary to correct the problem.

TSS2038E

CA Top Secret TSSFR00 INSTALLATION FAILED - RC 00000

Reason:

TSSMSI00 was unable to properly install TSSSFR00 - the MVS SAF router.

Action:

Check for other messages. An IPL will be necessary to correct problem.

TSS2039W

CA Top Secret MSTR MASTER ADDRESS SPACE ACEE CREATE FAILED

Reason:

An error occurred while processing the security environment for the Master Scheduler address space (ASID 1).

Action:

Check for other messages. An IPL may be necessary to correct the problem.

TSS2041E

CA Top Secret MSTR SVA CODE GETMAIN FAILED - RC nn

Reason:

TSSMSI00 was unable to NOOP the RACF SVCs. This is performed to allow the opening of data sets with the DSCB-1 RACF bit set prior to starting CA Top Secret.

Action:

Check for other messages. Unless System 913-38 abends occur prior to the start of CA Top Secret, no IPL will be required to correct the problem.

TSS2042E

CA Top Secret MSTR SVCUPDATE FAILED - RC nn-nn

Reason:

TSSMSI00 was unable to NOOP the RACF SVCs. This is performed to allow the opening of data sets with the DSCB-1 RACF bit set prior to starting CA Top Secret.

Action:

Check for other messages. An IPL may be required.

TSS2050E

CA Top Secret MSTR LINK TO TSSMSI00 FAILED WITH Sxxx-nn

Reason:

Module TSSMSI00 could not be found or has invalid attributes. TSSMSI00 must be located in the LINKLIST or LPA.

Action:

Check for other messages. An IPL may be required.

TSS2051E

CA Top Secret MSTR LOAD OF TSSMSI00 FAILED WITH Sxxx-nn CA TSS MSTR TSSMSI00 SUBTASK ATTACH FAILED nn

Reason:

Module TSSMSI00 could not be found or has invalid attributes.

Action:

Check for other messages. An IPL may be required.

TSS2060I

Subsystem xxxxxxxx is Waiting for TSS Initialization

Reason:

CA Top Secret has suspended the subsystem pending full security system availability.

Action:

None.

TSS2061E

Startup override options exceed maximum length and are ignored

Reason:

The total length of the startup override options in the SYS1.PARMLIB member CAITSSxx exceeds the maximum length of 100 characters.

Action:

Specify startup override options of 100 characters or less.

TSS2062I

Generated start command: *<start command>*

Reason:

This message displays the generated START command, including any override control options, when CA Top Secret is autostarted as a subsystem using SYS1.PARMLIB member CAITSSxx.

Action:

None.

TSS2063E

KEYWORD NOT IN PARM TABLE, KWD: XXXXXXXX

Reason:

An unsupported keyword was specified in SYS1.PARMLIB member CAITSSxx.

Action:

Correct or remove the keyword causing the error.

TSS2064E

PARMLIB OPERAND ERROR FOR KEYWORD XXXXXXXX

Reason:

An invalid value was specified for a keyword in SYS1.PARMLIB member CAITSSxx.

Action:

Specify a valid value for the keyword causing the error.

TSS2065E

INVALID PARM BUFFER ADDRESS

Reason:

An invalid buffer address was detected for building the startup override options.

Action:

Contact support.

TSS2066E

PARMLIB FILE NAME INVALID, NAME: XXXXXXXX

Reason:

The specified SYS1.PARMLIB member name is not in the format of CAITSSxx.

Action:

Contact support.

TSS2067E

INVALID VALUE FOR SUBSYSTEM NAME

Reason:

The specified subsystem name is not in the correct format.

Action:

Enter a subsystem name value in the format TS*xx*.

TSS2068E

PARM DATA MOVE FAILED, KWD: XXXXXXXX

Reason:

The specified keyword value could not be moved to the output buffer.

Action:

Contact support.

TSS2069I

Subsystem xxxx is Active

Reason:

The specified subsystem has been activated.

Action:

None.

TSS2070E

SAF UID|GID TABLE UPDATE FAILED FOR ACID *user_name|group_name*

Reason:

A TSS command or getUMAP/getGMAP callable service call failed to update the SAF UID/GID table. The UID/GID was added to the user.

Action:

Issue the F TSS,OMVSTABS command to update the table. If the command fails, contact CA Support.

TSS5587E to TSS5858E

TSS5587E

AUDIT FILE SYNAD ERROR:

Reason:

An unrecoverable I/O error has occurred while accessing the Audit/Tracking File. Execution terminates with a Return Code of 24. This message includes detailed information about the error in the “TEXT” field, as follows:

Column	Contents
1-6	Type of operation attempted.
8-22	General description of error.
24-37	Actual track address and block number at which error occurred (BBCCHHR in hexadecimal form).
39-44	Access method used

Action:

No action required.

We suggest that you enter the 53E ABEND into the System Recovery Table (SRT) as a recoverable ABEND. This avoids a CICS failure in the event any CA Top Secret generated subtasks fail. See the *Implementation: CICS Guide* for more details.

TSS5800E

VXPROXY FORMAT IS (REM_NODE,REM_USER,LOCAL_USER)

Reason:

This message was issued in response to a format error in using the VXPROXY keyword.

Action:

Reissue the command using the indicated syntax.

TSS5858E

EXTENT OVERFLOW IN NDT RECORD

Reason:

A serious internal error occurred during command processing. The NDT record structure was inconsistent and resulted in an overflow.

Action:

Contact CA Technical Support.

TSS6000I to TSS6099I

TSS6000I

TSS/CICS INITIALIZATION PHASE 1 STARTED

Reason:

CICS has determined that external security is required and issues a RACLIST which prompts TSS/CICS to begin its initialization.

Action:

No action required.

Module:

TSSCINIT

TSS6002I

TSS/CICS INITIALIZATION PHASE 2 STARTED

Reason:

CA Top Secret/CICS has entered Phase 2 of its initialization and is setting up its event points.

Action:

No action required.

Module:

TSSTCINT

TSS6003I

TSS/CICS INITIALIZATION PHASE 2 COMPLETED

Reason:

CA Top Secret/CICS event points set, Phase 2 of 3 completed.

Action:

No action required.

Module:

TSSTCINT

TSS6004I

TSS/CICS INITIALIZATION PHASE 3 STARTED

Reason:

CA Top Secret/CICS has entered Phase 3 of its initialization and is performing the TSS/CICS subsystem initialization.

Action:

No action required.

Module:

TSSTCINT

TSS6005I

TSS/CICS INITIALIZATION PHASE 3 COMPLETED

Reason:

CA Top Secret/CICS subsystem initialization complete, Phase 3 of 3 completed.

Action:

No action required.

Module:

TSSTCINT

TSS6006I

TSS/CICS SECURITY INACTIVE

Reason:

CA Top Secret/CICS FMID has been installed. If the region MASTFAC facility has FACMATRX=YES, then EXTSEC=NO in the facility has suppressed CA Top Secret/CICS security for the region. If the MASTFAC facility has FACMATRX=NO, then the SIT parameter SEC=NO (for CICS 3.3 and above) or EXTSEC=NO (for CICS 2.1 and below) suppresses CA Top Secret/CICS security for the CICS region.

For CICS release 4.1 and above, the region jobname will also appear in the message text.

Action:

No action required. To bring up the region with active security, modify the MASTFAC facility or alter the appropriate SIT parameter. Recycle the CICS region.

Module:

TSSTCINT/TSSCRT

TSS6007I

TSS/CICS SECURITY ACTIVATED

Reason:

CA Top Secret/CICS security has been activated for this CICS region.

For CICS release 4.1 and above, the region jobname will also appear in the message text.

Action:

No action required.

Module:

TSSTCINT/TSSCRT

TSS6008I

TSS/CICS TERMINATION STARTED

Reason:

CA Top Secret/CICS shutdown phase has started.

Action:

No action required.

Module:

TSSTCINT

TSS6009E

TSS/CICS ERROR TERMINATION CALL PROCESSING

Reason:

This message is generated during Phase 2 initialization. CA Top Secret/CICS has determined this is not a CICS region. No AFCB address was found, or CICS's AFCB header was not identified as “AFCX.”

Action:

No action required.

Module:

TSSTCINT

TSS6010I

TSS/CICS TERMINATION COMPLETED

Reason:

CA Top Secret/CICS has completed its termination process.

Action:

No action required.

Module:

TSSTCINT

TSS6011E

TSS/CICS PM ATTACH PROCESSING ERROR

Reason:

CA Top Secret/CICS has attempted to attach subtask DFHTSPM0 but the attach request failed.

Action:

Examine register 15 for attach return code. If LSQA shortage, lower CICS region size by 500k.

Module:

TSSCPI/TSSCRT

TSS6012E

TSS/CICS CM ATTACH PROCESSING ERROR

Reason:

CA Top Secret/CICS has attempted to attach subtask DFHTTSM0 but the attach request failed.

Action:

Examine register 15 for attach return code. If LSQA shortage, lower CICS region size by 500k.

Module:

TSSCPI

TSS6013E

TSS/CICS EXTSEC=NO PARAMETER INVALID

Reason:

An attempt to set the EXTSEC parameter to NO was denied due to no SYSID entry for this CICS region in the Facilities SYSID Bypass List.

Action:

Add the SYSID of the region to the Facilities Bypass List.

Module:

TSSCPI/TSSCRT

TSS6014I

TSS/CICS EXTSEC=YES PARAMETER IS FORCED

Reason:

No SYSID entry in the Facilities Bypass List was found, so the attempt to alter this parameter was overridden. External security remains in force.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6015I

TSS/CICS PTSCECB1 POSTED

Reason:

The Facility Matrix External Security Initialization Parameters have overlayed the DFHSIT Security Initialization Parameters.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6016I

TSS/CICS PTSCECB2 POSTED

Reason:

CA Top Secret/CICS program manager subtask initialization complete.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6017I

TSS/CICS PTSCECB3 POSTED

Reason:

CA Top Secret/CICS storage manager subtask initialization complete.

Action:

No action required.

Module:

TSSCPI

TSS6018E

TSS/CICS TSSCPI PROCESSING ERROR

Reason:

CA Top Secret/CICS subtask attach failure.

Action:

No action required.

Module:

TSSCPI

TSS6019E

TSS/CICS FREEMAIN ERROR FOR THE PTCB SP=230

Reason:

FREEMAIN was successful for CA Top Secret/CICS Product Token Control Block.

Action:

Contact CA Top Secret Support Center.

Module:

TSSCPI

TSS6020E

TSS/CICS SUBTASK MANAGER ATTACH FAILURE

Reason:

CA Top Secret/CICS signon subtask manager attach has failed. (DFHTRAC0)

Action:

Examine register 15 for attach return code.

Module:

TSSCSMGR

TSS6021E

TSS/CICS GETMAIN ERROR TSSCPTCB SP=230

Reason:

GETMAIN unsuccessful for CA Top Secret/CICS Product Token Control Block. (4000 bytes/SP230)

Action:

Reduce CICS region size by 500k.

Module:

TSSCPI

TSS6022E

TSS/CICS GETMAIN ERROR TSSCCMGR SP=230

Reason:

CA Top Secret/CICS control block getmain failure.

Action:

Reduce CICS region size by 500k.

Module:

TSSCPI/TSSCRT

TSS6023E

TSS/CICS FREEMAIN ERROR TSSCCMGR SP=230

Reason:

CA Top Secret/CICS control block FREEMAIN failure

Action:

Contact CA Technical Support.

Module:

TSSCPI

TSS6024E

TSS/CICS INITIALIZATION SUBTASK GETMAIN ERROR

Reason:

STCB getmain failure. (700 bytes/SP=230/24-bit)

Action:

Reduce CICS region size by 500k.

Module:

TSSCPI/TSSCRT

TSS6025E

TSS/CICS INITIALIZATION SUBTASK LOGIC ERROR

Reason:

TSSCPM program logic error. Invalid PTS$ECB3 function request.

Action:

Contact CA Technical Support.

Module:

TSSCPI/TSSCRT

TSS6027E

TSS/CICS FREEMAIN ERROR TSSCPTCB SP=230

Reason:

Freemain failure occurred.

Action:

Contact CA Technical Support.

TSS6029E

TSS/CICS SECURITY INITIALIZATION FAILURE

Reason:

CA Top Secret/CICS subtask initialization failure.

Action:

This message will be part of other CA Top Secret/CICS messages displayed. Obtain console log and contact CA Technical Support.

Module:

TSSCPI

TSS6030I

TSS/CICS INSTALL CHECK ===> FACMATRX=

Reason:

Displays the value of FACMATRX CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6031I

TSS/CICS INSTALL CHECK ===> EXTSEC=

Reason:

Displays the value of EXTSEC CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6032I

TSS/CICS INSTALL CHECK ===> XCMD=

Reason:

Displays the value of XCOMMAND CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6033I

TSS/CICS INSTALL CHECK ===> XDCT=

Reason:

Displays the value of XDCT CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6034I

TSS/CICS INSTALL CHECK ===> XFCT=

Reason:

Displays the value of XFCT CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6035I

TSS/CICS INSTALL CHECK ===> XJCT=

Reason:

Displays the value of XJCT CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6036I

TSS/CICS INSTALL CHECK ===> XPCT=

Reason:

Displays the value of XPCT CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6037I

TSS/CICS INSTALL CHECK ===> XPPT=

Reason:

Displays the value of XPPT CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6038I

TSS/CICS INSTALL CHECK ===> XPSB=

Reason:

Displays the value of XPSB CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6039I

TSS/CICS INSTALL CHECK ===> XDBD=

Reason:

Displays the value of XDBD CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6040I

TSS/CICS INSTALL CHECK ===> XTRAN=

Reason:

Displays the value of XTRAN CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6041I

TSS/CICS INSTALL CHECK ===> XTST=

Reason:

Displays the value of XTST CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6042I

TSS/CICS INSTALL CHECK ===> DSNCHECK=

Reason:

Displays the value of DSNCHECK CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6043I

TSS/CICS INSTALL CHECK ===> PCTEXTSEC=

Reason:

Displays the value of PCTEXTSEC CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6044I

TSS/CICS INSTALL CHECK ===> XAPPC=

Reason:

Displays the value of XAPPC CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6045I

TSS/CICS INSTALL CHECK ===> LTLOGOFF=

Reason:

Displays the value of the LTLOGOFF CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

TSS6046I

TSS/CICS INSTALL CHECK ===> PCTCMDSEC=

Reason:

Displays the value of PCTCMDSEC CA Top Secret/CICS is using for this execution of CICS.

Action:

No action required.

Module:

TSSCPI/TSSCRT

TSS6047I

TSS/CICS G U S H C I PROCESSING

Reason:

Successful GETMAIN of CA Top Secret/CICS User Hash Chain Index.

Action:

No action required.

Module:

TSSCCMGR

TSS6049I

TSS/CICS L C N-R D M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Non-Release Dependent Modules.

Action:

No action required.

Module:

TSSCPM

TSS6050I

TSS/CICS L C R D M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Release Dependent Modules.

Action:

No action required.

Module:

TSSCPM

TSS6051I

TSS/CICS L C R R T M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Resource Request Table Module.

Action:

No action required.

Module:

TSSCPM

TSS6052I

TSS/CICS L C E M T M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Error Messages Table Modules.

Action:

No action required.

Module:

TSSCPM

TSS6053I

TSS/CICS L C T M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Table Modules.

Action:

No action required.

Module:

TSSCPM

TSS6054I

TSS/CICS L C P A M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Patch Area Modules.

Action:

No action required.

Module:

TSSCPM

TSS6055I

TSS/CICS L C S M PROCESSING

Reason:

Successfully loaded CA Top Secret/CICS Stub Modules.

Action:

No action required.

Module:

TSSCPM

TSS6056I

TSS/CICS D C N-R D M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Non-Release Dependent Modules.

Action:

No action required.

Module:

TSSCPM

TSS6057I

TSS/CICS D C R D M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Release Dependent Modules.

Action:

No action required.

Module:

TSSCPM

TSS6058I

TSS/CICS D C R R T M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Resource Request Table Modules.

Action:

No action required.

Module:

TSSCPM

TSS6059I

TSS/CICS D C E M T M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Error Message Table Module.

Action:

No action required.

Module:

TSSCPM

TSS6060I

TSS/CICS D C T M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Table Modules.

Action:

No action required.

Module:

TSSCPM

TSS6061I

TSS/CICS D C S M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Stub Module.

Action:

No action required.

Module:

TSSCPM

TSS6063I

TSS/CICS SECURITY STATUS CHANGE PROCESSING STARTED

Reason:

CA Top Secret/CICS security parameter modification starting.

Action:

No action required.

Module:

TSSCRT

TSS6065I

TSS/CICS SECURITY STATUS CHANGE PROCESSING COMPLETED

Reason:

CA Top Secret/CICS security parameter modification completed.

Action:

No action required.

Module:

TSSCRT

TSS6067E

TSS/CICS SECURITY INITIALIZATION FAILURE

Reason:

This message is generated during Phase 3 initialization.

Any one of the following could have occurred:

- No AFCB address was found;
- CICS' AFCB header was not identified as “AFCX”;
- Cannot support this release of CICS;
- The PTCB address cannot be located;
- CA Top Secret/CICS subtask errors;
- TSSCPI errors.

Action:

This message may be part of other CA Top Secret/CICS messages displayed. Obtain console log and call CA Top Secret Support.

Module:

TSSTCINT

TSS6068I

TSS/CICS D C P A M PROCESSING

Reason:

Successfully deleted CA Top Secret/CICS Patch Area Modules.

Action:

No action required.

Module:

TSSCPM

TSS6069I

TSS/CICS C S T M A PROCESSING

Reason:

The CA Top Secret/CICS SIGNON/SIGNOFF subtask manager is being attached.

Action:

No action required.

Module:

TSSCSMGR

TSS6071E

TSS/CICS S S T M INVALID PARAMETER LIST PASSED

Reason:

Invalid TXSECREQ request function.

TSSCSMGR

Action:

No action required.

Module:

TSSCSMGR

TSS6072I

TSS/CICS C S T M T PROCESSING

Reason:

CA Top Secret/CICS SIGNON/SIGNOFF subtask manager terminating.

Action:

No action required.

Module:

TSSCSMGR

TSS6073I

TSS/CICS C S T M WAITING FOR ACTIVE TCBS TO COMPLETE

Reason:

CA Top Secret/CICS SIGNON/SIGNOFF subtask manager is waiting for all DFHTRAC0 subtasks to complete before terminating.

Action:

No action required.

Module:

TSSCSMGR

TSS6074E

TSS/CICS S S T M G W A PROCESSING ERROR

Reason:

TSSCSMGR STCB getmain failure. (700 bytes SP-230)

Action:

No action required.

Module:

TSSCSMGR

TSS6075I

TSS/CICS G U S C B C PROCESSING

Reason:

Successful GETMAIN of CA Top Secret/CICS User Signon Control Block (USCB) Cell Storage.

Action:

No action required.

Module:

TSSCCMGR

TSS6076I

TSS/CICS G U S C B B PROCESSING

Reason:

Successful build of the CA Top Secret/CICS User Signon Control Block (USCB) Block Storage.

Action:

No action required.

Module:

TSSCCMGR

TSS6077I

TSS/CICS G T T P T PROCESSING

Reason:

Successful Getmain of CA Top Secret/CICS Task Token Pointer Table storage.

Action:

No action required.

Module:

TSSCCMGR

TSS6078I

TSS/CICS G T T C B C PROCESSING

Reason:

Successful Getmain of CA Top Secret/CICS Task Token Control Block Cell storage.

Action:

No action required.

Module:

TSSCCMGR

TSS6079I

TSS/CICS G T T C B B PROCESSING

Reason:

Successful initialization of the TTPT.

Action:

No action required.

Module:

TSSCCMGR

TSS6080I

TSS/CICS G D U H C I PROCESSING

Reason:

Successful GETMAIN of CA Top Secret/CICS Duplicate User Hash Chain Index Storage.

Action:

No action required.

Module:

TSSCCMGR

TSS6081I

TSS/CICS G D U S B C PROCESSING

Reason:

Successful GETMAIN of CA Top Secret/CICS Duplicate User Signon Block (DUSB) Cell Storage.

Action:

No action required.

Module:

TSSCCMGR

TSS6082I

TSS/CICS G D U S B B PROCESSING

Reason:

Successful build of the CA Top Secret/CICS Duplicate User Signon Block (DUSB) Block.

Action:

No action required.

Module:

TSSCCMGR

TSS6083I

TSS/CICS MODULE REFRESH SUCCESSFUL FOR _____.

Reason:

Transaction TSSC was invoked to reload (refresh) a CA Top Secret/CICS module. It was successfully reloaded.

Action:

No action required.

Module:

TSSCPM

TSS6084E

TSS/CICS MODULE LOAD FAILURE FOR _____.

Reason:

An attempt was made to refresh a CA Top Secret/CICS module via the TSSC transaction, but was unsuccessful.

Action:

Retry TSS=NEWC command. If trouble persists, contact CA Technical Support.

Module:

TSSCPM

TSS6085E

TSS/CICS SIGNON BEING DELAYED DUE TO LACK OF LSQA

Reason:

Due to lack of LSQA, the signon could not be buffered for the CA Top Secret/CICS servers.

Action:

Reduce MAXSIGN parameter for the facility.

Module:

TSSCSMGR

TSS6086E

TSS/CICS SM ATTACH PROCESSING ERROR

Reason:

Due to lack of LSQA.

Action:

Reduce MAXSIGN parameter for the facility.

Module:

TSSCCMGR

TSS6087E

TSS COMMAND FAILED, OPERATOR NOT SIGNED ON

Reason:

You cannot invoke the TSS command without being signed on to CA Top Secret.

Action:

Signon to terminal using your CA Top Secret user id and password.

Module:

TSSCCTSS

TSS6088I

TSS/CICS CORE MANAGER SUBTASK IS ACTIVE

Reason:

The CA Top Secret CICS core manager subtask is currently active.

Action:

No action is necessary.

TSS6089I

TSS/CICS PROGRAM MANAGER SUBTASK IS ACTIVE

Reason:

The CA Top Secret CICS program manager subtask is currently active.

Action:

No action is necessary.

TSS6090I

MRO OPTIMIZED SIGNON (MOS) FEATURE ENABLED

Reason:

Indicates that the MOS feature is active for the region being initialized.

Action:

No action required.

TSS6091E

TSS/CICS ACID NOT AUTHORIZED FOR JOB SUBMISSION

Reason:

The submitting ACID does not have authority to submit the job with another ACID.

Action:

Cross-authorize the submitting ACID to the execution ACID via

```
TSS PERMIT(subacid) ACID(execacid)   - or -

TSS ADDTO(subacid) NOSUBCHK
```

TSS6092I

TSS/CICS FACILITY TYPE NOT CICS

Reason:

Indicates that the facility type was not CICS.

Action:

Re-issue facility type with a valid CICS facility.

TSS6093I

TSS/CICS INITIALIZATION PHASE 0 STARTED

Reason:

Indicates that the Phase 0 initialization has begun.

Action:

No action required.

TSS6094I

TSS/CICS INITIALIZATION PHASE 0 COMPLETE

Reason:

Indicates that the Phase 0 initialization has finished.

Action:

No action required.

TSS6095I

TSS/CICS SIGNON MANAGER SUBTASK IS ACTIVE

Reason:

The CA Top Secret CICS signon manager subtask is currently active.

Action:

No action is necessary.

TSS6096I

TSS/CICS ATTACHING *nnnn* SIGNON SERVER SUBTASK

Reason:

The CA Top Secret CICS signon server subtask is in the process of attaching *nnnn* servers.

Action:

No action is necessary.

TSS6097I

TSS/CICS DETACHING SIGNON SERVER SUBTASK

Reason:

CA Top Secret CICS is detaching the signon server subtask.

Action:

No action is necessary.

TSS6098I

TSS/CICS DETACHING SIGNON MANAGER SUBTASK

Reason:

CA Top Secret CICS is detaching the signon manager subtask.

Action:

No action is necessary.

TSS6099I

TSS/CICS INITIALIZATION PHASE 1 COMPLETE

Reason:

Phase 1 of 3 has successfully completed.

Action:

No action required.

Module:

TSSCINIT

TSS6100E to TSS6301I

TSS6100E

DSN SECURITY CHECK PROCESSING ERROR

Reason:

DSNB/File access error.

Action:

Open all CICS files or shutdown DSN security checking.

Module:

TSSCXS/TSSCFM

TSS6101I

TSS/CICS SIGNON PROCESSING DELAYED. MAXSIGN LIMIT HAS BEEN REACHED.

Reason:

MAXSIGN limit set in the CICS facility has been reached. The MAXSIGN action is set to "RETRY", CA Top Secret will re-attempt the signon after a four second wait.

Action:

No action required if the signon retry is successful. If repeated failures, check the MAXSIGN facility control option. Modify the limit or the action control sub-option if appropriate.

TSS6102E

SIGNON FAILURE FOR 'variable text'

Reason:

CA Top Secret CICS has had a failure for the listed reason.

Action:

No action is necessary.

TSS6103I

TSS/CICS SIGNON SERVER ATTACH FAILED. UNABLE TO ATTACH SERVER SUBTASK

Reason:

CA Top Secret CICS has had a failure in attaching the signon server, the server subtask will not run until the server is attached.

Action:

No action is necessary.

TSS6105I

TSS/CICS SECURITY OPTIONS BEING REFRESHED - xxxxxxx

Reason:

For CICS 4.1 and above, a facility matrix suboption has been changed on the facility. All XPARMS except XDCT and XTST and suboption RLP can be changed without recycling CICS. These three options can be changed to NO, but cannot be changed to YES without recycling CICS. Facility suboptions MAXSIGN, ASUBM, and SIGN(S) require recycling of CICS to change the option.

Action:

No action is necessary.

TSS6106I

MAXIMUM TS QUEUE LIMIT HAS BEEN REACHED

Reason:

A CICS application program has issued a LINK to program TSSCICS using a temporary storage queue for communications. If the application is executing from a VTAM or BTAM terminal, TSSCICS can issue a maximum of 500 24x80 temporary storage blocks during command execution. If the application is executing from a sequential terminal, TSSCICS may write up to 12000 80-byte records.

Action:

Performing this much I/O against the security file is not recommended. Online access to TSSCICS is intended for small outputs which will not degrade the performance of CICS or of CA Top Secret. You can lower the number of output blocks by:

- Executing the application signed on to an ACID with a smaller scope; or by
- Changing the command so that the output is limited to a smaller scope. For example, instead of entering this command

TSS LIST(ACIDS)

Enter the following command to result in less output:

TSS LIST(ACIDS)DEPT(dept1)

TSS6110E

TSS/CICS MAXUSER LIMIT REACHED – SIGNON REJECTED

Reason:

The maximum amount of signed-on users allowed in the region was reached, signon attempt rejected. Based on the MAXUSER facility option setting.

Action:

Wait one minute and re-attempt the signon. If MAXUSER is frequently reached, consider raising the value of the MAXUSER option.

Module:

TSSCRT

TSS6111E

TSS/CICS MAXSIGN LIMIT REACHED \emdash SIGNON REJECTED

Reason:

The maximum number of concurrent CICS signons was reached. Based on the facility option MAXSIGN. Signon was rejected due to the KILL suboption specified on the MAXSIGN facility option.

Action:

Wait one minute and re-attempt the signon. If MAXSIGN is frequently reached, consider raising the value of the MAXSIGN option or set the MAXSIGN suboption to RETRY.

Module:

TSSCPOST

TSS6120E

TSS/CICS INVALID SECURITY PARAMETER LIST PASSED

Reason:

The request code found in the Security Parameter List is invalid or not supported.

Action:

Contact CA Top Secret Support Center.

Module:

TSSCXS/TSSCXE

TSS6121E

SECURITY RESOURCE CHECK PROCESSING ERROR

Reason:

No resource class name block found, request failed.

Action:

Check if TSS/CICS is properly installed.

Module:

TSSCXS

TSS6130E

TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=8780

Reason:

DFHTRAC0 ACEE/SECREC getmain failure.

Action:

Reduce MAXSIGN parameter for the facility.

Module:

TSSCPOST

TSS6131E

TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=3220

Reason:

DFHTRAC0 attach failure due to lack of LSQA.

Action:

Reduce MAXSIGN parameter for the facility.

Module:

TSSCPOST

TSS6132E

TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=3230

Reason:

DFHTRAC0 attach failure.

Action:

Contact CA Technical Support.

Module:

TSSCPOST

TSS6133E

TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=0018

Reason:

Invalid Parameter List passed to DFHTRAC.

Action:

Contact CA Technical Support.

Module:

TSSCPOST

TSS6134E

TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=0099

Reason:

TSSCRINT STCB getmain error.

Action:

Lower MAXSIGN parameter of the facility matrix.

Module:

TSSCPOST

TSS6135E

TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR - RC=ERROR

Reason:

DFHTSSM0 subtask attach error (DFHTRAC0).

Action:

Contact CA Technical Support.

Module:

TSSCPOST

TSS6140E

TSS/CICS SECURITY TAMPERING CAUSED BY < _____ >

Reason:

Security violation detected.

Action:

Message and additional information may be located in the security log.

Module:

TSSCTSS

TSS6151E

TSS/CICS GETMAIN FAILURE RETURNED FROM RACINIT

Reason:

A CICS signon (RACINIT) was attempted, but failed due to getmain failure in the base CA Top Secret system.

Action:

Lower CICS Region by 500k. If problem persists, contact CA Technical Support.

Module:

TSSCPOST

TSS6152E

TSS/CICS BAD PARAMETER LIST RETURNED FROM RACINIT

Reason:

A CICS signon (RACINIT) was attempted, but failed due to invalid parameter passed to the base CA Top Secret system.

Action:

Contact CA Technical Support.

Module:

TSSCPOST

TSS6153E

TSS/CICS BAD RETURN FROM RACINIT

Reason:

A CICS signon (RACINIT) was attempted, but failed due to unknown reason.

Action:

Contact CA Technical Support.

Module:

TSSCPOST

TSS6160I

CA Top Secret CICS Initialization environment valid.

Reason:

The CICS PLTPI program TSSCPLT did not find any environment errors. This message is issued only if the site has added TSSCPLT to its running PLTPI list. It serves as confirmation that the program was executed.

Action:

This message is for information only. No action is required.

Module:

TSSCPLT

TSS6161E

CA Top Secret CICS Initialization Incomplete RSN=nn

Reason:

The CICS PLTPI program TSSCPLT found an initialization or environment error. Only the first error encountered is reported. The reason code (nn) indicates the specific problem and is explained below:

- 00—TSSCPLT could not find the z/OS CVT. There are serious errors with the z/OS control block structure.
- 01—TSSCPLT could not locate the SSCT anchor.
- 02—The SSCT entry for CA ACF2 is missing.
- 03—The ACEE for the region could not be located.
- 06—The root CA Top Secret CICS control block (KPGA) has an invalid header/eyecatch; it should start “KPGA.”
- 07—The version number in the KPGA is incorrect.
- 08—The “initialization in process” flag in the KPGA is still on, indicating the CA Top Secret CICS initialization failed to complete.
- 09—The region ACEE has an invalid header/eyecatch; it should start with “ACEE.”
- 10—The pointer to the ACEX in the region ACEE is null.
- 11—The pointer to the KPGA in the ACEX is null.
- 24—TSSCPLT was unable to find the ENF DCM for CA Top Secret CICS for the CICS release level being executed.

Action:

If the reason code is in the 00 to 11 range, contact CA Technical Support.

For reason code 24, follow the procedures in the CICS Support Guide for adding the CA Top Secret CICS DCM to the ENF database, then restart the CICS region.

Module:

TSSCPLT

TSS6200E

TSS Command OS Attach Failure <EP=TSS>

Reason:

A subtask creation for the TSS command failed due to an attach failure.

Action:

Contact CA Technical Support.

Module:

TSSCCTSS

TSS6201E

CA TSS is not Active

Reason:

CA Top Secret was found not to be active.

Action:

Start the CA Top Secret address space.

Module:

TSSCCTSS

TSS6202E

TSS Command Transaction Processing Error <ECB= ^0>

Reason:

The DETACH for the TSS command failed.

Action:

Contact CA Technical Support.

Module:

TSSCCTSS

TSS6203I

TSS Command Transaction Processing Error

Reason:

No data was returned from the TSS command.

Action:

Contact CA Technical Support.

Module:

TSSCCTSS

TSS6210WI

Unable to start TSSF transaction

Reason:

CA Top Secret was unable to initiate transaction TSSF, used with the MOS CICS feature.

Action:

Turn off the MOS feature by removing the MRO attribute from the region acid of related CICS regions. See PIB LI13100 for how to properly install MOS.

TSS6300I

TSS/CICS UNLOCK FUNCTION SUCCESSFUL

Reason:

Valid CA Top Secret password was entered, terminal unlocked.

Action:

No action required.

Module:

TSSCTSS

TSS6301I

SIT DEFAULT USER CANNOT BE LOCKED

Reason:

A TSS LOCK command was issued while signed on as the CICS SIT default user. The ACID assigned by the CICS SIT DFLTUSER specification should never issue the TSS LOCK command. If a user were allowed to do so, all users who were assigned to the default user would be locked when one user performed the command.

Action:

TSS LOCK requires an explicit signon to a CICS user other than the CICS SIT default user.

TSS7000I to TSS7054I

TSS7000I

acid LAST-USED date time SYSTEM=id FACILITY=facility SECLABEL=seclabel

Reason:

This message displays after successful initiation as controlled by FACILITY/LUMSG, where:

acid

Accessor ID associated with the job or session.

date

Date when the ACID was last used (day,month,year).

time

Time when the ACID was last used (hour,minutes).

id

SMF ID of the CPU on which the ACID was used.

facility

System facility last used.

seclabel

The seclabel assigned to the user.

Action:

No action required.

TSS7001I

COUNT=nnnnn MODE=mode LOCKTIME=nnn NAME=name

Reason:

The “status” message presented on successful initiation as controlled by FACILITY/STMSG control option, where:

COUNT

Number of times, to date, that the ACID has been used

MODE

User's current MODE (i.e. DORMANT,IMPL, WARN,FAIL)

LOCKTIME

Default terminal locking time

NAME

Name assigned to the user ACID

Action:

No action required.

TSS7002I

YOUR TIMEZONE ADJUSTMENT FACTOR IS #nn HOURS

Reason:

The “status” message indicates the value set by the TZONE keyword. The TZONE keyword allows you to adjust for time zone differences between the user's actual workstation and the CPU.

Action:

No action required.

TSS7003W

PASSWORD WILL EXPIRE ON mm/dd/yy

Reason:

The current password for the facility will expire on the date displayed.

Action:

Change the password soon.

TSS7004W

USE OF ACCESSORID EXPIRES ON mm/dd/yy

Reason:

The user's ACID for the facility is about to become invalid.

Action:

No action required.

TSS7005I

***** *nn* Password violations since last successful signon *****

Reason:

The user's ACID has incurred at least one password violation since the last time it successfully signed on.

nn

Specifies the actual number of password violations since the last successful signon.

Action:

No action required.

Note: The STMSG/NOSTMSG control option controls this message. If NOSTMSG is set, this message does not appear at signon. CA Top Secret administrators will not be subject to the STMSG/NOSTMSG control option setting. In that case, the TSS7005I message will always be issued when appropriate.

TSS7010A

PLEASE ENTER YOUR CA Top SecretPASSWORD

Reason:

CA Top Secret is requesting your TSO logon password.

Action:

Enter your CA Top Secret (TSO) password. To change your password, enter your current password, forward slash, new password in the following format: oldpassword/newpassword. To ensure that you entered the new password correctly, you may specify the new password twice in the following format:

```
oldpassword/newpassword/newpassword
```

TSS7011A

PLEASE ENTER YOUR *NEW* PASSWORD OR 'RANDOM'

Reason:

CA Top Secret requires your new password(s).

Action:

Enter your new CA Top Secret password. The password must follow the rules outlined in the NEWPW control option. Enter “RANDOM” if you want the system to randomly generate a new password for you.

TSS7012I

***WARNING* NEVER USE PERSONAL INFORMATION AS YOUR PASSWORD**

Reason:

The user supplied an expired password at signon and did not provide a new password. This message, along with TSS7013I, is displayed when the PRODUCTS control option is set to TSO.

Action:

A valid password must be supplied.

TSS7013I

INCLUDING NAMES,LOCATIONS, LICENSE/PHONE NUMBERS,SSN/SIN

Reason:

This is an informational message only. Using personal information in a password makes it easier for someone to guess a user's password.

Action:

No action required.

TSS7015I

Format is Password/New Password/Reverify Password

Reason:

Your password(s) were entered incorrectly. The correct format is displayed.

Action:

No action required.

TSS7016A

ENTER NEW PASSWORD AGAIN FOR REVERIFICATION

Reason:

CA Top Secret wants to make sure that the user entered (and/or remembers) the new password correctly, OR the user entered a “verification” password that did not match the new password.

Action:

Re-enter the password, being careful to match the original password exactly. If, after two verification retries, the passwords still do not match, the user receives a TSS7111E and a DRC(015).

TSS7020A

RANDOM PASSWORD ABOUT TO BE DISPLAYED; HIT ENTER TO CONTINUE

Reason:

A CA Top Secret-generated “RANDOM” password will be displayed until you press Enter.

Action:

Read and memorize the password. Then erase the password by pressing Enter.

TSS7021I

YOUR NEW PASSWORD IS password

Reason:

Your password expired and CA Top Secret assigned a new password to you OR you specified “RANDOM” as the new password.

Action:

Memorize your new password. To maintain a high level of security, do not write the new password down. Press the Enter key.

TSS7022A

MEMORIZE PASSWORD & HIT ENTER KEY - DO *NOT* RECORD

Reason:

Your password expired and CA Top Secret assigned a new password to you OR you specified “RANDOM” as the new password.

Action:

Memorize your new password. To maintain a high level of security, do not write the new password down. Press the Enter key.

TSS7030I

PASSWORD CHANGED

Reason:

You have successfully changed your password.

Action:

No action required.

TSS7031I

Facility ffffffff has been locked for user uuuuuuuu

Reason:

A CICS multiuser address space user was locked when the user reached pseudo conversational locktime.

Action:

Respond with the correct password when prompted with message TSS7199A.

TSS7032I

Facility *ffffffff* has been unlocked for user *uuuuuuuu*

Reason:

A CICS multiuser address space user was unlocked.

Action:

No action required.

TSS7040WI

PLEASE USE YOUR TSO(UADS) PASSWORD

Reason:

In DORMant, WARN, or IMPLement mode, undefined users must use their TSO UADS password to sign on.

Action:

Type in your UADS password to sign on to the system. Press the Enter key.

TSS7041A

PLEASE ENTER YOUR UADS FUNCTION/PASSWORD NEXT

Reason:

TSO is about to prompt the user for his UADS-defined password. The password may be interpreted as a function code.

Action:

Enter your TSO UADS function code or password.

TSS7050I

J=jobname A=acid -MRO ATTRIBUTE IGNORED

Reason:

An ACID with the MRO attribute specified signed on to an already existing address space. The MRO attribute is only assigned to the control ACID with which a job or STC is initiated in the address space.

jobname

Indicates the name of the job or started task to which the ACID was signing on.

acid

Indicates the accessor id assigned the MRO attribute.

Action:

If an error has been made assigning the ACID the MRO attribute, issue the following TSS command to remove the attribute:

```
TSS REMOVE(acid) MRO
```

TSS7051W

PASSWORD PHRASE CHECKING BYPASSED DUE TO CA ACF2 CO-EXISTENCE

Reason:

This is a reminder that the PRODUCTS(ACF2) control option is set. Batch password phrases cannot be verified until CA ACF2 is removed.

Action:

No action required.

TSS7052W

CURRENT PASSWORD EXPIRED-PREVIOUS BATCH PASSWORD USED

Reason:

Your password has expired. The system is using the expired password to run the submitted batch job. The HPBPW option, which limits the number of days the expired password will be honored, is active.

Action:

Change your password as soon as possible.

TSS7053I

DEFAULT ACID <acid name> ASSIGNED

Reason:

This is a reminder that you have been assigned the displayed default ACID.

Action:

No action required.

TSS7054I

SECURITY BYPASS ACTIVE FOR JOB=jobname ACID=acid

Reason:

This is to notify you that the specified job/user is using an ACID that is bypassing security. This may also occur if jobs start while CA Top Secret is being initialized and your DOWN control option specifies Bypass.

Action:

No action required.

TSS7100E to TSS7199A

TSS7100E

drc J=jobname A=acid T=terminal F=facility - reason

Reason:

This summary violation message displays when a system logon is rejected by security. The message is routed to any active security console.

drc

Indicates the detailed reason code indicates the type of violation.

jobname

Indicates the name of job or user that received the violation.

acid

Indicates the accessor id for which the violation occurred.

terminal

Indicates the online terminal or batch reader related to the user or job.

facility

Indicates the facility that was being used.

reason

Indicates the short explanation of the error may be present.

Action:

No action required.

TSS7101E

PASSWORD IS INCORRECT

Reason:

The password supplied for the ACID is invalid. Access to the facility will not be allowed unless the correct combination of ACID and password is supplied.

Action:

Supply the correct password.

TSS7101E

PASSWORD PHRASE IS INCORRECT

Reason:

The password phrase supplied for the ACID is invalid. Access to the facility will not be allowed unless the correct combination of ACID and password phrase is supplied.

Action:

Supply the correct password phrase.

TSS7102E

PASSWORD MISSING

Reason:

The required password for the ACID was not supplied. Access to the facility will not be allowed unless the correct combination of ACID and password is supplied.

Action:

Supply a password.

TSS7102E

PASSWORD PHRASE MISSING

Reason:

The required password phrase for the ACID was not supplied. Access to the facility will not be allowed unless the correct combination of ACID and password phrase is supplied.

Action:

Supply a password phrase.

TSS7104W

SECLABEL verification failed - Assigning SYSLOW.

Reason:

The user is not authorized to the SECLABEL specified at signon or assigned from the input device. When control option MLMODE is WARN or DORM, seclabel SYSLOW is assigned automatically.

Action:

The user is signed on with SYSLOW. Add the specified SECLABEL to the user's list of authorized SECLABELs if necessary.

TSS7105E

SECLABEL verification failed.

Reason:

The user is not authorized to the SECLABEL specified at signon or assigned from the input device.

When control option MLMODE is FAIL, the user is reprompted for a valid SECLABEL.

Action:

Add the SECLABEL to the user's list of authorized SECLABELs or the user can specify an authorized valid SECLABEL.

TSS7106I

Subject Never Dominates

Reason:

A RACROUTE REQUEST=AUTH,STATUS=EVERDOM,... request was issued and the subject's SECLABEL never dominates the resource SECLABEL.

Action:

No action required.

TSS7102W

SECLABEL not active on this system

Reason:

At signon the user was assigned a SECLABEL that is not active on this system. The SECLABEL may be undefined or defined with SYSIDs but not the sysid for this sytem.

Action:

Specify another SECLABEL and signon again or define the SECLABEL so it can be used on this system.

TSS7108W

Write-down not allowed - Resource not protected

Reason:

When the control option MLWRITE(NO) is set, every writedown to the MLS access records requires a permission for IBMFAC(IRR.WRITEDOWN.BYUSER). This message is issued when a user accesses an MLS protected resource and the above IBMFAC resource is not granted to the user.

Action:

You may take one of several actions to eliminate this message:

Provide a permission

TSS PERMIT(acid|profile|ALL) IBMFAC(IRR.WRITEDOWN.BYUSER)

for all users accessing MLS protected resources.

Modify MLACTIVE(NO)

Modify MLWRITE(YES)

TSS7109E

DIRAUTH processing failed

Reason:

RACROUTE REQUEST=DIRAUTH was invoked to compare two seclabels. The requested function could not be performed or the request failed.

Action:

Examine the RACROUTE return and reason codes to determine the cause of the error.

TSS7110E

PASSWORD HAS EXPIRED. NEW PASSWORD MISSING

Reason:

The current password is no longer valid. A new password must be entered to replace the current one.

Action:

User must supply current and new passwords.

TSS7110E

PASSWORD PHRASE HAS EXPIRED. NEW PASSWORD PHRASE MISSING

Reason:

The current password phrase is no longer valid. A new password phrase must be entered to replace the current one.

Action:

User must supply current and new password phrases.

TSS7111E

NEW PASSWORD CHANGE INVALID - *reason*

NEW PASSWORD PHRASE CHANGE INVALID - *reason*

Reason:

The password or password phrase change for the ACID is invalid. If the current password has expired, access to the facility is not allowed until you supply the correct combination of an ACID and password. Reasons are as follows:

At Least 1 Alphabetic Required

Indicates that the password must contain a alphabetic character

At Least 1 Numeric Required

Indicates that the password must contain a numeric character.

Cannot Be Changed Yet

Indicates that the password can be changed only after a set timeframe.

Does Not Conform to Mask

Indicates that an incorrect character type was specified in a masked position.

Encryption Error

Indicates that an internal error occurred while encrypting a password or password phrase.

Identical to Previous Password

Indicates that the password is identical to the current password (or a history password) and may not be used again.

Invalid Character

Indicates that the password contains unsupported characters.

Minimum Alpha Required

Indicates that the password does not contain the minimum required number of alphabetical characters.

Minimum Numeric Required

Indicates that the minimum number of numeric characters was not specified in the new password phrase.

Minimum Special Char Required

Indicates that the minimum required number of special characters was not met.

Must Have 1 Lowercase Char.

Indicates that the password must contain a lowercase character.

Must Have 1 Special Character

Indicates that the password must contain a character from the passchar list. This list contains valid characters for passwords.

Must Have 1 Uppercase Char.

Indicates that the password must contain an uppercase character.

Not Properly Split

Indicates that the password must contain a word that is split by a @,# ,or $ (for example, aaa@bbbb or abcd#ef).

Password/New Phrase Not Valid

Indicates that you cannot specify an old password and a new phrase.

Phrase/New Password Not Valid

Indicates that you cannot specify an old phrase and a new password.

Prior Batch Password Used

Indicates that the product is still honoring the expired password for a batch job (based on the HPBPW control option setting).

Random Password Not Supported

Indicates that the RN option of the NEWPW control option is not set for random password generation.

Rejected by Site Exit

Indicates that the password was failed by the password exit.

Restricted Word

Indicates that the password is restricted and cannot be used.

Reverification Failed

Indicates that password reverification was incorrect, meaning the second password entry did not match the first entry.

Too Many Characters

Indicates that the password contains too many characters.

Too Short

Indicates that the password has too few characters.

Too Similar to Old Password

Indicates that the password is too similar to the current password.

Too Similar to Userid

Indicates that the password is too similar to the user's ID.

Too Similar to Your Name

Indicates that the password is too similar to the user's name.

You Cannot Change Password

Indicates that the password cannot be changed by the user.

You Cannot Repeat Characters

Indicates that the password contains more than the acceptable amount of repeating characters.

You Cannot Use Vowels

Indicates that the password cannot not contain vowels.

You Must Use All Numerics

Indicates that the password must contain only numeric characters.

Action:

Make any adjustments and correct the new password or phrase if necessary. If the reason was Encryption Error, contact CA Support.

TSS7112E

INVALID CHARACTER IN PASSWORD

Reason:

Your password contains a character other than A through Z, 0 thru 9, $, #, and @.

Action:

Reenter your password.

TSS7115E

REVERIFY PASSWORD NOT THE SAME AS NEW PASSWORD

Reason:

Reverify password was entered incorrectly or is not the same as the new password entry.

Action:

Re-enter the password being careful to match the new password exactly.

TSS7116E

REVERIFY PASSWORD DOES NOT MATCH. TRY AGAIN.

Reason:

The new password was entered twice for verification (see message TSS7010A). The entries do not match, which indicates that a typing error was made.

Action:

Carefully reenter the request to change your password.

TSS7120E

PASSWORD VIOLATION THRESHOLD EXCEEDED

Reason:

The user has tried, but failed, to enter the correct password too many times. The number of acceptable unsuccessful attempts is determined by the PTHRESH setting. In any event, the ACID is suspended.

Action:

The Security Administrator must remove the SUSPEND attribute from the ACID.

TSS7120E

PASSWORD VIOLATION THRESHOLD EXCEEDED

Reason:

The user has tried, but failed, to enter the correct password or password phrase too many times. The number of acceptable unsuccessful attempts is determined by the PTHRESH setting. The number of unsuccessful attempts is the total of incorrect passwords and incorrect password phrases. In any event, the ACID is suspended.

Action:

The Security Administrator must remove the SUSPEND attribute from the ACID.

TSS7121E

DO NOT SUPPLY PASSWORD(S) WITH LOGON COMMAND

Reason:

You cannot include your password when entering a LOGON command. Control option FACILITY/PROMPT forces TSO to prompt for a password in a non-display field.

Action:

Wait for CA Top Secret to prompt you for a password during the logon session.

TSS7130E

OPERATOR ID CARD REQUIRED FOR LOGON/SIGNON

Reason:

The user did not supply an Operator ID Card for logon.

Action:

The user must specify the OIDCARD keyword on the TSS LOGON command. CA Top Secret will prompt the user to insert the OID card.

TSS7131E

OPERATOR ID CARD INCORRECT

Reason:

The user did not supply the correct OIDCARD for the ACID.

Action:

No action required.

TSS7132E

VOICE OR DIGITIZED IMAGE VERIFICATION FAILED

Reason:

A logon/signon was rejected because the security device did not recognize the user.

Action:

No action required.

TSS7133W

PASSWORD PHRASE WILL EXPIRE ON mm/dd/yy

Reason:

The current password phrase for the user will expire on the date displayed.

Action:

Change the password phrase soon.

TSS7135I

PASSWORD PHRASE CHANGED

Reason:

You have successfully changed your password phrase.

Action:

No action required.

TSS7140E

ACCESSOR ID HAS EXPIRED; NO LONGER VALID

Reason:

The FOR or UNTIL keyword of an ACID has expired. The ACID can no longer be used.

Action:

Report to the Security Administrator to renew the ACID.

TSS7141E

USE OF ACCESSOR ID SUSPENDED

Reason:

Use of the ACID has been revoked.

Action:

An administrator must remove the ACID's suspension by using the TSS REMOVE function.

TSS7142E

ACCESSOR ID NOT YET AVAILABLE FOR USE - STILL INACTIVE

Reason:

Use of the ACID has been temporarily revoked.

Action:

An administrator must remove the ACID's suspension by using the TSS REMOVE function.

TSS7143E

ACCESSOR ID HAS BEEN INACTIVE TOO LONG

Reason:

The ACID has exceeded an inactivity threshold set by the administrator. Inactivity is measured from the last time the ACID's password expired to the current date.

Action:

The Security Administrator must replace the user's password and unsuspend the user. This solves the immediate problem. The administrator should consider whether to increase the user's password interval if the user does not sign on often enough to maintain currency. If a large number of users experience this problem, the administrator may wish to consider altering the following:

- The PWEXP control option, which provides the default expiration interval for newly created ACIDs.
- INACTIVE control option, which triggers TSS7143E when the number of days specified has occurred since the user's password has expired.
- OPTION(36) control option (available after TSS 5.2 SP03) alters the meaning of the INACTIVE option to suspend ACIDs less often, when the ACID has exceeded the INACTIVE period past both the last-used date and the password-change date.

TSS7144E

ACCESSOR ID MISSING

Reason:

An attempt to access the system failed; the JOB card did not contain an ACID.

Action:

Supply the ACID on the JOB card.

TSS7145E

ACCESSOR ID <acid> NOT DEFINED TO SECURITY

Reason:

The ACID is not defined to the Security Record.

Action:

The Security Administrator can CREATE the desired ACID.

TSS7150A

SPECIFY PASSWORD FOR STC=stc ACID=acid

Reason:

The O/S START command entered is defined with a password.

Action:

Enter the password associated with the ACID and Started Task. When entering a mixed case response, enclose the text in single quotes.

TSS7151A

SPECIFY ACCESSORID/PASSWORD TO BE USED WITH STC=stc

Reason:

The Started Task Command is not associated with a specific ACID.

Action:

This will be the ACID under which the STC will run. Enter your ACID and password in the following format: acid/password. When entering a mixed case response, enclose the text in single quotes.

TSS7152A

SPECIFY YOUR ACCESSID/PASSWORD TO ALLOW USE OF STC=stc

Reason:

The started task is protected against unauthorized use.

Action:

Identify yourself to the system to continue with the started task. Enter your ACID and password in the following format: acid/password. When entering a mixed case response, enclose the text in single quotes.

This will not be the ACID that the STC runs under.

TSS7153E

STARTED TASK NOT DEFINED TO SECURITY SYSTEM

Reason:

The STC procedure name specified by an O/S START command is not defined to CA Top Secret. No default ACID was defined and the default option requires failure of undefined STCs.

Action:

If required, the STC procedure can be defined through the TSS ADDTO command.

TSS7160E

FACILITY <facility> NOT AUTHORIZED FOR YOUR USE

Reason:

The ACID is not authorized to access the named system facility.

Action:

The ACID must obtain proper authorization from his CA Top Secret administrator.

TSS7161E

FACILITY <facility> NOT AVAILABLE DURING THIS TIME PERIOD

Reason:

Access to the facility is controlled on a time-of-day basis.

Action:

Log on to the facility at the authorized time.

TSS7162E

FACILITY <facility> NOT AVAILABLE THIS DAY.

Reason:

Access to the facility is controlled on a day-to-day basis.

Action:

Log on to the facility on the authorized day.

TSS7170E

JOB ORIGINATED FROM PROTECTED READER reader

Reason:

The origin of this job is a defined reader (local or RJE) for which the user ACID does not have access authority. The ACID is not authorized for the TERMINAL.

Action:

No action required.

TSS7171E

UNAUTHORIZED SOURCE OF SYSTEM ENTRY

Reason:

The ACID (job or user id) cannot be used from this terminal or reader. The ACID source of origin is restricted by the SOURCE option to prevent its unauthorized use.

Action:

No action required.

TSS7172E

YOUR ACCESSOR ID IS ALREADY IN USE ON TERMINAL terminal

Reason:

Reason: The facility control sub-option SIGN(S) has been set for this multi-user address space. The ACID you have used to sign on was previously signed on at a different terminal. The SIGN(S) control option prevents an ACID in IMPL or FAIL mode from signing on to the address space from multiple terminals simultaneously.
.

Action:

No action is required. To enable signon from your current terminal with current settings, you must sign off from the original session at the “terminal” designated in the message. There may be tools in the address space which you can use to “kill” the current session.

To override the facility option SIGN(S) for a specific user, the SIGNMULTI attribute may be applied. See the *User Guide* and *Command Functions* for further details. To prevent CA Top Secret from restricting signons in this way, you may wish to consider applying SIGN(M) to the associated facility.

TSS7173E

AUTOMATIC TERMINAL SIGN-ON NOT ALLOWED FOR ACID=acidname. PLEASE SIGN ON

Reason:

CA Top Secret attempted to perform automatic sign-on based upon the terminal ID, and found that the ACID for the terminal had the NOATS attribute.

Action:

Sign on by specifying a valid ACID name and password.

TSS7174E

ONLY A TYPE(USER) ACID CAN BE USED FOR SYSTEM ENTRY

Reason:

An attempt was made to initiate a job or on-line session using an ACID defined as TYPE(DEPARTMENT or DIVISION or PROFILE).

Action:

A “user” ACID or “control” ACID should be used.

TSS7175E

INITIATION DENIED BY SITE SECURITY EXIT

Reason:

LOGON or job initiation has been failed by your installation exit.

Action:

No action required.

TSS7176E

OPERATOR NOT SIGNED ON, PLEASE SIGN ON

Reason:

A transaction was entered without first signing on.

Action:

Log on to the facility, using your CA Top Secret ACID and password.

TSS7180E

SECURITY IS INACTIVE - DOWN OPTION IS "FAIL"

Reason:

CA Top Secret is not active. If the facility is operating in any mode other than DORMANT, all requests will fail.

Action:

No action required.

TSS7181E

END OF DAY - NO FURTHER SYSTEM ACCESS ALLOWED

Reason:

Operations are in the process of shutting down the system. CA Top Secret has already been deactivated. No new jobs or sessions can be initiated.

Action:

To reset the system, enter an authorized RESETEOD control option.

TSS7182E

FACILITY DEACTIVATED BY ADMINISTRATOR. TRY LATER

Reason:

The facility being accessed is not available for job/session initiation. The SCA has defined the facility as unavailable.

Action:

Retry request at a later time.

TSS7183I

SIGNON SERVICES ARE BUSY. PLEASE TRY AGAIN LATER.

Reason:

The signon server is in use, CA Top Secret CICS cannot attach it until it become available.

Action:

No action required.

TSS7185E

PASSWORD VIOLATION FOR CENTRAL SECURITY ADMINISTRATOR AT T=terminal

Reason:

While attempting to use the master security administrator's ACID, on the named terminal, the MSCA did not supply a correct password. Possible breach of security.

Action:

No action required.

TSS7185E

PASSWORD PHRASE VIOLATION FOR CENTRAL SECURITY ADMINISTRATOR AT T=terminal

Reason:

While attempting to use the master security administrator's ACID, on the named terminal, the MSCA did not supply a correct password phrase. Possible breach of security.

Action:

No action required.

TSS7186I

SUSPENDED CENTRAL SECURITY ADMINISTRATOR ATTEMPTING SIGNON

Reason:

This is an informational message indicating a signon attempt has been made by a MSCA whose ACID is suspended.

Action:

This message will be followed by the TSS7187A message (which will require a response).

TSS7187A

SPECIFY <Y> TO CONFIRM SIGNON, ELSE <N> TO DENY USE OF MSCA ACID

Reason:

The MSCA ACID has been suspended and has signed on and entered the correct password.

Action:

Enter Y to allow access or enter N to deny access.

Depending on your current release of MVS/ESA, you may need to respond to this message multiple times.

TSS7188I

J=jobname A=aceeusi @AC=xxxxxxxx @NSR=xxxxxxxx @OSR=xxxxxxxx

Reason:

A security record is being refreshed. The message includes the jobname and the user being refreshed. All other information is for level II support only.

Action:

This is an informational message. No action required.

TSS7190E

JOB=jobname ACID=acid VIOLATION THRESHOLD EXCEEDED

Reason:

The session identified by “jobname” for the ACID has accumulated more violations than allowed by the VTHRESH control option. This message may be accompanied by TSS7191E or TSS7192E, which provide further instruction.

Action:

When presented without other messages, TSS7190E requires no further action; however, repeated violations during a session may indicate that a user is attempting activities that they know to be unauthorized, or that an ACID is being used by unauthorized persons. Further investigation may be warranted.

TSS7191E

JOB/SESSION CANCELLED - EXCESSIVE VIOLATIONS

Reason:

A user exceeded the maximum number of allowable violations set by VTHRESH, and the site has specified the VTHRESH (nn,CANCEL) option. The session is automatically cancelled.

Action:

No action required. If the VTHRESH option also specifies the SUSPEND parameter, the SUSPEND attribute must be removed from the ACID.

TSS7192E

SESSION LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF

Reason:

The user has exceeded the allowable number of violations, as determined by the VTHRESH setting. The session is automatically cancelled.

Action:

Sign off, and then sign on to unlock the session.

TSS7193E

UNLOCK REJECTED - PASSWORD IS INCORRECT

Reason:

The wrong UNLOCK password was entered. The terminal remains locked.

Action:

To unlock the terminal, enter: TSS UNLOCK. When prompted, enter your signon password.

TSS7194E

COMMAND REJECTED - TERMINAL IS LOCKED

Reason:

The terminal being used is currently locked, making it unavailable to all commands except TSS UNLOCK.

Action:

To unlock the terminal, enter: TSS UNLOCK. When prompted, enter your signon password.

TSS7195E

Resource Violation Threshold Exceeded

Reason:

ACID has exceeded the VTHRESH (violation threshold) during this session.

Action:

User will have to log off to reset violation count.

TSS7196E

CA TOP SECRET SECURITY HAS LOCKED THIS TERMINAL

Reason:

CA Top Secret rejected the transaction because the terminal was locked by a user or by the automatic terminal locking feature.

Action:

A terminal can be unlocked by entering the TSS UNLOCK command and the correct signon password.

TSS7197A

SPECIFY YOUR PASSWORD TO USE THIS TRANSACTION

Reason:

Your password must be verified for the transaction to continue.

Action:

Enter your password.

TSS7198A

SPECIFY YOUR PASSWORD TO UNLOCK THIS TERMINAL

Reason:

CA Top Secret has locked the terminal. The transaction cannot continue.

Action:

Enter your password.

TSS7199A

ENTER PASSWORD TO UNLOCK: CSSF OR CLEAR KEY TO SIGNOFF

Reason:

CA Top Secret has locked the terminal, and the transaction cannot continue.

Action:

Enter your password to unlock the terminal, enter “CSSF”, or press the Clear key to sign the terminal off.

TSS7200E to TSS7299I

TSS7200E

drc J=jobname A=acid VOL=volser ACC=rlevel/alevel

Reason:

This is a summary volume violation message.

drc

Indicates the detailed error reason code for violation.

jobname

Indicates the name of job or user session that caused the violation.

acid

Indicates the accessor ID associated with the job or user.

volser

Indicates the name of volume being violated.

alevel

Indicates the attempted access level.

rlevel

Indicates the user's requested access level.

Action:

No action required.

TSS7201E

VOLUME volser NOT AUTHORIZED FOR ACCESS

Reason:

An unauthorized ACID attempted to access a volume which he or she was not properly authorized to use.

Action:

No action required.

TSS7202E

VOLUME volser NOT AVAILABLE DURING THIS TIME PERIOD

Reason:

The volume is accessible during a restricted time period only.

Action:

No action required.

TSS7203E

VOLUME volser NOT AVAILABLE THIS DAY

Reason:

Volume access is permitted only on certain days.

Action:

No action required.

TSS7204E

VOLUME volser NOT AVAILABLE THROUGH THIS FACILITY

Reason:

Users must access the volume through an authorized facility.

Action:

No action required.

TSS7205E

VOLUME volser NOT ACCESSED THROUGH AUTHORIZED PROGRAM

Reason:

The volume access is restricted via a PRIVPGM rule. The program in use is unauthorized.

Action:

No action required.

TSS7206E

VOLUME volser ACCESS DENIED BY SITE EXIT

Reason:

The attempted access of a volume or data set on a volume failed during the installation exit's volume access validation.

Action:

No action required.

TSS7207E

VOLUME volser REQUESTED ACCESS LEVEL (level) NOT AUTHORIZED

Reason:

An attempt to access a volume or a data set on a volume was not allowed. The user did not own the volume or was not PERMITted to the volume at the requested access level.

Action:

No action required.

TSS7208E

VOLUME volser NOT AUTHORIZED FOR DATASET CREATION

Reason:

A data set cannot be created on the volume because 1) the volume is undefined, or 2) the user is not permitted volume access on the “CREATE” level.

Action:

No action required.

TSS7209E

VOLUME volser ACCESSED BUT NO DATASET NAME PROVIDED

Reason:

The user specified a volume but did not specify a data set name with ACCESS(CREATE).

Action:

No action required.

TSS7210E

VOLUME volser LABEL=BLP VIOLATION

Reason:

An unauthorized attempt was made to use Bypass Label Processing (BLP) for a volume.

Action:

No action required.

TSS7220E

drc J=jobname A=acid VOL=volser ACC=level DSN=dsname

Reason:

This is the summary violation message for unauthorized attempts to access a protected data set. The message is sent to the Security Console, routcde=9.

Action:

No action required.

TSS7221E

DATASET NOT ACCESSIBLE - *data_set_name*

Reason:

The user ACID does not own or is not authorized to access the named data set.

Action:

Have an administrator authorize the ACID through the TSS PERMIT function.

TSS7222E

DATASET NOT AVAILABLE DURING THIS TIME PERIOD

Reason:

Access to the data set is protected on a time-of-day basis.

Action:

No action required.

TSS7223E

DATASET NOT AVAILABLE THIS DAY

Reason:

The access to a data set is protected on a day-to-day basis. At present, access to the data set is not permitted.

Action:

No action required.

TSS7224E

DATASET NOT AVAILABLE THROUGH THIS FACILITY

Reason:

The access to a data set is protected on a facility basis. The current facility is not authorized.

Action:

No action required.

TSS7225E

DATASET NOT ACCESSED THROUGH AUTHORIZED PROGRAM

Reason:

An attempt was made to access a specially protected data set by using a program that was not authorized (via TSS PERMIT PRIVPGM), or the program was not loaded from the library indicated by the LIBRARY parameter on the permit. A PRIVPGM can be in a library that is linklisted as well as specified by the LIB parameter.

Action:

No action required.

TSS7226E

DATASET ACCESS DENIED BY SITE EXIT

Reason:

The site exit failed access to a data set.

Action:

Check with your site programmers to determine the purpose of the installation exit code.

TSS7227E

access ACCESS NOT GRANTED TO DATASET- dsname

Reason:

An ACID is permitted some access to a data set; however, he does NOT possess the required access level for a function he wishes to perform on that data set.

Action:

An administrator must authorize the ACID to the data set at the correct access level via the TSS PERMIT function using the ACCESS parameters.

TSS7228E

DATASET NOT AVAILABLE FROM THIS SYSTEM

Reason:

An ACID is permitted access to a data set with a SYSID authorization disallowing the access.

Action:

An Administrator must authorize the ACID to the data set for the correct system vai the TSS PERMIT function using the SYSID() parameter.

TSS7230E

DSNAME: dsname

Reason:

Indicates the data set for which access was denied.

Action:

No action required.

TSS7231E

UNAUTHORIZED JOB/STEP/TASK LIBRARY FOR DATASET

Reason:

An attempt was made to access a specially protected data set. The library containing the privileged program that is opening the data set is not one which was authorized by the owner.

Action:

The library must be authorized by the owner via a TSS PERMIT LIBRARY operation.

TSS7232E

access ACCESS DENIED TO FETCH-PROTECTED DATASET

Reason:

An attempt was made to open a FETCH-only program library. (If <access> = READ, the open was attempted by a system program that does not perform FETCH access.)

Action:

No action required.

TSS7233E

DATA SET SCRATCH DENIED DUE TO AUTOERASE ERROR

Reason:

The AUTOERASE option has failed.

Action:

A diagnostic dump must be taken; contact CA Technical Support.

TSS7234E

FETCH VIOLATION

Reason:

User attempted to perform a non-FETCH operation against a FETCH-protected data set.

Action:

User needs appropriate access level.

TSS7235E

DATASET GLOBALLY RESTRICTED - dsname

Reason:

One of two situations has occurred:

A user is attempting to open a VSAM data set by a component instead of by cluster, which is the standard VSAM access method.

The site has PRODUCTS (CA TAPE) specified in the Parameter File. A user is attempting to open a tape volume unknown to CA Tape, and does not have ABSTRACT (VCITAPE) or ABSTRACT (CA Tape) authority.

Action:

No action required.

TSS7236E

ENVIRONMENT IS CONTROLLED - UNIX MARK UNCONTROLLED REQUEST REJECTED

Reason:

IREENS00 processing rejected a UNIX request to mark the environment uncontrolled. This situation will happen if IRRENS00 has previously handed a request to keep the environment controlled.

Action:

Check for additional messages (typically with prefix BPX) that accompany this message and take the action specified for those messages.

TSS7237E

ENVIRONMENT IS CONTROLLED - MARK UNCONTROLLED REQUEST REJECTED

Reason:

IRRENS00 processing rejected a request to mark the environment uncontrolled. This situation will happen if IRRENS00 has previously handed a request to keep the environment controlled.

Action:

Check for additional messages that accompany this message and take the action specified for those messages.

TSS7250E

drc J=jobname A=acid TYPE=type RESOURCE=resource

Reason:

This is a summary security violation message which reports unauthorized resource access. Message is routed to Security Console.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7251E

ACCESS DENIED TO resclass<resname>

Reason:

The user is not allowed to access the named resource.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7252E

ACCESS DENIED THIS DAY TO resclass<resname>

Reason:

The resource is protected on a day-to-day basis. It is not available today.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7253E

ACCESS DENIED DURING THIS TIME PERIOD TO resclass<resname>

Reason:

The resource is available during restricted hours only. It is currently not available.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7254E

ACCESS NOT AVAILABLE THROUGH THIS FACILITY TO resclass<resname>

Reason:

The access to the named RESOURCE is illegal because an unauthorized facility is being used.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7255E

ACCESS NOT PERFORMED THROUGH AUTHORIZED PROGRAM TO resclass<resname>

Reason:

An attempt was made to access the named resource but the wrong program was in control.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7256E

ACCESS DENIED BY SITE EXIT to resclass<resname>

Reason:

Your site exit refused the user access to the named resource.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7257E

UNAUTHORIZED ACCESS LEVEL FOR resclass<resname>

Reason:

An attempt was made to access a resource at the wrong level.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7258E

PROGRAM cmd IS NOT AUTHORIZED FOR YOUR USE

Reason:

ACID is not authorized to use the named command.

Action:

The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7259E

ACCESS DENIED TO A RECORD IN RESCLASS<RESNAME>

Reason:

User has attempted to access a protected record to which he is not authorized.

Action:

If access to the record is valid, then a CA Top Secret administrator must grant security access to that record. The resource name can be truncated if RESCLASS MAXLEN>44. To obtain the non-truncated resource name, the user may execute TSSUTIL using REPORT LONG.

TSS7263W

INSUFFICIENT SECLABEL AUTHORITY WARNING

Reason:

A MLS validation failed while in MLMODE(WARN).

Action:

No action required.

TSS7264E

INSUFFICIENT SECLABEL AUTHORITY VIOLATION

Reason:

A MLS validation failed while in MLMODE(FAIL).

Action:

No action required.

TSS7265E

TRANSACTION REVERIFY PASSWORD INCORRECT

Reason:

The password that was entered in an attempt to proceed with the transaction was incorrect.

Action:

No action required.

TSS7266E

TRANSACTION REVERIFY PASSWORD MISSING

Reason:

The transaction requires that a password be entered before the user can proceed.

Action:

Self-explanatory.

TSS7267E

YOU ARE NOT AUTHORIZED TO USE TRANSACTION - transaction

TSS7270E

JOB SUBMIT/ACID AUTHORIZATION FAILED BY SITE SECURITY EXIT

Reason:

The job submission request was failed by the site's security exit code.

Action:

Check with your site programmers to determine the purpose of the installation exit code.

TSS7271E

JOB SUBMIT/ACID AUTHORIZATION DENIED. ACID <acidname> NOT AUTHORIZED FOR YOUR USE

Reason:

An attempt was made to submit a job via TSO SUBMIT or through an internal reader with a USER= parameter.

Action:

Supply an ACID. Re-submit the job.

TSS7272E

JOB SUBMIT/ACID AUTHORIZATION DENIED. ACID <acidname> NOT AUTHORIZED THROUGH THIS FACILITY

Reason:

An attempt was made to submit a job with a hard coded USER= in the JCL, and the ACID specified in the USER= is not authorized through this facility.

Action:

Remove the USER= from the JCL, or submit the job from another facility.

TSS7273E

JOB SUBMIT/ACID AUTHORIZATION DENIED. ACID <acidname> NOT ACCESSED THROUGH AUTHORIZED PROGRAM

Reason:

PRIVPGM on permit to ACID.

Action:

Submit through authorized program.

TSS7279E

RESTRICTED PROGRAM xxxxxxxx IS NOT AUTHORIZED FOR YOUR USE

Reason:

You are trying to execute a program that you are not authorized to use.

Action:

Delete or correct the program name.

TSS7280I

DATASET DELETED BY CATALOG ACCESS

Reason:

The Dataset was either deleted or un-catalogued because the User had Scratch or All access to the catalog for SMS or non-SMS data sets and not the access needed to delete the dataset. For a VSAM data set, it would be All access to the catalog. For a VSAM data set the message appears twice.

Action:

This message appears when CATADELPROT is set to no. No action required.

TSS7285I

Auditing disabled by MATCHLIM for TYPE=<resclass> RSRC=<resname>

Reason:

The specified resource is being audited with MATCHLIM specified. This resources has been logged the maximum number of times allowed by MATCHLIM processing.

Action:

No action required. If further auditing is desired, modify the MATCHLIM control option to specify a higher value or specify CLEAR to clear al logging counts. To log this resource without match limit processing, remove MATCHLIM from the AUDIT record for this resource.

TSS7286I

Auditing disabled by MATCHLIM for ACID <acidname>

Reason:

The specified acid is being audited with MATCHLIM specified. This acid has been logged the maximum number of times allowed by MATCHLIM processing.

Action:

No action required. If further auditing is desired, modify the MATCHLIM control option to specify a higher value or specify CLEAR to clear all logging counts. To log this acid without match limit processing, remove MATCHLIM from the AUDIT record for this acid.

TSS7287E

Audit Match Limit Internal Error - Processing deactivated

Reason:

An internal error occurred during audit match limit processing. Audit match limit processing has been deactivated and all audited events will be logged.

Action:

No action required.

TSS7299I

J=jobacid A=acidname TYPE=resclass RES=resource

Reason:

CA Top Secret sends this message to the security console to log access to resources permitted with an ACTION(NOTIFY).

Action:

No action required.

TSS7450I to TSS7802I

TSS7450I

LMP VERIFICATION COMPLETE

Reason:

LMP product key verification completed successfully. This message is issued in response to an F TSS,LMPCHECK operator console command.

Action:

No action required.

TSS7451E

CAIRIM IS NOT ACTIVE

Reason:

CAIRIM must be started prior to CA Top Secret.

Action:

Start CAIRIM if it has not been started. If CAIRIM has been started, make sure that CAIRIM is at the latest maintenance level and that is has been properly set up with the CA LMP service.

See the *CA Common Services for z/OS Getting Started* (formerly Unicenter TNG Framework for OS/390 Getting Started) and the *CA Common Services for z/OS Administrator Guide* (formerly Unicenter TNG Framework for OS/390 Administrator Guide) for more information regarding CAIRIM and CA LMP.

TSS7452W

CA Top Secret REQUIRES THAT CAIRIM BE ACTIVE

Reason:

LMP product key verification cannot be done because CAIRIM has not been started, the maintenance level of CAIRIM does not contain LMP support, or the LMP product keys have not been correctly defined to CAIRIM. This message can be issued at CA Top Secret initialization or during subsequent LMP verification. Normal operation of CA Top Secret requires that CAIRIM be active with LMP support.

Action:

Start CAIRIM if it has not been started. If CAIRIM has been started, make sure that it is at the latest maintenance level and that it has been properly set up with the CA LMP service.

See the *CA Common Services for z/OS Getting Started* and the *CA Common Services for z/OS Administrator Guide* for more information regarding CAIRIM and CA LMP.

TSS7453W

CA Top Secret OPERATING IN WARN MODE UNTIL THE ABOVE ERROR IS CORRECTED

Reason:

CA Top Secret has switched to WARN mode due to an error in LMP product key verification. The previous message indicates the cause of the problem. All accesses that normally would be prevented will be allowed and logged.

Action:

Take the action as indicated by the previous message.

TSS7454I

CA Top Secret NORMAL PROCESSING RESTORED

Reason:

CA Top Secret has successfully verified the LMP product keys and is no longer running in WARN mode.

Action:

No action is necessary.

TSS7456I

ISSUE CONSOLE COMMAND 'F TSS,LMPCHECK' WHEN THE LMP KEYS HAVE BEEN CORRECTED

Reason:

This message is issued when LMP product key verification has failed.

Action:

When the LMP product keys have been corrected, issue the F TSS,LMPCHECK operator console command to cause CA Top Secret to perform immediate verification. If the command is not issued, CA Top Secret will automatically perform verification every 30 minutes until the error is corrected.

TSS7457E

CPU cpuid REQUIRES A LMP KEY TO RUN PROD (KO) CA TOP SECRET

Reason:

No LMP Key was provided for this CPU.

Action:

Make sure the LMP key for this CPU is properly installed in the key file of CAIRIM in your SYS1.PARMLIB.

TSS7460E

CPU XXXXXX REQUIRES AN LMP KEY TO RUN PROD(CH) CHORUS

Reason:

No LMP key was provided for this CPU.

Action:

Make sure the LMP key for this CPU is properly installed in the key file of CAIRIM in your SYS1.PARMLIB.

TSS7461E

CIA Real Time Deactivated

Reason:

The CIA real-time subtask was deactivated because no LMP key was provided for this system.

Action:

Make sure the LMP key for this CPU is properly installed in the key file of CAIRIM in your SYS1.PARMLIB. Then activate CIA real-time again.

TSS7462E

CIA Real Time Subtask not activated. LMP Key not provided

Reason:

The CIA real-time subtask was not activated because no LMP key was provided for this system.

Action:

Make sure the LMP key for this CPU is properly installed in the key file of CAIRIM in your SYS1.PARMLIB. Then activate CIA real-time.

TSS7800A

CA Top Secret IS NOT ACTIVE, REPLY YES OR NO TO CONTINUE WITHOUT TOP SECRETSECURITY

Reason:

During IDMS/DC initialization, CA Top Secret is not active.

Action:

A reply of <Y> allows IDMS/DC to continue without CA Top Secret security. A reply of <N> causes IDMS/DC to ABEND with a S913 ABEND code.

TSS7802I

CA Top Secret IDMS/DC INTERFACE INITIALIZATION COMPLETE

Reason:

The CA Top Secret IDMS/DC Interface has been activated, and is fully initialized.

Action:

No action required.

TSS8001E to TSS8085E

TSS8001E

CA Top Secret MUST BE ACTIVE

Reason:

CA Top Secret must be active to run TSSUTIL.

Action:

Wait until CA Top Secret is active, then rerun TSSUTIL.

TSS8002E

USER NOT DEFINED TO CA Top Secret

Reason:

Data requested on an ACID which does not exist.

Action:

Define the ACID to CA Top Secret or verify that the ACID has been specified correctly.

TSS8003E

NO AUTHORITY TO USE THIS FUNCTION

Reason:

The ACID requesting this function must be defined to CA Top Secret as an SCA.

Action:

An SCA ACID must request this function.

TSS8004E

NO AUTHORITY (NOT YOUR DEPT)

Reason:

The user requested data on a department outside of his scope.

Action:

Correct TSSUTIL parameters for access to the department.

TSS8005E

NO AUTHORITY (NOT YOUR DIVISION)

Reason:

The user requested data on a division outside of his scope.

Action:

Correct TSSUTIL parameters for access to the division.

TSS8006E

DEPARTMENT UNKNOWN

Reason:

The department requested doesn't exist.

Action:

Define the department to CA Top Secret.

TSS8007E

ACCESSOR ID UNKNOWN

Reason:

Data requested on an ACID which does not exist.

Action:

Define the ACID to CA Top Secret or verify that the ACID has been specified correctly.

TSS8008E

ACCESSOR ID DOES NOT BELONG TO YOUR DEPARTMENT

Reason:

ACID requested is outside the department's scope.

Action:

Correct the department's control statement to include the ACID in the department's scope.

TSS8009E

ERROR IN CONTROL STATEMENT

Reason:

One of the control statements is incorrect.

Action:

See the *Report and Tracking Guide* for correct syntax.

TSS8010E

INVALID CONTROL STATEMENT <xxxxx>

Reason:

Selected invalid criteria options for the types of incidents to be processed.

Action:

See the *Report and Tracking Guide* for the correct criteria options.

TSS8011E

DCA CANNOT SUPPLY DEPT OPTION

Reason:

The DCA ACID cannot specify department.

Action:

Delete the department control statement from the DCA; the default is the DCA's department.

TSS8012E

DEPARTMENT DOES NOT BELONG TO YOUR DIVISION

Reason:

The VCA is requesting a department outside of his scope.

Action:

Delete the department control statement from the VCA or request a department within the scope; the default is all of the VCA's department.

TSS8013E

DIVISION UNKNOWN

Reason:

The division requested is not defined to CA Top Secret.

Action:

Define the division to CA Top Secret or correct the existing division.

TSS8014E

DIVISION NOT WITHIN YOUR SCOPE

TSS8015E

DEPARTMENT NOT WITHIN YOUR SCOPE

Reason:

Self-explanatory.

Action:

Delete or correct the department control statement.

TSS8016E

ACCESSOR ID NOT WITHIN YOUR SCOPE

Reason:

The specified ACID is not within your scope of authority. ACID must be an SCA to run the report.

Action:

Request SCA to run the report, or delete ACID(*) from the control statement.

TSS8017E

INSUFFICIENT REPORT AUTHORITY

Reason:

User does not have ACID(REPORT) administrative authority.

Action:

See the *Report and Tracking Guide* for the correct administrative authorities.

TSS8018E

INVALID DATE OR TIME SPAN

Reason:

Self-explanatory.

Action:

Enter the correct date and time in the proper format.

TSS8019E

STORAGE GETMAIN FAILED

Reason:

Insufficient storage was available for internal buffers. Execution terminates with a Return Code of 16.

Action:

No action required.

TSS8020E

CROSS MEMORY QUEUE FAILURE RC=xxx

Reason:

A cross-memory failure occurred when TSSUTIL attempted to obtain security information. Execution terminates with a Return Code of 12.

Action:

No action required.

TSS8021E

UNDEFINED RESOURCE CLASS NAME: xxxxxxxx

Reason:

Classname given is not defined to the RDT.

Action:

Use a valid class name.

TSS8022E

SMFIN AUDIT FILE NOT PREFORMATTED.

Reason:

Internal format of Audit File is invalid.

Action:

Format the Audit File using TSSMAINT.

TSS8023E

SMFOUT AUDIT FILE NOT PREFORMATTED

Reason:

Internal format of Audit File is invalid.

Action:

Format the Audit File using TSSMAINT.

TSS8025E

UNDEFINED ACCESS LEVEL: access level

Reason:

The access level requested is not defined to CA Top Secret.

Action:

Attempt a different access level.

TSS8026E

UNDEFINED ACCESS RESCLASS: resclass

Reason:

The access resclass specified is not defined to CA Top Secret.

Action:

Attempt a different resclass.

TSS8027E

FAILURE TO OPEN FILE: *xxxxxxxx*

Reason:

An error was encountered when TSSUTIL attempted to use the indicated DD name.

Action:

Insure the correct file and DD are being used and rerun the job.

TSS8028E

NO AUTHORITY (NOT IN YOUR ZONE)

Reason:

The user requested data on a zone outside of his scope.

Action:

Correct the TSSUTIL parameters for access to the zone.

TSS8029E

ZONE UNKNOWN

Reason:

The zone requested doesn't exist.

Action:

Define the zone to CA Top Secret.

TSS8030E

ZONE NOT WITHIN YOUR SCOPE

Reason:

The zone requested is not within your scope of authority.

Action:

Delete or correct the zone control statement.

TSS8032E

DUPLICATE KEYWORD ENTERED

Reason:

A control card keyword parameter has been entered twice on the same report request.

Action:

Remove one of the parameters and resubmit the TSSUTIL job.

TSS8033E

AT LEAST ONE SMFOUT RECORD TRUNCATED

Reason:

Only the SMFOUT DD statement was supplied to TSSUTIL for the EXTRACT function, and at least one record written to the file needs to be truncated.

Action:

Add the XTROUT DD statement to the JCL to produce an extract file with LRECL=27994.

TSS8034E

ERROR: STORAGE OBTAIN FOR INPUT BUFFER HAS FAILED.

Reason:

Available storage is insufficient for allocating the input buffer.

Action:

Contact CA Support for assistance.

TSS8035E

KEYWORD ERROR: MISSING CLOSING PARENTHESIS

Reason:

When processing a keyword and its parameters (if any), TSSUTIL reached the end of the keyword specification before reaching the closing parenthesis.

Action:

Correct the entry by ensuring that a closing parenthesis appears after the last item in the keyword specification.

TSS8036E

KEYWORD ERROR: INVALID CONTINUATION CHARACTER OR COMMENT LINE FOUND.

Reason:

A continuation character or comment line cannot in the middle of a keyword parameter list.

Action:

Remove the characters. Include these characters only at the end of lines TSSUTIL ignores everything from the continuation character through the start of the next line.

TSS8037E

FILTER SUBROUTINE FAILED: INVALID SPECIFIC RESOURCE FLAG…

Reason:

A storage overlay problem has occurred.

Action:

Contact CA Support for assistance.

TSS8080E

GETMAIN FAILED

Reason:

TSSCPR was unable to acquire a sufficient amount of memory for its work area.

Action:

No action required.

TSS8081E

MUST BE A MSCA or SCA

Reason:

User is not a MSCA or SCA

Action:

Sign-on with MSCA or SCA Control ACID.

TSS8082E

I/O ERROR DD - *xxxxxxxx*

Reason:

An I/O error was encountered for DD *xxxxxxxx*.

Action:

No action required.

TSS8083E

CA Top Secret IS NOT ACTIVE

Reason:

CA Top Secret must be active to run TSSCPR.

Action:

Attempt to rerun when CA Top Secret is up.

TSS8084E

INVALID CPF RECOVERY FILE

Reason:

The CPF Recovery File is not valid.

Action:

Insure that the DSNAME for the dd CPFFILE is a valid CPF Recovery File and rerun.

TSS8085E

OPEN ERROR DD - xxxxxxxx

Reason:

The dd-name of xxxxxxxx could not be opened.

Action:

No action required.

TSS8110I to TSS8199E

TSS8110I

AUTHORIZE RECOVERY PROCESSING

Reason:

CA Top Secret is not active to validate use of the TSSRECVR utility.

Action:

See TSS8111A

TSS8111A

REPLY: <Y> TO ALLOW; <N> TO ABORT

Reason:

See message number TSS8110I

Action:

To continue use of TSSRECVR, reply: Y, else, reply: N.

TSS8112E

SYNAD ERROR - error text

Reason:

An I/O error was encountered while processing the Recovery File.

Action:

If error is not due to a HARDWARE problem, get the dumps or traces and contact CA Technical Support.

TSS8125E

OPTION UNKNOWN OR INVALID

Reason:

An option specified in the control statement is invalid.

Action:

No action required.

TSS8126E

MEMBER NOT FOUND

Reason:

The member specified in the member operand of an APF control statement does not exist.

Action:

No action required.

TSS8127E

LIBRARY DOES NOT EXIST

Reason:

A program library specified in the statement identified by the DDNAME operand of an APF control statement, or searched as the result of a global scan of IEAAPFXX and LNKLSTXX members, does not exist. Although an S213-04 ABEND code occurs, TSSAUDIT recovers and continues processing.

Action:

No action required.

TSS8128E

SYSTEM ABEND XXX-XX OCCURRED

Reason:

This message is issued by an OPEN exit which TSSAUDIT uses to process S213 ABENDs that may occur when it attempts to open non-existent data sets whose names appear in IEAAAPFXX and LNKLSTXX members of SYS1.PARMLIB. After issuing this message, TSSAUDIT recovers and continues execution.

Action:

No action required.

TSS8130E

VOLUME XXXXXX IS NOT MOUNTED

Reason:

TSSAUDIT attempted to dynamically allocate a data set that resides on a volume not currently mounted.

Action:

No action required.

TSS8131E

DYNAMIC ALLOCATION FAILED WITH ERROR CODE=code

Reason:

An attempt to dynamically allocate a data set failed. The SVC 99 Error Code is included in the message to provide further information about the cause of the error. These error codes are explained in the IBM Manual, SPL: Job Management.

Action:

No action required.

TSS8132E

DATA SET IS NOT A PROGRAM LIBRARY

Reason:

A data set defined in the DD-statement specified in the DDname operand in an APF control statement is not a load module library.

Action:

No action required.

TSS8133E

ERROR READING DATA RECORDS FOR MEMBER xxxxxxxx

Reason:

While using BSAM to read records in the indicated PDS member, TSSAUDIT experienced an I/O error.

Action:

No action required.

TSS8134E

FIND FUNCTION FAILED FOR MEMBER xxxxx

Reason:

I/O Error occurred opening PDS member.

Action:

No action required.

TSS8135E

ERROR READING LIBRARY DIRECTORY

Reason:

While using BSAM to read the directory of the PDS being processed, TSSAUDIT experienced an I/O error.

Action:

No action required.

TSS8136E

FILE DDNAME OPEN FAILURE 2

Reason:

The data set defined by the indicated DD-statement could not be opened.

Action:

No action required.

TSS8137E

FILE DDNAME OPEN FAILURE 1

Reason:

The directory for the data set defined by the indicated DD-statement could not be opened for processing.

Action:

No action required.

TSS8138E

FILE xxxxxxxx NOT DEFINED IN JCL

Reason:

The DD-statement specified in the DDNAME operand of an APF control statement is not in the job's JCL.

Action:

No action required.

TSS8139E

CANNOT ALLOCATE PARMLIB

Reason:

An attempt to dynamically allocate the SYS1.PARMLIB data set failed.

Action:

No action required.

TSS8140E

FIND FAILED FOR MEMBER

Reason:

Attempting to locate the beginning of data for an IEAAPFXX or LNKLSTX member of a PARMLIB data set, TSSAUDIT received a nonzero Return Code from the find SVC.

Action:

No action required.

TSS8141E

INVALID PARMLIB - DSN

Reason:

Both the DDNAME and PARMLIB operands were specified, but the data set defined in the DD-statement was not a PARMLIB data set.

Action:

No action required.

TSS8142E

OPEN FAILED FOR DSN=DSN

Reason:

The indicated data set could not be opened for processing.

Action:

No action required.

TSS8143E

READ JFCB FAILED

Reason:

The JFCB associated with the SYS1.PARMLIB data set (or alternate data set indicated via the DDNAME and PARMLIB operands) could not be read.

Action:

No action required.

TSS8144E

SYNAD ERROR

Reason:

An I/O error that cannot be corrected occurred while attempting to read the CA Top Secret Recovery File. The “text” includes diagnostic data obtained via the SYNAD exit for the Recovery File.

Action:

No action required.

TSS8145E

NO FUNCTION SPECIFIED

Reason:

The first keyword specified as input to TSSAUDIT was not a valid TSSAUDIT function.

TSS8146E

Invalid LRECL or BLKSIZE on RECOVERY file.

Reason:

Wrong file specified for RECOVERY file for TSSAUDIT program.

Action:

Correct JCL to specify a valid RECOVERY file.

TSS8170E

TSSTRACK ENVIRONMENT ERROR

Reason:

The CA Top Secret address space was not active when TSSTRACK was run.

Action:

When CA Top Secret is active, run TSSTRACK.

TSS8171E

TRACKING TERMINATED WITH ERROR

Reason:

TSSTRACK was terminated. Will result in User Abend 1801.

Action:

Retry TSSTRACK. If problem persists, contact Technical Support.

TSS8172E

INVALID NUMERIC VALUE - ????????

Reason:

The value supplied (????????) for a TSSTRACK selection criteria/Control Option was invalid for the following reasons:

- It did not fall within the valid numeric range for the selection criterion; or,
- It was not numeric. The request to change the value is suppressed.

Action:

Correct the syntax error indicated and re-specify the option.

TSS8173E

SYNTAX ERROR IN OPTION - ???????

Reason:

A valid TSSTRACK selection criteria/control option has been entered, but the value specified (???????) for it is invalid. The option is ignored.

Action:

Correct the syntax error indicated and re-specify the option.

TSS8174E

UNKNOWN PARAMETER ENCOUNTERED - ???????

Reason:

'???????' from the input to TSSTRACK is not a valid selection criteria/control option.

Action:

Remove the incorrect parameter and re-specify other options if coded on the TSSTRACK Options prompt.

TSS8175E

UNLOCK LOCK FUNCTION FAILED

Reason:

The indicated function, locked or unlocked unsuccessfully due to receiving a non-zero return code from CA Top Secret. Function is ignored.

Action:

For the UNLOCK function, reissue the UNLOCK TSSTRACK control option and re-specify the correct password to message TSS8176A.

TSS8176A

ENTER PASSWORD TO UNLOCK THIS TERMINAL

Reason:

The TSSTRACK UNLOCK control option was specified.

Action:

Enter the correct CA Top Secret password to unlock the terminal.

TSS8177E

UNABLE TO OPEN HARDCOPY SYSOUT

Reason:

The SYSOUT data set allocated as a result of the hardcopy selection criterion could not be opened. The request for hardcopy logging is ignored.

Action:

To return to the TRACKing information display, press the ENTER key. To reenter the hardcopy selection criterion, press the PA1 key (3270 terminals) or the BREAK key (non-3270 terminals).

TSS8178E

UNABLE TO ALLOCATE xxxxxx

Reason:

TSSTRACK was unable to dynamically allocate the file indicated (xxxxxx).

Action:

See message TSS8180E. Function is terminated.

TSS8179E

THE AUDIT/TRACKING FILE IS NOT AVAILABLE

Reason:

TSSTRACK unable to access the Audit/Tracking File.

Action:

Retry when the Audit/Tracking File is available.

TSS8180E

RF=*rrrr*, EC=*cccc*, IC=*zzzz*, DDN=*xxxxxxxx*,*aaaaaaa*

Reason:

TSSTRACK was unsuccessful in dynamically allocating a file. This message gives helpful information to determine why the Dynamic Allocation request failed.

rrrr

Indicates the return codes from Dynamic Allocation.

cccc

Indicates the error code.

zzzz

Indicates the information code.

xxxxxxxx

Indicates the DD name of file TSSTRACK was trying to allocate.

aaaaaa

Indicates the data set name of file to be allocated if not SYSOUT.

Action:

Contact CA Technical Support.

TSS8181I

ONLINE TRACKING TERMINATED

Reason:

Issued in response to the “End” or “Stop” selection criterion. Execution terminates with a Return Code of 0.

Action:

No action required.

TSS8182E

INITIALIZATION ERROR

Reason:

TSSTRACK not able to initialize.

Action:

Reissue TSSTRACK later.

TSS8183E

UNABLE TO ESTABLISH ATTENTION EXIT

Reason:

A TSO attention exit could not be established. Execution terminates with a Return Code of 36.

Action:

No action required.

TSS8184I

AUDIT AUDIT2 File WRAP DETECTED AT hh:mm:ss

Reason:

CA Top Secret reused a data block on the Audit/Tracking File indicated in the message while TSSTRACK was processing a request to display the oldest events on the file.

Action:

This message is informational. The requested events are no longer available to TSSTRACK.

TSS8185E

UNABLE TO GETMAIN ENOUGH BUFFER STORAGE

Reason:

Insufficient storage was available for internal buffers. Execution terminates with a Return Code of 16.

Action:

No action required.

TSS8186E

AUDIT/TRACKING FILE IS NOT FORMATTED

Reason:

The Audit/Tracking File has not been formatted by the TSSMAINT Utility. Execution terminates with a Return Code of 20.

Action:

No action required.

TSS8187E

CONFLICTING/INCORRECT OPTION SPECIFIED - xxxxxxx

Reason:

The control options passed to TSSTRACK contain a conflict or the function is not supported by the terminal device. The variable, 'xxxxxxx' located in the message, is the control option in conflict, or it is incorrectly specified.

Action:

Review the control options and re-specify. Also, see the *Report and Tracking* Guide.

TSS8188E

AUDIT/TRACKING FILE IS EMPTY.

Reason:

No records were found in the Audit/Tracking File. Execution terminates with a Return Code of 20.

Action:

No action required.

TSS8189E

UNABLE TO OPEN AUDIT/TRACKING FILE

Reason:

The Audit/Tracking File could not be opened. Execution terminates with a Return Code of 16.

Action:

No action required.

TSS8190I

TSSTRACK FUNCTION COMPLETED

Reason:

Self explanatory.

Action:

No action required, informational message.

TSS8191E

NO AUTHORITY TO USE TSSTRACK

Reason:

You are not authorized to use the TSSTRACK Utility. Execution terminates with a Return Code of 8.

Action:

Obtain proper administration authorities; see the *Report and Tracking* Guide.

TSS8192A

ENTER TSSTRACK SELECTION CRITERIA/OPTIONS:

Reason:

TSSTRACK detected that the PA1/Attention key was hit or no Selection criteria/control options were specified on the TSSTRACK command/transaction.

Action:

Enter valid TSSTRACK selection criteria/control option parameters.

TSS8193A

ENTER LIST OF DETAIL REASON CODES, SEPARATED BY COMMAS

Reason:

TSSTRACK found the DRC control option, but no detail violation error reason codes were specified.

Action:

Enter Detail Error Reason: Code in hexadecimal notation, separated by commas.

TSS8194I

UNLOCK LOCK FUNCTION SUCCESSFUL

Reason:

Self explanatory.

Action:

No action required.

TSS8195W

UNLOCK IGNORED, TERMINAL NOT LOCKED

Reason:

The TSSTRACK UNLOCK function was specified, but the terminal was not in a locked condition.

Action:

Issue the LOCK control option if terminal must be locked.

TSS8196I

SELECTED EVENTS NOT FOUND

Reason:

Using the selection criteria specified, TSSTRACK could not find any matching events on the Audit/Tracking file(s).

Action:

No action required. Informational message.

TSS8197E

DETAIL ERROR REASON CODE NOT FOUND - xx

Reason:

The description of the DRC code specified is not available.

Action:

No action required. Informational message.

TSS8199E

TSSTRACK FUNCTION FAILED, REASON=xxxxxxxx

Reason:

TSSTRACK could not continue processing due to an error.

Action:

'xxxxxxxx' can be one of the following reasons:

ATTACH FAIL

TSSTRACK subtask ATTACH SVC was unsuccessful. Check OSCORE value and notify CA-Technical Support.

SYNTAX-ERROR

An invalid keyword or a keyword with an invalid or improper value was specified. Specify the proper keyword/parameter.

CMODE-LIMIT

The maximum number of terminals that TSSTRACK can support in Continuous Mode has been reached. No other TSSTRACK sessions in Continuous Mode are allowed. Execute TSSTRACK at a later time, if the problem persists contact CA-Technical Support.

NO-CMODE-TRM

An attempt was made to terminate "continuous" (CMODE) TSSTRACK sessions in CICS with one of:

- TSS TRACK=OFF,TERM=(trm1)
- TSS TRACK=OFF,TERM=(ALL)

None of the specified terminals were identified as running in "continuous" mode. To terminate "interactive mode" sessions in CICS, press F3 or F15, at the terminals where the sessions are taking place. If an individual terminal ID has been misspecified in TERM=(trm1), reissue the TSS command transaction with the correct terminal id.

STRG-UNAVAIL

TSSTRACK under CICS could not obtain the amount of DSA storage needed to continue processing. Execute TSSTRACK at a later time.

TSS8324E to TSS8399I

TSS8324E

USER IS NOT AUTHORIZED TO APPLY CRYPT KEY

Reason:

User is attempting to set the Encryption Key for the Security File. The user is not authorized to do so, or CA Top Secret is not active.

Action:

Check that the user is an SCA and that CA Top Secret is active.

TSS8330I

ENTER <SIMULATOR COMMAND> OR <END>

Reason:

TSSSIM is ready to process the next command.

Action:

Enter a valid command or END to terminate the simulation.

TSS8331I

TSS SIMULATION MONITOR ENDED

Reason:

Terminal operator has ended simulation.

Action:

No action is necessary.

TSS8332E

CA TSS IS NOT CURRENTLY ACTIVE

Reason:

The CA Top Secret address space was not active when TSSSIM was run. CA Top Secret is required to obtain Security File information during the simulation process.

Action:

Rerun when CA Top Secret is active.

TSS8333E

RSSCSIM0 INSUFFICIENT MEMORY.

Reason:

A GETMAIN has failed due to insufficient memory.

Action:

Allocate more memory and rerun.

TSS8334E

TSS/SIMULATOR VERSION MISMATCH.

Reason:

The version of TSSRSIM0 you attempted to run is not the same as the currently running version of CA Top Secret.

Action:

Investigate what version of CA Top Secret is running and use the correct version of TSSRSIM0 for that version.

TSS8335E

INVALID/MISSING SECURITY ENVIRONMENT.

Reason:

TSSSIM has found that no security environment has been established for this administrator.

Action:

No action required.

TSS8336E

SIMULATOR MODULE ENVIRONMENT ERROR.

Reason:

TSSSIM was unsuccessful in locating a simulator load module or the user does not have access to TSSSIM.

Action:

Check the install or give the user MISC1(TSSSIM) authority.

TSS8337E

TSSSIM IS ALREADY ACTIVE AT YOUR TERMINAL

Reason:

TSSSIM cannot be active under both screens of a split-screen session.

Action:

No action required.

TSS8338E

YOU ARE NOT AUTHORIZED TO USE TSSSIM.

Reason:

You do not have sufficient authority to use TSSSIM.

Action:

Obtain proper administrative authorities and retry.

TSS8339E

INVALID MONITOR SUFFIX CHARACTER.

Reason:

Unable to determine for interrupt.

Action:

Terminate TSSSIM and reinitiate the process.

TSS8341E

ENVIRONMENT COMMUNICATION ERROR -- MESSAGES LOST.

Reason:

No text buffer was returned from the simulation module.

Action:

Contact CA Technical Support.

TSS8342E

INTERNAL SYSTEM ERROR -- SIMULATION SUBTASK ABEND.

Reason:

The simulator subtask has abended.

Action:

Contact CA Technical Support.

TSS8343E

INTERNAL SYSTEM ERROR -- INITIALIZATION SUBTASK FAILURE.

Reason:

The simulator subtask has abended.

Action:

Contact CA Technical Support.

TSS8344E

INTERNAL SYSTEM ERROR -- SFS RC = (xxx)

Reason:

An error has occurred while trying to retrieve security information from the Security File.

Action:

Contact CA Technical Support.

TSS8351E

CA Top Secret IS NOT CURRENTLY ACTIVE

Reason:

The CA Top Secret address space was not active when TSSIM was run. TSS is required to obtain Security File information during the simulation process.

Action:

Return when CA Top Secret is active.

TSS8352E

UNABLE TO ALLOCATE DDNAME = dsname

Reason:

TSSSIM could not successfully dynamically allocate (or open) the indicated data set name.

Action:

No action required.

TSS8353E

<module> - INSUFFICIENT MEMORY, GETMAIN FAILED

Reason:

The module has been unable to acquire sufficient memory for its work area.

Action:

No action required.

TSS8354E

CA Top Secret/TSSSIM VERSION MISMATCH

Reason:

Different versions of CA Top Secret and TSSSIM are incompatible, for example, TSSSIM version 4 will not operate if version 3 is currently running.

Action:

No action required.

TSS8355E

MISSING/INVALID SECURITY ENVIRONMENT

Reason:

TSSSIM has found that no security environment has been established for this administrator.

Action:

No action required.

TSS8356E

TSSSIM ENVIRONMENT ERROR(S)

Reason:

TSSSIM was unsuccessful in locating a simulator load module.

Action:

Check the install of TSSSIM.

TSS8357E

TSSSIM IS ALREADY ACTIVE AT YOUR TERMINAL

Reason:

TSSSIM cannot be active under both screens of an ISPF split-screen session.

Action:

No action required.

TSS8358E

YOU ARE NOT AUTHORIZED TO USE TSSSIM

Reason:

You do not have sufficient authority to use TSSSIM.

Action:

User must have MISC1(TSSSIM) administrative authority.

TSS8359E

ISPLINK LOADMOD NOT FOUND

Reason:

TSSSIM was unsuccessful in locating the ISPLINK.

Action:

Verify that load module ISPLINK resides in a link-listed library.

TSS8360E

UNKNOWN COMMAND

Reason:

The length of simulator subcommand was less than 2 or greater than 9, or the name of simulator subcommand was unknown to TSSSIM.

Action:

For listing the simulator subcommands, enter HELP under TSSSIM running in TSO/E or BATCH mode.

TSS8361E

KEYWORD keyword IS MISSING OR INVALID

Reason:

An expected/required keyword was omitted from the subcommand or the subfield for the specified keyword was invalid.

Action:

No action required.

TSS8362E

COMMAND REQUIRES AN ACTIVE SIMULATED SESSION

Reason:

The last simulator subcommand entered is only valid when a simulated security environment has been established via the simulator LOGON or SIGNON command.

Action:

No action required.

TSS8363E

RESERVED COMMAND IS NOT AVAILABLE

Reason:

The last simulator subcommand entered is reserved for future use but is currently unavailable.

Action:

No action required.

TSS8364E

INSUFFICIENT SESSION AUTHORITY FOR THIS COMMAND

Reason:

You do not have sufficient authority to issue this simulator subcommand.

Action:

Obtain proper administrative authorities and reissue command.

TSS8365E

RESOURCE IS NOT OWNED WITHIN YOUR SCOPE

Reason:

The resource you are checking is not owned within your scope of authority.

Action:

No action required.

TSS8367E

RESOURCE NOT DEFINED in SYSRDT OR SIMCMD : xxxxxxxxx

Reason:

The simulator subcommand entered by users was not found in TSS Resource Class Name Table (SysRDT) or Simulator Command Name Table (SimCMD).

Action:

For listing the simulator subcommands, enter HELP under TSSSIM running in TSO/E or BATCH mode.

TSS8368E

RESCLASS NOT SIMULATABLE (TSS INTERNAL-USE) : xxxxxxxxx

Reason:

The resclass name selected from the simulator's ISPF-Dialog panel or the resclass name on the simulator subcommand beginning with $ or @ sign entered in TSO/E or BATCH mode, is not allowed to simulate because it is reserved for TSS internal-use ONLY.

Action:

No action required.

TSS8370I

SIMULATED SESSION SUCCESSFULLY ESTABLISHED

Reason:

This is an informational message indicating that no errors were encountered while processing the simulator LOGON or SIGNON commands. You may now issue resource-checking subcommands on behalf of the simulated acid session.

Action:

No action required.

TSS8371E

SIGNON ERROR(S) ENCOUNTERED - SESSION NOT ESTABLISHED

Reason:

TSSSIM encountered an error while processing the simulator LOGON or SIGNON command. This message is usually preceded by message TSS8385I, which contains more detailed information regarding the error. Resource check subcommands cannot be entered at this time, since the simulated acid session was not established.

Action:

No action required.

TSS8372W

NOTE: ACID IS SUSPENDED. .in 0 .ir 0

Reason:

This is a warning message indicating that the simulated ACID is currently suspended; however, LOGON/SIGNON processing continues.

Action:

No action required.

TSS8373W

NOTE: FACILITY IS NOT IN USE AT YOUR SITE

Reason:

This is a warning message indicating that the “in-use” bit is not currently set in the facility matrix for the desired facility. LOGON/SIGNON processing continues.

Action:

No action required.

TSS8374W

NOTE: FACILITY IS CURRENTLY DEACTIVATED.

Reason:

This is a warning message indicating that the requested facility is not currently accepting actual logons; however, the simulator LOGON/SIGNON processing continues.

Action:

No action required.

TSS8375W

NOTE: ACID IS NOT AUTHORIZED TO USE THIS FACILITY

Reason:

This warning indicates that the simulated ACID is not authorized to use the requested facility. LOGON or SIGNON processing continues.

Action:

No action required.

TSS8376W

NOTE: ACID IS NOT AUTHORIZED TO USE THIS CPU

Reason:

This is a warning message indicating that the simulated ACID is not authorized to use the current CPU. LOGON/SIGNON processing continues.

Action:

No action required.

TSS8377W

NOTE: ACID IS NOT AUTHORIZED TO USE THIS TERMINAL

Reason:

This is a warning message indicating that the simulated ACID is not authorized to use the requested terminal. LOGON or SIGNON processing continues.

Action:

No action required.

TSS8378W

NOTE: ACID HAS BEEN INACTIVE TOO LONG

Reason:

This is a warning message indicating that the simulated ACID has been inactive too long; however, LOGON/SIGNON processing continues.

Action:

No action required.

TSS8379W

NOTE: ACID IS NOT WITHIN YOUR SCOPE

Reason:

This warning indicates that the simulated ACID is not within your scope of authority. LOGON or SIGNON processing continues; however, when the session is established, resource checks are limited to those resources which fall within the administrator's scope.

Action:

No action required.

TSS8380I

SIMULATED RESOURCE ACCESS GRANTED

Reason:

This message is issued by TSSSIM to indicate that the ACID, which had simulated logon, is allowed to access the requested resource with current permissions. In non-FAIL modes, access can be granted in spite of violation.

Action:

No action required.

TSS8381I

SIMULATED RESOURCE ACCESS DENIED.

Reason:

This message is issued by TSSSIM to indicate that the ACID (which simulated logon for this session) would not have been allowed to access the resource requested with current permissions.

Action:

No action required.

TSS8385I

<SVCNAME> R15 = xx RC = xx DRC = xx VDRC=xx

Reason:

TSSSIM issues this message to summarize the results of a simulated resource request or resource check.

SVCNAME

Normally indicates the macro used to perform the simulated access (RACINIT, RACHECK, RACDEF, FRACHECK); in the case of $DSN checks, RENAME may also appear.

R15

Refers to the value of R15 when returned from the macro.

RC

Indicates the value of the security return code, and normally agrees with the value of R15.

DRC

Indicates the detailed reason code to explain the nature of the violation.

VDRC

Indicates the detailed reason code to explain the nature of a volume check during data set checking.

Additional parameters may be returned for support diagnostics.

Action:

No action required.

TSS8386I

<NO FEEDBACK MESSAGES>

Reason:

This TSSSIM message indicates that no feedback data has been returned from the simulated security request.

Action:

No action required.

TSS8390I

RESOURCE = (c) xxxxxxxx

Reason:

TSSSIM informational message showing the resource being simulated.

c

Indicates the resource class code in hexadecimal.

xxxxxxxx

Indicates the resource entity name.

This trace message display to assure the administrator that CA Top Secret checked the proper resource entity name.

Action:

Informational message. No action necessary.

TSS8389I

RESOURCE CLASS TRANSLATED (xxxx) : (yyyy)

Reason:

TSSSIM informational message showing that a resource class translation has occurred during the security check event.

XXXX

The original resource class code in hexadecimal

YYYY

The translated resource class code in hexadecimal

Action:

Informational message, no action necessary.

TSS8391I

TSS SVC=ss RC=rr DRC=dd VDRC=vv XSW=xx ALG=aa

Reason:

TSSSIM informational messages providing trace information summary:

- ss Security SVC called for the resource check: (00=FRACHECK, 82=RACHECK, 83=RACINIT, 85=RACDEF).
- rr CA Top Secret Security return code
- dd CA Top Secret Detailed Reason: Code for the resource
- vv CA Top Secret detailed reason code for volumes
- xx Algorithm results (00= auth, 04=not found, 08=unauthorized)
- aa Algorithm selection (00=override, 80=merge, 40=allmerge)

Action:

Informational message, no action necessary.

TSS8392I

REQUESTED ACCESS = nnnnnnnn

ALLOWED ACCESS = nnnnnnnn

<VOLUME ACCESS = nnnnnnnn>

Reason:

TSSSIM trace message indicating the access level requested and the access level allowed for the $SIGNON ACID. (The resource for the request will have been provided by a prior TSS8390I message.) In the case of a DATASET access request, the VOLUME allowed access will also be shown.

Action:

Informational message, no action necessary.

TSS8393I

OVERRIDES = xxxxxxxx,xxxxxxxx,...

Reason:

This is a TSSSIM TRACE message, which lists the overrides allowed for the simulated ACID. Any or all of the following overrides may be displayed:

- DSN (indicates NODSNCHK active)
- LCF (indicates NOLCFCHK active)
- RES (indicates NORESCHK active)
- SUB (indicates NOSUBCHK active)
- VOL (indicates NOVOLCHK active)
- USR-BYP (indicates BYPASS control option specifies ACID or JOB)
- EMG-BYP (indicates BYPASS control option specifies EVERYJOB)

Action:

Informational message, no action necessary.

TSS8394I

RES ORIGIN = rrrrrrrr - lllllllll

Reason:

This is a TSSSIM TRACE message, which lists whether the resource is OWNED or PERMITTED (rrrrrrrrr) as well as the location (lllllllll=*USER* | *ALL* | PROFILE = profile) for which the ownership/permission was retrieved.

Action:

Informational message, no action necessary.

TSS8395I

RES RULE # = nnn

Reason:

This is a TSSSIM TRACE message, which lists the position of the ownership/permission within the “location” displayed by message TSS8394I.

Action:

Informational message, no action necessary.

TSS8397I

SECURITY PERMISSION INFORMATION

Reason:

This is a TSSSIM TRACE message, displaying the permission specifications for the ownership/permission identified by TSS8394I. Typical characteristics include:

RESOURCE

Indicates the resource name.

ACCESS

Indicates the permitted access.

FACILITY

Indicates the facility restriction.

PRIVPGM

Indicates the program restriction.

Action:

Informational message. No action is necessary.

TSS8398I

VOLUME FEEDBACK: fl f2 f3 f4

Reason:

This is a TSSIM TRACE message, which displays bitmapped tape volume information. Normally, this is of significance only to CA Top Secret Technical Support to diagnose problems with TSSSIM.

Action:

Informational message, no action necessary.

TSS8399I

SUBRTN FLAGS: f1 f2 f3 f4 f5

Reason:

This is a TSSSIM TRACE message, which displays bitmapped subroutine information. Normally this is of use only to CA Top Secret Technical Support if you report a problem with TSSSIM.

Action:

Informational message, no action necessary.

TSS8400I to TSS8601A

TSS8400I

PARENT SVC = pp CALLING SVC = cc

Reason:

This is a TSSSIM TRACE message, which displays the hexadecimal numbers of the security caller and the security routine being called. This information is mainly of use to CA Top Secret Technical Support when diagnosing problems with TSSSIM.

Action:

Informational message, no action necessary.

TSS8401I

CURRENT/PARENT/BOTTOM PRIVPGM(S) = *cccccccc pppppppp bbbbbbbb*

Reason:

This is a TSSSIM TRACE message, which displays the names of the current (*cccccccc*) program, the PRIVPGM (*pppppppp*) and the "bottom" or "base" program (*bbbbbbbb*) in the active program chain.

Action:

Informational message. No action is necessary.

TSS8407E

INTERNAL SIMULATOR CONTROL BLOCK ERROR (xxxxxxxx).

Reason:

TSSSIM has encountered an unexpected error while identifying the indicated control block.

Action:

Contact CA Technical Support if this error persists.

TSS8408E

UNEXPECTED SECURITY FILE SERVICES ERROR (nnn).

Reason:

TSSSIM has encountered an unexpected non-zero return code from TSS, while attempting to retrieve information from the Security File.

Action:

Contact CA Technical Support if this error persists.

TSS8409E

TSSSIM FATAL ERROR(S).

Reason:

Due to an earlier-printed error message, TSSSIM was unable to continue.

Action:

Notify your systems programmer.

TSS8410I

SIMULATED ACID = aaaaaa QUALIFIER = bbbbbb MODE = cccc

SIMULATED FAC = ddd TERMINAL = eeeeeee CPU = ffff

DEFAULT SVC = ggg NUMBER = hh (HEX) ACCESS = ii

DEFAULT PRIVPGM = jjjjjj DEFAULT LIBRARY = kk

SECURITY TRACE = ll

Reason:

This message displays information about an ACID in response to a TSSSIM STATUS command.

The following information is displayed:

- Name of simulated ACID
- Data set qualifier
- simulation mode
- Simulated facility
- Terminal name
- CPU
- Default SVC name, number, and associated access
- Default privileged program PRIVPGM
- Default library
- Default TRACE setting

Action:

Informational message, no action necessary.

TSS8411W

DATASET PERMIT WITH LIBRARY UNSUPPORTED

Reason:

The TSSSIM $DSN command does not support checking of a data set permission with the PRIVPRM and LIBRARY specifications.

Action:

No action required.

TSS8429E

UNEXPECTED SECURITY FILE SERVICES COMMUNICATION ERROR (nnn)

Reason:

TSSCHART encountered an unexpected non-zero return code from the CA Top Secret address space when trying to obtain Security File information.

Action:

No action required.

TSS8600I

SECURITY INACTIVE FOR PROTECTION FACILITY

Reason:

Data access request cannot be validated.

Action:

No action required.

TSS8601A

REPLY <Y> TO CONTINUE; <N> TO ABORT

Reason:

To proceed to secure data sets without access validation, reply “Y”. To cancel TSSPROT, reply “N”.

Action:

No action required.

TSS8700E to TSS8860E

TSS8700E

COMMAND IS AMBIGUOUS OR UNKNOWN

Reason:

Keyword entered from TSSCHART or TSSSIM is ambiguous or unknown.

Action:

Enter correct keyword.

TSS8701E

KEYWORD < > IS MISSING OR INVALID

Reason:

Keyword is incorrect or needs to be supplied.

Action:

Provide or correct the specified keyword.

TSS8702E

KEYWORD < > IS AMBIGUOUS OR UNKNOWN

Reason:

Keyword supplied is unknown or requires additional information (additional operands).

Action:

Clarify or correct the specified keyword.

TSS8703E

COMMAND CONTAINS UNBALANCED PARENTHESES

Reason:

Command contains an odd number of parentheses indicating that one parenthesis needs to be added or subtracted.

Action:

Reissue the command with the correct number of parentheses.

TSS8709E

KEYWORD <XXXXXXXX> - SUBFIELD DATA TOO LONG

Reason:

The contents of a subfield of the keyword exceeds the maximum length permitted for that keyword. In the case of a resource class, the maximum length is determined by the MAXPERMIT(...) setting for the resource class.

Action:

Reenter the TSS command, specifying an appropriate subfield length.

TSS8730

TABLE FULL - USER TABLE

Reason:

The table generated to hold the users is full.

Action:

Program terminates. Increase the value for V1 with the TABLES control statement.

TSS8731

USER DOES NOT EXIST ON RACF. NO ACTION TAKEN

Reason:

An ACID or user in a control statement is specified that does not exist on the RACF data base.

Action:

The statement is ignored. No action required.

TSS8732

TABLE FULL - USER DEFINED PROFILE TABLE

Reason:

The user-defined profile table is full.

Action:

Program terminates. Increase the value for V2 with the TABLES control statement.

TSS8733

TABLE FULL - USERS TABLE FOR USER DEFINED PROFILES

Reason:

The user table for user-defined profiles is full.

Action:

Program terminates. Increase the value for V3 with the TABLES control statement.

TSS8734

TABLE FULL - GROUP TABLE

Reason:

The group table is full.

Action:

Program terminates. Increase the value for V4 with the TABLES control statement.

TSS8735

TABLE FULL - USERS TABLE FOR ALL GROUPS

Reason:

The user table for all groups is full.

Action:

Program terminates. Increase the value for V5 with the TABLES control statement.

TSS8736

TABLE FULL - DEPARTMENT TABLE

Reason:

The department table is full.

Action:

Program terminates. Increase the value for V6 with the TABLES control statement.

TSS8737

TABLE FULL - DSN LEVEL

Reason:

The data set level table is full.

Action:

Program terminates. Increase the value for V7 with the TABLES control statement.

TSS8742

TABLE FULL - GROUP OF DSNS ALL IN ONE DEPT

Reason:

The table defining the data sets owned by one department is full.

Action:

Program terminates. Increase the value for V9 with the TABLES control statement.

TSS8743

TABLE FULL - ALL USERS ACCESSING CONTIG GROUP OF DSNS ALL IN ONE DEPT

Reason:

The table defining the users accessing a contiguous group of data sets in one department is full.

Action:

Program terminates. Increase the value for V10 with the TABLES control statement.

TSS8744

TABLE FULL - USERS TABLE FOR PROFILES TO DESCRIBE ALL ACC LISTS WITH PROFILES

Reason:

The table defining all access lists with profiles is full.

Action:

Program terminates. Increase the value for V11 with the TABLES control statement.

TSS8745

TABLE FULL - USERS TABLE FOR DSN ACC LIST

Reason:

The table defining the data set access lists is full.

Action:

Program terminates. Increase the value for V12 with the TABLES control statement.

TSS8746

INVALID SYNTAX WORD

Reason:

An invalid control statement is encountered.

Action:

The statement is ignored. No action required.

TSS8747

VALUE TOO LONG

Reason:

A value specified in a control statement is too long.

Action:

The statement is ignored. No action required.

TSS8748

END OF VALID CONTROL CARDS

Reason:

Control card processing is finished.

Action:

An advisory message. No action required.

TSS8749

NO USERS

Reason:

No users are found on the RACF data base.

Action:

Program terminates. Make sure RACF is active and the RACF data base is valid.

TSS8750

TOO MANY IN LIST OF VALUES

Reason:

A control statement contains too many values in a list.

Action:

The statement is ignored. No action required.

TSS8751

DSN LEVEL NUMBER ERROR, IGNORED

Reason:

A level of ownership less than 1 or greater than 7 is specified in an OWN control statement.

Action:

The statement is ignored. No action required.

TSS8752

DSN LENGTH ZERO, IGNORED

Reason:

A “DSN ( )” is specified in an OWN control statement, which results in a data set length of zero.

Action:

The statement is ignored. No action required.

TSS8753

CONTROL CARD OUT OF SEQUENCE - SKIPPED

Reason:

Control statements are specified out of sequence. OWN control statements must come last.

Action:

Statements after the last OWN control statement are ignored. No action required.

TSS8754

DEPARTMENT NOT FOUND - SKIPPED

Reason:

A department in an ASSIGN control statement is specified that has not been created by the conversion process.

Action:

The statement is ignored. No action required.

TSS8755

GENERIC DEPARTMENT NOT ALLOWED FOR PROFILE NAME SELECTION - SKIPPED

Reason:

A generic department name is specified in an ASSIGN control statement.

Action:

The statement is ignored. No action required.

TSS8859E

VSAM opcd ERROR- RC=rc RS=rs KEY=*SDT recordkey

Reason:

An I/O error occurred accessing the VSAMFILE SDT records associated with the current SECFILE. *opcd* indicates the type of access macro associated with the error: GET, PUT, ERASE, VERIFY, MRKBFR, or POINT. OPEN and CLOSE errors generate standard MVS messages, and will not generate TSS8859E. For information on RC and RS return codes, see the IBM publication *DFSMS Macro Instructions for Data Sets*.

Action:

Call CA Top Secret Support.

TSS8860E

VSAMIRR *opcd* ERROR- RC=*rc* RS=*rs* KEY=*vsam_record_key*

Reason:

An I/O error occurred while accessing the VSAM mirror file that is associated with the current security file. Mirror file processing is now disabled.

opcd

Indicates the type of access macro that is associated with the error: GET, PUT, ERASE, VERIFY, MRKBFR, or POINT. OPEN and CLOSE errors generate standard MVS messages and do not generate TSS8860E.

Note: For information about RC and RS return codes, see the IBM publication *DFSMS Macro Instructions for Data Sets*.

Action:

Analyze the error and, if necessary, allocate and initialize a new mirror file. For example, a physical problem with the disk would require allocating a new file.

TSS9000I to TSS9099I

TSS9000I

CA Top Secret 14.0 140000KO00 ACTIVE

Reason:

The specified version of CA Top Secret is initialized and ready to control security. Where: 14 is the release, 0000 is the Servicepack, KO is the product code and 00 is the version number.

Action:

No action required.

TSS9001I

REINIT COMPLETE

Reason:

CA Top Secret successfully invoked the REINIT Control Option.

Action:

No action required.

TSS9002I

RACF CO-EXISTENCE FEATURE ACTIVE

Reason:

Operator or administrator activated TSS commands by replying T to message number TSS9055A. CA Top Secret administrative commands can only be used to define resources to CA Top Secret.

Action:

No action required.

TSS9003I

AUDIT/TRACKING FEATURE NOT ACTIVE

Reason:

The Audit/Tracking File is NOT being used to record security-related information.

Action:

To create an Audit/Tracking File, see the TSSMAINT utility in the Implemantation *Guide*. To direct security-related information to the Audit/Tracking File, see the LOG control option in the *Control Options Guide*.

TSS9004I

AUTOMATIC BACKUP FEATURE NOT ACTIVE

Reason:

A reminder that the CA Top Secret automatic backup feature is not installed.

Action:

To install automatic backup, see the BACKUP Control Option.

TSS9006E

CA SAF NOT UP. RE-IPL NECESSARY

Reason:

CA SAF was not started prior to your attempt to start CA Top Secret. The installation of CA Top Secret was done incorrectly or a required library is missing from the linklist or lpalist.

Action:

Confirm that the r5.1 CAILPA library is included in the LPA list and and is not included in the linklist, and that no members from the library have been copied into a linklist library. Confirm that SYS1.LINKLIB contains the IBM version of at least one module of ICHSCDMY, ICHSEC00, or ICHSEC05. Assure that none of the IBM versions of these modules are in SYS1.LPALIB or in any LPA list library.

TSS9007E

*****MAJOR VERSION CHANGE RE-IPL NECESSARY*****

Reason:

You are running with a previous release of CA Top Secret; internal control blocks not compatible.

Action:

No action required.

TSS9008E

CA Top Secret ALREADY ACTIVE

Reason:

An attempt to start CA Top Secret has failed because it is already executing. User ABEND 0002 results.

Action:

No action required.

TSS9010E

CANNOT OBTAIN FIXED CSA PAGE

Reason:

CA Top Secret requires a page of Common Storage for cross-memory communication. Insufficient CSA is available for the period, or real storage is insufficient. CA Top Secret can NOT start.

Action:

No action required.

TSS9011W

RECOVERY FILE HAS WRAPPED AROUND

Reason:

The CA Top Secret Recovery File is full. Changes to the Security File will be recorded at the beginning of the File; overwriting current data.

Action:

It is not necessary to back up the recovery file if backups are run daily before the file wraps. If the recovery file is wrapping more than once a day, it should be enlarged.

TSS9012W

RECOVERY FILE IS AT LEAST 90% FULL

Reason:

The CA Top Secret Recovery File is nearly full. Once full, the File's data is overwritten. This message is issued once the file reaches 90% capacity and subsequently, each time CA Top Secret is restarted as long as the condition persists.

Action:

Display the BACKUP control option to determine if a backup of the CA Top Secret Security File is occurring daily. If BACKUP(INACTIVE) is seen on the TSS MODIFY display output, a TSS MODIFY BACKUP command should be issued to request an immediate backup. As long as the TSS9012W message is not occurring more often than the security file is backed up, no action needs to be taken. If the message is occurring more often then the security file is backed up, the recovery file should be enlarged.

TSS9013I

GLOBAL STORAGE NOT FREED

Reason:

CA Top Secret was unable to free CSA unused storage.

Action:

This message is an indication of a potential storage utilization problem. If the problem persists then the DEBUG control option should be enabled via the “F TSS,DEBUG(ON)” which will produce an SVCDUMPT to one of the SYS1.DUMPnn data sets. The option should then be disabled via the “F TSS,DEBUG(OFF)” operator command. Contact CA Technical Support.

TSS9014E

SECURITY FILE BLOCKSIZE ILLEGAL

Reason:

The physical blocksize of the Security File is different from the BLOCKSIZE specified during file creation.

Action:

If the file was just copied, restore the backup copy. Otherwise, use utility TSSMAINT to rebuild the Security File. Do NOT specify a BLOCKSIZE keyword in the JCL.

TSS9015E

ERROR drc DURING SECURITY FILE INITIALIZATION

Reason:

During the CA Top Secret activation process, an error prevented the processing of the Security File.

DRC (xx) = 39 and 4B may indicate incorrect customer key

Action:

Restart CA Top Secret. If problem persists, see 2.

Re-IPL. If problem persists, the Security File may be damaged, and require reconstruction. Contact CA Technical Support if problem is not hardware-related.

TSS9016E

I/O ERROR. RESTORE SECURITY FILE FROM BACKUP PROCESS RECOVERY FILE

Reason:

During the CA Top Secret activation process, an I/O error prevented Security File processing.

Action:

Restore Security File using the latest backup copy.

Use the Recovery Procedures to recover changes that were made to the file. If problem persists, use the backup Security File without recovery. Contact CA Technical Support.

TSS9017I

SFS ABEND RECOVERY COMPLETE

Reason:

The CA Top Secret subtask, SFS, has been successfully reactivated after an ABEND.

Action:

If the ABEND was *not* a result of hardware damage to the Security or Recovery Files, send the dump produced by the ABEND to CA Technical Support.

TSS9018I

SECURITY FILE SERVICES REINSTATED

Reason:

CA Top Secret is able to process requests. See message TSS9017I.

Action:

No action required.

TSS9019E

INVALID START REQUEST

Reason:

You tried to start CA Top Secret from a facility other than as a Started Task.

Action:

Use the START TSS command from a console.

TSS9020WI

INVALID PARAMETER FILE OPTION

Reason:

A data set option reference by the PARMFILE DD-statement is in error. CA Top Secret continues processing.

Action:

Examine your options. To obtain the TSS log, enter the following O/S Console Control Option: F TSS,SYSOUT. The statement preceding the message is the option in error.

TSS9021W

INVALID EXECUTE OPTION

Reason:

A PARM option of the TSS EXEC statement is incorrect.

Action:

Check the PARM of the CA Top Secret Started Task Procedure.

TSS9022I

AUTOMATIC COMMANDS BEING ISSUED

Reason:

The commands in AUTOCMDS File are executing.

Action:

No action required.

TSS9023E

UNABLE TO OPEN AUTOCMDS FILE

Reason:

The AUTOCMDS File cannot be opened. Automatic commands contained in AUTOCMDS are not started.

Action:

Check to ensure that the AUTOCMDS DD-statement in the TSS STC points to a valid data set.

TSS9024E

UNABLE TO OPEN BACKUP FILE

Reason:

The automatic DASD backup file (referenced by the BACKUP DD-statement) is not usable. Automatic backup is ignored. Processing continues.

Action:

No action required.

TSS9025E

UNABLE TO OPEN PARAMETER FILE

Reason:

An attempt to read control options from the Parameter File was unsuccessful due to an open error. Processing continues.

Action:

Check processing options via O/S console control option F TSS,STATUS.

Examine DCB attributes of Parameter File.

TSS9026E

SECURITY FILE UNDEFINED

Reason:

The SECFILE DD-statement is missing from the TSS STC procedure.

Action:

Correct the SECFILE DD-statement in the TSS STC procedure.

TSS9027E

SECURITY FILE UNAVAILABLE

Reason:

CA Top Secret was not able to open and access the Security File.

Action:

Check the TSS STC procedure to ensure that the SECFILE DD-statement properly references the Security File.

TSS9028E

RECOVERY FILE UNDEFINED

Reason:

The RECFILE DD-statement is missing from the TSS STC procedure.

Action:

Correct the RECFILE DD-statement in the TSS STC procedure.

TSS9029E

RECOVERY FILE UNAVAILABLE

Reason:

CA Top Secret was not able to open or access the Recovery File.

Action:

Check the TSS STC procedure to ensure that the RECFILE DD-statement properly references the Recovery File. If recovery processing is not required, use the RECOVER(OFF) option on the START TSS Command.

TSS9030E

PRIMARY AND BACKUP SECURITY FILES IDENTICAL

Reason:

Both the SECFILE and BACKUP DD-statements in the TSS STC procedure reference the same data set name. CA Top Secret has deactivated the automatic backup feature.

Action:

If you are running from the Backup File, ignore this message. Otherwise, ensure that the TSS STC procedure references the correct data set names.

TSS9031E

UNSUPPORTED SECURITY FILE VERSION

Reason:

TSS has detected an older version of the security file which is no longer supported.

Action:

Ensure the security file was created by TSS release 5.2 or higher.

TSS9032E

UNSUPPORTED SECURITY FILE FEATURES

Reason:

TSS has detected a security file with enabled features which are not yet supported by the current release of TSS.

Action:

Ensure the security file was created by the current (or lower) release of TSS.

TSS9033E

VSAMFILE FILE UNAVAILABLE

Reason:

An error occurred while allocating internal storage areas for the VSAM dataset. The VSAM file can not be used.

Action:

Contact CA Technical Support.

TSS9034W

*****WARNING*** USE OF STEPLIB NOT RECOMMENDED**

Reason:

The TSS STC procedure contains a STEPLIB DD-statement. STEPLIB is tolerable during initial testing but is not recommended for long term. CA Top Secret should be link listed to avoid future maintenance problems resulting from duplicate load library modules. If any TSS modules are invoked outside of the TSS address space, there is no guarantee it will work unless the CAILIB is in the linklist or STEPLIBed to all address spaces.

Action:

Remove the STEPLIB DD-statement from TSS STC as soon as possible.

TSS9035E

VSAMFILE OPEN FAILED

Reason:

CA Top Secret was not able to open the VSAM file.

Action:

Check the CA Top Secret startup procedure to ensure that the VSAMFILE DD specifies a VSAM dataset initialized with TSSMAINT.

TSS9036E

RECOVERY FILE UNFORMATTED

Reason:

TSSMAINT was not used to format the Recovery File. Changes made to files cannot be recovered if system ABEND occurs.

Action:

Use TSSMAINT to format the Recovery File.

TSS9037E

VSAMFILE FILE NOT INITIALIZED

Reason:

The VSAM dataset specified on the VSAMFILE DD statement was not initialized with TSSMAINT.

Action:

Run TSSMAINT to initialize the VSAM dataset before using it with CA Top Secret.

TSS9038E

RECOVERY PROCESSING TERMINATED

Reason:

A previously reported recovery error has caused the RECOVERY feature to deactivate.

Action:

Investigate the reported error and check the Recovery File accordingly. Here are some possible causes:

- Damage to the volume (hardware).
- Recovery File was not initialized.
- RECFILE DD-statement is missing or invalid.

TSS9039E

UNEXPECTED RECOVERY END-OF-FILE

Reason:

CA Top Secret was not able to wrap around the Recovery File. Change recovery is deactivated.

Action:

Contact CA Technical Support.

TSS9040WI

SECURITY FILE ENCRYPTION UNAVAILABLE

Reason:

CA Top Secret cannot encrypt the information in the Security File because the customer encryption key has not been supplied.

Action:

Use TSSKEY00 to set your encryption key into CA Top Secret.

TSS9041E

CUSTOMER ENCRYPTION KEY REQUIRED TO UNLOCK FILE

Reason:

See message TSS9040W

Action:

See message TSS9040W

TSS9042A

SPECIFY <ABORT>; ELSE 16 HEX DIGIT KEY

Reason:

CA Top Secret will terminate unless you enter the Customer Encryption Key.

Action:

Enter the key as 16 hexadecimal digits or abort CA Top Secret by entering the command ABORT.

TSS9043W

KEY IS TEMPORARY - ZAP REQUIRED

Reason:

The encryption key being used is temporary. You must eventually place a permanent key into CA Top Secret, via TSSKEY00.

Action:

See message TSS9040W

TSS9044E

INVALID HEX DIGIT IN KEY

Reason:

The Security File Customer Encryption Key contains a character other than 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Action:

Reply to the TSS9042A message again, specifying a valid encryption key value.

TSS9045I

<RDT|FDT> SYNCHRONIZATION COMPLETE

Reason:

During startup CA Top Secret recognized that maintenance had been applied to the load module containing the system RDT/FDT definitions. This message acknowledges that the "synchronization" of the load module with the security file has completed. See message TSS9048I for more complete details.

Action:

Informational message only.

TSS9046I

<RDT|FDT> SYNCHRONIZATION FAILED - reason

Reason:

During startup CA Top Secret recognized that maintenance had been applied to the load module containing the system RDT/FDT definitions. This message acknowledges that the "synchronization" of the load module with the security file has failed due to the "reason" specified in the message.

During startup, CA Top Secret attempted to merge an updated base RDT with the Security File RDT. The merge failed for the indicated reason.

Action:

If the preceding reason text suggests a remedy, perform the suggested process: Stop TSS and REINIT.

If the preceding reason text does not indicate a remedy, contact CA Top Secret Support.

TSS9047E

CA Top Secret MODULE TSSMNGR DOES NOT HAVE REQUIRED APF AUTHORIZATION

Reason:

CA Top Secret was loaded from a library that is not APF-authorized. Processing terminates.

Action:

Ensure that the CA Top Secret load library is in the APF list and that the CA Top Secret modules have been link edited with the AC=1 keyword.

TSS9048I

<RDT> SYNCHRONIZATION RENAMED oldname1 newname1 DUE TO CONFLICT <FDT>

Reason:

The system versions of the RDT and FDT are stored in load modules as well as in the security file. From time to time, CA Top Secret adds new fields to the system FDT and new resource classes to the system RDT. These are distributed through APARs to the software. When a new version of system table is sensed, a “synchronization process” is initiated.

As new FDTNAMEs are added to the system FDT, it is possible that the new system name conflicts with a previously defined user FDTNAME. In such case, the user FDTNAME is renamed to UFLDhhhh (where “hhhh” is the hexadecimal representation of the FDTCODE assigned to the original user defined field).

As new RESCLASS's are added to the system RDT, it is possible that the new system name conflicts with a previously defined user RESCLASS. In such case, the user RESCLASS is renamed to USERhhhh (where “hhhh” is the hexadecimal representation of the RESCODE assigned to the original user defined resource class).

Action:

If programs or products on your system made use of “oldname1”, all affected ACID field references will now point to “newname1”: you will have to re-administer “oldname1” with its new system-supplied definition; or you will have to alter the programs or products so that they reference “newname1” instead.

For FDT definitions, the DISPLAY attribute supplies the text which labels the field value during TSS LIST and WHOHAS commands. Because the default DISPLAY attribute is the FDTNAME, users may believe that their field definitions are intact after synchronization, when in fact they have been altered. To avoid such display anomalies, you may wish to issue:

TSS REP(FDT) FDTNAME(newname1) DISPLAY(oldname1_O)

so that the field will display as:

oldname1_O = value

and thus distinguish your old administration from your new administration.

TSS9049I

CA Top Secret ABEND DURING INITIALIZATION

Reason:

Abend conditions occurred during initialization.

Action:

Restart TSS.

TSS9050E

NO IMS SECURITY

Reason:

A required module was not found in the CA Top Secret library.

Action:

Ensure that the CA Top Secret IMS FMID has been applied.

Make sure the module is linked to the load library.

If more than one load library exists, make sure you are pointing to the correct library.

Restart CA Top Secret.

TSS9051E

OID SUPPORT UNAVAILABLE

Reason:

A required module is missing from the CA Top Secret library.

Action:

See message TSS9050E.

TSS9052E

TSSRDT MODULE MISSING

Reason:

A required module is missing from the CA Top Secret library. CA Top Secret ABENDs with code 99.

Action:

See message TSS9050E.

TSS9053I

- RDT2BYTE OPTION ACTIVATED

Reason:

A resource class with a 2-byte RESCODE has at some time been defined by a CA Top Secret r5.2 system on this security file. Even if the resource class has since been deleted, the changes invoked by this definition to the Security File are irrevocable.

Action:

You are allowed to create additional resource classes in the RDT with 2-byte RESCODEs. However:

1. You cannot share this CA Top Secret Security file with a CA Top Secret 5.1 system.

2. The RDT2BYTE control option will remain activated, even after the option is removed from the Parameter File, and cannot be turned off with the MODIFY command.

The only way to reverse the activation of RDT2BYTE is to work from a BACKUP which does not have RDT2BYTE set; and to forward recover up to the point where RDT2BYTE had been set.

TSS9055A

SELECT PROCESSING: <X> TERMINATE TSS <T> ACTIVATE TSS COMMAND

Reason:

CA Top Secret detects the presence of RACF security.

Action:

Select “X” to terminate CA Top Secret or “T” to activate the TSS command while RACF security is still active.

TSS9055W

RACF SECURITY INTERFACE PRESENT

Reason:

CA Top Secret detects the presence of RACF security.

Action:

Message TSS9055A follows, select the correct option to specify security.

TSS9056E

COMMAND LIMITING & PROGRAM RESTRICTIONS UNAVAILABLE

Reason:

A required module is missing from the CA Top Secret library.

Action:

See message TSS9050E.

TSS9057E

FETCH PROTECTION UNAVAILABLE

Reason:

A required module is missing from the CA Top Secret library.

Action:

See message TSS9050E.

TSS9058E

UNABLE TO LOAD VAM/SPF MODULE VAMINF10, SECURITY WILL ONLY BE IN EFFECT FOR SIGNON.

Reason:

When attempting to initialize VAM/SPF, CA Top Secret was unable to obtain an interface module. Only signon and signoff security will be active.

Action:

Contact CA Technical Support.

TSS9059E

SAF NOT INITIALIZED - CSA SHORTAGE

Reason:

CA Top Secret was unable to install the SAF interface. Processing continues; however, unpredictable results will occur in a non-SU32 (SAF) environment.

Action:

Shut down CA Top Secret with BYPASS DOWN options and restart when CSA shortage is relieved. SAF interface uses less than 1K of CSA.

TSS9060E

SECURITY FILE SYNAD

Reason:

See TSS9063E

Action:

No action required.

TSS9060I

SECURITY FILE I/O ERROR DURING WRITE/READ SENSE=xxxx CSW=xxxxxxxx xxxxxxxx

Reason:

See TSS9063E.

Action:

No action required.

TSS9061E

RECFILE SYNAD

Reason:

An I/O error was returned on the Recovery File.

Action:

Stop CA Top Secret, take a backup of the Recovery File and format the new file, restart CA Top Secret.

TSS9062E

BACKUP FILE SYNAD

Reason:

See TSS9063E

Action:

No action required.

TSS9063E

AUDIT FILE SYNAD

Reason:

An I/O error occurred while processing the specified CA Top Secret File.

Action:

If error is not due to a HARDWARE problem, get the dumps or traces, and contact CA Technical Support.

TSS9064W

SYSOUT CURRENTLY IN USE - RETRY REQUEST

Reason:

An attempt to spin off the Trace Log failed.

Action:

Retry request.

TSS9065A

RESTART TSS WITH REINIT OPTION

Reason:

The REINIT option is only valid when starting up CA Top Secret.

Action:

Stop CA Top Secret and specify the REINIT option using the O/S start command.

TSS9066E

LOGICAL XE ERROR

Reason:

An invalid security record is present in CA Top Secret common storage.

Action:

A diagnostic dump will be taken. Call CA Technical Support.

TSS9066W

UNABLE TO ALLOCATE INTERNAL TRACE/LOG FILE

Reason:

CA Top Secret is unable to dynamically allocate the Trace/Log file.

Action:

Check the SYSOUT parameter in the CA Top Secret Parameter File for an invalid class name or destination. Correct the SYSOUT statement and restart CA Top Secret.

TSS9067W

UNABLE TO OPEN SYSOUT FILE

Reason:

An attempt to use a trace log has failed. Security is not affected.

Action:

No action required.

TSS9068I

TRACE/LOG SPUNOFF

Reason:

This message displays in response to the SYSOUT option.

Action:

No action required.

TSS9069E

TRACE/LOG NOT AVAILABLE

Reason:

TRACE/LOG could not be allocated.

Action:

Retry request.

TSS9069W

CA Top Secret STARTED AS A SUBSYSTEM, JES SYSOUT UNAVAILABLE. TRACE/LOG FILE IGNORED

Reason:

In CA Top Secret r5.3 and above, if CA Top Secret starts before JES is fully initialized, the $$$LOG$$ file will be suppressed until such time as JES becomes available, and entries which might have been written to the file will be ignored. When JES does become available, the file will be allocated according to the SYSOUT control option. The associated message $HASP250 TSS53 PURGED - (JOB KEY WAS BBA71465) may be ignored, when TSSMNGR4 attempts to spin off a non-existent old version of the log.

Action:

If you intended to start CA Top Secret before JES, the task is operating as designed. If you had intended to start after JES was completed, remove the SUB=MSTR operand from the operator command used to start the product.

TSS9070WI

SYSOUT UNAVAILABLE, CPF JOURNAL FILE IGNORED IN LOG/RECVCMDS

Reason:

This message is issued from TSSCPF if RECVCMDS or any node log files are allocated as SYSOUT in the startup procedure and CA Top Secret starts before JES.

Action:

No action required.

TSS9070I

OKAY

Reason:

Positive acknowledgement to a successful execution of a CA Top Secret control option.

Action:

No action required.

TSS9071E

OPTION IGNORED - END OF DAY

Reason:

Control Options defined as invalid after an end-of-day shutdown will be ignored by the system. This includes the LOG, MODE, and FACILITY options.

Action:

To allow the options:

Enter the O/S console control option: F TSS,RESETEOD

Reply with the correct password.

Re-enter the ignored options.

TSS9072I

**** SELECT TYPE OF SHUTDOWN ** <I> TO IGNORE**

TSS9072I

<Z> END OF DAY; RE-IPL WILL BE REQUIRED

TSS9072A

<T> TEMPORARY; MAY IMPACT THROUGHPUT

Reason:

All three of these messages are issued in response to the console command:

```
STOP TSS
```

Action:

A prompt for response is issued at the console.Valid responses are:

- I-Returns TSS to normal operation. Use this if the operator command was issued in error.
- Z-Terminates the TSS task for ZEOD (end-of-day) processing. Use this if a permanent shutdown is intended prior to an IPL.

  When OPTIONS(17) is in effect, the operator is prompted for the MSCA previous password or for a valid ACID and PASSWORD prior to confirmation, using TSS9080A.

  Normally, ZEOD processing will prompt for confirmation with TSS9102W.

  If Z was selected unintentionally, when ZEOD processing completes you can perform an emergency restart (without an IPL)with:

```
S TSS,,,RESETEOD
```

- T-Shuts down the TSS address space prior to a subsequent restart. Use this for a temporary shutdown to install software updates when an IPL is not required.

  The operator is prompted for the MSCA previous password, or for a valid ACID and PASSWORD prior to the normal confirmation using TSS9080A.

The system uses DOWN options if security is shut down in any mode other than DORMANT. DOWN options, associated with facilities, affect only job/session initiation and tape processing.

After the shutdown, use the following command to restart the product:

```
S TSS,,,REINIT
```

If CA Cleanup is installed, the ETCL or TASA task must be restarted manually.

TSS9073E

EXIT NOT ACTIVATED - reason

Reason:

If reason = LOAD ERROR, an attempt to load the installation exit failed. See the MVS Messages in the “Codes” chapter.

If reason = INVALID V4 FORMAT, the exit is not properly configured or Version 3 has not been converted.

Action:

For information on user exits, or the V4 Conversion Notebook for conversion, see the *User Guide*.

TSS9074E

OPTION NOT VALID AT STARTUP

Reason:

The selected option cannot be specified on the EXEC PARM or in the PARMFILE. Options such as TSS and BYPASS are entered through a MODIFY command.

Action:

No action required.

TSS9075E

INVALID OPTION

Reason:

The entered MODIFY option is not known to CA Top Secret.

Action:

Check spelling. Reenter option.

TSS9076I

CURRENT OPTION IS option

Reason:

The control option listed in message text contains an error.

Note: Because TSS9076I is displayed once for every operand with an error, this message may be displayed multiple times.

Action:

Re-enter the control option using correct syntax and operand values.

TSS9077I

OPTION IS OBSOLETE

Reason:

The control option specified is not valid for the current version of TSS.

TSS9078I

MODIFY OPTION IGNORED

Reason:

An erroneous or unauthorized option was ignored.

Action:

Retry the command if spelling/format is in error.

TSS9079E

INVALID DATA

Reason:

Incorrect parameter value entered.

Multiple occurrences of this message indicate that there are multiple errors found in the PARMFILE card.

Action:

Enter the correct data.

TSS9080A

ENTER OPERATOR ID/PASSWORD FOR MODIFY ACCOUNTABILITY

Reason:

The entered CA Top Secret control option requires operator accountability. The operator ACID must have the CONSOLE attribute.

Action:

Enter an authorized ACID and password to continue. When entering a mixed case response, enclose the text in single quotes.

TSS9081E

OPERATOR AUTHENTICATION FAILED

Reason:

The operator is not accountable due to one of the following conditions:

- the ACID is not defined
- the password is not correct
- the ACID has expired
- the ACID is suspended
- the ACID not type C/A or USER
- the ACID does not have CONSOLE attribute

Action:

If the ACID should be accountable, his administrator must assign the correct properties to the ACID.

TSS9082E

YOU ARE NOT AUTHORIZED TO MODIFY SECURITY

Reason:

An attempt to change security control options was halted because the Operator/Administrator does not have the CONSOLE attribute.

Action:

No action required.

TSS9083E

Q-FAILURE

Reason:

CA Top Secret internal communication error.

Action:

Retry command. If problem persists, contact CA Technical Support.

TSS9084E

OPERATOR ACID/PASSWORD INVALID OR ILLEGAL

Reason:

See message TSS9081E.

Action:

No action required.

TSS9086I

OPERATOR COMMUNICATIONS REINSTATED

Reason:

The CA Top Secret operator communications subtask has regained control after an ABEND.

Action:

No action required.

TSS9087I

OPCOM RECOVERY SUCCESSFUL

Reason:

See message TSS9086I.

Action:

No action required.

TSS9088E

INCORRECT PASSWORD

Reason:

Password entered in response to message TSS9089A is incorrect or missing.

Action:

No action required.

TSS9089A

ENTER PASSWORD FOR FUNCTION

Reason:

Restricted control options require authorization of the Central Security Administrator.

Action:

Verify request and, if valid, enter the previous MSCA password, not the current password.

TSS9090A

SECURITY EXIT FAILURE - EXIT DISABLED

Reason:

System ABEND while executing the installation code. The exit is automatically turned off.

Action:

A system dump was taken. Correct problem and reload the exit via the EXIT control option.

TSS9091E

SECURITY BREACH (x) - POSSIBLE TAMPERING DETECTED

Reason:

During a periodic internal check, CA Top Secret discovered modification to critical logic or an address. Modification may be intentional or accidental.

Action:

Notify your Security Administrator and Auditors. Notify CA Technical Support for a detailed description of what was modified. CA Top Secret should eventually be reinitialized using the command: START TSS,,,REINIT

TSS9092W

SECURITY IN EMERGENCY BYPASS STATE

Reason:

Reminder that BYPASS(EVERYJOB) is in effect. All jobs will bypass security. CA Top Secret commands will not work.

Action:

No action required.

TSS9093W

INVALID START OVERRIDE OPTION

Reason:

An option in the PARM field of the CA Top Secret procedure EXEC statement is incorrect.

Action:

CA Top Secret starts but you must correct the statement prior to the next START up of TSS commands.

TSS9094I

BACKUP COMPLETE

Reason:

Displays in response to the F TSS,BACKUP control option or automatic backup. DASD backup of the Security File is complete.

Action:

No action required.

TSS9095E

SECURITY FILE BACKUP FAILED

Reason:

Backup of the Security File failed due to a processing error, an I/O error, or incorrect file allocation.

Action:

If CA Top Secret ABENDed or produced a dump, contact CA Technical Support.

TSS9096I

SECURITY FILE BACKUP COMMENCING

Reason:

Backup of the Security File has begun. The Security File is unavailable during backup processing. Job/session initiations, and use of CA Top Secret commands must wait for backup to complete.

Automatic backups should occur when the system(s) are relatively inactive (production work complete; for example, at night).

Action:

No action required.

TSS9097E

TSS9097E BACKUP FILE UNAVAILABLE

Reason:

CA Top Secret was not able to open and access the Backup Security File. Automatic backup is ignored. Processing continues.

Action:

Check the TSS STC procedure to ensure that the BACKUP DD-statement properly references the Backup Security File.

TSS9098E

BACKUP FILE BLOCKSIZE INVALID

Reason:

The physical blocksize of the Backup Security File is different from the physical blocksize of the main Security File. Automatic backup is ignored. Processing continues.

Action:

Use utility TSSMAINT to re-initialize the Backup Security file with a physical blocksize that matches the main Security File.

TSS9099I

CA Top Secret SECURITY FILE SERVICES NOW INACTIVE

Reason:

Displays in response to a valid STOP TSS command. The DOWN options for the facilities take effect unless CA Top Secret was running in DORMANT mode.

CA Top Secret is active. Only I/O services to the Security File are inactive. Bottleneck problems for throughput may occur.

Action:

No action required.

TSS9101W to TSS9198I

TSS9101W

*****WARNING*** IPL WILL BE REQUIRED TO REINSTATE PROCESSING**

Reason:

Response to valid Z shutdown.

Action:

No action required.

TSS9102A

REPLY <Y> TO CONFIRM SYSTEM SHUTDOWN

Reason:

Response to a valid Z shutdown.

Action:

Enter Y to shutdown, N to discontinue, the Z end-of-day shutdown, which requires an IPL to restart CA Top Secret.

TSS9103E

VSAMFILE DD NOT SPECIFIED

Reason:

The VSAM file feature was specified on the security file but no VSAMFILE DD statement was found in the startup JCL for CA Top Secret.

Action:

Specify a VSAMFILE DD statement that references the VSAM dataset associated with the SECFILE DD security file dataset.

TSS9104E

OPTION NOT ACCEPTED AFTER STARTUP

Reason:

The option specified cannot be changed through a TSS MODIFY command. It may only be specified as a startup option in the Parameter File.

Action:

Add the option to the Parameter File and restart CA Top Secret.

TSS9105I

GETMAIN FAILED; CPF NOW INACTIVE

Reason:

The CPF component of CA Top Secret was unable to obtain enough CSA to initialize. The TSS command will still execute normally. However, no commands will be routed to or received from remote nodes.

Action:

Contact the systems programmer to determine the cause of the CSA shortage.

TSS9106E

CSA SHORTAGE-UNABLE TO INITIALIZE LOG INTERFACE

Reason:

CA Top Secret could not acquire sufficient common storage area. CA Top Secret needs a minimum of 100K CSA to start.

Action:

No action required.

TSS9107I

VSAMFILE Successfully Opened

Reason:

CA Top Secret has opened the VSAM dataset for storing security related information.

Action:

No action required.

TSS9108E

CPF SUBTASK CURRENTLY RESTARTING.

Reason:

A CPF(REFRESH) modify command failed because CPF is already restarting.

Action:

No action required.

TSS9109E

CPF SUBTASK CURRENTLY STARTING.

Reason:

A CPF(REFRESH) modify command failed because CPF is already initializing.

Action:

No action required.

TSS9110E

CPFNODE Modify already in progress

Reason:

A CPFNODE modify command failed because a previous CPFNODE command is already in progress.

Action:

No action required.

TSS9111E

CPFNODE syntax error

Reason:

A CPFNODE modify command failed because of a syntax error.

Action:

Correct the command syntax and retry.

TSS9112E

UNABLE TO DETERMINE JES LEVEL

Reason:

CA Top Secret is unable to determine your JES level. This can occur for a number of reasons:

The JES control option LEVEL sub-option was specified, but the level does not correspond to the installed JES software.

The TSS task was started before JES was initialized.

The level of JES software installed is not supported by the current release of CA Top Secret.

Action:

For items 1 or 2 above, determine the LEVEL required by installed software. To obtain a valid value for the JES release, see the JES3 initialization message:

```
IAT31 JES3 xx r.ss.tt SYSTEM LOCAL START on yyy.ddd AS main
```

Or the JES 2 message:

```
$HASP426 SPECIFY OPTIONS - JES2 xx r.ss.tt
```

Modify the JES control option to correspond with the installed level of JES. If you start TSS before JES, provide a PARMFILE entry which sets the correct level and type of JES.

For item 3, contact CA Top Secret Support. Provide a copy of your PARMFILE and a listing of TSS MODIFY(STATUS) at the time you received this message.

Once the TSS9112E error message is received you may experience unexpected security violations for RJE jobs, which should be using the following to derive the acid name:

```
DEFACID(RDR*TERM)
```

In this case, rather than deriving an acid of Rnn@RDn, the job will attempt to run with an acid name of 'RDR*TERM'.

TSS9113E

CPF IS DISABLED. COMMAND REJECTED.

Reason:

The MODIFY command is rejected because CPF is disabled on this system.

Action:

Enable CPF on this system and recycle CA Top Secret.

TSS9114E

LDAP Node is undefined

Reason:

A Modify command was issued for an LDAPNODE that does not exist in the LDAP node table.

Action:

Ensure the node name specified is correct and retry the command.

TSS9115E

LDAPNODE syntax error

Reason:

A Modify command was issued for an LDAPNODE with incorrect syntax.

Action:

Ensure the syntax is valid and retry the command.

TSS9116E

No LDAP nodes defined on this system

Reason:

A Modify command was issued for an LDAPNODE on s system that does not have any LDAP nodes defined.

Action:

Ensure the node name specified is defined in the NDT, and retry the command.

TSS9117E

VSAMFILE WRONG FILE IS USED

Reason:

The timestamp in the VSAM dataset header record does not match the timestamp in the CA Top Secret security file.

Action:

Ensure that the CA Top Secret startup JCL specifies the correct security file and the VSAM file datasets that were initialized with TSSMAINT.

TSS9118E

VSAMFILE type not supported

Reason:

CA Top Secret was started with a security file that was initialized with the TSSMAINT parameter INITVSAM=YES. This type of security file is no longer supported.

Action:

Initialize a new security file with TSSMAINT parameter INITVSAM=DIGICERT and copy (using TSSXTEND) the old file to the new file.

TSS9118I

VSAMFILE Secondary Extent Allocated - Closing File

TSS9119I

VSAMFILE Successfully Re-opened

Reason:

These two messages are issued when new records are added to the file and VSAM expands the file by allocating a secondary extent.

Action:

No action required.

TSS9120I

ENQ/DEQ DONE for acid

Reason:

The DEBUG control option was set ON. CA Top Secret is reporting when an ENQ or DEQ was done on an 'acid'.

Action:

No action required.

TSS9121I

TSSENQ: ENQ TABLE FULL, ENQ WAITING

Reason:

The TSS command cannot obtain an enqueue on a specific ACID. The table used to keep track of enqueues is full. The TSS command will wait for an enqueue table entry to be freed and then continue normally.

Action:

If this message occurs frequently, the blocksize of the Security File should be increased.

TSS9122I

TSSENQ: UNABLE TO ENQ ON ACID xxxxxxxx, ENQ HELD ON SYSTEM system

Reason:

The TSS command has not been able to enqueue on the named acid due to an enqueue being held from the system ('system' is the SMF identifier). CA Top Secret will continue waiting for the enqueue to free. If the enqueue does not free, message TSS9123A prompts for permission to reset the enqueue.

Action:

See message number TSS9123A.

TSS9123A

UNABLE TO OBTAIN {SECURITY or AUDIT} FILE LOCK.

TSS9123A

SYSTEM system HAS HELD LOCK FOR nnn MINUTES.

TSS9123A

IF system IS NOT OPERATIONAL

TSS9123A

REPLY 'RESET', OTHERWISE REPLY 'WAIT'.

TSS9123A

WARNING: INDISCRIMINATELY REPLYING 'RESET'

TSS9123A

MAY CAUSE CORRUPTION OF THE xxxxxxxxxxxx SECURITY FILE

Reason:

CA Top Secret has not been able to obtain the Security File lock or an enqueue. The resource has been held on the system for nn minutes. If BLP appears after the “system”, the initial system is in the process of backing up the security file.

If the system holding the resource has gone down, replying RESET recovers the Security File lock.

Replying WAIT retries the request a set number of times. If none of the retries are successful, TSS9123A is reissued.

If the message is issued for the security file lock and the security file lock record is being maintained in the coupling facility, then the system will be identified as $CFLOCK$ in the message. The number of minutes the lock has been held will be unreliable.

Action:

Reply with desired option: RESET or WAIT. The correct response to the message is WAIT unless all live systems sharing the Security File have been issued the TSS9123A message as well. When all systems have the message, respond RESET on the first system and WAIT on the remaining systems.

If no response is received after one minute has elapsed, CA Top Secret will automatically reply to this message with WAIT.

If you set up an automated reply to message TSS9123A:

- Do not automate a reply of RESET. This will cause security file corruption.
- Ensure that an automated WAIT response is not issued under the same subtask that issued the WTOR for the message. This may cause a system outage. For example, the CA-OPS/MVS AOF facility allows for inline responses and is not recommended. Generate the reply via the OPSCMD POI command processor. This allows the command to be issued from an OPS/MVS OSF server and not the subtask that issued the message.

TSS9124I

UNEXPECTED I/O ERROR DURING SECURITY FILE SERIALIZATION. SENSE DATA = 'ssss'

Reason:

An I/O error occurred during CA Top Secret Security File serialization; ssss is the first two bytes of sense information from the MVS IOB.

Action:

If the problem persists, contact CA Technical Support.

TSS9125I

TSSENQ: LOCK PROCESSING DELAYED, WAITING FOR BACKUP TO COMPLETE ON SYSTEM

Action:

While attempting to serialize the Security File, CA Top Secret recognized that the lock is being held by another system that is currently performing an automatic backup of the file. Since this is a relatively long duration event, Top Secret will wait an additional amount of time to retry the lock before issuing the TSS9123A message.

Action:

Informational message only.

TSS9126E

STRUCTURE (str_name) HAS NOT BEEN REALLOCATED SINCE LAST DISCONNECTING FROM XES ATTEMPTING TO FORCE ALL SYSTEMS TO DISCONNECT FROM XES

Reason:

When locking the Security File after previously disconnecting from XES, the structure name in the ENQ record is still active and has not been reallocated since the disconnect took place. Attempting to force the structure to disconnect from all systems.

If STR active and same version as one previously disconnected from

Action:

Look for other related error messages and contact CA Technical Support if you still need further assistance.

TSS9127E

SECURITY FILE BLKSIZE TOO SMALL FOR THIS RELEASE OF TOP-SECRET

Reason:

The minimum blocksize is 8192 for the current release of CA Top Secret.

Action:

Correct blocksize to be a minimum of 8192.

TSS9128I

ACID INDEX PERFORMANCE OPTION TURNED OFF

Reason:

An LPAR protected by CA Top Secret 5.0 or below is sharing a security file with an LPAR at a higher release. The higher release LPAR was already running with the control option AINDXPER, when the lower release CA Top Secret was initialized. This message disables AINDXPER in shared higher release LPARs.

Action:

You may want to upgrade your lower-level CA Top Secret LPAR to a release which supports AINDXPER, or consider a separate security file for the lower level release connected by the Command Propagation Facility.

TSS9129E

STRUCTURE NAME MISMATCH ? DISCONNECTING FROM XES

Reason:

All systems are forced to disconnect from the Coupling Facility. While the current system was active in the Coupling Facility, the ENQ record was altered by another system and the ENQ record no longer contains the same structure name.

Action:

Ensure that the same structure name is defined in all systems sharing the Security File in the Sysplex..

TSS9130A

SECFILE IS ACTIVE IN XES STRUCTURE (str_namE)

REPLY “YES” TO CONNECT TO ACTIVE STRUCTURE

REPLY “YES,XCF_GRP” TO CONNECT TO ACTIVE STRUCTURE AND TO XCF

REPLY “FORCE” TO DISCONNECT ALL SYSTEMS FROM XES

REPLY “YES”, “YES, XCF_GROUP_NAME”, “FORCE” OR “ABORT”

Reason:

When a local system attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name and the local system does not have a currently defined structure name. The operator is prompted to confirm whether a connection should be made to the active structure or whether all systems should be forced to disconnect from XES.

Note the following:

- This message includes the option to replay ABORT only if the message was issued during startup. If this message is issued after initialization completes, the operator is not given this option.
- The reply option “YES,xcf_group_name” appears in this message only when the local system is connecting to an active structure, and an XCF group name is not defined in the local system.

Action:

Reply YES or FORCE to connect or disconnect. Reply ABORT to abort the attempt by the local system to lock the Security File. If prompted, you can also reply YES and provide the XCF group name to be used when connecting to the active structure.

TSS9130I

SECFILE IS ACTIVE IN XES STRUCTURE (str_name) ATTEMPTING TO FORCE ALL SYSTEMS TO DISCONNECT FROM XES

Reason:

When a local system attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name.

Attempting to force the structure to disconnect from all systems.

Action:

Informational message only.

TSS9131I

SECFILE IS ACTIVE IN XES STRUCTURE (str_name).

TSS9131I

MISMATCH WITH LOCAL STRUCTURE (str name).

TSS9131I

ATTEMPTING TO FORCE ALL SYSTEMS TO DISCONNECT FROM XES

TSS9131A

REPLY “YES” OR “FORCE”

TSS9131A

REPLY “YES” OR “FORCE” OR “ABORT”

Reason:

When a local system attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name and the local system has a different structure name. The operator is prompted to confirm whether the local system should connect to the active structure or whether all systems should be disconnected from XES and the local system should connect using the local system's currently defined structure name.

This message includes the option to reply ABORT only if the message was issued during startup. If this message is issued after initialization completes, the operator is not given this option.

Action:

Reply YES to connect to active structure, or FORCE to disconnect all systems from active structure and then connect to the local system's currently defined structure name. Reply ABORT to abort the attempt by the local system to lock the Security File.

TSS9132I

SECFILE IS ACTIVE IN XES STRUCTURE (str_name)

TSS9132I

CONNECTING TO ACTIVE STRUCTURE

Reason:

When a local system attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name and the local system has the same structure name. The local system is connected to the active structure.

Action:

No action required. This is an informational message.

TSS9133E

UNABLE TO CONNECT TO STRUCTURE (str_name)

TSS9133E

ATTEMPTING TO FORCE ALL SYSTEMS TO DISCONNECT FROM XES

TSS9133A

REPLY “FORCE” or “RETRY”

TSS9133A

REPLY “FORCE”, “RETRY” or “ABORT”

Reason:

An attempt to connect to an XES structure failed.

This message includes the option to reply ABORT only if the message was issued during startup. If this message is issued after initialization completes, the operator is not given this option.

Action:

Reply FORCE to disconnect all systems from XES or RETRY to attempt a connection. Reply ABORT to abort the attempt by the local system to lock the Security File.

TSS9134A

TSS9134A SECFILE IS ACTIVE IN XES STRUCTURE (STR_NAME). MISMATCH WITH LOCAL

TSS9134A STRUCTURE (str-name).

TSS9134A REPLY "YES" TO CONNECT TO ACTIVE STRUCTURE.

TSS9134A REPLY "FORCE" TO DISCONNECT ALL SYSTEMS FROM XES.

TSS9134A REPLY "RECON" TO DEALLOCATE ACTIVE STRUCTURE AND RECONNECT USING LOCAL STRUCTURE.

TSS9134A REPLY "YES", "FORCE" OR "RECON"

Reason:

When a local system, which is not connected to the Coupling Facility, attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name and the local system has a different structure name. The operator can choose to have the local system connect to the active structure, or force all systems to disconnect from XES, or deallocate the active structure and reconnect the local system to the structure it previously disconnected from.

Action:

Reply FORCE to disconnect, YES to connect using the active structure, or RECON to deallocate the active structure and reconnect using the structure name defined in the local system.

TSS9134E

UNABLE TO CONNECT TO STRUCTURE (STR_NAME) CA Top Secret IS TERMINATING

Reason:

An attempt to connect to an XES structure failed.

Action:

Review related structure error messages and contact CA Technical Support for further assistance.

TSS9135E

ERROR OCCURRED DURING XES STRUCTURE PROCESSING. THIS SYSTEM IS NOT

TSS9135E

CONNECTED TO XES BUT OTHER SYSTEMS MAY STILL BE CONNECTED.

TSS9135E

ENSURE THAT ALL SYSTEMS ARE DISCONNECTED FROM XES

Reason:

A severe error was encountered during XES processing, and the local system stopped using the structure.

Action:

Manually disconnect all other systems from the Coupling Facility structure. Look for other Coupling Facility related error messages and contact CA Technical Support.

TSS9136I

SECURITY FILE CF SERIALIZATION ACTIVE

Reason:

Coupling facility locking is activated.

Action:

No action required. This is an informational message.

TSS9137E

ERROR PROCESSING CF LOCKING. DISCONNECTING FROM CF STRUCTURE

Reason:

An error occurred during Coupling Facility locking processing. All systems are forced to disconnect from the Coupling Facility.

Action:

Look for Coupling Facility related error messages and Contact CA Technical Support.

TSS9138E

SECFILE IS LOCKED IN XES STRUCTURE (str_name).

TSS9138E

BUT CF LOCKING IS DISABLED ON THIS SYSTEM

TSS9138

AS REPLY “YES”, “WAIT”, OR “ABORT”

Reason:

When the Security File is locked in the Coupling Facility by another system, and the local system attempts to use the same file while the Coupling Facility is not enabled, the operator is given the option to dynamically enable Coupling Facility locking, or wait for the other systems to release the file.

This message includes the option to reply ABORT only if the message was issued during startup. If this message is issued after initialization completes, the operator is not given this option.

Action:

Reply YES to enable Coupling Facility locking, or WAIT to wait until the file is released. Reply ABORT to abort the attempt by the local system to lock the Security File.

TSS9138E

SECFILE IS LOCKED IN XES STRUCTURE (str_name)

TSS9138E

BUT CF LOCKING IS DISABLED ON THIS SYSTEM

TSS9138E

ATTEMPTING TO FORCE ALL SYSTEMS TO DISCONNECT FROM XES

Reason:

A severe error was encountered during XES processing, and the local system stopped using the structure.

Action:

Manually disconnect all other systems from the Coupling Facility structure. Look for other Coupling Facility related error messages and contact CA Technical Support.

TSS9139E

SECFILE IS ACTIVE IN XES STRUCTURE (str_name)

TSS9139E

NO SYSPLEX PARMS ARE DEFINED ON THIS SYSTEM

TSS9139E

CA TSS IS TERMINATING

Reason:

When a local system, which is not connected to the Coupling Facility, attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name

Action:

Review similar SYSPLEX error messages and contact CA Technical Support for further assistance.

TSS9140E

SECFILE IS ACTIVE IN XES STRUCTURE (str_name)

TSS9140E

MISMATCH WITH LOCAL STRUCTURE (str_name)

TSS9140E

CA TSS IS TERMINATING

Reason:

When a local system, which is not connected to the Coupling Facility, attempts to lock the Security File, the structure name in the Security File ENQ record is compared to the local system's currently defined structure. A local system, which is not connected to the Coupling Facility, has attempted to lock the Security File when the ENQ record has a currently active structure name and the local system has a different structure name.

Action:

Reconnect using the structure name defined in the local system.

TSS9141E

SECFILE IS LOCKED IN XES STRUCTURE (str_name)

TSS9141E

BUT CF LOCKING IS DISABLED ON THIS SYSTEM

TSS9141E

CA TSS IS TERMINATING

Reason:

A severe error was encountered during XES processing, and the local system stopped using the structure.

Action:

Manually disconnect all other systems from the Coupling Facility structure. Look for other Coupling Facility related error messages and contact CA Technical Support.

TSS9142E

- Parameters in DIAGTRAP already entered for another ID

Reason:

This message is given when a DIAGTRAP entry is entered that has the same Type, Userid, DRC, Jobname, and Classname as one of the other entries.

Action:

Display the current DIAGTRAP entries using the TSS MODIFY STATUS command.

If trap(nn) for the characteristics you need is disabled, you may enable it using the following command:

TSS MODIFY DIAGTRAP(nn,ON)

You may also consider altering the parameters to something more specific, or altering the match limit appropriately if the trap is being triggered and disabled before a problem case is actually reproduced.

TSS9143E

- Diagtrap Id is [not] in use.

Reason:

This message is given when you are attempting to turn on a diagtrapid but specified a diagtrapid that is already in use or are attempting to turn off a diagtrapid that is not in use.

Action:

To turn on a diagtrapid, specify one that is not already in use. To turn off a diagtrapid, specify a diagtrapid that is in use.

TSS9144E

- Invalid Diagtrap - <bad field>

Reason:

An attempt has been made to specify the DIAGTRAP control option with invalid positional operand values. One or more of the following errors may have occurred:

Invalid diagtrapid is given. Specify an ID from 1-10. “All” is also a valid id as long as it is followed by “,Del” to indicate deleting all of the Diagtraps in the table. If no ID is specified while adding an entry, an error message is issued

“On”, “Off”, or “Del” is not given for switch.

Incorrect trap type given (Valid types are KER, SVC, SFS, SF1, SF2, FRA, TSS, PRO, DBG, DB1, and DB2).

Value given for Userid, Jobname, or Resclass is over 8 characters.

Invalid DRC given. (Valid DRC is 0-255).

Invalid match limit given (Valid is 1-255).

Action:

Verify the reason from the list above as to why the error occurred and correct the problem.

TSS9145I

VSAMFILE FILE BACKUP COMMENCING

Reason:

Backup of the VSAM security file dataset has begun.

Action:

No action required.

TSS9146I

VSAMFILE FILE BACKUP COMPLETE

Reason:

Backup of the VSAM file security data is complete.

Action:

No action required.

TSS9147E

VSAMFILE FILE BACKUP FAILED

Reason:

Backup of the VSAM security file dataset failed due to a processing error, an I/O error, or incorrect file allocation.

Action:

If CA Top Secret ABENDed or produced a dump, contact CA Technical Support.

TSS9148I

VSAMBKUP DD NOT SPECIFIED

Reason:

TSS found a VSAMFILE DD statement but no VSAMBKUP DD statement in the startup JCL. If the CA Top Secret security file backup is taken, the VSAM data will not be backed up.

TSS9149E

FEATURE NOT SUPPORTED BY SECURITY FILE

Reason:

This message is issued when an action is requested that requires a particular feature to exist in the security file that is not currently there.

Action:

Depending on the feature, create another security file or run TSSXTEND to include the feature in the security file.

TSS9150I

TRACE/LOG CLOSED

Reason:

CA Top Secret was notified of JES2 termination and closed the trace/log file.

Action:

No action is required.

TSS9151E

- Invalid data set name specified

Reason:

This message will be issued when the data set name entered via the AUTOEDSN ADD is found to be invalid.

Action:

Use a valid entry for the data set name: from 1-44 characters, using standard z/OS naming conventions. You can also specify a prefix which is a partial data set name.

TSS9152E

- No matching data set name found in the AUTOERASE table.

Reason:

This message is issued when the data set name entered via the AUTOEDSN REM (remove) is not found in the autoerase table.

Action:

Check the spelling of the data set you have specified to remove from the autoerase table. If the spelling is correct, no further action is needed since the specified data set does not exist in the autoerase table. To list data set names specified in the autoerase table, use the STATUS command.

TSS9153E

- Processing error in TSSPARAM - Contact CA Top Secret support.

Reason:

This message is issued if there is no room in the table to add a new entry. This should never occur since a check is made to determine if there is room to add an entry and if there is not enough room, a larger table is created.

Action:

Contact CA Technical Support.

TSS9154E

Table is full - Maximum of 150 entries - Entry not added

Reason:

This message will follow an add command to the AUTOERASE or R_CACHESERV table. Depending on which command was being processed, the corresponding table is full. Both tables are restricted to 150 entries. If this error follows a TSS MODIFY AUTOEDSN(ADD,....) command, the AUTOERASE table is full. If the error follows a TSS MODIFY RCQNAME(ADD,....) command, the R_CACHESERV table is full.

Action:

In order to add an entry, an existing entry must be removed.

TSS9155E

VSAMFILE REQUIRED

Reason:

An CA Top Secret r12 or later VSAM file is required for CA Top Secret r15.

Action:

Perform *one* of the following activities:

- Use an existing VSAM file from CA Top Secret r12 or later.
- Create a new r15 VSAM file (by using TSSMAINT).

Note: For information about creating a VSAM file, see the *CA Top Secret Installation Guide*.

TSS9156E

NEWPWBLOCK FEATURE REQUIRED ON SECFILE

Reason:

The NEWPWBLOCK feature is required on the security file and was not detected.

Action:

Create a security file with the NEWPWBLOCK feature by doing one of the following:

- Create the security file using CA Top Secret r14 and later.
- Copy the security file with TSSXTEND specifying the NEWPWBLOCK option for CA Top Secret r12.

For detailed information about creating a security file with the NEWPWBLOCK feature, see the *Installation Guide.*

TSS9160E

RCACHE Internal Error

Reason:

The CASAFIVT cannot be obtained during RCACHE(YES|NO) processing.

Action:

Contact CA Technical Support.

TSS9161E

RCQNADD Internal Error

Reason:

The CASAFIVT cannot be obtained during RCQNAME(ADD,…) processing.

Action:

Contact CA Technical Support.

TSS9162E

Invalid cache name: xxxxxx

Reason:

The R_cacheserv queue name entered via the RCQNAME control option is found to be invalid.

Action:

Correct the queue name in error and resubmit the entire entry. All cache names specified must pass the validation process before any entry is added to the table.

TSS9163E

RCQNAME input is not formatted correctly

Reason:

The RCQNAME ADD or REMOVE input data string is not properly formatted.

Action:

Correct the format and resubmit the entire entry.

For example, (Rxxxxx, Rxxxxx,…)

TSS9170E

Unable to start TSSLDAP server task

Reason:

The LDAP server task could not be started.

Action:

Contact CA Technical Support.

TSS9171E

TSSLDAP server task already active

Reason:

The LDAP server task is already active and was not started again.

Action:

Contact CA Technical Support.

TSS9172I

LDS SERVER NOT STARTED. NO ACTIVE LDAP NODES

Reason:

The control option LDS is set to (ON) and the NDT has no active nodes.

Action:

Add the active NODES to the NDT.

TSS9176E

Statistics Gathering Not Active

Reason:

The control option STATG is already set to (OFF).

Action:

None.

TSS9177E

Statistics Gathering Already Active

Reason:

The control option STATG is already set to (ON).

Action:

None.

TSS9181E

The (X Facility/Action) is not valid for the Down Control option

Reason:

The value entered for either the facility or action was not a valid value.

Action:

Reenter the command with the correct value.

TSS9180I

The Down option for facility (x) has been modified to (x)

Reason:

Informational message telling that the facility has been modified to what action.

Possible facilities:

- B—BATCH facility
- T—TSO
- S—STC initiation
- O—All other facilities

Actions:

- W—Wait for CA Top Secret to be reactivated.
- B—Bypass security checking. Does not invoke CA Top Secret until restarted.
- F—Fail the request.
- N—Revert to native security (if any) until restarted.

Action:

Informational no action needed.

TSS9182I

The (option) ETROPT control option (Added/Removed)

Reason:

The value for an ETROPT was either added or removed.

Action:

Informational no action needed.

TSS9183E

The (value) parameter is not valid for the (Control option) Control Option

Reason:

The value entered for that control option is not a valid value.

Action:

Reenter the command with the correct value.

TSS9184I

The (control/facility) option has been modified to (VALUE)

Reason:

The value for either the control or facility control option has been modified to.

Action:

Informational no action needed.

TSS9185I

The (product name) Product is active

Reason:

This product is now active.

Action:

Informational no action needed.

TSS9186E

The Facility name is invalid

Reason:

The value entered for the facility name is not valid.

Action:

Reenter the command with the correct value.

TSS9188I

The (Global/Facility value) Log Option has been set

Reason:

The Global or a facility control option has been set.

Action:

Informational no action needed.

TSS9189I

(value) was (added to/removed from) the (facility name) facility (list) list.

Reason:

The value was either added or removed from the bypass or protlist for this facility.

Action:

Informational no action needed.

TSS9190A

CA TSS COMMAND PROCESSOR ABEND *cccc* IN PROGRAM program

Reason:

The TSS command subtask has ABENDed while processing a TSS command. The request being processed will be failed and a SVC dump will be produced.

In most cases, an SVCDUMP accompanies this message. To obtain more information about the error including ABEND PSW and Registers, issue the MVS D D,E Operator Command. The message should be followed by message TSS9191I.

Action:

Examine the SVCDUMP and, unless it indicates a hardware/software problem, contact CA Technical Support for assistance.

TSS9191I

TSS COMMAND SUBTASK (RECOVERY COMPLETE|HALTED)

Reason:

A TSS command subtask has abended. The message text reflects one of two possible scenarios:

- The command processor has successfully recovered from the abend and has resumed processing TSS commands.
- The command processor has incurred multiple consecutive abends with no intervening successful commands. TSS has determined that further restarts of the command processor could impact the stability of the system and halted the command processor.

Action:

No action is required if the message indicates recovery. If the command processor is halted then contact CA Technical Support.

TSS9192E

MIXED CASE MUST BE SET BEFORE THIS OPTION -

Reason:

The NEWPW MC (Mixed Case) control option must be set before the LC (Lower case) or UC (Upper case) control option can be set.

Action:

Use the MODIFY command to set the NEWPW MC option first in the NEWPW control string. For example: TSS MODIFY NEWPW(MC,LC,UC).

TSS9193E

When EJBRPRFX starts with an apostrophe, it must also end with one.

Reason:

You entered a Facility EJBRPRFX command that started with an apostrophe; therefore, the command must also end with an apostrophe.

Action:

Reenter the command with the correct value.

TSS9194E

Inactive with LASTUSED set cannot be lower than PWEXP.

Reason:

The INACTIVE control option cannot be set lower than the PWEXP control option when LASTUSED is set with the INACTIVE option.

Action:

Raise the INACTIVE option or lower the PWEXP option.

TSS9195W

UNIQUSER parameter valid in z/OS 1.11 and above

Reason:

This control option is only valid for releases of z/OS 1.11 and above..

Action:

No action required.

TSS9196I

OMVSGRP NOT SUPPORTED IN z/OS 2.1 AND ABOVE.

Reason:

Starting with z/OS 2.1, OMVSGRP (BPX.DEFAULT.USER) is no longer supported.

Action:

Use the UNIQUSER and MODLUSER control options instead.

Note: For more information about using UNIQUSER and MODLUSER, see the *CA Top Secret Control Options Guide.*

Module:

TSSPARAM

TSS9197I

OMVSUSR NOT SUPPORTED IN z/OS 2.1 AND ABOVE.

Reason:

Starting with z/OS 2.1, OMVSUSR (BPX.DEFAULT.USER) is no longer supported.

Action:

Use the UNIQUSER and MODLUSER control options instead.

Note: For more information about using UNIQUSER and MODLUSER, see the *CA Top Secret Control Options Guide.*

Module:

TSSPARAM

TSS9198I

Inactive interval exceeds max value and was set to 999 days.

Reason:

The specified inactive interval was greater than the maximum allowable value (999) and was automatically set to 999.

Action:

No action is required; however, you can specify any value from 0 through 999.

TSS9203I to TSS9301I

TSS9203I

SWITCHED TO AUDIT/TRACKING OUTPUT FILE ddddddddd

Reason:

CA Top Secret has begun writing to the alternate Audit/Tracking File identified by ddddddddd.

Action:

No action required.

TSS9204E

AUDIT FILE UNAVAILABLE

Reason:

CA Top Secret was not able to open or access the Audit/Tracking File.

Action:

Check the TSS STC procedure to ensure that the AUDIT DD statement properly references the Audit/Tracking File.

TSS9205E

AUDIT FILE SYNCHRONIZATION ERROR

Reason:

An error occurred when CA Top Secret attempted to locate the logical point within the Audit/Tracking Files.

Action:

Contact CA Technical Support.

TSS9206E

CURRENT FILE, xxxxxxxx, UNAVAILABLE

Reason:

CA Top Secret encountered an error when it attempted to use the indicated Audit/Tracking File.

Action:

Ensure that the file has been properly formatted, and the data set name is properly spelled within the CA Top Secret Startup JCL.

TSS9207I

The (CURRENT|INITIAL) AUDIT/TRACKING OUTPUT FILE IS ddddddddd

Reason:

Identifies the Audit/Tracking File CA Top Secret is writing to at startup (INITIAL) or after another system has switched files (CURRENT).

Action:

None. Informational message only.

TSS9208I

AUDIT/TRACKING FILE, filename, AT LEAST 90% FULL

Reason:

The specified Audit/Tracking File is nearly full. When full, the file will wrap and data will be overlaid and lost.

This message is issued when the file is 90% full and subsequently, each time CA Top Secret is restarted until the situation is corrected.

Action:

Back up the Audit/Tracking File, or ignore the message if the File is large enough.

TSS9209I

AUDIT FILE HAS WRAPPED

Reason:

The Audit/Tracking File has filled up and wrapped.

Action:

No action required.

TSS9210E

AUDIT FILE ERROR - NOT PREFORMATTED

Reason:

The Audit/Tracking File header is not properly formatted.

Action:

Make sure the File was created with the current version of the TSSMAINT utility, and the AUDIT DD statement in the CA Top Secret startup procedure is pointing to the correct data set.

TSS9211E

AUDIT FILE ERROR - ENQ FAILURE

Reason:

CA Top Secret was unable to ENQ on the Audit/Tracking File.

Action:

Contact CA Technical Support.

TSS9212E

AUDIT FILE ERROR - INVALID FORMAT

Reason:

The Audit/Tracking File header is not properly formatted.

Action:

Make sure the File was created with the current version of the TSSMAINT utility, and the AUDIT DD statement in the CA Top Secret startup procedure is pointing to the correct data set.

TSS9213E

AUDIT FILE ERROR - UNEXPECTED EOF

Reason:

The Audit/Tracking File header is not properly formatted.

Action:

Make sure the File was created with the current version of the TSSMAINT utility, and the AUDIT DD statement in the CA Top Secret startup procedure is pointing to the correct data set.

TSS9214E

AUDIT FILE ERROR - HEADER ERROR

Reason:

The Audit/Tracking File contains invalid data within the first block.

Action:

Make sure the File was created with the current version of the TSSMAINT utility, and the AUDIT DD statement in the CA Top Secret startup procedure is pointing to the correct data set.

TSS9215I

INPUT BUFFER LENGTH IN ERROR

Reason:

The Audit/Tracking File header is not properly formatted.

Action:

Make sure the File was created with the current version of the TSSMAINT utility, and the AUDIT DD statement in the CA Top Secret startup procedure is pointing to the correct data set. In addition, ensure that if the Audit/Tracking File was moved, it was not reblocked.

TSS9216I

BLOCKSIZE ERROR IN AUDIT FILE

Reason:

The BLKSIZE JCL parameter in SAMPJCL(TSSMAINA) or the input parameter BLOCKSIZE to TSSMAINT has been incorrectly specified.

Action:

The following conditions must all be true for the AUDIT files to come up without error:

- When SAMPJCL(TSSMAINA) is submitted, the BLKSIZE JCL parameter and the BLOCKSIZE input parameter must be equal
- The maximum allowed blocksize must be a multiple of 256 in the range 512 – 32512 for the program TSSMAINT with the following conditions:
  - For 3390 DASD, the maximum allowed blocksize is 27468
  - For other DASD devices, the maximum allowed blocksize depends on track capacity
- If AUDIT and AUDIT2 files are used, the blocksize for both files must be the same

Make corrections to your JCL to create your AUDIT/AUDIT2 files. Resubmit, and alter your TSS startup proc if needed.

TSS9217I

QGET ERROR, CALL CA SUPPORT CENTER

Reason:

CA Top Secret experienced an error in the Audit/Tracking task queue.

Action:

Gather any traces or dumps and contact CA Technical Support.

TSS9218I

I/O ERROR ON AUDIT FILE

Reason:

An I/O error was encountered with the Audit/Tracking File.

Action:

Check the device the file is on, and if the error continues, try to create a new file on a different device.

TSS9219E

AUDIT/TRACKING TASK ABENDING

Reason:

An error occurred during logging to the Audit/Tracking File.

Action:

Gather any traces or dumps and contact CA Technical Support. CA Top Secret should be shutdown (temporarily), restart with a full REINT to restore auditing.

TSS9220E

AUDIT FILE DDNAMES DO NOT MATCH FILE IDS

Reason:

This message is issued at startup of CA Top Secret. The data set name indicated by the AUDIT DD DSN= or AUDIT2 DD DSN= statements are incorrect or mismatched. They should state AUDIT or AUDIT2 respectively.

Action:

Correct the DD statements.

TSS9221W

ECSA Shortage due to Excessive Logging - Events may be lost

Reason:

Due to excessive logging and ECSA shortage, non violation events are temporarily not being logged until the ECSA shortage condition is lifted.

Action:

Run TSSUTIL to identify the source and cause of the excessive logging.

TSS9230E

SECMIRR DD NOT SPECIFIED

Reason:

The MIRROR(ON) option was set, but no SECMIRR DD statement exists in the product startup JCL.

Action:

In the product startup JCL, specify a SECMIRR DD statement that references the BDAM data set that was initialized for the mirror file data set.

TSS9231E

VSAMIRR DD NOT SPECIFIED

Reason:

The MIRROR(ON) option was set, but no VSAMIRR DD statement exists in the product startup JCL.

Action:

In the product startup JCL, specify a VSAMIRR DD statement that references the VSAM data set that was initialized for the mirror file data set.

TSS9232E

SECMIRR NOT FOUND IN VTOC

Reason:

The SECMIRR DD statement references a data set that was not found in the disk device VTOC.

Action:

Modify the SECMIRR DD statement to point to the correct location of the BDAM data set that was initialized for the mirror file data set.

TSS9233E

SECMIRR ON SAME VOLUME AS SECFILE

Reason:

The SECMIRR DD statement references a mirror data set that is on the same DASD volume as the primary SECFILE data set. The mirror file should be on a separate volume so that the file remains available if a failure occurs on the volume of the primary security file.

Action:

Re-initialize the mirror data set, placing it on another DASD volume.

TSS9234E

SECMIRR FILE BLOCKSIZE INVALID

Reason:

The SECMIRR DD statement references a mirror data set with a block size that differs from the block size of the primary SECFILE data set.

Action:

Re-initialize the mirror data set with the same block size as the primary security file.

TSS9235E

SECMIRR FILE UNAVAILABLE

Reason:

The product could not access the mirror file that the SECMIRR DD statement references.

Action:

Check the product startup procedure to ensure that the SECMIRR DD statement properly references the security mirror file.

TSS9236E

SECMIRR INVALID FILE HEADER

Reason:

The mirror file header record format is invalid.

Action:

Check the product started task procedure to ensure that the SECMIRR DD statement properly references the mirror file that was initialized with TSSMAINT.

TSS9237I

SECMIRR out of sync with SECFILE

Reason:

At product initialization, the mirror security file header record timestamps were out of sync with the primary security file header record timestamps.

Action:

No action is required. The product automatically re-syncs the mirror file and primary security file. This message is followed by messages TSS9242I and TSS9243I.

TSS9238E

VSAMIRR FILE UNAVAILABLE

Reason:

The product could not access the mirror VSAM file that the VSAMIRR DD statement references.

Action:

Check the product started task procedure to ensure that the VSAMIRR DD statement properly references the VSAM mirror file.

TSS9239E

VSAMIRR WRONG FILE IS USED

Reason:

The timestamp in the mirror VSAM data set header record does not match the timestamp in the mirror BDAM file that the SECMIRR DD statement references.

Action:

Check the product started task procedure to ensure that the JCL references the mirror files that were initialized with TSSMAINT.

TSS9240I

Security file mirroring is active

Reason:

During product initialization, the mirror files were successfully opened and verified. The mirroring feature has been activated, which means that a mirror security file (an exact duplicate of the primary security file) is active. The mirror is updated as the primary file is updated, providing up-to-the-minute data in the event of a sudden problem with the primary file.

Action:

No action is required.

TSS9241E

SECMIRR size does not match SECFILE

Reason:

The SECMIRR DD statement references a mirror data set that has a different number of blocks than the primary SECFILE data set.

Action:

Re-initialize the mirror data set with the same number of blocks as the primary security file.

TSS9242I

Mirror Synchronization Started

Reason:

The mirror file synchronization process has started.

Action:

No action is required. This message follows message TSS9237I.

TSS9243I

Mirror Synchronization Ended

Reason:

The mirror file synchronization process has ended.

Action:

No action is required. This message follows messages TSS9237I and TSS9242I.

TSS9244E

Mirror Synchronization Failed

Reason:

During product initialization, the mirror file synchronization process failed.

Action:

Review the system and product log files for any error messages that indicate the cause of the failure.

TSS9245E

VSAMFILE FILE COPY TO MIRROR FAILED

Reason:

Copying the primary VSAM file to the mirror VSAM file failed due to a processing error, an I/O error, or incorrect file allocation.

Action:

Review the system and product log files for any error messages that indicate the cause of the failure.

TSS9246E

Mirror file must be re-formatted

Reason:

An error occurred during mirror file synchronization, so the mirror files must be re-initialized.

Action:

Re-initialize the mirror files with TSSMAINT, then restart the product. You can obtain statistics from the primary files to provide the correct block size and the correct number of records in each mirror component.

TSS9247E

Mirror File not Supported with Shared SECFILE

Reason:

The MIRROR(ON) option was selected when SHRFILE(YES) or SHRFILE(SECURITY) was already active. The MIRROR option is supported only with a non-shared security file.

Action:

Specify SHRFILE(NO) if mirroring is required. SHRFILE(NO) must precede the initialization of MIRROR(ON).

TSS9248I

Security file Mirroring is Disabled

Reason:

The MIRROR(ON) option was selected, but the product failed to initialize the mirroring process. This message is preceded by other messages specifying the cause of the failure.

Action:

Look for accompanying messages and correct the error conditions.

TSS9249E

VSAMIRR ON SAME VOLUME as VSAMFILE

Reason:

The VSAMIRR DD statement references a data set that is on the same DASD volume as the primary VSAM data set. The VSAM mirror data set should be on a separate volume so that the data set remains available if a failure occurs on the volume of the primary VSAM data set.

Action:

Re-initialize the VSAM mirror data set, placing it on another DASD volume.

TSS9250E

SAMIRR allocation size too small

Reason:

The VSAMIRR DD statement references a VSAM data set that has insufficient space to contain the data from the primary VSAM file.

Action:

Re-define the VSAM mirror data set with a size that matches or exceeds the size of the primary VSAM data set. Then re-initialize the mirror files with TSSMAINT and restart the product.

Note: For complete instructions on defining the mirror security file (BDAM and VSAM components), see the *CA Top Secret User Guide*.

TSS9251E

File sharing not allowed when Mirroring active

Reason:

An attempt was made to activate security file sharing (through the SHRFILE(YES|SECURITY) setting) while MIRROR(ON) was already set. The MIRROR option is supported only with a non-shared security file.

Action:

Set MIRROR(OFF) if file sharing is required.

TSS9252E

VSAMIRR max record size too small

Reason:

The VSAMIRR DD statement references a VSAM data set that has a maximum record size that is smaller than the size of the primary VSAM file.

Action:

Re-define the VSAM mirror data set with a maximum record size that matches or exceeds the size of the primary VSAM data set. Re-initialize the mirror files with TSSMAINT, then restart the product.

TSS9253E

SECMIRR Multi Block I/O interrupted. Mirror file Integrity Compromised

Reason:

An interruption occurred during an update to the mirror file, rendering the file unusable.

Action:

Re-initialize the mirror file with TSSMAINT, then restart the product. If the message was preceded by I/O errors on the primary security file, initiate recovery procedures.

Note: For information about recovering from a security file failure, see the *CA Top Secret User Guide*.

TSS9254A

Confirmation Required to Synchronize Mirror File
Primary File DSN: *primary_dataset_name*
Primary File Volser: *primary_volser*
Mirror File DSN: *mirror_dataset_name*
Mirror File Volser: *mirror_volser*
Reply 'YES' to Synchronize or 'NO' to Disable Mirroring

Reason:

At product initialization, the mirror security file header record timestamps and primary security file header record timestamps were not synchronized. The product now requests confirmation to synchronize the mirror file with the primary file.

This message follows message TSS9237I.

Action:

Verify that the specified primary file and mirror file are the correct files to use in the product startup, and then perform *one* of the following actions:

- Reply **YES** to proceed with synchronization.
- Reply **NO** to bypass synchronization and disable mirroring.

TSS9255E

ERROR WRITING TO MIRROR FILE
SECMIRR SYNAD WRITE ,COMMAND REJECT ,00000069000000,BSAM

Reason:

An I/O error occurred at startup during synchronization of the mirror file and primary file. The second part of the message provides hardware sense data about the nature and possible cause of the I/O error.

Mirror file processing is now disabled.

Action:

Analyze the error to determine whether to move the file to another DASD volume or re-define and initialize the file on the same volume.

Note: For more information that might help you diagnose the I/O error, see the IBM publication *z/OS DFSMSdfp Advanced Services*.

TSS9260E

MIRROR FILE I/O ERROR DURING WRITE/READ SENSE=*xxxx* CSW=*xxxxxxxx xxxxxxxx*

Reason:

An I/O error occurred while processing the mirror file. Mirror file processing is now disabled.

Action:

Contact CA Support.

TSS9269E

LOGICAL READ ERROR

Reason:

A logical error occurred during a read to the Security File.

Action:

Gather any traces or dumps and contact CA Technical Support.

TSS9270E

PASSWORD IS INCORRECT

Reason:

An attempt was made to utilize the TSS command from an O/S console, and the password supplied in response to the TSS9089A message was not the MSCA's current password.

Action:

Gather any traces or dumps and contact CA Technical Support.

TSS9271E

UNABLE TO EXECUTE THIS COMMAND

Reason:

An attempt was made to utilize the TSS command from an O/S console, and the TSS command was unable to execute.

Action:

Gather any traces or dumps and contact CA Technical Support.

TSS9272A

ENTER <TSS COMMAND> OR <END>

Reason:

You are requested to enter a TSS command or the characters END to terminate CA Top Secret command processing via the console.

Action:

When entering TSS commands, always enter the characters TSS as in TSS WHOOWNS TERMINAL(R10). The response generated is limited to 50 lines of output, so as not to flood the console.

TSS9273A

ENTER TSS COMMAND PASSWORD

Reason:

Displayed in response to “F TSS, TSS” command.

Action:

You must enter the MSCA's previous password to allow further continuation of the request.

TSS9274E

UNABLE TO LOAD TSS COMMAND

Reason:

The system was unable to load module TSSAUTH on behalf of TSS. Possible storage shortage.

Action:

No action required.

TSS9275I

***LOGON* CANCELLED - EXCESSIVE WAIT TIME**

Reason:

A user has not responded to a TSO logon prompt within the MVS job wait time limit. The logon is cancelled. MVS message IEF402I accompanies this message.

Action:

No action required.

TSS9301I

CA TOP SECRET TONE INTERFACE INITIALIZATION COMPLETE

Reason:

The CA Top Secret TONE Interface has been activated, and is fully initialized.

Action:

No action required.

TSS9400E to TSS9499I

TSS9400E

DUF/Extract Failed - User Has No INSTDATA

Reason:

A RACROUTE REQUEST=AUTH, CLASS=DUFXTR has been issued against an ACID that does not have any installation data associated with it.

Action:

Add installation data to the ACID.

TSS9401E

CA Top Secret CONTROL OPTION 'JCT' IS INCORRECTLY SET

Reason:

If CA Top Secret was started before JES, the JES option must be specified, indicating both TYPE and LEVEL in the parameter file.

At the time of job submission, the offsets for JCTINDEV, JCTROUTE, JCTNJHDR were set incorrectly.

An exit or OEM product has modified the JCT control block or a copy of this control block. The modified storage has been passed to CA Top Secret during job submission. In particular:

Module TSSMNJ2T must be the first program in line for JES2 exit 24

The CA Top Secret Installation Exit TSSINSTX may have to be modified if you employ the PRE-INIT or POST-INIT exit points to modify the JES control blocks.

The release of JES you have installed on your system is not supported by the current release of CA Top Secret.

Action:

Edit the parameter file so that the JES control option is correctly specified. Reinitialize CA Top Secret.

Unless your site makes modification to standard JES control blocks, you should allow the JCT control option to default. If your site makes use of standard offsets, this message can be caused by incorrect settings for the following parameters in the JES control option:

- SSID
- TYPE
- RELEASE

Make sure that all of these parameters correctly correspond to your implementation of JES on this system. When these have been corrected, you may or may not need to resubmit the job.

Determine whether an inhouse exit or an OEM product could be modifying the JCT passed to CA Top Secret. Consult the documentation for your exit or the OEM product to assure it is properly installed with macros corresponding to your operating system. If the JCT has been modified as designed, assure that the JCT offsets in the CA Top Secret JCT control option corrected to correspond with this design.

Contact CA Top Secret Support.

TSS9402E

ERROR OBTAINING SECURITY RECORD(S) FOR < > -RETRYING REQUEST

Reason:

CA Top Secret was unable to obtain an ACID's Security Record in response to a logon or other request. See other error messages issued in conjunction with TSS9402.

Action:

No action required.

TSS9403E

Insufficient CSA or Local Storage

Reason:

CA Top Secret was unable to satisfy a cross-memory request due to insufficient EST or insufficient local storage.

Action:

If the problem is insufficient CSA, enlarge the CSA/ECSA site and IPL. (In this case, the message will be issued by multiple address spaces at the same time.)

If the problem is insufficient local storage, decrease the region size and restart the address space.

TSS9404E

Security Record Damaged or Insufficient CSA. Try Again

Reason:

CA Top Secret was unable to process a logon request due to insufficient available CSA, or because a record was damaged.

Action:

If the problem is a CSA shortage, decrease CSA usage by other users or enlarge the system's CSA size.

TSS9405E

NO AUTHORITY FOR INTERNAL SECURITY FUNCTION ( )

Reason:

A RACROUTE request requiring APF authorization was issued in a non-APR state. Another reason may be that a DUFXTR/DUFUPD call was issued and the ACID making the call does not have the appropriate attribute added to its security record.

Action:

Correct the module or library attributes and restart the job or started task or add the DUFXTR/DUFUPD attributes to the ACID making the call. If accompanied by a TSS7100E message, see Page DRC-1 for an explanation of the Detailed Reason: Codes.

TSS9406E

PROBABLE SITE INTERFACING ERROR (drc)

Reason:

CA Top Secret was unable to satisfy a RACROUTE request due to errors in parameters passed on those RACROUTE or improper installation setup.

Action:

Check the DRC in the message text. If the DRC is:

030 A parameter list error.

035 You need to correct/update the Facility Matrix entry for this facility.

036 The issuer of the RACROUTE request has passed an invalid ACEE to CA Top Secret.

TSS9407E

INTERNAL SYSTEM ERROR ( )

Reason:

A logic error has occurred during RACROUTE request processing.

Action:

If problem persists, contact CA Technical Support.

TSS9408E

INTERNAL INTEGRITY CHECK FAILED

Reason:

A RACROUTE request detected an invalid or overlaid ACEE.

Action:

Restart the address space (batch job, STC or TSO user).

TSS9409I

xxx-yy ABEND IN rrrrrrrr PROCESSING reason

Reason:

During RACROUTE request processing, CA Top Secret terminated the request with a system abend code.

Action:

Correct errors in module(s) using RACROUTE request.

TSS9410E

UNKNOWN CLASSNAME (classname) for SVC (svcname)

Reason:

A RACROUTE REQUEST=AUTH or REQUEST=DEFINE has been issued for an undefined class name.

Action:

This is usually an implementation error. Add the Resource class to the RDT or correct the module issuing the request.

TSS9420E

RLP LOGIC ERROR. SEE CAS3xxxE MESSAGE FOR DETAILS. J=jobname, A=userid, T=term netname, R=resource name

Reason:

The component that performs RLP analysis encountered a logic error within RLP administration definitions. The RECORD, SELECT, or MASKREC definitions are incorrect.

If the user is in FAIL mode, access to the record will be denied.

Action:

See the CAS3 message for details of the error.

TSS9460E

INVALID CALL TYPE RECEIVED

Reason:

This message indicates an internal error. CA Top Secret for DB2 initialization will terminate, and CA Top Secret for DB2 will not protect the DB2 subsystem.

Module: CADB2TSS

Action:

Contact CA Technical Support for assistance

TSS9480I

TSS/IMS INTERFACE INITIALIZATION COMPLETE

Reason:

CA Top Secret has been correctly loaded into IMS.

Action:

No action required.

TSS9481I

TSS/DLI INTERFACE INITIALIZATION COMPLETE

Reason:

This message is issued every time an IMS batch job is started.

Action:

No action required.

TSS9482W

TSS/EXTENDED DLI SUPPORT WAS NOT SPECIFIED AND WILL NOT BE AVAILABLE

Reason:

Startup commands indicate that no DLI support was required.

Action:

If DLI support is necessary, specify ISIS=1 in the CA Top Secret STC procedure.

TSS9483E

TSS/DLI ENVIRONMENT ERROR

Reason:

System error.

Action:

Contact CA Technical Support.

TSS9485E

A SECURITY ABEND HAS OCCURRED DURING SIGNON/SIGNOFF PROCESSING

Reason:

An abend occurred while CA Top Secret was processing a signon or signoff request. Signon/signoff failed.

Action:

Contact CA Technical Support.

TSS9486E

UNABLE TO DELIVER TSS SIGNON ERROR MESSAGES

Reason:

Because of an internal design limitation, CA Top Secret was unable to deliver the error messages for a failed signon request to the user was signing on.

Action:

Contact CA Technical Support.

TSS9487E

UNABLE TO INSTALL MSC LINK INTERCEPT

Reason:

CA Top Secret was unable to install TSS-IMS MSC Link Intercept.

Action:

Contact CA Technical Support.

TSS9488E

UNSUPPORTED IMS RELEASE. SECURITY DISABLED

Reason:

The release of IMS in unsupported.

Action:

Contact CA Technical Support.

TSS9489E

UNABLE TO ESTABLISH IMSWA NAME/TOKEN PAIR

Reason:

During CA Top Secret initialization in an IMS control region, it was unable to establish the identification of a control block with MVS name/token services.

Action:

Contact CA Technical Support.

TSS9490E

UNABLE TO PLANT SIGNON SECURITY INTERCEPT

Reason:

During CA-Top Secret initialization in an IMS control region, it was unable to establish the environment to perform signon security.

Action:

Contact CA Technical Support.

TSS9491E

UNABLE TO PLANT RESOURCE SECURITY INTERCEPT

Reason:

During CA Top Secret initialization in an IMS control region, it was unable to establish the environment to perform resource security processing.

Action:

Contact CA Technical Support.

TSS9492E

Error loading TSS/DLI initialization module

Reason:

During CA Top Secret initialization in an IMS control region, it was unable to load the DLI initialization module TSSD###Z, where ### is the IMS release. This module must be available.

Action:

Determine why the TSSD###Z module is not available. If problems persist, contact CA Technical Support.

TSS9498A

ALLOW TRAP DUMP FOR JOB=xxxxxxxx ACID=xxxxxxxx DRC=nnn YES OR NO?

Reason:

Issued in response to a matching condition for the DIAGTRAP control option.

Action:

Reply YES to take a SVC dump or No to suppress the SVC dump.

TSS9499I

TRAP DUMP FOR JOB=xxxxxxxx ACID=xxxxxxxx

Reason:

This message lists the title of a DIAGTRAP SVC dump taken to a SYS1.DUMPnn data set.

Action:

No action required.

TSS9500I to TSS9599E

TSS9500I

FACILITY=facility id=id MODE=mode

Reason:

Response to F TSS,FACILITY(ALL) command. Displays basic information for each facility defined as in-use.

FACILITY

Facility name.

ID

ID used for logging in TSSUTIL/TSSTRACK reports.

MODE

Current mode of the facility.

Action:

No action required.

TSS9507I

JOBACID(c,n,n) SUBACID(c,n)

Reason:

Displays in response to the TSS MODIFY(STATUS) command.

JOBACID = how ACIDs for batch jobs are derived

SUBACID = how ACIDs for online batch jobs are derived

Action:

No action required.

TSS9519I

ADABAS(nnn,nnn,...) DLIB(YES|NO)

This will only display when a value is coded. If you are not using this control option it will not display when issuing the TSS MODIFY(STATUS) command.

DLIB indicates whether IMS BATCH DL1 calls are protected.

YES = ALL processing of BATCH DL/1 will be checked for DBD and PSB protection.

NO = NO security checking will be performed.

Reason:

ADABAS indicates the SVD numbers (up to 4) in decimal, specified for ADABAS.

This will only display when a value is coded. If you are not using this control option it will not display when issuing the TSS MODIFY(STATUS) command.

DLIB indicates whether IMS BATCH DL1 calls are protected.

YES = ALL processing of BATCH DL/1 will be checked for DBD and PSB protection.

NO = NO security checking will be performed.

Action:

No action required.

TSS9521I

DB2FAC(SSID=facility)

Reason:

Displays the DB2 subsystem name and the associated facility name.

Action:

No action required.

TSS9522I

TEXTTSS(ccccccccccccccccccccc)

Reason:

Displays the text string that will display on reports and messages. The default is CA Top Secret Security.

Action:

No action required.

TSS9534I

NJEUSR(*NONE*|acidname)

Reason:

Displays the default ACID to be used for NJE store-and-forward nodes where no other userid can be identified.

Action:

No action required.

TSS9537I

XCF NAME (connect-name) GROUP (group-name)

Reason:

Displays XCF information with the TSS MODIFY(STATUS) command, in the SYSPLEX control option.

Action:

No action required.

TSS9538I

STRUCTURE NAME (structure-name) ACTIVATED/CONNECTED

Action:

Displays as part of the TSS MODIFY(STATUS) command when CA Top Secret is connected to the remote system. With CA Top Secret in the SYSPLEX this message will show ACTIVATED. With CA Top Secret only using XCF for MODIFY commands it will show CONNECTED.

Action:

No action required.

TSS9539I

TNG MONITOR(ON|OFF)

Reason:

Displays the status of the TNG monitor.

Action:

No action required.

TSS9540I

TNG MONITOR DEST(ip addr)

Reason:

Displays the IP address of the PC to which CA Top Secret violations are sent.

Action:

No action required.

TSS9541I

DRC=nnn,MSG=TSSnnnn,SEC9=TSSnnnn,settings

Reason:

Displays the DRC control option setting for the specified DRC.

DRC

DRC number

MSG

Message issued to the end user when the violation occurs.

SEC9

Message issued to the security console when the violation occurs.

settings

Current options associated with the DRC; see the *Control Options Guide* for a description of their meanings.

Action:

No action required.

TSS9542I

rpw ppw rpw ppw

Reason:

Displays the passwords restricted through the RPW control option.

TSS9543I

msg# Settings

Reason:

Displays MSG control option settings for the specified message number (msg#).

Action:

No action required.

TSS9544I

PDSPROT(ON|OFF)

Reason:

Displays the status of PDS protection.

Action:

No action required.

TSS9545I

PDSPROT(DSN(dddddd),VOL(vvvvvv),CLASS(cccccc)

Reason:

Displays the data sets and the associated volume that will be subject to PDS protection via the designated class name.

Action:

No action required.

TSS9547I

OMVSUSR(uuuuuu) OMVSGRP(gggggg)

Reason:

OMVSUSR - Displays the ACID used to provide the OMVS segment for an extract for any user who does not have an OMVS segment.

OMVSGRP - Displays the ACID used to provide the OMVS segment for an extract for any group that does not have an OMVS segment.

Action:

No action required.

TSS9549I

FACMODE(nnx,nnx,nnx,...)

Reason:

During TSS MODIFY STATUS, displays in compressed form which facilities have been explicitly set to a mode other than default.

nn=ID of the facility and x=security mode the facility is operating under.

Valid values for “x” are: F=fail, W=warn, I=implement, D=dormant.

Action:

No action is required. However, to display the MODE for a particular FACILITY, give command TSS MODIFY FACILITY(none).

TSS9550I

FACILITY DISPLAY FOR facility

Reason:

Response to F TSS,FACILITY(facility) command. Messages TSS9551I through TSS9555I (through TSS9570I for CICS) will also be displayed.

Action:

No action required.

TSS9551I

INITPGM=pgmnamE

id=f

Reason:

INITPGM provides the name of the internal module program that is used to identify the facility that a user is signing on to.

ID 'f' indicates the unique code that identifies the facility for TSSUTIL/REPORT.

Action:

No action required.

TSS9552I

ATTRIBUTES=attributes list

Reason:

Lists the attributes that are in effect for the facility.

Action:

See the *Control Options Guide* for the meaning of the listed options.

TSS9553I

MODE=mode DOWN=options LOGGING=logging

Reason:

Specifies the MODE for the facility.

Action:

No action required.

TSS9554I

UIDACID=s LOCKTIME=nnn DEFACID=xxxx KEY=xxx

Reason:

Lists the logging options in use for the facility.

Action:

No action required.

TSS9560I

FACMATRX=YES|NO EXTSEC=YES|NO SAFMODE=YES|NO

Reason:

Lists the options in the facility for FACMATRX, EXTSEC and SAFMODE.

FACMATRX

Indicates whether CA Top Secret will use the settings from the Facility Matrix or the DFHSIT parameter settings (for XTRAN, XPCT, XFCT, etc.).

EXTSEC

Indicates whether external security is requested.

SAFMODE

Indicates whether SAF is requested.

Action:

No action required.

TSS9561I

XJCT=YES|NO XFCT=YES|NO XCMD=YES|NO XDCT=YES|NO XTRAN=YES|NO

Reason:

Identifies SIT parameters for a CICS facility.

XJCT

Indicates whether JCT security protection is active.

XFCT

Indicates whether FCT security protection is active.

XCMD

Indicates whether command security protection is active.

XDCT

Indicates whether DCT security protection is active.

XTRAN

Indicates whether transaction security protection is active.

Action:

No action required.

TSS9561I

XTST=YES|NO XPSB=YES|NO XPCT=YES|NO XPPT=YES|NO XAPPC=NO|YES XUSER=YES|NO

Reason:

Identifies SIT parameters for a CICS facility.

XTST

Indicates whether TCT security protection is active.

XPSB

Indicates whether PSB security protection is active.

XPCT

Indicates whether PCT security protection is active.

XPPT

Indicates whether PPT security protection is active.

XAPPC

Indicates whether session security protection is active.

XUSER

Indicates whether USER security protection is active.

Action:

No action required.

TSS9564I

PCTEXTSEC=HONOR|OVERRIDE PCTCMDSEC=HONOR|OVERRIDE PCTRESSEC=OVERRIDE|HOLD

Reason:

Indicates whether to honor or override the CICS DFHPCT parameter settings.

PCTEXTSEC

Indicates whether CA Top Secret will force transaction security or will honor what has been specified for the PCT EXTSEC= parameter.

PCTCMDSEC

Indicates whether CA Top Secret will force EXEC CICS command protection or will honor what has been specified for PCT CMDSEC= parameter.

PCTRESSEC

Indicates whether CA Top Secret will force resident security protection or will honor what has been specified for PCT RESSEC= parameter.

Action:

No action required.

TSS9565I

DSNCHECK=YES|NO LTLOGOFF=YES|NO|SIGNOFF RLP=NO|YES SLP=NO|YES

Reason:

Lists the data set name and LOCKTIME logoff options for the facility. It also lists whether Record Level Protection and/or Screen Level Protection is active.

DSNCHECK

Indicates whether data set name security is active.

LTLOGOFF

Indicates whether the user's terminal will be logged off from CICS after their locktime has expired a second interval.

RLP

Indicates whether Record Level Protection is active.

SLP

Indicates whether Screen Level Protection is active.

Action:

No action required.

TSS9566I

MAXUSER=nnnnn PRFT=nnn MAXSIGN=nnn,cccc

Reason:

User entered a TSS MODIFY(FACILITY(TSS PROD)) which generated a string of messages and options showing all settings on that facility.

Action:

No action required.

TSS9567I

MAXSIGN VALUE EXCEEDS LIMIT, MAXIMUM VALUE ASSIGNED

Reason:

The MAXSIGN facility sub option value entered is greater than the maximum allowed. The maximum acceptable value has been assigned.

Action:

No action required.

TSS9568I

MAXSIGN VALUE TOO LOW, MINIMUM VALUE ASSIGNED

Reason:

The MAXSIGN facility suboption value entered is less than the minimum allowed. The minimum acceptable value has been assigned.

Action:

No action required.

TSS9570I

BYPASS TABLE DISPLAY FOR FACILITY facility

Reason:

Identifies the CICS facility for which a bypass list is displayed.

Action:

No action required.

TSS9571I

RESOURCE=resourcE

BYPASS NAMES=name

Reason:

Identifies CICS resources and names which will bypass CICS security checking within a CICS facility.

RESOURCE

Identifies the type of resource

BYPASS NAMES

Identifies the name(s) of the resource(s).

Action:

No action required.

TSS9571I

PROTECT NAMES: name

Reason:

Identifies CICS resources that will not bypass CICS security checking within a CICS facility.

PROTECT NAMES

Identifies the name(s) of the resource(s) being protected.

Action:

No action required.

TSS9573I

----- COUPLING FACILITY STATISTICS -----

TSS9574I

Maximum Size (40192K) SizE (10240K)

TSS9575I

Max Entries (000000795) Entries (000000000)

TSS9576I

Requests (000000092) Hits (000000056)

TSS9577I

Writes (000000071) Clears (000000000)

TSS9578I

Locks (000000012) Waits (000000000)

TSS9579I

Unlocks (000000011) EXCPs (00000003)

These are informational messages issued as result of MODIFY STATUS(SYSPLEX)

Field explanations:

Max size

The maximum possible size of the CF structure.

Size

Current size of the CF structure.

Max entries

Number of file blocks that may fit into the current structure size

Entries

Number of file blocks currently in the CF structure

Requests

Total number of requests issued against the CF

Hits

Number of requested file blocks that were found in the cache

Writes

Number of blocks written to the CF

Clears

Number of times the CF was cleared.

Locks

Number of lock requests

Waits

Number of times the lock was busy

Unlocks

Number of unlock requests

Excps

Number of time the lock record was written to the file

TSS9580I

RESCLASS TRANSLATE TABLE DISPLAY FOR FACILITY facility

Reason:

Identifies the CICS facility for which a resource class translate table is displayed.

Action:

No action required.

TSS9581I

FORMAT OF A TRANSLATE ENTRY IS “oldclass : newclass”

Reason:

Identifies the format of a resource class translate entry.

Action:

No action required.

TSS9582I

oldclass : newclass oldclass : newclass oldclass : newclass

Reason:

Identifies the resource class translate entries that are active in the current table. An entry consists of a pair of resource class names, “oldclass” is the source resource class and “newclass” is the target resource class for the translate process. A maximum of 3 entries can be displayed.

Action:

No action required

TSS9583I

RESCLASS TRANSLATE TABLE DOES NOT EXIST

Reason:

An attempt was made to list a facility resource class translate table and it does not exist.

Action:

Create the translate table using the RXLTADD facility sub-option and attempt the list function again.

TSS9584E

A SECURITY ABEND HAS OCCURRED PROCESSING THE TSS TRANSACTION

Reason:

An ABEND occurred in CA Top Secret while processing the TSS transaction. The transaction was not processed.

Action:

Contact CA Technical Support.

TSS9586A

CA Top Secret/IMS FACILITY TYPE IS NON-IMS

Reason:

The facility type associated with the IMS register does not specify TYPE=IMS.

Action:

The Region ACID must be associated with a proper IMS facility such as IMSPROD, IMSTEST, or a user-defined facility specifying TYPE=IMS. See the *Implementation: IMS Guide* for more information.

TSS9588I

UNABLE TO SIGN ON ACID <imsmsc> FOR MSC LINK <msname>

Reason:

The Control Region ACID for an IMS Region has assigned a fixed ACID “imsmsc” to the MSC link name “msname”, but the ACID is not valid for sign on in the Control Region.

Action:

Verify that the name specified is a valid CA Top Secret ACID and has permissions to the IMS facility. In addition, the ACID may be invalid for other reasons such as being suspended. A TSSUTIL report may be helpful in determining the violation and the needed administration to correct the problem.

TSS9590I

INIT(n) XREQ(n) MVS(n)

Reason:

Displays in response to the STATUS option.

INIT

Number of job initiations validated

XREQ

Number of cross-memory requests processed

MVS

Number of MVS security calls processed

Action:

No action required.

TSS9591I

VIOL(n) EXEC(n) SMF(n)

Reason:

Displays in response to the STATUS option.

VIOL

Number of violations detected

SMF

Number of SMF security records logged

EXEC

Number of program executions validated

Action:

No action required.

TSS9592I

CHNG(n) RECV(n) AUD(nnn)

Reason:

Displays in response to the STATUS option.

CHNG

Number of changes made to the Security File

RECV

Number of changes saved in the Recovery File

AUD

Number of records logged to Audit File

The CHANGE value will only be incremented if any of the following commands are issued:

- ADD an ACID or a volume
- DELETE an ACID or a volume
- RENAME an ACID
- REMOVE a volume

Action:

No action required.

TSS9593I

READ(n) WRIT(n)

Reason:

Displays in response to the STATUS option.

READ

Number of Security File Input requests

WRIT

Number of Security File Output operations

HWM

High Water Mark; highest level of requests that were queued

Action:

No action required.

TSS9594I

#REQ(nnnnnn) LOCK(nnnnnn) LWAIT(nnnnnn)

Reason:

Displays in response to the TSS MODIFY(STATUS) option.

#REQ

Number of cross-memory security checks awaiting processing

LOCK

Number of Security File lock I/Os issued

LWAIT

Number of failed Security File lock I/Os causing a wait

Action:

No action required.

TSS9595I

KERNEL DIAGTRAP MATCHED, SFSDRC=XXX

Reason:

The criteria for one of the DIAGTRAP control options previously set has been satisfied.

Action:

No action required. The SFS DRC is listed in the message for all trap types and has been provided for support purposes. CA Top Secret will increment the match-count for the affected trap-id; when the match count reaches the match-limit, the trap-id will be disabled (set to OFF). This message is only displayed when a Kernel diagtrap is matched to DRC 33.

TSS9596I

-----COUPLING FACILITY STATISTICS------

TSS9597I

REQUESTS (000000000) HITS(000000000)

TSS9598I

WRITES (000000000) CLEARS(000000000)

Reason:

These messages provide statistics on Coupling Facility Usage. The display will be part of TSS MODIFY(STATUS).

Action:

No action required.

TSS9598A

ALLOW TRAP DUMP FOR JOB=xxxxxxxx ACID=xxxxxxxx DRC=000

Reason:

A trap event has occurred which requires operator prompting.

Action:

Reply YES to cause a dump for the specified job and ACID or NO to indicate that a dump should not be taken.

TSS9599E

TRAP DUMP FOR JOB=xxxxxxxx ACID=xxxxxxxx

Reason:

Diagtrap has been taken.

Action:

None required.

TSS9601E to TSS9692E

TSS9601E

INVALID PLIST WAS SPECIFIED TO THE CACHE MODULE

Reason:

The caller to the CACHE function did not prepare a valid Plist.

Action:

Contact CA Technical Support.

TSS9602E

INVALID ANCHOR WAS SPECIFIED TO THE CACHE MODULE

Reason:

The caller to the CACHE function did not provide a valid anchor in the Plist.

Action:

Contact CA Technical Support.

TSS9603E

INVALID OPCODE WAS SPECIFIED TO THE CACHE MODULE

Reason:

The caller to the CACHE function did not provide a valid OPCODE in the Plist.

Action:

Contact CA Technical Support.

TSS9604E

CACHE FAILED TO FREEMAIN

Reason:

The CACHE module tried to FREEMAIN a portion of the CACHE but the FREEMAIN SVC failed with a RC of 4. This means that some storage will stay allocated and may be a symptom of another problem.

Action:

Watch for other messages and if the problem recurs contact CA Technical Support.

TSS9605W

CACHE FAILED TO GETMAIN. WILL CAUSE LESS EFFICIENT PERFORMANCE IMPROVEMENTS

Reason:

The CACHE module tried to GETMAIN a storage area for CACHE but the GETMAIN SVC failed, probably due to a lack of storage. This means that the CACHE mechanism will not work at full capacity and may indicate some other problems in the system.

Action:

Watch for other messages and if the problem recurs contact CA Technical Support.

TSS9660I

VERSION=51yymmAKOnn

Reason:

Response to F TSS, VERSION command. Displays the CA Top Secret version number you are running. 51 indicates the 5.1 release, yymm is the genlevel, AKO is the international product code and nn is the level number.

Action:

No action required.

TSS9661I

CA Top Secret xxxxxxxx Status

Reason:

This is a title line for a subsection of output in response to the TSS MODIFY(STATUS) command. It will be followed by multiple lines of information displaying the settings of the control options within that subsection.

Action:

No action required.

TSS9680A

CA Top Secret MAINTASK MANAGER ABEND cccc IN PROGRAM program

Reason:

The CA Top Secret address space has failed. Existing jobs and users will continue to function with full security in effect. New initiations are subject to DOWN options.

In most cases an SVCDUMP will accompany this message. To obtain more information about the error including abend PSW and Registers, issue the MVS D D,E operator command.

Action:

Restart the CA Top Secret address space, obtain dumps (if produced) and report the error to CA Technical Support.

TSS9681A

CA Top Secret SECURITY FILE SERVICES ABEND cccc IN PROGRAM program

Reason:

The Security File services subtask has failed. Existing jobs will continue to function with full security in effect. New initiations are subject to DOWN options.

In most cases an SVCDUMP will accompany this message. To obtain more information about the error including abend PSW and Registers, issue the MVS D D,E operator command.

Action:

Restart the CA Top Secret address space, obtain dumps and report the error to CA Technical Support.

TSS9682A

CA Top Secret OPERATOR COMMUNICATIONS ABEND cccc IN PROGRAM program

Reason:

The operator communication subtask has failed.

Action:

See message TSS9681A

TSS9683A

CA Top Secret TIMER CONTROLS ABEND cccc IN PROGRAM program

Reason:

The asynchronous logging subtask has failed

Action:

See message TSS9681A

TSS9684A CA Top Secret AUDIT FILE SERVICES ABEND cccc IN PROGRAM program

Reason:

The asynchronous logging subtask has failed.

Action:

See message TSS9681A

TSS9685A

CA Top Secret LDAP SERVER TASK ABEND cccc IN PROGRAM program

Reason:

The LDAP server subtask has failed.

Action:

See message TSS9681A.

TSS9692E

PASSWORD IS INCORRECT

Reason:

The supplied password is incorrect.

Action:

No action required.

TSS9693E

CIA REAL TIME PROCESSING COMPONENT ASCRE ERROR – *RC* = XX *RS* = XX

Reason:

The CIA real-time processing component started task could not be started because the ASCRE macro returned an error.

rc

Specifies the return code from ASCRE.

rsn

Specifies the reason code from ASCRE.

Action:

Manually start the CIA real-time processing component started task. For assistance, contact CA Support at http://ca.com/support.

TSS9694E

CIA REAL TIME CA NOT BE ACIVATED WITHOUT *XXXXXXXX*

Reason:

The CIA real-time processing component started task could not be started because the *XXXXXXXX* option has not been specified.

Action:

Use the TSS MODIFY command to specify a value for *XXXXXXXX* and activate CIA real-time again.

TSS9695E

CIAPROCNAME MUST BE SPECIFIED BEFORE CIAAUTO

Reason:

Automatic startup of the CIA real-time processing component address space requires a procedure name to be specified.

Action:

Use the TSS MODIFY command to specify a procedure name. Then reissue the TSS MODIFY command for automatic startup.

TSS9696E

CIASYSID CAN NOT BE CHANGED WHEN CIA REAL TIME IS ACTIVE

Reason:

The CIA real-time system identifier cannot be changed when CIA real-time is active.

Action:

To change the system identifier, stop and restart CIA real-time.

TSS9697E

CIAGBLEXIT AND CIAGBLFIELD ARE MUTUALLY EXCLUSIVE

Reason:

CIAGBLEXIT and CIAGBLFIELD are mutually exclusive..

Action:

Remove one of the keywords.

TSS9698E

CIA REAL TIME SUBTASK NOT AVAILABLE

Reason:

TSS MODIFY(CIART(CONNECT)) or TSS MODIFY(CIART(DISCONNECT)) cannot be issued when the CIA real-time subtask is not active.

Action:

IF CONNECT was specified, issue TSSMODIFY(CIART(START)) to start CIA real-time processing and activate the subtask. If DISCONNECT was specified, no action is necessary.

TSS9699E

CIA Real Time Subtask not activated. z/OS 1.10 or above required

Reason:

The CIA real-time subtask was not activated because the system is at a lower release than z/OS 1.10.

Action:

CIA real-time updates require z/OS 1.10 or higher.

TSS9700E to TSS9769E

TSS9700E

DUF/EXTRACT FAILED - USER HAS NO (INST) DATA

Reason:

A DUFUPD, DUFXTR or EXTRACT request (RACHECK) failed because the specified ACID did not have INSTALLATION data.

Action:

No action required.

TSS9701E

TSS CONTROL OPTION "JCT" IS INCORRECTLY SET

Reason:

Self-explanatory.

Action:

Consult a system programmer to determine the type of primary JES2 active and correct the JCT control option for CA Top Secret.

TSS9702E

ERROR OBTAINING SECURITY RECORD(S) FOR acid. RETRYING REQUEST

Reason:

While initiating a job or session, CA Top Secret was unable to obtain the Security Record for the user due to an error in the TSS address space.

Action:

CA Top Secret retries once. If error persists, the Security Record may have been damaged or the Security File itself is damaged. Attempt recovery. If problem was not caused by system or hardware failure, contact CA Technical Support.

TSS9703E

INSUFFICIENT CSA OR LOCAL STORAGE

Reason:

During a job/session initiation, CA Top Secret was unable to transfer the user's security record(s) from the CA Top Secret address space to that of the user.

Action:

Probable cause is lack of common storage (CSA). This is a system-wide problem.

TSS9704E

SECURITY RECORD DAMAGED OR INSUFFICIENT CSA. TRY AGAIN.

Reason:

An error that cannot be corrected was detected in the Security Record.

Action:

Attempt to recover the Security Record. If the problem was not attributable to system software or hardware failure while updating the record, contact CA Technical Support.

TSS9705E

NO AUTHORITY FOR INTERNAL SECURITY FUNCTION function

Reason:

A RACINIT macro was issued by an unauthorized task or, the task has insufficient authority to DUFXTR or DUFUPD.

Action:

See the FACILITY/AUTHINIT control option, or add DUFXTR and/or DUFUPD to the ACID.

TSS9706E

PROBABLE SITE INTERFACING ERROR drc

Reason:

See the Detailed Reason: Code section for cause of problem.

Action:

If not a user error, contact CA Technical Support.

TSS9707E

INTERNAL SYSTEM ERROR (drc)

Reason:

See the Detailed Reason: Code section for cause of problem.

Action:

If not a user error, contact CA Technical Support.

TSS9708E

INTERNAL INTEGRITY CHECK FAIL

Reason:

CA Top Secret checks for user's environment every time an access takes place. The environment has been altered; possible subversion or system error.

Action:

Take a dump of the user's address space. Contact CA Technical Support.

TSS9709I

aaa-bb ABEND IN svcname PROCESSING- reason

Reason:

A system abend has been issued in response to an invalid condition being detected by the CA Top Secret SVC handler.

aaa

Abend code in hexadecimal.

bb

Reason: code in hexadecimal.

svcname

Name of security svc issued.

reason

Short explanation of error encountered.

Summary of 282 abend and reason codes and their meanings:

-10 ABEND IN RACHECK PROCESSING- NOT APF AUTHORIZED

The form of RACHECK issued requires APF authorization but was issued by a non-APF caller.

-1C ABEND IN RACHECK PROCESSING- PROFILE/ENTITY CONFLICT

The RACHECK parameter list has conflicting bit settings. The parameter list indicates that both the PROFILE= and ENTITY= parameters have been coded.

Action:

Correct the error(s) in the issuing code and rerun the job.

TSS9710E

SYSPLEX sysplex FAILED RC=nnnn RSN=nnnn sysplex = DISCONNECT / CONNECT / SEND MSG

Reason:

An error occurred during CONNECT, DISCONNECT or SEND MSG processing.

Action:

The return code and reason codes are from CASECCFS. See the chapter “Codes” for explanations of the codes.

TSS9711I

CA Top Secret IS NOW CONNECTED TO THE COUPLING FACILITY

Reason:

This is an informational message indicating that CA Top Secret has connected to the Coupling Facility.

Action:

No action required.

TSS9712E

CF DID NOT RETURN A LENGTH FOR WORKAREA

Reason:

CASECCFS failed to return a workarea size for the workarea.

Action:

Contact CA Technical Support.

TSS9713I

CA Top Secret IS NOW DISCONNECTED FROM THE COUPLING FACILITY

Reason:

This is an informational message indicating that CA Top Secret has disconnected from the Coupling Facility.

Action:

No action required.

TSS9714E

MODULE CASECCFS MISSING CONNECT / DISCONNECT FAILED

Reason:

CASECCFS could not be located in the RCVT.

Action:

Contact CA Technical Support.

TSS9715E

STORAGE OBTAIN FAILED <module/subroutine>

Reason:

An internal error occurred.

Action:

Contact CA Technical Support.

TSS9716E

STORAGE RELEASE FAILED <module/subroutine>

Reason:

An internal error occurred.

Action:

Contact CA Technical Support.

TSS9717I

CA Top Secret NOW USING THE COUPLING FACILITY

Reason:

A successful SYSPLEX(ACTIVATE) was issued.

Action:

No action required.

TSS9718I

MODIFY COMMAND SENT VIA XCF TO ALL CONNECTED SYSTEMS IN THIS SYSPLEX

Reason:

A TSS MODIFY command has been successfully sent to all systems defined in the SYSPLEX.

Action:

No action required.

TSS9719E

AN UNAUTHORIZED MODIFY COMMAND WAS ISSUED FROM SYSTEM system BY USER acid

Reason:

A TSS MODIFY command was received from another system but the acid issuing the command is not defined to this system or does not have CONSOLE authority.

Action:

Contact CA Technical Support.

TSS9720I

CA Top Secret CONNECTED TO TSSXCF

Reason:

Successful connection to the XCF function has been established. Message TSS9721I follows this message.

Action:

No action required.

TSS9721I

TSSXCF GROUP group-name MEMBER member-name

Reason:

This message notifies all systems that are members of the SYSPLEX that another system has joined the group. The system is identified by its group-name and member-name.

Action:

No action required.

TSS9722I

CA Top Secret DISCONNECTED FROM TSSXCF

Reason:

This is an informational message indicating that CA Top Secret successfully disconnected from TSSXCF.

Action:

No action required.

TSS9723E

INCORRECT BUFFER SIZE FOR CF

Reason:

A buffer size of 0 or larger than 32K was requested.

Module: TSSSFSC1

Action:

Specify a buffer size between 1 and 32K.

TSS9725E

CF LOCK HELD. DISCONNECTING FROM CF

Reason:

A lock is held in the Coupling Facility. Four tries have been attempted. A disconnect force is issued to ensure the integrity of the Security File. All other systems will be forced from the Coupling Facility on the next I/O for each.

Action:

Find which system is holding the lock and ensure all systems have been disconnected from the Coupling Facility. Once all systems are disconnected, issue a SYSPLEX(CONNECT) for all systems and then issue a SYSPLEX(ACTIVATE) for one system.

TSS9726E

CA Top Secret DISCONNECTED FROM COUPLING FACILITY. WRONG SECFILE IN USE.

Reason:

The wrong Security File is being used by the system requesting connection to the Coupling Facility. The DSNAME validation or VOLSER validation failed.

During connect processing, the validation record was checked to determine whether the correct Security file is being used with the system requesting to connect.

Message TSS9727I accompanies this message.

Action:

Correct the Security File used by the system to match the Security File defined to the Sysplex.

Module:

TSSMNGR

TSS9727I

SECFILE = securityfile, volser

Reason:

This is an informational message indicating the name of the first Security File that was connected to this structure. The VOLSER of the file currently active in the Coupling Facility structure is also displayed.

Action:

No action required.

Module:

TSSMNGR

TSS9728E

CA Top Secret DISCONNECTED FROM COUPLING FACILITY. SECFILE VALIDATION FAILED.

Reason:

Security File name validation failed.

Action:

Contact CA Technical Support.

Module:

TSSMNGR

TSS9729E

CA Top Secret ACTIVATED FAILED. NOT CF CONNECTED.

Reason:

SYSPLEX(ACTIVATE) failed because CA Top Secret was not connected to the Coupling Facility.

Action:

Issue a SYSPLEX(CONNECT) command prior to SYSPLEX(ACTIVATE).

Module:

TSSPARAM

TSS9730E

HEADER IS LOCKED.

Reason:

Coupling Facility header is locked. CA Top Secret will disconnect from the Coupling Facility.

Action:

Contact CA Technical Support.

Module:

TSSMNGR TSSSFSC1

TSS9731I

CF TRACE

READ , WRITE , READ/WRITE‡ RBA ??????

Reason:

This is an informational message indicating the type of request and the RBA being processed.

Action:

No action required.

Module:

TSSMNGR TSSSFSC1

TSS9732I

CF TRACE

READ , WRITE , READ/WRITE‡ RC=???? RSN=????

Reason:

This is an informational message indicating the type of request, the return code, and reason code from that request.

Action:

No action required.

Module:

TSSMNGR TSSSFSC1

TSS9733E

DUPLICATE NAME GIVEN FOR CONNECT/GROUP/STRUCTURE

Reason:

A duplicate name was specified in the SYSPLEX control option, or the connection has already been established with the remote system.

Action:

Review the SYSPLEX control option for duplicate names.

TSS9734E

CA Top Secret ALREADY CONNECTED

Reason:

The system was already connected when a second connect was issued.

Action:

If you wish to change connect information, you must first disconnect then reissue the connect.

TSS9737I

DUPLICATE NAME GIVEN FOR CONNECT/GROUP/STRUCTURE

Reason:

This is an informational message indicating that name specified on a SYSPLEX control option has already been used.

Action:

Reenter the command specifying a different name for the connection, group or structure.

TSS9738E

Neither XCF_Group nor XES_Structure are provided

Reason:

An attempt was made to connect, but neither an XCF group name nor XES structure name was provided.

Action:

Attempt to connect again, but provide the structure name, and the optional group name if you want to be connected to a group.

Reply YES to enable Coupling Facility locking, or WAIT to wait until the file is released. Reply ABORT to abort the attempt by the local system to lock the Security File.

TSS9740E

BAD PARM FOR TNGMON

Reason:

A user error was encountered.

Action:

You must correct parameters that caused error.

TSS9741E

TNGMON TABLE MISSING

Reason:

An internal CA Top Secret problem occurred.

Action:

Contact CA Technical Support.

TSS9742E

STORAGE OBTAIN FAILED

Reason:

Subpool 231 storage could not be obtained.

Action:

Contact CA Technical Support.

TSS9743I

ENTRY NOT FOUND

Reason:

Requested entry could not be found.

Action:

This is an informational message.

TSS9745E

Structure (str_name) has same version as structure previously disconnected from

Reason:

After a successful re-connect, the structure version is compared to the version that existed prior to the disconnect. If the version is the same, this message is displayed and the system is disconnected from the Coupling Facility structure.

Action:

Contact CA Technical Support.

TSS9746I

C.F. XES Str(SECURITY2) is now 075% full

Reason:

Indicates that the Coupling Facility structure entry utilization has gone over 75 percent. This warning is reissued whenever utilization changes by at least 5 percent.

Action:

This is an informational message. You may want to use the TSS MODIFY(STATUS(SYSPLEX)) command to check the structure utilization counts and structure size. Then use the z/OS operator SETXCF command to increase the structure size.

TSS9747I

Waiting for Security File CF lock

Reason:

Indicates that the lock is held by another system, when the current system tries to lock the file. This message is issued only if a system waits for the Coupling Facility lock for more than 15 seconds.

Action:

No action required. This is an informational message.

TSS9748E

Unable to obtain SECFILE lock. Disconnect aborted.

Reason:

Indicates that a disconnect was aborted, because a file lock could not be obtained when the disconnect was being processed.

Action:

Look for Coupling Facility related error messages and Contact CA Technical Support.

TSS9760I

SFSBSCER - Subtask started

Reason:

CA Top Secret has started a subtask to rebuild the digital certificates in-core table.

Action:

None.

TSS9761I

SFSBSCER - Subtask ended

Reason:

CA Top Secret finished rebuilding the digital certificates in-core table.

Action:

None.

TSS9762E

Unable to re-open VSAMAIX file.

Reason:

CA Top Secret was unable to re-open the VSAM alternate index file. Processing continues without using this file until CA Top Secret is recycled.

Action:

None.

TSS9763E

SFSBSCER - Certificate error, DIGICERT= certname, ACID= acidname

Reason:

CA Top Secret failed to add a certificate to the digital certificates in-core table.

Action:

Contact CA customer support.

TSS9766I

SFSCACRT - Subtask started

Reason:

CA Top Secret has started a subtask to auto-register CA certificates.

Action:

None.

TSS9767I

SFSCACRT - Subtask ended

Reason:

CA Top Secret has finished auto registering CA certificates.

Action:

None.

TSS9768E

Unable to add CA certificate. RC=*xxx* Label=*name*

Reason:

CA Top Secret failed to auto-register the CA certificate associated with the specified label name.

Action:

Contact CA customer support.

TSS9769I

CA certificate installed. Label=*name*

Reason:

CA Top Secret successfully registered the CA certificate associated with the specified label name.

Action:

None.

TSS9800E to TSS9999E

TSS9800E

CPF RECOVERY FILE FAILED TO OPEN: CONTINUING WITHOUT FILE

Reason:

CA Top Secret attempted to open the CPF recovery file (CPFFILE DD in the CA-TSS startup JCL) but failed. CPF processing will continue.

Action:

If you desire to use the automatic requeueing mechanism of CPF, ensure the CPFFILE DD is present in the startup proc for CA Top Secret.

TSS9801E

CPF RECOVERY FILE HDR INCORRECT: FILE WILL NOT BE PROCESSED

Reason:

CA Top Secret opened the CPF recovery file but found it was not properly formatted. CPF processing will continue.

Action:

Ensure the data set pointed to by the CPFFILE DD in the startup proc for CA Top Secret has been properly formatted by TSSMAINT.

TSS9802I

FREEMAIN FAILURE IN CPF TASK

Reason:

Internal CPF error.

Action:

Contact CA Technical Support.

TSS9803W

NO FREE RECORDS ON CPF RECOVERY FILE

Reason:

CA Top Secret attempted to write a record to the CPF recovery file, but the file was full.

Action:

Since CA Top Secret only writes to the recovery file when the receiving node is down, determine why that receiving has not restarted. If necessary, enlarge the CPF recovery file.

TSS9804A

CA-TSS CPF COMMUNICATIONS LINK ABEND *xxxx* IN *mmmmmmmm*

Reason:

The CPF communications services subtask abended with code *xxxx* in module *mmmmmmmm*.

Action:

Restart CPF by using the TSS MODIFY CPF(ON) command. Obtain dumps and report the event to CA Support.

In most cases, an SVCDUMP accompanies this message. To obtain more information about the error (including abend PSW and registers), issue the MVS D D,E operator command.

TSS9804I

CA Top Secret CPF TASK ABENDED; REMOTE COMMUNICATIONS LOST

Reason:

The CPF communications services subtask failed. TSS commands and password changes continue to function but will not be sent to remote nodes. CPF(OFF) is in effect.

Action:

Restart CPF by using the TSS MODIFY CPF(ON) command. Obtain dumps and report the event to CA Support.

In most cases, an SVCDUMP accompanies this message. To obtain more information about the error (including abend PSW and registers), issue the MVS D D,E operator command.

TSS9805I

CAICCI NOT AVAILABLE, AUTO RETRY IN PROGRESS

Reason:

The CPF task was active but Unicenter CA Common Services CCI was unavailable. This message can be completely normal during IPL until CCI can establish communications through VTAM or TCP/IP with one or more available nodes. It can also occur during a communications failure, or catastrophic system failure.

Action:

It will be obvious when this message occurs due to a system or communications failure. Recovery from such failures is beyond the scope of CA Top Secret. Remedy the problem if possible. If the problem is due to temporary timing issues during IPL, wait until the communications tasks have correctly initialized. The message will clear itself up and no action will be necessary.

TSS9806I

COMMAND QUEUED FOR DESTINATION cpfnode

Reason:

Indicates (on the CPF journal file) to which node a command has been routed.

Action:

No further action required.

TSS9807I

COMMUNICATIONS FAILURE (nnnn), COMMAND NOT SENT TO DESTINATION cpfnode

Reason:

The command was not sent to the specified destination or node. This probably occurred because the link to the remote destination is down.

Action:

Contact your systems programmer to activate the link.

TSS9808E

MSG FAILED VALIDITY CHECK ON REMOTE MACHINE

Reason:

Internal CPF error.

Action:

Contact CA Technical Support.

TSS9809E

MSG FAILED DUE TO TOP SECRET SYSTEM ERROR ON REMOTE MACHINE

Reason:

Internal CPF error.

Action:

Contact CA Technical Support.

TSS9810I

******* COMMUNICATIONS ESTABLISHED WITH NODE xxxxxxxx**

Reason:

CA Top Secret is establishing remote communications with the specified node. If activation completes successfully, no further messages appear. If activation fails, messages appear to explain the reason.

Action:

No further action required.

TSS9811I

******* CPF SUBTASK INITIALIZED FOR NODE *******

Reason:

A new target node has been added to the current list of CPF nodes (VIA the NODES control option) and communications have been established.

Action:

No further action required.

TSS9812I

REMOTE MACHINE NOT RECEIVING: CPF(OFF) SET

Reason:

A TSS command was routed though CPF to a remote node. The CA Top Secret running on the remote node had the CPF control option set to OFF. The command was rejected by the remote node.

Action:

Determine why CPF is inactive on the remote node.

TSS9813I

NODE BUSY; COMMAND NOT SENT TO NODE cpfnode

Reason:

Someone else is also in the process of sending a synchronous command (using WAIT(Y)) to the remote node. The command was not send to that node.

Action:

This should not happen often. If so, contact CA Technical Support.

TSS9814E

COMMAND RESULTS ON TARGET NODE node UNKNOWN; COMMUNICATIONS LOST

Reason:

The CA Top Secret command was successfully sent to the specified node but communications with the node were lost before a response to the command was received.

Action:

After communications are re-established with the node, issue additional TSS commands or check the CPF Journal File for the completion status of the command.

TSS9815I

CAICCI REASON TEXT: text

Reason:

This message is issued immediately after message TSS9807I to explain the reason for the communication failure. The reason text in this message was provided by CAICCI.

Action:

See the CA Common Services for z/OS documentation for more information.

TSS9816I

REMOTE MACHINE NOT ACCEPTING COMMANDS FROM THIS NODE

Reason:

A targeted node cannot accept commands from the originating node because the originating node is defined to the target node as send-only (i.e. 'CPFNODES(ORIGNODE(S))') or the target node is running with CPFRCVUND(NO) set.

Action:

Do not target any TSS commands to the remote node or have the control options changed at the remote node to accept TSS commands from this node.

TSS9817I

COMMANDS CANNOT BE SENT TO DESTINATION xxxxxxxx

Reason:

TSS commands cannot be sent to a targeted node because that node is defined as receive-only (for example, 'CPFNODES(TGTNODE(S))').

Action:

Do not target any TSS commands to the remote node or have the control options changed to allow commands to be sent to that node.

TSS9818E

CPF RECOVERY FILE CONTAINS BAD RECORDS. REFORMAT REQUIRED.

Reason:

During CPF recovery file initialization, records were discovered that do not match the CA Top Secret r5.0 structure.

Action:

Initialization will continue but CPF recovery will be turned off. Use the TSSMAINT to reformat the CPF recovery file to eliminate any bad records.

TSS9819I

COMMAND NOT SENT TO INACTIVE NODE XXXXXXXX

Reason:

CA Top Secret detected that a node was inactive, and did not send the command to that particular node.

Action:

After the node displays as active, re-execute all WAIT=YES commands for that node since they were not logged to the CPF Recovery File. By contrast, WAIT=NO commands were logged and will be transmitted during RETRY processing.

TSS9820I

***CPFRECV COMMAND SCHEDULED**

Reason:

This message is displayed in response to the following command:

```
TSS REM(*CPFRECVP) UNTIL(XX/XX/XX)
```

Action:

No action required.

TSS9823E

Unable to allocate CPF Node Table. CPF processing terminates

Reason:

Not enough storage available to allocate in-core CPF node table.

Action:

Increase CA Top Secret address space region size.

TSS9824E

Error reading NDT CPFNODE records. CPF processing terminates

Reason:

An error was encountered reading the NDT record from the security file. The file may be damaged. CPF initialization will terminate with an abend.

Action:

Perform security file recovery procedures. If the problem persits, contact CA Technical Support.

TSS9825I

CPF Node(xxxxxxxx) refreshed

Reason:

This message is issued after a CPF node is refreshed following CPFNODE REFRESH modify command.

Action:

No action required.

TSS9826E

Unable to expand CPF NODE table. CPF processing terminates.

Reason:

Not enough storage available to expand the in-core CPF node table.

Action:

Increase CA Top Secret address space region size.

TSS9827I

CPF Task restart in progress

Reason:

This message is issued when CPF is restarting following a CPF(REFRESH) modify command.

Action:

No action required.

TSS9828I

CPF Processing Terminated

Reason:

This message is issued when CPF has terminated following a CPF(OFF) modify command.

Action:

No action required.

TSS9829E

CPF Node(xxxxxxxx) Modify(yyyyyyyy) Failed. Reason:=nnn

Reason:

A CPFNODE modify command failed. *xxxxxxxx* is substituted by the node name which is the targe of the command. *yyyyyyyy* is one of the CPFNODE command verbs: STOP, START, or REFRESH. nnn is one of the following reason codes:

001-Node name not found in node table.

002-No XE04 segment found in NDT record.

003-No sysid entry found in XE04 segment.

004-Node name not found in XE04 segment.

005-Error building new in-core table node entry.

006-Unable to read NDT record.

Action:

For reason codes 001 through 004 it may be required to define the target node name in the NDT record for the local sysid and retrying the command. Else the security file might be damaged and recovery procedures have to be performed. For reason code 005, the region size may have to be increased to accommodate additional node entries.

TSS9830E

CPF Node(xxxxxxxx) Start failed. Node already active.

Reason:

A CPFNODE START modify command failed because the node is already active.

Action:

No action required.

TSS9831E

CPF Node(xxxxxxxx) Stop failed. Node already stopped.

Reason:

A CPFNODE STOP modify command failed because the node is already stopped.

Action:

No action required.

TSS9832I

CPF Node(xxxxxxxx) stopped.

Reason:

This message is issued after a CPF node is stopped following a CPFNODE STOP modify command.

Action:

No action required.

TSS9833I

CPF Node(xxxxxxxx) started.

Reason:

This message is issued after a CPF node is started following a CPFNODE START modify command.

Action:

No action required.

TSS9834E

Error occurred in CPF task reading NDT record.

Reason:

Error occurred in the CPF subtask reading the NDT record. The security file may have been damaged.

Action:

Perform security file recovery procedures. If the problem persists, contact CA technical support.

TSS9835E

Journal file for CPFNODE(xxxxxxxx) failed to open. Wrong DSORG

Reason:

Error occurred opening a DASD journal file because the file was created with an incorrect DSORG attribute.

Action:

Allocate the file as a physical sequential data set.

TSS9835I

REMOTE SYSTEM HAS STOPPED ACCEPTING COMMANDS FROM THIS NODE

Reason:

CPF is not receiving commands from the node because the node is in a stopped state.

Action:

Investigate why the node is in a stopped state. Re-activate stopped node.

TSS9836E

ALLOCATION ERROR: RC= $$ / $$ / $$

Reason:

Dynamic allocation for a CPF journal file has failed. The message includes the return code, error code and info code, returned by the SVC 99 call.

Action:

Consult IBM's “Auth Assembler Services Guide” for the meaning of the error codes, and attempt to correct the possible cause of the particular error. If the problem persists, contact CA technical support.

TSS9837I

DDNAME: xxxxxxxx / DSNAME: xxxxxxxxxxxxxxxx

Reason:

This message accompanies message TSS9836E and lists the DDNAME and DSNAME for which Dynamic allocation has failed.

Action:

No action required.

TSS9838E

DAIRFAIL FAILED: RC= $$

Reason:

This message may accompany message TSS9836E and is issued if a DAIRFAIL request fails to format the Dynamic allocation error messages.

Action:

No action required.

TSS9839I

CPF Node(xxxxxxxx) Quiesced and pending delete

Reason:

This message is issued after an active CPF node is deleted from the NDT record, and a CPFNODE REFRESH modify command is issued for the node. CPF will finish processing all currently queued commands while not allowing any new commands to be queued up against this node. When all queued commands are processed, the node will be removed from the in-core node table.

Action:

No action required.

TSS9840I

******* CPF Processing terminated for node *******

Reason:

This message is written to a CPF node journal file when the journal file is closed.

Action:

No action required.

TSS9841E

CPFNODE Start failed. Node is pending delete.

Reason:

This message is issued after a CPFNODE START modify command is issued for a CPF node which pending delete following a previous REFRESH command..

Action:

Wait for the REFRESH command to complete and retry the START command.

TSS9842I

CPF Node(xxxxxxxx) Deleted.

Reason:

This message is issued when a CPF node is removed from the in-core node table following a CPFNODE REFRESH modify command.

Action:

No action required.

TSS9843I

CPF Refresh Subtask Started

Reason:

This message is issued when CPF is activated following a CPF(ON) modify command, and the CPF refresh subtask is attached.

Action:

No action required.

TSS9844I

CPF Refresh Subtask Terminating

Reason:

This message is issued when CPF is terminating following a CPF(OFF) modify command, and the refresh subtask is being detached.

Action:

No action required.

TSS9845I

CPF Node(xxxxxxxx) Quiesced.

Reason:

This message is issued after an active CPF node is stopped after a CPFNODE REFRESH modify command is issued for the node. CPF will finish processing all currently queued commands while not allowing any new commands to be queued up against this node.

Action:

No action required.

TSS9846I

******* CPF Processing options changed for this node *******

TSS9846I

*********** BROADCAST(YES/NO)**

TSS9846I

*********** GATEWAY(YES/NO)**

TSS9846I

*********** SEND(ALL/NONE/CMD/PWD)**

TSS9846I

*********** RECEIVE(ALL/NONE)**

Reason:

These messages are written to a CPF node journal file when the CPF processing options for the node are changed following a CPFNODE REFRESH command. The new processing options for the node are listed.

Action:

No action required.

TSS9847E

CPF Node(xxxxxxxx) Modify(REFRESH) failed. Node is not NDT defined.

Reason:

A CPFNODE REFRESH modify command failed because the node is not defined in the NDT record.

Action:

Ensure the node name is defined in the NDT record and retry the command.

TSS9848E

CPF Node(xxxxxxxx) Modify(yyyyyyyy) failed. Node is undefined.

Reason:

A CPFNODE modify command failed because the node is not defined in the NDT record or does not exist in the in-core node table. xxxxxxxx is substituted by the node name which is the target of the command. yyyyyyyy is one of the CPFNODE command verbs, STOP, START or REFRESH.

Action:

Ensure the node name specified is correct and retry the command.

TSS9849I

CPF Processing Activated

Reason:

This message is issued when CPF is activated following a CPF(ON) modify command.

Action:

No action required.

TSS9851I

LDS server initialization complete

Reason:

The LDAP server task has successfully initialized.

Action:

None.

TSS9852E

LDAP Request not processed

Reason:

The LDAP node table is not built yet.

Action:

Contact CA Technical Support.

TSS9853I

LDAP TASK RECOVERY COMPLETE

Reason:

The LDAP server task has successfully recovered from a previous abend.

Action:

None.

TSS9854E

CA Top Secret not initialized

Reason:

The LDAP server task failed to start because TSS is not active.

Action:

Ensure TSS is active before TSSLDAP is started.

TSS9854E

CA Top Secret not initialized

Reason:

The LDAP server task will not start when the LDAP control options is OFF.

Action:

Ensure that LDAP control options are ON before TSSLDAP is started.

TSS9855E

CA Top Secret LDAP option disabled

Reason:

The LDAP option has been disabled.

Action:

Ensure LDAP control options is ON before TSSLDAP is started.

TSS9856E

CA Top Secret SAF error

Reason:

The LDAP server task failed to start because SAFIVT could not be located.

Action:

Ensure SAF is initialized before TSSLDAP is started.

TSS9857E

LDS server initialization error

Reason:

The LDAP server task failed to start after an abend has occurred.

Action:

Contact CA Technical Support.

TSS9858E

LDS server termination error

Reason:

The LDAP server task has abended during termination.

Action:

Contact CA Technical Support.

TSS9859E

TSSLDAP LDAP error code xxxxxxxx

Reason:

The LDAP server task has encountered an outbound runtime error.

Action:

Contact CA Technical Support.

TSS9860E

TSSLDAP is not APF authorized

Reason:

The LDAP server task is not APF authorized.

Action:

Contact CA Technical Support.

TSS9861I

LDS server termination complete

Reason:

The LDAP server task has terminated.

Action:

None.

TSS9862E

LDS server is already running

Reason:

The LDAP server task already has an active instance.

Action:

None.

TSS9863E

LDS request ignored - Invalid length

Reason:

The LDAP server received a request with invalid data length.

Action:

Contact CA Technical Support.

TSS9864E

TSSLDS Unable to start LDS journaling

Reason:

The LDAP server could not start LDS journaling.

Action:

Contact CA Technical Support.

TSS9868W

SYSOUT unavailable, LDS journal file ignored

Reason:

This message is issued from TSSLDS if LDSJRNL is allocated as SYSOUT in the startup procedure and CA Top Secret starts before JES.

Action:

No action required.

TSS9869E

Output file for xxxxxxxx failed to open. Wrong DSORG

Reason:

Error occurred opening a DASD journal file because the file as created with an incorrect DSORG attribute.

Action:

Allocate the file as a physical sequential dataset.

TSS9870E

ALLOCATION ERROR: RC= $$/$$/$$

Reason:

Dynamic allocation for LDS journal file has failed. The message includes the return code, error code and information code, returned by the SVC 99 call.

Action:

Consult the IBM *Auth Assembler Services Guide* for the meaning of the error codes and attempt to correct the possible cause of the particular error. If the problem persists, contact CA Technical Support.

TSS9871I

DDNAME: xxxxxxxx/DSNAME: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Reason:

This message accompanies message TSS9869E and lists the DDNAME and DSNAME for which Dynamic allocation has failed.

Action:

No action required.

TSS9872E

DAIRFAIL FAILED: RC= $$

Reason:

This message may accompany message TSS9869E and is issued if a DAIRFAIL request fails to format the Dynamic allocation error messages.

Action:

No action required.

TSS9873W

SYSOUT unavailable, LDS Trace file ignored

Reason:

This message is issued from TSSLDS if DDNAME=SYSOUT is allocated as SYSOUT in the startup procedure and CA Top Secret starts before JES.

Action:

No action required

TSS9874E

LDS Modify command already in progress. Retry the command later

Reason:

The LDAP server is processing a previous Modify command.

Action:

Retry the command later.

TSS9875E

LDS Node Table refresh already in progress. New table refresh will be delayed.

Reason:

The LDAP server is processing a previous LDAP node table refresh. A new table refresh will be delayed until the server completes the current refresh.

Action:

None.

TSS9876E

LDS request ignored - Invalid Parmlist

Reason:

The LDAP server detected an Invalid Parmlist.

Action:

Contact CA Technical Support.

TSS9877E

MLS NOT ACTIVATED. SECURITY FILE NOT INITIALIZED FOR MLS PROCESSING

Reason:

An attempt was made to set MLACTIVE(YES) when the security file was initialized with MLSBLOCKS=0 (the default).

Action:

Edit the CAI.SAMPJCL(SECPARMS) member: assure that MLSBLOCKS is of sufficient size for your use. Create new SECFILE and BACKUP files and to copy your existing SECFILE. Alter your TSS procedure JCL to point at the new SECFILE and BACKUP. Perform a temporary shutdown and REINIT of TSS. You may now activate MLS security.

TSS9878E

z/OS 1.5 or HIGHER REQUIRED FOR MLACTIVE(YES)

Reason:

An administrator attempted to activate MLS security on a system that was not running IBM's z/OS Version 1.5 operating system.

Action:

None.

TSS9879I

Stats Gathering Activated

Reason:

An administrator started Statistics Gathering by setting the STATG control option to ON.

Action:

None – information only.

TSS9880I

CPFRECV - NO LONGER IN STRESS MODE

Reason:

The CPF receive thread is no longer in stress mode.

Action:

No action required.

TSS9881I

CPFRECV - ENTERING STRESS MODE

Reason:

There are more incoming CPF commands queued than there are available TSS command subtasks to process them. While this situation exists, TSS places incoming commands from CPF onto a suspend queue pending availability of a command subtask. This message is informational and under normal processing is followed by message TSS9880I.

Action:

No action required.

TSS9882I

Stats Gathering Deactivated

Reason:

An administrator ended Statistics Gathering by setting the STATG control option to OFF.

Action:

None – information only.

TSS9883E

MLS IS NOT ACTIVE. COMMAND REJECTED

Reason:

An attempt was made to activate MLSLBLRQ but MLS was not active.

Action:

Activate MLS (MLACTIVE(YES)) and reissue command.

TSS9884I

MLS HAS BEEN DEACTIVATED

Reason:

An administrator issued a command to deactivate MLS.

Action:

None - information only.

TSS9885I

MLS HAS BEEN ACTIVATED

Reason:

An administrator has activated MLS.

Action:

None - information only.

TSS9886I

MLSLBLRQ HAS BEEN ACTIVATED

Reason:

An administrator has activated MLSLBLRQ.

Action:

None - information only.

TSS9887I

MLSLBLRQ HAS BEEN DEACTIVATED

Reason:

MLSLBLRQ has been deactivated via a command or because MLS was deactivated.

Action:

None - information only.

TSS9887I

Required input cfile //CFILEIN missing

Reason:

The required TSSCFILE output file is not specified in the TSSCFILX JCL.

Action:

Specify a TSSCFILE input file in the TSSCFILX JCL.

TSS9888I

Invalid format input file //CFILEIN

Reason:

The specified TSSCFILE input file is not in the proper format.

Action:

Ensure that the TSSCFILE input file is fixed block, record length 300, and blocksize 3600.

TSS9889I

Required input //IN file missing

Reason:

//IN was not specified in the TSSCFILX JCL.

Action:

Specify //IN DD * and a valid TSS LIST command in the TSSCFILX JCL.

TSS9890I

Required output file //OUT missing

Reason:

A required output file was not specified in the TSSCFILX JCL.

Action:

Specify an output file for the TSSCFILX utility.

TSS9891I

TSSCFILX+???? ABENDED S??? <----------

Reason:

The TSSCFILX utility has abended.

Action:

Review the TSSCFILX JCL submitted and contact Top Secret Support.

TSS9892I

INVALID/UNSUPPORTED REQUEST, RC=08, KEYWORD=

Reason:

The TSS command entered as input to the TSSCFILX utility was invalid.

Action:

Review and correct the TSS command entered as input for the TSSCFILX utility.

TSS9893I

NO RECORDS FOUND MATCHING REQUEST, RC=04

Reason:

No records were found in the TSSCFILE input file that matched the TSS command entered in the TSSCFILX JCL.

Action:

Enter a different TSS command in the TSSCFILX JCL.

TSS9894I

LIST FUNCTION SUCCESSFUL, OUTPUT RECORDS=

Reason:

TSSCFILX found matching records for the LIST command. The total number of record lines is displayed.

Action:

None. Information Only.

TSS9895I

Required input //IN file empty

Reason:

//IN was entered without a TSS LIST command in the TSSCFILX JCL.

Action:

Specify a TSS LIST on the next line after the //IN in the TSSCFILX JCL.

TSS9896I

Storage not available for input

Reason:

Storage was not obtained for the user input for TSSCFILX

Action:

Contact Top Secret Support.

TSS9897I

Storage not available for CFILE records

Reason:

Storage was not obtained for the CFILE records.

Action:

Contact Top Secret Support.

TSS9898I

Required print file //PRINT file empty

Reason:

//PRINT was omitted from the TSSCFILX JCL.

Action:

Specify //PRINT DD SYOUT=* in the TSSCFILX JCL.

TSS9899I

USER MUST BE AN MSCA OR AN SCA TO RUN TSSCFILX

Reason:

The user does not have the required authority to run TSSCFILX

Action:

Contact your system administrator.

TSS9901I

Node(xxxxxxxx) send request timed out. Retry started

Reason:

TSSCPF attempted to send a command to remote node xxxxxxxx, but the remote system did not acknowledge receiving the command. TSSCPF will retry sending the command.

Action:

Other messages that indicate if the retry was successful may be displayed with this message. If no other messages are displayed, and you are unable to determine the cause of the failure, contact CA Support.

TSS9902E

CPF Node(xxxxxxxx) send request timed out. Retry failed

Reason:

TSSCPF attempted to send a command to remote node xxxxxxxx and the retry process failed. Network problemes between the local and remote systems may exist.

Action:

Look for additional network component messages (VTAM, CCI, or others) to determine the cause of the send command failure. If you are unable to determine the cause of the failure, contact CA Support.

TSS9903I

CPF Node(xxxxxxxx) is being deactivated. A System Dump is generated

Reason:

TSSCPF attempted to send a command to the remote node xxxxxxxx and the retry process failed. The node is deactivated and CPF attempts to re-activate it once the communication link becomes operational. Problems between the local and remote systems may exist.

Action:

Other messages that indicate if the retry was successful may be displayed with this message. If no other messages are displayed and you are unable to determine the cause of the failure, contact CA Support.

TSS9905E

CPF Node(xxxxxxxx) Send/Cancel error. RC=xx, DRC=xx, XRC=xx

Reason:

TSSCPF attempted to cancel a send command request, but the CCI CANCELS function failed with an unacceptable error condition.

Note: For more information about error codes RC, DRC, and XRC, see the *CA Common Services* documentation for the CCI component.

Action:

Contact CA Support.

TSS9906I

CPF Node(xxxxxxxx) send request timed out. Retry successful.

Reason:

TSSCPF retried sending a command to remote node xxxxxxxx and the retry process was successful.

Action:

No action is required.

TSS9907I

Remote system rejected a duplicate command sent from this node

Reason:

TSSCPF attempted to recover from a send command time-out condition. The retry process caused the remote system to receive duplicate commands, which the remote system rejected and ignored. This message appears in the journal files of both the sending and receiving systems.

Action:

No action is required.

TSS9908I

Unmatched response received from remote system

Reason:

TSSCPF attempted to recover from a send response time out condition, and the retry process resulted in receiving of duplicate responses from the remote system. The sending system ignores and rejects the duplicate responses. This message appears in the journal file of the system receiving the duplicate response.

Action:

No action required.

TSS9909I

CPF Node(xxxxxxxx) send response timed out. Retry successful.

Reason:

TSSCPF retried sending a command response to the remote node xxxxxxxx, and the retry process was successful. The response is delivered to the remote system.

Action:

No action is required.

TSS9910E

CPF Node(xxxxxxxx) Unable to send response for TRAN#ID: nnnnnnnn

Reason:

TSSCPF was unable to send a command response to remote node xxxxxxxx, and the retry process failed. The response is discarded.

nnnnnnnn

Specifies the command response transaction ID number.

Action:

No action is required.

TSS9911I

CPF Node(xxxxxxxx) send response timed out. Retry started

Reason:

TSSCPF attempted to send a command response to the remote node xxxxxxxx, but the remote system did not acknowledge receiving the transmission. TSSCPF will retry sending the response.

Action:

Other messages that indicate if the retry was successful may be displayed with this message. If no other messages are displayed and you are unable to determine the cause of the failure, contact CA Support.

TSS9912E

CPF Node(xxxxxxxx) send response timed out. Retry failed

Reason:

TSSCPF was unable to send a command response to remote node xxxxxxxx and the retry process failed. Problems may exist between the local and remote systems.

Action:

Look for additional network component messages (VTAM, CCI, or others) to determine the cause of the send failure. If you are still unable to determine the cause of the failure, contact CA Support.

TSS9913I

CPF NODE(*xxxxxxxx*): COMMANDS ARE ROUTED TO CCI NODE(*yyyyyyyy*).

Reason:

The CA Top Secret Command Propagation Facility is sending commands to a generic node (*xxxxxxxx*), and the real receiving system is (*yyyyyyyy*).

Action:

No action is required.

TSS9914I

CPF NODE(*xxxxxxxx*): REMOTE CCI NODE(*yyyyyyyy*) IS UNAVAILABLE.

Reason:

The CA Top Secret Command Propagation Facility is sending commands to a generic node (*xxxxxxxx*), and the real receiving system (*yyyyyyyy*) became unavailable.

Action:

No action is required. CPF attempts to recover and route commands to another active system in the SYSPLEX.

TSS9920I

CPF Journal files Started

Reason:

CPF was notified of JES2 termination and started closing spooled journal data sets.

Action:

No action is required.

TSS9921I

Closing CPF Journal files Completed

Reason:

CPF finished closing spooled journal data sets. The product issues this message with message TSS9920I.

Action:

No action is required.

TSS9922I

Opening CPF Journal files Started

Reason:

CPF was notified that JES2 is active. CPF started opening spooled journal data sets.

Action:

No action is required.

TSS9923I

Opening CPF Journal files Completed

Reason:

CPF finished opening spooled journal data sets. The product issues this message with message TSS9922I.

Action:

No action is required.

TSS9924I

CPF Node(*node_name*) Journal file closed

Reason:

CPF was notified of JES2 termination and closed the spooled journal data sets for the specified CPF node. The product issues this message with message TSS9920I.

Action:

No action is required.

TSS9925I

CPF Inbound Journal file closed

Reason:

CPF was notified of JES2 termination and closed the spooled journal data sets for inbound commands. The product issues this message with message TSS9920I.

Action:

No action is required.

TSS9926I

CPF Node(*node_name*) Journal file opened

Reason:

CPF was notified that JES2 is active. CPF opened the spooled journal data sets for the specified CPF node. The product issues this message with message TSS9922I.

Action:

No action is required.

TSS9927I

CPF Inbound Journal file opened

Reason:

CPF was notified that JES2 is active. CPF opened the spooled journal data sets for inbound commands. The product issues this message with message TSS9922I.

Action:

No action is required.

TSS9951I

Closing LDS Spool files Started

Reason:

The LDAP server task was notified of JES2 termination and started closing spooled SYSOUT data sets.

Action:

No action is required.

TSS9952I

Closing LDS Spool files Completed

Reason:

The LDAP server task finished closing spooled SYSOUT data sets. The product issues this message with message TSS9951I.

Action:

No action is required.

TSS9953I

Opening LDS Spool files Started

Reason:

The LDAP server task was notified that JES2 is active. The task started opening spooled SYSOUT data sets.

Action:

No action is required.

TSS9954I

Restarting Common LDS Subtask

Reason:

The LDAP server task was notified that JES2 is active. The task is restarting the common LDAP API subtask. The product issues this message with message TSS9953I.

Action:

No action is required.

TSS9955I

Opening LDS Spool files Completed

Reason:

The LDAP server task finished opening spooled SYSOUT data sets. The product issues this message with message TSS9953I.

Action:

No action is required.

TSS9993E

STORAGE NOT FREED ©

Reason:

CA Top Secret was unable to FREEMAIN storage which it had allocated.

Action:

Contact CA Technical Support.

TSS9994E

THE FDT IS MISSING. RESTART CA TOP SECRET INFORM SUPPORT.

Reason:

This message can be expected the first time CA Top Secret 5.1 is brought up pointing to a Security File that has not been previously used by a CA Top Secret 5.1 system. This can also occur if CA Top Secret 5.0 and below share a CA Top Secret 5.1 Security File without compatibility fixes.

Action:

If you receive the message after restarting CA Top Secret pointing to the same Security File, contact CA Technical Support.

TSS9995E

Unable to write record - Time Series Facility Not Available

Reason:

Chorus STATG attempted to write CA Top Secret STATG (statistics gathering) to Time Series Facility (TSF), however, the TSF is not available to complete the writing of STATG records. The records are buffered up unitl the TSF is available, when ready those records will be sent to TSF.

Action:

Start up Time Series Facility (TSF).

TSS9996E

Security File contains 2-byte RESCODEs and cannot be used by this release

Reason:

The Security File (which is currently being accessed by a CA Top Secret 5.1 system) had been altered by a CA Top Secret 5.2 system to create an RDT resource class defined with a 2-byte RESCODE. Once this has occurred, the Security File is irrevocably altered, and can no longer be used by CA Top Secret 5.1.

Action:

You must convert this system to CA Top Secret 5.2, or you will have to forward recover a prior TSS 5.1 BACKUP file from a period of time when you are assured that the TSS 5.2 control option RDT2BYTE had not been activated. Contact Support for additional details.

TSS9998I

TSF BUFFER FULL - WRITE TO CHORUS ENDED
NO RECORD SENT TO TSF - BUFFER FULL

Reason:

CA Chorus statistics gathering (STATG) has been collecting CA Top Secret statistics records and attempting to write them to the Time Series Facility (TSF); however, the TSF is not available to receive the records. The buffer that has been holding the records is now full, so processing of TSF STATG records has ended.

Action:

Start the TSF.

TSS9999E

CA Top Secret SECURITY SVC ABEND cccc IN PROGRAM program

TSS9999E

ABENDING JOB=jjjjjjjj ACID=aaaaaaaa FUNCTION=f

Reason:

An error that cannot be corrected occurred when CA Top Secret tried to validate a user's request for access to a resource. The error occurred within the user's address space. Also used for DIAGTRAP dump.

In most cases an SVCDUMP will accompany this message. To obtain more information about the error including abend PSW and Registers, issue the MVS D D,E operator command.

Function=

- C-RACHECK
- I-RACINIT
- L-RACLIST
- D-RACDEF
- F-FASTAUTH

Action:

If a system dump was taken, contact CA Technical Support.

TSSC001E to TSSC105I

TSSC001E

USER DOES NOT HAVE AUTHORITY TO RUN THIS UTILITY

Reason:

The CA Top Secret CIA Unload Utility must be executed by the MSCA. The CA Top Secret CIA Unload Utility terminates.

Action:

Have the MSCA run the CA Top Secret Unload Utility.

TSSC002E

ERROR OPENING INPUT FILE file

Reason:

The CA Top Secret CIA Unload Utility had a problem finding or opening the input file. The CA Top Secret CIA Unload Utility terminates.

Action:

Make sure that the input file was created and that the CA Top Secret CIA Unload Utility procedure JCL contains a DD statement for the input file.

TSSC003E

ERROR OPENING OUTPUT FILE file

Reason:

The CA Top Secret CIA Unload Utility had a problem finding or opening the output file. The CA Top Secret CIA Unload Utility terminates.

Action:

Make sure that the output file was created and that the CA Top Secret CIA Unload Utility procedure JCL contains a DD statement for the output file.

TSSC004E

BAD VALUE FOR INCOMING parameter PARAMETER.

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a invalid parameter. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC005E

GETMAIN FAILURE FOR getmain name (storage add .name).

Reason:

TSSCIALD was unable to acquire sufficient amount of storage.

Action:

None.

TSSC006E

BAD KEYWORD (keyword) FROM INCOMING PARAMETER FILE.

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains an invalid keyword. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC007E

USERFIELD NOT DEFINED TO THE TOP SECRET FDT (field name).

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a User Defined field that is not defined to the FDT. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC008E

DUPLICATE FOR USER DEFINED FIELD (field name).

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a duplicate User Defined field name. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC009E

BAD LENGTH FOR USER DEFINED FIELD ((field name).

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a user-defined field with an invalid length for that type. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC010E

BAD VALUE (value) FOR KEYWORD (keyword).

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a bad value for the keyword. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC011E

UNLOAD PROCESSING TERMINATED

Reason:

The problem is in the processing error message. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error in the processing error message and run the utility again.

TSSC012E

RECORD LENGTH EXCEEDS THE MAXIMUM ALLOWED FOR USER DEFINED FIELDS

Reason:

You specified too many USERFIELD input control statements in the SYSIN input parameter file, which caused the variable record length for the USERUSER line in the UNLOAD process to exceed the maximum variable record length allowed for a line in the UNLOAD data set. The CA Top Secret CIA Unload Utility terminates.

Action:

Reduce the number of USERFIELD control statements in the SYSIN file and run the utility again. Make sure each record field specified in a USERFIELD control statement exists in the actual CA Top Secret FDT table for field definitions. Also, eliminate any duplicate field names in the USERFIELD control statements. There should not be more user-defined fields specified with USERFIELD control statements than actually exist in the FDT.

TSSC025E

INCOMING PARM USERFIELD( ) CANNOT BE USED WITH OTHER USERFIELDS.

Reason:

ALL or *NONE* was selected, but at least one other USERFIELD input control statement exists. If you specify USERFIELD(*NONE*) or USERFIELD(*ALL*), you cannot specify other USERFIELD input control statements.

Action:

Correct your incoming parameters, and run the job again.

Module:

TSSCIAPP

TSSC026I

USERFIELD(*ALL*) WAS SELECTED BY DEFAULT.

Reason:

If you do not specify any USERFIELD control statement in the CIA unload utility SYSIN file, the default value is USERFIELD(*ALL*).

Action:

No action is required.

Module:

TSSCIAPP

TSSC027E

USERFIELD( ) SELECTED TWICE AS AN INCOMING PARAMETERS.

Reason:

USERFIELD(*ALL*) or USERFIELD(*NONE*) was selected twice.

Action:

Remove any duplicate USERFIELD parameters, and run the unload again.

Module:

TSSCIAPP

TSSC028I

GLOBALID FIELD(*ACID*) WAS SELECTED BY DEFAULT.

Reason:

If you do not include a GLOBALID control statement that specifies an ACID field or exit routine to populate the GLOBALID column, the unload utility uses the default GLOBALID FIELD(*ACID*). This default value assigns a global ID value that corresponds to the eight-character ACID that is being processed for the unload.

Action:

No action is required.

Module:

TSSCIAPP

TSSC029E

GLOBALID FIELD( ) ALSO HAS TO BE SELECTED AS A USER FIELD

Reason:

A user-defined field was specified on the GLOBALID control statement; however, one of the following problems exists on the unload utility SYSIN input control statement:

- The list of specified user-defined fields in the USERFIELD statement does not include the field that was specified on the GLOBALID control statement.
- The statement includes USERFIELD(*NONE*), which specifies to omit user-defined field data.

Action:

Specify the same user-defined field in the USERFIELD statement or use USERFIELD(*ALL*), then rerun the job.

Module:

TSSCIAPP

TSSC050W

CFILE WAS NOT RUN BY A MSCA IT MAY BE AN INCOMPLETE FILE.

Reason:

The building of the input cfile for the CA Top Secret CIA Unload Utility was not run by the MSCA this file could possibly not be a full file.

Action:

Only a warning no action needed.

TSSC051W

TSSC051W - BAD RECORD TYPE (type) FOR ACID (acid) TYPE (t).

Reason:

The ACID type (prof,dept.,div….) is not allowed to have this kind of information on it.

Action:

Only a warning no action needed.

TSSC052W

BAD DATE OR DATE FORMAT IN RECORD REC # (record).

Reason:

The date on the record number is an invalid date or does not match the format for the cfile output.

Action:

Only a warning no action needed may want to check the ACID.

TSSC053W

BAD TIME OR TIME FORMAT IN RECORD REC # (record).

Reason:

The time for this record number is an invalid time.

Action:

Only a warning no action needed may want to check the ACID.

TSSC054W

BAD INTEGER VALUE FOR RECORD REC # (record).

Reason:

The integer is not a valid number on this record.

Action:

Only a warning no action needed may want to check the ACID.

TSSC055W

BAD TIME SHIFT RECORD REC # (record).

Reason:

The time shift record is incomplete or has a bad time value on it.

Action:

Only a warning no action needed may want to check the shift record.

TSSC056W

NO RESOURCE OWNERSHIP WAS FOUND FOR THIS PERMIT REC # (record).

Reason:

The Acid the a permit to a resource that is unowned.

Action:

Only a warning no action needed may want to check the Acid and correct the error.

TSSC057W

BAD CALENDAR RECORD REC # (record).

Reason:

The calendar record is incomplete or has a bad month value on it.

Action:

Only a warning no action needed may want to check the calendar record.

TSSC058W

BAD CONTINUATION IN RECORD REC # (record).

Reason:

The proceeding record was marked for continuation and this record is not a correct type of record for this continuation.

Action:

Only a warning no action needed.

TSSC100I

SYSID (sysid) WAS SET FROM (the system or parameter file)

Reason:

Informational message telling where theCA Top Secret CIA Unload Utility is picking up the sysid from.

Action:

No action needed.

TSSC104I

LPAR (*lpar*) was set from *(the system or parameter file*)

Reason:

Indicates the origin of the CA Top Secret CIA Unload Utility default LPAR.

Action:

This message is for informational purposes only. No action is necessary.

TSSC105I

Duplicate LPAR skipped - *lpar*

Reason:

Indicates that a duplicate LPAR parameter was entered and has been ignored.

Action:

This message is for informational purposes only. No action is required.

Chapter 2: Messages for SAF SECTRACE Reporter

The following messages for SAF SECTRACE Reporter differ from the standard CA Top Secret message convention in that they do not contain the message suffix letter by design.

TSS41022 to TSS9C000

TSS41022

INVALID OPERAND VALUE FOR KEYWORD *kkk*

Reason:

The value specified for the operand is invalid. *kkk* is the name of the parameter for which the invalid value was found.

Action:

Correct the parameter and rerun the report.

TSS41024

SYNTAX ERROR IN PARAMETER FIELD

Reason:

The input JCL parameter field contains a syntax error.

Action:

Correct the parameter and rerun the report.

TSS41028

TOO MANY JOBMASKS: 32 IS THE MAXIMUM

Reason:

More than 32 different masks were specified in the JOBMASK parameter. The maximum allowed is 32.

Action:

Correct the parameter and rerun the report.

TSS41029

INSUFFICIENT AUTHORIZATION

Reason:

An unauthorized user attempted to generate a SAF trace report.

Action:

No action required.

TSS41030

UNABLE TO PERFORM AUTHORIZATION

Reason:

CA Top Secret is not active or there is a severe problem with the MVS operating system.

Action:

Contact CA Technical Support.

TSS41069

DUPLICATE KEYWORD - *kkk*

Reason:

The same keyword parameter was specified more than once when running the report. *kkk* is the keyword parameter that was duplicated.

Action:

Remove the duplicate parameter and rerun the report.

TSS4B100

INVALID PARAMETER - *ppp*

Reason:

The CA Top Secret SMF record input processing routine received an invalid parameter. The ddname was missing or the ddname list was invalid. *ppp* is the ddname or a ddname list.

START DATE

The specified start date was invalid.

END DATE

The specified end date was invalid.

START TIME

The specified start time was invalid.

END TIME

The specified end time was invalid.

MINIMUM RECORD LENGTH

The specified minimum record length was larger than the size of the buffer area used by TSS4BSMF.

Action:

Correct the parameter and rerun the report.

TSS4B101

REQUESTED INPUT FILE NOT DEFINED - *ddd*

Reason:

The input SMF records file was not allocated. *ddd* is the name of the file.

Action:

Correct the parameter and run the report again.

TSS4B102

CONTROL BLOCK INITIALIZATION FAILURE - *ccc*

Reason:

TSS4BSMF cannot build the necessary control blocks for input SMF record processing. *ccc* is one of the following values:

ACB - TSS4BSMF

Failure to build an ACB for input processing.

RPL - TSS4BSMF

Failure to build an RPL.

Action:

Contact CA Technical Support.

TSS4B103

CLOSE FAILED FOR FILE *ddd*

Reason:

TSS4BSMF cannot terminate processing of an input file. *ddd* is the name of the file for which processing could not be terminated.

Action:

Contact CA Technical Support.

TSS4B104

INVALID DATE FIELD - X'*ddd*' - RECORD # *nnn* SKIPPED

Reason:

TSS4BSMF found an SMF record with a date field that does not contain a valid packed decimal number. The input record is skipped and processing continues.

ddd

Content of the date field.

nnn

Relative record number of this record.

Action:

None.

TSS4B105

UNANTICIPATED VSAM ERROR, FEEDBACK FIELD - *ccc*

Reason:

TSS4BSMF encountered an I/O error in VSAM record processing. *ccc* is the RPLFDBWD field from the VSAM request parameter list that is used for I/O processing.

Action:

None.

TSS4B106

PHYSICAL ERROR DURING I/O OPERATION

Reason:

TSS4BSMF encountered a physical I/O error during SMF record processing. This message is accompanied by message TSS4B107.

Action:

None.

TSS4B107

sss

Reason:

The text of this message contains the SYNAD analysis of the error. *sss* is the SYNAD text.

Action:

If the input SMF file is sequential, see the IBM OS/VS2 MVS Data Management Macro Instructions for a description of the message text. If the data set is VSAM, see the OS/VS1 Virtual Storage Access Method (VSAM) *Programmer's Guide*.

TSS4B108

OPEN FAILED FOR FILE - *ddd*

Reason:

TSS4BSMF cannot access the specified input SMF file. *ddd* is the ddname for the input SMF file that cannot be processed.

Action:

None.

TSS4B109

VSAM OPEN ERROR - *ccc*

Reason:

TSS4BSMF cannot access a VSAM input file. *ccc* is the ACBERFLG field from the input ACB.

Action:

None.

TSS4B110

NONZERO RETURN CODE FROM QSAM RECORD PROCESSING - *ccc*

Reason:

TSS4BSMF received a nonzero return code from a GET request while using the QSAM access method. *ccc* is the return code.

Action:

None.

TSS4B111

X '*nnn*'

Reason:

The SMF record header was invalid and was listed for debugging assistance. *nnn* is the SMF record header.

Action:

None.

TSS4B112

CONCATENATED SMF INPUTS NOT ALLOWED, FILE - *fff*

Reason:

An SMF input file was concatenated. This is not permitted by the SMF reader routines. *fff* is the ddname of the file containing the concatenated SMF inputs.

Action:

Allocate each SMF file to a separate DD statement and run it again.

TSS4B113

NO SMF RECORD NUMBERS PROVIDED BY CALLER

Reason:

The caller did not provide SMF record numbers, and the CA Top Secret CVT or the CA Top Secret FDR was not available to retrieve the default record numbers.

Action:

None.

TSS4B114

MAXIMUM RECORDS WITH BAD DATE ENCOUNTERED, PROCESSING TERMINATED

Reason:

TSS4BSMF has encountered the maximum of ten input records with invalid date fields. Further processing stops.

Action:

None.

TSS4B115

TOO MANY MASKS *mmm* FOR *ddd*

Reason:

TSS4BSMF received a parameter list containing more than 32 job names or ddname masks. *mmm* is the total number of masks supplied. *ddd* is one of the following values:

DDNAME

A ddname mask is in error.

JOBNAME

A job name mask is in error.

Action:

None.

TSS4B116

START DATE *sss*, GREATER THAN END DATE *eee*

Reason:

The start date supplied by the caller is chronologically later than the ending date.

sss

The start date supplied by the caller.

eee

The end date supplied by the caller.

Action:

None.

TSS9C000

TSS SAF INTERFACE INITIALIZATION FAILED, LOAD FAILED FOR lmod

TSS SAF INTERFACE INITIALIZATION FAILED, LOAD FAILED FOR *lmod*

Reason:

The specified module could not be loaded. lmod is the eight-character load module name.

Action:

Ensure that CA Top Secret has been installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Chapter 3: CAS20 – CAS4 Messages

CAS20 System Authorization Facility (SAF) Messages

CAS2000E

UNDEFINED MESSAGE NUMBER num

Reason:

An attempt was made to print a message with the specified message number, but the message number does not exist. The value of *num* is the specified message number that could not be identified.

Action:

Verify that CA Top Secret was installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Module:

SAFMSGFM

CAS2001E

UNABLE TO ISSUE MESSAGE NUMBER msg FOR UNDEFINED MESSAGE NUMBER num

Reason:

The CA SAF message formatter tried to issue a message not defined in the message table. When it tried to issue the message to report the error, that message was also unavailable. This could occur if your site modified and damaged the message table.

msg

Undefined message.

num

Unavailable error message.

Action:

Contact CA Top Secret Technical Support. Provide any messages issued just before or after you received this message.

Module:

SAFMSGFM

CAS2002E

UNABLE TO ISSUE sub MESSAGE NUMBER num; THE MESSAGE TABLE IS NOT AVAILABLE

Reason:

The CA SAF formatter tried to issue a message not in the message table.

sub

Name of the subsystem whose message table could not be found

num

Message number of the message that could not be issued.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and any messages issued just before or after this message.

Module:

SAFMSGFM

Security Initialization Routine

CAS2030E

CA SAF INTERFACE INITIALIZATION - LOAD FAILED FOR MODULE lmod

Reason:

The specified module could not be loaded. The value of *lmod* is the specified load module name.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Technical Support and provide this message number and diagnostic information.

Module:

SAFRTSEC

CAS2031I

CA SAF INTERFACE INITIALIZATION COMPLETE

Reason:

The CA SAF interface is successfully initialized.

Action:

This message is for information only. No action is required.

Module:

SAFRTSEC

CAS2032E

CA SAF INTERFACE INITIALIZATION FAILED

Reason:

The CA SAF interface initialization failed.

Action:

Contact CA Top Secret Technical Support and provide this message number and diagnostic information.

Module:

SAFRTSEC

CAS2050E

LOAD ERROR FOR SAFTRSFR, INSTALLATION ERROR

Reason:

An error occurred locating SAFTRSFR during SECTRACE initialization.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Module:

SAFTRINT

CAS2051E

LOAD ERROR FOR SAFTRRVT, INSTALLATION ERROR

Reason:

An error occurred locating SAFTRRVT during SECTRACE initialization.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Module:

SAFTRINT

CAS2052E

MISSING SSCT FOR TRCE, INSTALLATION ERROR

Reason:

The TRCE subsystem control vector table (CVT) could not be located.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Module:

SAFTRINT

CAS2053E

TRACE SUBSYSTEM INITIALIZATION FAILED

Reason:

An error occurred during SECTRACE initialization.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Module:

SAFTRINT

CAS2060E

KEYWORD NOT IN PARM TABLE; KWD: key

Reason:

A valid entry in the CAESEC00 member of SYS1.PARMLIB was properly parsed, but could not be found in the parmlib table passed to SAFRTPRM. The value of *key* is the keyword that could not be found. Its value is ACF2, MACS, TRCE, or TSS.

Action:

Contact CA Top Secret Technical Support. Provide the contents of the CAISEC00 parmlib member.

Module:

SAFRTPRM

CAS2061E

PARMLIB OPERAND ERROR FOR KEYWORD: key

Reason:

An entry in the CAISEC00 member of SYS1.PARMLIB could not be parsed because it contained invalid syntax or because it did not specify one of the supported keywords: ACF2, TRCE, MACS, or TSS. The value of *key* is the keyword in error.

Action:

Correct the syntax of the CAISEC00 parmlib member and ensure that it contains only supported keywords.

Module:

SAFRTPRM

CAS2062E

SUFFIX INVALID FOR KEYWORD: suf

Reason:

The first parameter specified for an entry in the CAISEC00 member of SYS1.PARMLIB was not a valid parmlib member suffix. The suffix must be no more than two characters long. The value of *suf* is the invalid parmlib member suffix.

Action:

Specify a suffix with no more than two characters.

Module:

SAFRTPRM

CAS2063E

START OPTION INVALID FOR KEYWORD: key

Reason:

The second parameter specified for an entry in the CAISEC00 member of SYS1.PARMLIB was not a valid start option. The option, if present, must be START or NOSTART. The value of *key* is the keyword with the invalid start option: ACF2, MACS, TRCE, or TSS.

Action:

Specify either START or NOSTART as the start option.

Module:

SAFRTPRM

CAS2064E

member PARMLIB MEMBER NOT FOUND

Reason:

The CAISEC*xx* member of SYS1.PARMLIB was not found during CA SAF initialization. The value of *member* is the member that could not be located.

Action:

Specify a valid CAISEC PARMLIB member suffix, CA SAF initialization parameters, or U to continue processing, to the CAS2071I message that follows.

Module:

SAFRTPRM

CAS2065E

INVALID MEMBER SUFFIX SPECIFIED suf

Reason:

You specified an invalid suffix name on the SEC= initialization keyword. The value of *suf* is the invalid suffix specified on the SEC= keyword.

Action:

Specify the valid CAISEC member suffix to the CAS2071I message that follows.

Module:

SAFRTPRM

CAS2066W

CAISEC PARMLIB MEMBER member ALREADY SELECTED

Reason:

The CAISECxx member of SYS1.PARMLIB was already processed during CA SAF initialization. The value of *member* is the PARMLIB member that was already processed.

Action:

Reply with a valid CAISEC PARMLIB member suffix, CA SAF initialization parameters, or U to continue processing. If you specify U, the CAS2071I message displays.

Module:

SAFRTPRM

CAS2067W

MEMBER STACK FULL, UNABLE TO PROCESS MEMBER member

Reason:

CA SAF maintains a stack of CAISEC members to process. This message is issued if the stack limit is exceeded. The value of *member* is the PARMLIB member that was not processed.

Action:

Reduce the number of SEC= keywords specified during CA SAF initialization.

Module:

SAFRTPRM

CAS2070I

SPECIFY CAISEC START OPTIONS OR REPLY U TO CONTINUE

Reason:

You specified the PROMPT keyword in the CA SAF initialization parmlib member CAISEC00.

Action:

You can reply with one of the following options:

```
TSS(xx)
TSS(xx START)
TSS(xx NOSTART)
```

CA SAF uses an alternate two-character CAISEC*xx* parmlib member that you supply.

```
TRCE(xx)
TRCE(xx START)
TRCE(xx NOSTART)
```

CA SAF uses the CAITRC*xx* parmlib member.

CA SAF uses the CAISEC00 parmlib member that is the default and allows you to continue processing.

For information on SAF SECTRACE, see the *Installation Guide*.

Module:

SAFRTPRM

CAS2071I

RESPECIFY CAISEC START OPTIONS OR REPLY U TO CONTINUE

Reason:

An error occurred when processing CA SAF initialization parameters. A reprompt allows respecification of the CA SAF initialization parameters.

Action:

Reply with valid CA SAF initialization parameters or U to continue processing.

Module:

SAFRTPRM

CAS20801

LANGUAGE ENVIRONMENT INITIALIZED

Reason:

The Language Environment subtask was successfully started.

Action:

None required. This message is for information only.

Module:

SAFRTCEE

CAS2081I

LANGUAGE ENVIRONMENT TERMINATED

Reason:

The Language Environment subtask was successfully shutdown.

Action:

None required. This message is for information only.

Module:

SAFRTCEE.

CAS2082E

LANGUAGE ENVIRONMENT INITIALIZATION FAILED

Reason:

The Language Environment subtask was not be successfully started. The return code is indicated by *rtncode*; the reason code is indicated by *rsncode*.

Action:

None required. This message is for information only.

Module:

SAFRTCEE.

CAS2083E

CEEPIPI ROUTINE COULD NOT BE LOADED, ABEND CODE= *abecode*, REASON CODE = *rsncode*

Reason:

The Language Environment service routine, CEEPIPI, could not be loaded. The ABEND code received is indicated by *abecode;* the reason code is indicated by *rsncode*.

Action:

Contact CA Technical Support.

Module:

SAFRTCEE.

CAS2084E

LANGUAGE ENVIRONMENT TERMINATION FAILED, R15 = rtncode, RO = rsncode

Reason:

An error occurred while shutting down the Language Environment subtask. The return code is indicated by *rtncode*; the reason code is indicated by *rsncode*.

Action:

Contact CA Technical Support.

Module:

SAFRTCEE.

CAS2085E

CEEPIPI CALLMAIN FAILED FOR routine ROUTINE, R15 = r15code, RC = rtncode, RSN = rsncode, FBK = fbkcode

Reason:

An error occurred while calling a CA SAF routine with the CEEPIPI service routine. The code received in register 15 is indicated by *r15code;* the return code is indicated by *rtncode*; the reason code is indicated by *rsncode*; the feedback code is indicated by *fbkcode*.

Action:

Contact CA Technical Support.

Module:

SAFRTCEE.

CAS2090E

DATA SET ALLOCATION/OPEN FAILED

Reason:

The data set specified on the DSNAME keyword for the EXPORT or GENREQ command could not be allocated or opened. There may be an existing data set with the same name, or the data set may be in use.

Action:

Ensure that the data set specified does not already exist, and is not in use. If the problem persists, contact CA Technical Support.

Module:

SAFCROUT.

CAS2091E

ABEND OCCURRED DURING PUT

Reason:

An ABEND occurred while the EXPORT or GENREQ command was writing to the output data set.

Action:

Contact CA Technical Support

Module:

SAFCROUT.

CAS2092E

MEMBER NAME IS NOT ALLOWED

Reason:

A member name was specified on the DSNAME keyword for the EXPORT or GENREQ command. The output file must be a sequential data set.

Action:

Specify a sequential data set, and do not specify a member name.

Module:

SAFCROUT.

CAS20A0E

SAFCRDNB: UNEXPECTED RETURN/REASON CODE FROM SAFAASCN: rtncode/rsncode

Reason:

While processing a GENCERT command, the SAFCRDNB routine received an unexpected return or reason code from the SAFAASCN routine. The return code is indicated by *rtncode;* the reason code is indicated by *rsncode*.

Action:

Contact CA Technical Support.

Module:

SAFCRDNB.

CAS20A1E

INVALID DELIMITER (PARENTHESIS) FOR keyword KEYWORD; YOU MUST USE AN EQUAL SIGN

Reason:

Parentheses were used to delimit a relative distinguished name RDN in the SUBJSDN field of the GENCERT command, for example "L(Lisle)". An equal sign must be used instead, for example "L=Lisle". They keyword in error is indicated by *keyword*.

Action:

Reissue the GENCERT command, specifying the RDN correctly.

Module:

SAFCRDNB.

CAS20A2E

YOU MUST SUPPLY A VALUE FOR THE keyword KEYWORD

Reason:

On the GENCERT command, a value was not specified for a keyword in the SUBJSDN field that requires a value.

Action:

Reissue the GENCERT command, and do not specify a value for the keyword.

Module:

SAFCRDNB.

CAS20A3E

YOU MAY NOT SUPPLY A VALUE FOR THE keyword KEYWORD

Reason:

On the GENCERT command, a value was specified for a keyword in the SUBJSDN field that does not allow a value.

Action:

Reissue the GENCERT command, and specify a value for the keyword.

Module:

SAFCRDNB.

CAS20A4E

THE keyword FIELD CONTAINS AN INVALID CHARACTER, char (hexchar)

Reason:

A relative distinguished name specified in the SUBJSDN field of the GENCERT command contained a character that is not valid for the type of RDN. For example, most RDNs are of the ASN.1 PrintableString type. The following characters are allowed.

- A through Z
- a through z
- 0 through 9
- space
- ’() +, -./:=?

The E, M, and UID RDNs are of the ASN.1 IA5String type. Any ASCII characters are allowed.

In the error message, the invalid character is indicated by *char*, and its hexadecimal representation is indicated by *hexchar.*

This error was detected by SAFAASCN.

Action:

Correct the RDN and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20A5E

QUOTES ARE NOT ALLOWED IN THE keyword FIELD

Reason:

A relative distinguished name (RDN) specified in the SUBJSDN field of the GENCERT command contained a single quote (apostrophe), but the particular RDN does not allow quotes. Quotes are allowed only in the CN, L, O, OU, S/SP/ST, STREET, and T RDNs.

Action:

Correct the RDN and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20A6E

YOUR OPTIONS CONTAIN AN INVALID CHARACTER, char (hexchar), IN POSITION pos

Reason:

The value specified in the SUBJSDN field of the GENCERT command contained an invalid character. The invalid character is indicated by *char;* its hexadecimal value is indicated by *hexchar;* column position in the field is indicated by *pos*.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20A7E

badrdn IS NOT A VALID RDN

Reason:

An unrecognized relative distinguished name (RDN) was specified in the SUBJSDN field of the GENCERT command. Currently recognized RDNs are C, CN, DC, E, L, M, O, OU, PC, S/SP/ST, T, STREET, and UID.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20A8E

VALUE LIST FOR keyword KEYWORD IS NOT CLOSED

Reason:

A value list was specified for a keyword in the SUBJSDN field of the GENCERT command. The value list did not have a closing parenthesis. The keyword in error is indicated by *keyword*.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20A9E

TOO FEW VALUES FOR KEYWORD keyword; THE MINIMUM IS min

Reason:

A value list with too few values was specified for a keyword in the SUBJSDN field of the GENCERT command. The keyword in error is indicated by *keyword*; the minimum number of values allowed is indicated by *min*.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20AAE

OPERAND FOR KEYWORD keyword IS TOO LONG (> maxchar CHARACTERS)

Reason:

The value specified for a relative distinguished name (RDN) in the SUBJSDN field of the GENCERT command was too long. The keyword in error is indicated by *keyword;* the maximum number of characters allowed is indicated by *maxchar*.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20ABE

KEYWORD IN COLUMN col, keyword.... IS TOO LONG (> 8 CHARACTERS)

Reason:

A keyword specified in the SUBJSDN field of the GENCERT command was longer than the maximum of eight characters. The beginning of the keyword in error is indicated by *keyword*.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20ACE

TOO MANY VALUES FOR keyword KEYWORD; THE MAXIMUM IS maxval

Reason:

A value list with too many values was specified for a keyword in the SUBJSDN field of the GENCERT command. The keyword in error is indicated by *keyword*; the maximum number of values allowed is indicated by *maxval*.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20ADE

KEYWORD keyword IS SPECIFIED MULTIPLE TIMES

Reason:

A relative distinguished name (RDN) was specified multiple times in the SUBJSDN field of the GENCERT command, and was not of a type that allows multiple specifications. Only the DC and OU RDNs may be specified multiple times.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20AEE

THE CHARACTER char (hexchar) IS NOT VALID IN THE keyword FIELD

Reason:

A relative distinguished name specified in the SUBJSDN field of the GENCERT command contained a character that is not valid for the type of RDN. For example, most RDNs are of the ASN.1 PrintableString type. The following characters are allowed:

- A through Z
- a through z
- 0 through 9
- space
- ’() +, -./:=?

The E, M, and UID RDNs are of the ASN.1 IA5String type. Any ASCII characters are allowed.

In the error message, the invalid character is indicated by *char*, and its hexadecimal representation is indicated by *hexchar*.

This error was detected by SAFCRDNB.

Action:

Correct the SUBJSDN field and reissue the GENCERT command.

Module:

SAFCRDNB.

CAS20AFE

THE ENCODED DISTINGUISHED NAME IS TOO LONG (> maxbytes BYTES)

Reason:

The value specified for SUBJSDN on the GENCERT command, when encoded into X.509 DER format, exceeded the maximum allowable length, which is given by *maxbytes*:

Action:

Simplify the value specified for SUBJSDN.

Module:

SAFCRDNB.

CAS20B0I

A SECURITY RELATED EVENT HAS BEEN LOGGED

Reason:

A security event was logged to SMF and/or the ATF as a result of an R_auditx call.

Action:

No action required.

Modules:

SAFRT009 and SAFRT00A

CAS20C0E

THE *message* DATE/TIME IS INVALID

Reason:

The date or time specified for the ACTIVE or EXPIRE keyword on the GENCERT command was invalid, either in format or value. *Message* is replaced with one of the following:

- **ACTIVE**—The date or time specified for the ACTIVE keyword on the GENCERT command was invalid, in format or value.
- **EXPIRE**—The date or time specified for the EXPIRE keyword on the GENCERT command was invalid, in format or value.
- **ACTIVE date must be earlier than the EXPIRE date – the EXPIRE**—The EXPIRE date/time specified was not later than the ACTIVE date/time specified and is invalid.

Action:

Correct the date in error and re-issue the GENCERT command.

Module:

SAFCRGCT

CAS20C1E

Invalid data in PKCS #10 request – RSN - *rsn*

Reason:

The data set contains a PKCS #10 request that does not meet the requirements for a PKCS #10 certificate request. The reason code specified by rsn will indicate to CA Top Secret Technical Support where the invalid data is occurring.

Reason Codes:

- 0—Function was successful
- 4—Certificate length error or no certificate address supplied
- 8—PEM translation error
- 12—Error parsing certificate
- 16—Invalid cert version number
- 20—Output field was truncated
- 24—Routine could not be found
- 28—Signature check failed

Action:

Contact CA Top Secret Technical Support.

Module:

SAFCRGCT

CAS20C2E

Unable to verify signature on PKCS #10 request

Reason:

The PKCS #10 certificate request in the input data set does not have a valid signature. The certificate request may have been altered

Action:

If the certificate request has been altered, obtain an unaltered copy and retry the request.

Module:

SAFCRGCT

CAS21 SECTRACE Routine

CAS2100I

CONTINUE SECTRACE SPECIFICATION, CANCEL, OR END

Reason:

This message prompts the operator to continue SECTRACE operand specifications.

Action:

Reply END to complete or CANCEL to terminate SECTRACE specifications. For an explanation of the valid SECTRACE operands and values, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRTCP

CAS2101E

SECTRACE REQUEST INVALID

Reason:

The requested SECTRACE function is invalid.

Action:

Reenter the SECTRACE command with a valid function and operands. For an explanation of the valid SECTRACE functions, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRTCP

CAS2102W

SECTRACE REQUEST INACTIVE

Reason:

The requested SECTRACE function is not available.

Action:

Verify that CA Top Secret is installed correctly. If so, contact CA Technical Support for assistance.

Module:

SAFTRTCP

CAS2103E

ADDRESS SPACE CREATE FAILED FOR SECTRACE, RC: retcode, RSN: rsncode

Reason:

A SECTRACE command was entered and the SECTRACE address space was not active. SECTRACE attempted to start it using the OS/390 ASCRE facility, but the attempt failed.

retcode

Return code from the ASCRE facility

rsncode

Reason code from the ASCRE facility

The return and reason codes are documented in the *IBM MVS Authorized Assembler Services Reference* guide.

Action:

Contact CA Technical Support.

Module:

SAFTRCMD

CAS2104E

SECTRACE COMMAND INACTIVE

Reason:

A SECTRACE command was entered. SECTRACE could not find the Subsystem Dependent Section (CASAFSDA) for the TRCE subsystem or the Trace Contents Vector Table (CASTRCVT). The command was rejected.

Action:

Contact CA Technical Support.

Module:

SAFTRCMD

CAS2105E

SECTRACE OPERAND ERROR FOR KEYWORD: key

Reason:

You specified an invalid keyword, operator, or value for a SECTRACE operand. The value of *key* is the keyword in error.

Action:

Correct the SECTRACE operand and continue the command specification. For a description of the SECTRACE operands and associated syntax, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRTCP, SAFTRSET, SAFTRENA, SAFTRDIS, SAFTRDEL, SAFTRDSP

CAS2106E

RSN: rsn

Reason:

You specified an invalid keyword, operator, or value for a SECTRACE operand. This message describes the reason (*rsn*) associated with the error.

Action:

See the accompanying message CAS2105E to identify the keyword in error. Correct the SECTRACE operand and continue the command specifications. For a description of the SECTRACE operands and associated syntax, see Appendix B of the *Troubleshooting Guide.*

Module:

SAFTRTCP, SAFTRSET, SAFTRENA, SAFTRDIS, SAFTRDEL, SAFTRDSP

CAS2107E

SECTRACE SECURITY AUTHORIZATION FAILED

Reason:

You issued a SECTRACE command for a resource but are not authorized to do so. The message containing the resource name and type you specified in the SECTRACE command, precedes this message.

Action:

Contact your local security administrator and provide the text of the message that preceded this one.

Module:

SAFTRTCP

CAS2108I

SECTRACE ADDRESS SPACE HAS TERMINATED

Reason:

The SECTRACE address space terminated, but restarts when another SECTRACE command is issued.

Action:

This message is for information only. No action is required.

Module:

SAFTRCMD

CAS2110I

SECTRACE SET ON yy.ddd hh:mm:ss ID=traceid

Reason:

This message indicates the date and time that a new trap was set. This message is deleted when the SECTRACE is removed. The value of *traceid* is the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRSET

CAS2111I

SECTRACE MODIFIED ON yy.ddd hh:mm:ss ID=traceid

Reason:

This message indicates the date and time that a new trap was modified. This message is deleted when the SECTRACE is removed. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRSET

CAS2112I

SECTRACE SET/MODIFY REQUEST CANCELLED

Reason:

A request canceled the SECTRACE SET or MODIFY command.

Action:

This message is for information only. No action is required.

Module:

SAFTRSET

CAS2113E

DUPLICATE KEYWORD SPECIFIED, KWD: key

Reason:

The keyword was previously specified. CA Top Secret ignores duplicate specifications of the keyword. The value of *key* is the duplicate keyword.

Action:

Specify the remainder of the SECTRACE operands again.

Module:

SAFTRSET

CAS2114E

SECTRACE ID=traceid ALREADY EXISTS

Reason:

You specified the trace ID on a previous SECTRACE SET command. The value of *traceid* is the name of the specified trace ID.

Action:

Either specify a trace ID that is not already specified or allow a default trace ID to be assigned. Reenter the subsequent SECTRACE operands.

Module:

SAFTRSET

CAS2115E

SECTRACE ID=traceid NOT FOUND

Reason:

You issued a SECTRACE MODIFY request for a trace ID that was not previously set. The value of *traceid* is the specified trace ID.

Action:

Enter the correct trace ID and reenter the SECTRACE operands.

Module:

SAFTRSET

CAS2116E

INVALID NUMERIC VALUE, KWD: key

Reason:

The value you supplied for the specified keyword is an invalid numeric value or out of range. The value of *key* is the name of the keyword in error.

Action:

Correct the keyword value and reenter SECTRACE operands. For an explanation of the valid values for the specified keyword, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRSET

CAS2117E

INVALID HEX VALUE, KWD: key

Reason:

The value supplied for the specified keyword is an invalid hexadecimal value or out of range. The value of *key* is the name of the keyword in error.

Action:

Correct the keyword value and reenter SECTRACE operands. For an explanation of the valid values for the specified keyword, see Appendix B of the *Troubleshooting Guide.*

Module:

SAFTRSET

CAS2118E

INVALID MASK VALUE, KWD: key

Reason:

You supplied an invalid mask string value for the specified keyword. The value of *key* is the name of the keyword in error.

Action:

Correct the keyword value and reenter the SECTRACE operands. For an explanation of the valid values for the specified keyword, see Appendix B of the *Troubleshooting Guide.*

Module:

SAFTRSET

CAS2119E

INVALID DESTINATION VALUE SPECIFIED

Reason:

You specified an invalid value for the SECTRACE output destination.

Action:

Correct the output destination value and reenter the SECTRACE operands. For an explanation of the valid values for this keyword, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRSET

CAS2120E

INVALID TRACE VALUE SPECIFIED

Reason:

You specified an invalid value for the SECTRACE TRACE environments. For an explanation of the valid values for this keyword, see Appendix B of the *Troubleshooting Guide*.

Action:

Correct the SECTRACE TRACE keyword value and reenter the SECTRACE operands.

Module:

SAFTRSET

CAS2121E

INVALID TYPE VALUE SPECIFIED

Reason:

The value specified for the SECTRACE event type is invalid.

Action:

Correct the SECTRACE event type and reenter the SECTRACE operands. For an explanation of the valid values for this keyword, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRSET

CAS2122E

KEYWORD key SKIPPED, ID VALUE REQUIRED

Reason:

CA Top Secret ignored the specified keyword for the SECTRACE MODIFY command because you did not specify the required trace ID. The value of *key* is the keyword that was ignored.

Action:

Specify the trace ID to modify; reenter the SECTRACE operands.

Module:

SAFTRSET

CAS2123E

INVALID TRACE FORMAT OPTION SPECIFIED

Reason:

You specified an invalid value for the SECTRACE output format options.

Action:

Correct the output format options and reenter the SECTRACE operands. For an explanation of the valid values for this keyword, see Appendix B of the *Troubleshooting Guide.*

Module:

SAFTRSET

CAS2124E

INVALID ACTION OPTION SPECIFIED

Reason:

You specified an invalid value for the SECTRACE action.

Action:

Correct the SECTRACE ACTION value and reenter the SECTRACE operands. For an explanation of the valid values for this keyword, see Appendix B of the *Troubleshooting Guide*.

Module:

SAFTRSET

CAS2125E

SECTRACE ID VALUE IS A RESERVED NAME

Reason:

The value specified for a SECTRACE ID is a reserved name. You cannot use it for a trace ID.

Action:

Specify the trace ID to set again or allow a default trace ID to generate.

Module:

SAFTRSET

CAS2126E

BAD RETURN CODE FROM 'TBS/SMF' WRITE

Reason:

An error occurred while attempting to write the RACROUTE parameter list data structure to SMF.

Action:

Contact CA Top Secret Technical Support and provide the message number and diagnostic information.

Module:

SAFTRSET

CAS2127E

DATA SET NAME FOUND ON ACTIVE SECTRACE DSN: dsn

Reason:

A SECTRACE was directed to a data set that was already in use by another SECTRACE. The new SECTRACE was disabled.

Action:

Choose another data set or disable the SECTRACE that is currently using the data set.

Module:

SAFTRENA, SAFTRSET

CAS2128W

SECTRACE ID=xxxxxxxx - DATA SET NAME MISSING FROM DATA SET TRACE - SECTRACE DISABLED

Reason:

DEST=DATASET was specified on the SECTRACE command and the trace does not contain a value for the DSName= operand.

Action:

Specify DSName=dsn on a SECTRACE MODIFY command for the given SECTRACE and enable the trace.

Module:

SAFTRSET

CAS2129E

SECTRACE ID=xxxxxxxx - ATTACH OF DATA SET REQUEST TASK FAILED - SECTRACE DISABLED

Reason:

An error occurred attempting to attach the data set processing task for a SECTRACE output to data set request.

Action:

Contact CA Top Secret Technical Support for assistance.

Module:

SAFTRCNA, SAFTRSET

CAS2130I

SECTRACE ID=traceid ENABLED

Reason:

The specified trace ID is enabled. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRENA

CAS2131I

SECTRACE REQUEST(S) ENABLED

Reason:

The requested trace IDs are enabled.

Action:

This message is for information only. No action is required.

Module:

SAFTRENA

CAS2132I

SECTRACE ENABLE REQUEST CANCELLED

Reason:

The request to enable the trace IDs was canceled.

Action:

This message is for information only. No action is required.

Module:

SAFTRENA

CAS2133W

SECTRACE ID=traceid NOT FOUND

Reason:

The specified trace ID could not be found. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRENA

CAS2140I

SECTRACE ID=traceid DISABLED

Reason:

The specified trace ID was disabled. The value of *traceid* is the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRDIS

CAS2141I

SECTRACE REQUEST(S) DISABLED

Reason:

The requested trace IDs are disabled.

Action:

This message is for information only. No action is required.

Module:

SAFTRDIS

CAS2142I

SECTRACE DISABLE REQUEST CANCELLED

Reason:

The request to disable the trace IDs was canceled.

Action:

This message is for information only. No action is required.

Module:

SAFTRDIS

CAS2143W

SECTRACE ID=traceid NOT FOUND

Reason:

The specified trace ID could not be found. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRDIS

CAS2150I

SECTRACE ID=traceid DELETED

Reason:

The specified trace ID is deleted. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRDEL

CAS2151I

SECTRACE REQUEST(S) DELETED

Reason:

The requested trace ID is deleted.

Action:

This message is for information only. No action is required.

Module:

SAFTRDEL

CAS2152I

SECTRACE DELETE REQUEST CANCELLED

Reason:

The request to delete the trace ID was canceled.

Action:

This message is for information only. No action is required.

Module:

SAFTRDEL

CAS2153W

SECTRACE ID=traceid NOT FOUND

Reason:

The specified trace ID could not be found. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRDEL

CAS2160I

SECTRACE DISPLAY ID: traceid DATE: yy.ddd TIME hh:mm:ss

Reason:

This message is issued in response to the SECTRACE DISPLAY command. It indicates the date and time that the specified trace was displayed.

traceid

The eight-character name of the trace ID.

yy.ddd

The date when the SECTRACE DISPLAY command was entered.

hh:mm:ss

The time when the SECTRACE DISPLAY command was entered.

Action:

This message is for information only. No action is required.

Module:

SAFTRDSP

CAS2161W

NO SECTRACE DEFINED FOR ID=traceid

Reason:

The specified trace ID could not be found. The value of *traceid* is the name of the specified trace ID.

Action:

This message is for information only. No action is required.

Module:

SAFTRDSP

CAS2162I

NO SECTRACE CURRENTLY DEFINED

Reason:

You requested a SECTRACE display, but no SECTRACE traps are currently defined.

Action:

This message is for information only. No action is required.

Module:

SAFTRDSP

CAS2163I

SECTRACE REQUEST CANCELLED

Reason:

The SECTRACE DISPLAY command was canceled.

Action:

This message is for information only. No action is required.

Module:

SAFTRDSP

CAS2164E

IMPROPER DUPLICATION OF OPERAND: key

Reason:

You specified a duplicate keyword on the SECTRACE DISPLAY command. The value of *key* is the duplicate keyword.

Action:

Correct the command syntax and issue the SECTRACE display command again.

Module:

SAFTRDSP

CAS2165E

NO ID SPECIFIED FOR SECTRACE DISPLAY

Reason:

You entered a SECTRACE DISPLAY command without the ID= keyword. SECTRACE cannot identify which SECTRACE to display, so the command is ignored.

Action:

Enter the SECTRACE DISPLAY command again with the ID= keyword.

Module:

SAFTRDSP

CAS2170E

SECTRACE DISABLED: DATASET ALLOCATE/OPEN FAILED

Reason:

An error occurred attempting to allocate and open the data set specified for a SECTRACE-OUTPUT-TO-DATA-SET request.

Action:

Check the spelling of the data set name entered in the SECTRACE command. Ensure that the data set is catalogued and available. Also check the access rules governing the data set and access permissions of the logonid assigned to the SECTRACE. Correct the problem and enable the trace. If problems persist, contact CA Top Secret Technical Support.

Module:

SAFTRDSN

CAS2171E

SECTRACE INVALID DATASET REQUEST TYPE

Reason:

An internal error occurred attempting to process a SECTRACE-OUTPUT TO-DATASET request.

Action:

Contact CA Top Secret Technical Support for assistance.

Module:

SAFTRDSN

CAS2172E

SECTRACE DISABLED: ABEND OCCURRED DURING PUT

Reason:

SECTRACE encountered an ABEND while writing a record to a data set. The SECTRACE was disabled. OS/390 messages accompanying this message indicate the cause of the ABEND. Typically, they will be IEC0301 or IEC0321 messages, indicating that the trace data set ran out of space.

Action:

If the trace data set ran out of space, delete it and allocate a larger data set, then re-enable the trace. If the OS/390 messages indicate some other sort of ABEND, contact CA Top Secret Technical Support for assistance.

Module:

SAFTRDSN

CAS2180I

SECTRACE ERROR LOGGING ACTIVE

Reason:

SECTRACE error logging was turned on as a result of a SECTRACE LOGERR command. This message acknowledges the command.

Action:

This message is for information only. No action is required.

Module:

SAFTRERR

CAS2181I

SECTRACE ERROR LOGGING INACTIVE

Reason:

SECTRACE error logging was turned off as a result of a SECTRACE NOLOGERR command. This message acknowledges the command.

Action:

This message is for information only. No action is required.

Module:

SAFTRERR

CAS21A0I

SPECIFY RACROUTE PARAMETERS, CANCEL, OR END

Reason:

You specified a SECTRACE TYPE=SAFP request.

Action:

Enter the RACROUTE parameters to further filter the trace criteria. Reply END to complete RACROUTE specifications or CANCEL to cancel RACROUTE specifications. For a detailed description of the RACROUTE parameters, see the IBM publication *OS/390 Security Server External* Security *Interface (RACROUTE) Macro Reference* (No. GC28-1922).

Module:

SAFTRRAC

CAS21A1I

CONTINUE SAF RACROUTE SPECIFICATIONS, CANCEL OR END

Reason:

You specified the SECTRACE TYPE=SAFP request.

Action:

Continue entering the RACROUTE parameters to further filter the trace criteria. Reply END to complete RACROUTE specifications or CANCEL to cancel RACROUTE specifications. For a detailed description of the RACROUTE parameters, see the IBM publication *OS/390 Security Server External Security Interface (RACROUTE) Macro Reference* (GC28-1922).

Module:

SAFTRRAC

CAS21A2E

RACROUTE ERROR, OPERAND: operand

Reason:

You specified an invalid keyword, operator, or value for a RACROUTE parameter. The value of *operand* is the invalid RACROUTE parameter. Message CAS21A3E accompanies this message.

Action:

For a description of the error, see the accompanying message CAS21A3E. Correct the keyword, operator, or value specified for the RACROUTE parameter.

Module:

SAFTRRAC

CAS21A3E

RSN: rsn

Reason:

You specified an invalid keyword, operator, or value for a RACROUTE parameter. This message accompanies message CAS21A2E and describes the reason for the error. The value of *rsn* appears as one of the reasons described below:

- **RELATIONAL OPERATOR MISSING OR INVALID—**The relational operator is missing or is not a valid operator constant.
- **SYNTAX** - **POINTER USED WITH VALUE**—A keyword with a pointer relational operator may not specify a value.
- **OPERATOR CONFLICTS WITH DATATYPE**—The relational operator is not valid for the data type associated with the specified keyword.
- **KEYWORD MISSING OR INVALID**—The keyword associated with the RACROUTE parameter is missing or is not valid.
- **KEYWORD USED OUT OF CONTEXT**—The keyword was not used properly for the RACROUTE specification.
- **UNKNOWN OPTION**—The operand value is not valid for the specified keyword with fixed values.
- **DUPLICATE OPERAND—**The keyword for the RACROUTE specification is specified more than once.
- **CONFLICTS WITH OTHER OPERANDS**—The keyword may not be specified because it conflicts with a previously specified parameter.
- **VALUE DOES NOT AGREE WITH DATA TYPE**—The specified value is not valid for the specified data type.
- **CANNOT ACCEPT STRUCTURED DATA**—The data type for the specified keyword is a data structure that cannot be specified by the RACROUTE specifications.
- **VALUE TOO LARGE FOR DATA TYPE**—The specified value is greater than allowed for the keyword data type.
- **INVALID VALUE LENGTH**—The specified value is not in the correct length range allowed for the keyword.
- **INVALID VALUE MASK**—The specified value mask is invalid for the keyword.
- **SYNTAX** - **VALUE OMITTED**—A syntax error check occurred because of missing value.
- **RELEASE NOT COMPATIBLE WITH REQUEST**—The RACROUTE parameter is not valid for the release of the RACROUTE specification generated. The release level may have been specified or automatically committed due to release-dependent parameters.

- **INVALID RELEASE ID SPECIFIED**—The specified release number is invalid for the RACROUTE specification.

Action:

To identify the keyword in error, see message CAS21A2E. Correct the keyword, operator, and value specified for the RACROUTE parameter.

Module:

SAFTRRAC

CAS21A4E

RACROUTE PLIST BUILD INITIALIZATION ERROR

Reason:

A severe error occurred during initialization of the parameter list build facility. This facility is invoked when SECTRACE TYPE=SAFP is requested.

Action:

Give CA Technical Support message number, diagnostic information.

Module:

SAFTRRAC

CAS21A5E

RACROUTE PLIST BUILD TERMINATION ERROR

Reason:

A severe error occurred during termination of the parameter list build facility. This facility is invoked when SECTRACE TYPE=SAFP is requested.

Action:

Give CA Technical Support message number, diagnostic information.

Module:

SAFTRRAC

CAS21A6E

RACROUTE PLIST BUILD OPERAND ERROR

Reason:

A severe error occurred during operand processing of the parameter list build facility. This facility is invoked when SECTRACE TYPE=SAFP is requested.

Action:

Give CA Technical Support message number, diagnostic information.

Module:

SAFTRRAC

CAS21A7E

ERROR PROCESSING OPERATOR COMMUNICATIONS

Reason:

An error occurred while attempting to prompt the operator for RACROUTE specifications.

Action:

Give CA Technical Support message number, diagnostic information.

Module:

SAFTRRAC

CAS21A8E

RACROUTE PLIST SCAN ERROR

Reason:

An error occurred while attempting to parse the RACROUTE parameter list the RACROUTE specifications created.

Action:

Give CA Technical Support message number, diagnostic information.

Module:

SAFTRRAC

CAS21A9W

WARNING: VALUE IGNORED FOR DATA SUPPRESSION, OPND: operand

Reason:

The RACROUTE operand specified (*operand*) contains sensitive security information so is suppressed/bypassed for SECTRACE SAF request filtering.

Action:

This message is for information only. No action is required.

Module:

SAFTRRAC

CAS21B0E

ERROR ENCOUNTERED IN SAF PARAMETER LIST

Reason:

CA SAF could not parse SAF parameter list. Is parameter list valid?

Action:

Contact your local systems programmer and provide any messages issued just before or after this one, plus the command or program that was running when the message occurred.

Module:

SAFTR003

CAS21D0I

TRACEID: traceid JOBNAME: jobname ASID: asid USERID: userid

Reason:

This is the SAF event trace header line for CONSOLE, JOBLOG, SYSLOG, and TSO user output destinations.

traceid

The trace ID requesting the trace.

jobname

*T*he job name issuing the SAF event.

asid

*T*he ASID of the job issuing the SAF event.

userid

*T*he user ID issuing the SAF event.

Action:

This message is for information only. No action is required.

Module:

SAFTR002

CAS21D1I

PROGRAM: ppppppp RB CURR: rrrrrrrr APF: aaaa SFR/RFR: rc/rc/rs

Reason:

This is the SAF event trace header line for CONSOLE, JOBLOG, SYSLOG, and TSO user output destinations.

ppppppp

The newest PRB program name issuing the SAF request.

rrrrrrrr

*T*he current RB program name or SVC name issuing the SAF request.

aaaa

Indicates whether the SAF request is APF-authorized.

rc/rc/rs

*S*pecifies the SAF return code, request-specific return code, and request-specific reason codes respectively. N/A appears for pre-SAF processing trace events.

Action:

This message is for information only. No action is required.

Module:

SAFTR002

CAS21D2I

num TRACE EVENTS NOT REPORTED

Reason:

This message indicates the count of trace events not presented to the specified trace output destination. For a description of the SECTRACE destinations where trace events can be blocked, see Appendix B of the *Troubleshooting Guide*.

Action:

This message is for information only. No action is required.

Module:

SAFTR002

CAS21D3I

SAFDEF: safdefid ttttttt MODE: mmmmmmmmmmm

Reason:

This is the SAF event trace header line for SAFDEF information.

safdefid

The ID of the SAFDEF that was used to process this request.

ttttttt

The type of safdef, INTERNAL or GSO.

mmmmmmmm

The mode specified in this SAFDEF. Valid modes are: IGNORE, GLOBAL, GLOBAL/LOG and GLOBAL/QUIET.

Action:

This message is for information only. No action is required.

Module:

SAFTR002

CAS21D5I

SECTRACE DISABLED FOR MATCHLIM ID=traceid

Reason:

The specified trace was automatically disabled because the event counter reached the specified MATCHLIM value. *traceid* is the specified trace ID.

Action:

Issue the SECTRACE ENABLE command to re-enable the trace.

Module:

SAFTR002

CAS21D6I

TRACE OUTPUT CANNOT BE FORMATTED DUE TO INSUFFIEICNT LINE LENGTH

Reason:

The output from a SECTRACE could not display because the line length specified by the LINELEN= keyword on the SECTRACE SET or SECTRACE MOD request was too short to hold the information.

Action:

Enter a SECTRACE MOD,LINELEN=xx command to set the line length to a larger value.

Module:

SAFTR002

CAS21E0W

WARNING TRACE EVENTS NOT PRESENTED: nnn

Reason:

The specified number of trace events that occurred and that were not delivered to the TSO user. Trace events cannot be delivered to a TSO user destination if there is a TPUT buffer shortage. The value of *nnn* is the number of trace events not delivered. For an explanation of the TSOUSER SECTRACE output destination, see Appendix B of the *Troubleshooting Guide*.

Action:

This message is for information only. No action is required.

Module:

SAFTRTSO

CAS21E1W

SECTRACE TSO USER NOT RECEIVING: userid

Reason:

The TSO user (*userid*) specified on the SECTRACE output destination is currently not logged on and cannot receive trace output events.

Action:

This message is for information only. No action is required.

Module:

SAFTRTSO

CAS22 SAF Common Service Routines

CAS2200I

text

Reason:

The value of *text* is a line of output from a SECTRACE. The contents of the line depend on the RACROUTE call displayed.

Action:

This message is for information only. No action is required.

Module:

SAFAAMAC

CAS2201E

text

Reason:

The value of *text* is a line of output from a SECTRACE. The SECTRACE issued encountered unknown data in a RACROUTE parameter, such as an undefined flag bit that was set. It can indicate an invalid RACROUTE call or a downlevel version of SECTRACE. The contents of the line depend on the RACROUTE call displayed.

Action:

This message is for information only. No action is required.

Module:

SAFAAMAC

CAS2202W

text

Reason:

The value of *text* is a line of output from a SECTRACE command. This message is issued when SECTRACE encounters data in a RACROUTE parameter that is too long to display on a single line. The contents of the line depend on the RACROUTE call displayed.

Action:

This message is for information only. No action is required.

Module:

SAFAAMAC

CAS2203I

title

Reason:

This message is issued by SECTRACE to display the title of a data area from a RACROUTE parameter list. The value of *title* is the title of the data area.

Action:

This message is for information only. No action is required.

Module:

SAFAAMAC

CAS2204I

data

Reason:

This message is issued by SECTRACE to display a line of data from a data area from a RACROUTE parameter list. The value of *data* is the line of data displayed.

Action:

This message is for information only. No action is required.

Module:

SAFAAMAC

CAS2205I

REQUEST=function, EXIT=eeee, RC= rc/rc:rs

Reason:

This is the OMVS SECTRACE header line for function and return codes.

Function

The OMVS callable service that is being requested.

eeee

Indicates whether this is pre-SAF processing or post-SAF.

rc/rc:rs

Specifies the SAF return code, request-specific return code, and request-specific reason codes respectively. N/A appears for pre-SAF processing trace events.

Action:

This message is for information only. No action is required.

Module:

SAFOETRC

CAS2206I

text

Reason:

The value of text is a line of output from an OMVS SECTRACE. The contents of the line depends on the function displayed.

Action:

This message is for information only. No action is required.

Module:

SAFOETRC

CAS2220E

***** PBLOCK DEFINITION IN ERROR *****

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide any messages that occurred just before or after this one.

Module:

SAFAATST

CAS2221E

***** PBLOCK OPERANDS IN ERROR *****

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide any messages that occurred just before or after this one.

Module:

SAFAATST

CAS2225E

RET: rrr RSN: sss PLF-ID: ppp OPDEF-ID: ooo

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide this message and any messages that occurred just before or after this one.

Module:

SAFAATST

CAS2226E

ASMNAME: aaa OPERAND: ooo POS: ppp

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide this message and any messages that occurred just before or after this one.

Module:

SAFAATST

CAS2227E

DATAPTR: ppp DATALEN: lll VALFLAGS: fff

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide this message and any messages that occurred just before or after this one.

Module:

SAFAATST

CAS2228E

text

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide this message and any other messages that occurred just before or after this one.

Module:

SAFAATST

CAS2230W

***** UNDEFINED DATA IN SOURCE PLIST *****

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide any messages received just before or after this one.

Module:

SAFAATST

CAS2235W

OFFSET: ooo LENGTH: lll NAME: nnn

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide this message and any other messages that occurred just before or after this one.

Module:

SAFAATST

CAS2236W

DATA: ddd

Reason:

There was an internal error in parsing a RACROUTE call.

Action:

Contact CA Technical Support. Provide any messages received just before or after this one.

Module:

SAFAATST

CAS2240W

SAF EXIT exit NOT IN LPA - IGNORED

Reason:

The specified SAFDEF exit could not be located in the OS/390 link pack area (LPA). The exit definition is ignored and processing continues. The value of *exit* is the exit name that cannot be located.

Action:

Place the defined SAFDEF exit in an LPA list and re-IPL with CLPA.

Module:

SAFAASDB

CAS2241E

SAF PLIST SCAN FAILED FOR BLOCK blk, RC=rc RSN=rsn

Reason:

An error occurred while trying to parse the RACROUTE parameter list the RACROUTE specifications in the SAFDEF record created.

Action:

Contact CA Technical Support and provide this message number and diagnostic information.

Module:

SAFAASDB

CAS2242E

INVALID RACROUTE REQUEST TYPE SPECIFIED, TYPE=type

Reason:

The RACROUTE REQUEST= parameter specifies a value unknown to the CA Top Secret RACROUTE parameter list data structure.

Action:

Contact CA Technical Support and provide this message number and diagnostic information.

Module:

SAFAASDB

CAS2243E

PLIST BUILD ERROR, REQUEST: parm FIELD: fld RC: rc RSN: rsn

Reason:

A severe error occurred while processing the SAFDEF RACROUTE parameters in the SAFDEF record.

parm

specifies the parameter list build request:

- 00—Initialization request
- 04—Process operand request
- 08—Termination request

fld

The keyword field in error. N/A indicates that the parameter is not applicable for the specified call.

rc

specifies the return code from the RACROUTE parameter list build service.

rsn

specifies the reason code from the RACROUTE parameter list build service.

Action:

Contact CA Technical Support and provide the message number and diagnostic information.

Module:

SAFAASDB

CAS2244E

PLIST BUILD ERROR, FIELD: fld RSN: rsn

Reason:

An error occurred while processing the SAFDEF RACROUTE parameter specifications.

fld

The keyword field in error.

rsn

The reason that the SAFDEF RACROUTE operand is in error. It appears as one of the reasons listed below:

- **RELATIONAL OPERATOR MISSING OR INVALID**—The relational operator is missing or is not a valid operator constant.
- **SYNTAX** - **POINTER USED WITH VALUE** —A keyword with a pointer relational operator cannot specify a value.
- **OPERATOR CONFLICTS WITH DATATYPE**—The relational operator is not valid for the data type associated with the specified keyword.
- **KEYWORD MISSING OR INVALID**—The keyword associated with the RACROUTE parameter is missing or invalid.
- **WORD USED OUT OF CONTEXT**—The keyword is not used properly for RACROUTE specification.
- **UNKNOWN OPTION**—The operand value is not valid for the specified keyword with fixed values.
- **DUPLICATE OPERAND**—The keyword was specified more than once for RACROUTE specification.
- **CONFLICTS WITH OTHER OPERANDS**—The keyword may not be specified because it conflicts with an operand previously specified.
- **VALUE DOES NOT AGREE WITH DATA TYPE**—The value is not valid for the specified data type.
- **CANNOT ACCEPT STRUCTURED DATA**—The data type for the specified keyword is a data structure that cannot be specified by the RACROUTE specifications.
- **VALUE TOO LARGE FOR DATA TYPE**—The specified value is greater than allowed for the keyword data type.
- **INVALID VALUE LENGTH**—The specified value is out of the range allowed for the keyword.
- **INVALID VALUE MASK**—The mask specified on the value is invalid for the keyword.
- **SYNTAX** - **VALUE OMITTED**—A syntax error check occurred because of a missing value.

- **RELEASE NOT COMPATIBLE WITH REQUEST**—The RACROUTE parameter is not valid for the release of the RACROUTE specification being generated. The release level may have been specified or automatically committed due to release-dependent parameters.
- **INVALID RELEASE ID SPECIFIED**—The specified release number is invalid for the RACROUTE specification.

Action:

Correct the SAFDEF RACROUTE parameter in error.

Module:

SAFAASDB

CAS2250E

THE LENGTH OF EACH FMID CAN NOT BE MORE THAN 7 BYTES (SMP/E STANDARD)

Reason:

The length of a FMID specified on a ++OLDZONE or ++NEWZONE statement was greater than seven.

Action:

Ensure that all specified FMIDs are no greater than 7 bytes long.

Module:

SAFTAXRF

CAS2251E

NO VALID FMID(S) COLLECTED FROM ++xxxZONE STATEMENT(S)

Reason:

No valid FMID(s) were found on the ++NEWZONE or ++OLDZONE statements. xxx is OLD or NEW.

Action:

Ensure that valid FMIDs are specified and the ++xxxZONE statement begins in column 1.

Module:

SAFTAXRF

CAS2252E

A TARGET ZONE WAS NOT SPECIFIED FOR xxxCSI ON THE SET BDY STATEMENT

Reason:

The zone specified on the SET BDY statement does not exist or is not a TARGET zone for the specified CSI. xxx is OLD or NEW.

Action:

Ensure that the correct TARGET zone is specified in the SAFTAXJC job.

Module:

SAFTAXRF

CAS2253E

CANNOT SPECIFY THE SAME TZONES FROM THE SAME GLOBAL CSI DATASET

Reason:

The CSI datasets and/or the specified zones must be different.

Action:

Ensure that the CSI datasets are different and/or the specified TARGET zones are different.

Module:

SAFTAXRF

CAS2254E

NO SYSMOD ENTRIES FOUND FOR FMIDS SPECIFIED ON ++OLDZONE STATEMENTS

Reason:

When processing sysmod entries in the old CSI, no entries were found for the FMID(s) specified on the ++OLDZONE statements.

Action:

Ensure that the correct FMIDs and CSI were specified.

Module:

SAFTAXRF

CAS2255I

NO OLDZONE SYSMODS FOUND IN NEWZONE. CHECK SPECIFIED FMID AND/OR CSI

Reason:

The zones specified in ++OLDZONE and ++NEWZONE do not have any sysmods in common. Report processing completed normally. However, it is likely that the FMIDs or the CSIs were specified incorrectly.

Action:

Ensure that the correct FMIDs and CSIs are specified.

Module:

SAFTAXRF

CAS2256E

xxxxxxxx DATASET OPEN FAILED

Reason:

An error occurred while attempting to open the dataset indicated. xxxxxxx is the DD name of the dataset that failed to open.

Action:

Ensure that the DD statement exists and is correct for the specified DD.

Module:

SAFTAXRF

CAS2257E

UNABLE TO OBTAIN STORAGE FOR ZONE COMPARE PROCESSING

Reason:

An attempt to obtain storage failed.

Action:

Increase the region size for this job.

Module:

SAFTAXRF

CAS2258E

NO VALID DATA IN DD=*xxxxxxxx*. CHECK THE SMP/E SMPOUT DD STATEMENT

Reason:

No valid data was found in the specified dataset generated by SMP/E. *xxxxxxxx* is the DD name of the dataset that failed to open.

Action:

Check the SMPOUT dataset for error messages.

Module:

SAFTAXRF

CAS2259E

MAXIMUM NUMBER OF SYSMODS EXCEEDED IN OLDZONE

Reason:

When processing sysmod entries in the old CSI, the maximum number of entries was exceeded.

Action:

Rerun the report with fewer FMIDs specified on the ++OLDZONE and ++NEWZONE statements.

Module:

SAFTAXRF

CAS2260E

comp abend AT addr LMOD mod CSECT csect +off job step proc

Reason:

This is a diagnostic information display for an ABEND. If any of these variable fields are unavailable at the time of the ABEND, N/A appears as the value.

comp

The component that requested the dump.

abend

The ABEND completion code.

addr

The address from the PSW at time of ABEND.

mod

The name of the load module that abended.

csect

The CSECT name in the abended load module.

off

The offset into the load module or the CSECT where the ABEND occurred. If the CSECT name is N/A, then the offset is in the load module.

job

The job name of the abending program.

step

The job step name of the abending program.

proc

The procedure step name of the abending program.

Action:

Contact CA Technical Support and provide the message number and diagnostic information.

Module:

SAFFETTL

CAS2261I

NSI: psw

Reason:

This message displays the program status word, in hexadecimal format, of the next sequential instruction after an ABEND has occurred. The value of *psw* is the current program status word, in hexadecimal format, at the time of the ABEND.

Action:

This message is for information only. No action is required.

Module:

SAFFEIDF

CAS2262I

ILC: *ilc* INTERRUPT CODE: *itc* REASON CODE: *rsn*

Reason:

This message displays the instruction length count, interrupt code, and reason code associated with an ABEND.

ilc

Indicates the instruction length code from the error PSW.

itc

Indicates the interrupt code associated with the error PSW.

rsn

Indicates the value of register 15 at the time of the ABEND.

Action:

This message is for information only. No action is required.

Module:

SAFFEIDF

CAS2263I

TRANSLATION EXCEPTION ADDRESS: addr

Reason:

This message displays the virtual address causing the translation exception displayed in hexadecimal format. The value of *addr* is the virtual address causing the translation.

Action:

This message is for information only. No action is required.

Module:

SAFFEIDF

CAS2264I

DATA AT FAILING PSW ADDRESS: data

Reason:

This message displays the data at the failing PSW address. The value of *data* is the twelve bytes of hexadecimal data at the PSW address.

Action:

This message is informational only. No action is required.

Module:

SAFFEIDF

CAS2265I

range regvalue regvalue regvalue regvalue

Reason:

This message displays the contents of the general registers at the time of the ABEND.

range

The register range that displays.

regvalue

The register value at the time of the ABEND.

Action:

This message is informational only. No action is required.

Module:

SAFFEIDF

CAS2266I

comp DUMP IN PROGRESS

Reason:

An SVC dump is in progress for the indicated processor id. The value of *comp* is the component that requested the dump.

Action:

This message is informational only. No action is required.

Module:

SAFFEDMP

CAS2267I

como DUMP COMPLETED

Reason:

The requested SVC dump successfully completed. The value of *comp* is the component that requested the dump.

Action:

This message is informational only. No action is required.

Module:

SAFFEDMP

CAS2268I

comp DUMP UNSUCCESSFULLY COMPLETED. R15 = rc

Reason:

An error occurred during an SVC dump.

comp

The component that requested the dump

rc

The return code from the SDUMP macro:

- **4**—The dump data set was too small to contain the whole dump.
- **8**—The dump data sets are full.

Action:

This message is informational only. No action is required.

Module:

SAFFEDMP

CAS2270E

TRACE DATA SET HAS DSORG=PO AND NO MEMBER NAME WAS SPECIFIED

Reason:

A SECTRACE request specified output to a data set (DATASET=). The data set specified was a partitioned data set, but no member name (MEMBER=) was specified. To avoid destroying the directory of the data set, the SECTRACE request was not honored.

Action:

Re-enter the SECTRACE request by specifying a member name or a data set that is not partitioned.

Module:

SAFAAALC

CAS2271E

TRACE DATA SET OPEN FAILED: ABEND CODE X'*abc*' REASON CODE X'*rsn*'

Reason:

A SECTRACE request specified output to a data set. SECTRACE encountered an ABEND while attempting to open the data set. *abc* is the ABEND code; *rsn* is the reason code.

Action:

If the ABEND code is 913, the data set could not be opened because of a security problem. Contact your security administrator. If the ABEND code is anything other than 913, contact CA Top Secret Technical Support.

Module:

SAFAAALC

CAS2280E

NOT ENOUGH STORAGE WAS MADE AVAILABLE TO CONSTRUCT LDAP REQUEST

Reason:

Not enough storage space was allocated in the CA Top Secret LDAP task to build the LDAP API request.

Action:

Contact local CA Top Secret systems programmer or CA Top Secret Technical Support. Provide any system messages issued just before or after this message that refer to shortages of CSA or SQA.

Module:

CAS4LDAP

CAS2281E

UNABLE TO VERIFY THE SECURITY PRODUCT THAT ISSUED THE LDAP REQUEST

Reason:

An internal consistency check failed. The type of security product that issued the LDAP request was not identifiable.

Action:

Contact CA Top Secret Technical Support.

Module:

CAS4LDAP

CAS2282I

LDAP TABLE IS NOT AVAILABLE FOR LDAP REQUESTS

Reason:

There are no LDAP directories defined for LDAP requests

Action:

Define LDS LDAP records and XREFLDAP records. Initialize the LDAP table by issuing the REFRESH operator command to activate any GSO XREFLDAP records. Then, issue the REFRESH operator command to activate any LDS LDAP records.

Module:

CAS4LDAP

CAS2283E

A PASSTICKET WAS NOT GENERATED FOR LDAP ADMINISTRATOR *XXX* FOR LDAP SERVER *xxx*

Reason:

A failure occurred while generating a PassTicket for the LDAP administrator *XXX* and the LDAP server *xxx*.

Action:

Verify the APPLNAME field in the LDS LDAP record specifies the application name of the SSIGNON profile data record that contains the CA Top Secret administrator's encryption key used for generating PassTickets. Verify the SSIGNON profile data record exists. If the information is incorrect, rectify the problem and refresh the records. If the problem still persists, contact CA Top Secret Technical Support.

Module:

CAS4LDAP

CAS2284E

PASSWORD DECRYPTION FAILED FOR LDAP ADMINISTRATOR *XXX* FOR LDAP SERVER *xxx*

Reason:

A failure occurred while decrypting the password for administrator XXX for the LDS LDAP record with the LDAP server indicated in *xxx*.

XXX represents the administrator-distinguished name for the outbound request. x*xx* represents the URL for the LDAP directory of the outbound request.

Action:

Contact CA Top Secret Technical Support.

Module:

CAS4LDAP

CAS2285E

LDAP RECORD WITH URL *XXX* WAS DEACTIVATED DUE TO PASSWORD PROCESSING ERRORS

Reason:

The LDS LDAP record with URL specified as *XXX* was deactivated due to a password decryption error or a PASSTICKET generation error. See massage CAS2284E for the specific type of error.

Action:

Issue the CA Top Secret command SHOW LDAP to display the record that was deactivated due to this error. Verify the GSO LDAP record field value for the ADMPSWD(LDAP administrator password) and the APPLNAME(application name) is correct and issue the REFRESH operator command for the LDS LDAP record to reactivate this node. If the problem still persists, contact CA Top Secret Technical Support.

Module:

CAS4LDAP

CAS2286E

LDAP REQUESTED FAILED. RC: *rc* USER DN: *XXX* URL: *xxx*

Reason:

The LDAP API support module *XXX* represents the administrator-distinguished name for the outbout request. *xxx* represents the URL for the LDAP directory of the outbound request. *rc* represents the return code from the LDAP API support module. The possible values of the *rc* are:

Return Codes	
CRITICAL ERROR	00
LDAP_OPERATIONS_ERROR	01
LDAP_PROTOCOL_ERROR	02
LDAP_TIMELIMIT_EXCEEDED	03
LDAP_SIZELIMIT_EXCEEDED	04
LDAP_COMPARE_FALSE	05
LDAP_COMPARE_TRUE	06
LDAP_AUTH_METHOD_NOT_SUPPORTED	07
LDAP_STRONG_AUTH_NOT_SUPPORTED	07
LDAP_STRONG_AUTH_REQUIRED	08
LDAP_PARTIAL_RESULTS	09
LDAP_REFERRAL	0a
LDAP_ADMINLIMIT_EXCEEDED	0b
LDAP_UNAVAILABLE_CRITICAL_EXTENSION	0c
LDAP_CONFIDENTIALITY_REQUIRED	0d
LDAP_SASL_BIND_IN_PROGRESS	0e
LDAP_NO_SUCH_ATTRIBUTE	10
LDAP_UNDEFINED_TYPE	11
LDAP_INAPPROPRIATE_MATCHING	12
LDAP_CONSTRAINT_VIOLATION	13
LDAP_TYPE_OR_VALUE_EXISTS	14
LDAP_INVALID_SYNTAX	15
LDAP_NO_SUCH_OBJECT	20

Return Codes	
LDAP_ALIAS_PROBLEM	21
LDAP_INVALID_DN_SYNTAX	22
LDAP_IS_LEAF	22
LDAP_ALIAS_DEREF_PROBLEM	24
LDAP_INAPPROPRIATE_AUTH	30
LDAP_INVALID_CREDENTIALS	31
LDAP_INSUFFICIENT_ACCESS	32
LDAP_BUSY	33
LDAP_UNAVAILABLE	34
LDAP_UNWILLING_TO_PERFORM	35
LDAP_LOOP_DETECT	36
LDAP_NAMING_VIOLATION	40
LDAP_OBJECT_CLASS_VIOLATION	41
LDAP_NOT_ALLOWED_ON_NONLEAF	42
LDAP_NOT_ALLOWED_ON_RDN	43
LDAP_ALREADY_EXISTS	44
LDAP_NO_OBJECT_CLASS_MODS	45
LDAP_RESULTS_TOO_LARGE	46
LDAP_AFFECTS_MULTIPLE_DSAS	47
LDAP_OTHER	50
LDAP_SERVER_DOWN	51
LDAP_LOCAL_ERROR	52
LDAP_ENCODING_ERROR	53
LDAP_DECODING_ERROR	54
LDAP_TIMEOUT	55
LDAP_AUTH_UNKNOWN	56
LDAP_FILTER_ERROR	57
LDAP_USER_CANCELLED	58
LDAP_PARAM_ERROR	59
LDAP_NO_MEMORY	5a

Return Codes	
LDAP_CONNECT_ERROR	5b
LDAP_NOT_SUPPORTED	5c
LDAP_CONTROL_NOT_FOUND	5d
LDAP_NO_RESULTS_RETURNED	5e
LDAP_MORE_RESULTS_TO_RETURN	5f
LDAP_CLIENT_LOOP	60
LDAP_REFERRAL_LIMIT_EXCEEDED	61

Action:

Critical errors can be storage related or invalid CODEPAGE related. For critical errors call Technical Support.

CAS2287E

INVALID PARAMETER LIST PASSED TO CAS4LDAP

Reason:

An internal error occurred in the CA TSS LDAP support module CAS4LDAP.

Action:

Contact CA Technical Support.

Module:

CAS4LDAP

CAS2288E

INVALID LDAP RECORD *XXX* SPECIFIED IN LDAP NODE LIST FOR USERID *xxx*

Reason:

The LDAP directory record specified in the node list for this user is not active.

XXX

Represents the LDAP record ID specified in the LDAP node list for this user. *Xxx* represents the userid of the outbound LDAP request to be processed.

Module:

CAS4LDAP

CAS2289E

Plist build error, LDAP REC ID: *id* RSN: *rsn* Field: *xxx* User DN: *XXX*

Reason:

A failure occurred while processing the parameter list for the LDAP API program. *id* represents the LDAP record ID that was being processed for the LDAP Directory Services (LDS) request. *XXX* represents the User Distinguished Name syntax for the LDAP LDS request. *xxx* represents the XREF LDAP attribute field being processed or the LDAP LDS request. *rsn* is the reason code. Possible reason code values are:

08

Error detected converting data to LDAP field type and format.

0C

Error detected converting data to character date format

10

Error detected converting binary data field

14

Truncation of data field is not supported.

Action:

If you received a reason code of 14, inspect the LDAPattributeLength of the described FIELD specified on the XREF field of the LDAP record ID indicated. CA Top Secret does not allow field data to be truncated. Modify LDAPattributeLength to not allow for the truncation of the LID field data. Refresh the LDAP records to activate this update. For all other reason codes, contact CA Top Secret Technical Support.

Module:

CAS4LDAP

CAS228AE

LDS request failed. LDAP node deactivated due to a previous error.

Reason:

LDS deactivates the LDAP node record for several reasons; either an incorrect administrator password was supplied to the LDAP server or the limit of consecutive LDAP requests that have timed-out was exceeded. Analyze the previous messages for the specific type of error.

Action:

Issue the TSS command to display the record that was deactivated due to this error. Verify the LDS LDAP record field value for the LDAP administrator password or the APPLNAME (application name) is correct. Verify the LDAP server and the communication services are running. Issue the REFRESH operator command for the LDS LDAP record to reactivate this node.

Module:

CAS4LDAP

CAS228BI

LDS synchronization request successful

Reason:

LDS journals the condition that the LDAP request has been transmitted to a LDAP server.

Action:

This message is informational only. No action is required.

Module:

CAS4LDAP

CAS228BI

LDS request failed. Request has timed-out for LDAP node *xxx* User DN: *yyy* URL: *zzz*

Reason:

The LDAP request has timed out due to the time limitation specified on TIMEOUT field of the LDS OPTIONS record. *xxx* is the LDS LDAP record id associated with the request. *yyy* is the User Distinguished Name associated with the request. *zzz* is the URL of the LDAP server associated with the request.

Action:

Ensure the LDAP server is not down and the LDS LDAP record is accurate. If the timeout specified is too small an interval, increase the number of seconds specified in the TIMEOUT field of the LDS OPTIONS record. Stop and restart LDS to enforce the new TIMEOUT specification.

Module:

CAS4LDAP

CAS228DE

LDAP Node xxx is deactivated due to excessive number of Time-out or Network errors

Reason:

The LDAP record specified was deactivated by CA Top Secret due to successive timeout failures. *xxx* is the LDS LDAP record id associated with the request.

Action:

Issue the TSS command to display the record that was deactivated due to this error. Ensure the LDAP server is not down and the LDS LDAP record is accurate and issue the REFRESH operator command for the LDS LDAP record to reactivate this node. If the problem still persists, contact CA Top Secret Technical Support. If the timeout specified is too small an interval, increase the number of seconds specified in the TIMEOUT field of the LDS OPTIONS record. Stop and restart LDS to enforce the new TIMEOUT specification.

Module:

CAS4LDAP

CAS228E

E LDS request failed. LDS API support subtask is down. User DN: *xxx* URL: *yyy*

Reason:

An internal error occurred during LDS node processing.

Action:

Contact CA Technical Support.

Module:

CAS4LDAP

CAS229OE

Unable to obtain storage for LDS journal processing

Reason:

CA Top Secret LDS was unable to obtain a block of storage.

Action:

Contact CA Technical Support.

Module:

CAS4LDJQ, CAS4LJFS

CAS2292E

UNABLE TO RELEASE STORAGE FOR LDS JOURNAL PROCESSING

Reason:

CA Top Secret LDS was unable to release a block of storage.

Action:

Contact CA Technical Support.

Module:

CAS4LDJQ, CAS4LJFS

CAS2293E

LDS JOURNAL PROCESS FAILED DUE TO AN INVALID PARAMETER LIST

Reason:

The main LDS task did not pass a required parameter to the LDS journal constructer routine.

Action:

Contact CA Technical Support.

Module:

CAS4LDJQ

CAS2294E

LDS API TASK ALREADY ACTIVE

Reason:

CA Top Secret LDS attempted to ATTACH a support service subtask CAS4LDSC that was already attached. This error should not occur.

Action:

Contact CA Technical Support.

Module:

CAS4LDAP

CAS2295E

UNABLE TO ATTACH LDS API TASK

Reason:

An internal error occurred during the startup of the LDS node processing.

Action:

Contact CA Technical Support.

Module:

CAS4LDAP

CAS2297E

LDAP NODE PROCESSOR SUBTASK HAS TERMINATED DUE TO AN ABEND

Reason:

An ABEND occurred during CA Top Secret node processing.

Action:

Contact CA Technical Support.

Module:

CAS4LDAP

CAS2298E

LDS API SUBTASK HAS TERMINATED DUE TO AN ABEND

Reason:

An abend occurred during CA Top Secret LDS processing of an LDAP request.

Action:

Contact CA Technical Support.

Module:

CAS4LDAP

CAS23 LDS Journal Messages

CAS2350E

LDS JOURNAL FILE INITIALIZATION COMPLETE

Reason:

The LDS journal file initialization job has completed successfully.

Action:

This message is informational only. No action is required.

Module:

CAS4LIJL

CAS2351E

SYSIN FILE OPEN ERROR

Reason:

The LDS journal file initialization could not successfully open the SYSIN file.

Action:

Determine the reason for the failure from the open failure messages received, correct the problem, and try again.

Module:

CAS4LIJL

CAS2352E

INVALID PARM, BLOCKS= NOT FOUND

Reason:

The SYSIN input card read in from the LDS initialization job was not the required card. The only valid card must begin with BLOCKS=.

Action:

Ensure that the only SYSIN input card begins with BLOCKS=. Correct the input card and rerun the job.

Module:

CAS4LIJL

CAS2353E

INVALID PARM, BLOCKS= INVALID

Reason:

The SYSIN input card read in from the LDS initialization job was not valid. The specified number of blocks contained an invalid amount.

Action:

Verify that the number of blocks specified for the BLOCKS= on the SYSIN input card contains a valid numerical value that does not begin with zero. Correct the value and rerun the job.

Module:

CAS4LIJL

CAS2354E

SYSIN FILE ERROR – NO PARMS ENTERED

Reason:

The SYSIN input file contained no data. A required input card that begins with BLOCKS= must be specified.

Action:

Ensure that the SYSIN input file contains one input card that beings with BLOCKS= and rerun the job.

Module:

CAS4LIJL

CAS2355E

JOURNAL FILE OPEN ERROR

Reason:

The LDS journal field initialization job could not successfully open the journal file.

Action:

Determine the reason for the failure from the open failure messages received. Correct the problem and try again.

Module:

CAS4LIJL

CAS2356E

ERROR WRITING TO JOURNAL FILE

Reason:

The LDS journal file initialization job could not successfully write to the journal file.

Action:

Determine the reason for the failure from open failure message received. Correct the problem and try again.

Module:

CAS4LIJL

CAS235DE

No free space on LDS Recovery file

Reason:

The LDS recovery file is full. LDS cannot store LDS transaction data to the recovery file.

Action:

Issue a SHOW LDS command to ensure the LDAP nodes are active. Correct connection problems with LDS defined LDAP servers and Issue the LDS(ACTIVE) command to reconnect to the LDAP server. Create a larger LDS recovery file or delete old transaction data from the file by issuing the LDS REMOVE command.

Module:

CAS4LDAP

CAS2360E

LDS JOURNAL DISABLED: ABEND OCCURRED DURING PROCESSING

Reason:

An abend occurred during CA Top Secret LDS journal processing.

Action:

Contact CA Top Secret Technical Support.

Module:

CAS4LJFS

CAS2361E

LDS JOURNAL FILE OPEN FAILED

Reason:

The data set specified in the DATASET field of the LDS OPTIONS record cannot be found.

Action:

Correct the error and try again.

Module:

CAS4LJFS

CAS2362E

LDS JOURNAL FILE ALLOCATE FAILED

Reason:

CA Top Secret LDS cannot dynamically allocate the data set specified in the DATASET field of the LDS OPTIONS record.

Action:

Ensure the data set exists. Run the INITLDSJ job to create and initialize the LDS journal. Make sure the LDS OPTIONS record specifices the correct DATASET name of the LDS Journal. Refresh the LDS OPTIONS record and restart the LDS journal.

Module:

CAS4LJFS

CAS2364E

UNABLE TO ESTABLISH ERROR RECOVERY ENVIRONMENT

Reason:

CA Top Secret LDS cannot create the requested abend recovery environment ESTAE to initialize the LS journal process. LDS journal initialization is terminated.

Action:

Contact CA Top Secret Technical Support

Module:

CAS4LJFS, CASULDAP

CAS2366I

LDS JOURNAL PROCESSING INITIALIZED

Reason:

This informational message is displayed on the console when CA Top Secret LD journal has completed initialization.

Action:

This message is informational only. No action is required.

Module:

CAS4LJFS

CAS2367I

LDS JOURNAL PROCESSING TERMINIATED

Reason:

This informational message is displayed on the console when CA Top Secret LD journal has completed termination.

Action:

This message is informational only. No action is required.

Module:

CAS4LJFS

CAS2368E

UNABLE TO ALLOCATE DDNAME rsn code=RC

Reason:

CA Top Secret cannot dynamically allocate the dataset that specified the DATASET field of the LDS OPTIONS record. The value of RC is the return code from the DYNALLOC macro.

Action:

Contact CA Top Secret Technical Support.

Module:

CAS4LJFS

CAS2369I

******LDS JOURNALING INITIALIZED FOR LDSJRNL FILE*******

Reason:

This informational message is printed in the CA Top Secret journal file after the file is opened.

Action:

This message is informational only. No action is required.

Module:

CAS4LJFS

CAS236AE

LDS JOURNAL FILE CLOSE FAILED

Reason:

CAS4LJFS cannot close the file specified in the JCL or the data set that specified in the DATASET field of the LDS OPTIONS record.

Action:

Contact CA Top Secret Technical Support.

Module:

CAS4LJFS

CAS23 SAF HFS Security

CAS2301E

EVENT PROCESSING ROUTINE COULD NOT BE LOADED

Reason:

The initialization process could not locate the event processing routine, SAFHFSEC.

Action:

Ensure that module SAFHFSEC is available in a link list library and that module SAFRTRLD contains the proper maintenance for CA SAF HFS security support.

Module:

SAFHFINT

CAS2302E

ENF/USS GLOBAL WORKAREA NOT PRESENT

Reason:

The ENF/USS initialization driver did not provide a required global work area to the security initialization routine.

Action:

Contact CA Technical Support.

Module:

SAFHFINT

CAS2303E

ENF/USS EVENT STRUCTURE ARRAY NOT PRESENT

Reason:

The ENF/USS initialization driver did not provide a required list of events to the security initialization routine.

Action:

Contact CA Technical Support.

Module:

SAFHFINT

CAS2304E

CA SAF IVT CONTROL BLOCK COULD NOT BE FOUND

Reason:

A critical CA SAF control block could not be located. An improper installation of the security product or corruption of common storage may cause this.

Action:

Contact CA Technical Support.

Module:

SAFHFINT, SAFHFMOD

CAS2305E

EVENT PROCESSING TABLE COULD NOT BE FOUND

Reason:

The table containing a list of security-related events could not be located or was corrupted.

Action:

Ensure that the module SAFHFSEC is properly link edited and has not been corrupted.

Module:

SAFHFINT

CAS2306W

xxxxxxxxxxxxxxxx EVENT COULD NOT BE FOUND

Reason:

An expected security event was not found in the list of events presented to security initialization by ENF/USS. The event may be obsolete or OS/390 release-dependent. Processing continues without security processing for the event.

Action:

Ensure that ENF/USS and the security product are at compatible maintenance levels. Contact CA Top Secret technical support providing the event name causing the error.

Module:

SAFHFINT

CAS2310E

PARAMETER ERROR DETECTED

Reason:

The ENF/USS event driver did not pass a required parameter to the security event processing routine.

Action:

Contact CA Technical Support.

Module:

SAFHFSEC

CAS2311W

ERROR DETECTED IN USER EXIT SAFHFUSR; EXIT PROCESSING BYPASSED

Reason:

The installation has provided user exit code to modify the HFS path and file name information. The exit has either provided an invalid path name or written beyond the path name field provided. Changes made by the user exit are ignored. The user exit is contained in CSECT SAFHFUSR in load module SAFHFSEC. This message is issued only when HFS tracing is enabled.

Module:

Ensure that the exit logic is correct. One way to do this is to set an instruction-fetch SLIP trap at the point where the user exit routine returns to the caller. The modified path name information should appear in the dump output. Contact CA Top Secret Technical Support for further assistance.

Module:

SAFHFSEC

CAS2312E

userid - access ACCESS DENIED

Reason:

Security processing has denied access to the HFS file or function. The message identifies the ID of the user attempting the access and the type of access. The type of access is reported in SAF terminology and can be EXECUTE, READ, UPDATE, CONTROL and ALTER. These accesses correspond to resource rule SERVICE of EXECUTE, READ, UPDATE, DELETE and ADD. EXECUTE access indicates that a program file is being accessed, READ that a file is opened for input, and UPDATE that a file is opened for output. CONTROL access indicates that some type of file function is being performed, such as changing file attributes. ALTER access indicates that a file is being created or deleted.

Action:

For more information, run the resource violation report. The report details the violation with the original HFS path name, the modified name, and the reason for access being denied.

Module:

SAFHFSEC

CAS2319I

TRACEID=aaaaaaaa USER=bbbbbbbb JOBNAME=cccccccc

Reason:

Output in response to a SECTRACE TYPE=HFS command. The first line of the trace output contains the trace ID, the current user ID, and the current job name. Subsequent lines contain other information specific to the request being processed. This information can include the event being processed, the HFS file name being accessed, return code values, and specific reasons for access being allowed or denied.

Action:

This information may be requested by CA Top Secret Technical Support to assist in problem resolution.

Module:

SAFHFTRC

CAS2320I

CA SAF HFS SECURITY IS ENABLED

Reason:

This message describes the current status of CA SAF HFS security. The message is issued as the result of a status request or the setting of CA SAF HFS security through the SAFHFMOD utility program.

Action:

This message is informational only. No action is required.

Module:

SAFHFMOD

CAS2321I

CA SAF HFS SECURITY IS DISABLED - NATIVE UNIX SECURITY IS IN USE

Reason:

This message describes the current status of CA SAF HFS security. The message is issued as the result of a status request or the setting of CA SAF HFS security through the SAFHFMOD utility program. When CA SAF HFS security is disabled, native UNIX security processing is enabled. Access to UNIX resources is granted through file permission bits, superuser status, and normal OS/390 UNIX security services.

Action:

This message is informational only. No action is required.

Module:

SAFHFMOD

CAS2322E

USER IS NOT AUTHORIZED TO PERFORM FUNCTION

Reason:

Use of the SAFHFMOD utility functions requires that access be allowed to a resource defined in the SAF FACILITY class. The resource name is BPX.CAHFS.SECURITY.*function*, where *function* can be STATUS, ENABLE, or DISABLE.

Action:

Determine why access is denied by reviewing the resource violation report.

Module:

SAFHFMOD

CAS2323E

PROGRAM IS NOT AUTHORIZED

Reason:

The SAFHFMOD program must run authorized.

Action:

Ensure that the SAFHFMOD module is link edited with code AC(1) and resides in an APF-authorized library. The TSO environment does not allow a program to run authorized without changing certain TSO-related tables, so the utility should normally be run in batch.

Module:

SAFHFMOD

CAS2324E

VALID PARAMETERS ARE: ENABLE, DISABLE, STATUS

Reason:

The SAFHFMOD utility requires a parameter describing the function to be performed. A parameter was not supplied or it was not recognized by the utility.

Action:

Ensure that a valid parameter was supplied to the utility.

Module:

SAFHFMOD

CAS2372E

LDS Connect failed. RC: rc LDAP Node: xxx

Reason:

LDS attempted to establish a connection to an LDAP server but failed due to the return code indicated in *rc*. *rc* is the return code from the CONNECT function. *xxx* specifies the LDAP NODE record ID of the defined LDAP server.

Action:

Examine the LDAP return code to determine how to correct the problem. For a list of LDAP API return codes, see message CAS2286E. Critical errors may be storage related or invalid CODEPAGE related. For critical errors, call Technical Support.

Module:

CAS4LDAP

CAS24 R_cacheserv SAF Callable Service

CAS2400E

Insufficient storage to create R_cacheserv subtask header

Reason:

Storage was not available in CSA subpool 231. The R_cacheserv subtask terminates.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2401E

Unable to locate the SAFIVT

Reason:

A critical CA SAF control block could not be located. An improper installation of the security product or corruption of common storage may cause this. The R_cacheserv subtask terminates.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2402E

Unable to establish error recovery environment

Reason:

Internal error. The R_cacheserv subtask terminates.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2404E

POST of R_cacheserv subtask requestor returned an error. R15=X'*rc*', R0=X'*rsn*'

Reason:

The R_cacheserv subtask issued the POST macro but it failed with return code *rc* in R15.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2405E

***macro service* request returned an error. R15='X'*rc*', R0=X'*rsn*'**

Reason:

An error was encountered on a macro call. *macro* is ALESERV or DSPSERV. *service* is SEARCH, ADD, or CREATE. *rc* is the return code in R15. *rsn* is the reason code in R0.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2406E

Dataspace created for R_cacheserv subtask was too small

Reason:

The dataspace created by the DSPSERV macro was too small to hold the maximum record data.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2407E

R_cacheserv *function* request returned an error. SAF RC=X'*rc*' RC=X'*rc*' RSN=X'*rsn*'

Reason:

The R_cacheserv subtask called R_cacheserv services, but the request failed. *function* is the type of call — START, ADD, or END. SAF *rc* is the SAF return code. *rc* is the return code from the service. *rsn* is the reason code from the service.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2408E

A field length in the hardened cache is invalid

Reason:

On a cache restore, the length for a record name or record data in the hardened copy of the cache is larger than the allowable maximum. The hardened cache is invalid. Restore processing fails.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS2409E

R_cacheserv request subtask is terminating after an abend

Reason:

The R_cacheserv subtask abended and will terminate.

Action:

Restart CA Top Secret to make the R_cacheserv subtask active again. Contact CA Top Secret Technical Support.

Module:

SAFOERCS.

CAS240AE

R_cacheserv file services — invalid request type encountered

Reason:

R_cacheserv file services module was called with an invalid request type.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCF.

CAS240BE

R_cacheserv file services — *xxx* initialization failed

Reason:

Inisitalization of the ACB or the RPL failed — *xxx* is either ACB or RPL. The R_cacheserv subtask terminates.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCF.

CAS240CE

file open failed — DDNAME: *dddddddd* RC=X'*rc*' RSN=X'*rsn*'

Reason:

The R_cahceserv file services OPEN request failed. *dddddddd* is the DD name. *rc* is the return code in R15. *rsn* is the reason code from the ACNERFLG field of the ACB. The R_cacheserv subtask terminates.

Action:

Make sure that the CA Top Secret procedure JCL contains a DD statement for the R_cacheserv VSAM file with the correct DD name.

Module:

SAFOERCF.

CAS240DE

R_cacheserv file services — unable to obtain record buffer storage

Reason:

R_cacheserv file services could not obtain the storage for the record buffer or the SHOWCB macro failed. The R_cacheserv subtask terminates.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCF.

CAS240EE

R_cacheserv VSAM I/O error — REQ=*request* RC=X'*rc*' RSN=X'*rsn*'

Reason:

R_cacheserv file services encountered a VSAM I/O error. *request* is the type of request being processed. *rc* is the return code in R15. *rsn* is the feedback code from the RPLERRCD field of the RPL.

Action:

Contact CA Top Secret Technical Support.

Module:

SAFOERCF.

CAS240FE

Previously hardened cache has equal version — cache harden rejected

Reason:

R_cacheserv file services detected that the cache to be hardened has the same version as one that is already hardened. The cache will not be re-hardened. This message is informational.

Action:

None.

Module:

SAFOERCF.

SAFCRINT

CAS2410E

Could not initialize CA PKI

Reason:

An internal error occurred during PKI initialization.

Action:

Contact CA Technical Support

Module:

SAFCRINT

CAS2411E

Etcer retun = nn

Reason:

An internal error occurred during PKI initialization.

Action:

Contact CA Technical Support

Module:

SAFCRINT

SAFCRENC

CAS2420E

Could not perform key generation initialization RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An internal error occurred while initializing the key generation process.

Action:

Contact CA Technical Support.

Module:

SAFCRGCT

CAS2421E

Provider Create Error RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An internal error occurred while initializing the key generation process.

Action:

Contact CA Technical Support.

Module:

SAFCRGCT

CAS2422E

Generate Key Error RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An internal error occurred while attempting to generate a public/private key pair.

Action:

Contact CA Technical Support.

Module:

SAFCRGCT

CAS2423E

Export Key Error RC: *rtncode,* RSN: *rsncode,* E-RC: *PKI rtncode*

Reason:

An internal error occurred while attempting to return the public/private key pair to the caller.

Action:

Contact CA Technical Support. Provide technical support with the RSN and E-RC codes.

Module:

SAFCRGCT

CAS2424E

Could not perform sign cert initialization RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An internal error occurred while initializing the signing of a certificate process.

Action:

Contact CA Technical Support.

Module:

SAFCRGCT

CAS2425E

Import Key Error RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An error occurred while processing the private key.

Action:

Validate the private key used for signing. If the private key is correct, contact CA Technical Support.

Module:

SAFCRGCT

CAS2426E

Cert Sign Error RC: *rtncode*, RSN: *rsncode,* E-RC*: PKI rtncode*

Reason:

An internal error occurred while attempting to sign a certificate.

Action:

Contact CA Technical Support.

Module:

SAFCRGCT

CAS2427E

Verify setup error RC: *rtncode*, RSN: *rsncode,* E-RC: *PKI rtncode*

Reason:

An internal error occurred while attempting to verify a certificate during initialization process.

Action:

Contact CA Technical Support.

Module:

SAFCRXTR, SAFCRXRQ

CAS2428E

Verify Import failed RC: *rtncode,* RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An error occurred while attempting to verify a certificate during public key processing.

Action:

Verify the public key is a valid key. If the public key is valid, contact CA Technical Support.

Module:

SAFCRXTR, SAFCRXRQ

CAS2429E

Verify Initialization Error RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An error occurred while attempting to identify the public key during verify certificate processing.

Action:

Verify the public key is a valid key. If the key is valid, contact CA Technical Support.

Module:

SAFCRXTR, SAFCRXRQ

CAS242AE

Verify Update Error RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An error occurred while attempting to verify the certificate data.

Action:

Verify both the certificate and public key being passed are correct. If they are correct, contact CA Technical Support.

Module:

SAFCRXTR, SAFCRXRQ

CAS242BE

Verify Cleanup Error RC: *rtncode*, RSN: *rsncode*, E-RC: *PKI rtncode*

Reason:

An internal error occurred during final processing of verification of a certificate.

Action:

Contact CA Technical Support.

Module:

SAFCRXTR, SAFCRXRQ

CAS242CE

Could not perform sign data initialization RC: *rtncode* RSN: *rsncode,* E-RC: *PKI rtncode*

Reason:

An internal error occurred during sign data processing.

Action:

Contact CA Technical Support.

Module:

CAS242DE

Sign data import failed RC: *rtncode* RSN: *rsncode* E-RC: *PKI rtncode*

Reason:

An internal error occurred during data import processing.

Action:

Contact CA Technical Support.

CAS242EE

Sign data init failed RC: *rtncode* RSN: *rsncode* E-RC: *PKI rtncode*

Reason:

An internal error occurred during sign data initialization processing.

Action:

Contact CA Technical Support.

CAS242FE

Sign data update failed RC: *rtncode* RSN: *rsncode* E-RC: *PKI rtncode*

Reason:

An internal error occurred during sign data update processing.

Action:

Contact CA Technical Support.

SAFCRMAN

CAS2460E

Length of passed public key area is nnnn, required length is dddd

Reason:

An internal error occurred during PKI services.

Action:

Contact CA Top Secret Technical Support

Module:

SAFCRMAN

CAS2461E

Length of passed private key area is nnnn, required length is dddd

Reason:

An internal error occurred during PKI services.

Action:

Contact CA Top Secret Technical Support

Module:

SAFCRMAN

CAS2452E

Length of passed signature area is nnnn, required length is dddd

Reason:

An internal error occurred during PKI services.

Action:

Contact CA Top Secret Technical Support

Module:

SAFCRMAN

CAS25 z/OS USS Logging Report and Statistics Gathering Report

CAS2510E

OPEN FAILED FOR SYSPRINT FILE

Reason:

The SYSPRINT File DD name was missing or OPEN had a problem with the data set attributes.

Action:

Confirm that the SYSPRINT File DD name is present and the data set attributes are correct. Correct the data and continue processing.

Modules:

SAFOERPT and SAFSGRPT

CAS2512E

OPEN FAILED FOR SYSIN FILE

Reason:

The SYSIN File DD name was missing or OPEN had a problem with data set attributes.

Action:

Confirm that the SYSIN File DD name is present and the data set attributes are correct. Correct the problem and continue processing.

Modules:

SAFOERPT and SAFSGRPT

CAS2514E

SYSIN CONTAINS TOO MANY STATEMENTS

Reason:

The statements contained in the SYSIN DD exceeded the size of the internal buffer for processing the statements.

Action:

Reduce the number of SYSIN statements by masking, where possible, or splitting up the statements into several job steps and separate executions of the utility.

Modules:

SAFOERPT and SAFSGRPT

CAS2520E

INVALID KEYWORD *kkkkkkkk*

Reason:

KEYWORD *kkkkkkkk* is not a valid keyword for the utility.

Action:

Enter a valid KEYWORD and continue processing.

Module:

SAFOERPT

CAS2521E

Unable to locate certificates on this system.

Reason:

No certificates currently exist in the security product database.

Action:

Generate some digital certificates or add them to the database via the TSS ADD command.

Module:

SAFCRRPT

CAS2522E

INVALID OPERAND VALUE FOR KEYWORD *kkkkkkkk*

Reason:

The value of KEYWORD *kkkkkkkk* is not a valid value.

Action:

Enter a valid KEYWORD value and continue processing.

Modules:

SAFOERPT and SAFSGRPT

CAS2523E

Incorrect maintenance level - certificate table size.

Reason:

You are attempting to run the certificate utility on a system that cannot support the utility. Internal control blocks must be at a specific level in order for the utility to work.

Action:

Contact CA support for the specific fixes required on your level of the CA Top Secret product.

Module:

SAFCRRPT

CAS2524E

No records match input criteria

Reason:

There are no certificates or key rings that match the input criteria specified.

Action:

Change your input criteria to match the records in your database. Make sure that you didn't have a typographical error when entering the keywords.

Module:

SAFCRRPT

CAS2525E

Not authorized to run the utility

Reason:

You are attempting to run a utility but do not have the required access level.

Action:

The certificate utility requires READ access to the IRR.DIGTCERT.LIST resource in the FACILITY class.

When the RINGNAME parameter is specified, READ access is required to IRR.DIGTCERT.LISTRING.

If RINGNAME is specified and the USER field is CERTAUTH, CERTSITE or a user other than the current user, UPDATE access is required to IRR.DIGTCERT.LISTRING.

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.

Module:

SAFCRRPT

CAS2527E

R_datalib error: $$

Reason:

The Certificate Utility invokes the R_datalib callable service when used with the RINGNAME parameter. The caller of the utility must have access to the IRR.DIGTCERT.LISTRING rule. For more information on the type of access required to use the RINGNAME parameter, see the documentation for the Certificate Utility in the *CA Top Secret Report and Tracking Guide*.

It is also possible that the Key Ring was not found. RINGNAME is tied to the USER parameter. If the USER parameter is not specified, USER defaults to the user invoking the utility.

Action:

Verify that the caller of the certificate is authorized to use the R_datalib callable service. If the caller is authorized, verify that you supplied the proper RINGNAME. The RINGNAME parameter is case-sensitive. If the internal error message displays, obtain an OMVS trace (FUNC=GET) or run the OM report and contact CA Top Secret support.

CAS2528E

AN I/O ERROR OCCURRED WHILE ATTEMPTING TO ACCESS AN SMF DATASET

Reason:

Self-explanatory.

Action:

See the previously issued messages.

Modules:

SAFOERPT and SAFSGRPT

CAS2530E

A LOGIC ERROR OCCURRED WHILE ATTEMPTING TO ACCESS AN SMF DATASET

Reason:

Self-explanatory.

Action:

See the previously issued messages.

Modules:

SAFOERPT and SAFSGRPT

CAS2532E

NO RECORDS MATCHED THE SPECIFIED CRITERIA OR THE SMF DATASET IS EMPTY

Action:

Verify that the report parameters are correct and that the proper SMF data set is being used.

Modules:

SAFOERPT and SAFSGRPT

CAS2534E

CANNOT SPECIFY INCLUDE AND SERVICE KEYWORDS

Reason:

You specified the SERVICE and INCLUDE keywords and they are mutually exclusive.

Action:

Remove one of the above keywords and run the report again.

Module:

SAFOERPT

CAS2536E

CANNOT SPECIFY EXCLUDE AND SERVICE KEYWORDS

Reason:

You specified the SERVICE and EXCLUDE keywords and they are mutually exclusive.

Action:

Remove one of the above keywords and run the report again.

Module:

SAFOERPT

CAS2538E

TOO MANY ENTRIES FOR *xxxxxxx*

Reason:

The number of INCLUDE or EXCLUDE statements exceeded the size of the internal buffer. *xxxxxxx* is either INCLUDE or EXCLUDE.

Action:

Reduce the number of INCLUDE or EXCLUDE statements by masking, where possible, or splitting up the statements into several job steps and separate executions of the utility.

Modules:

SAFOERPT and SAFSGRPT

CAS2540E

DUPLICATE SERVICE VALUE SPECIFIED

Reason:

You specified the same service keyword more than once when running the report.

Action:

Remove the duplicate parameter and run the report again.

Module:

SAFOERPT

CAS2599E

INTERNAL ERROR

Reason:

The CASAFIVT control block was not found, or there was a problem finding the internal SMF Read Routine.

Action:

Contact CA technical support.

Modules:

SAFOERPT and SAFSGRPT

CAS3 Common Record-Level Protection Routines

CAS3001E

SUPPLIED DATA BUFFER EXCEEDS MAXIMUM SIZE

Reason:

The input data buffer provided to the RECORD definition processor routine was too large.

Action:

Contact CA Top Secret Technical Support.

Module:

CRLPRECP

CAS3002E

DATA IS REQUIRED FOR KEYWORD

Reason:

You specified a RECORD definition record keyword that requires data. No data was found.

Action:

The RECORD definition record input process terminates. Determine the cause of the error and retry the data entry process.

Module:

CRLPRECP

CAS3003E

REQUIRED KEYWORD NOT FOUND

Reason:

The RECORD definition record input processor was unable to locate the RECNAME keyword. Input processing is terminated.

Action:

Check your input statements for correctness and retry the input process.

Module:

CRLPRECP

CAS3004E

INVALID KEYWORD FOUND

Reason:

The RECORD definition record input processor encountered an unknown keyword in the input data. Input processing is terminated.

Action:

Check your input data for correctness and retry the input process.

Module:

CRLPRECP

CAS3004I

COMMON DATASPACE INITILIAZED

Reason:

This message is issued during startup if tracing is enabled. It indicates that a SCOPE=COMMON dataspace has been built.

Action:

This message is informational only. No action is required.

CAS3005E

CRLPRECP INVOKED FOR ILLEGAL FUNCTION

Reason:

The RECORD definition record input processor was invoked to perform an unknown function. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3006E

CRLPRECP INVOKED FOR INCORRECT RECORD TYPE

Reason:

The RECORD definition record input processor was improperly invoked to handle a different type of record. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3007E

CRLPRECP FUNCTION=INIT, NO SOURCE BUFFER SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3008E

CRLPRECP FUNCTION=INIT, NO SOURCE BUFFER LENGTH SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3009E

CRLPRECP FUNCTION=PROCESS, NO INPUT BUFFER SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3012E

INVALID CHARACTER IN DATA FIELD

Reason:

The RECORD definition record input processor encountered invalid data in a data field. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPRECP

CAS3013E

CRLPRECP FUNCTION=PROCESS, INIT PROCESSING NOT PERFORMED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3014E

DUPLICATE FLDNAME SPECIFICATION

Reason:

The RECORD definition record input processor found two or more FLDNAME definitions in the definition of record field. Input processing terminates.

Action:

Remove the redundant FLDNAME specification and retry the input process.

Module:

CRLPRECP

CAS3015E

OPERAND TOO BIG FOR KEYWORD=VALUE

Reason:

The RECORD definition record input processor found a data element for a VALUE keyword larger than 44 characters. Input processing terminates.

Action:

Retry the input process specifying a VALUE keyword whose length is less than or equal to 44 characters.

Module:

CRLPRECP

CAS3016E

INVALID VALUE FOR TYPE KEYWORD

Reason:

The RECORD definition record input processor encountered an invalid value for the TYPE keyword. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPRECP

CAS3017E

DUPLICATE TYPE SPECIFICATION

Reason:

The RECORD definition record input processor encountered a duplicate TYPE keyword for a definition of a field. Input processing is terminated.

Action:

Remove duplicate TYPE specification; retry.

Module:

CRLPRECP

CAS3018E

DUPLICATE OFFSET SPECIFICATION

Reason:

The RECORD definition record input processor found a duplicate OFFSET keyword for a definition of a field. Input processing terminates.

Action:

Remove duplicate OFFSET specification; retry.

Module:

CRLPRECP

CAS3019E

KEYWORD=OFFSET, INVALID NUMERIC DATA

Reason:

The RECORD definition record input processor found too large of a number for the OFFSET keyword in the definition of a field. Input processing terminates.

Action:

Ensure that the OFFSET keyword data is in the proper range; retry.

Module:

CRLPRECP

CAS3020E

KEYWORD=OFFSET, NUMBER OUT OF RANGE

Reason:

The RECORD definition record input processor found an invalid number for the OFFSET keyword in the definition of a field. Input processing terminates.

Action:

Ensure that the OFFSET keyword data is in the proper range; retry.

Module:

CRLPRECP

CAS3021E

KEYWORD=OFFSET, NO VALUE FOUND

Reason:

The RECORD definition record input processor found an OFFSET keyword without data in the definition of a field. Input processing terminates.

Action:

Supply valid data for the OFFSET keyword; retry.

Module:

CRLPRECP

CAS3022E

DUPLICATE LENGTH SPECIFICATION

Reason:

The RECORD definition record input processor found a duplicate LENGTH keyword for a definition of a field. Input processing terminates.

Action:

Remove the duplicate LENGTH specification; retry.

Module:

CRLPRECP

CAS3023E

KEYWORD=LENGTH, INVALID NUMERIC DATA

Reason:

The RECORD definition record input processor found too large of a number for the LENGTH keyword in the definition of a field. Input processing terminates.

Action:

Ensure that the LENGTH keyword data is in the proper range; retry.

Module:

CRLPRECP

CAS3024E

KEYWORD=LENGTH, NUMBER OUT OF RANGE

Reason:

The RECORD definition record input processor found an invalid number for the LENGTH keyword in the definition of a field. Input processing terminates.

Action:

Ensure that the LENGTH keyword data is in the proper range; retry.

Module:

CRLPRECP

CAS3025E

KEYWORD=LENGTH, NO VALUE FOUND

Reason:

The RECORD definition record input processor found a LENGTH keyword without data in the definition of a field. Input processing terminates.

Action:

Supply valid data for the LENGTH keyword; retry.

Module:

CRLPRECP

CAS3026E

DUPLICATE ROW SPECIFICATION

Reason:

The RECORD definition record input processor encountered a duplicate ROW keyword for a definition of a field. Input processing is terminated.

Action:

Remove the duplicate ROW specification; retry.

Module:

CRLPRECP

CAS3027E

KEYWORD=ROW, INVALID NUMERIC DATA

Reason:

The RECORD definition record input processor encountered too large of a number for the ROW keyword in the definition of a field. Input processing is terminated.

Action:

Ensure that the ROW keyword data is in the proper range; retry.

Module:

CRLPRECP

CAS3028E

KEYWORD=ROW, NUMBER OUT OF RANGE

Reason:

The RECORD definition record input processor encountered an invalid number for the ROW keyword in the definition of a field. Input processing is terminated.

Action:

Ensure that the ROW keyword data is in the proper range; retry.

Module:

CRLPRECP

CAS3029E

VALUE SPECIFICATION REQUIRED

Reason:

The RECORD definition record input processor encountered an ROW keyword without data in the definition of a field. Input processing is terminated.

Action:

Supply valid data for the ROW keyword and retry the input process.

Module:

CRLPRECP

CAS3030E

DUPLICATE COL SPECIFICATION

Reason:

The RECORD definition record input processor encountered a duplicate COL keyword for a definition of a field. Input processing is terminated.

Action:

Remove the duplicate COL specification from the input data and retry.

Module:

CRLPRECP

CAS3031E

KEYWORD=COL, INVALID NUMERIC DATA

Reason:

The RECORD definition record input processor encountered too large of a number for the COL keyword in the definition of a field. Input processing is terminated.

Action:

Ensure that the data for the COL keyword is in the proper range and retry the input process.

Module:

CRLPRECP

CAS3032E

KEYWORD=COL, NUMBER OUT OF RANGE

Reason:

The RECORD definition record input processor encountered an invalid number for the COL keyword in the definition of a field. Input processing is terminated.

Action:

Ensure that the data for the COL keyword is in the proper range and retry the input process.

Module:

CRLPRECP

CAS3033E

KEYWORD=COL, NO VALUE FOUND

Reason:

The RECORD definition record input processor encountered a COL keyword without data in the definition of a field. Input processing is terminated.

Action:

Supply valid data for the COL keyword and retry the input process.

Module:

CRLPRECP

CAS3034E

FLDNAME SPECIFICATION REQUIRED

Reason:

The RECORD definition record input processor did not find a FLDNAME specification for an input line of a field definition. Input processing is terminated.

Action:

Each input statement describing a record field must have an associated FLDNAME definition. Supply a valid FLDNAME definition and retry the input process.

Module:

CRLPRECP

CAS3035E

LENGTH MUTUALLY EXCLUSIVE WITH VALUE

Reason:

The RECORD definition record input processor encountered both a LENGTH definition and VALUE DEFINITION in the input for a field definition. Input processing is terminated.

Action:

LENGTH and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module:

CRLPRECP

CAS3036E

ROW MUTUALLY EXCLUSIVE WITH VALUE

Reason:

The RECORD definition record input processor encountered both a ROW and VALUE definition in the input for a field definition. Input processing is terminated.

Action:

ROW and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module:

CRLPRECP

CAS3037E

COL MUTUALLY EXCLUSIVE WITH VALUE

Reason:

The RECORD definition record input processor encountered both a COL and VALUE definition in the input for a field definition. Input processing is terminated.

Action:

COL and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module:

CRLPRECP

CAS3038E

OFFSET MUTUALLY EXCLUSIVE WITH VALUE

Reason:

The RECORD definition record input processor encountered both an OFFSET and a VALUE definition in the input for a field definition. Input processing is terminated.

Action:

OFFSET and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module:

CRLPRECP

CAS3039E

TYPE SPECIFICATION REQUIRED

Reason:

The RECORD definition record input processor did not encounter a TYPE specification for a record field definition. This is required. Input processing is terminated.

Action:

Supply a valid TYPE definition and retry the input process.

Module:

CRLPRECP

CAS3040E

ROW MUTUALLY EXCLUSIVE WITH OFFSET

Reason:

The RECORD definition record input processor encountered both a ROW and OFFSET definition in the input for a field definition. Input processing is terminated.

Action:

ROW and OFFSET are mutually exclusive. Remove the redundant keyword and retry the input process.

Module:

CRLPRECP

CAS3041E

COL MUTUALLY EXCLUSIVE WITH OFFSET

Reason:

The RECORD definition record input processor encountered both a COL and OFFSET definition in the input for a field definition. Input processing is terminated.

Action:

COL and OFFSET are mutually exclusive. Remove the redundant keyword and retry the input process.

Module:

CRLPRECP

CAS3042E

ROW/COL, OFFSET OR VALUE MUST BE SPECIFIED

Reason:

The RECORD definition record input processor requires that you specify one of the ROW/COL, OFFSET or VALUE keywords for each record field definition. None was supplied. Input processing is terminated.

Action:

Supply the appropriate keyword and retry the input process.

Module:

CRLPRECP

CAS3043E

ROW REQUIRES COL

Reason:

The RECORD definition record input processor found a ROW keyword with no COL keyword. Input processing terminates.

Action:

Supply a COL definition; retry.

Module:

CRLPRECP

CAS3044E

MAXIMUM NUMBER OF INPUT LINES, TERMINATING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3045E

CRLPRECP FUNCTION=TERM, INIT PROCESSING NOT PERFORMED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3046E

CRLPRECP FUNCTION=TERM, NO PROCESS REQUESTS PERFORMED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3047E

KEYWORD=VALUE, DATA NOT VALID FOR TYPE SPECIFIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3048E

CRLPRECP FUNCTION=TERM, SECURITY HEADER LENGTH IS TOO BIG

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3049E

CRLPRECP FUNCTION=TERM, OBJECT BUFFER ADDRESS IS REQUIRED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3050E

CRLPRECP FUNCTION=TERM, OBJECT BUFFER LENGTH IS REQUIRED OR INVALID

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3051E

CRLPRECP FUNCTION=TERM, OBJECT BUFFER IS TOO SMALL

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECP

CAS3052E

DUPLICATE FIELD NAMES FOUND

Reason:

The RECORD definition record input processor found the FLDNAME names of two or more record fields identical. Input processing terminates.

Action:

All field names must be unique. Remove the duplicate field definition or assign a unique name to the duplicate field; retry.

Module:

CRLPRECP

CAS3053E

RECNAME MUST BE 24 CHARACTERS OR LESS IN LENGTH

Reason:

The RECORD definition record input processor found the RECNAME name longer than the allowable 24 characters. Input processing terminates.

Action:

Supply a valid RECNAME name; retry.

Module:

CRLPRECP

CAS3054E

NO CLOSING PARENTHESIS FOUND FOR KEYWORD=RECNAME

Reason:

The RECORD definition record input processor determined that the RECNAME name specification did not end with a closing parenthesis. Input processing is terminated.

Action:

Correct the input data to supply valid RECNAME data and retry the input process.

Module:

CRLPRECP

CAS3055E

DUPLICATE VALUE SPECIFICATION

Reason:

The RECORD definition record input processor encountered a duplicate VALUE keyword for a definition of a field. Input processing is terminated.

Action:

Remove the duplicate VALUE specification from the input data and retry the input process.

Module:

CRLPRECP

CAS3056E

INVALID SKIP VALUE SPECIFICATION

Reason:

An invalid SKIP parameter was entered. The valid values are NO or YES.

Action:

Correct the input stream and retry the input process.

Module:

CRLPRECP

CAS3057E

INVALID VALUE SPECIFICATION

Reason:

The RECORD definition record input processor encountered a VALUE keyword without data. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPRECP

CAS3058E

INVALID FLDNAME VALUE SPECIFICATION

Reason:

The RECORD definition record input processor encountered a FLDNAME keyword without data. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPRECP

CAS3059E

INVALID TYPE VALUE SPECIFICATION

Reason:

The RECORD definition record input processor found a TYPE keyword without data. Input processing terminates.

Action:

Correct the input data and retry the input process.

Module:

CRLPRECP

CAS3060E

SUPPLIED FLDNAME IS TOO BIG

Reason:

The RECORD definition record input processor found a FLDNAME name longer than 24 characters. Input processing terminates.

Action:

Supply a valid FLDNAME name and retry the input process.

Module:

CRLPRECP

CAS3101E

CRLPRECL INVOKED FOR ILLEGAL FUNCTION

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECL

CAS3102E

CRLPRECL INVOKED FOR UNSUPPORTED RECORD TYPE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECL

CAS3103E

MISSING OR INVALID TYPE DEFINED IN RECORD

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPRECL

CAS3126E

SUPPLIED DATA BUFFER EXCEEDS MAXIMUM SIZE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3127E

DATA IS REQUIRED FOR KEYWORD

Reason:

This EXPRESSN definition keyword requires data; no data was found.

Action:

EXPRESSN input processing terminates; correct error and retry.

Module:

CRLPEXPP

CAS3128E

REQUIRED KEYWORD NOT FOUND

Reason:

EXPRESSN definition processor cannot locate the EXPRESSN keyword. Input processing is terminated.

Action:

Check your input statements for correctness and retry the input process.

Module:

CRLPEXPP

CAS3129E

INVALID KEYWORD FOUND

Reason:

The EXPRESSN definition input processor encountered an unknown keyword in the input data. Input processing is terminated.

Action:

Check your input data for correctness and retry the input process.

Module:

CRLPEXPP

CAS3130E

CRLPEXPP INVOKED FOR ILLEGAL FUNCTION

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3131E

CRLPEXPP INVOKED FOR INCORRECT RECORD TYPE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3132E

CRLPEXPP FUNCTION=INIT, NO SOURCE BUFFERS SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3133E

CRLPEXPP FUNCTION=INIT, NO SOURCE BUFFER LENGTH SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3134E

CRLPEXPP FUNCTION=PROCESS, NO INPUT BUFFER SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3135E

CRLPEXPP FUNCTION=PROCESS, NO INPUT BUFFER LENGTH SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3136E

CRLPEXPP FUNCTION=PROCESS, INIT PROCESSING NOT PERFORMED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3137E

MAXIMUM NUMBER OF INPUT LINES, TERMINATING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3138E

CRLPEXPP FUNCTION=TERM, INIT PROCESSING NOT PERFORMED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3139E

CRLPEXPP FUNCTION=TERM, NO PROCESS REQUEST PERFORMED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3140E

CRLPEXPP FUNCTION=TERM, SECURITY HEADER LENGTH IS ZERO

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3141E

CRLPEXPP FUNCTION=TERM, SECURITY HEADER LENGTH IS TOO BIG

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3142E

CRLPEXPP FUNCTION=TERM, OBJECT BUFFER ADDRESS IS REQUIRED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3143E

CRLPEXPP FUNCTION=TERM, OBJECT BUFFER LENGTH IS REQUIRED OR INVALID

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3144E

CRLPEXPP FUNCTION=TERM, OBJECT BUFFER IS TOO SMALL

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPP

CAS3145E

NO INPUT DATA SUPPLIED

Reason:

The EXPRESSN definition input processor encountered no input data. Input processing is terminated.

Action:

Supply valid input data and retry the input process.

Module:

CRLPEXPP

CAS3146E

NO IF STATEMENT FOUND

Reason:

The EXPRESSN definition input processor encountered no input IF statement. Input processing is terminated.

Action:

Supply valid input data and retry the input process.

Module:

CRLPEXPP

CAS3158E

EXPRESSN NAME MUST CONTAIN VALID ALPHANUMERIC CHARACTERS

Reason:

The EXPRESSN record name is invalid.

Action:

Supply valid input data and retry the input process.

Module:

CRLPEXPP

CAS3201E

CRLPEXPL INVOKED FOR ILLEGAL FUNCTION

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPL

CAS3202E

CRLPEXPL INVOKED FOR UNSUPPORTED RECORD TYPE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPL

CAS3203E

MISSING OR INVALID LOGICAL OPERATOR FOR EXPRESSN RECORD

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPL

CAS3204E

NO FSDTE ENTRIES EXIST FOR EXPRESSN RECORD

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEXPO

CAS3213E

DEB: 00@@@@@@ JFCB: @@@@@@@@ UCB: @@@@@@@@ Seek: @@@@@@@@@@@@

Reason:

The three messages listed previously are issued any time an I/O error occurs when accessing the PDS directory (that is, an I/O error when CA Top Secret initially attempts to populate the dataspace, not an I/O error inside the user's application).

Action:

Contact CA Customer Support.

CAS3253E

EXPECTED OPERATOR NOT FOUND

Reason:

The EXPRESSN definition input processor was expecting a logical operator but did not encounter one. Input processing is terminated.

Action:

Check your input data for correct syntax and retry the input process.

Module:

CRLPEPOL

CAS3254E

INVALID NESTING OF PARENTHESIS

Reason:

EXPRESSN definition input processor found an illegal nesting of parenthesis. Input processing is terminated.

Action:

Check for odd number of parentheses. Correct and retry.

Module:

CRLPEPOL

CAS3255E

EXPECTED OPERATOR/SYMBOL NOT FOUND

Reason:

The EXPRESSN definition input processor expected an operator or symbol but did not encounter either. Input processing is terminated.

Action:

Check your input data for correct syntax and retry the input process.

Module:

CRLPEPOL

CAS3301E

OPERATOR EVALUATION ROUTINE UNDEFINED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPERSL

CAS3302E

INVALID CONSTANT TYPE

Reason:

The EXPRESSN definition input processor encountered an invalid constant or literal specification for a right hand side (RHS) value. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPERSL

CAS3303E

INVALID NUMERIC CONSTANT - EXCEEDS MINIMUM/MAXIMUM RANGE

Reason:

The EXPRESSN definition input processor encountered an invalid binary constant value that did not fall into the proper range of values for such operands. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPERSL

CAS3304E

INVALID DECIMAL CONSTANT

Reason:

The EXPRESSN definition input processor encountered an invalid binary constant value that did not contain valid numeric digits. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPERSL

CAS3305E

INVALID HEX CONSTANT

Reason:

The EXPRESSN definition input processor encountered an invalid hex constant value that did not contain valid hex digits. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPERSL

CAS3306E

ODD LENGTH HEX CONSTANT

Reason:

The EXPRESSN definition input processor encountered an invalid hex constant value that did not contain an even number of hex digits. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPERSL

CAS3307E

INVALID OPERATOR/OPERAND TYPES

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPERSL

CAS3308E

INTERNAL ERROR - INVALID TYPE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPERSL

CAS3309E

INTERNAL ERROR - INVALID PSCANX

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPERSL

CAS3310E

INTERNAL ERROR - INVALID OPERATOR TYPE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPERSL

CAS3321E

PDS INTERCEPTS NOT INSTALLED

Reason:

CAS3TRCE or CAS3STAT has been run but the PDS security component has never been initialized.

CAS3322E

MISSING OR INVALID PARAMETERS: %%%%%%%%%%%%%%%%

Reason:

CAS3TRCE has been run with an invalid parameter.

CAS3350I

TRACE STATUS - GENERAL: %%% CCW: %%% MEM: %%% SEC: %%%

Reason:

This message displays the status of various trace points. To enable these trace points, use the following parameters for CAS3TRCE:

- General: "TRACE=ON"—Basic trace messages
- CCW: "TRACE=CCW"—Detailed I/O trace
- Mem: "TRACE=MEM"—Member map manipulation
- Sec: "TRACE=SEC"—Only security calls

"TRACE=ALL" can be used to request all of the above options; "TRACE=OFF" can be used to suppress all tracing.

Action:

This message is for information only. No action is required.

Module:

CAS3352E

INTERNAL ERROR, INCORRECT FSDT NUMBER

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEFDT

CAS3362I

%%%%%%: %%%%%%%% TTR: @@@@@@ CCHHR: @@@@@@@@@@

Reason:

These messages display the status of the PDS member level protection component. Information displayed includes:

- Address and version information from the PSDDATA structure
- Overall system status (ACTIVE/INACTIVE)
- List of all modules loaded and their addresses
- Statistics and counts
- STOKEN, ALET, origin, and free space chain for the dataspace cache

For each protected PDS currently accessed: volser, data set name, creation date, last reference date, number of extents, total tracks allocated, last access record TTR, track balance, bytes used in last directory block, timestamp when last opened, allocated directory blocks, used directory blocks, member count, estimated maximum number of members that can be added

If tracing is enabled, a display of each member in the protected data set, and TTR and CCHHR of the first data record for the member.

CAS3363E

INTERNAL ERROR IN PSCANX STACK PROCESSING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEFDT

CAS3364E

INTERNAL ERROR ATTEMPTING TO POP PSCANX STACK

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPEFDT

CAS3401E

ILLEGAL OR INVALID EXPRESSN RECORD

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3402E

ERROR OCCURRED WHILE PERFORMING EVALUATION PROCESSING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3405E

ERROR EXTRACTING FILE DATA

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3406E

CRLPFILE FILE EXTRACT ROUTINE CANNOT BE LOCATED

Reason:

During evaluation of a logical expression the File extract processing routine could not be located during evaluation of a logical expression.

Action:

Evaluation processing is terminates. The host security system denied the access attempt. Have site management review their installation of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module:

CRLPFLDP

CAS3407E

CRLPSCRN SCREEN EXTRACT ROUTINE CANNOT BE LOCATED

Reason:

Screen extract processing routine could not be located during evaluation of a logical expression.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Have site management review their install of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module:

CRLPFLDP

CAS3408E

ERROR EXTRACTING SCREEN DATA

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3409E

CRLPCOMP LOGICAL COMPARATOR ROUTINE CANNOT BE LOCATED

Reason:

Logical comparison routine was not located during evaluation of a logical expression.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Have site management review their install of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module:

CRLPFLDP

CAS3410E

ERROR IN LOGICAL COMPARISON PROCESSING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3411E

CRLPMULT MULTIPLE EVALUATION ROUTINE CANNOT BE LOCATED

Reason:

Multiple comparison processing routine could not be located during evaluation of a logical expression.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Have management review their install of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module:

CRLPFLDP

CAS3412E

ERROR IN MULTIPLE EVALUATION PROCESSING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3413E

EXPRESSN RIGHT HAND SIDE (RHS) FIELD NOT FOUND

Reason:

During evaluation processing, the logical comparison routine could not locate the constant value defined as one of the right hand side values of the EXPRESSN record used. The cause might be something simple such as an error in defining the record field definitions in the appropriate RECORD definition record.

Action:

Evaluation processing terminated. The host security system denied the access attempt. Review the host security system logging and auditing mechanisms for information on the RECORD definition record and EXPRESSN record used during the evaluation. If the RECORD definition record has the field properly defined, ensure that your site properly made these definitions available for RLP processing.

Module:

CRLPFLDP

CAS3414E

EXPRESSN LEFT HAND SIDE (LHS) SYMBOLIC FIELD CANNOT BE A LITERAL

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3415E

EXPRESSN RIGHT HAND SIDE (RHS) SYMBOLIC FIELD CANNOT BE A SCREEN FIELD

Reason:

During evaluation processing the logical comparison routine determined that a symbolic right hand side definition naming a screen record field instead of a VALUE definition was specified. The comparison is illegal and disallowed.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Review the host security system logging and auditing mechanisms for information on the RECORD definition record and EXPRESSN record used in the evaluation process and use this information to correct the erroneous EXPRESSN or RECORD definition.

Module:

CRLPFLDP

CAS3416E

EXPRESSN RIGHT HAND SIDE (RHS) SYMBOLIC FIELD CANNOT BE A RECORD FIELD

Reason:

During evaluation processing the logical comparison routine determined that a symbolic right hand side definition naming a file record field instead of a VALUE definition was specified. The comparison is illegal and disallowed.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Review the host security system logging and auditing mechanisms for information on the RECORD definition record and EXPRESSN record used in the evaluation process and use this information to correct the erroneous EXPRESSN or RECORD definition.

Module:

CRLPFLDP

CAS3417E

EXPRESSN LEFT HAND SIDE (LHS) EXPLICIT ROW/COL SPECIFICATION IS INVALID

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3418E

EXPRESSN LEFT HAND SIDE (LHS) EXPLICIT ROW SPECIFICATION IS ZERO

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3419E

EXPRESSN LEFT HAND SIDE (LHS) EXPLICIT COL SPECIFICATION IS ZERO

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFLDP

CAS3451E

DATA BUFFER FOR EVALUATION IS TOO BIG

Reason:

During evaluation of an expression involving file record fields, the logical comparison routine determined that the size of the input file record exceeded the maximum size of 65535 bytes.

Action:

Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module:

CRLPFILE

CAS3452E

OFFSET FOR FIELD IS ZERO

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPFILE

CAS3453E

OFFSET FOR FIELD IS LARGER THAN BUFFER SIZE

Reason:

During evaluation of an expression involving file record fields, the logical comparison routine determined that the offset of a file record field was outside the range of the supplied file record.

Action:

Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module:

CRLPFILE

CAS3454E

FIELD NOT WITHIN RECORD BUFFER

Reason:

During evaluation of an expression involving file record fields, the logical comparison routine determined that a file record field started in the supplied file record, but ended outside of the supplied buffer.

Action:

Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module:

CRLPFILE

CAS3476E

DATA BUFFER FOR EVALUATION IS TOO BIG

Reason:

During evaluation of an expression involving screen record fields, the logical comparison routine determined that the size of the input file record exceeded the maximum size of 65535 bytes.

Action:

Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module:

CRLPSCRN

CAS3477E

OFFSET FOR FIELD IS ZERO

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPSCRN

CAS3478E

OFFSET FOR FIELD IS LARGER THAN BUFFER SIZE

Reason:

During evaluation of an expression involving screen record fields, the logical comparison routine determined that the offset of a screen record field was outside the range of the supplied screen record.

Action:

Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module:

CRLPSCRN

CAS3479E

FIELD NOT WITHIN RECORD BUFFER

Reason:

During evaluation of an expression involving screen record fields, the logical comparison routine determined that a screen record field started in the supplied screen record, but ended outside of the supplied buffer.

Action:

Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module:

CRLPSCRN

CAS3480E

COLUMN SPECIFIED WITHOUT ROW

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPSCRN

CAS3481E

ROW SPECIFIED WITHOUT COLUMN

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPSCRN

CAS3482E

ROW NUMBER USED EXCEEDS TERMINAL SIZE

Reason:

The logical comparison routine attempted to extract data from an input screen buffer during evaluation of an expression. The calling environment supplied the terminals with physical characteristics and the input screen buffer. The ROW number used in the evaluation processing exceeded the physical capability of the input terminal.

Action:

Evaluation processing terminated. The host security system denied the access attempt. Review your site's use of record level protection controls for screen input protection. Verify that these controls match the physical capabilities of the terminals.

Module:

CRLPRECP

CAS3483E

COL NUMBER USED EXCEEDS TERMINAL SIZE

Reason:

The logical comparison routine attempted to extract data from an input screen buffer during evaluation of an expression. The calling environment supplied the terminals with physical characteristics and the input screen buffer. The COL number used in the evaluation processing exceeded the physical capability of the input terminal.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Review your site's use of record level protection controls for screen input protection. Verify that these controls match the physical capabilities of the terminals.

Module:

CRLPRECP

CAS3484E

DATA AT ROW/COL VECTOR NOT FOUND

Reason:

The logical comparison routine attempted to extract data from an input screen buffer at a specific screen location during evaluation of an expression. The screen extractor could not locate data for the specified vector.

Action:

Evaluation processing is terminated. The host security system denied the access attempt. Review your site's use of record level protection controls for screen input protection. Verify that these controls match the physical capabilities of the terminals.

Module:

CRLPRECP

CAS3486E

MISSING OR ILLEGAL AID VALUE SUPPLIED

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPSCRN

CAS3501E

ILLEGAL LHS DATA TYPE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPCOMP

CAS3502E

ILLEGAL LOGICAL OPERATOR IN FSDTE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPCOMP

CAS3503E

ERROR WHILE PERFORMING COMPARISON PROCESSING

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPCOMP

CAS3504E

MISMATCHED LENGTHS FOR HEX COMPARISON

Reason:

During evaluation of an expression that involved two hex fields, the logical comparison routine determined that the length values for the LHS and RHS fields was not equal. When comparing a hex field to a hex constant or literal, both lengths must match.

Action:

Evaluation processing is terminated. The host security system denied the access. Review the host security system's logging and auditing mechanisms for assistance in finding the mismatched comparison.

Module:

CRLPCOMP

CAS3526E

ILLEGAL LOGICAL OPERATOR FOUND IN FSDTE

Reason:

An internal error occurred. Input processing is terminated.

Action:

Contact CA Technical Support.

Module:

CRLPMULT

CAS3551E

INVALID QUOTED STRING

Reason:

The EXPRESSN definition input processor encountered an invalid quoted string that did not end with a closing quote. Input processing is terminated.

Action:

Correct the input data and retry the input process.

Module:

CRLPESCN

CAS40 PDS Member-Level Protection Messages

CAS4001I

PDS member level protection component initializing

Reason:

Startup message from CAS4INIT

Action:

This message is for information only. No action is required.

CAS4002I

PDS member level protection initialized with RC = @@@@

Reason:

Startup message from CAS4INIT. If RC > 0, then a problem has occurred during initialization. See other messages for specific problem.

Action:

This message is for information only. No action is required.

CAS4003I

Global data area = @@@@@@@@

Reason:

Issued during startup if tracing is enabled. Shows the address of the CSA resident "PDSDATA" structure.

Action:

This message is for information only. No action is required.

CAS4004I

Common dataspace initialized

Reason:

Issued during startup if tracing is enabled. Shows that a SCOPE=COMMON dataspace has been built.

Action:

This message is for information only. No action is required.

CAS4005I

Installed %%%%%%%% at @@@@@@@@

Reason:

Issued during startup if tracing is enabled. Shows the address of each module loaded.

Action:

This message is for information only. No action is required.

Module:

CAS4010E

Error: Can't initialize %%%%%%%%

Reason:

Issued during startup if unable to load a module (%%%%%%%% = module name).

CAS4011E

Service: %%%%%%%% RC: @@@@@@@@

Reason:

Issued during startup if an OS/390 service returns with an error. %%%%%%%% = name of service invoked (ALESERV, DSPSERV, ...) and @@@@@@@@ = return value.

CAS4012E

Unable to locate module CAILPAM. Initialization terminated.

Reason:

The module CAILPAM (provided by CA Common Services) was not found in the standard module search sequence (TASKLIB,STEPLIB,JOBLIB,LNKLST).

Action:

Since STEPLIB/JOBLIB is not permitted for the CA Top Secret started task, the library containing module CAILPAM must be placed in the system linklist.

Module:

CAS4INIT

CAS4205E

PDS initialization failure: *<error description>*

Reason:

Issued upon encountering an error before attempting to read a PDS directory into the dataspace cache. <*error description*> can be:

- CVAF error—Cannot read a VTOC record
- Parameter error—User passed invalid DCB
- DEVTYPE error—Cannot obtain device parameters
- No memory—Insufficient memory
- No cells—Insufficient memory

CAS4210E

PDS directory error: <error description>

Reason:

Issued if a logical error exists within a PDS directory. <*error descriptio*n> can be:

- Invalid format—Wrong length directory block, invalid record key, or record not in proper sequence.
- IECPCNVT TTR error—An untranslatable TTR has been encountered by IECPCNVT.
- I/O error—An I/O error occurred while reading a directory block.
- Member miscount—Internal error
- Dataspace allocation—The SCOPE=COMMON dataspace is full or has been corrupted.

CAS4211E

EXCP error: ECB:@@@@@@@@ Sense: @@@@ CSW: @@@@@@@@ @@@@@@@@

CAS4212E

Vol: %%%%%% DSN: %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

CAS4213E

DEB: 00@@@@@@ JFCB:@@@@@@@@ UCB:@@@@@@@@ Seek: @@@@@@@@@@@@

Reason:

The above three messages are issued any time an I/O error occurs while accessing the PDS directory (that is, an I/O error when we initially attempt to populate the dataspace; not an I/O error inside the user's application).

CAS4250E

%%%% Access to Protected PDS Member Denied. SAF RC @@/@@

CAS4251E

DSN: %%%

CAS4252E

Vol: %%%%%% Pgm: %%%%%%%% Class: %%%%%%%%

Reason:

The above three messages are issued any time a security violation occurs when accessing a protected PDS member. The task which generates this message will be subsequently failed with a 913 abend. Data displayed includes:

- Attempted access level
- SAF return and reason codes
- Data set name accessed
- Volume that the dataset resides on
- Program in control
- Class name in which resource check was performed

CAS4260E

CCW parse error during EXCP/EXCPVR

Reason:

The user has generated an invalid channel program

CAS4270W

%%%% storage not freed: SP=@@ Len=@@@@ Addr=@@@@@@@@

Reason:

A STORAGE RELEASE request has failed for the named area. Processing continues.

CAS4295E

R0: @@@@@@@@ R1: @@@@@@@@ R2: @@@@@@@@ R3: @@@@@@@@

CAS4296E

R4: @@@@@@@@ R5: @@@@@@@@ R6: @@@@@@@@ R7: @@@@@@@@

CAS4297E

R8: @@@@@@@@ R9: @@@@@@@@ RA: @@@@@@@@ RB: @@@@@@@@

CAS4298E

RC: @@@@@@@@ RD: @@@@@@@@ RE: @@@@@@@@ RF: @@@@@@@@

CAS4299E

%%%%%%%% PDS Abend @@@@: PSW = @@@@@@@@ @@@@@@@@ Offset: +@@@@

Reason:

The above five messages are issued should an abend occur in a PDS module. In most instances, a dump will be written to a system dump dataset.

CAS430E

Sign data cleanup failed RC: *rtncode* RSN: *rsncode* E-RC: *PKI rtncode*

Reason:

An internal error occurred during sign data cleanup processing.

Action:

Contact CA Technical Support.

CAS4300I

Utility complete: RC = @@@@

Reason:

The CAS4STAT or CAS4TRCE utilities have completed.

Action:

This message is for information only. No action is required.

CAS4310E

Utility error: %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Reason:

An internal error has occurred within CAS4TRCE or CAS4STAT.

Action:

Contact CA Technical Support.

CAS4321E

PDS Intercepts not installed

Reason:

CAS4TRCE or CAS4STAT has been run, but the PDS security component has never been initialized.

CAS4322E

Missing or invalid parameters: %%%%%%%%%%%%%%%%

Reason:

CAS4TRCE has been run with an invalid parameter

CAS4350I

Trace status - General: %%% CCW: %%% Mem: %%% Sec: %%%

Reason:

Displays status of various trace points. To enable these trace points, here are the proper parameters to CAS4TRCE:

General	TRACE=ON	Basic trace messages
CCW	TRACE=CCW	Detailed I/O trace
Mem	TRACE=MEM	Member map manipulation
Sec	TRACE=SEC	Only security calls

TRACE=ALL can be used to request all of the above options; TRACE=OFF can be used to suppress tracing.

Action:

This message is for information only. No action is required.

CAS4351I

Status from global structure @@@@@@@@ @@@@ @@

CAS4352I

System %%%%%%%%, intercepts %%%%%%%%%%%%%%%%

CAS4353I

Module %%%%%%%% loaded at @@@@@@@@

CAS4354I

Statistics:

CAS4355I

$$$$$$$ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

CAS4356I

Dataspace cache STKN @@@@@@@@@@@@@@@@ ALET @@@@@@@@

CAS3357I

Cache index origin: @@@@@@@@ Free space origin: @@@@@@@@

CAS4358I

Vol: %%%%%% DSN: %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

CAS4359I

Credt: @@@@@@ Refdt: @@@@@@ Extents: @@ Tracks @@@@

CAS4360I

LSTAR: @@@@@@@@ Trbal: @@@@ BDB: @@ TOD: @@@@@@@@@@

CAS4361I

Dir-A: $$$$$$ Dir-U: $$$$$$ Members: $$$$$$ Maxmem: $$$$$$

CAS4362I

%%%%%%: %%%%%%%% TTR: @@@@@@ CCHHR: @@@@@@@@@@

Reason:

Displays status of the PDS member level protection component. Information displayed includes:

- Address and version information from the PDSDATA structure.
- Overall system status (ACTIVE/INACTIVE).
- List of all modules loaded and their addresses
- Statistics and counts.
- STOKEN, ALET, origin and free space chain for the dataspace cache.
- For each protected PDS currently accessed: volser, dataset name, creation date, last reference date, number of extents, total tracks allocated, last accessed record TTR, track balance, bytes used in last directory block, timestamp when last opened, allocated directory blocks, used directory blocks, member count, estimated maximum number of members that can be added.
- If tracing is enabled, a display of each member in the protected dataset, along with TTR and CCHHR of the first data record for the member.

Action:

This message is for information only. No action is required.

CAS4365W

WARNING: No entries in dataspace cache

Reason:

Issued during status display if no data sets have been accessed since startup.

Action:

This message is for information only. No action is required.

CAS4401I

Shutdown in progress

Reason:

The CAS4TERM utility is about to shut down PDS protection.

Action:

This message is for information only. No action is required.

CAS4402I

Termination complete: RC = @@@@

Reason:

The CAS4TERM utility is finished disabling PDS protection.

Action:

This message is for information only. No action is required.

CAS4403E

Can’t shutdown - was never initialized

Reason:

CAS4TERM was run to shut down PDS protection, but it had never been initialized.

CAS4413E

Shutdown permission not granted

Reason:

CAS4TERM was run to shut down PDS protection, but the user does not have the proper authority to the CAPDSSEC.TERM resource in the FACILITY class.

Diagnostic Messages

The following are diagnostic messages only; they are only generated if tracing is enabled.

CAS4800D

DEBD Delete/Purge for DEB = 00@@@@@@’

Reason:

CLOSE has been issued for the DEB at the address shown.

CAS4801

D DEBK %%%%%%%% @@/@@@@@@@@@@/@@@@@@ %%%%%%%%%%%%%%%%%%%%%%

Reason:

Issued during OPEN for a protected dataset. Shows: DDNAME, number of extents, CCHHR of 1st extent, DEB flag settings (DEBOFLGS, DEBOPATB, DEBFLGS1), and the dataset name.

CAS4802D

%%%% @@@@@@@@ - %%%%%%%% %%%%%%%% in %%%%%%%%%%%%

Reason:

Issued during BLDL/FIND/STOW for protected dataset. Shows: function (BLDL/FIND/STOW), TTR, DDNAME, member name and the dataset name.

CAS4803D

SEC: A:%%%% C:%%%%%%%% V:%%%%%% D:%%%%%%%%%%%%%%%%%%%%%%%%%%

Reason:

Trace message prior to issuing resource checks. Shows: Access level, Class, Volume and Dataset.

CAS4804D

SEC: C:%%%%%%%% E:%%%%%%%% P:%%%%%%%% A:@@ RC:@@

Reason:

Trace message after resource check. Shows: Class, Entity (<BYPASS>, <DIR> or member name), Program in control, Access level (ATTR) and RC.

CAS4805D

DIRV Reload triggered by %%%%%%%% now at @@@@@@

Reason:

A protected dataset has been updated and the named member is at a location that disagrees with that in the dataspace cache. The dataspace cache will be refreshed.

CAS4806D

DIRU Unbind complete for %%%%%%%%%%%%%%%%%%%%%%%%

Reason:

A protected dataset has been closed, and the dataspace cache information describing it has been marked as eligible for release.

CAS4807D

DIRB Using cached entry at @@@@@@@@

Reason:

A protected dataset has been opened and a current map has been found in the data space cache.

CAS4808D

DIRB $$$$ Members - $$$$ Dirblks, $$$$ Used

Reason:

Issued after directory has been populated into the dataspace cache. Shows number of members found and a count of directory blocks allocated versus used.

CAS4809D

ADDR @@@@@@@@@@@@-@@@@@@@@@@@@ %%%%%%%% @@@@@@@@@@@@-@@@@@@@@

Reason:

I/O is occurring to a protected dataset. Shows low and high disk addresses referenced by the channel program, access (Rd, Wr, Sk), whether EOF is honored, and the start/end addresses of the currently accessible area of the PDS.

CAS4810D

BPIO CCW @@@@@@@@: @@ @@@@@@ @@ @@@@ @@@@@@@@@@@@:@@@@@@@@ @@

Reason:

I/O is occurring to a protected dataset. Shows the CCW command code, buffer address, flags and length of each CCW in the user's channel program. Only produced if "TRACE=CCW" is specified to CAS4TRCE.

CAS4811D

BPIO IOB @@@@@@@@: @@@@@@@@@@@@@@@@ CCW: @@@@@@@@ DEB: @@@@@@

Reason:

I/O is occurring to a protected dataset. Shows user's IOB address, initial seek location, address of the channel program and address of the DEB.

CAS4812D

DEBK Installed I/O filter for %%%%%%%%

Reason:

An APF authorized program which performs EXCP level I/O has opened a protected dataset and will be monitored.

CAS4813D

DEBK %%%%%%%% $$$$ DEB: @@@@@@@@ SIO: @@@@@@@@ IOAWA: @@@@@@@

Reason:

A protected PDS is being accessed. Shows the DDNAME and the number of protected data sets (if the DDNAME represents a concatenation of multiple protected members), plus the addresses of the OS/390 DEB, the I/O filter intercept and initial work area.

CAS4814D

DEBK table error @@ during %%%%%%%%

Reason:

A non-critical error occurred adding a DEB address to an internal work area.

CAS4815D

GETM %%%%%%%% = @@@@@@@@@@@@ - @@@@@@@@@@@@

Reason:

A member name has been associated with the disk address being accessed during an I/O. Shows the member name and the starting/ending addresses for that member.

CAS4816D

DEBK Monitoring DCB for %%%%%%%%

Reason:

A program has specified certain QSAM options which can cause I/O to be issued to a protected dataset from within OPEN.

CAS4817D

GETM LSTAR/C: @@@@@@/@@@@@@@@@@@@ Members: $$$$

Reason:

The dataspace cache is being searched for a member associated with a particular disk address. Shown are the DS1LSTAR field from the DSCB (as both TTR and CCHHR) and a member count.

CAS4818D

OPEN DCB monitor complete

Reason:

A program has specified certain QSAM options which can cause I/O to be issued to a protected dataset from within OPEN and the OPEN has completed.

CAS4889D

PCCW Data Record ID: @@@@@@@@@@@@@@@@

Reason:

A CCW which specifies a record ID as an operand has been encountered (such as “SEARCH ID EQUAL”).

CAS4890D

ADDM Member: %%%%%%% TTRN: @@@@@@@@ CCHHR: @@@@@@@@@@@@@@

Reason:

The dataspace cache is being populated due to an OPEN of a protected PDS. Shows the member name plus TTR and CCHHR of the start of data for this member. Only shown if "TRACE=MEM" is specified to CAS4TRCE.

CAS41 Compliance Information Analysis Report Messages

CAS4100E

SQLCODE = sqlcode

Reason:

The CIA report issues this message when an error is detected during execution of native SQL code. sqlcode is the value of the SQL Return Code.

Action:

Analyze the database SQL return code for more detailed explanation of the error. Correct the SQL problem and rerun the report.

CAS4101E

Text: *sqlerrmc*

Reason:

The CIA report issues this message when an error is detected during execution of native SQL code. *sqlerrmc* is the value of the SQL Error Message Code.

Action:

See the previously issued message for SQL error code. Analyze the database SQL error code and message text for more detailed explanation of the error. Correct the SQL problem and rerun the report.

CAS4102E

Cursor Name: cursor_name

Reason:

The CIA report issues this message when an error is detected during execution of native SQL code. cursor_name is the name of the SQL cursor being processed in the CIA report.

Action:

See previously issued messages for action.

CAS4103E

parm_name must by Y or N

Reason:

The CIA report issues this message when an invalid input parameter value is detected. parm_name is the input parameter name. Valid values for this input parameter are the following: 'Y', 'y', 'N' or 'n'.

Action:

Correct the input parameter value and rerun the report.

CAS4104E

Invalid Parm Name = parm_name

Reason:

The CIA report issues this message when an invalid input parameter is detected. parm_name is the invalid input parameter name.

Action:

Double check the input parameters for any errors. Parm names must start in column 1. Correct the input parameter name and rerun the report.

CAS4105E

Invalid Parm Value = parm_value

Reason:

The CIA report issues this message when an invalid input parameter value is detected. parm_value is the invalid input parameter value.

Action:

Double check the input parameters for any errors. Parm values must start in column 10. Correct the input parameter value rerun the report.

CAS4106E

SYSID must be specified

Reason:

The CIA report issues this message when the SYSID input parameter is not specified.

Action:

Add the SYSID input parameter and rerun the report.

CAS4107E

LINECNT must be a number between 10 and 999999999999999999

Reason:

The CIA report issues this message when the LINECNT input parameter is invalid. LINECNT must be a valid number between 10 and 999999999999999999.

Action:

Correct the LINECNT input parameter and rerun the report.

CAS4108E

ERRORS FOUND - PROCESSING TERMINATED

Reason:

The CIA report issues this message when an error was detected during processing. CIA report execution terminates with RC =16.

Action:

Refer to previously issued message for action.

CAS4130E

RESOURCE value is too long

Reason:

The CIA report issues this message when the RESOURCE value specified is longer than 256 characters.

Action:

Correct the RESOURCE input parameter and rerun the report.

CAS4131E

RESOURCE was incorrectly specified

Reason:

The CIA report issues this message when the RESOURCE value specified is invalid. RESOURCE contains invalid data or no data was specified.

Action:

Correct the RESOURCE input parameter and rerun the report.

CAS4132E

RESOURCE must be specified

Reason:

The CIA report issues this message when the RESOURCE input parameter is not specified and is required to run this report.

Action:

Add the RESOURCE input parameter and rerun the report.

CAS4133E

CLASS must be specified

Reason:

The CIA report issues this message when the CLASS input parameter is not specified and is required to run this report.

Action:

Add the CLASS input parameter and rerun the report.

CAS4134E

INVALID DATASET NAME

Reason:

The CIA report issues this message when it fails to parse the high level qualifier of the RESOURCE input parameter for a DATASET.

Action:

Correct the RESOURCE and CLASS input parameters and rerun the report.

CAS4140W

USERNAME ignored because USERIDS is NO

Reason:

The CIA report issues this message when the USERNAME input parameter is specified and the USERIDS input parameter is missing. The USERNAME parameter is valid only when USERIDS is also specified. The parameter is ignored by the CIA report and execution resumes without interruption.

Action:

This message for informational purposes only. No action is required.

CAS4141W

VOLSER ignored because CLASS is not DATASET

Reason:

The CIA report issues this message when the VOLSER input parameter is specified for a resource that is not a DATASET. The VOLSER parameter is valid only for CLASS = DATASET. The parameter is ignored by the CIA report and execution resumes without interruption.

Action:

This message is for informational purposes only. No action is required.

CAS4142W

SPECIAL ignored because USERIDS is NO

Reason:

The CIA report issues this message when the SPECIAL input parameter is specified and the USERIDS input parameter is missing or is NO. The SPECIAL parameter is valid only when USERIDS is also specified. The parameter is ignored by the CIA report and execution resumes without interruption.

Action:

This message is for informational purposes only, no action is required.

CAS4150E

One of the following parameters must be specified: GLOBALID, USERID or ROLE

Reason:

The CIA report issues this message when a required input parameter is missing. One of GLOBALID, USERID or ROLE is required to be specified to run the CIA report.

Action:

Specify only one of GLOBALID, USERID or ROLE and rerun the report.

CAS4151E

Only one of the following parameters can be specified: GLOBALID, USERID or ROLE

Reason:

The CIA report issues this message when more than one of the parameters listed in the message are specified. Only one of GLOBALID, USERID or ROLE input parameter may be specified to run the CIA report.

Action:

Specify only one of GLOBALID, USERID or ROLE and rerun the report.

CAS4170E

Only one of the following parameters must be specified: USERID, GLOBALID, ALLUSERS or ALLGBLS

Reason:

The CIA report issues this message when more than one of the parameters listed in the message are specified. Only one of USERID, GLOBALID, ALLUSERS or ALLGBLS may be specified to run the CIA report.

Action:

Specify only one of USERID, GLOBALID, ALLUSERS or ALLGBLS and rerun the report.

CAS4171E

One of the following parameters must be specified: USERID, GLOBALID, ALLUSERS or ALLGBLS

Reason:

The CIA report issues this message when none of the parameters listed in the message are specified. One and only one of the following parameters must be specified: USERID, GLOBALID, ALLUSERS or ALLGBLS.

Action:

Specify only one of USERID, GLOBALID, ALLUSERS or ALLGBLS and rerun the report.

CAS4180E

Only one of the following parameters can be used: ROLE or ALLROLES

Reason:

The CIA report issues this message when ROLE and ALLROLES were both specified. Specify either ROLE or ALLROLES, but not both.

Action:

Specify either ROLE or ALLROLES, but not both, and rerun the report.

CAS4181E

One of the following parameters must be specified: ROLE or ALLROLES

Reason:

The CIA report issues this message when neither ROLE nor ALLROLES were specified. Either ROLE or ALLROLES must be specified.

Action:

Specify either ROLE or ALLROLES and rerun the report.

CAS4182E

POST-INSTALL JOB CIALINK FROM SAMPLIB WAS NOT RUN

Reason:

A user has submitted a CIA job that uses of the CAS4IAUx modules, but the post-install CIALINK job was not run and the DB2 runtime routines have not yet been linked into the modules.

Action:

The WLM-started DB2 started task aborts with a U203 ABEND. Run the CIALINK job to link the DB2 service routines into the CAS4IAUx modules before re-submitting the CIA request.

Module:

SAFIADB9

CAS4183E

RUN CIALINK BEFORE RERUNNING THIS JOB

Reason:

This message is issued in conjunction with CAS4182E to further document what must be done before CIA jobs can run successfully.

Action:

Run CIALINK.

Module:

SAFIADB9

CAS4184E

THIS PROGRAM WILL NOW ABEND U203

Reason:

Issued in conjunction with CAS4182E and CAS4183E to document that SAFIADB9 now aborts the DB2 workload started task since the required DB2 service routines have not been linked-in.

Action:

Run CIALINK before resubmitting the CIA request.

Module:

SAFIADB9

Chapter 4: TSSPAN Administration Panel Messages

The following messages display when an error is detected using the CA Top Secret Administration Panels.

TSSPAN8001I

KEY NOT SUPPORTED

TSSPAN8002I

HELP IS NOT AVAILABLE

TSSPAN8003E

FIELD ENTRY MUST BE “YES” OR “NO”

TSSPAN8100I

PRESS ENTER TO PROCESS REQUEST

TSSPAN8101W

NO HELP AVAILABLE FOR THIS FUNCTION

TSSPAN8102W

INVALID SELECTION SPECIFIED

TSSPAN8103W

THIS FUNCTION HAS NOT BEEN IMPLEMENTED

TSSPAN8104E

UNKNOWN OR INVALID COMMAND SPECIFIED

TSSPAN8105E

INVALID OR CONFLICTING OPTION SPECIFIED

TSSPAN8110E

FILED REQUIRED

TSSPAN8111E

CONFLICTING OPTION SPECIFIED

TSSPAN8112E

ACID NOT FOUND

TSSPAN8201E

INVALID ACID TYPE SPECIFIED

TSSPAN8202E

SPECIFIED OWNER CANNOT OWN TARGET ACID

TSSPAN8203E

TSS COMMAND ACTIVE; COMMAND LINE IGNORED

TSSPAN8204E

SUSPEND OR EXPIRE MUST BE SELECTED

TSSPAN8205E

AT LEAST 1 RESOURCE MUST BE SELECTED

TSSPAN8206E

AT LEAST 1 ACID AUTH MUST BE SELECTED

TSSPAN8207E

AT LEAST 1 DATA AUTH MUST BE SELECTED

TSSPAN8208E

AT LEAST 1 MISC1 AUTH MUST BE SELECTED

TSSPAN8209E

AT LEAST 1 MISC2 AUTH MUST BE SELECTED

TSSPAN8210E

AT LEAST 1 MISC9 AUTH MUST BE SELECTED

TSSPAN8211E

INVALID DATE ENTERED

TSSPAN8212E

ONLY 1 OPTION CAN BE SELECTED

TSSPAN8213E

AT LEAST 1 OPTION MUST BE SELECTED

TSSPAN8214E

OPTION INVALID FOR CURRENT ENVIRONMENT

Chapter 5: CIA Unload Utility Messages

The following messages are displayed when an error is detected using the CA Top Secret CIA unload utility.

TSSC001E

USER DOES NOT HAVE AUTHORITY TO RUN THIS UTILITY

Reason:

The CA Top Secret CIA Unload Utility must be executed by the MSCA The CA Top Secret CIA Unload Utility terminates.

Action:

Have the MSCA run the CA Top Secret Unload Utility.

TSSC002E

ERROR OPENING INPUT FILE *file*

Reason:

The CA Top Secret CIA Unload Utility had a problem finding or opening the input file. The CA Top Secret CIA Unload Utility terminates.

Action:

Make sure that the input file was created and that the CA Top Secret CIA Unload Utility procedure JCL contains a DD statement for the input file.

TSSC003E

ERROR OPENING OUTPUT FILE *file*

Reason:

The CA Top Secret CIA Unload Utility had a problem finding or opening the output file. The CA Top Secret CIA Unload Utility terminates.

Action:

Make sure that the output file was created and that the CA Top Secret CIA Unload Utility procedure JCL contains a DD statement for the output file.

TSSC004E

BAD VALUE FOR INCOMING *parameter* PARAMETER.

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains an invalid parameter. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again

TSSC005E

GETMAIN FAILURE FOR getmain name (storage add .name) .

Reason:

TSSCIALD was unable to acquire sufficient amount of storage.

TSSC006E

BAD KEYWORD (*keyword)* FROM INCOMING PARAMETER FILE.

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a invalid keyword. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC007E

USER FIELD NOT DEFINED TO THE TOP SECRET FDT (*field name*).

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a user-defined field that is not defined to the FDT. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again

TSSC008E

DUPLICATE FOR USER DEFINED FIELD (*field name).*

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a duplicate User Defined field name. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again

TSSC009E

BAD LENGTH FOR TYPE USER DEFINED FIELD (field name)

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a User Defined field with an invalid length for that type. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC010E

BAD VALUE (*value*) FOR KEYWORD (*keyword).*

Reason:

The input JCL in the SYSIN file for the CA Top Secret CIA Unload Utility contains a bad value for the keyword. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error and run the utility again.

TSSC011E

UNLOAD PROCESSING TERMINATED

Reason:

The problem is in the processing error message. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the error in the processing error message and run the utility again.

TSSC012E

RECORD LENGTH EXCEEDS THE MAXIMUM ALLOWED FOR USER DEFINED FIELDS

Reason:

You specified too many USERFIELD input control statements in the SYSIN input parameter file, which caused the variable record length for the USERUSER line in the UNLOAD process to exceed the maximum variable record length allowed for a line in the UNLOAD data set. The CA Top Secret CIA Unload Utility terminates.

Action:

Reduce the number of USERFIELD control statements in the SYSIN file and run the utility again. Make sure each record field specified in a USERFIELD control statement exists in the actual CA Top Secret FDT table for field definitions. Also, eliminate any duplicate field names in the USERFIELD control statements. There should not be more user-defined fields specified with USERFIELD control statements than actually exist in the FDT.

TSSC014E

SYNTAX ERROR IN PARAMETER FILE

Reason:

An input control statement in the SYSIN file for the CA Top Secret CIA Unload Utility contains a syntactical error. The CA Top Secret CIA Unload Utility terminates.

Action:

Specify a valid input control statement and run the utility again.

TSSC015E

BAD TYPE type FOR USER DEFINED FIELD field.

Reason:

An input control statement in the SYSIN file for USERFIELD of the CA Top Secret CIA Unload Utility contains bad field type. The CA Top Secret CIA Unload Utility terminates.

Action:

Correct the field type and run again.

TSSC016E

INCOMING PARAMETER SYSID CAN ONLY BE SPECIFIED ONCE.

Reason:

You specified the SYSID input control statement more than once in the SYSIN file.

Action:

Remove all occurrences, except for one, of the SYSID input control statement in the SYSIN file and run the utility again.

TSSC017E

INCOMING PARAMETER GLOBALID CAN ONLY BE SPECIFIED ONCE

Reason:

You specified the GLOBALID input control statement more than once in the SYSIN file.

Action:

Remove all occurrences, except for one, of the GLOBALID input control statement in the SYSIN file and run the utility again.

TSSC018E

INVALID FIELD NAME FOR GLOBAL IDMAP fieldname

Reason:

The field you specified the GLOBALID FIELD input control statement in the SYSIN file is not in the list of valid field or a valid User Defined Field.

Action:

Remove the GLOBALID FIELDS input control statement in the SYSIN file or find a valid field and run the utility again.

TSSC019E

NO GLOBALID VALUE WAS RETURNED FROM USER EXIT FOR ACID.

Reason:

The user exit module you specified in the EXIT keyword of the GLOBALID input control statement did not return any globalid value in the parameter list passed to it from the CA Top Secret CIA Unload Utility. The CA Top Secret CIA Unload Utility terminates.

Action:

Ensure that your GLOBALID user exit module returns a valid value in the parameter list passed to it from the CA Top Secret CIA Unload Utility, and rerun the utility.

TSSC020E

LOAD FAILED FOR USER EXIT exit name.

Reason:

The user exit module name specified in the EXIT keyword of the GLOBALID input control statement could not be located and loaded. The CA Top Secret CIA Unload Utility terminates.

Action:

Ensure that the user exit module exists in LPA and that the name is correct in the GLOBALID EXIT input control statement, and rerun the utility.

TSSC021E

INVALID FIELD LENGTH FOR GLOBAL IDMAP fieldname

Reason:

The GLOBALID FIELD you specified in the input control statement more Of the SYSIN file was longer than the maximum length allowed for the IDMAP field.

Action:

Remove the GLOBALID FIELDS input control statement in the SYSIN file or find a valid field and run the utility again.

TSSC022E

NO USER DEFINED FIELD DEFINED TO THIS SECURITY FILE FDT.

Reason:

You specified the USERFIELD input control statement in the SYSIN file and there are no User Defined Field defined to this security file.

Action:

Remove the USERFIELD input control statement in the SYSIN file and run the utility again.

TSSC023E

INTERNAL PROCESSING PROBLEM, REASON CODE xxxx.

Reason:

There was a internal processing error encounter which caused processing to terminate.

Action:

None.

TSSC024E

INCOMING PARAMETER FILTERSYSID CAN ONLY BE SPECIFIED ONCE

Reason:

You specified the FILTERSYSID input control statement more than once in the SYSIN file.

Action:

Remove all occurrences, except for one, of the FILTERSYSID input control statement in the SYSIN file and run the utility again.

TSSC060W

FIELD VALUE IS INVALID AS GLOBALID FOR ACID ACID.

Reason:

The field name specified in the FIELD keyword of the GLOBALID input control statement from which the globalid value is to be extracted, does not contain a value for the ACID currently being processed. ACID is the current ACID being processed. The CA Top Secret CIA Unload Utility continues processing using the current ACID as the globalid.

Action:

This message is a warning. No action is necessary.

TSSC050W

CFILE WAS NOT RUN BY A MSCA IT MAY BE AN INCOMPLETE FILE.

Reason:

The building of the input cfile for the CA Top Secret CIA Unload Utility was not run by the MSCA this file could possibly not be a full file.

Action:

This message is a warning. No action is necessary.

TSSC051W

TSSC051W - INVALID RECORD TYPE (*type*) FOR ACID (*acid*) ACID TYPE(*t*).

Reason:

The ACID type (prof,dept.,div….) is not allowed to have this kind of information on it.

Action:

This message is a warning. No action is necessary.

TSSC052W

BAD DATE OR DATE FORMAT IN RECORD REC # (*record*).

Reason:

The date on the record number is an invalid date or does not match the format for the cfile output.

Action:

This message is a warning. Check the ACID.

TSSC053W

BAD TIME OR TIME FORMAT IN RECORD REC # (*record*).

Reason:

The time for this record number is an invalid time.

Action:

This message is a warning. Check the ACID.

TSSC054W

BAD INTEGER VALUE FOR RECORD REC # (*record*).

Reason:

The integer is not a valid number on this record.

Action:

This message is a warning. Check the ACID.

TSSC055W

BAD TIME SHIFT RECORD REC # (*record*).

Reason:

The time shift record is incomplete or has a bad time value on it.

Action:

This message is a warning. Check the shift record.

TSSC056W

NO RESOURCE OWNERSHIP WAS FOUND FOR THIS PERMIT REC # (*record*).

Reason:

The ACID the a permit to a resource that is unowned.

Action:

This message is a warning. Check the ACID.

TSSC057W

BAD CALENDAR RECORD REC # (*record*).

Reason:

The calendar record is incomplete or has a bad month value on it.

Action:

This message is a warning. Check the calendar.

TSSC058W

BAD CONTINUATION IN RECORD REC # (*record*).

Reason:

The proceeding record was marked for continuation and this record is not a correct type of record for this continuation.

Action:

This message is a warning. No action is necessary.

TSSC061W

NO RESOURCE WAS FOUND FOR RESOURCE OWNER.

Reason:

The WHOOWNS command found a resource owner for a resource that does not exist.

Action:

This message is a warning. No action is necessary.

TSSC062W

EXPECTED DATA MISSING UNABLE TO TELL RECORD TYPE REC #

Reason:

While processing your unload file, there was an EIM record that did not have enough information specified to determine if this is a EIM or PROXY record type.

Action:

This message is for informational purposes only. No action is necessary.

TSSC100I

TSSC100I - SYSID (*sysid*) WAS SET FROM (*the system or parameter* file)

Reason:

Informational message telling where the CA Top Secret CIA Unload Utility is picking up the sysid from.

Action:

This message is for informational purposes only. No action is necessary.

TSSC101I

THE SYSID DOES NOT MATCH THE FILTER FOR INCOMING permit/facility REC# (record)

Reason:

The facilty or permit has a SYSID that does not match the FILTERSYSID. In the SYSIN file.

Action:

This message is for informational purposes only. No action is necessary.

TSSC102I

FILTER SYSID WAS SET FROM (the system or parameter file).

Reason:

Informational message telling where the CA Top Secret CIA Unload Utility is picking up the filter sysid from.

Action:

This message is for informational purposes only. No action is necessary.

Chapter 6: Detailed Reason Codes

Detailed reason codes (DRC) appear in CA Top Secret messages, TSSUTIL, and Diagnostic Traces. Each code represents a detailed explanation of the cause of a violation. This section is designed to explain the following:

- The detailed reason codes (in decimal and hexadecimal)
- The violation's corresponding message id
- The error message
- The corrective action

Reserved DRCs

The following DRC hexadecimal codes are reserved for internal error conditions:

- 27 through 29, 2B, 2D through 38
- 3A through 45, 4A, 4B
- 71, 72, 7C, 7D, 82, 83, 86, 87
- 89 through 8B, 8D

Reason:

An internal error condition was detected during security environment create or update processing.

Action:

Report the error to CA Technical Support for analysis. Retain a detailed log of system and security events surrounding the error in the event that additional diagnostic information is required.

Conventions

The following conventions apply to DRCs:

- The detailed reason codes are listed in *decimal* order.
- The hexadecimal number is in parenthesis following the decimal number.
- The applicable CA Top Secret user messages.

  Here is a sample entry:

001 (01) 7141 Use of ACID suspended

001

The decimal code number.

(01)

The hexadecimal code number.

7141

The violation message.

Each code is followed by a reason and, if appropriate, a user action for correcting the situation.

Detailed Reason: Codes

001 (01) 7141

Use of ACID suspended

Reason:

Check VTHRESH and PTHRESH control options for violation thresholds that result in automatic suspension of users.

Action:

TSS REMOVE(acid) SUSPEND

002 (02) 7175

Initiation failed by site security exit

Reason:

Your site security exit (TSSINSTX) determined that it was not valid for your job or session to initiate. Exit may have issued a message.

Action:

Determine the reason for the violation and correct the job.

003 (03) 7144

ACID not supplied on jobcard

Reason:

CA Top Secret could not derive an ACID for your batch job or STC.

Action:

Code USER= on the jobcard. Submit the job from a defined or authorized ACID. A default ACID could also be set up for the BATCH facility. The JOBACID control option can also be set to automatically generate the USER JOB operand.

004 (04) 7182

Facility deactivated by Administrator

Reason:

Administrator issued FACILITY(fac=INACTIVE) control option.

Action:

F TSS,FACILITY(fac=ACTIVE)

005 (05) 7140

ACID expired

Reason:

Authority to use ACID has lapsed.

Action:

TSS REMOVE(acid) FOR(1)

006 (06) 7161

Access to facility not authorized

Reason:

ACID does not have authority to use the accessed facility.

Action:

TSS ADDTO(acid) FACILITY(facility) will explicitly authorize acid to facility.

007 (07) 7102

Password missing

Reason:

ACID requires a password but it was not supplied.

Action:

Code PASSWORD= on jobcard; supply password with logon; supply password after STC prompt; submit job from defined or authorized ACID.

007 (07) 7102

Password phrase missing

Reason:

A password phrase was required but was not supplied.

Action:

Code PHRASE= on the RACROUTE macro or supply the password phrase in the appropriate field on the logon screen for the application that is being accessed.

008 (08) 7121

Password supplied with LOGON

Reason:

Via TSO (not TSO/E) logon, user entered “LOGON userid/password”

Action:

LOGON with userid only. Wait for CA Top Secret to prompt for your password. To allow a password with LOGON: F TSS,FACILITY(TSO=NOPROMPT)

009 (09) 7101

Password incorrect

Reason:

The password supplied for the ACID is not correct.

Action:

Specify correct password. If using multiple TSO password option, remember to use UADS password.

009 (09) 7101

Password phrase incorrect

Reason:

The password phrase supplied for the ACID is not correct.

Action:

Specify correct password phrase.

010 (0A) 7110

Password expired and new password missing

Reason:

The current password for the ACID has expired and is no longer valid.

Action:

Specify the new password according to the facility entry method.

010 (0A) 7110

Password phrase expired and new password phrase missing

Reason:

The current password phrase for the ACID has expired and is no longer valid.

Action:

Specify the new password phrase according to the facility entry method.

011 (0B) 7111

New password invalid.

Reason:

Supplied password does not follow the rules set via the NEWPW control option, is a restricted password, or the site exit has ruled it invalid.

Action:

Examine message TSS7111E for the specific reason. Change NEWPW control option.

011 (0B) 7111

New password phrase invalid.

Reason:

Supplied password phrase does not follow the rules set via the NEWPHRASE control option, or the site exit has ruled it invalid.

Action:

Examine message TSS7111E for the specific reason. Change NEWPHRASE control option.

012 (0C) 7181

Security inactive - end of day

Reason:

TSS terminated with “Z EOD” option. Normally, this requires an IPL.

Action:

F TSS,RESETEOD or re-IPL

013 (0D) 7130

Operator ID card required for logon

Reason:

The ACID has the OID attribute.

Action:

LOGON userid OID; then insert OID card when prompted.

014 (0E) 7131

Operator ID card invalid

Reason:

Using incorrect OID

Action:

May have to re-record OID by TSS REPLACE(acid) OID

015 (0F) 7251

New password reverify failed

Reason:

User incorrectly entered a password in response to a reverify request.

Action:

No action required.

016 (10) 7191

Cancellation due to excessive violations

Reason:

VTHRESH control option action is CANCEL.

Action:

Check/change the VTHRESH control option.

017 (11) 7153

Started task (STC) not defined to CA Top Secret

Reason:

A start command specified a procedure that is not associated with an ACID and the STC default is to FAIL undefined STCs.

Action:

TSS ADDTO(STC) PROCNAME(stcprocname) ACID(acid) will explicitly assign acid to the named PROCNAME.

018 (12) 7251

Access denied to IBMGROUP xxxxxx

Reason:

A signon specified a group to which the user does not have access.

Action:

If the signon should be allowed, make certain the user has access to the group specified as an IBMGROUP resource or by having a TYPE(GROUP) acid attached which matches the group name.

019 (13) 7192

Terminal locked up due to excessive violations

Reason:

User has caused too many violations and the terminal has become permanently locked. The user's ACID may also have been suspended.

Action:

Only SIGNOFF or LOGOFF is accepted. TSS REMOVE(acid) SUSPEND may also be required.

020 (14) 7172

Userid already in use elsewhere

Reason:

User is attempting to sign on twice in the same online region. Ability to do so is governed by: FACILITY(fac=SIGN(M)) or SIGN(S)

Action:

Check/change FACILITY(facility=SIGN(?)) or SIGN(?) control option.

021 (15) 7174

Division, Department, or Profile cannot be used

Reason:

Attempt to log on or run job using a Profile, Department, or Division ACID.

Action:

Use and ACID defined as TYPE(USER|DCA|VCA|ZCA|LSCA|SCA) for system entry.

022 (16) 7170

Protected JES reader or remote not authorized

Reason:

Job was submitted from RJE reader that is implicitly or explicitly protected, or ACID has ACTION(DENY).

Action:

TSS PERMIT(acid) TERMINAL(reader) explicitly authorizes acid to reader.

023 (17) 7180

Security inactive

Reason:

DOWN option specifies FAIL.

Action:

Check the status of CA-Top Secret and DOWN control option.

024 (18) 7142

ACID temporarily suspended

Reason:

Administrator has temporarily suspended the ACID.

Action:

TSS REMOVE(acid) ASUSPEND FOR (0)

025 (19) 7173

ACID not eligible for automatic terminal signon

Reason:

User attempted to perform automatic signon based upon terminal ID, and found that the ACID for the terminal had the NOATS attribute.

Action:

Sign on by specifying a valid ACID name and password.

026 (1A) 7171

Use of terminal or reader source not authorized

Reason:

ACID has SOURCE restrictions and this reader or terminal is not in the list.

Action:

TSS ADDTO/REMOVE(acid) SOURCE(reader)

027 (1B) 7120

Too many incorrect password/password phrase attempts

Reason:

Too many attempts were made at guessing the ACID's password/password phrase.

Action:

Check/change PTHRESH control option. May have to REMOVE the SUSPEND attribute from the user ACID, in order to reinstate security access for the user.

028 (1C) 7143

ACID inactive too long

Reason:

Attempt to use an ACID that has not been used for some time.

Action:

Check/change the INACTIVE control option.

TSS REPLACE(acid) PASSWORD(password)

029 (1D) 7132

Voice or image authentication failed

Reason:

Signon failed because voice or image did not match ACID.

Action:

Check CA Top Secret site installation exit message for details.

030 (1E) 9406

Internal reader - usually bad parameters

Reason:

Security driver passed invalid or incorrect parameters via the RACROUTE, RACINIT, RACHECK, or RACDEF SVCs.

Action:

If site-written code, check macro expansions. Check for invalid parameter list length. Ensure proper specification of MF=E versus MF=L and skeleton macros. Also check that the ACEE= parameter is present for multi-user address spaces.

031 (1F) 9406

Not authorized for function

Reason:

Security driver call does not have adequate authority.

Action:

If DUFXTR or DUFUPD: TSS ADDTO(acid) DUFXTR/DUFUPD. If RACINIT, program must be APF-authorized.

032 (20) 9407

RACF SVC classname unknown

Reason:

The type of security check is not defined to CA Top Secret.

Action:

If site-written code, check macro expansion for proper CLASS value or classname length. If IBM code, check for possible new IBM function. If installation-defined resource, it must be added to the RDT via a TSS command.

033 (21) 9407

Internal system error

Reason:

Abnormal condition or ABEND has occurred.

Action:

If site-written code, check macro expansion for proper values. Obtain dump and contact CA Technical Support.

034 (22) 9407

TSS command failed

Reason:

A logic error has occurred during RACROUTE REQUEST processing.

Action:

If problem persists, contact CA Technical Support.

035 (23) 9406

Cannot determine facility

Reason:

Site-written interface to support new facility. Program in control (TOP PRB) does not match the program (prefix key) in the matrix.

Action:

Check the facilities matrix entry via FACILITY(fac) control option. Change the program name via FACILTY(fac=PROGRAM=pgmname) to the first three letters of the program in control at the time the RACINIT macro is issued.

036 (24) 9406

Internal system error

Reason:

Abnormal condition or ABEND has occurred.

Action:

If site-written code, check macro expansion for proper values. Obtain dump and contact CA Technical Support.

037 (25) 9407

Error obtaining security record

Reason:

Abnormal condition or ABEND has occurred.

Action:

If site-written code, check macro expansion for proper values. Obtain dump and contact CA Technical Support.

038 (26) 7171

Integrity check

Reason:

The ACID (job or userid) cannot be used from this terminal or reader.

Action:

No action required. macro expansion for proper values. Obtain dump and contact CA Technical Support.

040 (28) 9403

Insufficient CSA or LSQA storage

Reason:

Not enough memory to initiate user.

Action:

Try again later.

042 (2A) 7111

Multiple password update has failed.

Reason:

The new password supplied is invalid.

Action:

Issue a valid new password and retry. See the message text for more information.

043 (2B) 9407

AREC has no password

Reason:

A logic error has occurred during RACROUTE request processing.

Action:

If problem persists, contact CA Technical Support.

044 (2C) 9403

Insufficient CSA or Local Storage

Reason:

CA Top Secret was unable to satisfy a cross-memory request due to insufficient EST or insufficient local storage.

Action:

If problem is insufficient CSA, enlarge CSA/ESCA site and IPL. In this case, the message will be issued by multiple address spaces at the same time.

If the problem is insufficient local storage, decrease the region size and restart the address space.

057 (39) 9015

Incorrect Customer Key

Reason:

A probable cause is that the Security File's Customer Encryption Key is not correct.

Action:

If CA-Top Secret Security File size was reduced or enlarged, check the TSSXTEND JCL. Contact CA Technical Support.

64 (40)

Write without ENQ

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

65 (41)

Invalid volser

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

67 (43) 9407

SFS I/O error

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

68 (44) 9407

SFS internal error

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

69 (45) 9407

SFS abend

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

070 (46) 7145

ACID not defined

Reason:

Specified ACID does not exit.

Action:

TSS CREATE(acid)...

Check default ACID value. If installation exit is generating ACID, then the value is not being built or returned correctly.

071 (47)

ACID already defined

Reason:

Attempt to define an ACID that is already defined to CA Top Secret.

Action:

Define the ACID using a different user ID.

072 (48)

ENQ Failure

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

076 (4C)

Invalid resource name/length

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

077 (4D)

Error doing backup

Reason:

An open/close error occurred during an attempt to access the backup file.

Action:

See accompanying TSS message for clarification.

078 (4E) 9700

DUF/EXTRACT FAILed - user has no (INST)DATA

Reason:

A DUFUPD, DUFXTR or EXTRACT request (RACHECK) failed because the specified ACID did not have INSTALLATION data.

Action:

No action required.

79 (4F)

The MAX size of SECREC has been exceeded

Reason:

The SECREC pointer for the ACID has exceeded the 256K maximum.

Action:

Move ownership of the target resource to a new ACID.

81 (51)

Volume not found

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

82 (52)

Volume not owned

Reason:

SFS logic error.

Action:

Contact CA Technical Support.

84 (54)

Volume already defined generically

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

85 (55)

Volume already defined

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

86 (56)

Volume prefix not owned

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

87 (57)

DSN/prefix not defined

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

88 (58)

DSN/prefix already defined

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

89 (59)

Prefix owned

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

90 (5A)

Resource already defined

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

91 (5B)

Resource not found

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

92 (5C)

Resource not owned

Reason:

Self-explanatory.

Action:

See accompanying TSS messages for clarification.

100 (64) 9707

TSS address space inactive

Reason:

A function cannot be performed because the Security File cannot be indirectly accessed.

Action:

Restart TSS started task.

101 (65) 7221

Data set not authorized

Reason:

A data set is protected by a defined data set prefix or by default, but the ACID does not have authority to access it.

Action:

Enter TSS ADDTO(acid) DSNAME(data set prefix) or TSS PERMIT(acid) DSNAME(dsname) or check for the DEFPROT control option.

102 (66) 7227

Data set accessed at unauthorized level

Reason:

ACID has been permitted data set access but not at the attempted level.

Action:

TSS PERMIT(acid) DSNAME(dsname) ACCESS(correct-access-level)

Perform TSS WHOHAS or LIST DATA(XAUTH) and look for conflicts. See the discussion of the Security Validation Algorithm in the *User Guide.*

103 (67) 7235

Global data set access is denied

Reason:

Access has been denied to the data set while using CA-TAPE, or an attempt was made to open a VSAM data set component (INDEX, DATA, and so on) without going through the CLUSTER.

Action:

To adjust data set access, see violation 101.

104 (68) 7232

FETCH-only library opened for other than read

Reason:

Data set is FETCH protected through ACCESS(FETCH) but an open was attempted for other than FETCH access.

105 (69) 7233

Unable to erase residual data

Reason:

A scratch operation was attempted and the AUTOERASE control option was set. CA-Top Secret could not overwrite the data set with binary zeroes.

Action:

Contact CA Technical Support.

106 (6A) 7225

Data set accessed with unauthorized program

Reason:

Data set access restricted via a privileged program or the program was not found in the library.

Action:

Check PERMIT(acid) DSNAME(dsname) PRIVPGM(pgmname) restrictions.

107 (6B) 7231

Job/step/task library invalid or present

Reason:

Data set access by program that did not come from authorized origin.

For PRIVPGM and no LIBRARY: task library (job or step) is present— check for STEPLIB or JOBLIB in JCL or in TSO LOGON procedure. Also check if CALL command is not allowed.

For PRIVPGM and LIBRARY: program did not come from task library— examine STEPLIB or JOBLIB in JCL or in TSO LOGON procedure. Or, library is not listed in PERMIT.

Action:

Check PERMIT(acid) DSNAME(dsn) PRIVPGM(pgm) restrictions. Check for/examine STEPLIB or TASKLIB.

108 (6C) 7234

Fetch violation

Reason:

An illegal I/O operation was attempted against a data set that was restricted with ACCESS(FETCH).

Action:

Check permissions or program.

109 (6D) 7226

Dataset access denied by installation exit

Reason:

Your security exit determined that access was illegal.

Action:

Check any site-issued violation message for reason of denial.

110 (6E) 7222

Dataset accessed at unauthorized time of day

Reason:

A DAY restriction is active for the data set.

Action:

TSS PERMIT(acid) DSNAME(dsname) DAYS(list-of-days)

111 (6F) 7223

Dataset accessed on unauthorized day of week

Reason:

A DAY restriction is active for the data set.

Action:

TSS PERMIT(acid) DSNAME(dsname) DAYS(list-of-days)

112 (70) 7224

Dataset accessed through unauthorized facility

Reason:

A facility restriction is active for the data set.

Action:

TSS PERMIT(acid) DSNAME(dsname) FACILITY(facility-list)

115 (73) 7206

Volume access denied by installation exit

Reason:

Your security exit determined that access was illegal.

Action:

Check any site-issued violation message for reason of denial.

116 (74) 7210

BLP access unauthorized

Reason:

Acid is not authorized to use BLP.

Action:

PERMIT acid to volume with ACCESS (BLP)

117 (75) 7201

Volume access not authorized

Reason:

An ACID tried to access a volume he or she was not authorized to access.

Action:

PERMIT acid to volume.

118 (76) 7221 Volume Not Available from this System

Reason:

An ACID is permitted access to a volume with a SYSID authorization disallowing the access.

Action:

An Administrator must authorize the ACID to the volume for the correct system via the TSS PERMIT function using the SYSID() parameter.

119 (77) 7207

Volume accessed at unauthorized (wrong) level

Reason:

A permitted volume has an access level restriction.

Action:

TSS PERMIT(acid) VOLUME(volser) ACCESS(level)

120 (78) 7208

Volume not available for dataset creation

Reason:

Data set cannot be created on this volume due to no permission or ACCESS(NOCREATE) restriction.

Action:

TSS PERMIT(acid/ALL) VOLUME(volser) ACCESS(CREATE)

121 (79) 7201

Tape volume error

Reason:

An ACID tried to access a tape volume he or she was not authorized to access.

Action:

Permit ACID to tape volume if necessary

122 (7A) 7209

Volume accessed without dataset specification

Reason:

A TAPEVOL or DASDVOL request was performed against a volume that only had ACCESS(CREATE) authority. A data set name was not passed with the request but is required for CREATE restrictions.

Action:

TSS PERMIT(acid) VOLUME(volser)

For volume backup/restore, use PRIVPGM as well.

123 (7B) 7228

Data Set Not Available from this System

Reason:

An ACID is permitted access to a data set with a SYSID authorization disallowing the access.

Action:

An administrator must authorize the ACID to the data set for the correct system via the TSS PERMIT function using the SYSID() parameter.

126 (7E) 7203

Volume accessed on unauthorized day of week

Reason:

Volume permission has a DAYS restriction.

Action:

TSS PERMIT(acid) VOLUME(volser) DAYS(days)

127 (7F) 7202

Volume accessed at unauthorized time of day

Reason:

Volume permission has a TIME restriction.

Action:

TSS PERMIT(acid) VOLUME(volser) TIMES(tt,tt)

Also check for time zone (TZONE) adjustments.

128 (80) 7204

Volume accessed through unauthorized facility

Reason:

Volume permission has a FACILITY restriction.

Action:

TSS PERMIT(acid) VOLUME(volser) FACILITY(facility)

129 (81) 7205

Volume access not allowed through this program

Reason:

Volume permission has a PRIVPGM restriction.

Action:

TSS PERMIT(acid) VOLUME(volser) PRIVPGM(pgmname)

132 (84) 7251

Minidisk not owned

Reason:

User is not allowed to access the minidisk.

Action:

TSS PERMIT(acid) VMMDISK (minidisk)

133 (85) 7251

No authorization for minidisk

Reason:

User is not allowed to access the minidisk.

Action:

TSS PERMIT(acid) VMMDISK (minidisk)

136 (88) 7251

Resource access denied

Reason:

CA Top Secret's authorization algorithm has denied access.

Action:

TSS PERMIT(acid)

140 (8C) 7250

IMS transaction denied - no password

Reason:

The attempted IMS transaction is password protected and the password was not supplied.

Action:

Supply password with the transaction as follows:

transid(password) ... data ...

142 (8E) 7250

IMS transaction denied - bad password

Reason:

An invalid password was supplied for the IMS transaction.

Action:

Supply valid password.

144 (90) 7256

Resource access denied by installation exit

Reason:

Your site exit denied access to the resource

Action:

Check for any site-issued violation message to determine cause.

145 (91) 7252

Resource accessed on unauthorized day of week

Reason:

Access denied to resource due to DAYS restriction.

Action:

TSS PERMIT(acid) resource DAYS(days)

Also check for time zone (TZONE) adjustments.

146 (92) 7253

Resource accessed at unauthorized time of day

Reason:

Access denied to resource due to TIME restriction.

Action:

TSS PERMIT(acid) resource TIME(tt,tt)

147 (93) 7194

Terminal locked

Reason:

Terminal activity denied due to previous TSS LOCK.

Action:

Unlock the terminal via TSS UNLOCK

148 (94) 7193

Terminal unlock failed

Reason:

TSS UNLOCK failed because the wrong password was entered.

Action:

Enter correct password for UNLOCK.

149 (95) 7255

Resource accessed by unauthorized program

Reason:

Wrong program was in control when resource was accessed.

Action:

TSS PERMIT(acid) resource(res) PRIVPGM(pgmname)

150 (96) 7254

Unauthorized facility for resource

Reason:

Resource not accessed from proper facility.

Action:

TSS PERMIT(acid) resource FACILITY(fac)

151 (97) 7257

Unauthorized access level for resource

Reason:

Permitted resource accessed with wrong level.

Action:

TSS PERMIT(acid) resource ACCESS(accesslevel)

152 (98) 7192

Terminal locked due to excessive violations

Reason:

Further use of terminal denied.

Action:

LOGOFF or SIGNOFF. Determine reason for violations and take corrective actions (PERMIT user or reprimand user). Check VTHRESH 2ontrol option.

153 (99) 7054

Security bypass active for this job or user

Reason:

Job or session will execute without security restrictions. This may also occur if jobs start while CA-Top Secret is reinitialized.

Action:

Check BYPASS control option for correctness. Check site security exit code for correctness.

154 (9A) 7254

ACID submission through wrong facility

Reason:

Submission was attempted but ACID has restriction set up by:

TSS PERMIT(acid) ACID(acid) FACILITY(fac)

Action:

Check permission restrictions.

155 (9B) 7255

ACID submission through wrong program

Reason:

Submission was attempted but ACID has restriction set up by:

```
TSS PERMIT(acid) ACID(acid) PRIVPGM(privpgm)
```

Action:

Check permission restrictions.

156 (9C) 7270

Job submission failed by installation exit

Reason:

Site security exit determined that the submission was illegal.

Action:

Check for site message giving reason for denial.

157 (9D) 7271

Job submission ACID not authorized

Reason:

Submitting ACID does not have authority to submit job with another ACID.

Action:

TSS PERMIT(acid) ACID(submit-ACID)

TSS ADDTO(acid) NOSUBCHK

158 (9E) 7258

Attempt to use restricted TSO command

Reason:

An attempt was made to use a TSO command that is not present in the ACIDs LCF list.

Action:

TSS ADDTO(acid) COMMANDS(TSO(cmd, cmd, ...))

159 (9F) 7258

Attempt to use restricted program

Reason:

A protected program cannot be used by the ACID.

Action:

TSS PERMIT(acid) PROGRAM(pgmname)

160 (A0) 7161

Facility not authorized during this time

Reason:

An attempt was made to log on to a facility at a restricted time.

Action:

Check FACILITY restrictions for the ACID.

161 (A1) 7162

Facility not authorized on this day

Reason:

An attempt was made to log on to a facility on a restricted day.

Action:

Check FACILITY restrictions for the ACID.

162 (A2) 219 (DB)

Internal TSS command codes

Action:

Provide CA Technical Support with dumps and/or trace/logs.

163 (A3) 7250

Port of ENTRY POE APPCPORT(poe) not authorized

Reason:

APPCPORT resource is owned and but is not PERMITted to user issuing APPC conversation request.

Action:

TSS PERMIT user to APPCPORT resource.

164 (A4) 7251

Access denied to JESJOBS

Reason:

JESJOBS resource is owned and but is not PERMITted to user issuing JESJOBS request.

Action:

This message is a result of a failed VERIFYX call in the JES address space. Please search the SYSLOG for the corresponding TSS7250E 151 TYPE=JESJOBS message for the same resource and permit the A=acid from the DRC 151 message to the JESJOBS resource.

165 (A5) 7251

Record (RLP) access denied.

Reason:

CA Top Secret has denied access to a record within a file. In CICS, it would be an FCT.

Action:

TSS PERMIT(acid) FCT(fctname) SELECT(selname)

166 (A6) 7251

Screen (SLP) access denied.

Reason:

CA Top Secret has denied access to a screen within CICS.

Action:

TSS PERMIT(acid) OTRAN(tranid) SELECT(selname) MAPREC(mapname)

167 (A7) 7163

Illegal facility for this system

Reason:

An attempt was made to log onto a facility on a restricted system.

Action:

Check the SYSID restrictions for the ACID.

168 (A8) 7259

RLP logic error--access denied to a record

Reason:

An internal logic error occurred within the RLP analyzer.

Action:

Contact CA Technical Support.

169 (A9) 7260

SLP logic error--access denied to a screen

Reason:

An internal logic error occurred within the SLP analyzer.

Action:

Contact CA Technical Support.

174 (AE) 324

Admin's ACID does not exist

Reason:

A TSS command has been send to another node using CPF but the ACID for the administrator issuing the command does not exist on the remote system.

Action:

Define administrator's ACID on the remote node.

178 (B2) 7105

User not authorized to SECLABEL

Reason:

At signon a user specified or was assigned a SECLABEL that the user is not authorized to use.

Action:

Add the SECLABEL to the user’s authorized list of seclabels.

179 (B3) 7221

DSN access denied: no SECLABEL

Reason:

A user attempted to access a dataset that was protected by a SECLABEL and the user does not have a SECLABEL.

Action:

Add the SECLABEL to the user's authorized list of seclabels.

180 (B4) 7251

RESOURCE access denied: no SECLABEL

Reason:

A user attempted to access a resource that was protected by a SECLABEL and the user does not have a SECLABEL.

Action:

Add the SECLABEL to the user's authorized list of seclabels.

181 (B5) 7221 - DSN SECLABEL verify failed

Reason:

A user attempted to access a dataset that was protected by a SECLABEL and the user's SECLABEL does not have MAC dominance over the dataset SECLABEL.

Action:

Add the SECLABEL to the user's authorized list of seclabels.

182 (B6) 7252

Resource SECLABEL verify failed

Reason:

A user attempted to access a resource that was protected by a SECLABEL and the user's SECLABEL does not have MAC dominance over the resource SECLABEL.

Action:

Add the SECLABEL to the user's authorized list of seclabels.

183 (B7) 7106

Subject Never Dominates

Reason:

A RACROUTE REQUEST=AUTH,STATUS=EVERDOM,... request was issued and the subject's SECLABEL never dominates the resource SECLABEL.

Action:

None.

197 (C5) 7101

User has no PW Phrase

Reason

A user specified a password phrase for signon, but there were no password phrases defined for the user acid.

Action

Have an administrator define a password phrase for the user ACID.

220 (DC)

Cross-memory communication failure

Action:

Provide CA with dumps and/or trace/logs.

DRC To Message Cross-Reference

This section summarizes CA-Top Secret Detailed Violation Codes, associated messages, and attributes. The table headings represent the following:

DRC CODE

Decimal code.

HEX CODE

Hexadecimal code.

TSS MSG

The CA-Top Secret user message number related to the violation.

SEC9 MSG

The summary violation message sent to the security console.

ATTRIBUTES

States code attributes, where:

- FAIL—The violation results in real denial of access in all security modes.
- FAILWARN—Like FAIL, except in all modes but DORMANT
- AUDIT—Violation is flagged as an audited event
- PASSWORD—Password violation that honors ARNPW controls
- NOVIOL—Do not treat as a violation

DRC attributes can be modified (for site customization) via the DRC control option.

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
001	01	7141	7100	AUDIT, FAILWARN	ACID suspended
002	02	7175	7100	AUDIT, FAILWARN	Initiation failed by site exit
003	03	7144	7100		ACID missing (from job card)
004	04	7182	7100	FAILWARN	Facility is inactive
005	05	7140	7100	FAILWARN	ACID access has expired
006	06	7160	7100		Cannot use this facility
007	07	7102	7100	PASSWORD	Password/password phrase is missing
008	08	7121	7100	NOVIOL	Password supplied with LOGON

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
009	09	7101	7100	PASSWORD, AUDIT	Incorrect password/password phrase
010	0A	7110	7100	PASSWORD	Password/password phrase has expired
011	0B	7111	7100	PASSWORD	New password/password phrase invalid
012	0C	7181	7100	FAILWARN	End-of-Day Access revoked
013	0D	7130	7100	FAILWARN, AUDIT	Operator ID card required
014	0E	7131	7100	AUDIT, FAILWARN, PASSWORD	Incorrect OID card
015	0F	7111	7100	PASSWORD	New password reverified incorrectly
016	10	7191	7100		VTHRESH (cancellation)
017	11	7153	7100		Undefined Started Task
018	12				
019	13	7192	7100	AUDIT	Terminal locked due to violations
020	14	7172	7100		Already signed on
021	15	7174	7100		Not a User, Control ACID
022	16	7170	7100		Reader is protected
023	17	7180	7100		TSS DOWN - cannot LOGON
024	18	7142	7100	FAILWARN	User still on vacation
025	19	7173	7100	AUDIT	NOATS
026	1A	7171	7100		Invalid source of submission
027	1B	7120	7100	AUDIT, FAILWARN	PTHRESH limit exceeded
028	1C	7143	7100	AUDIT, FAILWARN	ACID inactive too long
029	1D	7132	7100	AUDIT, FAILWARN, PASSWORD	Bad image
030	1E	9406	7100	AUDIT, FAILWARN	Invalid internal parameter passed
031	1F	9405	7100	AUDIT, FAIL	No authority for internal function
032	20	9410	7100	AUDIT, NOVIOL	classname unrecognized

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
033	21	9407	7100	AUDIT, FAILWARN	Internal system error or abend
034	22	9407	7100	AUDIT	TSS command failed
035	23	9406	7100	AUDIT, FAILWARN	Unknown Facility
036	24	9406	7100	AUDIT, FAILWARN	GETAR error
037	25	9407	7100	AUDIT, FAILWARN	Unable to obtain security record
038	26	7171	7100	AUDIT, FAIL	Internal integrity check failed
039	27				Reserved
040	28				
041	29				
042	2A	7111	7100	AUDIT, FAIL	SFS - MULTIPW PW update
043	2B	9407	7100	AUDIT, FAIL	SFS - AREC has no PW
044	2C	9403	7100	AUDIT, FAIL	No CSA for GETAR
045	2D				SFS - Internal error
046	2E				SFS - Internal error
047	2F				SFS - Internal error
048	30				SFS - Internal error
049	31				SFS - Internal error
050	32				SFS - Internal error
051	33				SFS - Internal error
052	34				SFS - Internal error
053	35				SFS - Internal error
054	36				SFS - Internal error
055	37				SFS - Internal error
056	38				SFS - Internal error
057	39				Incorrect customer key
058	3A				SFS - Internal error
059	3B				SFS - Internal error

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
060	3C				SFS - Internal error
061	3D				SFS - Internal error
062	3E				SFS - Internal error
063	3F				SFS - Internal error
064	40				SFS - Internal error
065	41				SFS - Invalid volser
066	42				SFS - Internal error
067	43	9407	7100		SFS - I, O error
068	44	9407	7100		SFS - Internal error
069	45	9407	7100		SFS - abend
070	46	7145	7100		ACID not defined
071	47				SFS - ACID already exists
072	48				SFS - Internal error
073	49				SFS - Internal error
074	4A				SFS - Invalid resource name length
075	4B				SFS - Internal error
076	4C				SFS - Internal error
077	4D				SFS - Error during backup
078	4E	9700	900	NOVIOL	ACID has no INSTDATA for DUF.
079	4F	0473E			SFS - Internal error
080	50				SFS - Internal error
081	51				SFS - Volume not found
082	52				SFS - Volume not owned
083	53				SFS - Volume not owned
084	54				SFS - Volume already defined
085	55				SFS - Volume already defined
086	56				SFS - Volume prefix not owned
087	57				SFS – DSNAME/prefix not defined
088	58				SFS - DSNAME/prefix already defined

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
089	59				SFS - Prefix owned
090	5A				SFS - Resource already defined
091	5B				SFS - Resource not found
092	5C				SFS - Resource not owned
093	5D				SFS - Internal error
094	5E				SFS - Internal error
095	5F				SFS - Internal error
096	60				SFS - Internal error
097	61				SFS - Internal error
098	62				SFS - Internal error
099	63				SFS - Internal error
100	64	9407	7100	AUDIT	TSS is down - unable to perform
101	65	7221	7220		Data set not defined
102	66	7227	7220		Unauthorized access
103	67	7235	7220		Bad VSAM opn, no ABSTRACT(CATAPE)
104	68	7232	7220		FETCH-only data set violation
105	69	7233	7220		Unable to erase residual data on a scratch request
106	6A	7225	7220		Data set accessed with wrong program
107	6B	7231	7220		Data set accessed from wrong library
108	6C	7234	7220		FETCH violation
109	6D	7226	7220	FAILWARN	Data set access rejected by exit
110	6E	7222	7220		Data set accessed at wrong time
111	6F	7223	7220		Data set accessed on wrong day
112	60	7224	7220		Data set accessed thru wrong facility
113	71				Reserved
114	72				Reserved
115	73	7206	7200	FAILWARN	Volume access denied by exit
116	74	7210	7200		BLP violation
117	75	7201	7200		Volume access not authorized

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
118	76	7221			Volume Not Available from this System
119	77	7207	7200		Volume access at wrong level
120	78	7208	7200		Cannot create on this volume
121	79	7201	7200		System error getting volume info
122	7A	7209	7200		Cannot access volume w, o data set
123	7B	7228	7220		Data set not available from this system
124	7C				Reserved
125	7D				Reserved
126	7E	7203	7200		Volume accessed on wrong day
127	7F	7202	7200		Volume accessed at wrong time
128	80	7204	7200		Volume accessed through wrong facility
129	81	7205	7200		Volume accessed with wrong program
130	82				Reserved
131	83				Reserved
132	84	7251	7250		Minidisk not owned
133	85	7251	7250		No authority for minidisk
134	86				Reserved
135	87				Reserved
136	88	7251	7250		Resource - Access denied
137	89				Reserved
138	8A				Reserved
139	8B				Reserved
140	8C				IMS xactn denied – no password
141	8D				Reserved
142	8E				IMS xactn denied – bad password
143	8F				Reserved
144	90	7256	7250	FAILWARN	Resource access denied by site exit
145	91	7252	7250		Resource accessed on wrong day
146	92	7253	7250		Resource accessed at wrong time

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
147	93	7194	7250	FAIL	Terminal locked
148	94	7193	7250	FAIL, PASSWORD	Unlock failed - bad password
149	95	7255	7250		Resource accessed via wrong program
150	96	7254	7250		Resource accessed via wrong facility
151	97	7257	7250		Resource access level not authorized
152	98	7192	7250		VTHRESH locked
153	99	7054	7100	NOVIOL	Bypass active - not a violation
154	9A	7272	7250		ACID submit through wrong facility
155	9B	7273	7250		ACID submit through wrong program
156	9C	7270	7250	FAILWARN	ACID submit failed by site exit
157	9D	7271	7250		Not authorized to submit this acid
158	9E	0000	7250		Not authorized to use this command
159	9F	0000	7250		Not authorized to use this program
160	A0	7161	7250		Facility accessed at wrong time
161	A1	7162	7250		Facility accessed on wrong day
162	A2	219			CMD UNAUTHORIZED FOR APPL
163	A3	7250			CMD NOT AUTHORIZED FROM POE
164	A4	7251			CMD DUPLICATE RDT NAME
165	A5	7259	7250		Resource access denied to a record
166	A6	7260	7250		Resource access denied to a screen
167	A7	7163	7100		Illegal facility for this system
168	A8	7259	7250		RLP logic error--access denied to a record
169	A9	7260	7250		SLP logic error--access denied to a screen
170	AA				CMD ADMIN SCOPE MUST BE LSCA
171	AB				CMD RXE17-WORKATTR FIELD NF
172	AC				CMD APPCLU INVALID FUNCTION
173	AD				CMD APPLCU ETAL NOT FOUND
174	AE	0324			Target node admin ACID missing
177	B1				RESULT=FAILURE ON RACROUTE=AUDIT

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
175	AF				CPF (SEV) PSWD VERIFICATION FAILED
176	B0				DUPLICATE PROFILE FOR ACID
177	B1				RESULT=FAILURE ON RACROUTE=AUDIT
178	B2				USER NOT AUTHORIZED TO SECLABEL
179	B3				DSN ACCESS DENIED: NO SECLABEL
180	B4				RESOURCE ACCESS DENIED: NO SECLABELS
181	B5				DSN ACCESS DENIED: NO SECLABEL
182	B6				RESOURCE ACCESS DENIED: NO SECLABEL
183	B7				SUBJECT NEVER DOMINATES
184	B8				BAD SDT RECORD PASSED FOR ADD
185	B9				CERTIFICATE NOT FOUND FOR REM
186	BA				EXPIRE DATE NOT AFTER START DATE
192	C0				INVALID SUSPEND USE
193	C1				NO ROOM IN ACID RECORD FOR UNDERCUT
197	C5	7101	7100	PASSWORD NOVIOL	User has no Password Phrase
220	DC				CROSS MEMORY COMMUNICATION FAILED
221	DD				ATTENTION INTERUPT REQUESTED
232	E8				LOCKED:UNLOCK FAILED-WRONG PASSWORD:ILL
243	F3				LLY RESTRICTED:IMS XACTN DENIED-BAD PAS

Chapter 7: CASECCFS Codes

Codes

The results of a call to the CA Security Call Coupling Facility (CASECCFS) are reported in message formatted as follows:

CASECCFS - Function: xxxxxxxx Rc=xxxxxxxx Rs=xxxxxxxx

If this message is accompanied by message TSS9710E, that message can be used to determine exactly what the return codes mean. Otherwise, the message is documenting the return codes and reason codes returned by a call to Sysplex Services. These codes are documented in the IBM z/OS and *OS/390 Sysplex Services Reference*.

A common CASECCFS message is:

CASECCFS - Function: Write Rc=1033000C Rs=0C1C0C17

This message indicates that an attempt was made to write data to the coupling facility, but the attempt failed because the coupling facility was full. This is a normal occurrence, but the message is displayed so that it is possible to determine how often the coupling facility is filling up.

The following return codes and reason codes from the CA Security Coupling Facility service are associated with message TSS9710E.

Return Codes	
0	SUCCESS
4	WARNING ISSUED
8	INVALID PLIST
12	INPUT VALIDATION FAILED
16	FUNCTION FAILED
Reason Codes	
1	INVALID FUNCTION CODE
2	INVALID WORK AREA
3	INVALID TOKEN PASSED
4	GETMAIN FAILED

Return Codes	
5	INVALID STRNAME
6	INVALID CONNAME
7	INVALID NUMBER OF HEADERS
8	INVALID ENTRY SIZE
9	INVALID NAME FIELD
10	INVALID BUFFER ADDRESS
11	INVALID BUFFER LENGTH
12	INVALID OPTION FIELD
13	IXLCONN FAILED
14	IXLDISC FAILED
15	IXLLIST READ FAILED
16	IXLLIST WRITE FAILED
17	IXLLIST DELETE FAILED
18	IXLLIST LOCK FAILED
19	ENTRY IS LOCKED
20	ENTRY NOT FOUND
21	LOCK NOT HELD
22	LOCK HELD
23	LOCK NOT SET
24	LOCK NOT RESET
25	MSGALL FAILED
26	GETMSG FAILED
27	GETMSG NO MORE MESSAGES
28	INVALID ECB ADDR
29	INVALID MSG ADDRESS
30	INVALID MSG LENGTH
31	LXCF INITIALIZE FAILED
32	LXCF REGISTER FAILED
33	LXCF QUERY FAILED
34	LXCF SEND MESSAGE ERROR

Return Codes	
35	LXCF GETEVENT ERROR
36	LXCF ENDEVENT ERROR
37	NO OTHER XCF CONNECTED NODES
38	LXCF DEREGISTER ERROR
39	LXCF TERMINATE ERROR
40	STORAGE POOL INIT ERROR

Chapter 8: CIA0101E - CIA0199E Messages

This section contains the following topics:

CIA0101E CIA Real-Time Initialization Routines (see page 869)
CIA0201E - CIA0249E Messages (see page 871)
CIA0300I CIA Processing Component Messages (see page 891)
CIA0400 Series Messages (see page 911)
CIA0500 Series Messages (see page 931)
CIA0800 Series Messages (see page 934)
CIA0900 Series Messages (see page 944)

CIA0101E CIA Real-Time Initialization Routines

CIA0133E

Userfield xxxxxxxx not defined to the Top Secret FDT

Reason:

The input control statements for CIA real-time processing contain a user-defined field that is not defined to the CA Top Secret FDT.

Action:

Correct the error and restart the address space.

Module:

TSSIRPRM

CIA0134E

Bad length for type user defined field - xxxxxxxx

Reason:

The input control statements contain a User Defined field with an invalid length for that type.

Action:

Correct the error and restart the address space.

Module:

TSSIRPRM

CIA0135E

Invalid field name for Global IDMAP - xxxxxxxx

Reason:

The field specified on the GLOBALID FIELD input control statement not in the list of valid fields or a valid User Defined Field.

Action:

Remove the GLOBALID FIELDS input control statement or find a valid field and restart the address space.

Module:

TSSIRPRM

CIA0136E

Invalid field length for Global IDMAP - xxxxxxxx

Reason:

The GLOBALID FIELD you specified in the input control statement was longer than the maximum length allowed for the IDMAP field.

Action:

Remove the GLOBALID FIELDS input control statement or find a valid field and restart the address space.

Module:

TSSIRPRM

CIA0137E

CIA/RT initialization terminated - incompatible database data

Reason:

The filter records that are being processed during initialization of the CIA real-time feature are not valid.

Action:

Rerun the CIA batch unload utility with valid filter records specified, reload the database, and restart the CIA real-time component.

Module:

TSSIRPRM

CIA0201E - CIA0249E Messages

CIA0201E

Insufficient storage for execution

Reason:

The external security manager could not obtain the storage for a record buffer or an internal table. CIA real-time processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRDB1, ACFIRDB4, ACFIRDS1, ACFIRDS4, ACFIRIOS, ACFIRLDS, ACFIRLID, ACFIRPEV, ACFIRPRM, ACFIRRS1, ACFIRRS4, ACFIRSCP, ACFIRSFT, ACFIRSMS, ACFIRSRC, ACFIRUSR

CIA0202E

Unable to locate ACF2 ACCVT

Reason:

A critical CA ACF2 control block could not be located. An improper installation of the external security manager or corruption of common storage may cause this. CIA real-time processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRLID, ACFIRPEV

CIA0203E

Unable to locate ACF2 SAF IVT

Reason:

A critical CA SAF control block could not be located. An improper installation of the external security manager or corruption of common storage may cause this. CIA real-time processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRPEV

CIA0204E

An invalid field was specified on entry to ACFIRIOS

Reason:

An internal error occurred in processing external security manager databases. CIA real-time processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRIOS

CIA0205E

An unexpected return code was returned from the criteria service routine

Reason:

An unexpected error occurred in an internal service routine that processes and evaluates the CIA selection criteria. CIA real-time processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRDB2, ACFIRDSN, ACFIRLID, ACFIRPEV, ACFIRPRM, ACFIRRSC, ACFIRSON, ACFIRUSR

CIA0206E

An invalid CIA real-time event record was found

Reason:

CIA real-time processing encountered an invalid event record. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message is informational only. No action is required.

Module:

ACFIRIOS, ACFIRPEV

CIA0208E

Unable to locate the ACF2 ACIVT

Reason:

A critical CA ACF2 control block could not be located. An improper installation of the external security manager or corruption of common storage may cause this. CIA real-time processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRLID

CIA0209E

Unable to locate the logonid CFDEs

Reason:

The CA ACF2 Field Definition Record (ACFFDR) could not be located from the ACCVT and/or the ACFFDR Field Definition Record field definitions (@CFDEs) could not be found. CIA real-time processing terminates.

Action:

Ensure that all @CFDE entries are defined or contact CA Support at http://ca.com/support.

Module:

ACFIRLID, ACFIRPRM

CIA0210E

The requested field *fld* was not found in the logonid CFDEs *reason*

Reason:

The logonid record field does not exist in the actual CA ACF2 Field Definition Record (ACFFDR) field definitions (@CFDEs). CA ACF2 checks this field to obtain its value to write to the CIA real-time database. Because this field is not defined, it cannot be written to the CIA real-time database. The value of *fld* is the external name of the logonid record field which does not exist in the @CFDEs. The value of *reason* is blank or displays "for logonid", which is the logonid for which the CFDE field check is performed. CIA real-time processing terminates.

Action:

Ensure that an @CFDE macro for the specified field is included in the ACFFDR module.

Module:

ACFIRLID

CIA0211E

The value in field *fld* is invalid *reason*

Reason:

CA ACF2 encountered an error processing a logonid field value in the Logonids database. The value of *fld* is the name of the logonid field which contains an invalid value. The value of reason is blank or displays "for logonid", which is the logonid of the user for which the field value was invalid. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

Correct the field value in the logonid record or delete the logonid record and reinsert it.

Module:

ACFIRLID, ACFIRSFT, ACFIRSON, ACFIRUSR

CIA0212E

Internal error in definition of target field *fld*

Reason:

CA ACF2 CIA real-time processing encountered an internal error while processing field values from a logonid record in the Logonids database into the CIA real-time database. This error occurs when the target field length in the database does not support the length of the logonid field value being processed from the Logonids database. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRLID

CIA0213E

Invalid date value found in rule *rule*

Reason:

CIA real-time processing encountered an error while trying to process a date field in a data set rule, resource rule, or DB2 resource rule. The value of *rule* is the $KEY of the rule set which contains the invalid date. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

Correct the date in the rule line.

Module:

ACFIRDB1, ACFIRDB4, ACFIRDS1, ACFIRDS4, ACFIRRS1, ACFIRRS4

CIA0214E

A resource mask is too long in rule *rule*

Reason:

CIA real-time processing encountered an error while trying to process a resource mask which exceeded the maximum length allowed in a resource rule or DB2 resource rule. The value of *rule* is the $KEY of the rule set which contains the invalid resource mask. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

Correct the resource mask in the rule.

Module:

ACFIRDB1, ACFIRDB4, ACFIRRS1, ACFIRRS4

CIA0215E

Record length exceeds maximum allowed for user-defined fields

Reason:

You specified too many USERFIELD input control statements in the SYSIN input parameter file in the UNLOAD Utility, which caused the variable record length for the USERUSER table in the CIA real-time database to exceed the maximum variable record length allowed for the table. CIA real-time processing terminates.

Action:

Reduce the number of USERFIELD control statements in the UNLOAD Utility SYSIN file and run the utility again. Make sure each logonid record field specified in a USERFIELD control statement exists in the actual CA ACF2 Field Definition Record (ACFFDR) field definitions (@CFDEs). Also, eliminate any duplicate field names in the USERFIELD control statements. There should not be more user-defined fields specified with USERFIELD control statements than actually exist in a logonid record.

Module:

ACFIRPRM

CIA0216E

Invalid event type – *type*

Reason:

An invalid external security manager record type was encountered in an event. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRSRC, ACFIRUSR

CIA0217E

An error was returned from the CIADBBLD service routine

Reason:

An error code was returned from an internal service routine that processes and builds the request lists for the CIA real-time updates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRDB1, ACFIRDB4, ACFIRDCO, ACFIRDEL, ACFIRDS1, ACFIRDS4, ACFIRLDS, ACFIRLID, ACFIRRS1, ACFIRRS4, ACFIRSCP, ACFIRSFT, ACFIRSMS, ACFIRSON, ACFIRSRC, ACFIRUID, ACFIRUSR

CIA0218E

Duplicate keyword found on input statement

Reason:

You specified the same keyword more than once on a CIA UNLOAD utility input control statement when running the CIA Unload Utility. CIA real-time processing terminates.

Action:

Remove the duplicate keyword on the input control statement and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0220E

Value is too long for keyword - *key*

Reason:

You specified a value for a keyword on a CIA UNLOAD utility input control statement that was greater than the maximum length allowed. The value of *key* is the keyword that contains the invalid value. CIA real-time processing terminates.

Action:

Specify a value that does not exceed the maximum length for the keyword and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0221E

No value was specified for keyword - *key*

Reason:

No value was specified for the keyword on a CIA UNLOAD utility input control statement. The value of *key* is the keyword for which there was no value specified. CIA real-time processing terminates.

Action:

Specify a value for the keyword on the input control statement in the SYSIN file and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0222E

No field definition for field – *fld*

Reason:

The logonid record field specified in a CIA UNLOAD utility input control statement does not exist in the actual CA ACF2 Field Definition Record (ACFFDR) field definitions (@CFDEs). The value of *fld* is the external name of the logonid record field specified in an input control statement. CIA real-time processing terminates.

Action:

Ensure that an @CFDE macro for the specified field is included in the ACFFDR module and run the CIA UNLOAD utility again. If you are sure the field is defined in the ACFFDR, then verify that the CIA UNLOAD utility input control statement specifies the correct external name of the field.

Module:

ACFIRPRM

CIA0223E

Multi-valued field not allowed – *fld*

Reason:

The logonid record field specified in the GLOBALID FIELD input control statement is defined as a multi-valued field in the CA ACF2 Field Definition Record (ACFFDR) field definitions (@CFDEs). CA ACF2 does not allow a multi-valued, user-defined field to be specified in a GLOBALID FIELD input control statement. Because the field is multi-valued, it cannot be written to the CIA real-time database. The CA ACF2 CIA unload utility terminates.

fld

Specifies the external name of the logonid record field in the GLOBALID FIELD input control statement.

Action:

Ensure that the field name specified in the GLOBALID field input control statement is defined as single-valued in the @CFDE macro included in the ACFFDR module. Run the utility again.

Module:

ACFIRPRM

CIA0224E

Invalid value was specified for keyword - *key*

Reason:

You specified an invalid value for a keyword on a CIA UNLOAD utility input control statement. The value of *key* is the keyword that contains the invalid value. The CA ACF2 CIA real-time processing terminates.

Action:

Correct the value for the keyword and run the CIA UNLOAD utility again.

Note: If you specified a USERFIELD input control statement, make sure the field name is valid (with no leading or trailing blanks) and its length is from 1 to 8 characters long. If you specified a field type with the field name in the USERFIELD input control statement, make sure there is a comma delimiter between the field name and field type and that the field type is VARCHAR or INTEGER (with no leading blanks).

Module:

ACFIRPRM

CIA0225E

Input parameter *value* may only be specified once

Reason:

You specified a CIA UNLOAD utility input control statement more than once in the SYSIN file. *Value* is the control statement that was specified more than once. CIA real-time processing terminates.

Action:

Remove all occurrences, except for one, of the CIA UNLOAD utility input control statement in the SYSIN file and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0226E

Duplicate value *value* skipped in rule *rule*

Reason:

CIA real-time processing encountered a duplicate value in a rule field. CIA real-time processing ignores the duplicate value and continues processing.

Action:

This message is informational only. No action is required.

Module:

ACFIRDB1, ACFIRDB4, ACFIRDS1, ACFIRDS4, ACFIRRS1, ACFIRRS4, ACFIRSCP

CIA0227E

A required parameter was not entered on a control statement

Reason:

You did not specify a required input parameter in a CIA UNLOAD utility SYSIN input control statement. CIA real-time processing terminates.

Action:

Specify all required parameters for each CIA UNLOAD utility SYSIN input control statement and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0228E

Mutually exclusive parameters were entered on a control statement

Reason:

A CIA UNLOAD utility input parameter conflicts with another input parameter in the same SYSIN file input control statement. CIA real-time processing terminates.

Action:

Resolve the conflict and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0229E

An invalid parameter was encountered in the SYSIN control statements

Reason:

CIA real-time processing does not recognize the keyword as one of its input parameters. CIA real-time processing terminates.

Action:

Specify a valid CIA UNLOAD utility input parameter and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0230E

Error processing the criteria

Reason:

There was an error processing the CIA UNLOAD utility SYSIN input parameters that were stored as criteria in the CIA real-time database. CIA real-time processing terminates.

Action:

Make sure that the CIA UNLOAD utility SYSIN file was created and that the CA ACF2 CIA Unload Utility procedure JCL contains a DD statement for the SYSIN file with the name SYSIN and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0231E

Load failed for user exit - *exit*

Reason:

The user exit module name specified in the EXIT keyword of the CIA UNLOAD utility GLOBALID input control statement could not be located and loaded. CIA real-time processing terminates.

Action:

Ensure that the user exit module exists in LPA and that the name is correct in the CIA UNLOAD utility GLOBALID EXIT input control statement, and rerun the CIA UNLOAD utility.

Module:

ACFIRPRM

CIA0232E

Field type *fld-type* invalid for user-defined field - *fld*

Reason:

You specified an invalid field type in the CIA UNLOAD utility USERFIELD input control statement for a logonid record field. The value of *fld-type* is the field type specified in a USERFIELD input control statement; VARCHAR or INTEGER. The value of *fld* is the logonid record field whose field type in the CA ACF2 Field Definition Record (ACFFDR) field definitions (@CFDEs) does not correspond to the requested overriding field type. CIA real-time processing terminates.

Action:

Specify field type VARCHAR in the USERFIELD input control statement for a logonid record field whose @CFDE field type is CHAR (or) specify field type INTEGER in the USERFIELD input control statement for a logonid record field whose @CFDE field type is BINARY (or) do not specify any field type in the USERFIELD input control statement for a logonid record field and run the CIA UNLOAD utility again.

Module:

ACFIRPRM

CIA0236E

No GLOBALID value was returned from userexit

Reason:

The user exit module you specified in the EXIT keyword of the CIA UNLOAD utility GLOBALID input control statement did not return any globalid value in the parameter list passed to it from CIA real-time processing. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

Ensure that your GLOBALID user exit module returns a valid value in the parameter list passed to it from CIA real-time processing.

Module:

ACFIRLID

CIA0238E

SAFFFCPC returned an error, RC=xx, Reason=xx

Reason:

The external security manager tried to convert the IDMAPDN or IDMAPRN in a User Profile IDMAP record from UTF-8 format into EBCDIC, but an error occurred.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRUSR

CIA0239E

Profile User IDMAP record processing failed

Reason:

There was an error while processing the Profile User IDMAP records.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

ACFIRUSR

CIA0240E

Event record is missing or invalid

Reason:

CA Top Secret encountered an error processing the event record.

The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0241E

CA Top Secret is not active

Reason:

CIA Real Time detected that CA Top Secret was not active at the point of processing the event record.

Action:

Start CA Top Secret

Module:

TSSCIRDR

CIA0242E

Unable to locate CIARTCVT

Reason:

A critical CIA Real Time control block could not be located. An improper installation or corruption of common storage may cause this.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0243E

CFILE record error

Reason:

CA Top Secret encountered an error while processing the CIA Real Time event record during the cfile process. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0244E

CIA Load record error

Reason:

CA Top Secret encountered an error while processing the CIA Real Time event record during the load record process. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0245E

Error building request record list

Reason:

CA Top Secret encountered an error while processing the CIA Real Time event record request building process. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0246E

Acid type invalid for event

Reason:

This is an internal error in which the event record generated specifies an event inconsistent with the acid in the event request. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0247E

GETMAIN/FREEMAIN error

Reason:

This is an internal error in which there was a problem obtaining or freeing storage. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0248E

Error from call to DSI

Reason:

This is an internal error in which there was a problem sending the requests to DSI. The event record was not processed, but the error was journaled to an output Journal dataset, if one was defined.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRDR

CIA0249E

Invalid plist parameter list

Reason:

The plist parameter list does not have the correct structure.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSMSG, CIAIRFRE, CIAIRSDR

CIA0251E

Getmain failure for xxxxxxxx

Reason:

TSSCIRIE was unable to acquire sufficient storage for the table.

Action:

This is an internal error. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRIE

CIA0252E

Internal processing problem, reason code - xx

Reason:

There was an internal processing error that caused CIA Real Time to terminate.

Action:

This is an internal error. For assistance, contact CA Support at http://ca.com/support.

Module:

TSSCIRIE

CIA0300I CIA Processing Component Messages

CIA0300I

CIA Real-Time Logging Task is Initializing

Reason:

The CIA real-time logging task has started the initialization process.

Action:

None

Module:

CIARTLGR

CIA0301I

CIA Real-Time Rcvr Queue Allocation: RC=rc RSN=rsn

Reason:

The CIAI Real-Time Task has allocated the queue for temporary storage of event records.

rc

Specifies the return code from the IARCP64 Service.

rsn

Specifies the reason code associated with the return code.

Action:

If both values are zero, no action is required. The storage was successfully allocated. Determine the reason for the allocation error from the IARCP64 Service Documentation and make any necessary corrections to the environment.

Module:

CIARTLGI

CIA0302I

CIA Real Time Rcvr Queue Max Entries now nnn cells

Reason:

The CIA real-time task has calculated the number event records it can temporarily store until they can be written to the z/OS system logger. This number is a function of the amount of storage specified by the CIAMAXSTOR control option.

Action:

None

Module:

CIARTLGI

CIA0303I

CIA Real-Time DASD Log Stream Detected

Reason:

The CIA real-time logging task has connected to the z/OS system logger. It has determined that the logstream is a DASD Only Logstream

Action:

None

Module:

CIARTLGC

CIA0310I

CIA Real-Time Sys Logger Connect LogStream=name RC=*rc* RSN=*rsn*

Reason:

The CIA real-time logging task has connected the z/OS system logger.

name

Identifies the logstream specified on the connect request.

rc

Indicates the return code from the IXGCONN request.

rsn

Indicates the reason code associated with the return code.

Action:

If both values are zero, no action is required. If a non zero value is observed, determine the error from the IXGCONN documentation provided by IBM. Correct any condition and restart the CIA real-time logging task using the Chorus command. This may be a temporary condition which CIA real-time is programmed to recover from when the condition is corrected. In such a case the task will remain active and additional messages will be displayed indicating the action it is taking.

Module:

CIARTLGC

CIA0311I

CIA Real Time Log Info LSVERSION=*version*

Reason:

The CIA real-time logging task has connected to the z/OS system logger. When the connection is successful as indicated in message CIA0301I, this message is displayed to identify the version of the logstream definition of the connected logstream.

Action:

None

Module:

CIARTLGC

CIA0312I

CIA Real-Time Log Info Structure Name=name

Reason:

The CIA real-time logging task has connected to the z/OS system logger. When the connection is successful as indicated in message CIA0301I and the logstream is maintained in a coupling facility, this message is displayed to identify the name of the structure within the coupling facility in which the log stream is stored.

Action:

None

Modules:

CIARTLGC

CIA0313I

CIA Real-Time Log Info Structure Buf Sizes MAX=*max* AVG=*avg*

Reason:

This message is displayed upon successful connection to a log stream which is resident in a coupling facility structure. The maximum (*max*) and average (*avg*) buffer sizes as reported by the z/OS system logger are displayed.

Action:

None

Modules:

CIARTLGC

CIA0314I

CIA Real-Time Log Info Diag 1-4: *value1 value2 value3 value4*

Reason:

These diagnostic values are displayed upon completion of a connection request to a z/OS system logger log stream. *Value1* through *value4* are diagnostic codes which may be valuable for problem determination.

Action:

None

Modules:

CIARTLGC, CIARTLGD

CIA0315I

CIA Real-Time Log Info GAPS=*gaps* FLAGS=*flags*

Reason:

These diagnostic values are displayed upon completion of a connection request to a z/OS system logger log stream. *Gaps* and *flags* are diagnostic codes which may be valuable for problem determination.

Action:

None

Modules:

CIARTLGC, CIARTLGD

CIA0320I

CIA Real-Time Sys Logger Disconnect LogStream=logstream RC=*rc* RSN=*rsn*

Reason:

A disconnect was issued to the Log Stream identified by logstream. The rc is the return code and rsn is the reason code associated with the request.

Action:

If both values are zero, no action is required. If a non zero value is observed, determine the error from the IXGCONN documentation provided by IBM. Errors indicated here may be a result of timing and or normal error recovery processes. An example would be a return code of 4 with a reason code of xxxx0404 indicating a delay in the disconnect process or a return code of 8 with a reason code of xxxx082D indicating a bad stream token.

Module:

CIARTLGD

CIA0321I

CIA Real-Time Rcvr Queue Deallocation Successful

Reason:

This message indicates the storage associated with the Receiver Queue was successfully released.

Action:

None

Modules:

CIARTLGI

CIA0322I

CIA Real-Time Rcvr now accepting events

Reason:

The CIA real-time receive process is now accepting event records to be passed to the z/OS System Logger. This message is displayed to confirm processing of the Chorus CIA(START) command.

Action:

None.

Module:

CIARTLGR

CIA0323I

CIA Real-Time Rcvr no longer accepting events

Reason:

The CIA real-time receive process is no longer accepting event records to be passed to the z/OS System Logger. The ESM will not generate them. This message is displayed to confirm processing of the Chorus CIA(STOP) command.

Action:

None.

Module:

CIARTLGR

CIA0348I

CIA Real-Time Logging Task - Termination Process Complete – Re-initialization is being attempted

Reason:

The CIA real-time logging task encountered a serious error. In an attempt to correct the error, the termination process was executed. Re-initialization will now be attempted to continue execution. The process of attempting to correct an error via this process is only attempted twice per execution of the CIA Real-Time Logging Task. On a third error or if an error occurs during the execution of the Termination Process in an attempt at recovery, the task is shutdown. The task can be started manually with the CIA(START) command.

Action:

Provide any documentation related to the error or errors to CA Support at http://ca.com/support.

Module:

CIARTLGR

CIA0349I

CIA Real-Time Logging Task - Termination Process Complete – Task will end

Reason:

The CIA real-time logging task is terminating. The logging task can be started manually with the CIA(START) command.

Action:

None

Module:

CIARTLGR

CIA0351E

CIA Real-Time Recovery unavailable, RC=rc

Reason:

This message indicates the recovery environment could not be established for the process. This may be a program logic error or an error in the installation of the software.

rc

Indicates the return code from the recovery program logic.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIARTLGA, CIARTLGC, CIARTLGD, CIARTLGI, CIARTLGM, CIARTLGR, CIARTLGT, SAFRT101

CIA0352E

LOAD failed for module name R1=r1 R15=r15

Reason:

This message indicates an attempt was made to load a program indicated by the variable name. The operating system could not load the module. The reasons indicated by values in general register one (r1) and general register fifteen (r15) are the values provided upon return from the LOAD Macro and indicate the reason for the failure.

Action:

Determine the reason for the failure. Consult the *IBM MVS Programming: Authorized Assembler Services Reference*. This is likely due to a program installation error. For additional information, contact CA Support at http://ca.com/support.

Module:

CIARTLGR

CIA0354E

CIA Real-Time Sys Logger Write Error LogStream=name RC=*rc* RSN=*rsn* Cnt=cnt

Reason:

An attempt was made to add a record to the logstream identified by name. The request did not complete successfully. The return code (rc) and the reason code (rsn) indicate the cause of the error. They are the values returned by the IXGWRITE Macro. The value of cnt indicates the number of times this error was returned consecutively. The message is only displayed the first time it occurs and again after each group of 256 consecutive occurrences.

Action:

Determine the cause of this error from the return code and reason code displayed. This may be due to a temporary condition such as a structure rebuild or offload. In such a case, an attempt to write the record will be made when the condition is cleared. Additional messages may be displayed showing status changes. Consult IBM documentation for the IXGWRITE Macro for an explanation of the return and reason codes.

Module:

CIARTLGM

CIA0355W

CIA Real Time Logger Lost Record CIARC=*reason* Count now count

Reason:

An attempt was made to queue a record to the CIA real-time logger task. The record could not be queued as indicated by the reason. A reason of 24 indicates a storage limitation imposed value supplied with the CIAMAXSTOR control option. Other values indicate a problem with the record itself or an error with storage management. The value of count indicates the total number of lost records including this one.

Action:

If a reason code of 24 is returned, the self imposed storage has been reached. This may be due a temporary condition such as the z/OS system logger not accepting records while rebuilding or offloading a structure. It may also be due to a spike in record production by the ESM. Consider the circumstances and other factors such paging space on the system or increase the amount of storage specified in the CIAMAXSTOR control option.

Module:

SAFRT101

CIA0356W

CIA Real-Time Rcvr Queue cannot be deleted - Receiver Active

Reason:

An attempt was made to delete the receiver queue. The receiver was active. No action was taken.

Action:

Inactivate the Receiver and retry the sequence.

Module:

CIARTLGI

CIA0357I

CIA Real Time Logstream Connection Successful - Awaiting Structure Rebuild

Reason:

The connection to the log stream was successful, however the structure in which the z/OS system logger stores these records was in the process of being rebuilt. Records cannot be written to this structure and will be accumulated in storage (see the CIAMAXSTOR control option) until the limit is reached or the z/OS system logger can accept records.

Action:

None.

Modules:

CIARTLGC

CIA0358I

CIA Real-Time Logstream now disconnected

Reason:

The CIA logstream has been disconnected and records cannot be written to the z/OS system logger at this time. This may occur due to an explicit action, such as a disconnect command. It may also be initiated by the z/OS system logger. Depending on the reason for the disconnect, the CIA real-time logging component may attempt reconnect, wait on a notification that the stream is again available and attempt to connect to it, or terminate the logging task within the ESM.

Action:

This may be a normal condition and no action is necessary. If this is not expected, determine the reason the log stream was disconnected. Issue a reconnect command when appropriate or restart the CIA real-time logging task.

Module:

CIARTLGA

CIA0359I

CIA Real Time Logstream - Writes pending

Reason:

The CIA real-time logger has received notification from the z/OS system logger to stop writing to the log stream. This is usually due to a temporary condition such as a structure rebuild. The reason for the condition is usually indicated by the codes displayed in message CIA0371I. The CIA real-time logger waits for notification to again write records to the log stream. During this time records are queued in storage up to the limit specified by the CIAMAXSTOR control option. Once the limit is reached, any new records will be discarded until such time that storage becomes available.

Action:

This is likely a temporary condition. Ensure sufficient storage is available to store records until the temporary condition is resolved.

Module:

CIARTLGA

CIA0360I

CIA Real-Time Logger - Shutdown ordered

Reason:

The CIA real-time logger has received notification from the z/OS system logger that further connections to the logger are not possible. The reason for this condition is likely evident from the codes supplied in message CIA0371I. The CIA real-time logger task will terminate.

Action:

Determine the reason this has occurred from message CIA0371I and any additional information in the processing environment. Make any corrections and restart the CIA real-time logger task. At times an IPL may be necessary.

Module:

CIARTLGA

CIA0361I

CIA Real-Time Logger - Attempting connection

Reason:

The CIA real-time logger has received notification that connections to a log stream are now possible. An attempt to connect to the log stream will now be performed.

Action:

None.

Module:

CIARTLGA

CIA0362I

CIA Real-Time Logger - Waiting for ENF notification

Reason:

A condition has occurred which prevents further interaction with the z/OS system logger at this time. A disconnect is permitted. Message CIA0371I may contain further information. The z/OS system logger notifies the CIA real-time logger when activity can resume and whether the condition causing the delay has been cleared.The CIA real-time logger is waiting for that notification. It is possible to receive further notifications which may indicate the condition cannot be cleared.

Action:

None.

Module:

CIARTLGA

CIA0363I

CIA Real-Time Logger - Disconnect ordered

Reason:

The CIA real-time logger has received notification of a condition which requires it to disconnect from the log stream. Message CIA0371I may contain further information. The CIA real-time logger will disconnect from the log stream. Message CIA0362I may be displayed if the condition causing the error is such that a reconnect will be possible at a future time.

Action:

Correct the condition which caused the disconnect. Restart the CIA real-time logging task if needed.

Module:

CIARTLGA

CIA0370E

CIA Real-Time Logger - ENF Exit Storage Error RC=*rc*

Reason:

The ENF listen exit which is part of the CIA real-time logger attempted to allocate storage. The request failed with a return code of rc. It is possible that an ENF Notification is will be missed.

Action:

Determine the meaning of *rc*. This may give you sufficient information to correct the error. Otherwise, contact CA Support at http://ca.com/support.

Module:

CIARTLGN

CIA0371I

CIA Real-Time Logger - ENF Event Selected, EVENT=*event*, RSN=*reason*

Reason:

The CIA real-time logger ENF exit has been driven for the event identified by event and reason. The event and reason codes are documented in Macro IXGENF in the SYS1.MACLIB library provided by IBM. The event has been selected by the exit for further processing. Additional messages will be displayed as the event is processed and action is taken by the CIA real-time logging task.

Action:

No action specific to this message. However, once the event and reason code is identified, it may signify a condition in the environment upon which further action is necessary.

Module:

CIARTLGN

CIA0372E

CIA Real-Time Logger - ENF Event Not Freed, RC=*v1*, R0=*v2 xxxxx*

Reason:

The storage holding an ENF Event Record could not be freed. The operating system returned the values v1 and v2 when the request was made. The value following the RO value in the message text provides identifying information for CA Support personnel.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIARTLGA

CIA0373E

CIA Real-Time Logger - ENF Event Queue Error

Reason:

The queue containing ENF event records was determined to be corrupted. The queue is cleared.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIARTLGA

CIA0374I

CIA Real-Time Logger - ENFREQ RC=*rc*

Reason:

The CIA real-time logging task has requested the z/OS event notification facility (ENF) to notify it of events provided by the z/OS system logger or to no longer notify it of such events. If the value of rc is other than zero, the request failed. The CIA real-time logging task will fail to initialize or in the case of termination will continue to terminate

rc

Indicates the value of return code associated with the request.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIARTLGI

CIA0375I

CIA Real-Time Logger - ENF Event Processing, EVT=*nnnnn*, RSN=*nnnnn*

Reason:

The CIA real-time logging task has begun processing a Logger Event which was passed to it by the event notification exit. The event is identified by the Event and Reason variables.

Action:

This information is provided as a debugging tool for CA Technologies Technical Support. The codes displayed are defined in the *IBM z/OS MVS Authorized Assembler Services Guide*. Some errors can be due to transient conditions such as short on storage. The CIA Real-Time task should resume normal processing.

Module:

CIARTLGA

CIA0376I

CIA Real Time Logger - ENF Action Selection, EVT=*nnnn*, RSN=*nnnn*, ACT=*nnnn*

Reason:

The CIA real-time logging task has selected a set of action parameters needed to handle a Logger Event passed to it by the event notification exit. The event is identified by the Event and Reason variables. The action is identified by the Action variable. As each action is processed, other messages may appear indicating their completion.

Action:

This information is provided as a debugging tool for CA Technologies Technical Support. The event and reason codes displayed are defined in the IBM manual: *z/OS MVS Authorized Assembler Services Guide.* Some errors may be due to transient conditions such as short on storage. The CIA Real-Time task should resume normal when appropriate and processing has been completed

Module:

CIARTLGA

CIA0380I

CIA Real Time Logger - ResMgr Add RC=*dd*

Reason:

The CIA real-time logging task attempted to define a z/OS Resource Manager. The decimal return code showing the result of this request is displayed. It is expected that this value be zero. Values other than zero indicate and error occurred and the z/OS Resource Manager was not defined.

Action:

Return Codes are those defined in the *IBM manual: z/OS MVS Authorized Assembler Services Reference* under the RESMGR ADD Macro Function. Determine the reason for the error and correct any environmental conditions. Some errors may be due to transient conditions such as short on storage. Once corrected, restart the ESM Address Space. Provide any documentation related to the error to CA Support.

Module:

CIARTLGI

CIA0381I

CIA Real Time Logger - ResMgr Completed RC=*dd*

Reason:

The CIA real-time logging task z/OS Resource Manger has run due to the termination of the ESM Address Space.

dd

Indicates the resultant status.

0

Indicates all resources were properly reset.

4

Indicates the CIARTCVT could not be located or validated.

If the message does not appear at the termination of the ESM address space, CIA real-time was not activated for the currently terminating instance of the ESM address space or CASAFIVT may be corrupted.

Action:

For values other than zero, contact CA Support at http://ca.com/support

Module:

CIARTLGZ

CIA0385I

CIA Real Time Logger - Connect requested, already connected; attempt Disconnect or Reconnect

Reason:

A command was issued instructing the CIA real-time logging task to connect to the z/OS System Logger managed logstream. The task determined the logging task was already connected.

Action:

Issue the Disconnect command to disconnect from the logstream and reset any indication that the task is connected. Issue a Connect command to establish a connection to the logstream. Alternatively, you may issue a Reconnect command to perform the disconnect function followed by the connect function.

It is possible for the disconnect function to fail with various error conditions due to environmental or out of sync conditions. The Disconnect command may only be needed to reset indicators and values maintained by the CIA Real-Time Logger Task to facilitate a clean connect function.

Module:

CIARTLGC

CIA0386I

CIA Real Time Logger - Disconnect Requested, Token=zero, flags reset, attempt Connect

Reason:

A Disconnect or Reconnect command was issued. The CIA real-time Task determined the connection token was zero and therefore could not issue the necessary request to the z/OS System Logger. Any indicators within the CIA real-time task regarding the connection were reset.

Action:

Issue a Connect command to instruct the CIA real-time task to attempt a connection to the z/OS System Logger managed logstream.

Module:

CIARTLGD

CIA0400 Series Messages

CIA0401I

CIA/RT Component Activation

Reason:

The CIA real-time processing component has started its initialization sequence.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR

CIA0402I

CIA/RT Component Activation Complete

Reason:

The CIA real-time processing component has successfully completed initialization.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR

CIA0403I

CIA/RT Component Termination

Reason:

The CIA real-time processing component has started its termination sequence.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR

CIA0404I

CIA/RT Component Termination Complete

Reason:

The CIA real-time processing component has successfully completed termination.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR

CIA0405I

CIA/RT Component MODIFY Command Complete

Reason:

The CIA real-time processing component has completed processing of a MODIFY console command.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR

CIA0406I

CIA/RT Component Options Processing

Reason:

The CIA real-time processing component has started processing the supplied control options.

Action:

This message is informational only. No action is required.

Module:

CIARTOPT

CIA0407I

CIA/RT Component Options Processing Success

Reason:

The CIA real-time processing component has successfully completed processing of the supplied control options.

Action:

This message is informational only. No action is required.

Module:

CIARTOPT

CIA0408I

CIA/RT Component Communications Task Activation

Reason:

The CIA real-time processing component has started the communications manager task.

Action:

This message is informational only. No action is required.

Module:

CIARTRTC

CIA0409I

CIA/RT Component Communications Task Termination

Reason:

The CIA real-time processing component is terminating the communications manager task, this occurs during the address space termination phase.

Action:

This message is informational only. No action is required.

Module:

CIARTRTC

CIA0410I

CIA/RT Component Attaching Permanent Servers

Reason:

The CIA real-time processing component communications task has started the permanent ESM event server tasks.

Action:

This message is informational only. No action is required.

Module:

CIARTRTC

CIA0411I

CIA/RT Component Detaching Servers

Reason:

The CIA real-time processing component communications task is terminating the ESM event server tasks, this occurs during the address space termination phase.

Action:

This message is informational only. No action is required.

Module:

CIARTRTC

CIA0415I

CIA/RT Component Event Server Activated

Reason:

A CIA real-time processing component ESM event server task is initializing. This message occurs for each permanent server started by the CIA real-time communications task at start up.

Action:

This message is informational only. No action is required.

Module:

CIARTPEV

CIA0416I

CIA/RT Component Event Server Terminated

Reason:

A CIA real-time processing component ESM event server task is terminating. This message occurs for each active server at address space termination.

Action:

This message is informational only. No action is required.

Module:

CIARTPEV

CIA0417I

CIA/RT Component Option GTRACE is &status

Reason:

The current status of the GTRACE option is displayed in response to a MODIFY console command. If the MODIFY command is 'GTRACE', the status will display as 'Active'. If the MODIFY command is 'NOGTRACE', the status will display as 'Inactive'.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR

CIA0418I

CIA/RT Module Reload Success - &modname reloaded

Reason:

The RELOAD request from the operator console for module &modname was successful.

Action:

This message is informational only. No action is required.

Module:

CIARTRLD

CIA0420I

CIA/RT Component Retry Initialization <Y> or <N> ?

Reason:

The CIA real-time processing component initialization has failed due to the error condition specified in the previous CIA real-time error message.

Action:

Correct the error condition from the prior message and reply 'Y' to continue the initialization process, or reply 'N' to terminate the CIA real-time component address space.

Module:

CIARTMGR

CIA0440I

CIA/RT Status Messages

Reason:

All CIA real-time processing component messages generated by the MODIFY console command STATUS are prefixed with this message number. For a complete explanation of the information included in these messages, see the *Compliance Information Analysis Guide*.

Action:

This message is informational only. No action is required.

Module:

CIARTSTS

CIA0450E

CIA/RT Component Not Authorized

Reason:

The CIA real-time processing component program CIARTINT has been loaded from a non-APF authorized library. Start up for the CIA real-time component address space is terminated.

Action:

Make sure the module CIARTINT is resident in an APF authorized library and restart the CIA real-time component address space.

Module:

CIARTINT

CIA0451E

CIA/RT Component Storage Obtain Failure

Reason:

An attempt has been made to obtain storage in the CIA real-time component address space, and the request has failed.

Action:

Increase the region size for the CIA real-time component address space to provide more available storage.

Module:

CIARTMGR, CIARTRTC

CIA0452E

CIA/RT Component ESM Subsystem Unavailable

Reason:

An attempt has been made to start the CIA real-time processing component prior to the start of the SAF sub system or the ESM.

Action:

Start the missing component (SAF sub system or ESM) and restart the CIA real-time component address space.

Module:

CIARTINT, CIARTMGR, CIARTRTC

CIA0453E

CIA/RT Component Already Active – terminating this instance

Reason:

An attempt has been made to start the CIA real-time processing component but it was already active in another address space and only one instance of the component is allowed per system.

Action:

This message is informational only. No action is required.

Module:

CIARTINT

CIA0454E

CIA/RT Component Module Load Failure

Reason:

An attempt has been made to start the CIA real-time processing component and the necessary programs cannot be found in an available library, so the startup has been terminated.

Action:

Place the CIA real-time product install library in the link list or make it available as a STEPLIB to the address space and restart the CIA real-time component address space.

Module:

CIARTINT, CIARTMGR

CIA0455E

CIA/RT Component ESM Initialization Failure

Reason:

An error has occurred during the initialization phase of the CIA real-time processing component and the startup has been terminated. A CIA real-time ESM specific error message should precede this message in the log.

Action:

See the CIA real-time ESM specific error message and correct the error condition, then restart the CIA real-time component address space.

Module:

CIARTMGR

CIA0456E

CIA/RT Component Options Failure

Reason:

An error has occurred during the processing of control options at CIA real-time processing component initialization. An option specific error message should precede this message in the log.

Action:

See the CIA real-time control option specific error message and correct the error condition, then restart the CIA real-time component address space.

Module:

CIARTOPT

CIA0457E

CIA/RT Component Task Attach Failure

Reason:

The CIA real-time processing component task manager has attempted to start a new operating system task but the request has failed. This is normally due to a lack of available system storage.

Action:

Increase the amount of available system storage to avoid a repeat of this error.

Module:

CIARTMGR, CIARTRTC

CIA0458E

CIA/RT Component Command Unrecognized

Reason:

A MODIFY command was entered at the console, but the command entered was not a valid CIA real-time processing component command.

Action:

See the *Compliance Information Analysis Guide* for a complete list of CIA real-time console MODIFY commands. Correct the command input and reenter the MODIFY command.

Module:

CIARTMGR

CIA0459E

CIA/RT Component Option &option Error, Using Default

Reason:

The CIA real-time processing component control option listed in the error message has been entered in the control options data set incorrectly. The default value for the control option will be used during this instance of the CIA real-time component.

Action:

See the *Compliance Information Analysis Guide* for a complete list of CIA control options and their acceptable values. Correct the option in error for the next instance of the CIA real-time component.

CIA0461E

CIA/RT Component Abend Limit Exceeded

Reason:

The abend counter for the current CIA real time processing component task has reached an internal limit. Prior to the limit the component attempts abend recovery. But once the limit is reached the component will terminate the task to avoid recursion. If the abend limit is reached in either the main task or the communications manager task then the CIA real-time component is terminated. If the abend limit is reached in an ESM event server task then only that task is terminated.

Action:

Gather all console and dump documentation from the abends and contact CA Support at http://ca.com/support.

Module:

CIARTMGR, CIARTRTC, CIARTPEV

CIA0462E

CIA/RT Component Control Block &block not found

Reason:

A service call within the CIA real-time processing component has attempted to reference an internal control block and the control block could not be found.

Action:

This is an internal error, for assistance, contact CA Support at http://ca.com/support.This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

Various CIA real-time component event processing modules

CIA0463E

CIA/RT Module Reload Failure - Name not entered

Reason:

A MODIFY RELOAD console command was entered but no module name was supplied.

Action:

Correct the RELOAD command input by supplying a valid module name or ALL.

Module:

CIARTMGR

CIA0464E

CIA/RT Module Reload Failure - Plist or control block in error

Reason:

A request to load or RELOAD a module could not be executed because the parameter list contained invalid data or a required control block could not be found.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIARTRLD

CIA0465E

CIA/RT Module Reload Failure - No match for module &modname

Reason:

A request to load or RELOAD a module could not be executed because the supplied module name could not be found in the internal module name table.

Action:

If this was a MODIFY RELOAD console command, verify that the name of the module was entered correctly. If this was an internal load request at initialization, for assistance contact CA Support at http://ca.com/support.

Module:

CIARTRLD

CIA0466E

CIA/RT Module Reload Failure - &modname RC=&retcode RSN=&rsncode

Reason:

A request to load or RELOAD &modname failed. &retcode and &rsncode are the return code and reason code for the failure. The possible return codes and reason codes include:

Return Code	Reason Code	Explanation
4	4	BLDL request failed
4	8	Module length from DBLD request was zero
4	12	LOAD request failed
4	16	Insufficient storage to load module

Action:

Make sure a valid copy of &modname is available in the load library for the component address space.

Module:

CIARTRLD

CIA0470E

CIA/RT Component Logger &function Failure - RC=*&retcode* RSN=*&rsncode*

Reason:

The CIA/RT processing component has attempted to access the System Logger and the request has failed. The logger function attempted will be one of the following: CONNECT, DISCONN, BROWSE, RESET, READ, or DELETE. *&retcode* and *&rsncode* are the return code and reason code for the failure. Some of the more common return codes and reason codes include:

Return Code	Reason Code	Explanation
8	80B	Invalid log stream name – check ESM controls
8	80D	User not authorized for log stream – check ESM security

Return Code	Reason Code	Explanation
8	831	Invalid log stream name – check ESM controls
8	846	Log stream is empty – wait for events to be added
8	890	System Logger address space failed – start System Logger
8	891	System Logger is initializing – wait for initialization to complete
C	xxx	System Logger address space failed – start System Logger

Action:

Refer to the *IBM Assembler Services Reference* guides for a complete description of the return and reason codes supplied as output from the use of the following macros: IXGBRWSE, IXGCONN, and IXGDELET. In most cases the component will recover from the failure and continue to process events. If the component fails and you need help contact CA Support at http://ca.com/support.

Module:

CIARTMGR, CIARTRTC

CIA0471E

CIA/RT System Logger is Down and needs Restarting

Reason:

The CIA real-time processing component has attempted to access the System Logger and the request has failed due to the System Logger address space being inactive.

Action:

Start or restart the System Logger address space and then retry the CIA real-time component processing.

Module:

CIARTMGR, CIARTRTC

CIA0476E

CIA/RT Component <DSI or DB2> Processing Failure Condition

Reason:

The CIA real-time processing component has suspended processing of events due to a process failure in either DSI or DB2. These messages should be preceded by additional messages containing information to help diagnose the failure condition.

Action:

Correct the failing condition in either DSI or DB2 and enter 'Y' to resume the processing of events, or enter 'N' to terminate the CIA real-time component address space.

Module:

CIARTRTC

CIA0477E

CIA/RT Correct condition and reply <Y> to continue or <N> to terminate

Reason:

The CIA real-time processing component has suspended processing of events due to a process failure in either DSI or DB2. These messages should be preceded by additional messages containing information to help diagnose the failure condition.

Action:

Correct the failing condition in either DSI or DB2 and enter 'Y' to resume the processing of events, or enter 'N' to terminate the CIA real-time component address space.

Module:

CIARTRTC

CIA0480E

CIA/RT Component – CIASTATS file error, &status

Reason:

The CIA/RT processing component has detected an error on the CIASTATS file while attempting to add result data generated by the STATUS command. In most cases this error represents an out of space condition in the CIASTATS file. &status will display as one of the following:

File has been closed to future requests

Error has been ignored

STATUS command output will continue displaying on the operator console but no additional data will be added to the CIASTATS file.

Action:

Enter the “F CIARTUPD,RESET CIASTATS” command to erase all current CIASTATS data and begin adding new STATUS command output at the start of the file. You may also want to consider increasing the size of the CIASTATS file to avoid the loss of data on future requests.

Module:

CIARTSTS

CIA0481I

CIA/RT Component – CIASTATS file reset - &status

Reason:

The CIA/RT processing component has successfully processed a request to RESET the CIASTATS file following the error condition highlighted by message CIA0480E. &status will display as one of the following:

Action will be taken on next I/O

Action successfully completed

The first &status message displays immediately following the successful execution of the “F CIARTUPD,RESET CIASTATS” command. The second &status message displays when the first "F CIARTUPD,STATUS” command is entered following the RESET.

Action:

This message is informational only. No action is required.

Module:

CIARTMGR, CIARTSTS

CIA0490I

CIA/RT Journal File Initialization Complete

Reason:

The CIA real-time journal file initialization job has completed successfully.

Action:

This message is informational only. No action is required.

Module:

CIARTIJL

CIA0491E

CIA/RT SYSIN File Open Error

Reason:

The CIA real-time journal file initialization job could not successfully open the SYSIN file.

Action:

Determine the reason for the failure from the open failure messages received. Correct the problem and rerun the job.

Module:

CIARTIJL

CIA0492E

CIA/RT Invalid Parameter, BLOCKS= Not Found

Reason:

The SYSIN input card read in from the CIA real-time initialization job was not the required card. The only valid card must begin with BLOCKS=.

Action:

Ensure that the only SYSIN input card begins with BLOCK=. Correct the input card and rerun the job.

Module:

CIARTICL

CIA0493E

CIA/RT Invalid Parameter, BLOCKS= Invalid

Reason:

The SYSIN input card read in from the CIA real-time initialization job was not valid. The specified number of blocks contained an invalid amount.

Action:

Verify that the number of blocks specified for the BLOCKS= on the SYSIN input card contains a valid numerical value that does not begin with zero. Correct the value and rerun the job.

Module:

CIARTIJL

CIA0494E

CIA/RT SYSIN File Error - No Parameters Entered

Reason:

The SYSIN input file contained no data. A required input card that begins with BLOCKS= must be specified.

Action:

Ensure that the SYSIN input file contains one input card that begins with BLOCKS= and rerun the job.

Module:

CIARTIJL

CIA0495E

CIA/RT Journal File Open Error

Reason:

The CIA real-time journal file initialization job could not successfully open the journal file.

Action:

Determine the reason for the failure from the open failure messages received. Correct the problem and rerun the job.

Module:

CIARTIJL

CIA0496E

CIA/RT Error Writing to Journal File

Reason:

The CIA real-time journal file initialization job could not successfully write to the journal file.

Action:

Determine the reason for the failure from the write failure messages received. Correct the problem and rerun the job.

Module:

CIARTIJL

CIA0497E

CIA/RT Component Journal &function Failure - RC=*&retcode* RSN=*&rsncode*

Reason:

The CIA real-time processing component has attempted to access the journal file and the request has failed. The journal function attempted will be one of the following: OPEN, CLOSE or WRITE. &retcode and &rsncode are the return code and reason code for the failure.

Action:

If the function request is OPEN, check the CIA real-time component procedure for a valid CIAJRNL DD statement. For all other failures contact CA Support at http://ca.com/support.

Module:

CIARTMGR, CIARTJNL

CIA0500 Series Messages

CIA0500E

***Modname* parameter error**

Reason:

The CIA real-time stored procedure module identified in the message was called with an invalid parameter list. The CIA real-time stored procedure processing terminates and the message is returned to the request to be recorded in the CIA real-time component journal.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIASPAL1,CIASPAR1,CIASPCR1,CIASPDR1,CIASPROL

CIA0501E

Module *modname* routine *rtnname* insufficient storage for execution

Reason:

The processing in the module routine identified in the message could not obtain the storage required for an internal buffer or table. The CIA real-time stored procedure processing terminates and the message is returned to the request to be recorded in the CIA real-time component journal.

Action:

Increase the region size for the WLM environment defined for the CIA real-time stored procedure to provide more available storage

Module:

CIASPAL1,CIASPAR1,CIASPCR1,CIASPDR1,CIASPROL

CIA0502E

Module *modname* routine *rtnname* CIASPSQL error - RC=*returncode* RSN=*reasoncode*

Reason:

The processing in the module routine identified in the message received an unexpected error calling an internal service routine. The CIA real-time stored procedure processing terminates and the message is returned to the request to be recorded in the CIA real-time component journal.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIASPAL1,CIASPAR1,CIASPCR1,CIASPDR1

CIA0503E

Module *modname* routine *rtnname* SQL error – SQLCODE=*sqlcode*

Reason:

The processing in the module routine identified in the message received an unexpected error from DB2 in response to an SQL request. This may be caused by a problem in the stored procedure definition or by inconsistencies in the data in the CIA repository. The CIA real-time stored procedure processing terminates and the message is returned to the request to be recorded in the CIA real-time component journal.

Action:

Look up the meaning of the SQL code in the DB2 manuals. If you can identify the problem with the DB2 environment or the CIA repository, correct the problem. For assistance, contact CA Support at http://ca.com/support.

Module:

CIASPAL1,CIASPAR1,CIASPCR1,CIASPDR1

CIA0504E

LOAD failed for module *modname* R1=*abendcode* R15=*reasoncode*

Reason:

The CIA real-time stored procedure request to load the program indicated by the message failed. The reasons indicated by values in general register one (r1) and general register fifteen (r15) are the values provided upon return from the LOAD Macro and indicate the reason for the failure.

Action:

Consult the IBM MVS Programming: Authorized Assembler Services Reference to determine the reason for the failure. The most like error is that the module is not available to the CIA real-time stored procedure WLM environment. If you can identify the problem, correct it. For assistance, contact CA Support at http://ca.com/support.

Module:

CIASPROL

CIA0800 Series Messages

CIA0801I

CIA process initialization has begun

Reason:

The CIA DB2 processing component has begun the initialization process.

Action:

This message is informational only. No action is required.

Module:

CIADSINI

CIA0802I

CIA process initialization complete

Reason:

The CIA DB2 processing component has successfully completed initialization.

Action:

This message is informational only. No action is required.

Module:

CIADSINI

CIA0803E

Unable to load module *modname*. CIA initialization terminated

Reason:

An attempt has been made to start the DSI component and the necessary programs cannot be found in an available library, so the startup has been terminated.

modname

Identifies the module that failed to load.

Action:

Place the DB2 library containing the specified module in the link list or make it available as a STEPLIB to the DSI address space and restart the DSI component address space.

If DBTYPE=DATACOM and you are using CA Datacom as your repository, contact CA Support for assistance.

Module:

CIADSINI, CIADSPRM

CIA0804E

Unable to locate module *modname*. CIA initialization terminated

Reason:

An attempt has been made to start the DSI component and the necessary programs cannot be found in an available library, so the startup has been terminated.

modname

Identifies the module that was not found.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSINI

CIA0805W

The DB2 subsystem *ssid* is not active

Reason:

An attempt to connect to the specified DB2 subsystem failed because it was not active. Processing is not terminated.

ssid

Identifies the DB2 subsystem id that was specified in the DSI configuration file.

Action:

Start the specified DB2 subsystem or further errors may occur.

Module:

CIADSPRM

CIA0809I

CIA process termination complete

Reason:

The DSI CIA plugin has successfully terminated processing.

Action:

This message is informational only. No action is required.

Module:

CIADSTRM

CIA0810E

The *keyword* keyword is not supported. CIA initialization terminated

Reason:

The specified keyword is not valid.

keyword

Specifies the invalid keyword.

Action:

Correct the keyword in the DSI configuration file and restart DSI.

Module:

CIADSPRM

CIA0811E

The *keyword* parameter value is invalid. CIA initialization terminated

Reason:

The value specified for the keyword is not valid.

keyword

Specifies the keyword for which an invalid value is specified.

Action:

Correct the value for the keyword in the DSI configuration file and restart DSI.

Module:

CIADSPRM

CIA0812E

The *parm* parameter is required. CIA initialization terminated

Reason:

The specified parameter was not found in the configuration file.

parm

Specifies the required parameter that was not provided.

Action:

Modify the configuration file so it contains the required parameter.

Module:

CIADSPRM

CIA0819E

Mutually exclusive values were specified for *keyword* keyword. CIA initialization terminated

Reason:

More than one value was specified for the *keyword* and the values are mutually exclusive.

keyword

Specifies the keyword for which mutually exclusive values are specified.

Action:

Determine the correct value for the keyword. Correct the DSI configuration file and restart DSI.

Module:

CIADSPRM

CIA0821E

CIA/RT SQL ERROR - SQLCODE= *code*

Reason:

A request to update the CIA database was denied.

code

Specifies the SQLCODE that was returned in decimal format.

Action:

Additional messages with a DSNT message ID prefix might be displayed to provide diagnostic information about the SQL error. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSREQ

CIA0890E

Error in *modname* request parameter list

Reason:

The specified module detected an error in the parameter list that was passed.

modname

Identifies the module that detected an error in a parameter list.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Modules:

CIADSINI, CIADSPRM, CIADSREQ, CIADSTRM, CIADSCLN

CIA0891E

Insufficient storage for *modname* execution

Reason:

An attempt has been made to obtain storage in the DSI address space, and the request has failed.

modname

Identifies the module that attempted to obtain storage.

Action:

Increase the region size for the DSI address space to provide more available storage.

Module:

CIADSINI, CIADSREQ

CIA0892E

RRSAF function to DB2 subsystem ssid failed. Return: *retcode* Reason: *rsncode*

Reason:

An attempt to connect to DB2 using RRSAF failed.

function

Identifies the RRSAF function that failed.

ssid

Identifies the DB2 subsystem that was specified in the function call.

retcode

The return code received from RRSAF.

rsncode

The reason code received from RRSAF.

Action:

For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSPRM, CIADSREQ, CIADSTRM

CIA0893E

Error in *modname* - CIA Global area not found

Reason:

The CIA Global area was not found by the specified module.

modname

Identifies the module that could not locate the Global control block.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSDSN

CIA0894E

The CIA repository must be either DB2 or Datacom

Reason:

During the processing of a specific CIA update request, the CIA processing found that DB2 or CA Datacom indicators were set in the internal control blocks. These are the only two supported repository types. The CIA update request is failed and CIA real-time processing is suspended until the problem is resolved.

Action:

This is probably an internal process error. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSPEI, CIADSRQ1, CIADSRQ2, CIADSPET, CIADSTRM

CIA0895E

Unable to load module *modname*. CIA update request terminated

Reason:

During the processing of a specific CIA update request, the necessary programs could not be found in an available library. *Modname* identifies the module that failed to load. The CIA update request is failed and CIA real-time processing is suspended until the problem is resolved.

Action:

The programs were available during the DSI address space initialization, so something has changed in the execution environment. Identify and correct the problem to make the program available to the DSI address space.

Module:

CIADSPEI

CIA0896E

The *function* of Datacom region *mufid* failed. Return: *retcode* Reason: *rsncode*

Reason:

The attempt to connect to a Datacom address space failed.

function

Identifies the Datacom function that failed.

mufid

Identifies the Datacom region that was specified in the function call.

retcode

The return code received from Datacom.

rsncode

The reason code received from Datacom.

If the error is encountered during CIA initialization, the CIA initialization process is terminated. If the error is encountered during the processing of a specific CIA update request, the CIA update request is failed and CIA real-time processing is suspended until the problem is resolved.

Action:

Determine why the connection to the Datacom region failed and resolve the problem. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADSPRM,CIADSPEI

CIA0900 Series Messages

CIA0901E

Unable to locate SAF IVT

Reason:

A critical CA SAF control block could not be located. An improper installation of the external security manager or corruption of common storage can be the cause. CIA Datacom conversion utility processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADCCNV

CIA0902E

Insufficient storage for execution

Reason:

The CIA Datacom conversion utility could not obtain the storage for a record buffer or an internal table. CIA Datacom conversion utility processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADCCNV

CIA0903E

Unable to open the *file* data set

Reason:

The CIA Datacom conversion utility job could not successfully open the *file* file.

Action:

Determine the reason for the failure from the open failure messages received. Correct the problem and rerun the job.

Module:

CIADCCNV

CIA0904E

The *ti* table encountered in an input record is not supported for Datacom conversion

Reason:

An input record has a table identifier that is not known or supported for the CIA unload DB2 to Datacom conversion utility. The value of *ti* specifies the invalid table identifier.

Action:

The version of the CIA DB2 to Datacom conversion utility is probably different than the version of the CIA unload utility, which has unloaded a table that the conversion utility does not support. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADCCNV

CIA0905E

An invalid record was encountered in the UNLDUSER input data set

Reason:

The UNLDUSER input to the CIA Datacom conversion utility contained a reference to a table other than USERFLD. CIA Datacom conversion utility processing terminates.

Action:

This message indicates that there is a logical problem with the product execution. For assistance, contact CA Support at http://ca.com/support.

Module:

CIADCCNV

Chapter 9: Abend Codes

ABEND codes tell you when a task ends abnormally because of an unrecoverable system error. The following ABEND codes indicate problems with CA Top Secret or TSS commands.

TSSMNGR4 (TSS Address Space) ABEND Codes

USER — 0001

Reason:

CA Top Secret was started as other than an O/S command.

Action:

Start CA Top Secret from a console as a started task.

USER — 0002

Reason:

CA Top Secret is already active.

Action:

Bring down the existing CA Top Secret before starting a new CA Top Secret.

USER — 0003

Reason:

Insufficient fixed storage exists in CSA for CA Top Secret to start. CA Top Secret requires a fixed CSA page (4K).

Action:

This is probably a system-wide problem and will require an IPL.

USER — 0004

Reason:

Operator replied “x” in response to the TSS9055A prompt.

Action:

None. Restart CA Top Secret again to replace RACF or activate the TSS command.

USER — 0006

Reason:

The Security File cannot be accessed.

Action:

Ensure that the SECFILE DD statement exists in the CA Top Secret procedure.

USER — 0009

Reason:

Major version change. CA Top Secret was restarted on a machine running a prior version of CA Top Secret.

Action:

IPL to start the new version of CA Top Secret.

USER — 0010

Reason:

A required module was not found in the program library.

Action:

See the *Installation Guide*.

USER — 0011

Reason:

A required module was not found in the program library.

Action:

See the *Installation Guide*.

USER — 0012

Reason:

A required module, TSSFLIH, was not found in the program library or was not loadable.

Action:

See the *Installation Guide*.

USER — 0015

Reason:

Unable to establish ESTAE for the TSS address space.

Action:

Restart CA Top Secret. If problem persists, contact CA Technical Support.

USER — 0020

Reason:

Unable to load module, TSSSYSFM, from the program library.

Action:

Check the CA Top Secret program library for TSSSYSFM.

USER — 0030

Reason:

Unable to initialize log interface due to CSA shortage.

Action:

Increase available (E)CSA and re-IPL.

USER — 0031

Reason:

CA Top Secret was unable to FREEMAIN its temporary restart copy of the RCVT.

Action:

Restart CA Top Secret. If problem reoccurs, IPL.

USER — 0099

Reason:

An error occurred during SFS initialization.

Action:

Examine abend code and/or TSS dump. If the problem resulted from CA Top Secret, you may have to recover the Security File.

USER — 0101

Reason:

TSSOPCOM can not locate the RCVT.

Action:

Restart CA Top Secret. If problem reoccurs, contact CA Technical Support.

USER — 0999

Reason:

Security File Services failure.

Action:

Restart CA Top Secret. If problem reoccurs, use alternate Security File.

TSSPROT ABEND Codes

Code	Explanation
1201	Unable to open PROTIN
1202	Unable to open PROTOUT
1205	Reply was “N” to TSS8601A
1210	I/O error occurred while reading the VTOC
1211	Unable to open a VTOC
1212	Cannot locate VTOC
1213	Volume not mounted
1214	No authority. Not an SCA.
1215	I/O error occurred while updating the VTOC
1218	Cannot load module IDCAMS
1299	Trace dump

TSSMAINT ABEND Codes

Code	Explanation
1500	Unable to open MAINTIN
1501	Unable to open MAINTOUT
1502	Invalid control statement verb (not CREATE)
1503	CA Top Secret cannot be active for CREATE
1504	Invalid control statement
1505	Syntax error in control statement

Code	Explanation
1506	Unable to open Security File
This abend is also displayed as a normal part of running TSSMAIND. (TSSMAIND is used during installation to calculate the number of blocks required for the Security File).	
1508	Password required for SCA definition
1509	Non-numeric specified.
1510	Error creating Security File. See SYSPRINT output for further details.
1513	Not Master SCA
1514	Same as 1506 for DUMP option
1515	Security File BLOCKSIZE is different from JCL-supplied BLOCKSIZE. Do not code the BLKSIZE keyword in the JCL.
1516	Unable to open Audit/Tracking File.
1517	Unable to open Recovery File or the Recovery File was specified incorrectly with Keys.
1518	Blocksize too small
1519	Unable to open CPF Recovery File
1520	VSAMFILE initialization failed. **Note:** TSSMAINS can be run only once using the same VSAMFILE DD data set. To rerun TSSMAINS, delete and recreate the VSAMFILE data set.
1521	AESENCRYPT can only be specified when running CA Top Secret r14 or higher
Review the sysprint output of the TSSMAINT job for further information about the error or abend.	

TSSCNV43 ABEND Codes

U0001

Reason:

The CNVIN (SYSIN) file did not open or the KEY= parameter was not specified.

Action:

Rerun TSSCNV43, including the missing parameter.

U0002

Reason:

The CNVOUT (SYSPRINT) file did not open successfully.

Action:

Rerun TSSCNV43, including the CNVOUT DD statement.

U0003

Reason:

TSSCNV43 was unable to open the existing 4.2 security file, or the data set pointed to by the SECFOLD DD statement was not a valid 4.2 security file.

Action:

Ensure that SECFOLD DD statement is pointing to the active 4.2 security file.

U0004

Reason:

TSSCNV43 was unable to open the new 4.3 file or the data set pointed to by the SECFNEW DD statement was not a valid 4.3 security file.

Action:

Ensure that SECFNEW DD statement is pointing to the new security file created by the 4.3 version of TSSMAINT.

U0005

Reason:

The ACID is not authorized to run TSSMAINT. Only the MSCA may run TSSMAINT.

Action:

Have the MSCA rerun the job or have an authorized user submit the job while specifying the USER=msca-acid parameter in the JCL.

U0006

Reason:

CA Top Secret 4.2 is not active.

Action:

Rerun the job after bringing up CA Top Secret.

U0007

Reason:

The KEY= parameter specified an invalid value.

Action:

Rerun the job using the proper syntax for the KEY= parameter. If specified as an eight digit character string, it must be contained within single quotes. If specified as a string of sixteen hexadecimal digits, it must be specified as a single string, without quotes, imbedded blanks or commas.

U0008

Reason:

Partially converted security file

Action:

A previous run of TSSMDS on CA Top Secret VM failed and left a partially converted Security File. Restore the Security File at a point previous to that failed run or specify CUUCONV=AUTO.

U0009

Reason:

Duplicate CUU conversion attempted

Action:

You specified CUUCONV=YES but the CUU conversion had previously been done on CA Top Secret VM. Specify CUUCONV=NO or CUUCONV=AUTO and rerun the job.

U1001

Reason:

During conversion, the volume index within the security file filled.

Action:

Create a new security file with TSSMAINT specifying a larger value for the VOLUMES= parameter.

U1002

Reason:

Internal conversion error. Resource Index is full.

Action:

Contact CA Technical Support.

U1003

Reason:

Internal conversion error. Prefix Index is full.

Action:

Contact CA Technical Support.

U1004

Reason:

During conversion, the ACID index within the security file filled.

Action:

Create a new security file with TSSMAINT specifying a larger value for the ACCESSORS= parameter.

U1005

Reason:

During conversion, the ACID record pool within the security file filled.

Action:

Create a new security file with TSSMAINT specifying a larger value for the ACCESSORS= parameter.

U1006

Reason:

Internal conversion error.

Action:

Contact CA Technical Support.

U1007

Reason:

Internal conversion error.

Action:

Contact CA Technical Support.

U1010

Reason:

Internal conversion error. RDT conversion error.

Action:

Contact CA Technical Support.

U1011

Reason:

Internal conversion error.

Action:

Contact CA Technical Support.

U1012

Reason:

Internal conversion error.

Action:

Contact CA Technical Support.

U1013

Reason:

Internal conversion error. Block map out of sync.

Action:

Re-create Security File and rerun.

U1014

Reason:

Internal conversion error.

Action:

Re-create Security File and rerun.

U1015

Reason:

Internal conversion error. Allocated block out of range.

Action:

Recreate 4.3 Security File and rerun.

U1016

Reason:

Internal conversion error.

Action:

Contact CA Technical Support.

U1017

Reason:

Internal conversion error.

Action:

Contact CA Technical Support.

U1018

Reason:

GETMAIN error.

Action:

Increase region size.

U1019

Reason:

During conversion process, CA Top Secret detected an existing ACID that was using a reserved ACID number.

Action:

DELETE and re-CREATE specified ACID and re-run conversion utility.

TSSUTIL ABEND Codes

Code	Explanation
1600	User not authorized to use TSSUTIL (for example, user is not a control ACID or does not have REPORT authority)
1601	CA Top Secret is not active
1602	No authority
1603	No report administration authority
1604	Referenced department is not yours
1605	Referenced division is not yours
1606	Department unknown
1607	ACID not defined to CA Top Secret
1608	Referenced ACID not in your department
1609	Syntax error in control statement
1610	Unknown option in control statement
1611	DCA can not supply departments
1612	Specified department not in your division
1613	Division unknown
1614	Division not within your scope of authority
1615	Department not within your scope of authority
1616	ACID not within your scope of authority
1617	No report authority (for example, a user who is not an SCA attempted to use the ACID( ) keyword
1618	Unable to open SYSPRINT

Code	Explanation
1619	Unable to open SYSIN
1620	Invalid date or time span
1621	Unable to open GRO file
1690	Storage GETMAIN failed
1692	Unable to open SMFIN
1693	Unable to open SMFOUT
1699	CA Top Secret cross-memory communications failure

TSSRECVR ABEND Codes

Code	Explanation
1700	No authority to use utility (not an SCA).
1701	Unable to open RECVFILE, RECVCMDS, or RECVPRT.
1702	CA Top Secret is not active; abort requested.
1703	Invalid option supplied via EXEC PARM.
1717	I/O error occurred when processing the Recovery File. See message TSS8112E.

TSSTRACK ABEND Codes

Code	Explanation
1801	Server error occurred.
1802	Diagnostic trap location reached.
1804	Terminal I/O Interface routine error.
1805	Terminal I/O Interface routine error.

TSSAUDIT ABEND Codes

Certain error conditions cause TSSAUDIT to abend with one of the user abend codes shown below.

Code	Explanation
2700	User not authorized to perform function
2701	CA Top Secret inactive
2702	CA Top Secret is down
2703	Unable to open RECOVERY data set
2704	Unable to open AUDITIN data set
2705	Unable to open AUDITOUT data set
2706	Invalid function specified
2708	Could not obtain security information
2709	Could not obtain security information
2713	Wrong file specified for RECOVERY file
2717	Could not obtain user's security record
2718	Could not access Security File
2719	Insufficient storage in region running report.
2720	Unable to free storage
2729	Permanent I/O error-accessing RECOVERY data set

TSSCHART ABEND Codes

Code	Description
0998	Produced immediately after TSS1004E or TSS1017E message issued the error was caused by CA Top Secret or another vendor product.

TSSXTEND Abend Codes

The following table describes TSSXTEND ABEND codes:

Code	Description
0001	SYSIN DD missing or KEY= missing
0002	SYSPRINT DD missing
0003	SECFILE DD missing or specified file is invalid format
0004	SECFNEW DD missing
0005	ACID supplied is not the MSCA
0006	CA Top Secret is not active
0007	Key parameter is invalid
0008	New file not formatted
0010	Unable to open VSAM file
0999	DEBUG ABEND
1001	Volume index full
1002	Resource index full
1003	Prefix index full
1003	Prefix index full
1004	ACID index full
1005	ARLB segments full
1006	QMAN failure
1007	RARB not returned from SFS
1010	Error converting RDT
1011	Allocated too many blocks for AREC
1012	Allocated an ARLB out of range
1013	Block map out of synch with key
1014	Free ARLB not nulls
1015	Allocated block out of range
1016	BAD ENTRY IN VIX
1017	BAD ENTRY IN PIX
1018	BAD ENTRY IN MLX

Code	Description
1019	MLS INDEX FULL
3000	No function supplied
3001	Cannot open SECFOLD
3002	Cannot open SECFNEW
3003	Cannot open MAINTOUT
3004	Cannot open MAINTIN
3005	Encryption Key (existing) is incorrect
3006	Invalid Encryption Key or Damaged ACID
3007	New file incorrectly formatted
3008	New file contains too few BLOCKS in TSSXTEND JCL or incorrect SYSIN parameters: use TSSFAR.
3009	New File is not new; prior EXTEND failed and file is not reformatted
3010	Logical error. Contact CA with dump.
3013	SECFOLD missing
3014	Not enough private storage area
3015	Unknown function specified in the control statements input file.
3016	Unknown input parameter specified in the control statements input file.
3018	Invalid parameter in control statement
3019	AES encryption error processing password
3020	Encryption Key not supplied
3021	Invalid Key
3028	Security File repair function was unable to verify unexpected anomaly
3029	AES encryption error processing password phrase
3031	Invalid Parameter encountered
3032	Illegal syntax specified for parameter
3033	Hexadecimal value must be 0-9, A-F
3034	Length value must be between 01 and FFFF
3055	Invalid hexadecimal number

Code	Description
3036	Data is missing
3037	Invalid acidname
3038	RBA not within file
3039	ACID not defined
3040	Max ACID size in new file header is smaller than the value in old file header
3042	Input file does not have AES feature
3044	Output file does not have AES feature
3045	Max ORG ACID size in new file header is smaller than the value in old file header
3046	No max ORG ACID size defined in new file and max ACID size in new file header is smaller than max ORG ACID size in old file header
3099	WHOHAS function disabled

TSSFAR ABEND Codes

Code	Explanation
2700	Not the MSCA
2701	Failed getmain
2702	Bad input parameters
2703	KEY= card missing
2704	Bad hex character in supplied key
2705	Error trying for security file lock
2706	Error trying for security file unlock
2707	Target XE area too small for input
2708	Duplicate or missing file specification
2709	RACVT missing
2710	SYSPRINT open error
2711	SYSIN open error
2712	SECFILE open error

Code	Explanation
2800	Error reading resource index (RIE)
2801	Error reading volume index (VIE)
2802	Error reading volume prefix index (VIE)
2803	Error reading prefix index (PIE)
2804	Block read is not a valid reader record
2805	Get ARLB error
2806	Error reading ACID index (AXE)

TSSENQ ABEND Code

Code	Description
U007	The operator selected the ABORT option during system startup after receiving message TSS9130A, TSS9131A, TSS9133A, or TSS9138A. One of these messages appeared when the operator's local system encountered a problem attempting to connect to the Coupling Facility.

CICS Abend Codes

Code	Module that Issued the ABEND and Explanation
KR01	CAKSROUT - Allocation task token failure.
KR02	CAKSROUT - Allocation session related token failure.
KR03	CAKSROUT - Session related token missing ACEE address.
KS01	CAKSIGN - Maximum signon limit reached.
KV01	CAKSRVAL - File open error.
PW01	CAKSPWH - A command error occurred during an EXEC CICS receive.
TBZ5	TSSCPW - Password prompt send/receive error.
TAZ6	TSSCMS - Message send command error.
TAZ7	TSSCMS - ABEND request from message exit routine.
TAZ8	TSSCMS - Message send to invalid device error.
TEZ0	TSSCST - Command error.

Code	Module that Issued the ABEND and Explanation
TG1B	TSSCPOST - ACEE/SECREC getmain failure.
TG1C	TSSCPOST - DFHTRAC0 attach failure due to lack of LSQA.
TG1D	TSSCPOST - DFHTRAC0 attach failure.
TG1E	TSSCPOST - Invalid parameter list passed to DFHTRAC0.
TG1F	TSSCPOST - TSSCRINT STCB getmain error (lower Maxsign parameter).
TG1G	TSSCPOST - TSSCSMGR logic error.
TG1H	TSSCPOST - MAXSIGN limit reached. Maximum SIGNON/SIGNOFF requests, No Retry Specified.
TG8W	TSSCPOST - Storage manager DUSB getmain failure.
TG8X	TSSCPOST - Storage manager DUSB invalid parameter list.
TMOS	Sending CICS region has MOS feature active, but receiving system does not.
TSF1	TSSCDFSB - Attempt to run TSSF attached to terminal. A user has attempted to run this transaction at a terminal. This is an internal transaction and cannot be executed.
TSF2	TSSCDFSB - CA Top Secret is not active. This may indicate an installation 00878 problem. Contact CA Top Secret Technical Support.
TS1A	TSSCCTSS - CA Top Secret write error or more than 500 CA Top Secret puts.
TS1B	TSSCCTSS - Send command error KA52151.
TS1C	TSSCCTSS - Receive command error KA52151.
TS1D	TSSCCTSS - Command error KA52151.
TUZ3	TSSCICS - CA Top Secret is not active.
TUZ4	TSSCICS - TSS/CICS control block location error.
TUZ5	TSSCICS - Assign Command Failure.
TZZ1	TSSCAI - TSS/CICS application interface transaction is not associated with a terminal.
TZZ2	TSSCAI - TSS/CICS application interface logic error (Assign Command Error).
TZZ3	TSSCAI - TSS/CICS application interface parameter list address invalid.

Code	Module that Issued the ABEND and Explanation
TZZ4	TSSCAI - TSS/CICS application interface Read Temporary Storage Queue ID error.
TZZ5	TSSCAI - TSS/CICS application interface parameter list length error.
TZZ6	TSSCAI - TSS/CICS application interface Write Temporary Storage Queue ID error.
TZZ7	TSSCAI - TSS/CICS application interface parameter list length does not equal parameter list type or invalid value in header field.
TZZ8	TSSCAI - TSS/CICS application interface call was unable to attach a subtask to complete the request.
T11W	TSSCRT - Storage manager USCB/TTCB bad parameter list.
T11X	TSSCRT - MAXUSER limit reached (reset maxuser).
T11Y	TSSCRT - Storage manager USCB/TTCB getmain failure.
T26Z	TSSCXS - CICS control block address error.
T283	TSSCXS - DSNB/FILE access error.
T310	TSSCXE - Invalid function request parameter.
T634	TSSCFM - DSNB/FILE access error.
T6??	TSSCFM - CICS resource control block not found.
U751	CAKSALOC - LOCATE SRT FAILURE
U752	CAKSALOC - SRT CONTAINS AN INVALID ACEE ADDRESS

In addition to these CICS ABENDs, CA Top Secret invokes the External Security Manager and makes checks against the PSB at scheduling time. If the installation is able to schedule the PSB, it returns the DBD names. If you are not authorized to access the DBD, a DHA4 ABEND occurs.

CA C Runtime ABEND Code

CA C Runtime can issue the following ABEND:

UPRG

The CA Common Services for z/OS, CA C Runtime, has not been fully installed. Confirm that the CA-C Runtime programs and transactions are fully defined and installed in your CICS environment. For installation details, see the *CA Common Services for z/OS Getting Started*.