CA Top Secret® for z/OS

Control Options Guide

r15

Ninth 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.

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 in this release of this documentation:

- CICS-Related FACILITY Suboptions (see page 93)—Added CISP, CIS1, CJSL, CRST, and CPCT to the default Bypass and Protect List information.
- Options for Invoking Predefined Facilities (see page 107)—Added CISP, CIS1, CJSL, CRST, and CPCT to the bypass list information.
- INACTIVE—Deny Use of Unused ACIDs (see page 119)—Modified the maximum value for the number of days after which the product prohibits signon for an unused ACID that is connected to an expired password.
- NEWPW—Restrict Password Alterations (see page 157)—Added { and } to the list of characters that passwords can contain by default; indicated that MINDAYS is applicable to password changes made with the TSS ADDTO/REPLACE command, except when the PWADMIN(YES) control option is specified; noted that PWADMIN(YES) is not applicable to the NU or RN setting.
- PWADMIN—Enforce NEWPW Rules for Administrative Password Changes (see page 186)—Added this section, describing control option that enforces NEWPW control option rules and password interval specification when an administrator or user with MISC8(PWMAINT) or ACID(MAINTAIN) authority performs a password change through a TSS command.

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

- Options for Invoking Predefined Facilities (see page 107). Provided an introductory explanation for the section; updated the default settings for the CICSPROD and CICSTEST facilities.
- CPFAUTOGID—Insert a Specific USS GID During CPF Command Processing (see page 49). Added this section for a new control option that transmits a TSS command with an assigned GID value, instead of the '?' value, when you are using the Command Propagation Facility (CPF) feature.
- CPFAUTOUID—Insert a Specific USS UID During CPF Command Processing (see page 50). Added this section for a new control option that transmits a TSS command with an assigned UID value, instead of the '?' value, when you are using the Command Propagation Facility (CPF) feature
- FSACCESS—Enable or Disable FSACCESS Resource Class Checks (see page 114). Clarified that all entry methods are accepted.
- MODLUSER—Identify an OMVS Model User (see page 150). Removed UID from the list of fields that is provided to ACID. Announced variable specification for HOME field; which the current user ID value replaces when MODLUSER information is added to a user’s ACID record. Added DFLTGRP to the list of fields that is provided to the ACID.

- OMVSGRP—Assign an OMVSGRP Segment and Default Group (see page 166). Clarified that OMVSGRP is not supported in z/OS 2.1 and above, in which case you can use UNIQUSR and MODLUSER instead.
- OMVSUSR—Assign an OMVS Segment for Extract (see page 167). Clarified that OMVSUSR is not supported in z/OS 2.1 and above, in which case you can use UNIQUSR and MODLUSER instead.
- OPTIONS—Specify Configuration Options (see page 168). Added description for option value 79, which specifies to write an SMF record when control option OMVSUSR or OMVSGRP is used to provide a default UID or GID, respectively. Updated description for option 72, which allows a MASTFAC (Master Facility) on all ACID types capable of signon.
- UNIQUSER—Assign a UID Automatically During OMVS Logon (see page 236). Corrected the example syntax.

Contents

Chapter 1: Introduction 15

Chapter 2: Specific Control Options 25

Chapter 1: Introduction

This section contains the following topics:

About Control Options

Control options allow selected operators and security administrators to specify how CA Top Secret controls security. Use control options to:

- Reset the security MODE.
- Determine how CA Top Secret processes successfully and under specific security MODES and circumstances.
- Indicate what features, facilities, or products are on the operating system.
- Specify how individual facilities are handled.
- Specify password selection rules and violation thresholds.
- Issue the commands that force CA Top Secret to reset after shutdown or reinitialize after installation of CA Top Secret maintenance.

Control Option Entry Methods

CA Top Secret provides five methods for selecting and changing control options:

O/S START Command

Specify that a control option initiates with the O/S START command.

Started Task Procedure

Add or change control options at CA Top Secret startup.

Parameter File

Specify a set of control options at CA Top Secret startup. CA Top Secret takes site-standard control options from the Parameter File (PARMFILE). The parameters can optionally be overwritten by specifying an option list as part of the START command for the CA Top Secret started task.

TSS MODIFY Command

Add or change control options from an online terminal.

O/S Modify Command

Add or change control options from the O/S console. For example:

Commands continue in effect until they are overridden or until the TSS task is terminated.

The O/S START Command

The CA Top Secret START command specifications:

- Replace any specified in the CA Top Secret Procedure PARM field
- Override parameters that are specified in the Parameter File

CA Top Secret control options can be specified as part of the O/S Start command that is used to initiate the CA Top Secret started task. The format for the O/S Start command is:

```
S TSS,,,(option,option,...)
```

If a restricted CA Top Secret control option is specified as part of the started task, CA Top Secret prompts the person entering the command for authorization before processing the request.

The Started Task Procedure

The started task procedure must be entered into a started task procedure library (PROCLIB) during the installation of CA Top Secret. TSS procedure PARM overrides the Parameter File. The TSSMNGR4 initialization program honors options that are specified in the PARM field.

Example: The PARM field

```
//TSS      PROC     FILE='name of security file'
//TSS      EXEC     PGM=TSSMNGR4,DPRTY=(15,14),TIME=1440,
//                  REGION=500K,PARM='control options'
//SECFILE     DD      DISP=SHR,DSN=&FILE.
//RECFILE     DD      DISP=SHR,DSN=name-of-recovery file
//BACKUP      DD      DISP=SHR,DSN=name-of-backup file
//PARMFILE    DD      DISP=SHR,DSN=name-of-parameter file,
//     FREE=CLOSE
//AUTOCMDS    DD      DISP=SHR,DSN=name-of-commands file,
//     FREE=CLOSE
//AUDIT       DD      DISP=SHR,DSN=name-of-audit file
//AUDIT2      DD      DISP=SHR,DSN=name-of-alternate audit file
//SYSUDUMP    DD      SYSOUT=A
```

Limited Space for Options

The MVS limits the PARM field to a maximum of 100 characters. To specify any initial set of control options during the installation of CA Top Secret, use this Parameter File.

Options Execute with STC

Control options that are put into the PARM field execute when START TSS is issued for CA Top Secret startup. The options that are specified in the PARM field override similar options that are listed in the Parameter File.

Invalid Commands at Startup

If specified when CA Top Secret starts up, several control options are not valid. If a command specified in the PARM file is invalid at startup, CA Top Secret displays the message:

TSS9074E OPTION NOT VALID AT STARTUP

If an option is misspelled or unsupported by CA Top Secret, the system displays:

TSS9093W INVALID START OVERRIDE OPTION

CA Top Secret starts up but ignores the incorrect option. Correct the option in the PARM field, before issuing the next START TSS command. CA Top Secret displays the invalid option with the message:

TSS9076I CURRENT OPTION IS <option>

The Parameter File

You can change any default setting to tailor security during the security implementation phase. The default for the MODE option is FAIL.

Once entered into the Parameter File, the initial options become a base or foundation. Although these options can be overridden, CA Top Secret reverts to the options listed in the Parameter File when CA Top Secret is restarted after a shutdown.

Creating the Parameter File

During the installation of CA Top Secret, a systems programmer creates a Parameter File. The Parameter File contains an initial set of MSCA selected control options.

The Parameter File is:

- A standard sequential data set.
- Any number of records.
- Control options are entered into the file without commas or separators.
- To delimit a title or comment statement, use an asterisk.
- Entries begin in column one.

Example: parameter file

This example separates several options that are longer than a single command line:

```
FAC(TSO=MODE=IMPL,LOG=(ALL)) * TSO DIFFERENCES
FAC(TSO=LOCKTIME=5)
FAC(TSO=NOLUMSG,RNDPW)
```

Sequential Processing

CA Top Secret processes most of the control options in the Parameter File sequentially. The Global entries must be entered before facility-specific entries to ensure that the facility-specific entries take effect.

Place FACILITY modifications after *all* global modifications:

- MODE
- BACKUP
- NEWPW
- LOG
- DOWN
- FAC(TSO.....)

Example: sequential processing

In this example, CA Top Secret is in WARN mode with TSO in IMPL mode:

```
* SECURITY CONTROL OPTIONS FOR TEST MACHINE
  MODE(WARN)                      * SELECT PROCESSING MODE
  FAC(TSO=MODE=IMPL,LOG=(ALL))    * TSO IS DIFFERENT
  BACKUP(0400)                    * 4 IN MORNING
  NEWPW(MIN=5,MASK=CVCVCV)        * NEW PASSWORD MASKING
```

If the FACILITY control option was specified before the MODE option, CA Top Secret would process all requests under the WARN MODE. Regardless of the facility from which the request was entered.

Examples: changing facility names

This example changes a facility name:

```
FACILITY(USER4=NAME=CICSA)
```

All subsequent control option entries that interact with the newly named facility must contain the new facility name.

This example changes the name of USER4 to CICSA and forces CICSA to process in WARN mode:

```
FACILITY(USER4=NAME=CICSA)
FACILITY(CICSA=MODE=WARN)
```

Given the entries that are shown below, the CICSA facility processes security in WARN mode and contains the NOABEND attribute. More changes must be made to CICSA, not USER4.

```
FACILITY(USER4=MODE=WARN)
FACILITY(USER4=NOABEND)
FACILITY(USER4=NAME=CICSA)
```

Important! Only modify the names of USERxxx facilities. Do not modify the names of product-supplied facilities, except under the direction of CA Top Secret Support.

MODIFY Command for Manipulating Options from an Online Terminal

You can enter control options by using the TSS MODIFY command function.

Note: The administrator attempting to issue the command must have previously been granted CONSOLE authority or PRIVILEG access to TSSCMD.ADMIN.MODIFY in the CASECAUT resource class. For complete information about the MODIFY command, see the *CA Top Secret Command Functions Guide*.

Use the following format for entering control options with TSS MODIFY:

```
TSS MODIFY(control_option[(suboption_list)])
```

If the administrator uses the FACILITY control option with the TSS MODIFY command, the following formats apply:

```
TSS MODIFY(FACILITY(BATCH=MODE=WARN))
```

```
TSS MODIFY(FACILITY(IMSPROD=DEFACID(X)))
```

The Console MODIFY Command

CA Top Secret control options can be entered from a console using the O/S MODIFY command. The operator has the option of entering the command as part of the operator command syntax:

```
MODIFY TSS,(control option(suboption-list))
```

Commands that are entered in this way must conform to operating system restrictions for operator console commands. Use of multiple commas, apostrophes, or parentheses can cause some control options to be rejected when issued as a console operator command. Only one control option is modified in a single operator command, although multiple sub options can be modified within that control option.

Hierarchy of Entry Methods

Control options such as MODE and LOG can be specified globally and by facility. Within the MODE option, user and profile specify control options. You can also specify options using different entry methods at different times. Consider the following points:

- Control options that are entered using the PARM field of the CA Top Secret started-task procedure override similar options in the Parameter File.
- Control options entered using the O/S start command override similar started-task procedure options that are entered in either the Parameter File or the PARM field. They must be keyed in each time.
- The start command overrides can also be specified in the SYS1.PARMLIB member CAITSSxx, where the XX suffix is specified in the SAF initialization member CAISECxx.
- Control Options entered using the O/S Modify or TSS MODIFY commands override similar options entered using other entry methods. Control Options are not retained after CA Top Secret is stopped.
- The TSS commands that specify settings for a specific user override any similar control option for that user.

Stopping the CA Top Secret Started Task

The CA Top Secret started-task procedure can be terminated with the O/S Stop command:

```
P  TSS
```

This operation is protected. Terminating the started task does not terminate the Security Interface. The Security Interface remains active, validating requests even though the started task has been terminated. Shutting down the CA Top Secret started task deactivates Security File inputs and outputs, console communication to the operator, and use of the TSS command. The DOWN options affect all modes, except DORMANT, after the CA Top Secret address space is deactivated. See the control option for details on options available when bringing down the CA Top Secret address space.

If an “end-of-day” shutdown is required to complete an orderly CPU termination, CA Top Secret does not prompt the operator for authorization.

For information about temporary and end-of-day shutdown, see the *User Guide*.

Authority to Enter Options

CA Top Secret protects the most powerful control options against unauthorized entry and change. When a restricted option is changed on the O/S console, CA Top Secret prompts the user for one of the following authorizations before allowing the change to take effect:

- The MSCA's *previous* password
- An ACID that contains the CONSOLE attribute followed by the ACID's password in the format ACID/password

This allows for emergency changes without compromising the MSCA's current password.

Restricted and Unrestricted Options

Control options are categorized as follows:

Restricted control options

Includes any control option that changes the security environment. Any non-MCSA user who attempts to change or specify restricted options at the O/S console must supply the name and password (in ACID/password format) of an ACID that contains the CONSOLE attribute or PRIVILEG access to TSSCMD.ADMIN.MODIFY in the CASECAUT resource class.

Requiring this information allows operations supervisors or CA Top Secret administrators to specify control options. It also leaves an audit trail that leads directly to the ACID under which the specification was made.

PRIVILEG access is granted through the following command:

```
TSS PERMIT(acid) CASECAUT(TSSCMD.ADMIN.MODIFY) ACCESS(PRIVILEG)
```

Note: When an MSCA changes or specifies a restricted option at the O/S console, the product automatically uses the MSCA's previous password. This process allows for emergency changes without compromising the MSCA's current password.

Unrestricted control options

Includes control options that request product status displays. Unrestricted control options are as follows:

- FACILITY(*fac*)
- MSG(*nnnn*)
- RPW(LIST)
- ST
- STATS
- STATUS
- VERSION

Chapter 2: Specific Control Options

This chapter provides the format, defaults, entry methods, and descriptions of the CA Top Secret control options.

ADABAS—Control SVC Numbers

Valid on z/OS.

The ADABAS control option controls SVC numbers that ADABAS uses at startup.

This control option uses the parameter file entry method.

Note: Valid for ADABAS 4.8 and 4.9 only. For information about the Software AG security interface for ADABAS r5.0 and above, contact Software AG.

This control option has the following format:

```
ADABAS(nn1,nn2,nn3,nn4)
```

nn1,...,nn4

The SVC numbers (in decimal format) that can be specified.

Range: Up to 4

Example: ADABAS control option

This example indicates that ADABAS uses SVCs 221 and 222 at startup:

```
ADABAS(221,222)
```

ADMINBY—Record Administration Information

Valid on z/OS and z/VM.

The ADMINBY control option records information in ACID security records to indicate:

- Administrative ACID who performed the change.
- Date, time, and system SMFID where the change was performed.

ADMINBY data is stored when:

- An ACID is created.
- A FACILITY is added.
- Resources are permitted.

When ADMINBY is turned on:

- 20 extra bytes are required to store ADMINBY information for the acid being permitted in the owning acid of the resource.
- Extra I/O can be required to record the administration time-stamp.
- The LIST command looks for ADMINBY information, but prints this output only if it is present in the security record.

When ADMINBY is turned off:

- CA Top Secret does not list administrative date-time stamps, even if they were previously generated when ADMINBY was set.
- Administration date-time stamps are not recorded for any ACID administration.

When a security file is shared between systems, one system with ADMINBY turned on and the other system with ADMINBY turned off. Administrative date/time stamps are only recorded on systems where ADMINBY is on.

Administrative date/time stamps are listed when they have been recorded, and on systems where ADMINBY is set.

All entry methods are accepted.

On a *z/VM* system, this control option has the following format:

```
ADMINBY(YES|OFF)
```

ADMINBY(YES)

Administrative date-time stamp to show when and by whom an ACID has been created or altered is written.

ADMINBY(OFF)

(Default) The recording and listing of administrative date-time stamps is suppressed.

On a *z/OS* system, this control option has the following format:

```
ADMINBY|NOADMBY
```

ADMINBY

Administrative date-time stamp to show when and by whom an ACID has been created or altered is written.

NOADMBY

(Default) The recording and listing of administrative date-time stamps is suppressed.

Note: Although it is syntactically incorrect, TSS MODIFY ADMINBY(ON) or NOADMBY(ON) set the control option on and off, respectively. An error message noting the incorrect syntax is displayed.

ADSP—Security Indicator

Valid on z/OS.

The Automatic Data Set Protection (ADSP) control option controls the setting of the security-indicator (RACF bit) in the DSCB of newly created data sets. If the security-indicator is set for a data set and a security product is not operating in the system, the data set cannot be opened. For CA Top Secret, if SAF has been initialized, the security product is considered to be operating and the security-indicator is not checked. For this reason, ADSP(NO) is the recommended setting for this option.

All entry methods are accepted.

This control option has the following format:

```
ADSP (YES|NO|ALL)
```

YES

(Default) Security bit is turned ON for defined users operating in non-DORMANT MODE when any data set is created.

NO

(Recommended) Security indicator is never turned on.

ALL

All entry methods are accepted. The security indicator is turned on in all modes for all users, regardless whether the user is defined to CA Top Secret.

The ADSP control option is not reset to default values when the TSS address space is recycled between IPLs. If ADSP is modified after initialization, that value is preserved across re-initialization unless explicitly modified in the parameter file.

The TSSPROT utility turns the security indicator ON or OFF for selected data sets. For information, see the *Report and Tracking Guide*.

Examples: ADSP control option

This example ensures that the ADSP option remains OFF. Place this example in the parameter file:

```
ADSP(NO)
```

This example ensures that all data sets for all users, which are defined or undefined, have the security-indicator set on:

```
F TSS,ADSP(ALL)
```

AUDIT(SWITCH)—Switch to Alternate Audit Tracking File

Valid on z/VM.

The AUDIT(SWITCH) option forces a switch to the alternate Audit Tracking File if multiple files are being used. If only one ATF is being used, it forces a wrap to the top of the file.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY AUDIT(SWITCH)
```

Example: AUDIT(SWITCH) control option

This example wraps to the top of the alternate ATF when the primary ATF is full:

```
TSS MODIFY AUDIT(SWITCH)
```

AUTH—Merge Records for Search

Valid on z/OS and z/VM.

The AUTH control option indicates whether CA Top Secret:

- Merges the User, Profile, and ALL records for its access authorization search.
- Searches each record separately.

All entry methods are accepted.

This control option has the following format:

```
AUTH(OVERRIDE[,ALLOVER])
```

```
AUTH(MERGE,[ALLOVER|ALLMERGE])
```

OVERRIDE

(Default) Indicates that the User, Profile, and All records are searched separately in the following manner:

- User Record—CA Top Secret searches an ACID's user record for the authorization to access a resource. If CA Top Secret locates this authorization, it continues its search of the entire user record, and grants access to the resource. If the system finds another authorization for the same resource, it grants or denies access based on the PERMIT containing the resource prefix that most explicitly matches the resource being requested. Once this authorization is found in a user record, CA Top Secret does not verify profile records.
- Profile Record—If the system cannot locate the authorization in the user record, it searches each profile in sequence. CA Top Secret searches the entire profile record. Once an authorization record is found in a profile, subsequent profiles are not searched. If more than one authorization is found for the same resource, it grants or denies access using the PERMIT containing the resource prefix that most explicitly matches the resource being requested.

Note: OVERRIDE is mutually exclusive with MERGE and ALLMERGE. OVERRIDE implies ALLOVER.

MERGE

CA Top Secret merges user and profile records, and searches this merged record for the requested authorization. The system does not make an access decision until it has searched the entire merged record.

ALLOVER

(Default) Indicates that if no authorization is found in the user or profile records ALL record are searched.

Note: ALLOVER is mutually exclusive with ALLMERGE.

ALLMERGE

Indicates that the ALL record is merged with user and profile records. ALLMERGE implies MERGE.

AUTOEDSN—Edit AUTOERASE Data

Valid on z/OS.

The AUTOEDSN control option edits the data set selection list that is associated with AUTOERASE(YES). At most, 150 data sets or prefixes can be added to this list.

All entry methods are accepted.

This control option has the following format:

```
AUTOEDSN((ADD|REM),(dataset.prefix|'exact.dataset.name'))
```

ADD

Adds an entry to the list.

REM

Removes an entry from the list.

exact.dataset.name

Any valid O/S data set name enclosed by quotes. When AUTOERASE(YES) is set and a data set is SCRATCHed, if the exact entry on the AUTOEDSN table matches the data set name, DADSM is invoked to overwrite the DASD with nulls.

Range: Up to 44 characters

dataset.prefix

Any valid O/S data set name that is not enclosed by quotes. When AUTOERASE(YES) is set, and a data set is SCRATCHed, if the entry on the AUTOEDSN table matches the initial segment of the data set name, DADSM is invoked to overwrite the DASD with nulls.

Range: Up to 44 characters

Examples: AUTOEDSN control option

This example adds the exact name *highlvl.sampdata* to the autoerase table:

```
TSS MODIFY(AUTOEDSN(ADD,'highlvl.sampdata'))
```

This example adds prefix *sampdata* to the autoerase table as a prefix:

```
TSS MODIFY(AUTOEDSN(ADD,sampdata))
```

This example removes the exact name *highlvl.sampdata* from the autoerase table:

```
TSS MODIFY(AUTOEDSN(REM,'highlvl.sampdata'))
```

This example removes the prefix *sampdata* from the autoerase table:

```
TSS MODIFY(AUTOEDSN(REM,sampdata))
```

AUTOERASE—Control Automatic Data Erase

Valid on z/OS.

The AUTOERASE control option controls the CA Top Secret Automatic Data Erasure feature.

Important! AUTOERASE(YES|ALL) is mandatory if the Department of Defense at C-2 level or higher is certifying the site.

This feature adds extra overhead to the DELETE process adding significant time and physical I/O cycles.

All entry methods are acceptable.

This control option has the following format:

```
AUTOERASE(YES|NO|ALL)
```

YES

When in IMPL or FAIL mode, indicates that AUTOERASE is active for the list of data sets specified by the AUTOEDSN control option. If there are no data set prefixes or data set specifications added to this list; no data sets are auto-erased until entries are added.

NO

(Default) Indicates that the AUTOERASE feature applies to no data sets.

ALL

Indicates that AUTOERASE feature applies to all data sets in all modes.

Examples: AUTOERASE control option

This example ensures that the Automatic Data Erasure feature is active, by entering the AUTOERASE option into the Parameter File:

```
*
SAMPLE CONTROL OPTIONS
*
MODE(FAIL)
BACKUP(0400)
AUTOERASE(YES)
```

This example temporarily turns off the feature:

```
F TSS,AUTOERASE(NO)
```

BACKUP—Backup the Security File

Valid on z/OS and z/VM.

The BACKUP control option:

- Immediately backs up the Security File
- Selects a time for an automatic daily backup
- Deactivates the automatic backup

All entry methods are accepted.

Note: The MODIFY command can be used to override the entry in the Parameter File if BACKUP is set to OFF. This option only works if the Backup DD card is included in the start JCL.

This control option has the following format:

```
BACKUP blank|(hhmm)|(OFF)
```

blank

If the backup DD statement is in the CA Top Secret STC procedure, CA Top Secret immediately backs up the Security File.

hhmm

If the backup DD statement is in the CA Top Secret STC procedure, CA Top Secret backs up the Security File at the time specified.

Default: 0100

OFF

CA Top Secret discontinues automatic backup of Security File. CA Top Secret must be restarted to reset BACKUP(OFF).

Use of BACKUP Option

Use of the BACKUP option is contingent on two factors:

- BACKUP is available only if the BACKUP DD statement is entered into the CA Top Secret started task procedure.
- The Backup File must be exactly the same size as the Security File.

When CA Top Secret Will Not Perform BACKUP

CA Top Secret will not back up the Security File on the same day that CA Top Secret is started, unless it is started BEFORE any scheduled backup time.

Multiple CPUs

It is only necessary to perform backup from one CPU in a multiple CPU environment. The site needs only activate backup through one CPU's CA Top Secret Parameter File or STC procedure. Multiple backups are redundant, and do not occur simultaneously due to device locking.

D37 Abends

D37 abends during backup indicate that the Backup File is too small. Recreate the Backup File according to instructions in the *Installation Guide*.

Recommended Use

Security administrators use the automatic backup feature to protect the Security File. To use the backup feature, the security administrator or programmer must first create a backup file on an alternate DASD volume. Place this Backup File on a different string with a different control unit than the primary file. This file placement ensures that the Backup File is available in the event of a hardware failure. This Backup File is a copy of the Security File, and as such it must be considered a sensitive, high-risk data set.

Examples: BACKUP control option

This example automatically backs up the Security File at 2 a.m:

```
BACKUP(0200)
```

This example immediately backs up the file:

```
F TSS,BACKUP
```

BYPASS—Bypass Resource Checking

Valid on z/OS and z/VM.

The BYPASS control option allows the MSCA to request emergency bypassing of resource checking for a specific ACID. Administrators must be given MISC9(BYPASS) authority to use this control option.

Note the following rules for use:

- BYPASS takes effect in all modes
- Up to ten BYPASS users can be specified in one or more options

This control option uses the MODIFY entry method.

This control option has the following format:

```
BYPASS(userid(1)[,userid(2),...userid(10)][ALL][RESET]
```

userid(n)

Represents the virtual machine userid for bypassed security.

ALL

Allows **all** virtual machines to bypass security.

Important! Use with extreme caution.

RESET

Terminates security bypass for all users that were specified to bypass security.

Examples: BYPASS Control Option

This example causes the virtual machine USER01 to bypass all resource security checking:

```
TSS MODIFY('BYPASS(USER01)')
```

This example terminates security bypass for USER01, and any other ACID that was specified to bypass security:

```
TSS MODIFY('BYPASS(RESET)')
```

CACHE—Reserve Memory

Valid on z/OS.

The CACHE control option provides an area of memory for CA Top Secret to place frequently used items from the security file. Provision for sufficient CACHE reduces I/O against the security file and increases system performance.

CA Top Secret uses virtual storage above the line within its address space as a method to keep commonly used records from the Security File.

CA Top Secret comes with the CACHE option off. To activate CACHE or specify the CACHE option in the PARMFILE, use the TSS MODIFY control option.

The CACHE provides benefits in two areas. The first is that users commonly log in multiple times in a short duration of time. Because the logon mechanism as in TSO, or logon to multiple regions such as CICS. Second, the CACHE benefits profile sharing by allowing I/O performed for one user to benefit another user logging on to a different address space.

All entry methods are accepted.

This control option has the following format:

```
CACHE (nnnn|CLEAR|STATUS|OFF)
```

nnnn

Sets the number of kilobytes of storage that is allocated for caching. If previously set to OFF, providing this value activates the CACHE feature. CA Top Secret never allows the actual CACHE allocated to exceed the storage to operate. To accommodate your cache request, assure adequate region size is allocated for the TSS task. The recommended value for the CACHE control option can be determined using the TSSFAR utility SFSTATS function. For information, see the *Troubleshooting Guide*.

When using large file sizes, the requested cache size cannot be met due to operating system constraints. If your recommended cache size is not being met, an increase in the region size for CA Top Secret is recommended. Consult your system programmer regarding the maximum address space size set within your system.

CLEAR

Empties the CACHE. The CACHE starts to fill again as applications request security records. Clear is also automatically performed when a CACHE request is issued causing the CURRENT SIZE to exceed the MAXSIZE.

STATUS

Provides statistics on how much CACHE is used and how efficient CACHE is in avoiding extra I/O. If CACHE is not active, message TSS1303I is displayed. If CACHE is active, the following statistics are displayed:

MAXSIZE

The maximum number of kilobytes used by CACHE as the storage threshold.

SIZE

The current number of kilobytes in use because the last CLEAR.

CALLS

The number of calls that are made to CACHE.

SATISFIED

The number of calls that are satisfied in CACHE.

CLEARED

How many times CACHE was clear for the life of this CA Top Secret address space.

OFF

(Default) Deactivates CACHE. The CACHE is emptied and used when requested by a CACHE(*nnnn*) command.

CANCEL—Allow Operating System CANCEL

Valid on z/OS.

The CANCEL control option allows security administrators to use the O/S CANCEL command to bring the CA Top Secret address space down. The CA Top Secret address space is eligible for cancellation after CANCEL is specified.

For information about the CA Top Secret address space deactivation options, see the DOWN control option.

Important! Use O/S CANCEL in emergency situations only. This option is not recommended as the normal shutdown method for CA Top Secret.

If the z/OS FORCE command is used:

- CA Top Secret cannot process the DOWN options.
- CA Top Secret must be restarted or an IPL performed to proceed.
- CA Top Secret processes in an unpredictable manner.

All entry methods are accepted.

This control option has the following format:

```
CANCEL
```

CATADELPROT—Prevent Dataset Deletion

The CATADELPROT control option prevents an SMS or VSAM data set deletion by a specific user type. The user does not have delete privileges to the dataset, but does have alter (ALL) access to the catalog where the SMS or VSAM dataset is catalogued.

This control option has the following format:

```
CATADELPROT(YES|NO)
```

YES

Users must have delete privileges to delete a dataset. Alter access to the catalog does not override.

NO

(Default) Allows users with alter access to the catalog to delete a dataset.

CHORUSSTATG—Enable CA Chorus Statistics Gathering

Valid on z/OS.

The CHORUSSTATG control option specifies to start or stop statistics gathering for CA Top Secret. Statistics gathering is the process of collecting system statistics and creating records to be sent to CA Chorus Time Series Facility (TSF) for a given time frame and is measured in seconds using the CHORUSSTATI control option.

All entry methods are accepted.

This control option has the following format:

```
CHORUSSTATG(ON|OFF)
```

ON

Specifies that statistics gathering is activated.

OFF

(Default) Specifies that statistics gathering is not active. No statistical information is gathered and recorded to the CA Chorus Time Series Facility.

CHORUSSTATI—Specify CA Chorus Statistics Gathering Time Interval

Valid on z/OS.

The CHORUSSTATI control option specifies the time interval for statistics gathering and CA Chorus Time Series Facility record creation. This control option is used with the CHORUSSTATG(ON) control option.

Note: CHROUSSTATI(0000) indicates that the CHORUSSTATG option is not activated.

All entry methods are accepted.

This control option has the following format:

```
CHORUSSTATI(nnnn)
```

nnnn

Time interval in seconds.

Range

15 to 3600. The valid values are 15, 30, 60, 300, 900, 1800, 3600.

Default

15

CHORUSTSFDB—Specify CA Chorus Time Series Facility (TSF) Debug Option

Valid on z/OS.

The CHORUSTSFDB control option starts or stops Time Series Facility (TSF) API debug tracing.

The DEBUG option is used to troubleshoot the flow between the CA Chorus STATG feature and its interface to Time Series Facility (TSF). Once you turn on the DEBUG option, CA Top Secret sends trace records to the DD of SYSPRINT under the CA Top Secret address space. Three levels of trace detail exist.

This control option has the following format:

```
CHORUSTSFDB(n)
```

n

Debug level number

0 = The debug tracing if off.

1 = First level trace records written.

2 = Second level trace records written.

3 = Third level trace records written.

Range

0-3

Default

0

CHORUSTSFSX—Specify CA Chorus Time Series Facility (TSF) Suffix Indicator

Valid on z/OS.

The CHORUSTSFSX control option identifies the CA Chorus instance where statistical data is provided for use by the Time Series Facility (TSF). You can specify multiple suffix values to define up to five instances.

Note: If you do *not* have multiple instances, use the default value P. When you use P, the TSFSUFFIX in the TSFPARMS member of *high level*.CETJOPTN is left blank. If you use multiple suffix values to identify multiple instances, specify matching suffix values in the TSFRPRMS member of *high level*.CETJOPTN.

TSF acquires the TCPIP token name for the server port number. If you want the TSF API server port number for a test TSF, set this character to the corresponding test instance character for that test TSF region.

Note: TSF startup parameters let you run test TSF regions in parallel with a production TSF.

This control option has the following format:

```
CHORUSTSFSX(x,x,x,x,x)
```

x,x,x,x,x

Specifies a suffix value. You can specify a maximum of five suffix values.

Range: A-Z, 0-9, and P (PROD)

Default: P

CIAAUTO—Automatically Start the CIA Real-Time Processing Component Started Task

Valid on z/OS.

The CIAAUTO control option specifies whether CA Top Secret, at initial start after IPL, will automatically start the CIA real-time processing component started task.

This control option has the following format:

```
CIAAUTO(START|NOSTART)
```

START

Starts the CIA real-time processing component address space at the first TSS startup after an IPL.

NOSTART

(Default) Do not automatically start the CIA real-time processing component address space.

Example: CIAAUTO Control Option

CIAAUTO automatically starts the CIA processing component address space.

```
F TSS,CIAAUTO(START)
```

CIAHOST-Host Name

Valid on z/OS.

The host name for the DSI server. This field is required when CIART is specified.

This control option has the following format:

```
CIAHOST(hostname)
```

hostname

Specifies the host name of the DSI server. The valid values are 1-255 characters. To specify more than 71 characters, use multiple options. On the second and subsequent lines, specify the continuation character “-“ as the first character.

Example: CIAHOST Control Option

CIAHOST specifies the DSI host name.

```
F TSS,CIAHOST(SYSAHOST)
```

This example specifies a DSI host name of more than 71 characters.

```
F TSS,CIAHOST(THISSYSAHOSTNAMEISMORETHAN71CHARACTERSSOITWILLBE) F
TSS,CIAHOST(-ENTEREDONMULTIPLELINESWITHACONTINUATIONCHARACTER)
```

CIALOGNAME-Log Name

Valid on z/OS.

The name of the log stream that CIA uses to provide real-time updates. This field is required when CIART is specified.

To change the log stream that CIA uses, change the name using the TSS MODIFY command. Then issue the following commands:

```
F TSS,CIART(DISCONNECT)
F TSS,CIART(CONNECT)
```

Stop and start the Processing Component started task procedure after a few minutes.

This control option has the following format:

CIALOGNAME(logname)

logname

The name of the CIA log stream.

Example: CIALOGNAME Control Option

CIALOGNAME specifies the log name.

```
F TSS,CIALOGNAME(SYSA.CIALOG)
```

CIAMAXSTOR—Maximum Storage Size

Valid on z/OS.

The maximum size of storage that CIA real-time subtask use, which is specified in megabytes. The storage is used for storing records temporarily in 64-bit storage before they are placed into the Log Stream.

CIAMAXSTORE has the following format:

`CIAMAXSTOR(`*`nnn`*`)`

nnn

1-3 digits. The valid values are from 5 to 100 MB. The default is 25 MB.

Example: CIAMAXSTOR Control Option

CIAMAXSTOR specifies a maximum storage value of 50.

```
F TSS,CIAMAXSTOR(50)
```

CIAPORT—Port Number

Valid on z/OS.

The port number for the DSI server. This field is required when CIART is specified.

This control option has the following format:

`CIAPORT(`*`nnnnn`*`)`

nnnnn

1-5 digit port number value. The valid values are from 1 to 65535.

Example: CIAPORT Control Option

CIAPORT specifies the port number as 73.

```
F TSS,CIAPORT(73)
```

CIAPROCNAME—Started Procedure Name

Valid on z/OS.

The library member name for the CIA real-time Processing Component started task procedure.

This control option has the following format:

```
CIAPROCNAME(procname)
```

sysid

1-8 character started task procedure name. The default is CIARTUPD.

Example: CIAPROCNAME Control Option

CIAPROCNAME specifies the procedure name.

```
F TSS,CIAPROCNAME(CIARTPRC)
```

CIART—CIA Real-Time Updates

Valid on z/OS.

CIART specifies CIA real-time updates are active. All entry methods are accepted.

Note: This control option functions only if you have a CA Chorus license.

This control option has the following format:

```
CIART(ACTIVE|INACTIVE|CONNECT|DISCONNECT)
```

ACTIVE

Starts the CIA real-time processing component task. The task only terminates when TSS is shut down.

INACTIVE

(Default) Specified after CIART was activated, then TSS will not pass events to the CIA real-time subtask.

CONNECT

Indicates that the CIA real-time subtask connects to the CIA log stream. Specified after a disconnect.

DISCONNECT

Tells the CIA real-time subtask to disconnect from the CIA log stream. TSS continues to pass events to the subtask and records are stored in the 64-bit storage area (defined by CIAMAXSTOR). If the 64-bit storage area becomes full and no new records can be added, the new records are discarded. This parameter is used to switch to a new CIA log stream.

Example: CIART Control Option

CIART activates the CIA Real-Time updates.

```
F TSS,CIART(ACTIVE)
```

This example implements a new CIA log stream.

```
F TSS,CIART(DISCONNECT)
```

```
F TSS(CIALOGSTREAM(NEWLOGSTR))
```

```
F TSS,CIART(CONNECT)
```

CIASYSID—Customize the System ID Assigned to LPAR Security Information

Valid on z/OS.

When the security information for an LPAR is unloaded to CIA, the information is tagged with the SYSID of the LPAR. By default, this ID is the SMFID, but you can customize it to any value with an unload parameter. The database portion of the real-time component must have access to the SYSID value so that the database can update the correct information.

This control option has the following format:

```
CIASYSID(sysid)
```

sysid

Specifies a one- to eight-character system ID. The default is the system SMFID.

Example: Specify System ID PRD1

This example specifies the SYSID PRD1:

```
F TSS,CIASYSID(PRD1)
```

CMDNUM—Number of Command Processors

Valid on z/OS.

The CMDNUM control option determines the number of command processors at startup of the CA Top Secret address space initiates.

This control option uses the parameter file entry method.

This control option has the following format:

```
CMDNUM(nn)
```

N

Specifies the number of command processors that CA Top Secret initiates at startup.

Range: 2 to 10

Default: 5

If TSS MODIFY STATUS is issued, no messages display. If TSS MODIFY is issued, messages showing the workload balance appear in the output. After changing TSS MODIFY STATUS to TSS MODIFY, the messages that show when CMDNUM(10) is set are:

```
TSS9610I ----- COMMAND PROCESSOR WORKLOAD BALANCE -----
TSS9611I total Commands Issued = 0000000004
TSS9612I Cmd 01  =  000.00%            Cmd 02  =  098.94%
TSS9612I Cmd 03  =  001.05%            Cmd 04  =  000.00%
TSS9612I Cmd 05  =  000.00%            Cmd 06  =  000.00%
TSS9612I Cmd 07  =  000.00%            Cmd 08  =  000.00%
TSS9612I Cmd  09 =  000.00%            Cmd  10 =  000.00%
```

Two is the minimum number of command processors. However, with the NT workstation and the higher number of commands being issued, you can start more processors.

When CMDNUM is set to three or higher, the first three processors are set up the following way:

- Processor number 1 is used for all outbound CPF commands when WAIT=YES and the TARGET keyword is used.
- Processor number 2 is used for all incoming CPF commands.
- Processor number 3 is used for all other regular commands.

Example: CMDNUM control option

This example indicates that five command processors are initiated at startup.

```
CMDNUM(5)
```

CPF—Activate Command Propagation Facility at Startup

Valid on z/OS and z/VM.

The CPF control option specifies whether the Command Propagation Facility (CPF) of CA Top Secret is activated at startup.

At least one of the CPF-related control options must be entered at CA Top Secret startup to use the CPF. If not, the CPF activation is delayed until the next CA Top Secret startup. CA Top Secret does not honor CPF control options until that time.

All entry methods are accepted.

This control option has the following format:

```
CPF(ON|OFF|KILL|REFRESH|INACTIVE)
```

ON

Specifies that the CPF modules are loaded into memory, and that the CPF subtask is initiated. The NDT CPFNODE definitions override the CPFNODES control option definitions. Before encountering CPF(ON), STATUS(CPF) displays CPF(INACTIVE), indicating that the CPF modules have not been loaded.

If CPF(ON) is specified, but CCI is not available or not fully initialized; CPF status is displayed as CPF(INIT). While CPF is in this status, commands are not propagated through CPF and are not logged to the CPF recovery file. Once CCI completes its initialization, CPF status displays as CPF(ON) and command propagation logging takes place.

OFF

Specifies that no TSS commands transmitted by this node or received from other nodes until the operator sets CPF(ON) with the TSS MODIFY command (if any CPF-related control option was entered), or at the next startup of CA Top Secret.

KILL

Terminates the CPF subtask and produces a dump. Once the subtask has been killed, it can later be reactivated using TSS MODIFY(CPF(ON)). CPF(KILL) produces an SVC dump with abend S33E. If a dump is desired, be certain to disable any active SLIP commands set to suppress S33E abend dumps.

REFRESH

Issues CPF(OFF) followed by CPF(ON). During the internal shutdown, the STATUS(CPF) shows CPF(OFF). When CPF is restarted, any changes to the NDT CPFNODE definitions override previous control option settings. Any commands queued in storage are released during shutdown and are rebuilt from the recovery file at startup. Commands and password changes, already on the recovery file before shutdown, are executed verbatim; regardless of NDT changes implemented at startup.

INACTIVE

(Default) Although this value cannot be used in a command, it is displayed in STATUS(CPF) to indicate that CPF has not been activated.

Example: CPF control option

This example indicates that a user does not want to use the CPF:

```
CPF(OFF)
```

CPFAUTOGID—Insert a Specific USS GID During CPF Command Processing

Valid on z/OS.

The CPFAUTOGID control option transmits a TSS command with an assigned GID value, instead of the '?' value, when you are using the Command Propagation Facility (CPF) feature.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY(CPFAUTOGID(NO|YES))
```

NO

(Default) Retains any existing '?' value during the CPF command transmission. For example, the command TSS ADD(JONATHAN) GID(?) retains the '?' value during transmission.

YES

Transmits a TSS command with an assigned GID value, instead of the '?' value. For example, TSS ADD(JONATHAN) GID(256) is transmitted instead of the TSS ADD(JONATHAN) GID(?).

CPFAUTOUID—Insert a Specific USS UID During CPF Command Processing

Valid on z/OS.

The CPFAUTOUID control option transmits a TSS command with an assigned UID value, instead of the '?' value, when you are using the Command Propagation Facility (CPF) feature.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY(CPFAUTOUID(NO|YES))
```

NO

(Default) Retains any existing '?' value during the CPF command transmission. For example, the command TSS ADD(JONATHAN) UID(?) retains the '?' value during transmission.

YES

Transmits a TSS command with an assigned UID value, instead of the '?' value. For example, TSS ADD(JONATHAN) UID(100) is transmitted instead of the TSS ADD(JONATHAN) UID(?).

CPFLISTMULT—Propagate LIST/WHOHAS commands

Valid on z/OS.

Some LIST and WHOHAS commands generate large amount of output. Therefore, by default CPF does not propagate these commands to remote nodes.

The CPFLISTMULT control option specifies whether CPF allows routing of LIST(ACIDS) and WHOHAS FACILITY commands to more than one node.

All entry methods are accepted.

This control option has the following format:

```
CPFLISTMULT(YES|NO)
```

YES

Specifies to routes any LIST or WHOHAS command for target nodes.

NO

Specifies that a LIST(ACIDS) or WHOHAS FACILITY command that is targeted to multiple nodes is executed only on the local node.

Note: This option replaces OPTIONS(71).

CPFNODE—CPF Node Changes

Valid on z/OS and z/VM.

This control option changes the status and attributes of a CPF node after CA Top Secret has initialized and CPF is activated.

When a node is defined using the parmlib CPFNODE method rather than the NDT, the word STATIC appears in the display when a TSS MODI STATUS(CPF) command is issued. For example:

```
TSS966II CA Top Secret CPF Status
?
CPFNODE(XE58) Static Status(ACTIVE,NOSPOOL,...)
```

This control option uses the O/S and TSS MODIFY command entry methods.

This control option has the following format:

```
CPFNODE(nodename=STOP|START|REFRESH)
```

STOP

Stop sending and receiving commands and passwords for the specified node. Currently queued messages are processed but no new messages are queued to this node.

While the specified node is stopped, entries for the node are not written to the CPF Recovery File. Entries for the other CPF nodes continue to be written to the CPF Recovery File.

START

Activate a previously stopped node, or install and activate a new NDT defined node.

REFRESH

Modify the node attributes based on current the NDT definitions. The new attributes only affect commands and password changes not yet queued to the node. Recovery file records and in-core queue entries are processed based on the attributes in effect before the refresh.

Examples: CPFNODE control option

This example modifies the attributes of CPF node SYS2 using the O/S Modify command:

```
F TSS,CPFNODE(SYS2=REFRESH)
```

This example uses the CPFNODE REFRESH option with the TSS MODIFY command:

```
TSS MODIFY(CPFNODE(SYS2=REFRESH))
```

CPFNODES—Identify Remote Nodes for CPF

Valid on z/OS and z/VM.

The CPFNODES control option identifies remote CA Top Secret nodes with which CPF can propagate commands. These nodes are one- to eight-characters.

If the NDT record already has a CPFNODE definition for the same node ID, the control option definition is ignored.

This option, with the GW (gateway) operand, is used to connect CA Common Services for the z/OS node to a CPF network. A CA Common Services node must be connected to only one CA Top Secret mainframe within a CPF network. That mainframe must have the GW operand that is specified on the CPFNODES( ) statement. For information, see the *User Guide*.

The word *node* when used regarding the CPF, refers to the unique identifier assigned to a node when it is defined using CAICCI.

To display the contents of a CPFNODE, enter:

```
TSS MODIFY STATUS(CPF)
```

For information about defining a node, see the *CA Common Services for z/OS Administration Guide*.

This control option uses the Parameter file or PARM field of started-task procedure entry methods and has the following format:

```
CPFNODES(nodename(S,C))
CPFNODES(nodename(S,P))
CPFNODES(nodename(S,GW))
CPFNODES(nodename(S,P,GW))
CPFNODES(nodename(S,C,GW))
CPFNODES(nodename(R))
CPFNODES(nodename(R,GW))
CPFNODES(nodename(NB))
```

nodename

Specifies remote CA Top Secret nodes from and to which the TSS commands are transmitted.

(S)

Specifies that the local node can only send commands to that particular remote node.

(R)

Specifies that the local node can only receive commands from that particular remote node.

(C)

Specifies that only administrative command changes and DUF updates are sent to a node.

(P)

Specifies that only password changes and suspensions are sent to a node.

Note: Password changes made through the CA Top Secret command are not sent.

(GW)

Specifies a node which acts as a CPF gateway or CPF server for another node.

(NB)

Specifies a CPF node as a no-broadcast node. Password changes and commands are sent to the node when the ACID has DEFNODES. The password changes are also sent for commands, when the TARGET with this node is specified on the command line. NB takes effect when CPFTARGET(*) is the default only. For information, see the *User Guide* and the *Command Functions Guide*.

Examples: CPFNODES control option

This example identifies nodes A1B2C3 and D4E5F6 as potential targets of TSS commands:

```
CPFNODES(A1B2C3,D4E5F6)
```

This example indicates that the local node can send and receive commands from the CHI and NYC nodes. It only sends commands to the PHIL node:

```
CPFNODES(CHI,NYC,PHIL(S))
```

This example indicates that the local node can send and receive commands from the LA and NJ nodes. It only receives commands from the NY node:

```
CPFNODES(LA,NJ,NY(R))
```

This example indicates that the local node can send and receive command and password changes from the SYS1 node. The local node can send only the password changes to node SYS2, but can receive. Both command and password changes from node SYS2. Since both S and P are specified, the local node can only send password changes to SYS3:

```
CPFNODES(SYS1,SYS2(P),SYS3(S,P))
```

This entry indicates that node HPUX2 serves as a gateway for another CPF node.

```
CPFNODES(HPUX2(GW))
```

This entry indicates that node UNI1 serves as the gateway for CA Common Services for z/OS.

```
CPFNODES(UNI1(GW))
```

This example indicates that node SYS2 is a no-broadcast node:

```
CPFNODES(SYS2(NB))
```

User password changes propagate to all nodes except those nodes that are designated by the CPFNODES option as RECEIVE (R) or COMMAND (C) only nodes.

CPFRCVUND—Receive Commands from Undefined Nodes

Valid on z/OS and z/VM.

The CPFRCVUND control option indicates whether the local node can receive propagated commands from nodes that have not been defined to the CPFNODES list.

All entry methods are accepted.

This control option has the following format:

```
CPFRCVUND(YES|NO)
```

YES

The local node receives commands from defined and undefined remote nodes.

NO

(Default) The local node rejects transmitted commands from remote nodes that are not listed in the CPFNODES list.

CPFTARGET—TARGET Keyword Default

Valid on z/OS and z/VM.

The CPFTARGET control option sets a default value for the TSS command TARGET keyword.

At least one of the CPF-related control options *must* be entered at CA Top Secret startup to use the CPF. Otherwise, CPF deactivates until the next CA Top Secret startup and CA Top Secret rejects CPF control options until that time.

This control option uses the parameter file or PARM field of started-task procedure entry methods.

This control option has the following format:

```
CPFTARGET(LOCAL|AUTO|*)
```

LOCAL

(Default) Specifies that the default for the TARGET keyword is to restrict command execution to the local node only.

AUTO

Indicates default routing that is based on the DEFNODES associated with the ACID. The user's default nodes are assigned implicitly on a TSS CREATE function or manually using the TSS ADDTO function. For information about DEFNODES, see the *Command Functions Guide*.

*****

Specifies the TARGET keyword default is to transmit the command to all nodes defined in the CPFNODES control option; excluding the receive-only nodes.

The TARGET value on the individual TSS command can override the default.

Example: CPFTARGET control option

This example indicates that, by default, all TSS commands are routed to all nodes defined in the CPFNODES control option:

```
CPFTARGET(*)
```

CPFWAIT—WAIT Keyword Default

Valid on z/OS and z/VM.

The CPFWAIT control option sets a default value for the TSS command WAIT keyword.

At least one of the CPF-related control options *must* be entered at CA Top Secret startup to use the CPF. Otherwise, CPF deactivates until the next CA Top Secret startup and CA Top Secret rejects CPF control options until that time.

If any of the following conditions exist, you cannot view the output generated as the result of the CPFWAIT command:

- The CPF journal file has not been specified.
- WAIT(NO) is specified on the TSS command.
- The CPFWAIT control option is set to NO.

The CPF recovery file is used when defined and when CPFWAIT(NO) or WAIT(NO) is specified.

All entry methods are accepted.

This control option has the following format:

```
CPFWAIT(YES|NO)
```

YES

(Default) Specifies a default value for the TSS command WAIT keyword.

NO

Specifies that no waiting occurs for messages.

The WAIT value on an individual TSS command can override the values that are entered.

Example: CPFWAIT control option

This example indicates that when a TSS command is routed to a remote node. Additionally, the issuer of the command does not wait for a response from that remote node before continuing:

```
CPFWAIT(NO)
```

DATE—Date Format

Valid on z/OS and z/VM.

To specify the format for dates displaying in listings, use the DATE control option. The DATE option accommodates various multinational date standards.

All entry methods are accepted.

This control option has the following format:

```
DATE(yy/dd/mm)
```

YY

Year. For YY > 80, the year is assumed to be in the 20th century. For YY < 80, the year is considered to be in the twenty-first century.

DD

Day (01 - 31)

MM

Month (01 - 12)

Any character such as hyphen (-), period (.), comma(,) can be used as a delimiter between the date fields. Some characters, such as comma(,) and blanks require that the entire DATE control option be enclosed within quotes:

```
TSS MODIFY('DATE(MM DD YY)')
```

The choice of delimiters here affects the syntax of the UNTIL keyword during command administration. For example, if DATE('MM DD YY') were chosen then a command with the UNTIL keyword would be specified as follows:

```
TSS PERMIT(USER01) DSN(****.FILE)
                   UNTIL('05 01 94')
```

Examples: DATE control option

These examples produce listings for December 29, 2006:

```
TSS MODIFY DATE(mm/dd/yy)
```

```
TSS LIST(mult03) DATA(ALL,PASS,EXPIRE)
```

```
    ACCESSORID = MULT03 NAME = MULT03
    TYPE = USER SIZE = 256 BYTES
    FACILITY = CICSPROD
    ADMIN BY= BY(USERSCA) SMFID(XE14) ON(12/29/2006) AT(12:44:48)
    DEPT ACID = CICSDEPT DEPARTMENT = CICS DEPARTMENT
    CREATED = 12/29/06 12:38 LAST MOD = 12/29/06 12:44
    ATTRIBUTES = MULTIPW
    ALL =
    CICSPROD = EXPIRES = 01/28/07 INTERVAL = 030
```

```
TSS MODIFY DATE(yy-mm-dd)

TSS LIST(mult03) DATA(ALL,PASS,EXPIRE)

    ACCESSORID = MULT03 NAME = MULT03
    TYPE = USER SIZE = 256 BYTES
    FACILITY = CICSPROD
    ADMIN BY= BY(USERSCA ) SMFID(XE14) ON(2006-12-29) AT(12:44:48
    DEPT ACID = CICSDEPT DEPARTMENT = CICS DEPARTMENT
    CREATED = 06-12-29 12:38 LAST MOD = 06-12-29 12:44
    ATTRIBUTES = MULTIPW
    ALL =
    CICSPROD = EXPIRES = 07-01-28 INTERVAL = 030
```

DB2FAC—Group and Protect DB2 Subsystems

Valid on z/OS.

Use the DB2FAC control option to:

- Logically group DB2 subsystems under different facility names for protection under the CA Top Secret Option for DB2
- Control whether the resources in a DB2 subsystem is protected using the CA Top Secret Option for DB2

All entry methods are supported.

This control option has the following format:

`DB2FAC(`*`ssid=facility|NONE`*`)`

ssid

Identifies the name of the DB2 subsystem

facility

Indicates the facility name to which the DB2 subsystem is associated.

NONE

Removes the assignment of a facility from the specified DB2 subsystem. Required when using the TSS MODIFY command to remove the facility assignment for a subsystem temporarily. To remove the assignment of a facility, remove the ssid=facility definition from the CA Top Secret startup parameter file permanently.

Examples: DB2FAC control option

This example indicates that DB2 subsystems DB2A and DB2B are grouped under DB2PROD, while DB2 subsystems DB2C and DB2D are under DB2TEST:

```
DB2FAC(DB2A=DB2PROD)
DB2FAC(DB2B=DB2PROD)
DB2FAC(DB2C=DB2TEST)
DB2FAC(DB2D=DB2TEST)
```

This example indicates that DB2 subsystems DB2A is no longer assigned to the DB2PROD facility:

```
DB2FAC(DB2A=NONE)
```

Protect DB2 Subsystem Resources

The mode on the facility that is defined for the DB2 subsystem controls the protection of the DB2 subsystem resources. Specifying a non-DORMANT mode for the facility that is associated with the DB2 subsystem protects its resources. A mode of DORMANT indicates that *neither* CA Top Secret for DB2 *or* native DB2 protects the resources in the DB2 subsystem. DORMANT indicates no DB2FAC control option specification for a DB2 subsystem. For information, see the *Implementation:DB2 Guide.*

This example allows the protection of DB2 resources:

```
DB2FAC(DB2A=DB2PROD)
DB2FAC(DB2B=DB2PROD)
```

This example of a specified mode allowing protection of DB2 resources:

```
FACILITY(DB2PROD=MODE=FAIL)
```

The settings of the DB2PROD facility (LOG, ABEND/NOABEND) determine the mode for the checks and other facility options. For example, if the user is logged on to TSO the MODE and all other facility control options are determined by the DB2PROD facility but only for DB2 resource checks. All other normal functions of TSO continue to occur under the TSO facility.

DEBUG—Produce Dumps

Valid on z/OS and z/VM.

Use the DEBUG control option to control the production of debugging dumps used to determine the cause of abnormal error conditions. DEBUG is issued at the request of Technical Support to help determine the cause of specific abnormal events. Event output from this command is written to the system console.

All entry methods are accepted.

This control option has the following format:

```
DEBUG(ON|OFF)
```

ON

Produces a diagnostic dump. Use *only* upon request of Technical Support.

OFF

(Default) Deactivates the DEBUG feature.

DFLTRNGG—GID Default Range

Valid on z/OS and z/VM.

Use the DFLTRNGG control option to specify a default range for the GID auto assignment. Enter a range of (0,0) to clear the DFLTRNGG.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY(DFLTRNGG(xxx,xxx))
```

Default: 1 to 2,147,483,647

DFLTRNGU—UID Default Range

Valid on z/OS and z/VM.

Use the DFLTRNGU control option to specify a default range for the UID auto assignment.

Enter a range of (0,0) to clear the DFLTRNGU.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY(DFLTRNGU(xxx,xxx))
```

Default: 1 to 2,147,483,647

DIAGTRAP—Produce Diagnostic Dump

Valid on z/OS.

Use the DIAGTRAP control option to produce a diagnostic dump, based on limitations of ACID, JOBNAME, RESCLASS, and Detailed Reason Code. This is the CA Top Secret equivalent to O/S SLIP.

Apart from '*' by itself, the DIAGTRAP control option does not support masking. Specify the exact ACID, resource class, or jobname.

Use this control option only under the direction of CA Top Secret Support.

All entry methods are accepted.

This control option has the following format:

```
DIAGTRAP(id,enable_swtich[,trap_type,acid,drc,resclass,job,matchlim])
DIATRAP(id,OFF)
DIAGTRAP(id,DEL)
DIAGTRAP(ALL,DEL)
```

id

Specify an ID. “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.

Range: 1 to 10

enable_switch

Enable or disable the given id. Valid values are:

- On—Enable the diagtrapid entry.
- Off—Disable the diagtrapid entry while keeping its information.
- Del—Delete the entry.

Note: The enable and the id are the only entries required for turning an ID off.

trap_type

Activates the trap in a particular location. This field must be entered and there is no default. A “)” can be entered any time after the trap to indicate defaults are to be taken for remaining fields. Valid traps are:

- KER—Trap within security kernel (TSSKERNL)
- SFS—CA Top Secret Security File services debugging
- SF1—CA Top Secret Security File services debugging for GETAR.
- SF2—CA Top Secret Security File services debugging for UPDATE

IF SF1 or SF2 is set, SFS is also set.

- DBG—Interactive TSO or console debugging (online)
- DB1—Diagnostic location-1
- DB2—Diagnostic location-2

Important! Initially, when an entry is created, the trap_type is a required parameter in the DIAGTRAP syntax.

acid

The ACID entered as a parameter to be matched for producing a dump.

Default: Any User id (*).

drc

The Detailed Reason Code that must be produced to trigger the dump.

Default: Any violation (255).

resclass

Tests the resource class name.

Default: Any (*).

job

Specifies the job name of the job or started task to be monitored. The restrictions on acid, drc, resclass, and job are combined to trigger the DIAGTRAP: all conditions listed must be simultaneously present for the dump to be triggered.

Default: Any (*).

matchlim

Sets the maximum number of dumps to be taken.

Range: 1 to 255

Default: 1

Examples: DIAGTRAP control option

This example triggers a diagnostic dump when ACID DUMPE01 is executing JOB DUMPE01A, and a security error with detailed reason code 075 occurs during a check for an OTRAN resource, while CA Top Secret is executing modules in the TSS Kernel. The command assigns this diagtrap an id of 1, and remains active through a maximum of 2 occurrences where these conditions are detected:

```
TSS MODIFY(DIAGTRAP(1,ON,KER,DUMPE01,075,OTRAN,DUMPE01A,2))
```

This example checks for a Security File Services (SFS) error of any kind while processing user EXAMP01. The diagtrap is assigned an id of 7, and will remain active until such an error is detected once.

```
TSS MODIFY(DIAGTRAP(7,ON,SFS,EXAMP01,255,*,*,1)
```

This example sets Kernel diagtrap #6 to check any job for any acid against any non-zero DRC in any resource and also sets the match limit to 1:

```
TSS MODIFY(DIAGTRAP(6,ON,KER))
```

This example turns DIAGTRAP number 3 off (as long as number 3 is active):

```
TSS MODIFY(DIAGTRAP(3,OFF))
```

This example deletes diagtrap number one:

```
TSS MODIFY(DIAGTRAP(1,DEL))
```

This example sets Diagtrap #5 to check against a successful validation (DRC=0) for any ACID executing job DUMPE01A with resource OTRAN. The matchlim defaults to 1:

```
TSS MODIFY(DIAGTRAP(5,ON,KER,*,0,OTRAN,DUMPE01A)
```

This example deletes all of the existing diagtraps (whether set “on” or “off”):

```
TSS MODIFY(DIAGTRAP(ALL,DEL))
```

DISPMASK—Display Attribute of MASK

Valid on z/OS and z/VM.

Use the DISPMASK control option to distinguish permissions which contain mask characters in a MASKABLE resource class.

When the DISPMASK(ON) control option is set, the LIST and WHOHAS commands:

- Look for the presence of a mask in the PERMIT for a MASKABLE resource class
- Display the presence of the mask character with the extra line:

  ```
  ATTRIB=MASK
  ```

Generation of this line is not affected by DATA(TERSE) or by TSSCMDOPTION(TERSE) options. DISPMASK(OFF) is over ridden by DATA(ENHANCED) or TSSCMDOPTION(ENHANCED).

All entry methods are accepted.

This control option has the following format:

```
DISPMASK(ON|OFF)
```

ON

Permits the LIST and WHOHAS commands to display of the ATTRIB=MASK line for permissions with masked resource names.

OFF

(Default) Suppresses the display of the ATTRIB=MASK line.

Examples: DISPMASK control option

This example shows the output of a WHOHAS command when DISPMASK(ON) is set:

```
TSS WHOHAS DATASET(%.)
```

```
 DATASET    = %.             OWNER(MASTER1 )
  XAUTH     = %.             ACID(ACLADM  )
    ACCESS  = ALL
    ATTRIB  = MASK
```

This example shows the output of a LIST command when DISPMASK(ON) is set under TSSCFILE:

```
<......HEADING...><....+....1....+....2....+....3....+....4...
<0001            ><TSS LIST(ACLADM) DATA(XA) RESCLASS(DATASET)
<0100  ACLADM    ><SETFACL ADMIN                     >
<2002  ACLADM    ><DATASET MASTER1         %.
<2021  ACLADM    ><ALL
                  <
<2030  ACLADM     ><MASK    >
```

DL1B—PSB and DBD Security

Valid on z/OS.

Use the DL1B control option to:

- Implement PSB and DBD security for IMS batch regions
- Provide access to the CA Top Secret Application Interface Program

This option does not apply to IMS, BMP, or MPP regions and to IMS/DC transactions for which PSB and DBD security is automatically applied through the IMS control region.

All entry methods are accepted.

This control option has the following format:

```
DL1B(YES|NO)
```

YES

Indicates that PSB and DBD security checking is implemented in IMS batch regions. The CA Top Secret Application Interface is available to user programs executing in the IMS batch region.

NO

(Default) Indicates that PSB and DBD security checking is suppressed when executing IMS batch regions. The CA Top Secret Application Interface is not available to user programs executing in a batch region. This control option defaults to NO because most installations do not want to implement their BATCH DL1 security concurrent with their IMS/DC security.

DOWN—Inactive Characteristics

Valid on z/OS and z/VM.

Use the DOWN control option to determine how jobs are initiated and passwords changed when the CA Top Secret address space is inactive. This control option must be set while CA Top Secret is active.

All entry methods are accepted.

This control option has the following format:

```
DOWN(facility,action,facility,action,…facility,action)
```

facility

Identifies the system facility being affected by the DOWN action. Valid values are:

- B—BATCH facility
- T—TSO
- S—STC initiation
- O—All other facilities

action

Identifies the action that CA Top Secret performs when its address space is DOWN. Valid values are:

- 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.

The default is DOWN(BW,SB,TW,OW).

The DOWN options are ignored if CA Top Secret is processing in global DORMANT mode.

The following table shows how DOWN actions affect various CA Top Secret processes:

PROCESS	WAIT	BYPASS	FAIL	NORMAL
Initiation or Logon	Initiations held and terminals locked	Security Ignored	Initiation Terminated	TSO UADS Password Required
Request for Password change	Initiations held and terminals locked	Wait	Wait	Wait
TSS command	Failed	Failed	Failed	Failed

PROCESS	WAIT	BYPASS	FAIL	NORMAL
Data set in FAIL mode	Failed	BYPASS	Failed	Failed
Submit a permitted ACID	Job submitted without password	Job submitted without password	Job submitted without password	Job submitted without password
TAPE(DEF) processing (volume level)	Volume access denied	BYPASS	Volume access denied	Volume access denied

Examples: DOWN control option

This example shows how the default DOWN(BW,SB,TW,OW) forces CA Top Secret to process security when its address space is down.

BW

Batch jobs and password changes (B) will wait for CA Top Secret to be reactivated (W).

SB

STC initiations (S) will bypass security checking (B).

TW

TSO logons and password changes (T) will wait for CA Top Secret to be reactivated (W).

OW

Online initiations and password changes (O) will wait for CA Top Secret to be reactivated (W).

Note: An action of B normally indicates to bypass all security. However, a TSO logon with a DOWN option of TB in effect will result in the UADS password for the user being checked.

DRC—Detailed Error Reason Code Characteristics

Valid on z/OS and z/VM.

Use the DRC control option to modify the characteristics of Detailed Error Reason Codes (DRCs).

This control option uses the Parameter file, O/S and TSS MODIFY commands entry methods.

This control option has the following format:

```
DRC(nnn,option,option...)
```

nnn

A three-digit decimal number which represents the DRC being modified or listed. Hexadecimal equivalents appear in many messages and on violation reports in TSSUTIL. Do not use these equivalents.

Range: 001 to 159

AUDIT

Violation event is tagged with an audit attribute to allow TSSUTIL to select it with EVENT(AUDIT) as well as normal EVENT(VIOL).

NOAUDIT

Resets the AUDIT suboption.

FAIL

Violation causes CA Top Secret to terminate the access attempt in ALL modes.

NOFAIL

Resets the FAIL suboption.

FAILWARN

Violation causes CA Top Secret to terminate access attempts in WARN as well as FAIL or IMPL modes.

NOFAILWARN

Resets the FAILWARN option.

PW

Indicates that the violation is a password type violation, such as an invalid password entry, as opposed to an access violation such as an unauthorized resource access attempt.

NOPW

Resets the PW suboption.

NOVIOL

Do not treat event as a violation. Instead, flag the event, but do not FAIL the user.

VIOL

Resets the NOVIOL suboption.

Additional violation control can be performed in the installation exit via the VIOLATION call.

Examples: DRC control option

This example indicates that DRC 002: “Initiation failed by site exit” will terminate access attempts in all modes, including both DORMANT and WARN modes. CA Top Secret will also write an Audit Record for this type of violation:

```
DRC(002,FAIL,AUDIT)
```

This example displays the characteristics of DRC 002 as an O/S Modify command:

```
F TSS,DRC(002)
```

DUFPGM—Program to Use INSTDATA

Valid on z/OS.

Use the DUFPGM control option to:

- Identify programs which allow for the extraction or update of the user installation data field (INSTDATA), bypassing the requirement that the ACID issuing the DUFXTR and/or DUFUPD call have the DUFXTR and/or DUFUPD ACID attribute.
- Authorize a user to perform the FLDXTR function of TSSAI.

If DUFPGM was changed using a TSS MODIFY command, the changes made remain in effect even if CA Top Secret is restarted. Most control options revert to their default settings, the exceptions are DUFPGM, JESNODE, and NJEUSR.

All entry methods are accepted.

This control option has the following format:

```
DUFPGM(pgm1,...|RESET)
```

pgm1

The programs that can be specified.

Range: Up to 5

RESET

Clears the entire program list.

Examples: DUFPGM control option

This example indicates the first program allowing for the extraction or update of the user installation data field:

```
DUFPGM(pgm1)
```

This entry indicates that the entire program list is cleared:

```
DUFPGM(RESET)
```

DUMP—Dump Control Blocks

Valid on z/OS and z/VM.

Use the DUMP control option to produce a diagnostic dump of control blocks within the CA Top Secret address space and common system storage. Only use this option when requested by Technical Support. This option is protected by the accountability feature.

The O/S and TSS MODIFY commands entry methods are accepted.

In z/OS, this control option has the following format:

```
DUMP
```

In z/VM this control option has the format:

```
DUMP(n)
```

n

Sets the maximum number of times per restart that the server machine can take system dumps.

Range: 1 to 9

Default: 3

Note: If you specify DUMP(0), there are no restrictions to the number of dumps taken.

Examples: DUMP control option

This example uses the DUMP option with the O/S Modify command:

```
F TSS, DUMP
```

This example uses the DUMP option with the TSS MODIFY command:

```
TSS MODIFY(DUMP)
```

ETRLOG—Send Security Events

Valid on z/OS.

Use the ETRLOG control option to send mainframe security events, such as loggings and violations, to the CA Audit product. The ETROPTS control option is used to control the events that can be logged.

All entry methods are accepted.

This control option has the following format:

```
ETRLOG(ON|OFF)
```

ON

Enables Monitor to transmit security events to CA Audit. If the monitor is on, violations, loggings, and start/stop of CA Top Secret message is sent to CA Audit.

OFF

Disables the Monitor from sending events to CA Audit.

ETROPTS—Events Sent

Valid on z/OS.

Use ETROPTS to control which events the Monitor sends to the CA Audit product.

All entry methods are accepted.

This control option has the following format:

```
ETROPTS(ADD|REM,VIO,LOG,START,INIT,USS,CMDADM,CONTROL)
```

ADD

Indicates that a new category of events are added to the current list of events.

REM

Indicates that a category of events are removed from the current list.

VIO

Transmits security violation events to CA Audit. This includes initiations and resource access violations.

LOG

Sends Audited events to CA Audit.

START

Sends CA Top Secret startup and termination events to CA Audit.

INIT

Sends successful initiations and terminations (signon/signoff) to CA Audit.

USS

Indicates that all USS activity logged to ATF/SMF is sent to CA Audit. You can also specify the calls:

- INITUSP for initUSP
- DELUSP for deleteUSP
- CHKACC for ck_access
- SETUID for R_setuid
- SETEUID for R_seteuid
- SETGID for R_setgid
- SETEGID for R_setegid
- CHOWN for R_chown
- CHMOD for R_chmod

- RAUDIT for R_chaudit
- CHAUD   for R_audit
- INITAC for initACEE
- SETFACLfor R_setfacl
- AUDITX for R_auditx

The maximum number of characters for each command is 80. If more characters are needed, another MODIFY command is required.

CMDADM

Sends TSS administrative commands (successes and failures) to CA Audit.

CONTROL

Sends control options changed from the console (F TSS,...) and from TSO (TSS MODIFY(...)) to CA Audit.

Examples: ETROPTS control option

This example adds successful initiations/terminations and administrative commands to the current list of events sent to CA Audit:

```
F TSS,ETROPTS(ADD,INIT,CMDAMD)
```

This example specifies that the R_chown and R_chmod USS calls are sent to CA Audit:

```
TSS MODIFY(ETROPTS(ADD,USS(CHOWN,CHMOD)))
```

EVALMODE—Common Criteria Evaluation Mode

Valid on z/OS.

Use the EVALMODE control option to specify whether the Common Criteria evaluation mode is active in CA Top Secret.

All entry methods are accepted.

This control option has the following format:

```
EVALMODE(YES|NO)
```

YES

Indicates that Common Criteria evaluation mode is active.

NO

Indicates that Common Criteria evaluation mode is not active.

EXIT—Installation Exit

Valid on z/OS and z/VM.

Use the EXIT control option to activate and deactivate the installation exit.

EXIT processing for resource checking requires the RDT attribute EXIT to be turned on for each resource class called the exit. By default the exit is not called for resources in the RDT. For information on the RDT attribute, see the *Command Functions Guide*.

All entry methods are accepted.

This control option has the following format:

```
EXIT(ON|OFF)
```

ON

Causes CA Top Secret to call the installation exit module (TSSINSTX) at all exit control points.

OFF

(Default) Deactivates the installation exit.

Installation Exit

CA Top Secret provides more than 17 control points at which systems programmers might write code to define security-checking procedures for initiation, volumes, and resources. This installation-unique code is housed in the TSSINSTX module, which resides in a link-listed library. CA Top Secret accesses this module and performs all functions and validations. If the EXIT option is not specified, CA Top Secret will assume EXIT(ON) provided that TSSINSTX exists. CA Top Secret ignores this option if no exit code exists.

If the exit abends, CA Top Secret automatically deactivates the exit and attempts to take a system dump.

The site must properly format and assemble the installation exit before it can be activated. A matrix within the exit will indicate the calls that the exit will accept.

EXPDAYS—Security File Expiration Interval

Valid on z/OS and z/VM.

Use the EXPDAYS control option to set how many additional days after a FOR or UNTIL clause has expired that an ADD or PERMIT is kept on the Security File before deletion.

After EXPDAYS, temporary ADD and PERMIT commands are not displayed by the TSS LIST, TSS WHOOWNS, or TSS WHOHAS commands.

Note: For the user to have the expired access again, issue a new TSS ADDTO or TSS PERMIT command.

This control option uses the Parameter file entry method.

This control option has the following format:

```
EXPDAYS(nn)
```

nn

Specifies the number of days a PERMIT or ADD is held in the Security File and displayed past its expiration date.

Range: 1 to 30

Default: 0

Example: EXPDAYS control option

This example indicates that the specific add or permit is held in the Security File and displayed three days beyond its expiration date:

```
EXPDAYS(3)
```

FACILITY—System Facility Processing

Valid on z/OS and z/VM.

Use the FACILITY control option to:

- Control the processing of each system facility
- Obtain the status of a facility

All entry methods are accepted.

This control option has the following format:

```
FACILITY(facility|ALL)
FACILITY(facility=subopt1<=value1>,...)
```

facility

The full name of a single facility.

Examples: FACILITY control option

This example displays the status of the TSO facility:

```
F TSS,FACILITY(TSO)
```

This example updates the FACILITY option:

```
TSS MODIFY(FACILITY(subopt1=operand<=value><,subopt2<=value2>>…))
```

This example alters the BATCH facility to WARN mode and sets NOLUMSG. Note that the suboption MODE requires a value, but that the NOLUMSG suboption does not:

```
TSS MODIFY('FACILITY(BATCH=MODE=WARN,NOLUMSG)')
```

Universal Suboptions

The following suboptions are available for facilities of all types:

ABEND

Resets the NOABEND suboption.

NOABEND

A multiuser address space facility (CICS, IMS, CA-Roscoe) will not abend if one user in the region causes a violation. This does not imply that the ACID used to define the Facility itself is immune from security abends during startup.

If NOABEND is set, CA Top Secret will not cancel the user's activity even if the violations exceed the violation's threshold (VTHRESH). CA Top Secret locks the user's terminal.

ACTIVE

Reactivates a facility that was deactivated via the FACILITY(facility=INACT) command.

CA Top Secret Status/Diagnostic Log listings displays "IN-USE" to indicate that a facility is active.

For example, to allow signons to the IMSPROD facility, enter:

```
FACILITY(IMSPROD=ACTIVE)
```

ASUBM

Indicates that CA Top Secret-authorized job submission is being used for the given facility.

NOASUBM

Resets the ASUBM suboption

AUDIT

Audits all activity for users who subsequently logon to the specified facility.

For example, to audit all user activity of a newly activated facility, enter:

```
FACILITY(IMSPROD=AUDIT)
```

NOAUDIT

Deactivates auditing of users who subsequently logon to the facility.

AUTHINIT

Requires an application to execute APF authorized in order to execute a RACINIT or RACROUTE REQUEST=VERIFY. See the *User Guide* for more information.

NOAUTHINIT

(Not recommended) Allows an application which is not APF authorized to execute a RACINIT or RACROUTE REQUEST=VERIFY. NOAUTHINIT requires that the program issuing the request must come from an APF authorized library, whether or not it is running with APF authorization. Another requirement for NOAUTHINT is that the request cannot include the PASSCHK=NO parameter.

DEFACID(*acid*)

Assigns a default ACID used for access to the specified facility by users who do not have defined ACIDs but require access to the facility. The TSS CREATE function must be used to define this default ACID. For example, a production CICS default ACID can be defined so that users who do not require specific security requirements are governed by the blanket requirements that are defined by the default ACID.

The DEFACID under CICS is used to satisfy an ATS signon only. In CICS3.2.1 or above, a DEFACID is not recommended and using CICS DFLTUSR is preferred. For example:

```
FACILITY(TSO=DEFACID(TSODEF))
```

Note: DEFACID is not needed for CICS 3.2 and above.

DEFACID(RDR*TERM)

Indicates that CA Top Secret derives the default ACID from the terminal or batch reader name, if the userid entered at signon is not defined as an ACID, or if the batch ACID is not supplied.

A default ACID for BATCH can be defined to handle RJE (Remote Job Entry) or NJE (Network Job Entry) job submission. If so defined, all jobs that are submitted derive a default ACID associated with the NJE or RJE node. This eliminates required JCL changes or possible viewing of passwords over the NJE or RJE lines.

A BATCH default ACID can also be defined for jobs submitted through a card reader. This will eliminate required JCL changes that include coding of passwords on the job card.

To establish a default ACID for RJE remotes 1, 2, and 3, the security administrator would specify the following the in the Parameter File:

```
FACILITY(BATCH=DEFACID(RDR*TERM))
```

The security administrator would then create and define ACIDS for remote readers 1, 2, and 3. CA Top Secret will use these ACIDS to derive the default ACIDS.

```
TSS CREATE(RM1) DEPARTMENT(XXX)
                FACILITY(BATCH)
                SOURCE(RM1)
                NAME('DEFAULT-FOR-SHOP-1')
```

The security administrator would continue to create ACIDS for readers 2 and 3. When a default ACID is assigned, the user receives message TSS7053I.

DEFACID(*NONE*)

Removes the default ACID for the facility specified. For example:

```
FACILITY(BATCH=DEFACID(*NONE*))
```

Note: DEFACID should never be used with facility TSO.

DORMPW

Honors password validation in DORMANT mode when specified for a facility. A DORMANT mode user must give the correct password to log on. For details, see the WARNPW sub-option.

Note: Message TSS7102E will only be issued for control type ACIDs.

NODORMPW

Does not honor CA Top Secret password validation in DORMANT mode.

DOWN=suboption

Controls how jobs are initiated and passwords changed for a facility when CA Top Secret's address space is inactive. There are six suboptions associated with the DOWN option:

- GLOBAL | *—Defaults to the setting defined by the DOWN control option. An asterisk (*) has the same meaning as GLOBAL.
- WAIT—Waits for CA Top Secret to be restarted.
- BYPASS—Bypasses security checking, does not invoke CA Top Secret until it is restarted.
- FAIL—Fails the request
- NORMAL—Reverts to native security (if any) until CA Top Secret is restarted. Overrides the global DOWN option for the particular facility.

EODINIT

Indicates that a RACINIT can be performed for the facility after a TSS ZEOD has been issued. Required for JES and Console facilities.

NOEODINIT

Indicates that a RACINIT cannot be performed for the facility after a TSS ZEOD has been issued.

ID=

Equals one or two alphanumeric characters that represents the facility for reporting purposes. This value is predefined in the Facilities Matrix Table and should not be changed unless defining or renaming a facility.

IJU

CA Top Secret inserts USER= and PASSWORD= into the JCL.

NOIJU

CA Top Secret will not insert USER= or PASSWORD= into the JCL. Under the FTP facility, specify NOIJU to ensure FTP userid ACID is propagated.

INACT

Deactivates ability to sign on to the facility specified. Active users will continue normally. For example, FACILITY(IMS=INACT) prevents users from signing on to IMS.

INSTDATA

Allows installation data to be stored within a region of the specified facility. See the *User Guide* for a description of INSTDATA.

For example:

```
FACILITY(TSO=INSTDATA)
```

NOINSTDATA

Prohibits storing of installation data in a facility region. Usually done to conserve space in large user regions.

IN-USE

Indicates that the facility definition has been updated. It is used to determine if the facility should be displayed as a result of a TSS MODIFY, FACILITY(ALL) or a TSS MODIFY, STATUS command. FACILITIES are marked as IN-USE as soon as a user signs on to them. Although it cannot be set directly, it is set by changing any option of the facility, through the PARMFILE or via a TSS MODIFY command. IN-USE is turned on even if the option is set to its default value.

KEY=n

Can be set to equal the TCB protect key that the facility uses for storage.

Default: 8

LCFCMD

Specifies that all LCF (Limited Command Facility) associated messages will refer to “Commands” in their text.

LCFTRANS

Specifies that all LCF-associated messages will refer to “Transactions” in their text.

LOCKTIME=n

Assigns the amount of time after which a terminal connected to a specific facility will lock, if CA Top Secret does not detect activity. Facility specific locktimes are overridden by a user's or profile's locktime.

The following example indicates that terminals logged on to CICSPROD will lock if CA Top Secret does not detect activity after five minutes.

```
FACILITY(CICSPROD=LOCKTIME=5)
```

LOG(log,log...)

LOG indicates what types of security events CA Top Secret will record, and where it will record them.

The LOG option allows this to be done for all facilities (global) while the LOG suboption allows LOG options to be specified for each facility. Facility-specific LOG options entered after any global LOG option will override the global option.

The security administrator might use the LOG suboption in one of three ways:

```
FACILITY(fac=LOG(ACTIVITY,ACCESS,SMF,INIT,MSG))
FACILITY(fac=LOG(NONE))
FACILITY(fac=LOG(ALL))
```

For example, to indicate that all events should be logged for CICS, enter:

```
FACILITY(CICSPROD=LOG(ALL))
```

LTLOGOFF=NO|YES

YES

CA Top Secret logs the user's terminal off when his locktime has expired for a second interval. Locktime transactions must be correctly installed. See the *Implementation: CICS Guide* for details.

NO

(Default) CA Top Secret will not log the user off.

LUMSG

Requests that the system display the “last-used” message when a user signs on to the specified facility. This operand only applies to USER type ACIDs running in other than DORMANT mode. USER type ACIDs will not display the “last-used” message in DORMANT mode in any case. Administrator type ACIDs will always display the “last-used” message.

For example:

```
FACILITY(CICSPROD=LUMSG)
```

NOLUMSG

Terminates the last-used message display. This operand does not apply to administrator type ACIDs that will always display the “last-used” message.

LUUPD

Activates the update of last used statistics for most successful signons. Automatic Terminal Signon (ATS) and preset terminal security normally do not update last used statistics. Last used statistics can be activated for these signons using OPTIONS(30) at TSS startup. This setting is the default for all facilities and should typically remain so.

NOLUUPD

Prevents updating of the last—used statistics for all successful signon events within this facility, regardless of the setting of the RACROUTE macro specification of the STAT=ASIS/NO parameter. Use NOLUUPD to reduce the amount of I/O to the security file when experiencing severe I/O performance problems.

This sub-option does not prevent the display of the last used messages. Use the NOLUMSG option for this.

With this sub-option set, the last used statistics are only updated when a user incurs a password violation in this facility. This event updates the password violation count and the last used statistics.

MAXSIGN=(nnn,RETRY|KILL)

nnn

Specifies the maximum number of queued signon/signoff requests that are processed..

Default: 10

Range: 5 to 100.

For example, to manually set the threshold at 15.

```
TSS MODIFY FACILITY(CICSPROD=MAXSIGN=(15))
```

Note: The parentheses around the value are required.

RETRY

Signon/signoff requests that exceed the threshold are requeued. For example, in the sample command shown next, additional attempts to sign on are requeued to CICS.

```
TSS MODIFY FACILITY(CICSPROD=MAXSIGN=(100,RETRY))
```

KILL

Abends the signon/signoff transaction. When Kill is set and the number of users attempting to sign on equals the threshold, additional attempts to sign on are failed. For example, you can restrict the number of concurrent signons to a CICS facility called CICSPAY to a threshold of 15 by using the TSS MODIFY command like this:

```
TSS MODIFY FACILITY(CICSPAY=MAXSIGN=(15,KILL))
```

When coding MAXSIGN and MAXUSER in the CA Top Secret PARM field, the MAXUSER option must be coded before MAXSIGN. If MAXUSER is not coded first, an invalid data error will occur during CA Top Secret initialization.

MAXUSER=nnnn

Specifies the size of the ACID cross-reference table in any multi-user address space system. In order to increase the size of the cross-reference table, you must recycle the address space. In CICS, the MAXUSER value specified is also used to calculate necessary USCB allocation at startup.

When a multi user region starts up, the MAXUSER XREF table is built to hold the user ID and key. This table is 16 bytes times the MAXUSER value, one 16 byte entry for each user that signs on. When a user signs off, the entry is cleared and available for reuse.

When the XREF table fills up, message TSS0962E is issued. Users can sign on, but there is no entry added to the XREF table so if the region abends the storage for the user(s) is not freed. This can cause orphaned storage.

Default: 3000

Minimum: 256

MODE=mode

Specifies a specific security mode for the facility:

- DORM
- FAIL
- IMPL
- WARN

Modes specified by facility must be entered after global or system-wide mode selections in the PARMFILE. Thus, if the global mode is FAIL, but WARN is specified for the IMS facility, then all users initiating from IMS will operate in the WARN mode.

If the global mode is changed via an O/S Modify command:

```
F TSS,MODE(D|W|I|F)
```

MSGLC indicates that user violation messages are issued in mixed case. NOMSGLC indicates that user violation messages are issued in upper case only.

MULTIUSER

Used to indicate a multiuser address space.

A multiuser address space supports multiple users. Security is generally not handled by z/OS. The following facilities are examples of multiuser address space facilities: CICS, IMS, CA-Roscoe, and CA-IDMS.

An example of a multiuser address space appears next.

```
FACILITY(IMS1=MULTIUSER)
```

NAME=fffff

Changes the base name of a facility in the Facility matrix table. Once changed, the new facility name must always be used. To change a facility name from CICSPROD to CICSPAY, enter:

```
FAC(CICSPROD=NAME=CICSPAY)
```

NPWR

Specifies whether a TSO or CICS facility supports password reverification. There is a default of two attempts for new passwords to be verified before complete logon sequence needs restarting. To set the threshold value for TSO and CICS, see NPWRTHRESH for details. When a user logs on to a facility that has activated the NPWR sub-option of the FACILITY control option, and enters a new password, the following message is issued:

```
TSS7016A ENTER NEW PASSWORD AGAIN FOR REVERIFICATION
```

The user then enters the new password a second time for reverification. This ensures that the user correctly enters and remembers the new password. If the user enters an incorrect reverified password, he is prompted again. After the second attempt, if the reverified new password is still incorrect, the following message is issued and an accompanying DRC(015) is returned.

```
TSS7111E NEW PASSWORD CHANGE INVALID - REVERIFICATION FAILED
```

NONPWR

Does not force password reverification.

PGM=xxx or xxxxxxxx

Supplies all eight or just the first three characters of the program name issuing RACINIT SVC's. Online systems use RACINIT to support signon validation for individual users. This is the key to determining the (generic) facility. See the *User Guide* for details on RACINIT.

PRFT=nnnn

Specifies the size of the shared profile table in increments of 256 entries. A single shared profile table is allocated at the start of a region if its facility has SHRPRF set. The storage for the shared profile table is in extended private, subpool 230. Each entry in the table is 16 bytes long and contains the:

- Profile ACID ID
- Number of users sharing the profile
- Profile address
- Change indicator

A region's shared profile table must have enough entries to hold the highest number of unique profiles that can be allocated within the region at any time. For example, a region supporting 250 users, each sharing 3 common profiles, where each user also has 1 unique profile, must have a shared profile table with no less than 253 entries.

When the shared profile table becomes full, the address space reads 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.

Default: 3

PROMPT

FOR TSO ONLY: Makes it useless for users to enter their passwords with their userid when logging on. This helps prevent CA Top Secret from displaying passwords on the terminal. If a user enters his password and user ID at the same time, CA Top Secret will issue a warning message and lock the user's terminal for 10 seconds (the default), then prompt for the password.

NOPROMPT

Deactivates the PROMPT suboption.

RES

Provides for the interpretation and recognition of maskable resources within the facility. Some examples of maskable resource classes are DATASET, JESSPOOL, DB2DBASE and DB2COLL. Without RES on the facility, security checks against these resource classes will fail. To identify a maskable resource class, see the *Command Functions Guide*.

RXLTLIST

Lists all the resource class translate entries defined to the translate table.

RXLTADD(oldclass:newclass)

Specifies a resource class translate entry to be added to the translate table.

oldclass

Specifies the source resource class.

newclass

Specifies the target resource class for the translation that occurs during the resource validation process.

Both old and new resource classes must exist in the RDT. An old class defined to the RDT as a type PIE or MRIE cannot be translated to a new class type RIE.

RXLTREM(oldclass)

Specifies a resource class translate entry to be removed from the translate table.

NORES

Prevents the interpretation and recognition of maskable resources within a facility. In high performance transaction managers that do not normally make use of maskable resource classes, this can improve performance. However, security features, which do involve maskable resources, cannot be used.

RNDPW

Enables random password generation in a facility. Two methods are supported:

- User initiated—random password generation is in effect when the facility suboption RNDPW is set. Users can have CA Top Secret generate a password for them by entering RANDOM in the New Password field. This option does not preclude users from specifying their own password in accordance with NEWPW criteria.
- Automatic initiated—random password generation takes place when the user's current password expires, and both facility suboption RNDPW and global option NEWPW(RN) are in effect.

RNDPW is set by default for TSO, CICS, and IMS. Some facilities might not display new, randomly generated passwords. Each facility, therefore, should test RNDPW before placing it into production.

Note: When neither RNDPW facility suboption nor NEWPW(RN) option are set and a user enters RANDOM as a new password, RANDOM is evaluated literally and set the user's password to RANDOM. NEWPW(RN) global option must not be set if user-initiated random password generation is required.

NORNDPW

Cancels the RNDPW suboption.

SHRPRF

Allows profile sharing in multiuser address space environments such as CA-Roscoe®, IMS, and CICS where it is important to conserve storage. SHRPRF allows a copy of the profile to be shared by all users in the multiuser facility. Thus, storage is used efficiently.

After a profile has been updated, users must have their profile refreshed by the security administrator, or sign on again to access the new profile. If not, the user will continue to access the version with which he signed on.

NOSHRPRF

Prohibits profile sharing for the specified facility.

SIGN(M)

Allows simultaneous logons with the same ACID for the specified facility.

SIGN(S)

Sets CA Top Secret to disallow simultaneous signon for an address space by the same ACID from different sources (e.g. network terminals). When a duplicate signon is sensed, CA Top Secret issues message TSS7172E and disallows the second session. In IMPL and FAIL mode, this restriction is strictly enforced. In WARN mode, only a message is issued: signon by the same ACID from multiple terminals is logged and the user is warned, but the restriction is not enforced.

Note: Keyword SIGNMULTI allows specific user ACIDs to sign on multiple times, when the facility sub-option is SIGN(S) and you have specified TYPE=CICS as the FACILITY option. See information, see the *Command Functions Guide.*

STMSG

Requests that the system display the status message when a user signs on to the specified facility. This operand only applies to USER type ACIDs running in other than DORMANT mode. USER type ACIDs will not display the status message in DORMANT mode in any case. Administrator type ACIDs will always display the status message.

NOSTMSG

Terminates the status message display. This operand does not apply to administrator type ACIDs that will always display the status message.

SUAS

Used to indicate a single-user address space. For the purposes of CA Top Secret, a single-user address space requests data sets directly from z/OS. These facilities are single-user address spaces: TSO, BATCH, and STC.

TRACE

Allows entire facility to be traced. See SECTRACE for more information.

NOTRACE

Deactivates the TRACE suboption.

TSOC

Indicates that a facility is TSO compatible, the facility can handle TGET and TPUT SVCs.

NOTSOC

Cancels the TSOC suboption.

TYPE

When listing all facilities, a three-digit numerical value (ranging from 000 to 100) displays for the TYPE= parameter. This parameter should not be changed except when defining or renaming a new CICS, CA-IDMS®, DB2, CA-ROSCOE, or IMS facility. Then TYPE= must be specified as TYPE=CICS, TYPE=IDMS, TYPE=DB2, TYPE=ROSCOE, or TYPE=IMS. These changes will also update the facility ID numbers (CICS=004, IDMS=011, DB2=100, ROSCOE=007, and IMS=005.) A facility with no predefined keyword is assigned display type 099.

When used to modify a dummy facility, the keyword facility TYPE must be used as follows:

```
TSS MODIFY FACILITY(xxxxx=TYPE=IMS)
```

UIDACID=n

Specifies that the first n characters of an online userid is used to derive the ACID for the user.

WARNPW

Forces defined users and jobs to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a job to process, even if the user omitted his password or entered it incorrectly.

If the user signs on with a security administrator's ACID, and omits or enters an invalid password, CA Top Secret will FAIL the request regardless of the current security mode, or control option settings. CA Top Secret ignores the WARNPW option for undefined user ACIDS, and in DORMANT mode.

NOWARNPW

Cancels the WARNPW suboption.

XDEF

Sets protection in place by default for all commands and transactions controlled by the facility. Explicit authorization is required through LCF (Limited Command Facility) or through OTRAN permission.

NOXDEF

Indicates that transactions and commands need not be authorized through LCF before they can be used.

CICS-Related FACILITY Suboptions

The following suboptions are CICS-specific and can be used when you have specified TYPE=CICS as the FACILITY option.

Note: For information about how these CICS suboptions are used, see the *Implementation: CICS Guide*.

The following suboptions comprise the CICS BYPASS and CICS PROTECT resource lists:

BYPLIST

Lists all CICS resources on the bypass list and protect list.

To display the default Bypass and Protect Lists, issue the following command:

```
TSS MODIFY(FACILITY(CICSPROD=BYPLIST))
```

Results of the command are displayed below.

Important! The ellipsis (....) punctuation is essential and represents internal CICS transactions with hexadecimal unprintable names.

```
FACILITY DISPLAY FOR CICSPROD
BYPASS TABLE DISPLAY FOR FACILITY  CICSPROD
RESOURCE=LOCKTIME BYPASS  NAMES:   TSS
RESOURCE=TRANID   BYPASS  NAMES:   CAQP   CATA   CATD   CATP
 CATR   CAUT   CCIN   CCMF   CDBD   CDBN   CDBO   CDBT
 CDTS   CECS   CEGN   CEHP   CEHS   CESC   CESF   CESN
 CFTS   CGRP   CITS   CLQ2   CLR1   CLR2   CLS3   CLS4
 CMPX   CMTS   CNPX   COVR   CPLT   CPMI   CQPI   CQPO
 CQRY   CRDR   CRMD   CRSQ   CRSR   CRSY   CRTE   CRTR
 CSAC   CSCY   CSFU   CSGM   CSGX   CSHR   CSIR   CSJC
 CSKP   CSLG   CSMI   CSM1   CSM2   CSM3   CSM4   CSM5
 CSNC   CSNE   CSPG   CSPK   CSRK   CSPP   CSPQ   CSPS
 CSRS   CSSC   CSSF   CSSN   CSSX   CSSY   CSTA   CSTB
 CSTE   CSTP   CSTT   CSXM   CSXX   CSZI   CVMI   CVST
 CWTR   CXCU   CXRE   CXRT   TS     8888   9999   ....
 ....   ....   ....   ....   ....   CFTL   CFSL   CKTI
 CKAM   CFCL   CIOD   CIOF   CIOR   CIRR   CJTR   CSHA
 CSHQ   CSOL   CTSD   CWBG   CWXN   CDBF   CEX2   CFQR
 CFQS   CSFR   CSQC   CDBQ   CRMF   CLSG   CFOR   CJMJ
 CLS1   CLS2   CPIH   CPIL   CPIQ   CRTP   CWXU   CPIR
 CPIS   CISC   CISD   CISE   CISR   CISS   CIST   CJGC
 CJPI   CISB   CEPD   CEPM   CISQ   CISU   CISX   CIS4
 CRLR   CISM   CEPT   CPSS   CJSR   CESL   CISP   CIS1
 CJSL   CRST   CPCT   CFCR   CJLR
RESOURCE=TRANID   PROTECT NAMES:   CEDF   TSEU
```

BYPADD(*class=resource*)

Specifies a CICS resource prefix to add to the bypass list. Resources of this class that match this prefix are not checked by CA Top Secret security when used on a CICS with this facility.

BYPREM(*class=resource*)

Specifies a CICS resource prefix to remove from the bypass list.

DB2=*name*

Contains the resource names for CICS keywords DB2CONN, DB2ENTRY, and DB2TRANS. These resource names are checked against the resource class associated with the XDB2 SIT or FACILITY option. For example, DB2=P8 bypasses security checking for DB2CONN(P8*), DB2ENTRY(P8*), and DB2TRANS(P8*) when FACMATRX=YES and XDB2=YES in the associated CICS facility.

PROTADD(*class=resource*)

Specifies CICS resources that are added to the protect list and will override a (generally shorter) entry on the bypass list.

PROTREM(*class=resource*)

Specifies CICS resources to remove from the protect list.

Resources can be added to the bypass list (to avoid checking by CA Top Secret) or added to the protect list (to be checked). If a resource is added to both lists, the entry on the protect list overrides the bypass list. For example, the following entry on the bypass list would bypass security checking for all transactions beginning with XY:

```
TSS MODIFY FACILITY(CICSTEST=BYPADD(TRANID=XY)
```

You can still check for security on transaction XYZ by entering the following command:

```
TSS MODIFY FACILITY(CICSTEST=PROTADD(TRANID=XYZ)
```

The PROTADD(TRANID=XYZ) command overrides the BYPADD(TRANID=XY) command. The transactions XYAB and XYQZ match the prefix on the bypass list but do not match the override protection in the protect list: these transactions would be bypassed. The transactions XYZ and XYZQ match the entries in both the bypass list and the protect list; so the protect list entry takes precedence.

CICS Resource Class

The following CICS resource classes can be used with the BYPADD, BYPREM, PROTADD, and PROTREM suboptions.

Note: This list is intended for a limited number of resources and should not be used as an alternative for the ALL Record.

CEMT=action

Contains Extended Master Terminal Command actions, valid actions are; ADDTO, INQUIRE, PERFORM, REMOVE, and SET. For example, to bypass all CEMT INQUIRE commands, enter:

```
TSS MODIFY FACILITY(CICSTEST=BYPADD(CEMT=INQUIRE))
```

DCT=tdq

Contains transient data entries.

DSNAME=name

Contains the File Control Table entries associated with the data set. The DSNCHECK= suboption must be set to YES.

FCT=ddname

Contains File Control Table entries. The DSNCHECK= suboption must be set to NO.

JCT=name

Contains Journal Control Table entries.

LOCKTIME=(list)

The elements in the list may be transactions or terminals:

```
TSS MODIFY (fac(xxxxxxxx=PROTADD(LOCKTIME=yyyy)))
```

xxxxxxxx

CICS facility name.

yyyy

Transaction or Terminal. For transactions, supply the complete transaction ID. For terminals, the resource should be specified according to the access method:

- VTAM=Netname
- TCAM=Terminal ID
- BTAM=Terminal ID
- PCLOCK=YES|NO

Specifies whether LOCKTIME is pseudo-conversational or conversational. YES equals pseudo-conversational. Recycling of CICS is required when this control option is changed.

PCT=tranid

Contains interval control started transaction identifiers that are not checked by CA-Top Secret.

PPT=name

Contains program processing control entries that are not checked by CA-Top Secret.

PSB=name

Contains PSB entries.

SPI=action

Contains a list of CICS command level application programming interface commands. Valid commands are: EXEC CICS SET and EXEC CICS INQUIRE. For example, to protect all EXEC CICS SET commands, enter:

```
TSS MODIFY FACILITY(CICSTEST=PROTADD(SPI=SET))
```

To bypass all EXEC CICS INQUIRE commands, except SYSTEM, enter:

```
TSS MODIFY FACILITY(CICSTEST=BYPADD(SPI=INQUIRE))
```

To bypass EXEC CICS INQUIRE SYSTEM, also enter:

```
TSS MODIFY FACILITY(CICSTEST=BYPADD(CEMT=INQUIRE))
```

SYSID=sysid

Contains system identification names of the CICS systems. SYSID= is only applicable to CICS 3.3 and below.

Note: If EXTSEC=NO is coded in the DFHSIT parameter or the FACMATRX suboption, you must add SYSID to the bypass list.

TCT=(list)

Contains a list of terminal entries.

VTAM=Netname, TCAM=Terminal ID and BTAM=Terminal ID

TRAN=tranid

Contains transaction identifiers that are not checked by CA-Top Secret.

TRANID=tranid

Contains transaction identifiers that will bypass all security checking for the transaction. When issuing a TSS MODIFY(FACILITY(CICS facname)) command, the bypass list for TRANID will contain '...'. These periods represent CICS internal transactions whose names contain unprintable characters. These entries cannot be removed.

TRANID is different from TRAN in that TRANID uses all types of security checking (OTRAN, LCF, file, program, locktime). TRAN only uses OTRAN or LCF security checking.

TSS MODIFY FACILITY(CICS=BYPADD(TRANID=HELP))

Note: TRANID=TS should not be removed from the CICS Bypass List. It is always needed for LOCK/UNLOCK. Security for the TSS transaction is controlled entirely through administrative authorities; not through transaction protection.

TRANID overrides TRAN in the FACILITY BYPASS LIST.

TST=tsq

Contains Temporary Storage entries.

DSNCHECK=YES|NO

Specifies whether individual data set names or File Control Table entries are checked. XFCT=YES is required for DSNAME checking if running CICS 3.3 or below. See the FACMATRX in the CICS SIT/PCT Override FACILITY Settings section. If DSNCHECK is specified, then RES must also be set.

CICS SIT/PCT Override FACILITY Settings

CICS SIT/PCT settings defined to CICS might be overridden by FACILITY settings as described next.

FACMATRX=YES|NO

Specifies whether CA Top Secret is to override definitions defined to CICS through table assemblies or the CSD file.

YES

CA Top Secret facility settings override CICS definitions.

NO

(Default) CICS definitions override conflicting facility settings.

EXTSEC=

Indicates whether CA Top Secret security is active or inactive.

YES

CA Top Secret security is invoked for this region.

NO

One of the following:

- For CICs 3.3 and below, CA Top Secret security is inactive, but still present. CA Top Secret is running in an inactive state. An entry has to be made to the SYSID bypass list if you are running in any mode except DORMANT.
- For CICS 4.1 and above, CA Top Secret security is not present. No SYSID bypass list is necessary to inactivate security with this release.
- CA-ENF is invoked together with CA Top Secret to process the security parameters set for your CICS region. We recommend the use of the facility matrix (FACMATRX=YES) for setting these security parameters, since this centralizes security functions in data sets controlled by the security administrator. The alternative (FACMATRX=NO) distributes the responsibility to the SIT assembly or to the SIT override data set (if used). When external security is enabled (SIT SEC=YES or FACMATRX EXTSEC=YES), depending upon your security implementation, you might choose to selectively disable external security which you do not employ by setting off one or more of the "XPARMS" below; setting such parameters OFF prevents CICS from generating security queries, and can reduce security file I/O searching for resources and permissions which do not exist. For information about disabling CAIENF calls when using XPARMS, see the *Implementation: CICS Guide*.

XAPPC=

Indicates whether session security can be used.

YES

Session security can be used.

NO

Session security cannot be used. Only the BIND password (defined to CICS for the APPC connection) is checked.

XCMD=

Indicates whether EXEC CICS commands are checked by CA Top Secret.

YES

All SPI commands *are* checked by CA Top Secret.

NO

All SPI commands *are not* checked by CA Top Secret.

SPI commands include both CEMT commands and EXEC CICS SPI commands from an application program.

XDB2=YES|NO

Enables/disables secondary resource checking for resource class CTSDB2 to substitute for CICS/DB2 keywords:

- DB2CONN
- DB2ENTRY
- DB2TRANS

During initialization, for CTS 1.2 and above, CICS activates a profile for class CTSDB2. CICS performs security checking by substituting CTSDB2 for the keyword. When XDB2=YES, and FACMATRX=YES, the administrator is also expected to provide security for IBMFAC(DFHDB2.) as documented by IBM in the CICS RACF Security Guide.

XDCT=

Indicates whether transient data entries are checked by CA Top Secret.

YES

Transient data entries for this region *are* checked by CA Top Secret.

NO

Transient data entries for the region *are not* checked by CA Top Secret.

XEJB=

Specifies whether support of security roles is enabled.

YES

CICS Support for security roles is enabled:

When an application invokes a method of an enterprise bean, CICS calls the external security manager to verify that the userid associated with the transaction is defined in at least one of the security roles associated with the method.

When an application invokes the following method:

```
isCallerInRole()
```

CICS calls the external security manager to determined whether the userid associated with the transaction is defined in the role specified on the method call.

NO

CICS support for security roles is disabled. CICS does not perform enterprise bean method level checks, allowing any userid to invoke any enterprise bean method. The following method always returns a value of TRUE:

```
isCallerInRole()
```

Note: To enable security role support, you must also specify SEC=YES (when FACMATRX=NO) or EXTSEC=YES (when FACMATRX=YES). A change to XEJB or EJBRPRFX requires the CICS region to be recycled in order to implement.

XFCT=

Indicates whether file control entries for the region are checked by CA Top Secret.

YES

File control entries for this region *are* checked by CA Top Secret. Required for DSNAME checking.

NO

File control entries for this region *are not* checked by CA Top Secret. Deactivates DSNAME checking.

XHFS=

Specifies whether or not CICS is to check the transaction user's ability to access files in the z/OS Unix System Services file system. This parameter is automatically set to NO in CTS release 3.1 and below.

YES

CICS calls CA Top Secret to check whether or not the user is authorized to access the file identified by the URIMAP that matches the incoming URL.

NO

CICS is not to drive a validation of access permission for z/OS UNIX files.

XJCT=

Indicates whether journal entries are checked for this region by CA Top Secret.

YES

Journal entries for this region *are* checked by CA Top Secret.

NO

Journal entries for this region *are not* checked by CA Top Secret.

XPCT=

Indicates whether EXEC-started transactions for this region are checked by CA Top Secret.

YES

EXEC-started transactions for this region *are* checked by CA Top Secret.

NO

EXEC-started transactions for this region *are no***t** checked by CA Top Secret.

XPPT=

Indicates whether program entries for this region are checked by CA Top Secret.

YES

Program entries for this region *are* checked by CA Top Secret.

NO

Program entries for this region *are not* checked by CA Top Secret.

XPSB=

Indicates whether PSB entries for this region are checked by CA Top Secret.

YES

PSB entries for this region *are* checked by CA Top Secret.

NO

PSB entries for this region *are not* checked by CA Top Secret.

XRES=

On CTS 3.2 and above systems, indicates whether or not CICS DOCCTEMPLATE resource validations should be processed. This parameter is treated as NO for all CICS releases below CTS 3.2.

YES

DOCTEMPLATE resource validations are performed.

NO

DOCTEMPLATE resource validations are not performed and all attempts to access DOCTEMPLATE resources are allowed.

XTRAN=

Indicates whether attached transaction entries for this region are checked by CA Top Secret.

YES

Attached transaction entries for this region are checked by CA Top Secret

NO

Attached transaction entries for this region are not checked by CA Top Secret.

XTST=

Indicates whether temporary storage entries for this region are check by CA Top Secret.

YES

Temporary storage entries for this region are checked by CA Top Secret.

NO

Temporary storage entries for this region are not checked by CA Top Secret.

XUSER=

Indicates whether surrogate user checking is performed by CA Top Secret.

YES

Surrogate user checking is performed by CA Top Secret.

NO

Surrogate user checking is not performed by CA Top Secret.

EJBRPRFX=16-byte-value

Enables the use of EJB Role Prefixing (for CTS 2.2 and above). This facility suboption specifies a 16-byte-value as the prefix that is used to qualify the security role defined in an enterprise bean's deployment descriptor. The prefix is applied to the security role when:

- A role is defined to an external security manager. CICS calls the external security manager to perform method authorization checks
- An application invokes the following method:

isCallerInRole()

You can specify a prefix of up to 16 characters. The prefix must not contain a period (.) character. If you specify a prefix that contains lowercase characters, blanks, or punctuation characters, you must enclose it in apostrophes. If the prefix contains an apostrophe, code two successive apostrophes to represent it.

The EJBRPRFX facility control sub-option overrides the CTS 2.2 SIT parameter EJBROLEPRFX when FACMATRX=YES. CA Top Secret does not support the use of mixed case with EJBRPRFX. If FACMATRX=YES and EJBRPRFX is not modified, CA Top Secret will interpret EJBROLEPRFX as the null string. You might implement mixed case security role support if you specify EJBROLEPRFX in the CICS SIT, and set FACMATRX=NO.

The EJBROLEPRFX parameter is ignored if security role support is not enabled. To enable security role support you must specify SEC=YES and XEJB=YES. If there is a change to security role support while a CICS region is executing, a recycle of the region is required in order to implement the change.

PCTCMDSEC=HONOR|<u>OVERRIDE</u>

Specifies whether CA Top Secret will honor the SIT parameter CMDSEC=. PCTCMDSEC= is only applicable to CICS 3.1.1 and above.

OVERRIDE

(Default) CA Top Secret will not honor the PCT CMDSEC= parameter and will force a security call.

HONOR

CA Top Secret will honor the SIT parameter CMDSEC=.

PCTEXTSEC=HONOR|<u>OVERRIDE</u>

Specifies whether CA Top Secret will honor the PCT parameters EXTSEC= and RSLC=. PCTEXTSEC= is only applicable to CICS 3.1 and below.

OVERRIDE

(Default) CA Top Secret will not honor the PCT EXTSEC= and RSLC= parameters and will force a security call.

HONOR

CA Top Secret will honor the PCT parameters EXTSEC= and RSLC=.

PCTRESSEC=HONOR|OVERRIDE

Specifies whether CA Top Secret will honor the SIT parameter RESSEC=. PCTRESSEC= is only applicable to CICS 4.1 and above.

OVERRIDE

(Default) CA Top Secret will not honor the SIT RESSEC= parameter and will force a security call.

HONOR

CA Top Secret will honor the SIT parameter RESSEC=.

CICS Specific Suboptions

CICSCACHE

Identifies the facility matrix sub option in the modification of the CICS caching option. This option sets the processing options and size for the memory "cache box" that TSS allocates for each terminal session. As resources are successfully accessed, resources are cached to minimize security file and audit file access. Cached resources are not rechecked against the security file. By default, cached resources will not be audited, and the cache is cleared at the end of every transaction. The cache box size defaults to 512 bytes.

```
TSS MODI FAC(CICSPROD=CICSCACHE(SESSLIFE,AUDIT,2048))
```

TASKLIFE|SESSLIFE

Defines CICS resources to be cached for the life of the transaction (TASKLIFE) or the life of the signed—on user (SESSLIFE).

Default: TASKLIFE.

NOAUDIT|AUDIT

Defines whether new resource checks of previously cached resources will be written to the ATF (audit tracking file).

512, 1024, 2048, or 4096

Defines the size of the CICS cache box. The larger the size the more resources can be kept inside. Once the cache box is full, the oldest entries get removed.

Default: 512

RLP=

Indicates whether RLP processing is activated by CA Top Secret. Valid operands include:

YES

RLP processing is activated by CA Top Secret

NO

RLP processing is not activated by CA Top Secret

SIGN(M)

Sets CA Top Secret to allow simultaneous signon for an address space by the same ACID from different sources (for example, network terminals). CA Top Secret will not convert a product to allow multiple signons where the product itself only tolerates single signons within the address space. It is recommended that you recycle the related CICS region(s) after dynamically changing SIGN(M); otherwise, unpredictable effects can occur.

Note: This parameter interacts with the CICS SIT parameter SNSCOPE. For details, see the *Implementation: CICS Guide*.

SIGN(S)

Sets CA Top Secret to disallow simultaneous signon for an address space by the same ACID from different sources (network terminals). When a duplicate signon is sensed, CA Top Secret issues message TSS7172E and disallows the second session. It is recommended that you recycle related CICS region(s) after dynamically changing SIGN(S); otherwise, unpredictable effects can occur.

Note: This parameter interacts with the CICS SIT parameter SNSCOPE. For details, see the *Implementation: CICS Guide*.

SLP=

Indicates whether SLP processing is activated by CA Top Secret.

YES

SLP processing is activated by CA Top Secret

NO

SLP processing is not activated by CA Top Secret

Options for Invoking Predefined Facilities

You can use the following default option specifications to invoke predefined facilities in CA Top Secret:

```
ACEP
INITPGM=ACE    ID=A  TYPE=27
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
APPC
INITPGM=ATB    ID=AP TYPE=03
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=IN-USE,ACTIVE,NOSHRPRF,NOASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,EODINIT,DORMPW,NONPWR
MODE=WARN  DOWN=GLOBAL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
MAXUSER=03000  PRFT=003
BATCH
INITPGM=IEFIIC    ID=B   TYPE=01
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9,SMF
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
CA7
INITPGM=SAS   ID=U  TYPE=025
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=NOLUMSG,NOSTMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
MODE=WARN DOWN-GLOBAL LOGGING=ACCESS,INIT,SMF,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
CICSPROD
INITPGM=DFH      ID=C  TYPE=004
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
ATTRIBUTES=LUUPD
MODE=WARN  DOWN=GLOBAL  LOGGING=ACCESS,INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE*   KEY=8
FACMATRX=NO       EXTSEC=YES      EJBRPRFX=NO
```

```
XJCT=YES XFCT=YES XCMD=YES XDCT=YES XTRAN=YES XDB2=NO  XEJB=NO
XTST=YES XPSB=YES XPCT=YES XPPT=YES XAPPC=NO  XUSER=NO
XHFS=NO  XRES=NO
PCTEXTSEC=OVERRIDE    PCTCMDSEC=OVERRIDE  PCTRESSEC=OVERRIDE
DSNCHECK=NO   LTLOGOFF=NO       RLP=NO   SLP=NO   PCLOCK=NO
MAXUSER=03000  PRFT=003  MAXSIGN=010,RETRY
CICSCACHE=TASKLIFE,NOAUDIT,0512
FACILITY DISPLAY FOR CICSPROD
BYPASS TABLE DISPLAY FOR FACILITY  CICSPROD
RESOURCE=LOCKTIME BYPASS  NAMES:   TSS
RESOURCE=TRANID   BYPASS  NAMES:   CAQP   CATA   CATD   CATP
 CATR   CAUT   CCIN   CCMF   CDBD   CDBN   CDBO   CDBT
 CDTS   CECS   CEGN   CEHP   CEHS   CESC   CESF   CESN
 CFTS   CGRP   CITS   CLQ2   CLR1   CLR2   CLS3   CLS4
 CMPX   CMTS   CNPX   COVR   CPLT   CPMI   CQPI   CQPO
 CQRY   CRDR   CRMD   CRSQ   CRSR   CRSY   CRTE   CRTR
 CSAC   CSCY   CSFU   CSGM   CSGX   CSHR   CSIR   CSJC
 CSKP   CSLG   CSMI   CSM1   CSM2   CSM3   CSM4   CSM5
 CSNC   CSNE   CSPG   CSPK   CSRK   CSPP   CSPQ   CSPS
 CSRS   CSSC   CSSF   CSSN   CSSX   CSSY   CSTA   CSTB
 CSTE   CSTP   CSTT   CSXM   CSXX   CSZI   CVMI   CVST
 CWTR   CXCU   CXRE   CXRT   TS     8888   9999   ....
 ....   ....   ....   ....   ....   CFTL   CFSL   CKTI
 CKAM   CFCL   CIOD   CIOF   CIOR   CIRR   CJTR   CSHA
 CSHQ   CSOL   CTSD   CWBG   CWXN   CDBF   CEX2   CFQR
 CFQS   CSFR   CSQC   CDBQ   CRMF   CLSG   CFOR   CJMJ
 CLS1   CLS2   CPIH   CPIL   CPIQ   CRTP   CWXU   CFIR
 CPIS   CISC   CISD   CISE   CISR   CISS   CIST   CJGC
 CJPI   CISB   CEPD   CEPM   CISQ   CISU   CISX   CIS4
 CRLR   CISM   CEPF   CPSS   CJSR   CESL   CISP   CIS1
 CJSL   CRST   CPCT   CFCR   CJLR
 RESOURCE=TRANID   PROTECT NAMES:   CEDF   TSEU

CICSTEST
INITPGM=DFH      ID=K  TYPE=004
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
ATTRIBUTES=LUUPD
MODE=WARN  DOWN=GLOBAL  LOGGING=ACCESS,INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE*   KEY=8
FACMATRX=NO       EXTSEC=YES      EJBRPRFX=NO
XJCT=YES XFCT=YES XCMD=YES XDCT=YES XTRAN=YES XDB2=NO  XEJB=NO
XTST=YES XPSB=YES XPCT=YES XPPT=YES XAPPC=NO  XUSER=NO
XHFS=NO  XRES=NO
PCTEXTSEC=OVERRIDE    PCTCMDSEC=OVERRIDE  PCTRESSEC=OVERRIDE
DSNCHECK=NO   LTLOGOFF=NO       RLP=NO   SLP=NO   PCLOCK=NO
MAXUSER=03000  PRFT=003  MAXSIGN=010,RETRY
CICSCACHE=TASKLIFE,NOAUDIT,0512
```

```
FACILITY DISPLAY FOR CICSTEST
BYPASS TABLE DISPLAY FOR FACILITY  CICSTEST
RESOURCE=LOCKTIME BYPASS  NAMES:   TSS
RESOURCE=TRANID   BYPASS  NAMES:  CAQP  CATA  CATD  CATP
   CATR  CAUT   CCIN   CCMF   CDBD   CDBN   CDBO   CDBT
    CDTS   CECS   CEGN   CEHP   CEHS   CESC   CESF   CESN
    CFTS   CGRP   CITS   CLQ2   CLR1   CLR2   CLS3   CLS4
    CMPX   CMTS   CNPX   COVR   CPLT   CPMI   CQPI   CQPO
    CQRY   CRDR   CRMD   CRSQ   CRSR   CRSY   CRTE   CRTR
    CSAC   CSCY   CSFU   CSGM   CSGX   CSHR   CSIR   CSJC
    CSKP   CSLG   CSMI   CSM1   CSM2   CSM3   CSM4   CSM5
    CSNC   CSNE   CSPG   CSPK   CSRK   CSPP   CSPQ   CSPS
    CSRS   CSSC   CSSF   CSSN   CSSX   CSSY   CSTA   CSTB
    CSTE   CSTP   CSTT   CSXM   CSXX   CSZI   CVMI   CVST
    CWTR   CXCU   CXRE   CXRT   TS     8888   9999   ....
    ....   ....   ....   ....   ....   CFTL   CFSL   CKTI
    CKAM   CFCL   CIOD   CIOF   CIOR   CIRR   CJTR   CSHA
    CSHQ   CSOL   CTSD   CWBG   CWXN   CDBF   CEX2   CFQR
    CFQS   CSFR   CSQC   CDBQ   CRMF   CLSG   CFOR   CJMJ
    CLS1   CLS2   CPIH   CPIL   CPIQ   CRTP   CWXU   CFIR
    CPIS   CISC   CISD   CISE   CISR   CISS   CIST   CJGC
    CJPI   CISB   CEPD   CEPM   CISQ   CISU   CISX   CIS4
    CRLR   CISM   CEPF   CPSS   CJSR   CESL   CISP   CIS1
    CJSL   CRST   CPCT   CFCR   CJLR
RESOURCE=TRANID   PROTECT NAMES:   CEDF   TSEU
COMPLETE
INITPGM=THR    ID=C   TYPE=21
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
CONSOLE
INITPGM=***    ID=CN  TYPE=02
ATTRIBUTES=ACTIVE,NOSHRPRF,NOASUBM,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,EODINIT,DORMPW,NONPWR,
MODE=FAIL  DOWN=BYPASS  LOGGING=ACCESS,INIT,SMF,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
MAXUSER=03000  PRFT=003
DB2PROD
INITPGM=CAD    ID=DB  TYPE=100
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
```

```
UIDACID=8  LOCKTIME=000  DEFACID=*NONE*  KEY=8
DB2TEST
INITPGM=CAD   ID=DT   TYPE=100
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000  DEFACID=*NONE*  KEY=8
ENVIRON
INITPGM=ENV    ID=E   TYPE=15
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL
LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
HSM
INITPGM=ARC    ID=H  TYPE=099
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOABEND,SUAS,NOXDEF
ATTRIBUTES=NOASUBM,MSGLC,NOEODINIT,IJU
ATTRIBUTES=NOLUMSG,NOSTMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC,LCFCMD
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR
MODE=WARN  DOWN=GLOBAL LOGGING=INIT,SMF,MSG,ACCESS,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
IDMSPROD
INITPGM=RHD    ID=M  TYPE=11
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=ACCESS,INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
IDMSTEST
INITPGM=RHD    ID=Q  TYPE=11
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
IMSPROD
INITPGM=DFS    ID=I  TYPE=05
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
```

```
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
IMSTEST
INITPGM=DFS    ID=X  TYPE=05
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
INTERACT
INITPGM=MEN    ID=I  TYPE=14
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=5
JES
INITPGM=HAS    ID=J  TYPE=12
ATTRIBUTES=ACTIVE,NOSHRPRF,NOASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,DORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
OPENMVS
INITPGM=IEFIIC   ID=OE TYPE=093
ATTRIBUTES=IN-USE,ACTIVE,NOSHRPRF,NOASUBM,NOABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,EODINIT,IJU,DORMPW,NONPWR
MODE=WARN  DOWN=GLOBAL  LOGGING=INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE*   KEY=8
NCCF
INITPGM=DSI    ID=N  TYPE=06
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,ABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,NOAUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR,NOEODINIT,IJU
MAXUSER=03000, PRFT=003 LOGGING=INIT,MSG DOWN=GLOBAL
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
ROSCOE
INITPGM=ROS    ID=R  TYPE=07
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,MSG,SEC9
```

```
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
STC
INITPGM=IEESB605    ID=S  TYPE=02
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,NOSTMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
TONE
INITPGM=TON    ID=T  TYPE=13
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,ABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,TSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=ACCESS,INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
TSO
INITPGM=IKJEFLC    ID=T  TYPE=03
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,TSOC,LCFCMD
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
UNICNTR
INITPGM=***    ID=UN  TYPE=104
ATTRIBUTES=IN-USE,NOSHRPRF,NOASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,DORMPW,NONPWR
MODE=WARN  DOWN=GLOBAL  LOGGING=MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
MAXUSER=03000  PRFT=003
VAMSPF
INITPGM=VAM    ID=V  TYPE=09
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,TSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
VM
INITPGM=TSS    ID=V  TYPE=08
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=NOLUMSG,NOSTMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
```

```
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
WYLBUR
INITPGM=UEX    ID=W  TYPE=10
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

User Facilities

In addition to the pre-defined facility entries, there are 222 user facility entries, named USER0 through USER221, available for site customization. Each facility entry has identical attributes with only the ID field unique to each. The following table illustrates this relationship:

Facilities	ID Field
USER0 — USER99	0 through 99
USER100 - USER109	A0 through A9
USER110 - USER119	B0 through B9
USER120 - USER129	C0 through C9
USER130 - USER139	D0 through D9
USER140 - USER149	E0 through E9
USER150 - USER159	F0 through F9
USER160 - USER169	G0 through G9
USER170 - USER179	H0 through H9
USER180 - USER189	I0 through I9
USER190 - USER199	J0 through J9
USER200 - USER209	K0 through K9
USER210 - USER219	L0 through L9
USER220 - USER221	M0 through M1

The ID field is the same as the numeric value of the USERnnn facility. For example, for facility USER0 the id= will be 0, for facility USER23 the id= will be 23, and so on.

```
USERnnn
INITPGM=********  id=xx    TYPE=99
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000  DEFACID=*NONE*    KEY=8
```

FSACCESS—Enable or Disable FSACCESS Resource Class Checks

Valid on z/OS.

Use the FSACCESS control option to enable or disable FSACCESS resource class checks that originate from the SAF component. The FSACCESS IBM z/OS feature added a security check for the FSACCESS resource class to verify user authority to access the file system objects on z/OS UNIX zFS. This support was added by IBM APARS OA35970/OA35974 at z/OS 1.12 and is included at base z/OS 1.13.

With the IBM feature installed, the resource class checks occur by default many times, so disabling the calls can help significantly reduce overhead.

All entry methods are accepted.

This control option has the following format:

```
FSACCESS(ENABLE|DISABLE)
```

ENABLE

Allows USS authorization requests to generate RACROUTE AUTH requests for the FSACCESS class. This value is the default value.

DISABLE

Prevents USS authorization requests from generating RACROUTE AUTH requests for the FSACCESS class.

GOSETGID—SAF Callable Service

Valid on z/OS.

Use the GOSETGID (Group Owner SETGID) control option to alter the way the makeFSP SAF callable service works. When GOSETGID is set and a new directory is created, the new directory inherits the S_ISGID setting from the parent directory. Otherwise, the bit is set to zero.

When a file or directory is created the owning GID of the new file is normally set to the parent directory setting. When GOSETGID is set and the parent's set—gid bit is off, then the owning GID of the new file or directory is set to the effective GID of the process.

This control option has the following format:

```
TSS MODIFY(GOSETGID(ON|OFF))
```

ON

Activated.

OFF

(Default) Deactivated.

HFSACL—HFS File System

Valid on z/OS.

Use the HFSACL control option to use Access Control Lists (ACLs). ACLs provide more control over the HFS file system than native HFS security.

When HFSACL is activated, Access Control Lists (ACLs) are used in the z/OS UNIX security access validation process in addition to the checking of file permission bits and superuser status. When HFSACL is not activated, normal z/OS UNIX security access validation is done, including the checking of file permission bits and superuser status. ACLs are supported in z/OS release 1.3 and above. If HFSSEC is enabled, ACLs are not used regardless of the setting of this field.

This control option has the following format:

```
TSS MODIFY HFSACL(ON|OFF)
```

ON

HFSACL is activated.

OFF

(Default) HFSACL is deactivated.

HFSSEC—HFS Security On or Off

Valid on z/OS.

Use the HFSSEC control option to turn HFS security on or off.

All entry methods are accepted.

This control option has the following format:

```
HFSSEC(ON|OFF)
```

ON

Enables CA SAF HFS security. Normal z/OS UNIX security access validation is bypassed. This includes checking of file permission bits, superuser status, and normal z/OS UNIX security services.

OFF

(Default) Disables CA SAF HFS security. Normal z/OS UNIX security access validation is enabled. This includes checking of file permission bits, superuser status, and normal z/OS UNIX security services.

HPBPW—Expired Password for Batch Job

Valid on z/OS.

Use the HPBPW control option to specify the maximum number of days that CA Top Secret honors an expired or previous password for batch jobs.

All entry methods are accepted.

This control option has the following format:

```
HPBPW(n)
```

n

The number of days that CA Top Secret will honor an expired or previous password associated with a batch job.

Range: 0 to 9

Default: 0

CA Top Secret will check the HPBPW setting if a user submits a job and changes his password prior to the job's initiation.

CA Top Secret will check the HPBPW setting to determine if the job has initiated within the number of days specified. CA Top Secret will honor the user's previous password if the job initiates within the HPBPW setting.

This option is useful if jobs are left on the hold queue for later execution.

HPBPW is not required if using the JES Early Verify feature of z/OS. Since all verification has been performed at submit, there is no check on password validity when the job initiates.

Examples: HPBPW control option

This example indicates that CA Top Secret will honor a batch job's expired or previous password for one day:

```
HPBPW(1)
```

This example deactivates the option:

```
HPBPW(0)
```

IMS—Control IMS Security Processing

Valid on z/OS.

Use the IMS control option to set six different suboptions for IMS security processing. All entry methods are accepted.

When you use the IMS control option, the following requirements apply:

- DBD validation, LCF message logging, and PSB validation are activated at the time of installation or when the region is recycled. If these values are changed, any region requiring the new settings must be recycled.
- You must enter the LU6.1 subpool, Automatic Terminal Signon (ATS) default ACID, ATS logging, and APPL validation suboptions for them to be enabled.

This control option has the following format:

```
IMS([NO] {IMS61SUB} )
    [NO] {IMSATSDF}
    [NO] {IMSATSLG}
    [NO] {IMSDBDVL}
    [NO] {IMSLCFMG}
    [NO] {IMSPSBVL}
```

IMS61SUB

Specifies to use the LU6.1 subpool name for the ATS connection. The NO prefix disables this suboption and uses the LUNAME for the connection.

Default: NOIMS61SUB

IMSATSDF

Specifies to use the DEFACID facility for ATS. The NO prefix disables this suboption.

Default: NOIMSATSDF

IMSATSLG

Specifies that ATS signons are logged. The NO prefix disables this suboption.

Default: NOIMSATSLG

IMSDBDVL

Specifies that DBD validation is performed in IMS. The NO prefix stops DBD validation.

Default: IMSDBDVL

IMSLCFMG

Specifies that IMS transaction warning messages are displayed. The NO prefix disables IMS warning messages.

Default: IMSLCFMG

IMSPSBVL

Specifies that PSB validation occurs in IMS. The NO prefix stops PSB validation.

Default: IMSPSBVL

IMSAPPLL

Specifies that APPL validation occurs in IMS. The NO prefix disables APPL validation.

Default: NOIMSAPPLL

Example: Stop PSB Validation

This example stops PSB validation:

```
TSS MODIFY(IMS(NOIMSPSBVL))
```

Example: Use LU6.1 Subpool Name for the ATS Connection

This example allows the LU6.1 subpool name to be used for the ATS connection:

```
TSS MODIFY(IMS(IMS61SUB))
```

INACTIVE—Deny Use of Unused ACIDs

Valid on z/OS and z/VM.

Use the INACTIVE control option to prohibit the use of ACIDs that are connected to an expired password and have not been used for certain periods of time. You can specify a number of days. If no activity is detected for an ACID within this time period after password expiration, CA Top Secret suspends the ACID (to deny system access to any user or job that uses this ACID).

You can also specify LASTUSED to use additional criteria to determine whether to suspend the ACID.

Note: This control option has no function in a CPF target side. CPF command checking uses the XE23 of the administrator to perform authorizations.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY INACTIVE((0|nnn) [,LASTUSED])
```

0

Deactivates the INACTIVE option. This value is the default value.

nnn

Specifies a number of days, after which the product prohibits signon for an unused ACID that is connected to an expired password. For example, specifying 5 means that five days after the ACID's password expires, CA Top Secret suspends the ACID if no activity is detected for the ACID. Suspending the ACID denies system access to any user or job that uses this ACID.

Range: 1 to 999

LASTUSED

Specifies to suspend the ACID if *both* of the following values are greater than the *nnn* setting:

- Number of days between the last date that an ACID was used and today's date
- Number of days between the last date that the ACID's password was changed and today's date

With this specification in place, CA Top Secret also suspends an ACID that has never signed on for a number of days exceeding the *nnn* setting. For example, if you create ACID BOB on July 5, and INACTIVE(30,LASTUSED) is set, BOB must sign on between July 5 and August 4; otherwise, CA Top Secret suspends the ACID.

Note: If you specify LASTUSED, the *nnn* value must be greater than or equal to the password expiration (PWEXP) and password phase expiration (PPEXP) values.

Example: Deny Access for an Unused ACID

This example denies access to any user or job that attempts to access the system by using an ACID that has not been used for five consecutive days after password expiration:

```
TSS MODIFY INACTIVE(5)
```

To avoid encountering this access denial, change your password before the password expiration date, or change your password within the five-day threshold specified in the INACTIVE control option.

Example: Specify LASTUSED to Require a Combination of ACID-Related Events to Suspend an ACID

This example denies access to any user or job that attempts to access the system with an ACID that meets *both* of the following conditions:

- The ACID has not been used for 30 days after its password expires.
- The ACID has not had its password changed for 30 days after its password expires.

```
TSS MODIFY INACTIVE (30,LASTUSED)
```

Example: Reactivate an Inactive ACID

This example reactivates an inactive ACID by removing SUSPEND from a user and replacing the password (while also specifying the expiration interval or expiration option). The following syntax removes the SUSPEND:

```
TSS REMOVE(acid) SUSPEND
```

Perform *one* of the following actions to replace the password:

- Issue the following command to replace the password and set the password expiration interval to 30 days:

  ```
  TSS REPLACE(acid) PASSWORD(xxx,030)
  ```

  xxx

  Specifies the new password.

- Issue the following command to replace the password, retain the expiration interval, and force the password to expire when the ACID signs on (thus requiring the user to change the password):

  ```
  TSS REPLACE(acid) PASSWORD(xxx,,EXP)
  ```

  xxx

  Specifies the new password.

More information:

PPEXP—Days Before Password Phrase Expires (see page 179)
PWEXP—Password Expiration Interval (see page 188)

INSTDATA—Global Installation Area

Valid on z/OS.

Use the INSTDATA control option to control the value of a 4 byte global installation data area. Data is entered in the control option in a hexadecimal character string as 1 to 4 pairs of hexadecimal nibbles. This data is passed to the CA Top Secret Installation Exit TSSINSTX. The global INSTDATA control option is unrelated to the ACID Installation Data (INSTDATA) keyword, which can be added or removed from individual ACIDS.

All entry methods are accepted.

This control option has the following format:

```
INSTDATA(0|XXXX...)
```

0

(Default) Resets the field to zero.

XXXX

Alters the value to hexadecimal xx, where each xx is 1 to 4 pairs of hexadecimal digits.

IOTRACE—Trace Activity

Valid on z/OS and z/VM.

Use the IOTRACE control option to govern trace activity against the CA Top Secret file, directed to the TSS JESLOG.

Important! Do not use this option unless requested to do so by CA Top Secret Technical Support. When not OFF, this option generates voluminous output and adds overhead to every Security File access.

All entry methods are accepted.

This control option has the following format:

```
IOTRACE{(OFF|ON|SRI)}
```

OFF

(Default) IOTRACE deactivated.

ON

Summary IOTRACE activated.

SRI

Detail IOTRACE activated.

JCT—JES2 JCT Offsets

Valid on z/OS.

Use the JCT control option to establish offsets to fields referenced by CA Top Secret within the JES2 JCT. CA Top Secret has default values for all current levels of JES2, and this control option is intended for use ONLY by those sites that have made modifications to the JCT. Under normal circumstances, when the JCT has not been modified, CA Top Secret should be allowed to dynamically determine the JES level and the offsets to be used.

All entry methods are accepted.

This control option has the following format:

```
JCT [INDEV=nnnn][,ROUTE=nnnn][,NJHDR=nnnn)]
```

The following table lists default offsets within the JCT:

JES2 LEVEL	INDEV	ROUTE	NJHDR
JES2 SP 3.1.3	316	312	1056
JES2 SP 4.1.0	316	312	1056
JES2 SP 4.2.0	320	316	0
JES2 SP 4.3.0	320	316	0
JES2 SP 5.1.0	328	324	0

Note the following:

- All JES2 levels above SP 5.1.0, including all JES2 levels for z/OS, use the same offsets as SP 5.1.0.
- This control option has no effect on CICS JCT resources.

JES—JES Subsystem Information

Valid on z/OS.

Use the JES control option to provide CA Top Secret with JES subsystem information and to indicate whether CA Top Secret needs to provide support for the Early Verify feature.

All entry methods are accepted.

This control option has the following format:

```
JES(SSID=cccc)
JES(TYPE=JES2 | JES3)
JES(LEVEL RELEASE n.n)
JES(VERIFY|NOVERIFY)
```

SSID=cccc

Specifies the name of the primary JES subsystem if it is other than JES2 or JES3. SSID only applies to the primary JES subsystem.

TYPE

TYPE must be entered if SSID is coded, and indicates the type of | primary JES system which is or will be active. TYPE can be abbreviated as 2, for JES2, and as 3, for JES3.

Note: If CA Top Secret is started before JES, both TYPE and LEVEL must be specified. If CA Top Secret is started after JES, CA Top Secret gets the TYPE and LEVEL from JES itself. In this case, we do not recommend entering TYPE and LEVEL.

LEVEL|RELEASE|VERSION=xx r.ss.tt

Indicates the level of JES operating in your system. Because this operand is specified with spaces, a command to modify the JES version must be enclosed in single quotes. An operator command or parameter file entry must *not* use single quotes.

Note: If CA Top Secret is started before JES, both TYPE and LEVEL must be specified. If CA Top Secret is started after JES, CA Top Secret gets the TYPE and LEVEL from JES itself. In this case, we do not recommend entering TYPE and LEVEL.

xx=SP|OS|z/OS

Specifies the operating system.

r.ss.tt

Specifies the JES release number. This number may not correspond with the operating system. 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 JES2 message:

```
$HASP426 SPECIFY OPTIONS – JES2 xx r.ss.tt
```

Limits: This operand can be a maximum of 8 characters. If you are running z/OS 1.10 and higher, do not include a space in the LEVEL= operand.

Examples

These examples show only eight characters used:

```
LEVEL=z/OS1.10
```

```
LEVEL=z/OS1.11
```

This example shows a TSS command with single quotes:

```
TSS MODIFY('JES(SSID=JES2,TYPE=2,RELEASE=OS 2.8)')
```

This example shows an operator command without single quotes:

```
F TSS,JES(SSID=JES2,TYPE=2,RELEASE=OS 2.8)
```

This example shows a parameter file entry without single quotes:

```
JES(SSID=JES2,TYPE=2,RELEASE=OS 2.8)
```

VERIFY

(Default) Indicates CA Top Secret verifies USER and PASSWORD parameters implicitly without inserting these parameters into the JOB JCL statement. This is the default for JES2 and JES3. If a USER is present in the JOB statement, then the USER is checked to see that the submitter is cross-authorized. If submission is allowed, no password processing will take place unless the password is explicitly coded. For information, see the *Implementation: Other Interfaces Guide*.

NOVERIFY

Indicates CA Top Secret will insert USER and PASSWORD information explicitly into the JOB JCL processing if it is not already present. We recommend that you do not include explicit USER and PASSWORD information, as this can be intercepted from spool.

The JES control option is required if the CA Top Secret main task is started before JES completes initialization. In this case, the control option indicates JES subsystem and release level, as well as whether the JES Early Verify feature is desired.

When JES is initialized before starting the CA Top Secret main task, the release and subsystem information is available to CA Top Secret, and need not be explicitly specified. CA Top Secret locates the first subsystem with type JES and interprets the information provided there.

Note: If the JES2 control option is supplied incorrectly by the user, the following message can be released during job submission:

```
TSS9401E TSS CONTROL OPTION 'JCT'IS INCORRECTLY SET
```

It is actually unlikely that the JCT control option is set incorrectly. Unless your site makes modifications to JES control blocks, the JCT option should be allowed to default.

Before attempting to adjust the JCT option, assure that the JES RELEASE has been correctly specified.

JESNODE—JES Local Node Name

Valid on z/OS.

Use the JESNODE control option to indicate the name by which JES2 knows the local node. This allows jobs and SYSOUT where the submitting node is the local node to be treated differently from NJE jobs and SYSOUT originating from other nodes.

This control option has the following format:

JESNODE(*nodename*)

nodename

Indicates the name of the local JES2 node.

If JESNODE was changed using a TSS MODIFY command, the changes made remain in effect even if CA Top Secret is restarted. Most control options revert to their default settings, the exceptions are DUFPGM, JESNODE, and NJEUSR.

JOBACID

Valid on z/OS.

JOBACID identifies the field on every batch job card from which the ACID is derived when the source of the submission cannot be identified and if no USER= field is present on the job card.

If a value for the USER= parameter is coded on the jobcard, this value will override any JOBACID option unless the USER= acid is undefined.

This control option uses all entry methods.

This control option has the following format:

JOBACID(*field*,*position* [,*Start*])

The following tables details operands to use with the JOBACID control option:

Field Prefix	Field Name	Operand	Position Name and Meaning
A	Accounting	Digit from 1-8	Parameter within the field becomes the ACID, optionally starting in the nth position within that field.
U	Undefined	Digit from 1-7	Disable JOBACID processing. Both numeric values are ignored. No JOBACID default is derived, but other default processing such as DEFACID in the batch facility or the UNDEFIND entry point of TSSINSTX will still be used.
J	Job Name	Digit from 1-8	First *n* characters become the ACID.
R	Reader Name	Digit from 1-8	First n characters become the ACID.

All batch jobs must be identified with an ACID and password in the FAIL mode, unless default ACIDS are assigned. The security administrator can use the JOBACID control option to indicate which field on the JOB card should be used as the ACID.

The default is:

```
JOBACID(A,1)
```

It indicates that the first parameter of the Accounting field should be used as the ACID:

```
//EXAMPLEA  JOB (ADMIN,ADM100)
```

The ADMIN parameter is used as the ACID.

Sub-accounting

For installations that use sub-accounting, CA Top Secret will treat the slash '/' and dash '-'as delimiters of an accounting number that is used as an ACID.

Examples: JOBACID control option

When JOBACID(A,1) is used, the ACID is ADM200 in the following account specifications:

```
ADM200-SMYTHE
```

```
ADM200/JUN82
```

This example sets USER=CST:

```
//EXAMPLEB JOB 123,'CST-5NG'
```

In this example JOBACID(J,5) indicates that the first five characters of the job name are used as the USER=ACTRC:

```
//ACTRCV7 JOB 12B,'SMITH,ACTRCV7'
```

Note: USER is restricted to a maximum of seven characters by z/OS and JCL rules.

KERBLVL—Highest Kerberos Encryption Level Available

Valid on z/OS 1.8 and below.

Use the KERBLVL control option to specify the highest available encryption level available for Kerberos certificates. This varies according to the level of z/OS and the Kerberos configuration file parameters at your site. KERBLVL is is valid on z/OS 1.8 and below only. For z/OS 1.9 and above, all encryption types are supported.

For information, see the *IBM Secure Way Network Authentication* Service *Administration Guide*.

All entry methods are accepted.

This control option has the following format:

```
KERBLVL(0|1)
```

0

(Default) Indicates that only DES encryption is available.

1

Indicates that DES, DES3, DESD, AES128, and AES256 encryption are available.

Example: KERBLVL control option

This example indicates that both 24 bit encryption (DES) and extended encryption are available for REALM definition and Kerberos principal definition:

```
TSS MODIFY(KERBLVL(1))
```

LDAPNODE—LDAP Node

Valid on z/OS.

Use the LDAPNODE control option to modify the LDAP node status and trace option.

The LDAP node initial ACTIVE and TRACE options, are established based on the NDT LDAPNODE attributes when the LDS server is activated. The LDAPNODE control option allows for dynamically modifying these options without recycling the LDS server.

The ACTIVE option controls whether commands are propagated to the remote LDAP server. Setting ACTIVE(NO) will close an active connection, and eligible commands will be stored in the LDS recovery file for later propagation. Setting ACTIVE(YES) enables command propagation to the remote LDAP server, and any commands queued in the LDS recovery file, will be transmitted as soon as the connection to the remote server is established.

This control option uses the O/S and TSS MODIFY commands entry methods.

This control option has the following format:

```
LDAPNODE(nodename,[ACTIVE(Yes|No)]
                  ,[TRACE(On|Off)]
                  ,[RECOVERY(Yes|No)]
```

Active(Yes|No)

Specify the status of the LDAP node.

Trace(On|Off)

Enable/Disable node level tracing.

Recovery(Yes|No)

Enable/Disable node level recovery option.

Example: LDAPNODE control option

This example uses the LDAPNODE control option to dynamically enable a CA Top Secret system:

```
F TSS,LDAPNODE(nodename,ACTIVE(YES),TRACE(YES))
```

LDS—LDAP Outbound Processing

Valid on z/OS.

Use the LDS control option to enable LDAP outward data sync processing for the TSS region.

LDAP nodes are defined to the TSS database through NDT table entries. Each node entry controls what update events are sent to the LDAP server, and how ACID fields are mapped to LDAP directory attribute fields.

The LDS control option enabled/disables processing in a TSS region. On the ACID level, the LDS command adds or removes the LDS attribute to or from an ACID record, the LDAPNODE command defines LDAP nodes to the TSS database as NDT node elements, and the LDAPDEST command adds, removes, or replaces nodes to the LDAP node list of an ACID record. For information, see the *Command Functions Guide*.

All entry methods are accepted.

This control option has the following format:

```
LDS(ON|OFF)
```

ON

Enable LDAP outbound processing for the TSS region.

OFF

(Default) Disable LDAP outbound processing for the TSS region.

Examples: LDS control option

The LDS control option indicates that the LDAP Directory Synchronization can be utilized in the current execution of CA Top Secret.

This example indicates that LDS can be dynamically enabled in a CA Top Secret system with the following operator command to start LDAP Directory Synchronization:

```
F TSS,LDS(ON)
```

This example uses an operator command to stop LDAP Directory Synchronization:

```
F TSS,LDS(OFF)
```

LDSRETRY—LDS Server Retry Count

Valid on z/OS.

Use the LDSRETRY control option to set the retry count for the LDS server.

The LDS server task propagates eligible TSS commands to remote LDAP directories defined through NDT LDAPNODE records. The LDS server sends each command to the remote directory and waits for acknowledgment before sending out the next command. The LDSRETRY count controls the number of times a failed send operation will be retried, before the LDAPNODE is deactivated and further send operations are stopped.

All entry methods are accepted.

This control option has the following format:

```
LDSRETRY(nnn)
```

nnn

Specifies the number of times the LDS server task will retry a failed send operation to the remote LDAP directory, before deactivating the LDAP node.

Default: 3

Example: LDSRETRY control option

This example uses the LDSRETRY control option to dynamically enable a CA Top Secret system:

```
F TSS,LDSRETRY(nnn)
```

LDSTIMEOUT—LDS Server Timeout

Valid on z/OS.

Use the LDSTIMEOUT control option to set timeout interval value for the LDS server.

The LDS server task propagates eligible TSS commands to remote LDAP directories defined through NDT LDAPNODE records. The LDS server sends each command to the remote directory and waits for acknowledgment before sending out the next command. The LDSTIMEOUT interval controls the amount of time the LDS server will wait to receive an acknowledgment from the remote directory before issuing an error message and scheduling a retry attempt of the failed send operation.

All entry methods are accepted.

This control option has the following format:

```
LDSTIMEOUT(nnn)
```

nnn

Specifies the time interval in seconds at which the LDS server task will stop waiting for a response from the remote LDAP directory and schedule a retry attempt for the stalled send operation.

Default: 5

Example: LDSTIMEOUT control option

This example dynamically enables the LDSTIMEOUT control option in a CA Top Secret system:

```
F TSS,LDSTIMEOUT(nnn)
```

LDSTRACE—Control LDS Tracing

Valid on z/OS.

Use LDSTRACE to control tracing of LDS outbound processing.

The LDS trace records are written to the SYSOUT data set and provide diagnostics information useful for debugging LDS server problems.

All entry methods are accepted.

This control option has the following format:

```
LDSTRACE(ON|OFF)
```

ON

Enables LDS tracing.

OFF

(Default) Disables LDS tracing.

Example: LDSTRACE control option

This example dynamically enables the LDSTRACE control option in a CA Top Secret system:

```
F TSS,LDSTRACE(ON)
```

LMPCHECK—Verify LMP Key

Valid on z/OS and z/VM.

Use the LMPCHECK control option to verify that the correct License Management Program (LMP) encryption key is being used for this system.

Under normal processing, if a valid LMP key has not been found, CA Top Secret issues a warning message every 30 seconds until LMP verifies a valid key. For information, see the CA Common Services for z/OS documentation.

This control option uses the O/S Start command and O/S Modify commands entry methods.

This control option has the following format:

```
LMPCHECK
```

LOG—Control Event Logging

Valid on z/OS and z/VM.

Use the LOG control option to perform the following activities:

- Identify the types of events that CA Top Secret logs.
- Specify whether events are logged onto the ATF (Audit Tracking File) and SMF (System Management Facility) files.
- Specify whether to display violation messages.

The LOG option affects all facilities. A global LOG command can be overridden by a LOG operand that you enter as a suboption for a specific facility.

All entry methods are accepted.

This control option has the following format:

```
LOG(ACTIVITY,ACCESS,SMF,SEC9,INIT,MSG)|(NONE)|(ALL)
```

ACTIVITY

Logs all activity for all facilities. This specification is the same as the following specification:

```
LOG(ACCESS,INIT)
```

SMF

Writes events to the SMF file in addition to the ATF.

ACCESS

Logs all resource access, except for the following access:

- DBD
- FCT
- JCT
- LCF
- OTRAN
- PPT
- PROGRAM
- PSB

SEC9

Routes the following violation summary messages to the security console through route code 9:

- TSS7100E
- TSS7220E
- TSS7200E
- TSS7250E

INIT

Logs all job/session initiations and terminations.

MSG

Displays violation messages for batch jobs, started tasks, or at the online user's terminal.

For users in FAIL mode, violation messages always appear, regardless of the MSG setting. Password violations also appear.

ALL

Selects all log options for all facilities.

NONE

Deactivates all SMF and ATF logging, except for violations and audited events, which continue being written to the ATF.

If the user facility is in DORMANT mode, no logging takes place unless the permitted resource is specified with ACTION(FAIL).

The default is LOG(SMF, INIT, SEC9, MSG).

More information:

FACILITY—System Facility Processing (see page 80)

Type 80 Format

CA Top Secret uses SMF type 80 format records. A DSECT (Dummy Control Section) for these records is documented in the installation exit (TSSINSTX) source code.

LOG(ACCESS), LOG(ACTIVITY), and LOG(ALL) are primarily diagnostic tools for Technical Support people. Because each option produces a large number of records, dumping such a large volume of records on the Audit/Tracking File, might cause excessive wrapping of the File, which, in turn, means you need a larger File. In short, limit your use of these three options.

Important! A LOG option issued after the startup of CA Top Secret resets not only the global LOG options, but also the LOG setting of every facility.

Protection of Option

The LOG option is protected by the operator accountability feature. CA Top Secret will prompt the person entering the command for the proper ACID/password combination before processing the LOG option. CA Top Secret will also create an audit trail identifying the ACID under which the LOG specification was made.

Recording Violations

If the AUDIT DD-statement is entered into the CA Top Secret started task procedure, then the recording of violations into the ATF will always occur. Violations are always written to available files. Violation recording cannot be prevented (in all modes except DORMANT), even if LOG(NONE) is entered. See DRC and MSG for instructions on how to tailor and/or suppress violation messages.

Use of Report Utilities

An important prerequisite to the reporting and tracking of security events is the correct specification of log options. TSSUTIL and TSSTRACK can be used to build reports, but only based on data that is stored in the SMF and ATF. For information, see the *Report and Tracking Guide*.

LUUPDONCE—Force Statistics Update

Valid on z/OS.

Use the LUUPDONCE control option to enforce the update of the last-used statistics within the user's security file record once a day following their first successful logon. Subsequent update attempts during the same day are bypassed. This option overrides any FACILITY specific setting of the LUUPD or NOLUUPD sub-options.

This option reduces security file I/O and improves system performance by only updating last-used statistics once a day for most successful logons. Automatic Terminal Signon (ATS) and preset terminal security normally do not update last-used statistics. Last-used statistics can be activated for these logons using OPTIONS(30) at TSS startup.

All entry methods are accepted.

This control option has the following format:

```
LUUPDONCE(YES|NO)
```

YES

(Default) All users have their last-used statistics updated once a day following their first successful logon.

NO

The update of the last-used statistics is controlled by the FACILITY control sub-options LUUPD and NOLUUPD.

Example: LLUPDONCE

This example enforces last-used statistics updating once a day:

```
F  TSS,LUUPDONCE(YES)
```

MATCHLIM—Set Audit Match Limit

Valid on z/OS

Use the MATCHLIM control option to specify a global value for the number of loggings that will be done because of an audit request. Only audit requests that have MATCHLIM specified are affected by this control option value.

For more information about the MATCHLIM keyword, see the Command Functions Guide.

All entry methods are accepted.

This control option has the following format:

MATCHLIM (n*nnnn*|CLEAR)

n*nnnn*

Sets the maximum number of loggings that can occur before auditing is discontinued for a specific resource or user. The default value is zero which indicates that match limit processing is not active and no loggings are suppressed.

Limits: 0 – 65535

Default: 0

CLEAR

Clears out all logging counts for resources and users that are being audited with MATCHLIM specified. Audit Match Limit processing continues using the existing maximum value.

MAXKEYSIZE—Maximum Digital Private Key Size

Valid on z/OS.

Use MAXKEYSIZE to control the maximum private key size for digital certificates added to the security file.

All entry methods are accepted.

This control option has the following format:

```
MAXKEYSIZE(2048|4096)
```

2048

(Default) Allows private key sizes between 512 and 2048.

4096

Allows private key sizes between 512 and 4096.

Example: MAXKEYSIZE control option

This example dynamically changes the maximum allowed private key size to 4096:

```
F TSS,MAXKEYSIZE(4096)
```

MIRROR—Maintain a Mirror Copy of the Security File

Valid on z/OS.

Use the MIRROR control option to specify whether the product maintains a mirror copy of the primary security file. Having a mirror file available allows greater flexibility for when to schedule backup processing (for example, less frequently). Additionally, the mirror file is an exact duplicate of the primary security file and provides up-to-the-minute data in the event of a sudden problem with the primary file.

This control option uses the parameter file entry method.

This control option has the following format:

```
MIRROR(ON|OFF)
```

ON

Maintains a mirror copy of the security file. The ON specification must be included in the CA Top Secret parameter file, where it takes effect at the next product startup.

OFF

Does *not* maintain a mirror copy of the security file. This value is the default value.

MLACTIVE—Multilevel Security Checking

Valid on z/OS.

MLACTIVE is used to specify whether Multilevel Security checking is performed.

All entry methods are accepted.

This control option has the following format:

```
MLACTIVE(YES|NO)
```

YES

Activates MLS security.

NO

(Default) Deactivates MLS security.

Example: MLACTIVE control option

This example activates MLS security:

```
F TSS,MLACTIVE(YES)
```

MLFSOBJ—UNIX Labels

Valid on z/OS.

Use the MLFSOBJ control option to specify whether UNIX files and directories are required to have security labels.

All entry methods are accepted.

This control option has the following format:

```
MLFSOBJ(YES|NO)
```

YES

Indicates that UNIX files and directories must have security labels.

NO

(Default) Security labels are not required for UNIX files and directories.

Example: MLFSOBJ control option

This example makes security labels required for UNIX files/directories:

```
F TSS,MLFSOBJ(YES)
```

MLIPCOBJ—UNIX IPC Labels

Valid on z/OS.

Use the MLIPCOBJ control option to specify whether UNIX IPC objects are required to have security labels.

All entry methods are accepted.

This control option has the following format:

MLIPCOBJ(YES|NO)

YES

UNIX IPC objects must have security labels.

NO

(Default) Security labels are not required for UNIX IPC objects.

Example: MLIPCOBJ control option

This example specifies that security labels are required for UNIX IPC objects:

```
F TSS,MLIPCOBJ(YES)
```

MLMODE—Multilevel Security Mode

Valid on z/OS.

Use the MLMODE control option to select the security mode in which Multilevel Security checking is performed.

The MLS mode operates independently of the CA Top Secret DAC security mode that is set with the MODE control option.

All entry methods are accepted.

This control option has the following format:

```
MLMODE(DORMANT|WARN|FAIL)
```

DORMANT

(Default) CA Top Secret performs security label validation at signon for all users that have a seclabel in their security record. Security labels are validated at system entry only. Violations are logged. No messages are returned to the console or the user.

WARN

CA Top Secret performs security label validation for all access attempts for resources that have a security label assigned to them.

Users guilty of security label violations receive a message indicating that they have violated security, but are not denied access to the resource unless DAC validation fails the request.

Permits MLS accesses to classified data sets and resources that normally would violate MLS validation rules and sends a warning message to the user (or system log). Violations are logged.

FAIL

CA Top Secret denies all unauthorized access attempts due to security label validation violations. It prevents MLS accesses to classified data sets and resources based on MLS validation rules and sends an error message to the user (or system log). Violations are logged.

Example: MLMODE control option

This example sets WARN mode for MLS security:

```
F TSS,MLMODE(WARN)
```

MLNAME—Name Display

Valid on z/OS.

Use the MLNAME control option to restrict the display of names of datasets, and UNIX files and directories to only those for which the user is authorized to read. This is known as name hiding. Name hiding can be activated when MLS security is not active, for example, when MLACTIVE(NO) is specified.

All entry methods are accepted.

```
MLNAME(YES|NO)
```

YES

Restrict the display of the names of datasets and UNIX files and directories.

NO

(Default) The display of names of datasets and UNIX files and directories is not restricted.

Example: MLNAME control option

This example activates name hiding:

```
F TSS,MLNAME(YES)
```

MLSECAUD—Multilevel Seclabel Auditing

Valid on z/OS.

Use the MLSECAUD control option to specify whether Multilevel Seclabel Auditing is performed.

This control option has the following format:

```
MLSECAUD(YES|NO)
```

All entry methods are accepted.

YES

Activates MLS Seclabel Auditing.

NO

(Default) Deactivates MLS Seclabel Auditing.

Example: MLSECAUD control option

This example activates MLS Seclabel Auditing:

```
F TSS,MLSECAUD(YES)
```

MLSLBLRQ—Security Labels in Multilevel Environment

Valid on z/OS and z/VM.

Use the MLSLBLRQ control option to specify if security labels are required for all users, datasets, and resources in an MLS environment.

The MLSLBLRQ option requires security labels for most resources except those resources related to UNIX. For information on the resource classes that require a security label when MLSLBLRQ is active, see the IBM *z/OS Planning for Multilevel Security and the Common Criteria Guide*.

This control option has the following format:

```
TSS MODIFY MLSLBLRQ(YES|NO)
```

YES

Activates MLSLBLRQ. MLACTIVE(YES) must be specified if this option is specified.

NO

(Default) Disables MLSLBRQ.

If MLACTIVE(NO) is specified, MLSLBLRQ(NO) is automatically set.

All entry methods are accepted.

MLWRITE—Data Write

Valid on z/OS.

Use the MLWRITE control option to allow or prevent the write down of data.

All entry methods are accepted.

```
MLWRITE(YES|NO)
```

YES

(Default) Allows the write down of data.

NO

Prevents the write down of data.

Example: MLWRITE control option

This example prevents the write down of data:

```
F TSS,MLWRITE(NO)
```

MODE—Security Mode

Valid on z/OS and z/VM.

Use the MODE control option to select the security mode in which CA Top Secret will operate for all facilities.

The MODE option is used to set a global mode. Modes can be assigned to a specific subsystem facility, permitted to a specific ACID, or assigned by the ACTION keyword on a permission. The order of the search for MODE is:

- ACTION on a permission
- Subsystem facility (DB2FAC)
- User mode permission
- Facility
- Global

More information on how to assign

- A MODE to a facility, see the FACILITY control option
- A facility to a DB2 subsystem, see the DB2FAC control option
- A mode for a specific resource permission, see the ACTION keyword

All entry methods are accepted.

This control option has the following format:

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

DORMANT

CA Top Secret will not perform security validation for normal users (everyone except security administrators). Normal users will enter their current signon and password, not a CA Top Secret password.

CA Top Secret will always perform password validation for Security Control ACIDs (security administrators). Security administrators who sign on with their security control ACID, is prompted for their CA Top Secret password. CA Top Secret will also always perform password validation for those users whose UADS data fields are being managed by CA Top Secret.

Exceptions can be specified via the DRC control option, or via the TSS PERMIT ACTION(FAIL) command.

WARN

CA Top Secret will perform security validations for all access attempts. Users who are guilty of security violations will receive a message indicating that they have violated security, but is not denied access to the resource unless exceptions have been specified.

All specified LOG options are in effect.

Exceptions can be specified via the DRC control option, or via the TSS PERMIT ACTION(FAIL) command.

IMPL

This mode is referred to as a gradual implementation mode since it will fully protect defined resources, and monitor all access requests made by defined users. Defined resources are protected and violations result in denied access. This mode will, however, allow undefined users uninhibited access to undefined resources. Thus, security can be gradually applied to selected users and resources with little or no impact.

FAIL

(Default) CA Top Secret will deny all unauthorized facility or resource access unconditionally. All users must be defined.

The MODE option is protected by the operator accountability feature. CA Top Secret prompts you for the proper ACID/password combination before processing the MODE option. CA Top Secret also creates an audit trail that identifies the ACID under which the MODE was specified.

Important! A MODE option issued after the startup of CA Top Secret resets not only the global MODE, but also resets the MODE of every facility.

MODLUSER—Identify an OMVS Model User

Valid on z/OS.

Use the MODLUSER control option to specify the ACID that contains a model for a default OMVS segment. If the UNIQUSER control option is ON, any signed-on session ACID that accesses OMVS services without an OMVS segment receives the segment from the designated MODLUSER ACID and receives an automatically generated UID.

If the session ACID has no DFLTGRP, the MODLUSER DFLTGRP is also copied. If the DFLTGRP GROUP assigned to the session ACID has not been assigned a GID, an automatic GID is assigned to the GROUP.

This control option has the following format:

```
MODLUSER(acid)
```

acid

Specifies the ACID that contains a model of the OMVS segment. The ACID can be given the fields UID, HOME, OMVSPGM, OECPUTM, PROCUSER, ASSIZE, THREADS, MMAPAREA, MEMLIMIT, SHMEMMAX, and DFLTGRP. DFLTGRP will be copied if the OMVS user does not already have a DFLTGRP assigned.

We recommend DFLTGRP, HOME, and OMVSPGM for the MODLUSER ACID (to guarantee a valid entry to OMVS service environment). OECPUTM, PROCUSER, ASSIZE, THREADS, MMAPAREA, MEMLIMIT, and SHMEMMAX provide override values for identically named variables in the z/OS PARMLIB member BPXPRMxx; copying these values to session ACIDs overrides changes to your system PARMLIB and might require additional maintenance.

Note: For HOME, you can specify a variable that is replaced by the current user ID value when MODLUSER information is added to a user’s ACID record. Specifying &ACID (or a mixed-case entry) translates to an uppercase user ID value; specifying &acid translates to a lowercase user ID value. For complete information about the HOME keyword, see the *CA Top Secret Command Functions Guide*.

Example: Identify an OMVS Model User

This example specifies that the ACID JDOE contains a model of the OMVS segment:

```
F TSS,MODLUSER(JDOE)
```

More information:

UNIQUSER—Assign a UID Automatically During OMVS Logon (see page 236)

MSG—Messages

Valid on z/OS and z/VM.

Use the MSG control option to modify the characteristics of certain CA Top Secret violation messages that are contained in the CA Top Secret Message Table. You can alter the characteristics of the message, such as when and how the message is issued or suppressed, but not the text of the message.

MSG control option considerations:

- MSG modifications can be made to CA Top Secret messages in the range of 7000 to 7999.
- Additional message editing can be performed in the installation exit via the MESSAGE EDIT call. For information, see the *User Guide*.
- Suppressions are in effect only if all suppress conditions are valid, for example, “AND” logic is used.

All entry methods are accepted.

This control option has the following format:

```
MSG(nnnn,option,option,...)
MSG(nnnn)
```

nnnn

The four-digit CA Top Secret message number that corresponds to the message being listed or modified.

SEC9

Indicates that the message is a violation summary that is sent to the security console by using WTO route code 9.

NOSEC9

Cancels the SEC9 suboption.

USER

Indicates that the message is directed to the user.

NOUSER

Cancels the USER suboption.

FORCE

Message must always be issued, even if the LOG option does not include the MSG suboption.

NOFORCE

Cancels the FORCE suboption.

DSNAME

Message is associated with data set name indicator message TSS7230I.

NODSN

Cancels the DSNAME suboption.

SWARN

Suppress message display if user is in WARN mode.

NOSWARN

Cancels the SWARN suboption.

SIMPL

Suppress the message display if user is in the IMPL mode.

NOSIMPL

Cancels the SIMPL suboption.

SDEF

Suppress the message display for defined users.

NOSDEF

Cancels the SDEF suboption.

SUNDEF

Suppress the message display for undefined users.

NOSUNDEF

Cancels the SUNDEF suboption.

SBATCH

Suppress message display if user is using BATCH processing.

NOSBATCH

Cancels the SBATCH suboption.

STSO

Suppress the message display if user is on TSO.

NOSTSO

Cancels the STSO suboption.

SONLINE

Suppress the message display for online users (CICS, IMS, and so on).

NOSONLINE

Cancels the SONLINE suboption.

SUPPRESS

Suppress the message display at all times for all users.

NOSUPPRESS

Cancels the SUPPRESS suboption.

Examples: MSG control option

This example displays the characteristics of a specific MSG or MSGs:

```
F TSS,MSG(nnnn)
```

This example indicates that message TSS7205 is suppressed for undefined batch jobs in the IMPL mode only:

```
F TSS,MSG(7205,SBATCH,SUNDEF,SIMPL)
```

This example determines the characteristics of message TSS7003W:

```
F TSS,MSG(7003)
```

This example goes in the Parameter File:

```
*
* CONTROL OPTIONS
*
MODE(WARN)
MSG(7003,SBATCH,SUNDEF,SIMPL)
```

MSUSPEND—MSCA ACID Protection

Valid on z/OS and z/VM.

Use the MSUSPEND control option to allow the MSCA's ACID to be suspended automatically if the password violation threshold set via the PTHRESH option is exceeded. This prevents a user from making an unlimited number of guess attempts to determine the MSCA's password.

This option is ignored for BATCH or STC use.

All entry methods are accepted.

This control option has the following format:

```
MSUSPEND(YES|NO)
```

YES

MSCA's ACID is suspended if the password violation threshold is exceeded.

NO

(Default) Cancels the MSUSPEND option.

If a suspended MSCA signs on and enters the password correctly, CA Top Secret prompts the master console via message:

TSS7186I SUSPENDED CONTROL SECURITY ADMINISTRATOR ATTEMPTING SIGNON

TSS7187A SPECIFY <Y> TO CONFIRM SIGNON, <N> TO DENY USE OF MSCA ACID

Examples: MSUSPEND control option

This example protects the MSCA's password from password-guessing attempts:

```
F TSS,MSUSPEND(YES)
```

NEWPHRASE—Password Phrase Rules

Valid on z/OS and z/VM.

Use the NEWPHRASE control option to specify the controls for password phrases.

Important! The alpha count minimum (MA), digit count minimum (MN), and special character count minimum (SC) must not exceed the total phrase character maximum (MAX). This constraint is evaluated sequentially from left to right each time you change any of these variables.

Note: You can enter all values in any order.

This control option has the following format:

```
TSS MODIFY NEWPHRASE([MA=nn],[MN=nn],[ID],[MAX=nnn],[MIN=nn],
                     [MINDAYS=nn],[NR=nn],[NU],[SC=nn],[WARN=nn])
```

MA=nn

Specifies the minimum number of alpha characters.

Range: 0 to 32

Default: 0

MN=

Specifies the minimum number of numeric characters.

Range: 0 to 32

Default: 0

ID

Prevents users from specifying a new password phrase that contains their ACID name.

MAX=nnn

Specifies the maximum length of a password phrase.

Range: 9 to 100

Default: 100

MIN=nn

Specifies the minimum length of a password phrase.

Range: 9 to 32

Default: 9

MINDAYS=

Specifies the number of days after a password phrase is changed before the user can change the password phrase again.

Range: 0 to 99

Default: 0

NR=

Specifies the number of pairs of repeating characters in a new password phrase.

Range: 0 to 5

Default: 0

NU

Specifies that an ACID TYPE(USER) cannot change their own password phrase.

SC=nn

Specifies the minimum number of characters that the new password phrase must have from the PPSCHAR list. If no PPSCHAR set is available, no action is taken.

Range: 0 to 32

Default: 0

WARN=nn

Specifies the warning days given that a password or ACID is about to expire.

Range: 0 to 99

Default: 3

NEWPW—Restrict Password Alterations

Valid on z/OS and z/VM.

Use the NEWPW control option to set restrictions on creating a new password. The restrictions apply to the following users:

- Any user who enters a new password through an application
- Any non-administrator who enters a new password through a TSS command

NEWPW restrictions do not apply when an administrative ACID enters a new password with the TSS command. If no NEWPW control option is set in the parameter file when CA Top Secret starts, the NEWPW control option defaults to the following settings:

```
NEWPW(MIN=04,MAX=008,WARN=03,MINDAYS=01,NR=0,ID,TS,RS)
```

The option has the following format:

```
TSS MODIFY NEWPW ([FA],[FN],[ID],[MASK=mask],[MC],[MAX=n],[MIN=n],
                     [MINDAYS=nn],[NM],[NO],[NR=n],[NU],[NV],[RN],[RS],[RT],[SC],
                     [SW],[TS],[LC],[UC],[WARN=nn])
```

By default, passwords can contain the following components:

- Alphabetic uppercase characters (A-Z)
- Numeric digits (0-9)
- National characters ($#@{})

Use the following options to construct your site's local password standards:

Important! If you change one of the options, you must also respecify other active options (except MIN, MAX, WARN, and MINDAYS), even if the options are not being changed; otherwise, the product deactivates the options.

FA

Forces specification of at least one alphabetic character in a new password. When MC is also set, lowercase and uppercase alphabetic characters can be used.

FN

Forces specification of at least one numeric character in a new password.

ID

Prevents a user from specifying a new password that:

- Contains the user's ACID
- Starts with four characters that are equal to any word of the ACID NAME attribute

For example, a user with a USERNAME field value of "Percy Snorthammer" is prohibited from entering new passwords like SNORT or PERC56 (Percy's ACID). When MC is also set, SnoRT and pERc56 are prohibited.

MASK=*mask*

Allows the security administrator to create a mask to dictate the type of character that is accepted for each position in a password. CA Top Secret applies this mask to user-initiated and randomly generated password changes. The following character types are used in the mask:

- a—Any alphabetic character
- c—Consonant
- v—Vowel (A,E, I, O, U, and Y)
- n—Numeric character (0–9)
- x—Non-vowel (National character (@,#,$), or alphabetic including Y but excluding other vowels)
- ?—Any character

An entry of MASK=vnvn could generate password A5I6.

If more than one of the options MASK, NM, and NV are specified, the mask takes the value of the rightmost option.

When MC is also set, the alphabetic mask characters a, c, v, and x are satisfied by an uppercase or lowercase letter. For example, "a" and "A" are considered vowels.

MAX=*n*

Specifies the maximum password length.

Note: This entry can be set only when the security file has been copied by TSSXTEND with the option NEWPWBLOCK.

Minimum: Set by the MIN=*n* option

Maximum: 8 bytes

Default: 8 (If NEWPW is specified again and MAX is omitted, the previous value of MAX is preserved.)

MIN=*n*

Selects the minimum length of a password or the mask used to generate random passwords.

Range: 1 to 8

Default: 4 (If NEWPW is specified again and MIN is omitted, the previous value of MIN is preserved.)

MC

Indicates that passwords are processed in mixed-case format. This entry can be set only when the security file has been copied by TSSXTEND with the option NEWPWBLOCK. z/OS 1.7 or higher is required to use mixed-case passwords during system entry validation.

Note: Applications that do not support mixed-case passwords convert the password to uppercase, which can cause a password verification failure. If an application does not support mixed-case passwords, use the MULTIPW attribute of the FACILITY control option to allow a different password to be specified for that facility. Any passwords for that facility must be specified in uppercase. For more information about using the MULTIPW keyword, see the *CA Top Secret Command Functions Guide.*

MINDAYS=*nn*

Sets the number of days after a password has been changed that users cannot change their password again. To have no limitation on how frequently a password can be changed, specify MINDAYS=00.

Range: 00 through 99

Default: 01 (If NEWPW is respecified and MINDAYS is omitted, the previous value of MINDAYS is preserved.)

Note: MINDAYS is applicable only for user ACIDs and does not apply when administrative ACIDs change their password at signon. MINDAYS is *not* applicable to users who have a non-expiring password.

NM

Indicates that a new password can contain only numbers. NM is the equivalent of MASK=NNNNNNNN. If MASK, NM, or NV is specified in NEWPW, only the rightmost option is in effect.

NO

Indicates that only the MIN= and MINDAYS= suboptions apply to new passwords. WARN= remains in effect.

NR=*n*

Specifies the number of pairs of repeating characters allowed in a new password. NR or NR=0 indicates that no characters can be repeated.

When MC is also set, an alphabetic character (in uppercase or lowercase) is considered a repetition. For example, rABbiT contains a repetition of “B” despite the change in case.

Default: If NR is specified without =*n*, the default is NR=0. Omitting NR triggers a default NR value that matches the setting for MAX. For example, if you specify MAX=8 but omit NR, the product generates a default setting of NR=8, which allows eight pairs of repeating characters in a new password.

NU

Prevents non-administrative users from changing their passwords.

Note: PWADMIN(YES) is not applicable to the NU setting.

NV

Indicates that vowels cannot appear in a new password. NV is the equivalent of MASK=XXXXXXXX. If options MASK, NM, and NV are specified, only the rightmost option is in effect. If MC is also set, NV is satisfied by any lowercase or uppercase nonvowel.

RN

Specifies that CA Top Secret randomly generates a password for users whose password expires (if the FACILITY control option contains RNDPW). If the NEWPW option does not have RN set, a user can still specify a random password by typing *RANDOM* in the new password field at logon.

Note: If the FACILITY control option does *not* contain RNDPW, CA Top Secret ignores this RN option. Additionally, STC and BATCH facilities do not support this feature.

Random password generation is always uppercase, regardless of whether MC is set.

Note: PWADMIN(YES) is not applicable to the RN setting.

RS

Prevents the user from specifying a new password whose initial characters match one of the password prefix entries in the restricted password (RPW) list. When MC is set, the product checks the RPW list for uppercase and original mixed-case formats of the prefix.

RT

Prevents the user from specifying a new password that contains any string that matches an entry from the restricted password (RPW) list. The restriction applies regardless of where the string occurs within the password. When MC is set, the product checks the RPW list for uppercase and original mixed-case formats of the string.

SC

Specifies that all new passwords must have at least one character selected from the PASSCHAR list. If a list is not defined, this option is ignored. This option is global. Implementing this option is the administrator's responsibility.

Note: Some applications or operating systems might not accept special character in passwords.

SW

Specifies that the new password must contain a special character ($, @, #) between the first and last position. The following examples show samples of this type of password:

```
BIG$RED, I$AM@ME
```

TS

Prevents users from specifying a password that is too similar to the previous password. If any of the following conditions exist, a new password is considered to be too similar:

- The first three characters are identical.
- The second three characters are identical.
- The last three characters are identical.

New passwords that are identical to previous passwords are always rejected, regardless of the NEWPW setting. When MC is set, both password history checking and TS processing test for mixed-case and uppercase equivalents.

LC

Specifies that the new password must contain at least one lowercase letter.

Note: Before you set this option, the MC option must be specified

UC

Specifies that the new password must contain at least one uppercase letter. Before you set this option, the MC option must be specified.

WARN=*nn*

Specifies the number of days leading up to expiration during which users receive warnings that their passwords or ACIDs are about to expire.

Example: WARN=3 specifies that a user receives a warning during each of the last 3 days before expiration occurs.

Default: 3 (If you respecify NEWPW and omit WARN, the product preserves the previous value of WARN.)

Example: Deny Password Use Based on a PGMR String

This example prevents a user from specifying a new password that contains one of the entries in the restricted password list. The entry can be any string that occurs within the password.

```
TSS MODIFY NEWPW(MIN=04,MAX=008,WARN=03,MINDAYS=01,NR=0,ID,TS,RT)
```

For this example, the restricted password list contains the entry *PGMR*. Later, a user needs a password change and tries to use the password *STARPGMR*; however, *PGMR* exists in the restricted password list, making the password unacceptable. If the ACID tries *12PGMR34* as the new password, the same rejection occurs.

More information:

FACILITY—System Facility Processing (see page 80)
RPW—View and Modify the Restricted Password List (see page 197)

NJEUSR—NJE Store and Forward Nodes ACID

Valid on z/OS.

Use the NJEUSR control option to define a default ACID to be used for NJE Store-and-Forward nodes where no other userid can be identified. This control option is used to specify the userid when building a default token in response to a verify SESSION=TKNUNKWN request.

Notes:

- This ACID is used for the owner of the JOB or SYSOUTdata on the Store-and-Forward node and it will have no effect on the userid on the execution node.
- This control option can be included in the startup parms for CA Top Secret. It needs to be set on the intermediate node where the job or output is being lost, and should be a valid ACID for that node, as well as having access to JES and BATCH. However, no checking is done at the time the NJEUSR is set to make certain that the ACID specified is valid.
- If NJEUSR is modified while TSS is executing, and no value is set in the PARMFILE, the modified value will persist.
- If a value is present in PARMFILE for NJEUSR, that value will replace any modified value, if CA Top Secret is restarted with the REINIT option.

This control option uses the Parameter File and TSS MODIFY Command entry methods.

This control option has the following format:

```
NJEUSR(acidname)
```

acidname

The ACID that is used in the VERIFYX call.

Examples: NJEUSR control option

This example sets the NJEUSR ACID using the TSS MODIFY command:

```
TSS MODIFY(NJEUSR(acidname))
or
F TSS,NJEUSR(acidname)
```

This example deactivates the NJEUSR control option:

```
TSS MODIFY('NJEUSR( )')
```

Note: The new option displays as

```
TSS9661I CA Top Secret JES      Status
 JCT(INDEV=0328,ROUTE=0324,NJHDR=0000)
 JES(SSID=JES2,TYPE=JES2,LEVEL=OS 2.10,VERIFY)
 JESNODE(*NONE*)            NJEUSR(*NONE*)
 JOBACID(U,7,0)             SUBACID(U,7)
```

NPPTHRESH—Maximum Password Phrase Attempts

Valid on z/OS and z/VM.

Use the NPPTHRESH control option to specify the maximum number of retry attempts allowed to verify a new password phrase before the logon sequence needs restarting.

This control option has the following format:

```
TSS MODIFY NPPTHRESH(nn)
```

nn

Maximum retry attempts permitted.

Range: 1 to 99

Default: 2

NPWRTHRESH—New Password Reverification Threshold

Valid on z/OS and z/VM.

Use the NPWRTHRESH control option to set the threshold value for the number of attempts allowed for new password reverification before the complete logon sequence needs restarting.

This option:

- Is applicable to TSO and CICS only
- Will not take effect unless the NPWR suboption of the FACILITY control option is added to the TSO or CICS facilities.
- Uses the TSS MODIFY command and as parameter of START command entry method.

This control option has the following format:

```
NPWRTHRESH(nn)
```

Nn

Sets the maximum number of retry attempts the user is allowed when attempting new password reverification before the complete logon sequence needs to be restarted.

Range: 1 to 99

Default: 2

Examples: NPWRTHRESH control option

This example sets the retry password threshold to three:

```
S TSS,,,NPWRTHRESH(3)
```

This example sets the retry password threshold to one using the TSS MODIFY command:

```
TSS MODIFY('NPWRTHRESH(1)')
```

OMVSGRP—Assign an OMVSGRP Segment and Default Group

Valid on z/OS 1.13 and below.

Use the OMVSGRP control option to specify an ACID that provides the OMVSGRP segment for an extract (REQUEST=EXTRACT call) for any group that does not have an OMVSGRP segment.

Note: OMVSGRP and OMVSUSR are not supported in z/OS 2.1 and above.

This specified ACID will also be the value used as DFLTGRP for an extract for any user who does not have the DFLTGRP field defined. The ACID is *not* used as a default group for such a user at signon time.

All entry methods are accepted.

This control option has the following format:

```
OMVSGRP(acid)
```

acid

Specifies an ACID that provides the OMVSGRP segment (for groups) and DFLTGRP (for users) on an extract. The specified ACID should be a group ACID and should be given the GID field.

OMVSTABS—UID and GID Tables

Valid on z/OS.

Use the OMVSTABS control option to request that CA Top Secret refresh the internal UID and GID tables used by OpenEdition for UID and GID processing. Refreshing these tables makes OpenEdition aware of all UID and GID administration since the last IPL table refresh.

The OMVSTABS control option rebuilds internal tables used by OpenEdition for UID and GID processing. Refreshing these tables makes OpenEdition aware of all UID and GID administration since the last IPL or table refresh.

This control option uses the O/S and TSS MODIFY commands and O/S Start command entry methods.

This control option has the following format:

```
OMVSTABS
```

OMVSUSR—Assign an OMVS Segment for Extract

Valid on z/OS 1.13 and below.

Use the OMVSUSR control option to specify the ACID that provides the OMVS segment for an extract (REQUEST=EXTRACT call) for any user who does not have an OMVS segment.

Note: OMVSGRP and OMVSUSR are not supported in z/OS 2.1 and above.

All entry methods are accepted.

This control option has the following format:

```
OMVSUSR(acid)
```

acid

Specifies the name of the ACID that has the OMVS defaults. The ACID should be given the fields UID, HOME, and OMVSPGM. This ACID might also be given DFLTGRP to provide a default for the OMVSGRP control option.

OPTIONS—Specify Configuration Options

Use the OPTIONS control option to specify configuration options. The first 32 option numbers are related to several optional APARs in releases of CA Top Secret prior to 5.1. Option numbers above 32 are general-purpose configuration options (not related to any specific APAR).

You can set any combination of options by using the appropriate numbers.

Note: This control option can be used only at startup. Multiple OPTIONS statements in the parameter file are supported.

This control option has the following format:

```
OPTIONS(n,n,...)
```

n

Specifies any of the following option values:

Option Value	Description	5.0 Fix Number
1	Honor facility options NOLUMSG and NOSTMSG for administrator ACIDs.	LS11840
2	Do not update LASTUSED information on the Security File more than once per day.	LS38929

Option Value	Description	5.0 Fix Number
3	Disable inbound CPF old/new password verification. This allows gradual implementation of Security File synchronization.	LS04865
4	Disable STC PASSCHK=YES. This allows STC's to be defined with passwords without forcing operators to supply a password when the STC is started.	GS81598
5	Allow TSS WHOOWNS without SCOPE checking.	GS95314
6	Suppress the delay after displaying the CA Top Secret message (for TSO sessions) that can occur before the '***' are displayed.	LS11824
7	Truncate JOBACID at the period. For example, a job from R3.RD1 would be assigned ACID R3 even with JOBACID(R,3).	GS88723
8	For a job from R3.RD1, for example, the ACID used is R3 instead of R3@RD1.	GS89207
9	Do not abend CA-11 with S913 abend when VTHRESH is reached.	GS89315
10	Stop jobcard scan at col 68 if CA-7 is the submitter.	GS89316
11	In TYPE=CICS facilities, generate WTO for TSS7100E to ROUTCDE=9 (SYSLOG) when security violations are sensed. This option can degrade performance, but provides a way to monitor violations from the console. Consider TSSTRACK as an alternative.	LS33429
12	Make message TSS9208I deletable and rollable on the console.	LS00838
13	Disable implied FETCH access to database in the LIB() keyword of a permit.	GS89920
14	Allow PRIVPGM from any library when no LIB() keyword is on the permit.	LS11835
15	Make message TSS9209I deletable and rollable on the console.	LS00838
16	Support lowercase letters, enabling Icelandic and Hebrew characters in fields coded in quotes. This option will not uppercase anything that is coded in quotes. See OPTIONS(73) if you wish to restrict this feature to only NAME, INSTDATA, and PHYSKEY.	LS19775
17	Require operator accountability on ZEOD shutdown of CA Top Secret.	LS26244

Option Value	Description	5.0 Fix Number
18	Ensure the CICS region ACID is used for all job submit authorizations unless one is supplied through SPOOLWRITE or TRANSIENT DATA interfaces.	LS26245
19	Place the IMS XREF signon table in private storage by default (instead of in ECSA) for control and associated message regions. Enable sensitivity of region ACIDs to the MRO attribute.	LS26647 LS26644
20	Assign CICS facility DFLTACID for ATS sign on from undefined terminal.	LS33432
21	In TYPE=IMS facilities, generate WTO for TSS7100E to ROUTCDE=9 (SYSLOG) when security violations are sensed. This option can degrade performance, but provides a way to monitor violations from the console. Consider TSSTRACK as an alternative.	LS33433
22	Force logging if using 4.1 plist for TSSAI.	LS33985
23	Do not do any translation on a TSSUTIL report.	LS34770
24	Audit entire session if terminal is audited.	LS38930
25	Issue abend for invalid control option setting during initialization of CA Top Secret.	LS26246
26	Disable ACID XAUTH check out of CA-Roscoe exit TSSRXOUT.	LS19963
27	Treat IMS TIMS resource class checks as LCF.	LS38964
29	CICS: Lock terminal during TSS messages.	GS99164
30	CICS: Last-used stats for ATS.	LS34319
31	CICS: Use LUname on APPL verify signon.	LS34320
32	Enable USS logging feature.	L066385
35	CICS: Enable APPL resource checking.	n/a
36	Modifies the use of the INACTIVE control option. The user is suspended if both of the following are greater than the INACTIVE control option setting: 1) the number of days between the last date an ACID was used and today's date, and 2) the number of days between the last date the ACID's password was changed and today's date. This will *not* work in a CPF environment, since date changes will not be sent along with other CPF data.	n/a

Option Value	Description	5.0 Fix Number
37	Allows the keyword WORKATTR to be used with an ACID TYPE other than GROUP. However, data cannot be extracted except for users, which are capable of signing on, and data cannot be extracted from a connected PROFILE.	n/a
38	Modifies the processing of CICS EXEC VERIFY to make use of cached and encrypted password data already accessed, rather than rereading SECREC data at each subsequent VERIFY during the session.	n/a
40	Disables TSS /DB2 subsystem mode.	n/a
41-60	Reserved for specific VSE options.	n/a
61	Utilizes the Coupling Facility to hold the File Lock record reducing the number of I/Os to the Security File. (The *Lock Record* in the Coupling Facility is a feature of CA Top Secret 5.2) This increases the amount of CPU used due to the IBM support required for the Coupling Facility. You cannot use the Lock Record feature when sharing a Security File and using the Coupling Facility between the two releases. CA Top Secret 5.2 recognizes that the file is in use by a system that does not support the feature and turn the feature off. If CA Top Secret 5.2 gets control of the file first, the file is locked away from other systems that do not support the feature. The SYSID field contains $CFLOCK$. This shows that the system holding the lock is using the Lock Record in the Coupling Facility. If SHRFILE(NO) is set, the CF locking option is ignored.	n/a
62	Forces validation of ACIDs.	n/a
63	Reserved (not implemented)	n/a
64	Honor TSSACEE in TSSCAI.	n/a
65	Controls the action taken when the structure name of the Security File that is active in the Coupling Facility is different from a local Security File structure name. If this option is turned on and the structure names are different during CA Top Secret startup, the local system disconnects from the Coupling Facility and aborts. If CA Top Secret is up when this option is turned on, the local system disconnects from the Coupling Facility and forces other systems to disconnect from the Coupling Facility. When the option is off, which is the default, CA Top Secret will connect to the active structure and override the local structure.	n/a
66	Uppercase the userid during a signon.	n/a

Option Value	Description	5.0 Fix Number
67	Prevent DUF updates from being sent via CPF.	n/a
68	Wait for recovery file update of password change during signon	n/a
69	Fail signon if no access to specified group	n/a
70	Add security to terminals defined as output only under CICS.	n/a
71	Reserved (replaced by CPFLISTMULT option)	n/a
72	Allow a MASTFAC (Master Facility) on all ACID types that are capable of signon.	n/a
73	Support lower case letters for fields NAME, INSTDATA and PHYSKEY when the field is coded in quotes.	n/a
74	Allow non-SCA to administer UID(0)	n/a
75	Do not issue TSS9806I if TARGET(*)	n/a
76	Do not uppercase output in CPF journal file	n/a
77	Normally, a LIST issued after an ACID characteristic expires but before EXPDAYS deletes the characteristic, the UNTIL date displays EXPIRED. With OPTIONS(77) set, LIST displays the actual UNTIL date even when expired.	n/a
78	If CA Top Secret is started with SUB=MSTR, CA Top Secret will not allocate sysout $$$LOG$$ file. This allows CA Top Secret to remain up after JES terminates.	n/a
79	When control option OMVSUSR or OMVSGRP is used to provide a default UID or GID, respectively, write an SMF record to acknowledge the substitution. **Note:** This option takes effect only in z/OS 1.13 or below.	n/a

Example: Invoke Option 1 (to Honor NOLUMSG and NOSTMSG) and Option 5 (to Ignore Scope Checking)

This example honors facility options NOLUMSG and NOSTMSG for administrator ACIDs and also ignores scope checking on TSS WHOOWNS:

```
OPTIONS(1,5)
```

OPTIONS in z/VM

Use the OPTIONS control option to replace several fixes in releases of CA Top Secret prior to r1.4. Any combination of the below options can be set by using the appropriate numbers as indicated.

This control option has the following format:

```
OPTIONS ({n,n,})
```

Where *n* represents any of the following numbers:

1

Enable APPCONN security. Turn on the optional APPCCONN security calls.

2

Do not audit CP commands. Do not cut an AUDIT Record for any CP commands unless a violation has taken place or the CP command is added to the AUDIT Record.

3

Do not audit DIAGNOSE checks. Do cut an AUDIT Record for any CP DIAGNOSE unless a violation has taken place or the CP DIAGNOSE is added to the AUDIT Record.

4

Enable IUCV security calls. Turn on the optional IUCV security calls.

5

Allow ' ' as VMMDISK character and not as a mask. Allow the administrator to use the character ' ' as data in a VMMDISK permit and do not treat it as a masking character.

6

Disable CPF old password reverification. When CPF routes automatically a changed password, the old password must match on the target node before the new password will replace it. This optional removes that matching requirement and causes this system to accept the password change.

7

User message modifications. Allow installation to optionally change the text of the TSS0100A, TSS0101A, TSS0102A, TSS0115E, and TSS0120A messages.

Notes:

- If option 7 is set but no zap applied, you will get the normal message.
- Only above listed messages can be modified by this control option.

- Message replacement must be the exact length of the existing message. If shorter, then pad with blanks.
- You do not need to replace all five messages, only what you wish to change.
- TSSVM MACLIB contains five members, names matching the message number, that contain the VER/REP statements needed to apply your message text. Punch from the MACLIB the number(s) needed. They will punch out with a filetype of COPY, and must be renamed to a filetype of ZAP..

8

Do not reset VMDALTID to ACID=. Normally a logon with ACID= has the VMDALTID replaced by the ACID name. This meant that the origninID of a spooled file would show the ACID and not the machine to which it was logged on. This optional prevents that replacement.

9

Save ACI groupname in VMDUSER7 8. Clients running product VSEG must use this control option to store the directory groupname into VMDUSER7 8 fields for that product's use.

10

TSS0540I displays comments. Normally TSSCRIPT clears comments from input prior to printing. This optional prints the comments from the card also.

11

VFORCE support. This optional is required if you are using the product VFORCE.

12

Allow '+' as SFS FILE character and not as a mask. Allow the administrator to use the character '+' as data in an SFS FILE permit and do not treat it as a masking character.

13

Display IP address as terminal address. If a user logs on through TCP/IP, show the IP address as the terminal address in TSSUTIL reports and TSS WHOAMI output. The IP address will be displayed as an 8 character hex field. If OPTIONS(13) is not set, then the logical device address (LDEVnnnn) will display as the terminal address.

14

Audit all activity at an audited terminal. If a terminal is being audited, audit all activity that takes place during the logon session at that terminal. If OPTIONS(14) is not set, then only the access of the terminal itself (but no subsequent activity) is audited.

15

Enforce CA Top Secret password for APPC logon. By setting OPTIONS(15) all APPC logons use the CA Top Secret password instead of the directory password. This setting is a subset of OPTIONS(1).

16

Include Scandinavian letters with NEWPW(FA) option. By default, the control option NEWPW(FA) forces a new password to contain one of the 26 letters in the English alphabet. Setting OPTIONS(16) expands the letters to include the letters in the Scandinavian alphabet.

17

By default to issue an XAUTOLOG command specifying a terminal you must have the XAUTOLOG command permitted with ACTION(XAUTO-ON). Setting OPTIONS(17) eliminates the need for ACTION(XAUTO-ON) on the permit.

There is no default for this control option.

18

Allow use of application interface to verify a specified ACID exists.

19

Enable CP level OS/DSN security. This option must be selected during CP generation.

PASSCHAR—Password Valid Characters

Valid on z/OS and z/VM.

Use the PASSCHAR control option to add, replace, or remove characters from the password valid character list. When using PASSCHAR:

- Data can be in hex or character format
- Up to 16 unique characters can be defined
- The list can contain one or more special characters
- To enter more than one special character, separate the characters with a comma

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY PASSCHAR(c,c,c,c,c,c,c,c,c,c,c,c,c,c,c,c)
```

Default: Binary zeros.

Note: Without PASSCHAR set, the following special characters are still valid in new passwords: nNational characters ($, @, #) and characters '{' and '}'.

PASSCHAR with NEWPW(SC)

When used in conjunction with control option NEWPW(SC), all passwords must be defined with at least one of the characters in the PASSCHAR list. If NEWPW(SC) is absent, PASSCHAR characters are optional. If no characters are defined in PASSCHAR, NEWPW(SC) has no effect. NEWPW(SC) is a global option for all passwords and facilities. Only use NEWPW(SC) if every application which requires a security password accepts special characters

Special Characters

PASSCHAR contains a list of special characters which can be used in new passwords. Special characters may not be acceptable in some applications or at some levels of the operating system. Valid special characters are:

- Ampersand &
- Asterisk *
- At @
- Carat ^
- Colon :
- Dollar $
- Equal sign =
- Exclamation mark !
- Hyphen -
- Percentage sign %
- Period .
- Pound (hash) #
- Question mark ?
- Underscore _
- Vertical line |

Examples: PASSCHAR control option

This example sets the PASSCHAR to %,&,=,*,-,^

```
TSS MODIFY PASSCHAR (%,&,=,*,–,^)
```

This example replaces the current PASSCHAR with :, ?, and |.

```
TSS MODIFY PASSCHAR(:,?,|)
```

This example removes the current PASSCHAR set.

```
TSS MODIFY PASSCHAR()
```

This example replaces the current PASSCHAR with &, —, and %.

```
TSS MODIFY PASSCHAR(50,60,6C)
```

PDSPROT—Protected PDSs

Valid on z/OS.

PDSPROT is used to identify partitioned (PDS) data sets that are protected at the member level. It is also used to enable or disable PDS member level protection.

If PDSPROT is being used with CA PDSMAN, set FASTSTOW=N in the CA PDSMAN startup parms. This setting allows other products to share STOW processing.

This control option has the following format:

```
PDSPROT(ON|OFF)
PDSPROT(ADD|REMOVE,DSN(dsn),[VOL(vol),]CLASS(resclass))
```

ON

Enables PDS member level protection for only those PDS data sets that have been identified by a PDSPROT(ADD) statement.

OFF

Disables PDS member level protection for all data sets.

ADD

Indicates that a single PDS data set is to be protected at the member level. ADD requires both DSN() and CLASS() operands to be specified. VOL() might optionally appear.

Multiple PDSPROT(ADD) can specify the same resource class name. By doing this, multiple PDS data sets may share common PDS member level protection.

REMOVE

Indicates that a single PDS data set is to be removed from PDS member level protection. Remove requires both DSN() and CLASS() operands to be specified and requires a VOL() operand if it was specified when the data set was added.

DSN

Identifies the data set name of a single PDS being affected during an ADD or REMOVE statement. No masking is allowed. The data set name should be fully qualified and without quotes.

Range: 1 to 44 characters

VOL

Optionally identifies the disk volume serial (volser) of the PDS data set named on the same statement. The VOL() operand may be omitted and is only recommended when needed to distinguish between identically named PDS data sets. If coded, specify a complete six-character volser without masking.

CLASS

Identifies the name of the resource class under which all PDS member level protection for the named data set will occur. Note that the CA Top Secret Resource Definition Table (RDT) contains five predefined resource classes named PDSMEM1 through PDSMEM5 for this use. Specify one of these predefined class names or the 1 to 8 character name of another resource class.

PPEXP—Days Before Password Phrase Expires

Valid on z/OS and z/VM.

Use the PPEXP control option to specify the number of days before a password phrase expires.

This control option has the following format:

```
TSS MODIFY PPEXP(nnn)
```

nnn

The number of days before a password phrase expires. Use 0 for a password that does not expire.

Range: 0 to 255

Default: 30

PPHIST—Number of Password Phrases Recorded

Valid on z/OS and z/VM.

Use the PPHIST control option to specify the number of previous password phrases maintained in an acid's password phrase history.

This control option has the following format:

```
TSS MODIFY PPHIST(nn)
```

nn

Specifies the number of password phrases (past and current) maintained for each ACID. Specify 1 to record the current password phrase only.

Range: 1 to 64

Default: 3

PPSCHAR—Special Characters in Password Phrases

Valid on z/OS and z/VM.

Use the PPSCHAR control option to add, replace, or remove characters from the password phrase valid character list.

The list can:

- Be in hex or character format
- Contain special characters from the list below
- Contain up to 18 unique characters separated with a comma

Valid special characters are:

- Ampersand &
- Asterisk *
- At @
- Blank (must be entered in hex)
- Carat ^
- Colon :
- Dollar $
- Equal sign =
- Exclamation mark !
- Hyphen -
- Percentage sign %
- Period .
- Pound (hash) #
- Question mark ?
- Vertical line |
- Underscore _

This control option has the following format:

```
TSS MODIFY PPSCHAR(c,c,c,c,...)
```

Example: PPSCHAR control option

This example uses character format to set the special characters to *, &, and %:

```
TSS MODIFY PPSCHAR(*,&,%)
```

This example uses hexadecimal format to set the special characters to &, _, and %.

```
TSS MODIFY PPSCHAR(50,60,6C)
```

This example resets the PPSCHAR control option:

```
TSS MODIFY PPSCHAR()
```

PRODUCTS—Special Products

Valid on z/OS.

Use the PRODUCTS control option to list special products, if any, that are installed on the system.

All entry methods are accepted.

This control option has the following format:

PRODUCTS(*name*,*name*...)

TSO/E

(Default) Indicates that TSO/E is being used instead of TSO. This is the default.

ACF/2

Indicates that CA-ACF2® is temporarily active, awaiting conversion to CA Top Secret.

CA-Tape

Indicates that CA-Tape is active for processing tape volumes at the data set name level.

TSO

Indicates use of TSO.

NONE

Resets the option.

Example: Products control option

This Parameter File example indicates that CA-Tape is active at the installation:

```
*
* CONTROL OPTIONS
*

PRODUCTS(CA-Tape)
```

PROFINTERVAL—Profile Non-refreshable Period

Valid on z/OS.

Use the PROFINTERVAL control option to specify how long a profile stays non-refreshable if no further updates are made to the profile record.

This allows a profile with the NOREFRESH attribute set to become refreshable after the specified interval has passed.

For information on NOREFRESH, see the *Command Functions Guide*.

All entry methods are accepted.

This control option has the following format:

```
TSS MODIFY PROFINTERVAL(nnnn)
```

nnnn

Specifies a value in seconds.

Range: 0 to 9999.

PROPXREP—Propagate Results of an Extract Replace

Valid on z/OS and z/VM.

Use the PROPXREP control option to allow or prevent the propagation of the results of a successful extract/replace call to other systems and the recovery file. This control option is a global setting. You must also configure specific profile field attributes to allow propagation. You can only modify user-defined fields and pre-defined fields that do not already specify NOXTRPRP.

All entry methods are accepted.

This control option has the following format:

```
PROPXREP(ON|OFF)
```

ON

The results of an extract/replace call are sent to the recovery file and propagated to other systems via CPF or LDS provided that the applicable field does not display the NOXTRPRP attribute.

OFF

The results from a successful extract/replace are not sent to the recovery file or propagated to other systems. (Default) For information regarding turning off this functionality on individual fields in the FDT, see the ATTR keyword in the *Command Functions Guide*.

PSWDPHRASE—Allow Password Phrases

Valid on z/OS.

Use the PSWDPHRASE control option to globally allow all users to specify a password phrase.

Note: z/OS 1.10 supports password phrases for TSO signon but changes are required to the IKJTSOxx member in SYS1.PARMLIB. For more information, see IBM's *z/OS MVS Initialization and Tuning Reference*.

This control option has the following format:

```
TSS MODIFY PSWDPHRASE(ON|OFF)
```

ON

All users can specify a password phrase.

OFF

(Default) Users must have the PSWDPHR attribute set to specify a password phrase.

PTHRESH—Password Violation Threshold

Valid on z/OS and z/VM.

Use the PTHRESH control option to specify the maximum password violation threshold. If the user exceeds the specified threshold by entering the wrong password too many times, CA Top Secret suspends the ACID.

Note the following rules:

- Password thresholding only pertains to incorrect passwords. It does not pertain to missing passwords, or new-password specification violations. Password specification and reverification both are counted.
- Each user ACID has an associated invalid password counter.
- CA Top Secret counts invalid password attempts from the last valid signon.

All entry methods are accepted.

This control option has the following format:

```
PTHRESH(0|nnn)
```

0

Deactivates password thresholding.

nnn

Specifies the number of incorrect passwords a user can enter before being suspended.

Range: 1 to 254

Default: 4

Example: PTHRESH control option

In this example, if a user enters an invalid password twice in succession, but successfully signs on with their third attempt, CA Top Secret resets the counter to 0. However, if the user enters an invalid password for the third straight time, CA Top Secret suspends this user after his third violation:

```
F TSS,PTHRESH(2)
```

PTKRESCK—Pass Ticket Authorization

Valid on z/OS.

Use the PTKRESCK control option to indicate whether or not a FASTAUTH resource validation check is performed to verify that a user has the appropriate authority to generate a Pass Ticket for a specific user and application. This FASTAUTH call is made with the CLASS=PTKTDATA, ATTR=UPDATE, and ENTITYX='PTKTGEN.applid.userid' parameters, where:

applid

The application ID associated with the PassTicket.

userid

The ID of the user for which the PassTicket is being generated.

This security call is issued regardless of any other PassTicket security calls.

This control option has the following format:

```
PTKRESCK(YES|NO)
```

YES

Activates the PTKRESCK feature.

NO

(Default) Deactivates the PTKRESCK feature.

Example: PTKRESCK control option

This example activates PTKRESCK:

```
F TSS,PTKRESCK(YES)
```

PWADMIN—Enforce NEWPW Rules for Administrative Password Changes

Valid on z/OS.

Use the PWADMIN control option to enforce NEWPW control option rules and the password interval specification when an administrator or user with MISC8(PWMAINT) or ACID(MAINTAIN) authority performs a password change through a TSS command.

Note: When PWADMIN(YES) is active, the NEWPW MINDAYS option is *not* enforced.

This control option may be entered as a MODIFY command or through the parameter file.

This control option has the following format:

```
PWADMIN(YES|NO)
```

YES

Enforces NEWPW controls during TSS command administrative password changes (also checks password history for identical passwords), and does *not* allow expiration interval changes.

NO

(Default) Does *not* enforce NEWPW rules (or check password history) during TSS command administrative password changes and allows expiration interval changes.

Note: The CASECAUT resource class allows an override of NEWPW restrictions through CASECAUT resource permissions with UPDATE access. For details about using CASECAUT to provide restricted administrative authorities, see the *CA Top Secret User Guide*.

More information:

NEWPW—Restrict Password Alterations (see page 157)

PWENC—Select AES Encryption Method

Valid on z/OS.

Use the PWENC control option to select whether AES encryption is performed by software or hardware.

This option applies only when AES encryption is used for passwords and password phrases.

All entry methods are accepted.

This control option has the following format:

```
PWENC(AES|ICSF)
```

AES

(Default) Indicates that AES encryption is performed by software routines.

ICSF

Indicates that AES encryption is performed by ICSF hardware.

PWEXP—Password Expiration Interval

Valid on z/OS and z/VM.

Use the PWEXP control option to specify a password expiration interval.

Note the following:

- PWEXP is modifiable during CA Top Secret execution and requires console authority.
- Changing the expiration interval would have no effect on current users; only on users who have been created after the change.

All entry methods are accepted.

This control option has the following format:

```
PWEXP(0|nnn)
```

nnn

The number of days before passwords expire.

Range: 1 to 255

Default: 30

0

Passwords for all new users never expire.

Example: PWEXP control option

This example sets the default password expiration interval for new ACIDs to 50 days.

```
F TSS,PWEXP(50)
```

PWHIST—Number of Previous Passwords Retained

Valid on z/OS and z/VM.

Use the PWHIST control option to specify the number of previous passwords maintained as part of an ACID's password history. Password history prevents users from reusing old passwords when their current password expires. CA Top Secret always rejects new passwords that are identical to the previous password.

This control option has the following format:

```
PWHIST(nn)
```

nn

Specifies the number of passwords (past and current) maintained for each ACID. Specify 1 to record the current password only.

Range: 1 to 64

Default: 3

Example: control option

This example sets the number of previous passwords to be maintained for each ACID to five.

```
F TSS,PWHIST(5)
```

PWVERIFY—Force Password Verification

Valid on z/OS and z/VM.

Use the PWVERIFY control option to force users to verify their old password before changing to a new password. When this option is set to YES, users should do an ACID refresh or log off and back on after changing their password.

The parameter file entry method is used for this control option.

This control option has the format:

```
PWVERIFY(YES|NO)
```

YES

Users changing their password are prompted for their old password before the change is allowed.

NO

(Default) Users can change their password without entering their old password.

PWVIEW—(Obsolete)

This control option is no longer supported.

PWVIEW(NO) can remain in the parameter file. If PWVIEW(YES) is specified an error message is displayed on the console.

RCACHE—Cache Hardening

Valid on z/OS.

Use the RCACHE control option to specify whether hardening is allowed or disallowed.

This control option has the following format:

```
TSS MODIFY(RCACHE(YES|NO))
```

YES

Allows hardening of R_cacheserv. When yes is specified, the global hardening option is set to on.

NO

(Default) Disallows hardening of R_cacheserv. When no is specified, the global hardening option is set to off.

RCQNAME—Caches Hardening Selection

Valid on z/OS.

The RCQNAME control option specifies which caches can be hardened. For information on the R_cacheserv SAF Callable Service, see the IBM manual *z/OS Security Server RACF Callable Services*.

No more than 10 queue names may be entered at a time. Cache names must be exactly 6 characters long and must start with the capital letter R. Valid names may contain the following characters: A-Z, 0-9, @, #, and $. Blanks are not allowed.

This control option has the following format:

```
TSS MODIFY(RCQNAME(ADD,Rxxxxx,Rxxxxx,…)
TSS MODIFY(RCQNAME(REM,Rxxxxx,Rxxxxx,…)
```

ADD(Rxxxxx)

Specifies whether a name is added to the R_cacheserv table.

REM(Rxxxxx)

Specifies whether a name is removed from the R_cacheserv table.

RDT2BYTE—(Obsolete)

RDT2BYTE allows the administrator to ADD 2-byte RESCODE values to RDT resource classes. Although CA Top Secret 5.2 allows clients the ability to create such resource classes, caution must be exercised if the Security File is to be shared with a CA Top Secret 5.1 system.

All entry methods are accepted.

This control option has the following format:

```
RDT2BYTE
```

CA Top Secret 5.2 introduced 256 additional resource classes, which are represented internally with 2-byte RESCODEs. These resource classes are incompatible with lower-level releases, which only allow 1-byte RESCODEs. The control option RDT2BYTE must be set before a 2-byte RESCODE can be added to the RDT.

Once a resource class has been added to the RDT with a 2-byte RESCODE, irrevocable changes are made to the Security File.

In this case, we say that the RDT2BYTE control option has been activated. CA Top Secret r5.2 will initialize with the message

```
TSS9053I - RDT2BYTE OPTION ACTIVATED
```

Once RDT2BYTE is activated, any CA Top Secret 5.1 system attempting to initialize with such a Security File will terminate with the message

TSS9996E - Security File contains 2-byte RESCODEs and cannot be used by this release

If an CA Top Secret 5.1 system shares a Security File with a CA Top Secret 5.2 system, and the latter defines a 2-byte RESCODE resource class to the RDT, results can be unpredictable, and may compromise Security File integrity. When the 5.1 system is shut down, it will no longer be able to initialize with the same security file.

Unlike other control options, once RDT2BYTE has been activated, it cannot be modified by altering the Parameter File or executing a MODIFY command. RDT2BYTE should not be activated in any system until all systems sharing the Security File are running with CA Top Secret r5.2.

When listing an RDT reclass the RESCODE will display as RESOURCE CODE = X'nnn'. User written programs that run against the output from the LIST command will need to be reviewed to allow for this change. In particular, the output layout for the TSSCFILE utility has been changed to accommodate the rescode field, which has increased from a 2-byte field to a 3-byte field.

Examples: RDT2BYTE control option

This example sets the control option RDT2BYTE:

```
TSS MODIFY RDT2BYTE
```

This example activates RDT2BYTE irrevocably in the security file:

```
TSS ADD(RDT) RESCLASS(yourclas)
             RESCODE(12F)
             ACLST(ALL,EXEC=200,NONE)
             DEFACC(EXEC=200)
```

Notice that the RESCODE(12F) can no longer be expressed as a single byte hexadecimal representation. This is why it is called a 2-byte RESCODE. For information on defining resource classes to the RDT, see the *Users Guide*, and the *Command Functions Guide*.

RECOVER—Record Changes in Recovery File

Valid on z/OS and z/VM.

Use the RECOVER control option to indicate whether CA Top Secret records changes made to the Security Database onto the Recovery File. Changes include those made automatically by CA Top Secret (automatic volume ownerships, password changes) and those made by security administrators via the TSS command.

If this option is omitted at CA Top Secret startup, RECOVER(ON) is in effect if the RECFILE DD-statement is in the CA Top Secret started task.

This control option has the following format:

```
RECOVER(ON|OFF)
```

ON

(Default—As long as RECFILE DD-statement is in CA Top Secret started task procedure) Activates the Recovery File. Indicates that changes made to the security database is recorded in the Recovery File.

OFF

Deactivates the Recovery File. Turn Recovery OFF when running the TSSRECVR utility to prevent double recording of changes.

REFRESH—Reinitialize CA SAF Modules into CSA

Valid on z/OS.

Use the REFRESH control option to request that CA Top Secret reinitialize all CA SAF modules from the system linklist into CSA. This control option should be used only under the direction of CA Top Secret Technical Support. The command should normally be preceded by an LLA refresh.

The REFRESH control option is protected by the Operator Accountability feature (CONSOLE attribute). CA Top Secret prompts you from the console for the proper ACID and password before processing the REFRESH request.

This control option has the following format:

```
REFRESH(SAF|modabbrv)
```

<none>

REFRESH without operands performs the same function as SAF.

SAF

Refresh all SAF modules from LINKLIST into CSA.

modabbrv

Refresh an individual SAF load module from LINKLIST into CSA. The module abbreviation (modabbrv) omits the prefix “SAF” from the actual load module name.

Examples: REFRESH control option

This example reloads module SAFOEDRV from linklist into CSA, deleting the existing copy:

```
TSS MODIFY(REFRESH(OEDRV))
```

This example refreshes the SAFOEDRV module:

```
F TSS,REFRESH(OEDRV)
```

REINIT—Control Blocks and Modules

Valid on z/OS.

Use the REINIT control option to request that CA Top Secret reinitialize its internal control blocks and modules. Use this option only after new maintenance to CA Top Secret has been installed.

This control option uses the Parameter of START command entry method.

This control option has the following format:

```
REINIT[(K|E|M|1|2|3|S|R)]
```

REINIT

Reinitializes everything

REINIT(K)

Reloads module TSSKERNL

REINIT(E)

Reloads module TSSEXEC

REINIT(1)

Reloads module TSSMVS01

REINIT(2)

Reloads module TSSMVS02

REINIT(3)

Reloads module TSSMVS03

REINIT(M)

Reloads TSS, TSSIMS, TSSRESPW

REINIT(S)

Reloads module TSSSAF

REINIT(R)

Reloads module TSSRFRVT

Examples: REINIT control option

This example reinitializes all CA Top Secret modules:

```
S TSS,,,REINIT
```

This example reinitializes the TSSMVS1 module only:

```
S TSS,,,REINIT(1)
```

Note: z/OS systems syntax format requires the insertion of three commas.

RESETEOD—Restart After Z Stop

Valid on z/OS.

Use the RESETEOD control option to allow CA Top Secret to be restarted, without an IPL, after it has been brought down (accidentally) at the end of a day with a 'Z' stop.

This control option uses the O/S Console commands entry method only.

This control option has the following format:

```
RESETEOD
```

End-of-day shutdown prohibits new initiations in all modes. No new users can sign on to any facility, and no new batch jobs can start. When CA Top Secret is restarted, all control options show up in error, and the system defaults (including the default FAIL mode) are automatically restored.

Example: RESETEOD control option

This example restarts CA Top Secret after an accidental end-of-day shutdown:

```
S TSS

F TSS,RESETEOD

P TSS

S TSS,,,REINIT
```

RESETSTATS—Reset Stats Counters

Valid on z/OS and z/VM.

Use the RESETSTATS control option to reset all counters displayed by the STATS control option to zero.

All entry methods are accepted.

This control option has the following format:

```
RESETSTATS
```

Example: RESETSTATS control option

This example resets all counters, except HWM, displayed by the STATS control option:

```
F TSS,RESETSTATS
```

RPW—View and Modify the Restricted Password List

Valid on z/OS and z/VM.

Use the RPW control option to view and modify the restricted password list, which contains entries that cannot be used as new passwords. Viewing and modifying this list allows a site to manage passwords and prevent the use of obvious passwords (such as company names, titles, months, and names). Mixed-case passwords are temporarily transformed to uppercase before being checked against the RPW entries.

The restricted password list is loaded initially at startup but can be modified anytime. The list is not rebuilt other than from a reinitialization of CA Top Secret. CA Top Secret provides 33 default entries in the list but allows a maximum of 511 entries.

Note: The restricted password list is in effect only for *new* passwords that are entered while the NEWPW(RS) control option is in effect.

All entry methods are accepted. The RPW control option is protected by the operator accountability feature. CA Top Secret prompts the person entering the command for the authorized ACID/password combination before processing the command.

This control option has the following format:

```
RPW(LIST)|(RESET)|(ADD,password_entry,...)|(REMOVE,password_entry,..)
```

LIST

Displays the contents of the restricted password list.

RESET

Removes all entries from the restricted password list (including the product defaults). After the RESET option clears all password restrictions, the 33 default entries can be recovered only by manual RPW(ADD,…) or automatically by a reinitialization of CA Top Secret.

ADD

Adds one or more entries to the restricted password list.

password_entry

Specifies a one- to seven-character password entry.

REMOVE

Removes one or more entries from the restricted password list.

Default entries in the restricted password list are as follows:

APPL	APR	ASDF	AUG	BASIC	CADAM
DEC	DEMO	FEB	FOCUS	GAME	IBM
JAN	JUL	JUN	LOG	MAR	MAY
NET	NEW	NOV	OCT	PASS	ROS
SEP	SIGN	SYS	TEST	TSO	VALID
VTAM	XXX	1234			

Example: Add Passwords to the Restricted Password List

This example adds entries to the restricted password list:

```
F TSS,RPW(ADD,STAFF1,BATMAN,MYPASSW,MGRPASS)
```

The entries represent *new* passwords that CA Top Secret will not accept from users. Any users who currently use these passwords will function normally.

Example: Remove a Password from the Restricted Password List

This example removes a password from the restricted password list:

```
F TSS,RPW(REMOVE,BATMAN)
```

BATMAN may now be selected as a new password.

Example: Display the Contents of the Restricted Password List

This example lists the current contents of the restricted password list:

```
TSS MODIFY(RPW (LIST))
IBM     TEST    SYS     LOG     SIGN    TSO
PASS    NEW     VTAM    NET     APPL    ROS
BASIC   FOCUS  CADAM   VALID   DEMO    GAME
JAN     FEB     MAR     APR     MAY     JUN
JUL     AUG     SEP     OCT     NOV     DEC
XXX     ASDF    1234    STAFF1  BATMAN  MYPASSW
MGRPASS
MODIFY   FUNCTION SUCCESSFUL
```

Example: Reset the Restricted Password List

This example removes all restricted passwords entries (including the product defaults) and restores the product defaults at the next REINIT of CA Top Secret:

```
TSS MODIFY RPW(RESET)
```

SDNSIZE—Digital Certificate SDN Size

Valid on z/OS.

Use the SDNSIZE control option to set the maximum size for the SDN (Subject's Distinguished Name) and SN.IDN (Serial Number.Issuer's Distinguished Name) fields in a digital certificate that is added to the security file. SDNSIZE should be set to 255 until all systems sharing the security file are running CA Top Secret release 15 and higher.

Note: SDNSIZE also controls the maximum size of the data specified with the SDNFILTR and IDNFILTR keywords on a TSS command.

This control option uses the Parameter file entry method.

This control option has the following format:

```
SDNSIZE(nnnn)
```

nnnn

Specifies the maximum SDN and SN.IDN field size for a digital certificate.

Limits: 255 or 1024

Default: 255

Example: SDNSIZE control option

This example indicates that the larger SDN and SN.IDN fields supported:

```
SDNSIZE(1024)
```

SECCACHE—Security Record Cache

Valid on z/OS.

Use the SECCACHE control option to provide a cache for CA Top Secret to place security records that reflect the status of a user following a RACROUTE VERIFY request. The cache is managed in a common data space that can be accessed from all address spaces. The cache increases system performance by:

- Reducing CPU cycles in both the user and security address spaces required to complete subsequent RACROUTE VERIFY requests
- Reducing I/O against the security file when the file is shared between multiple systems

Important! The SECCACHE control option parameters are positional, they must be entered in the order listed.

All entry methods are accepted.

This control option has the following format:

```
SECCACHE(SIZE=mmmm,INDEX=nnnnnn,EXP=hhh,WARN=ppp)
SECCACHE(CLEAR,EXP=hhh|acidname)
SECCACHE(STATUS)
SECCACHE(OFF)
```

SIZE=mmmm

Specifies the number of megabytes of data space storage allocated for caching. If previously set to OFF, providing this value activates the SECCACHE. The cache CAnnot be increased without a re-cycle of the SECCACHE feature. Assure that there is sufficient virtual storage to accommodate your SECCACHE request.

Range: 20 to 2048

INDEX=nnnnnn

Sets the number of index entries pre-allocated within the cache. This value cannot be increased without a re-cycle of the SECCACHE.

Range: 10 to 999999

Default: 5000

EXP=hhh

Sets the expiration interval, in hours, for existing records in the cache. The expiration interval is used by the SECCACHE(CLEAR) request to recover cache space from expired records.The TOD value for each record in the cache is set when it is added and reset on every successful get request for that record. An expiration interval of 0 prevents existing records from expiring.

Maximum: 255

Default: 0

WARN=ppp

Sets the threshold full warning level for both the data and index areas of the cache. If the warning level is reached by either the data or index areas, an automatic CLEAR attempt is made to recover space using the expiration interval supplied at cache initialization. If sufficient space cannot be recovered to lower the percentage full below the warning level, message TSS1366W is sent to the operator console and remains there until sufficient space can be recovered, the security record cache is deactivated, or the security address space is terminated. Records can still be added to the cache up to the point where either the data are index areas become 100% full.

Maximum: 100

Default: 90

CLEAR

Attempts to recover cache space by deleting existing records that have expired based on the expiration interval supplied at cache initialization.

CLEAR,EXP=hhh

Attempts to recover cache space by deleting existing records that have expired based on the expiration interval supplied as input. This method overrides the expiration interval supplied at cache initialization and can be used in response to message TSS1366W to attempt space recovery.

CLEAR,acidname

Attempts to recover cache space by deleting an existing record that matches the acid name supplied as input. This method does not check any expiration interval and it can be used to refresh a user experiencing authorization problems.

STATUS

Provides statistics on how the security record cache is used and how efficient the cache is in improving system performance. If SECCACHE is active, the following statistics are displayed:

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. This is the best indication of how well the cache is performing in minimizing RACROUTE VERIFY request overhead.

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. A large number indicates the data size allocated to the cache is too small. You can attempt to recover space with a CLEAR,EXP=nnn request.

NOINDEX

Number of index entry allocation requests failing due to no available space. A large number here indicates the number of index entries allocated to the cache is too small. You can attempt to recover space with a CLEAR,EXP=nnn request.

Warn %

Threshold full level to trigger console warning messages. This value applies to both the data and index areas of the cache independently.

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. This value may be useful in calculating the amount of storage to allocate to the cache.

OFF

Deactivates SECCACHE. The cache is emptied and is not used until requested by a SECCACHE(SIZE=mmmm) command. SECCACHE does not deactivate when the security manager address space is terminated. Use the OFF option to deactivate.

SECCACHE in a Shared Security File Environment

In a shared security file environment, it is important that policy changes made on one system are reflected within any in-core processing tables on all remote systems as soon as possible. This is accomplished internally when a security file I/O is performed on the remote system, for example when a user logs on.

The SECCACHE control option eliminates much of the security file I/O associated with a user log on event. To improve the synchronization an internal processing event performs any in-core table refresh, if required, at the end of two TIMER cycles. This keeps the tables up to date even though the security file has not been accessed. You can manually synchronize the in-core tables with the MODIFY SYNCH control option. This allows you to immediately see the effects of remote changes to selected SDT records with the TSS LIST command.

SECTRACE—Security Trace

Valid on z/OS and z/VM.

Use the SECTRACE control option to activate a diagnostic security trace on the activities of all defined users or of specific users.

All entry methods are accepted.

This control option has the following format:

```
SECTRACE(WTO|WTL|OFF)|(ACT,WTO|WTL)|(ON)
```

WTO

Activates the trace, and routes messages to the master console for all users and events.

WTL

Activates the trace and routes messages to the SYSLOG (system log). Use with the ACT operand.

ON

Activates global trace.

OFF

(Default, as long as a command is not specified in the PARMLIB) Deactivates diagnostic tracing. OFF is only used as a default when a command is not specified in the PARMLIB.

ACT

Activates the trace for users that have the TRACE attribute attached to their ACIDs. ACT must be specified with WTL or WTO in this format:

```
SECTRACE(ACT,WTL|WTO)
```

Destinations of Trace Messages

In TSO, trace information always goes to both the terminal and SYSLOG.

The following operands indicate the possible destinations of the trace messages:

WTO

To the master console

WTL

To SYSLOG

The SECTRACE control option is usually issued at the request of Technical Support.

TRACE messages use the following prefixes:

TSS-I

For initiations.

TSS-E

For terminations.

TSS-C

Access validation done through RACHECK.

TSS-D

Access validation done through RACDEF

TSS-F

Access validation done through FRACHECK.

TSS-T

TSS command.

TSS-V

JES Early Verify Password support.

SHRFILE—Share Files

Valid on z/OS and z/VM.

Use the SHRFILE control option to specify whether files used by CA Top Secret are shared among other operating systems and/or CPUs.

Important! Due to the VSAM file requirement for r15, z/OS can no longer share secfiles with z/VM or z/VSE.

All entry methods are accepted.

This control option has the following format:

```
SHRFILE(YES[,AINDXPER])|(SECURITY[,AINDXPER])|(NO)
```

YES

(Default) Specifies that both the security file and the AUDIT files are shared among other operating systems and/or CPUs. This is the default. If you are not actually sharing the security file and audit files, this option will generate significant unnecessary I/O to the security file and the AUDIT files.

SECURITY

Specifies that the security file but not the AUDIT files are shared among other operating systems and/or CPUs. CA Top Secret will perform lock processing on the Security File (and subsequently on the Recovery File), but will not perform lock processing on the Audit File. Audit File processing is handled as if SHRFILE(NO) had been specified.

NO

Specifies that neither the security file nor the AUDIT files are shared among other operating systems and/or CPUs. The LOCK records on the Security and Audit Files are obtained at startup and never released, totally eliminating all I/O required for lock record processing in a single CPU environment.

AINDXPER

(Obsolete) This is no longer an option, it is now the default method of processing I/O when the security file is shared between multiple systems. The control option syntax checking still supports specification of the option so that existing parameter files do not experience problems.

Examples: SHRFILE control option

This example indicates that all of the files used by CA Top Secret is shared among other operating systems and/or CPUs.

```
SHRFILE(YES)
```

Make the following entry if you want to share the file between CA Top Secret 5.2 systems only.

```
SHRFILE(YES,AINDXPER)
```

This example indicates that file is standalone but performance feature is not on.

```
SHRFILE(NO)
```

Make the following entry if the performance feature should be on and the file is a standalone.

```
SHRFILE(NO,AINDXPER)
```

You cannot issue a MODIFY with SHRFILE(YES) to turn off just the AINDXPER suboption if SHRFILE(NO)AINDXPER was originally issued. For example.

```
SHRFILE(NO)
```

SHRPROF—Shared Profile Table

Valid on z/OS.

Use the SHRPROF control option to display the shared profile table percentage used for a multiuser address space (For example, an IMS or CICS region). Use this option to detect potential problems when the percentage used of the shared profile table is increasing.

This control option uses the O/S and TSS MODIFY commands entry methods.

This control option has the following format:

```
SHRPROF(jobname)
```

jobname

Specifies a JOB/STC name for a multi—user address space (MUAS) whose shared profile table statistics you wish to display.

When the job name specified does not have a shared profile table, the following message is displayed:

TSS0964I NO SHARED PROFILE TABLE FOR JOB xxxxxxxx

When the shared profile table is full, the following message is displayed:

TSS0960E SHARED PROFILE TABLE IS FULL — JOB xxxxxxxx

When a shared profile table has been allocated and it is not full, the following message is displayed:

TSS0963I SHARED PROFILE TABLE > nn% FULL — JOB xxxxxxxx (PRIVATE/CSA)

SMA—Start SMA Dynamically

Valid on z/OS.

Use the SMA control option for the TSSSMA address space to start dynamically and establish communication with the remote SMA host defined in the NDT SMANODE record.

This control option is specified in the startup JCL parameters file or dynamically issued with the TSS MODIFY command.

This control option has the following format:

```
SMA (ON|OFF)
```

SMFTYPE—Change SMF Record Type

Use the SMFTYPE control option to change the SMF record type for SAF trace, USS logging, and STATG records from 231 to another type.

All entry methods are accepted.

This control option has the following format:

```
SMFTYPE(nnn)
```

nnn

Specifies the SMF record type to use for SAF trace, USS logging, and STATG records.

Range: 0 to 255

IBM Reserved: 0 to 127

Available for user-written records: 128 to 255

More information:

STATG—Start or Stop Statistics Gathering (see page 211)

ST—Control Option Display

Valid on z/OS and z/VM.

Use the ST control option to produce a display that combines the information produced for the VERSION, STATUS, and STATS control options.

This control option uses the O/S or TSS MODIFY commands entry methods.

This control option has the following format:

```
ST
```

See VERSION, STATUS, and STATS for examples of information displayed in response to the ST command.

Example: ST control option

This example determines complete information about the security control status at his installation, the SCA would enter at the control console:

```
F TSS,ST
```

STATG—Start or Stop Statistics Gathering

Valid on z/OS.

Use the STATG control option to start or stop statistics gathering for CA Top Secret. Statistics gathering collects system statistics and creates SMF records for a given time frame (measured in minutes through the STATGINT control option). By default, the SMF record type for STATG records is 231, but you can use the SMFTYPE control option to change this type.

Note: Use the TSSRPTSG program to report on the collected statistics. For information about TSSRPTSG, see the *Report and Tracking Guide*.

All entry methods are accepted.

This control option has the following format:

```
STATG(ON|OFF)
```

ON

Specifies that statistics gathering is activated.

OFF

(Default) Specifies that statistics gathering is not active. No statistical information is gathered and recorded to the SMF files.

More information:

SMFTYPE—Change SMF Record Type (see page 210)

STATGINT—Specify Statistics Gathering Time Interval

Valid on z/OS.

Use the STATGINT control option to specify the time interval for statistics gathering and SMF record creation. This control option is used in conjunction with the STATG(ON) control option.

Note: STATGINT(00) indicates that the STATG option is not activated.

All entry methods are accepted.

This control option has the following format:

```
STATGINT(nn)
```

nn

Time interval in minutes.

Range: 1 to 60

Default: 15

STATREC—Statistics Processed

Valid on z/OS.

Use this control option to specify the types of statistics to be processed.

All entry methods are accepted.

This control option has the format:

```
STATREC(CACHE, COMMAND, CPF, IOSTATS, RACROUTE, SECCACHE, SYSPLEX, WORKLOAD)|(ALL)
```

Examples: STATREC control option

This example processes cache and command statistics, the ALL is ignored:

```
STATREC(CACHE,COMMAND,ALL)
```

This example processes all statistics:

```
STATREC(ALL)
```

STATS—Display Statistics

Valid on z/OS and z/VM.

Use the STATS control option to display numeric counts concerning CA Top Secret security processing.

This control option uses the O/S or TSS MODIFY commands entry methods.

This control option has the following format:

```
STATS
```

STATS

Generates a console display identified by messages in the TSS95xxI series.

STATS produces a display showing the number of:

- Job initiations validated
- Cross-memory requests processed
- z/OS security calls processed
- SMF security records logged
- Program executions validated
- CACHE statistics processed
- Changes made to the Security File
- Changes saved in the Recovery File
- Security File input requests made
- Security File output operations since IPL on this CPU
- Audit events recorded in the Audit/Tracking File
- Counts of each TSS command issued
- CPF statistics

STATSLOG—Statistics Dataset Name

Valid on z/OS.

Use the STSTSLOG control option to specify the name of a pre-allocated dataset where statistics are written to.

All entry methods are accepted.

This control option has the format:

```
STATSLOG(DSNAME)
```

DSNAME

The dataset statistics are written to. The dataset must have a format of RECFM=FB, LRECL=100, DSORG=PS.

Default: SMF

STATUS—Control Options Settings

Valid on z/OS and z/VM.

Use the STATUS control option to provide the current settings of various control options. You can specify which option to display when you enter a TSS MODIFY(STATUS) command.

Change the default by specifying STATUS(option,option,...) in your PARMFILE.

The options listed in the STATUS control option can be in any order, and the output is presented in the order used in the control option.

The TSS MODIFY(STATUS) command can include a single option to display only that information requested, or to acquire information not set in the STATUS control option. For example, the TSS MODIFY(STATUS(JES)) will show the JES information.

All entry methods are accepted.

In z/OS this control option has the following format:

```
STATUS(option)
```

Optional displays are valid with z/OS only. The following statuses are displayed by the STATUS command:

BASE

Shows base system and miscellaneous control options. FEATURES is an extension of BASE that displays MAX_ACID_SIZE, RDT2BYTE, NEW_PASSWORD, and VSAM_SDT.

CPF

Shows CPF related control options, and displays the current settings for CPFNODES. Note that NDT CPFNODE definitions will override control option settings for CPFNODES.

CIART

Shows the CIA real-time control option settings.

FACMODE

Shows facility modes.

JES

Shows JES-related control options.

LDS

Shows LDS related fields

PASSWORD

Shows password-related control options.

PHRASE

Displays the password phrase control options.

STATG

Includes statistics control options in the output.

SYSPLEX

Shows sysplex related data.

VERSION

Includes the system version in the output.

Note: The CPF option will display everything that the CPFSTAT control option formerly provided.

The default is:

```
STATUS(BASE,JES,PASSWORD,FACMODE,CPF,SYSPLEX)
```

In z/VM this control option has the format:

```
STATUS
```

Status Output

The output of the TSS MODIFY(STATUS) command has headers in both upper and mixed case. Any header in mixed case denotes information not set by a control option but rather derived from the system.

The following details status values returned in the STATUS field:

ACTIVE

Connection to the remote node is active.

INACTIVE

Connection to the remote node is inactive.

SPOOL

The Journal file on the remote node has been defined.

NOSPOOL

The Journal file on the remote node has not been defined.

PRE50

No commands have been sent to the remote nodes yet. After the first is sent, PRE50 will no longer appear.

RETRY

Indicates attempts are being made to re-establish the connection to the remote node.

Examples: STATUS control option

This example determines complete information about the various CPF control options, as well as the current status of CPF and the nodes defined to it:

```
TSS MODIFY(STATUS(CPF))
```

This example generates a display of sysplex related data:

```
TSS MODIFY(STATUS(SYSPLEX))
```

SUBACID—Batch Job ACIDs

Valid on z/OS.

Use the SUBACID control option to indicate how CA Top Secret derives an ACID for batch jobs that are submitted by the following methods:

- Through an online terminal
- From another batch job
- From a started task

All entry methods are accepted.

This control option has the following format:

```
SUBACID(J|U,n)
```

SUBACID(J,n**)**

Indicates that the first n characters of the jobname parameter on the job card is used as the ACID, unless USER=acid is present.

Specifying SUBACID(J,7) restricts jobnames to the user's userid plus one character. This will occur unless the user is explicitly PERMITted to submit other ACIDS.

SUBACID(U,n**)**

Indicates that the first n characters of the logged on user's ACID, or of the ACID associated with the started task, is used as the ACID for the batch job.

Default: SUBACID(U,7).

Application of SUBACID

SUBACID only applies to jobs issued through an internal reader. It does NOT apply to jobs submitted via remotes, nodes, or local readers.

CA Top Secret uses settings for the JOBACID and DEFACID control options to derive ACIDS for jobs issued from physical card readers or NJE and RJE remote readers. For information, see JOBACID or the DEFACID suboption of the FACILITY control option.

SUBACID Algorithm

The following algorithm assumes that the JES control option is set to JES(NOVERIFY).

This indicates that the JES Early Verify feature is not in effect. In FAIL mode, all jobs must have an ACID in order to be processed by CA Top Secret.

JES Early Verify Feature

If IBM's JES Early Verify feature is active (JES(VERIFY) control option is set), then jobs submitted through TSO is checked for valid USER and PASSWORD specification as part of job submission. CA Top Secret will not insert USER= or PASSWORD= as described in the algorithm. The job will run under the signed-on User's ACID if USER= is the same as the TSO userid.

SUBSYS—Modify Defaulting Subsystem Name

Valid on z/OS

Use the SUBSYS control option to modify the TSS subsystem name that defaults to TSS. The modified subsystem name must be in the format TS*xx*.

This control option uses the SYS1.PARMLIB member CAITSSxx entry method.

This control option has the following format:

```
SUBSYS(TSxx)
```

xx

Specifies the name of the subsystem that defaults to TSS.

Range: 1 to 2 nonblank alphanumeric characters

SVCDUMP—System Dump

Valid on z/OS.

Use the SVCDUMP control option to produce a system dump of the CA Top Secret region.

This control option uses the O/S or TSS MODIFY commands entry methods.

This control option has the following format:

```
SVCDUMP
```

The SVCDUMP option is primarily provided to aid in CA Top Secret problem determination. An un-formatted dump of the CA Top Secret region is written to an available SYS1.DUMPxx data set.

SWAP—Program Swapping

Valid on z/OS.

Use the SWAP control option to control the swapping (transfer of programs between main memory and auxiliary storage) of the CA Top Secret address space by the z/OS operating system.

All entry methods are accepted.

This control option has the following format:

```
SWAP(YES|NO)
```

YES

Allows z/OS to swap CA Top Secret address space.

NO

(Default) Makes the CA Top Secret address space non-swappable.

z/OS and PPT

Use this option instead of the z/OS Program Properties table to make the CA Top Secret address space non-swappable.

Increased CA Top Secret Command Response Time

The CA Top Secret address space is extremely busy during the implementation phase or whenever a large volume of TSS commands is being processed. To minimize paging, and increase response time during implementation, enter the SWAP(NO) option to make the CA Top Secret address space non-swappable.

Paging

z/OS uses a technique known as Paging to allocate storage space in main memory. Paging enables z/OS to divide main memory into blocks of storage called Page Frames. Programs, like the one stored in the CA Top Secret address space, are divided into blocks of storage called pages. z/OS will only assign page frames to those pages of a program that are active. Inactive pages are stored on DASD until they are required to execute. When a page is required to execute, it is swapped into main memory and the page that has already executed is swapped out into auxiliary storage.

The CA Top Secret address space is active (swapped in):

- Whenever a user initiates or a job starts
- Whenever a password is changed (initiation only)
- For a violation statistics update/reset (initiation only)
- For the submission of a permitted ACID other than active user
- Whenever a TSS command is issued
- Every fifteen seconds (usually for logging/tracking) as specified by the TIMER control option default value
- Generally in IMPL mode for some data set violations.

SYNCH—Synchronize Tables

Valid on z/OS and z/VM.

Use the SYNCH control option to request the immediate synchronization of global in-memory tables (ALL, AUDIT, RDT, STC) with the Security File.

SYNCH is usually only required for processors in global DORMANT mode.

This control option uses the O/S or TSS MODIFY command entry methods

This control option has the following format:

```
SYNCH
```

Examples: SYNCH control option

This example synchronizes in-memory tables (ALL, STC, AUDIT) with the Security File:

```
TSS MODIFY(SYNCH)
```

This example uses the SYNCH option with the OS command:

```
F TSS,SYNCH
```

SYSOUT—Diagnostic Log

Valid on z/OS and z/VM.

Use the SYSOUT control option to spin off a CA Top Secret diagnostic log (DDNAME=$$LOG$$) and specifies the SYSOUT class and destination for the log.

Note: If this parameter is entered more than once in the Parameter File, the first entry is used.

All entry methods are accepted.

In z/OS this control option has the following format:

SYSOUT(*class*,*dest*)

class

Identifies the JES SYSOUT class for diagnostic log output.

dest

Indicates the destination of the diagnostic log output.

Default: SYSOUT(A,LOCAL)

In z/VM this control option has the format:

```
SYSOUT(userid)
```

userid

Specifies the userid of the virtual machine to receive the console log and server dumps.

Default: SYSTEM

Example: SYSOUT control option

This example:

- Causes the class and destination of the diagnostic log to be changed to class B and routed to REMOTE1, and the output is written after the command is issued.
- Spins off the CA Top Secret diagnostic log. Specifies the SYSOUT class and destination used the next time the SYSOUT option is specified.

```
TSS MODIFY('SYSOUT(B,REMOTE1)')
```

SYSPLEX—XES and XCF Availability

Valid on z/OS.

Use the XES and XCF SYSPLEX control options to make the capabilities of both XES and XCF available.

XES is the z/OS Coupling Facility service that allows sharing of data across the SYSPLEX. CA Top Secret uses an XES list structure to share file blocks between all connected systems. XES enables CA Top Secret to share data between systems joined to the Coupling Facility sharing the same Security File.

XCF is a message routing facility, used by CA Top Secret to propagate commands issued on one system to all the other connected systems. XCF enables CA Top Secret to send TSS MODIFY commands to other systems in the sysplex joined to the sending-systems' group. XCF can be active even when XES is not used. This is the case when the CONNECT command only has a group-name but no structure-name.

Note: There is no CONNECT parameter. The Coupling Facility is connected implicitly when the SYSPLEX control option is used for the connect process.

This control option uses the Parameter file and O/S or TSS MODIFY command entry methods.

This control option has the following format:

```
SYSPLEX(connect-name,group-name,structure-name)
        |(DISCONNECT[XES])
        |(TRACE(ON|OFF))
```

connect-name

Indicates the connection by which this system is known. A connect-name can be any alphanumeric combination. If a connect-name is not specified, CA Top Secret substitutes the SMFID in this field and adds an alpha prefix, “S”, to ensure a valid connect-name.

Range: Up to 16 bytes

group-name

Indicates the group to which the system belongs in the sysplex. The group-name can be any alphanumeric combination. Providing a group name is optional.

Range: Up to eight bytes

structure-name

Indicates the List structure being used to contain the Security File in the Coupling Facility. The structure-name has no default and can be alphanumeric combination.

Range: Up to 16 bytes

DISCONNECT

Without specifying any options, informs CA Top Secret to disconnect from both XES and XCF. If you specify:

- XES—Informs CA Top Secret to disconnect from only XES.
- XCF—Informs CA Top Secret to disconnect from only XCF.
- **Note:** If a system that is connected to the Coupling Facility is manually disconnected from the structure, all other connected systems are forced to disconnect.

No re-connect is attempted until a new structure is allocated in the Coupling Facility by a manual CONNECT command. To determine if a structure was reallocated, use the TSS MODIFY(STATUS(SYSPLEX)) command, or the D XCF,STR z/OS operator command.

An XES connection without an XCF connection is allowed.

TRACE

Activates (ON) or deactivates (OFF) a trace of all calls to the Coupling Facility. There are two messages issued:

- TSS9731—Issued before the call to the Coupling Facility, and gives the function and the RBA (relative block address) that is being processed.
- TSS9732—Gives the return and reason codes provided by the Coupling Facility.

Default: SMFID.

Examples: SYSPLEX control option

This examples connects to XCF only, and enables CA Top Secret to initiate using the Coupling Facility:

```
F TSS,SYSPLEX(SYSTEM1,GROUP1)
```

In this example, SYSTEM1 connects to GROUP1, and will connect to XCF only.

This example uses the default SMFID that is SYSTEM1.

```
F TSS,SYSPLEX(,GROUP1)
```

In this example, the system connects to GROUP1 as SYSTEM1.

Note: The comma (,) in the first position represents the skipped connect-name field, which is the default: SMFID.

This example uses a structure and activates CA Top Secret 's use of the Coupling Facility:

```
F TSS,SYSPLEX(,GROUP1,SECURITY3)
```

This example to connect to XES only:

```
SYSPLEX(,,structure)
```

TAPE—Tape Protection

Valid on z/OS.

Use the TAPE control option to specify the type of tape protection (if any) in effect at the installation.

This control option has the following format:

```
TAPE(OFF|DSNAME|DEF)
```

OFF

(Default) z/OS will not invoke CA Top Secret to validate a tape access request. TAPE(OFF) is used to indicate the use of external tape management packages such as TMS or TLMS.

DEF

CA Top Secret will validate access requests for defined volumes only.

DSNAME

CA Top Secret will perform data set name checking using the full data set name supplied on the DSNAME keyword of the JCL. If CA Top Secret cannot determine what the DSNAME is, such as when creating an NL tape from an SL tape, CA Top Secret supplies a data set name of:

```
$$.UNKNOWN.TAPE.DSN
```

If you encounter this problem, you will need to add a PERMIT for this data set name as follows:

```
TSS PERMIT(ALL) DSNAME($$.UNKNOWN.TAPE.DSN)
                ACCESS(ALL)
```

Appropriate Settings for TAPE Option

- Set TAPE(OFF) for BrightStor™ CA-1® (TMS) with the BrightStor CA-1 interface active and BrightStor™ CA-TLMS.
- Set TAPE(DSNAME) for CA-Tape.

See the *User Guide* for detailed descriptions of volume security and tape data set security.

Examples: TAPE control option

The following table details individual option to enter and its result:

Enter:	To:
TAPE(DEF)	Protect defined volumes only
TAPE(DSN)	Use CA Top Secret to protect tape data sets
TAPE(OFF)	To indicate the use of a TLMS or TMS interface
TAPE(DSN)	To use CA Tape

TEMPDS—Protect Temporary Data Sets

Valid on z/OS.

Use the TEMPDS control option to allow an installation to determine whether temporary data sets are protected.

All entry methods are accepted.

This control option has the following format:

```
TEMPDS(YES|NO)
```

YES

Indicates that temporary data sets are treated like any other data set and users must be permitted to access them. The following example authorizes users to have ALL access to temporary data sets with the prefix SYS in the ALL Record. These data sets can be audited.

```
TSS PERMIT(ALL) DSNAME(SYS9++++.T++++++.RA)
                ACCESS(ALL)
```

NO

(Default) Indicates that temporary data sets are not protected, and cannot be audited.

Example: TEMPDS control option

This example indicates that temporary data sets are not protected and, consequently, cannot be audited.

```
TSS MODIFY(TEMPDS(NO)
```

TEXTTSS—Report and Message Text

Valid on z/OS.

Use the TEXTTSS control option to replace the string CA Top Secret in reports and messages. Any string may be used.

Note: This is the only control option that allows spaces between words.

All entry methods are accepted.

This control option has the following format:

TEXTTSS(*replacement text*)

replacement text

The string which replaces the words CA Top Secret in reports and messages.

Range: Up to 24 characters

Default: CA Top Secret

Example: TEXTTSS control option

This example in the parameter:

```
*

* sample control options

*

TEXTTSS(CAI ACCESS CONTROL)
```

Causes startup message TSS9000I to be displayed as:

TSS9000I CAI ACCESS CONTROL INITIALIZATION COMPLETE.

TIMELOCK—Lock Interval

Valid on z/OS.

Use the TIMELOCK control option to control the interval at which CA Top Secret will attempt to obtain the Security File lock or an acid enqueue.

All entry methods are accepted.

This control option has the following format:

TIMELOCK(*nnn1*,*nnn2*,*nnn3*,*nnn4*)

The operand values are specified as whole numbers with up to four digits in each.

nnn1

The number of .01 second units between tries for the lock.

nnn2

The number of retries for the lock.

nnn3

The number of retries for an acid enqueue.

nnn4

The number of retries for the lock after it is determined that a BACKUP is in progress.

Default: (25,64,128,1200). The default value specifies a retry for the lock every 25 hundredths of a second (every quarter second), and that the TSS9123A message is issued after 64 tries. Thus, it takes 16 seconds of trying for the lock before the TSS9123A message is issued. When trying to obtain an acid enqueue, the third parameter (128) is used. The TSS9122I message is issued after the first 128 tries (32 seconds), and the ENQ variation of the TSS9123A message after another 128 tries (32 seconds). If a backup is in progress on another system, the TSS9125I message is issued when the first 16 seconds (from the second parameter) expires, and the TSS9123A message is issued after an additional 1200 tries, or 300 seconds, based on the fourth parameter.

Example: TIMELOCK control option

It is not recommended that changes be made to any of the default values. However, the following illustrate some circumstances under which you may wish to change them.

If the backup consistently takes longer than 300 seconds (5 minutes), and the TSS9123A message is always seen, the fourth parameter can be increased. A value of 1800 would allow 450 seconds (7.5 minutes) (after the first 16 seconds) for the backup:

```
TIMELOCK(25,64,128,1800)
```

If the Security File is shared among several systems, but the total amount of I/O from all of the systems is well under the capacity of the device, significant time may be lost to lock contention due to the quarter second delay any time the attempt to get the lock fails. In this case, reducing the first parameter will have little effect on the average response time for a security request but may reduce the peak response time considerably. If the first parameter is reduced, the second, third, and fourth should be increased so that the time intervals before issuing the messages remains constant. For example:

```
TIMELOCK(10,160,320,3000)
```

The two previous examples can be combined as follows:

```
TIMELOCK(10,160,320,4500)
```

TIMER—AUDIT/TRACKING File Write Interval

Valid on z/OS and z/VM.

Use the TIMER control option to control the interval at which data is written from CA Top Secret buffers to the AUDIT/TRACKING file. This includes writing IMS and CICS transaction events to SMF.

All entry methods are accepted.

This control option has the following format:

TIMER(*nnn*)

nnn

Time interval in seconds.

Range: 10 to 300

Default: 15

Example: TIMER control option

This example forces CA Top Secret to write from CA Top Secret buffers every 45 seconds:

```
F TSS,TIMER(45)
```

TNGMON—Error Messages

Valid on z/OS.

Use the TNGMON control option to set and activate error messages sent to a Unicenter console.

You can identify one or many Windows NT machines as CA Common Services monitors. However, you can also identify other CA Common Services monitors from within CA Common Services.

Considerations:

- Sending error messages to multiple Unicenter monitors affects the performance of your z/OS system and increases work traffic. Identifying multiple Unicenter TNG monitors ensures that you will always have at least one CA Common Services monitor up and running.
- Identifying additional Unicenter monitors from within CA Common Services is easy, and it lets you create filters and calendars to route error messages more efficiently. For more details, see the *Getting Started* for CA Top Secret WorkStation.

All entry methods are accepted.

This control option has the following format:

```
TNGMON(ON|OFF) (ADDTO|REMOVE, ip address[,DEBUG])
```

ON

Enables the TNG monitor to send error messages to a Unicenter console. If the monitor is on, and there are no TNG monitor table entries, the monitor does not process any data. The same is true if the table has entries but monitor is off.

OFF

Disables the TNG monitor from sending error messages to a Unicenter console.

ADD

Indicates that a new IP address is added to the TNG monitor table.

CA Top Secret will not allow duplicate entries to the TNG monitor table. If an entry is added that already exists, CA Top Secret recognizes its existence and returns a MODIFY FUNCTION SUCCESSFUL.

REM

Indicates that an IP address is removed from the TNG monitor table.

If you remove the last entry in the TNG monitor table, and the internally used entry count is set to zero, the TNG monitor is automatically placed in an off status.

Note: The REM function used with DEBUG only removes the DEBUG function, not the IP address.

ip address

Identifies the PC address for which CA Top Secret violations are sent.

TSS—Console Prompts

Valid on z/OS.

Use the TSS control option to generate prompts at the operator console for the operator to enter emergency CA Top Secret commands. Commands entered using this method are audit events and are recorded. To avoid flooding the console command output is limited to 50 lines.

To protect secure data from being posted on the system, log command output is routed to the console only. Command input requires the entry of the MSCA previous password at the console. To avoid security exposure, end the session after the needed commands are complete.

All entry methods are accepted.

This control option has the following format:

```
TSS
```

Protection

The TSS control option is protected by a special prompt for the MSCA's previous password. A record of the event is recorded to provide an audit trail.

TSS Command Entry

This command is designed mainly for entry from the system console:

```
F TSS,TSS
```

However, it may also be entered as a command:

```
TSS MODIFY(TSS)
```

or from PARMLIB:

```
TSS
```

An operator console prompt requests the MSCA previous password:

TSS9273A ENTER TSS COMMAND PASSWORD

After successful entry of this password, a second prompt allows the entry of any CA Top Secret command:

TSS9690A ENTER <TSS COMMAND> OR <END>

The command is entered as a console response, including the initial TSS keyword.

Example: TSS control option

This example enters a TSS command function at the O/S console:

1. Enter:
   ```
   F TSS,TSS
   ```
   The system displays:
   ```
   TSS9691A ENTER TSS COMMAND PASSWORD
   ```
2. Enter the MSCA's previous password:
   ```
   R xx,password
   ```
   If this password is correct, the system displays:
   ```
   TSS9272A ENTER <TSS COMMAND> OR <END>
   ```
3. Enter the TSS command function:
   ```
   R xx,TSS ADDTO(USER01) DSNAME(ABC.DEF)
   ```

Note: If this command is entered from anywhere else but the O/S console, a prompt at the console awaits a response.

TSSCMDOPTION—Command Defaults

Valid on z/OS.

Use the TSSCMDOPTION control option to allow users to establish default settings for TSS command specific options. The options can be in any order, however the right most takes precedence.

All entry methods are accepted.

This control option has the following format:

```
TSSCMDOPTION (option1,option2,…)
```

TSSCMDOPTION Valid Options

ADMINBY|NOADMBY

ADMINBY

When enabled, CA Top Secret records and lists information in ACID security records to indicate the:

- Administrative ACID who performed the change
- Date, time, and system SMFID where the change was performed

ADMINBY data is stored each time an ACID is created, a FACILITY is added, or a resource is permitted.

When ADMINBY is turned on:

- 20 additional bytes are required to store the ADMINBY information for the acid being permitted in the owning acid of the resource
- Additional I/O may be required to record the administration time—stamp
- The LIST command looks for ADMINBY information, but only prints this output if it is present in the security record

NOADMNBY

(Default) Suppresses the administrative date—time stamp storage and LIST display.

TERSE|VERBOSE|ENHANCED

VERBOSE

(Default) Displays all the related hierarchy ACIDs information beyond the owning ACIDs And the full NAME attributes.

TERSE

Does not display the ADMINBY information, ACID hierarchy information beyond the owning ACID, or the full NAME attribute. This saves significant overhead in security file access and in CPU time expended.

ENHANCED

Displays all information included in VERBOSE plus:

- MASK attribute information on a PERMIT
- ACID type for target acid in an ADMIN SCOPE listing
- RDT attribute will display PIE for Prefixed resources

UNIQUSER—Assign a UID Automatically During OMVS Logon

Valid on z/OS.

Use the UNIQUSER control option to automatically assign a UID to any user who logs on to OMVS without an OMVS segment.

This control option has the following format:

```
UNIQUSER(ON|OFF)
```

ON

Assigns a UID to the signed-on session ACID of any user who logs on to OMVS without an OMVS segment. The assignment is equivalent to the UID being added by the administrator through a TSS command. If you have specified the MODLUSER control option, the ACID also receives OMVS segment information from the ACID that MODLUSER designates. If the DFLTGRP assigned to the session ACID has not been assigned a GID, a GID is automatically assigned to the DFLTGRP.

OFF

(Default) Prevents the automatic assignment of UIDs during OMVS logon.

Example: Activate Automatic Assignment of UIDs During OMVS Logon

This example activates the automatic assignment of UIDs during OMVS logon:

```
F TSS,UNIQUSER(ON)
```

More information:

MODLUSER—Identify an OMVS Model User (see page 150)

UNIXOPTS—Special Options for USS

Valid on z/OS.

Use the UNIXOPTS control option to control USS auditing and the maximum number of supplemental groups supported.

All entry methods are accepted.

This control option has the following format:

```
UNIXOPTS(MAXSGRPS=nnnn,DIRACC,DIRSCH,FSOBJ,FSSEC,IPOBJ,PROCACT,PROCESS)
UNIXOPTS(NONE)
```

MAXSGRPS

Specifies the maximum number of supplemental groups supported.

Range: 1 to 8192

Default: 300 (when MAXSGRPS is not specified or when UNIXOPTS is turned off)

DIRACC

Specifies if SMF records are cut for USS that control access checks for read/write access to directories. Some of the functions that access directories with read or write access are open, opendir, rename, rmdir, mount, mkdir, link, mknod, getcwd, and vlink. The Security Server callable services that control cutting this SMF record are ck_access and ck_owner_2_files.

DIRSCH

Specifies if SMF records are cut for USS that control directory searches. Some of the functions that search directories are chmod, chown, chaudit, getcwd, link, mkdir, open, opendir, stat, ttyname and vlink. The Security Server callable service that controls cutting this SMF record is ck_access.

Auditing directory searches generates an extremely large amount of SMF records in a short period of time.

FSOBJ

Specifies if SMF records are to be cut for USS that control the auditing of the creation and deletion of system objects. It also cuts SMF records for all access checks except directory searches. Some of the functions that do this are chdir, link, mkdir, open, mount, rename, rmdir, symlink, vmakedir, and vcreate. The Security Server callable services that control cutting of this SMF record are ck_access, ck_owner_2_files, ckpriv, makeISP, and R_audit.

FSSEC

Specifies if SMF records are cut for USS that control the auditing of changes to the security data (FSP) for file system objects. Some of the functions that modify the FSP are chaudit, chmod, chown, chattr, write, fchaudit, and fchmod. The Security Server callable services that control cutting of this SMF record are R_chaudit, R_chown, R_chmod, and clear_setid.

IPOBJ

Specifies if SMF records are cut for USS that control the auditing of the access control, IPC object changes, and the creation and deletion of IPC objects. Some of the functions that will do this are msgctl, msgget, msgsnd, semctl, semget, semop, shmat, shmget and shmctl. The Security Server callable services that control cutting of this SMF record are ck_IPC_access, R_IPC_ctl, and makeISP.

PROCACT

Specifies if SMF records are to be cut for USS that control the auditing of services that look at data from or effect other processes. Some of the functions that effect other processes are getpsent, kill, ptrace, recv, recvmsg and sendmsg. The Security Server callable services that control cutting of this SMF record are ck_process_owner and R_ptrace.

PROCESS

Specifies if SMF records are cut for USS that control the dubbing and undubbing of processes, changes to the UIDs and GIDs of processes, and changes to the thread limits and other privileged options. Some of the functions that dub processes or change process values are exec, setuid, setgid, seteuid, setegid, dub, undub, and vregister. The Security Server callable services that control cutting of this SMF record are R_exec, R_setuid, R_setgid, R_seteuid, R_setegid, ck_priv, initUSP, and deleteUSP.

NONE

Turns off all of the options.

Examples: UNIXOPTS control option

This example specifies that SMF records are to be cut for USS that control the auditing of changes to the security data (FSP) for file system objects and control access checks for read/write access to directories:

```
F TSS,UNIXOPTS(DIRACC, FSSEC)
```

This example specifies that SMF records are to be cut for USS that control the auditing of services that look at data from or effect other processes and also sets the maximum number of supplemental groups to 100:

```
TSS MODIFY(UNIXOPTS(MAXSGRPS=100,PROCACT))
```

This example specifies that all UNIXOPTS options are to be turned off:

```
TSS MODIFY(UNIXOPTS(NONE))
```

VERSION—Version Display

Valid on z/OS and z/VM.

Use the VERSION control option to display the version of CA Top Secret.

This control option uses O/S and TSS MODIFY commands the entry methods.

This control option has the following format:

```
VERSION
```

Example: VERSION control option

This example produces a version message:

```
F TSS,VERSION
```

TSS9660I VERSION= r.r *rr*SP*xx*AKO*nn*

rr

Specifies the release.

SP*xx*

Specifies the service pack level.

AKO

Specifies the Product Code.

nn

Specifies the version.

In z/VM the result is:

TSS0029I Version=12.0 SP0 Generated on 12/03/07 at 12:50:39 IPL: 0100

TSS0028I CP Version=12.0 SP0 Generated on 04/29/08 at 11:11:19

VSAMCAT—Catalog Volume Check

Valid on z/OS.

Use the VSAMCAT control option to bypass user catalog volume checks on VSAM data sets.

During VSAM data set creation, z/OS passes the volume number of the user catalog, rather than the volume(s) where the data set is going to be located. This necessitates permitting CREATE access to the user catalog volume although the data set is not placed there.

All entry methods are accepted.

This control option has the following format:

```
VSAMCAT(YES|NO)
```

YES

(Default) Continue to enforce checking the user for CREATE access to the user catalog.

NO

Skip the volume checking; data set checking will occur unchanged. This setting eliminates the need to grant users the authority to create data sets on the catalog volume.

VTHRESH—Access Violation Response

Valid on z/OS and z/VM.

Use the VTHRESH control option to:

- Select an access violation threshold for online users, batch jobs, and started tasks
- Select the action that CA Top Secret takes when the threshold is reached

This control option uses all entry methods.

This control option has the following format:

```
VTHRESH(nn,[NOT],[CAN],[WARN]),[SUS],[CAN],[WARN]
        ,[RES]
```

nn

Sets the maximum number of resource access violations that a user may accumulate during an online session or job execution. This operand must be specified when changing any of the action operands. Specifying a value of 0, signifies that no violation threshold processing is performed.

Range: 0 to 254

Default: 5

NOT

(Default) CA Top Secret issues a message at the security console and the user's terminal to notify the security administrator of a security violation.

CAN

For TSO: CA Top Secret will O/S CANCEL the TSO session or batch job, and will issue this message:

```
TSS7191E JOB/SESSION CANCELLED EXCESSIVE VIOLATIONS
```

- For non-TSO online sessions—CA Top Secret will prevent further access of any kind by locking the terminal. This forces the user to sign off. CA Top Secret will issue the message:
- TSS7192E SESSIONL LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF
- For CICS online sessions—CA Top Secret will cancel the session and issue following messages:

```
TSS7191E JOB/SESSION CANCELLED EXCESSIVE VIOLATIONS
TSS7192E SESSION LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF
```

SUS

For TSO: CA Top Secret will O/S CANCEL the session and suspend the violator's ACID.

For non-TSO online sessions: CA Top Secret will prevent further access of any kind. This forces the user to sign off.

RES

Resets actions SUS, CAN or WARN to NOT.

WARN

Indicates that CAN and SUS is enforced for users operating in WARN mode as well as in FAIL or IMPL.

The VTHRESH option is in effect during WARN, FAIL, and IMPL modes. CA Top Secret will not, however, SUSPEND or CANCEL violators during WARN mode unless VTHRESH(WARN) is set.

TSO users who reach the VTHRESH limit while in ISPF browse or edit is not suspended or cancelled until they leave the screen. VTHRESH operands are not in effect when TSS LOCK is active. You must specify TSS UNLOCK first. Then the VTHRESH options take effect after the next user action. If you want to change the SUSPEND suboption to CANCEL, you must specify the RES suboption first. This resets SUSPEND and CANCEL actions to NOT.

Examples: VTHRESH control option

This example suspends the ACID of any user who logs 3 or more violations:

```
F TSS,VTHRESH(3,SUSPEND)
```

This example changes the number of resource access violations to 6, but keep everything else the same:

```
F TSS,VTHRESH(06)
```

XCF(*)—Information to Remote Systems

Valid on z/OS.

Use the XCF(*) control option as the CA Top Secret “send” command to route information to all remote systems in the sysplex.

Note the following:

- XCF(*) must be entered as the last parameter on the TSS MODIFY command
- Single quotes are required, as shown in the above entry

This control option uses the MODIFY commands entry method.

This control option has the following format:

```
XCF(*)
```

Example: XCF(*) control option

This example updates the violation threshold on all systems in a group on a sysplex with the VTHRESH control option.

```
TSS MODIFY('VTHRESH (10,NOT), XCF(*)')
```