CA Top Secret® for z/OS

Quick Reference Guide

r15

Third Edition

CA Technologies Product References

This documentation set references the following CA products:

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

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Control Options (see page 45)—Added entries for CPFAUTOGID and CPFAUTOUID.

Contents

Chapter 1: Command Functions

This section contains the following topics:

Command Functions

Function	Use to:	Syntax
ADDTO	Assign resource ownership and attributes to an ACID Define started tasks Add a resource to the Audit Record Connect profiles to users Grant access to non-ownable installation-defined resources Add resource classes to the RDT Add fields to the FDT Assign PassTickets, Node, NETUAF and volume records to the NDT Identify which LUs can participate in APPC conversations	`TSS ADDTO(acid) KEYWORD[(operand)]`
ADMIN	Assign administrative capabilities to subordinate administrators.	`TSS ADMIN(acid) keyword(authority level)` `ACCESS(access level)`
CHKCERT	Display information about certificates.	`TSS CHKCERT DCDSN(input-data-set-name)` `PKCSPASS('pkcs#12-password')`
COMPARE	Compare the security records of two users.	`SS COMPARE(acid1) USING(acid2)`
CREATE	Define new ACIDs. Assign resource ownership and/or security attributes while creating the ACID.	`TSS CREATE(acid)`

Function	Use to:	Syntax
DEADMIN	Remove administrative capabilities. The formats, rules, and restrictions that apply to the ADMIN function also apply to the DEADMIN function.	`TSS DEADMIN(acid)`
DELETE	Remove an ACID's definition from the Security Record.	`TSS DELETE(acid)`

EXPORT	Export digital certificates to a new data set (DCDSN) after it has been added to a user.	`TSS EXPORT(acid) [DIGICERT(name)`
		`|LABLCERT(label-name)]`
		`DCDSN(output-datasetname)`
		`FORMAT(format type)`
		`PKCSPASS(PKCS#12 password)`

GENCERT	Generate a digital certificate and insert a CERTDATA profile record into the info-storage database.	`TSS GENCERT [{CERTAUTH|CERTSITE|acid}]`
		`DIGICERT(8-byte-name)`
		`{DCDSN(request-dataset-name)\}`
		`{SUBJECTN ('CN="common-name"`
		`T="title"`
		`OU="org unit-name1,`
		`org-unit-name2"`
		`O="org-name"`
		`L="locality"`
		`ST="state"`
		`C="country code"')}`
		`[NBDATE(mm/dd/yy)`
		`NBTIME(hh:mm:ss)]`
		`[NADATE(mm/dd/yy)`
		`NATIME(hh:mm:ss)]`
		`[KEYSIZE(nnnn)]`
		`[LABLCERT(label-name)]`
		`[ICSF|PCICC|DSA|NISTECC|BPECC]`
		`[SIGNWITH(acid,digicert)]`
		`[SIGNALG(SHA1|SHA256)]`
		`[KEYUSAGE(HANDSHAKE`
		`DATAENCRYPT DOCSIGN`
		`CERTSIGN KEYAGREE)]`
		`[ALTNAME('IP=num-IPaddress`
		`DOMAIN=net-domainname`
		`EMAIL=emailaddress`
		`URI=universal-resource-id')]`

GENREQ	Generate a PKCS#10 base64-encoded digital certificate request and write it to a data set.	`TSS GENREQ(acid) DCDSN(output-datasetname)`
		`DIGICERT(name) |`
		`LABLCERT(labelname)`

HELP	Provide basic information about the use of each TSS command function.	`TSS HELP OPERAND(function)`

Function	Use to:	Syntax
LIST	Display data from the security record of: ■ A specific ACID ■ All ACIDs that match a specific prefix ■ All ACIDs of a specific type ■ All ACIDs in a department, and/or division Display data from the AUDIT, STC, NDT, RDT, FDT, DLF, SDT, APPCLU and/or ALL Records	`TSS LIST ??????????`
LOCK	Lock a terminal so it cannot be used when unattended.	`TSS LOCK`
MODEL	Copy permissions from one acid to another acid.	`TSS MODEL USING(`*`modelacid`*`) ACID(`*`newacid`*`)` `[INTO(`*`datasetname(membername`*`))]`

MODIFY	Display the status of the global security environment.
	Enter, change, or display control options.
		To display the status of the security environment:
		`TSS MODIFY STATUS`
		To enter or change control options:
		`TSS MODIFY(control option [(suboption)])`

MOVE	Move an ACID from one department, division or zone to another
	Change a user, ZCA, DCA and/or VCA into an SCA
	Promote or demote the type of ACID
		`TSS MOVE(acid) DEPARTMENT(acid)`
		`|DIVISION(acid)|ZONE(acid)`
		`TYPE(acid)`

P11TOKEN	Manage Certificate and Keys	`TSS P11TOKEN` *`keyword keyword`*

PERMIT	Authorize ACIDS full or restricted access to resource they do not own.	`TSS PERMIT(`*`acid`*`) keyword(`*`p-fix`*`)`
		`ACCESS(`*`level`*`)`
		`keyword(`*`oper`*`)`

REFRESH	Renew the ACIDs in any address space in the security environment. Use in multi-user address spaces like CICS and IMS, where an ACID can have multiple instances of signed on users.	`TSS REFRESH[(`*`acid`*`) [JOBNAME(`*`job`*`|*)]]`

Function	Use to:	Syntax
REKEY	Create a new certificate from an existing certificate with a new public/private key pair.	TSS REKEY {*acid*|CERTAUTH|CERTSITE} [DIGICERT(*existing-id*)] [NEWDIGIC(*new-id*)] [NEWLABLC(*new-label*)] [KEYSIZE(*nnnn*)] [ICSF|PCICC|NISTECC|BPECC] [NBDATE({*not-before-date*) NBTIME(*not-before-time*)] [NADATE(*not-after=date*|) NADATE(*not-after-date*)] [LABLPKDS]
REMOVE	Remove ownership of the keyword specified in the ADDTO function. The functional opposite of ADDTO.	TSS REMOVE(*acid*) *keyword*[(*operand*)]
RENAME	Change the access ID of any ACID.	TSS RENAME(*acid*) ACID(*new acid*)
REPLACE	Change the values, names, or data of attributes or keywords assigned to ACIDs.	TSS REPLACE(*acid*) *attribute keyword(value*)
REVOKE	Revoke access to ownable resources when no longer needed, or when the access restrictions (levels and/or controls) must be changed. A command can revoke multiple permissions or one specific permission.	TSS REVOKE (*acid*) *keyword*(*p-fix*) ACCESS(*level*) *keyword*(*oper*)
ROLLOVER	Specify the original certificate to be superseded by the a certificate. The ROLLOVER sub-command is the final step in the REKEY command, rollover process.	TSS ROllOVER {*acid*|CERTAUTH|CERTSITE|} [DIGICERT(*old-cert-id*)] [NEWDIGIC(*new-cert-id*)] [Forcer]
SIGNALG	Specify a signing algorithm	TSS GENCERT SIGNALG(SHA1|SHA256)
UNLOCK	Unlock a terminal.	TSS UNLOCK
WHOAMI	Display complete ACID attributes.	TSS WHOAMI

Function	Use to:	Syntax
WHOHAS	Display all ACIDs that have access to a specified resource, facility, field, or attribute.	`TSS WHOHAS keyword(value|*) [DATA{literal}|Mask[,NOPREFIX]}`
WHOOWNS	Display the ACID that owns a specific resource Display the ACIDs that own each resource of a specific type	`TSS WHOOWNS keyword(prefix|TSS mode|*)`

Chapter 2: Command Function Keywords

This section contains the following topics:

Command Function Keywords

Keyword	Use to	Syntax
ACID	Give administrators authority to specify the authority levels to manage ACIDS. Cross authorize an ACID to submit jobs under another ACID.	`TSS ADMIN(acid) ACID (authority levels)` `TSS PERMIT(acid) ACID (acid)`

ACIDPRFX	List ACIDs that begin with a specified prefix.	`TSS LIST(ACIDS) ACIDPRFX(prefix)`
		`DATA(datatype(s))`
		`TYPE(acidtype)]`
		`[ZONE|DIVISION|DEPARTMENT(acid)]`

ACLST	Change, or remove access levels for the resource in the RDT Record.	`TSS ADDTO(RDT) RESCLASS(type)`
		`RESCODE(hex code)`
		`[ACLST(access level list)]`

ACTION	Assign action(s):
	■ To an ACID when access to a FACILITY is attempted
	■ Taken when access to a resource is attempted
		`TSS ADDTO(acid) FACILITY(facility)`
		`ACTION(AUDIT,NOTIFY,DENY)`
		`TSS PERMIT(acid) resource(prefix)`
		`ACTION(FAIL,AUDIT,NOTIFY,`
		`DENY,VMPRIV,PASSWORD,NODSNCHK,ADMIN,`
		`EXIT,REVERIFY)`
		`TSS REVOKE(acid) resource(prefix)`
		`ACTION(ADMIN)`

AFTER and BEFORE	Add a profile to a specific location in the order of profiles.	`TSS ADDTO(acid) PROFILE(new profile)` `AFTER|BEFORE(existing profile)`

ALTNAME	Specify the appropriate values for the SubjectAltname extension, of which values might be coded.	`TSS GENCERT(acid) ALTNAME('IP-address`
		`DOMAIN=internet-domain-name`
		`EMAIL=email-address`
		`URI=universal-resource-id')`

Keyword	Use to	Syntax
APPLDATA	Associate data with a particular PERMIT.	TSS PERMIT(*acid*) RESOURCE(*prefix*) APPLDATA(*data*)
ARCHIVE	Archive the permissions and resources of a user.	TSS DELETE|LIST(*acid*) ARCHIVE INTO(*datasetname*(*membername*))
ASSIZE	Maximum address space size	TSS ADD(*acidname*) ASSIZE(*nnnnnnnn*)
ASUSPEND	Remove the suspension of an ACID suspended for administrative reasons.	TSS REMOVE(*acid*) ASUSPEND
ATTR with FDT	Add or replace attributes to a field in the FDT Record.	TSS ADDTO(FDT) FDTNAME(*field name*) FDTCODE(*hex code*) MAXLEN(*40*) ATTR(*attribute list*)
ATTR with the RDT	Define or change a resource to the RDT Record with attributes.	TSS ADDTO(RDT) RESCLASS(*resource Type*) RESCODE(*hex code*) ATTR(*attribute*)
AUDIT	Allow an audit of ACID activity.	TSS ADDTO(*acid*) AUDIT TSS ADDTO(AUDIT) *res class(res name*) [ACCESS(level1, level2, …)]
AUTOUID	Automatically assign the next available number in a given range.	TSS ADDTO(*acid*) UID(?) RANGE(*xxx*,*xxx*)
BIND	Bind PKCS #11 certificate to token	TSS P11TOKEN BIND LABLCTKN(token name) TOKNDATA(userid,digicert) LABLCERT(certabel)|TOKNUSER(userid) [KEYUSAGE(PERSONAL|CERTSITE|CERTAUTH] [DEFAULT]
CALENDAR	Name a CALENDAR record Add, remove, replace, or list an existing calendar in the SDT Record Permit or revoke a CALENDAR to an ACID	TSS ADDTO(SDT) CALENDAR(*calname*) [YEAR(*yyyy*)] [DAYS(daywk1,,,)] [INCLUDE(*mm/dd*)] [EXCLUDE(*mm/dd*)]
CATEGORY	Define or remove categories to isolate users, data and resources within the organization.	TSS ADDTO(MLS) CATEGORY(*category name*)

Keyword	Use to	Syntax

CERTMAP	Associate a certificate name filter with an ACID and define the filter. TSS ADDTO CERTMAP identifies the ACID assigned to a user if a user's digital certificate matches the subject's distinguished name filter and/or the issuer's distinguished name filter specified in the command.	`TSS ADDTO(acid) CERTMAP(recid)`
		`SDNFILTR('subject-filter')`
		`IDNFILTR('issuer-filter')`
		`[LABLCMAP('32-byte label')]`
		`[DCDSN(data set name)]`
		`[TRUST|NOTRUST]`
		
		`TSS ADDTO(MULTIID) CERTMAP(recid)`
		`SDNFILTR('subject-filter')`
		`IDNFILTR('issuer-filter')`
		`CRITERIA(criteria-template)`
		`[LABLCMAP('32-byte label')]`
		`[DCDSN(data set name)]`
		`[TRUST|NOTRUST]`

CERTNSER	Specify the next serial number used by a certificate to sign another certificate.	`TSS REPLACE(acid) DIGICERT(8-byte name)` `CERTNSER(number)`

CHKADDRS	Enable address checking in tickets for a Kerberos server running on z/OS 1.13 or higher.	`TSS ADDTO(SDT) REALM(KERBDFLT)`
		`REALMNAME('kerberos realm name')`
		`MINTKTLF(minimum ticket life)`
		`MAXTKTLF(maximum ticket life)`
		`DEFTKTLF(default ticket life)`
		`KERBPASS(kerberos password)`
		`CHKADDRS`

CNFAPP	Specify the application variable that acts as a filter to assign users to an ACID.	`TSS ADDTO(acid) CRITMAP(recid)` `CNFAPP(application name)`
CNFUVAR	Specify user defined criteria that acts as a filter to assign users to an ACID.	`TSS ADDTO(acid) CRITMAP(recid)` `CNFUVAR(site variable list)`
COMMAND	Confine ACIDs to using a specific command or subset of commands	`TSS ADDTO(acid) COMMAND(fac,(cmd[(G,V)]))`
CONSOLE	Grant or remove an ACID's ability to modify control options.	`TSS ADDTO(acid) CONSOLE`

CRITERIA	Define additional criteria that act as a filter to assign users to a MULTIID.	`TSS ADDTO(MULTIID)CERTMAP(recid)`
		`SDNFILTR('subject filter')`
		`IDNFILTR('issuer filter')`

CRITMAP	Identify the additional criteria that act as a filter to assign an ACID to a user.	`TSS ADDTO(acid) CRITMAP(recid)`
		`SYSID(sys id)} {CNFAPP(appl name)}`
		`CNFUVAR(site variable list)}`

Keyword	Use to	Syntax
DATA with ADMIN	Remove administrators authority to list Security File information.	`TSS ADMIN(acid) DATA(authority level(s))`
DATA with WHOHAS	Interpret a resource name literally or as a mask.	`TSS WHOHAS resclass(resname)` `DATA(MASK|NOPREFIX|LITERAL)`

DATA with LIST	Specify which portion of a Security Record is listed.	`TSS LIST(acid|ACID) DATA(datatype(s))`
		`TYPE(USER|PROFILE|DEPARTMENT|DIVISION`
		`|ZONE|SCA|LSCA|ZCA|VCA|DCA)`

DAYS
(for ACIDs)
	Restrict access to a specific day(s) of the week.	`TSS ADDTO(acid) resource(prefix)`
		`FACILITY(facility name)`
		`DAYS(day-list)`

DAYS
(for SDT)
	Add, remove, or replace the days of the week in a calendar in the SDT Record.	`TSS ADDTO(SDT) CALENDAR(cal-name)`
		`[YEAR(yyyy)]`
		`[DAYS(days)]`
		`[INCLUDE(mm/dd,...]`
		`[EXCLUDE(mm/dd,...)]`

DCDSN with GENREQ	Specify the name of the data set into which the certificate request is written.	`TSS GENREQ(name) DCDSN(data set name)`

DCDSN with ADDTO	Specify the MVS data set containing the digital certificate.	`TSS ADDTO(acid) DIGICERT(name)`
		`DCDSN(dsname)`
		`[START(sdate)]`
		`[FOR (ddd)]`
		`[UNTIL(date)]`
		`[LABLCERT(labelname)]`
		`[TRUST|NOTRUST]`
		`[ICSF]`
		
		`TSS ADDTO(acid) CERTMAP(recid)`
		`SDNFILTER('subject dn filter')`
		`IDNFILTR('issuer dn filter')`
		`DCDSN(dsname)`

DCENCRY	Provide a key name to encrypt and decrypt passwords.	`TSS ADDTO(SDT) KEYSMSTR(XXX.XXXXXX.XXX)`
		`DCENCRY(CCCCCCCCCCCCCCC)`
		`[KEYMASK|KEYENCRY]`

DEFACC	Assign the default access used on a TSS PERMIT for a resource added to the RDT Record.	`TSS ADDTO(RDT) RESCLASS(resource Type)`
		`RESCODE(hex code)`
		`[DEFACC(access list)]`

Keyword	Use to	Syntax
DEFAULT	Specify that the digital certificate being added to a key ring is the default certificate for the key ring.	TSS ADDTO(*acid*) KEYRING(*8-byte name*) [LABLRING(*237-byte ring name*)] \{RINGDATA(*acid,digicert*)\} \{RINGDATA(CERTSITE,*digicert*)\} \{RINGDATA(CERTAUTH,*digicert*)\} [DEFAULT] [USAGE(PERSONAL|CERTSITE|CERTAUTH)]
DEFNODES	Maintain a list of default routing nodes for an individual ACID.	TSS ADDTO(acid) DEFNODES(oper,oper,...)
DEFTKTLF	Specify the default ticket life in the KERBDFLT REALM record in the SDT.	TSS ADDTO(SDT) REALM(KERBDFLT) REALMNAME('*kerberos-realmname*') MINTKTLF(*min-ticket-life*) MAXTKTLF(*max-ticket-life*) DEFTKTLF(*nnnnnnnnnn*) KERBPASS(*kerberos-password*) CHKADDRS
DEPARTMENT	Assign a new ACID to a department List data about ACIDs in a department	TSS CREATE(*user*|*profile*|DCA *acid*) NAME('*name*') FACILITY(*facname*) PASSWORD(*password*) DEPARTMENT(*acid*) TSS LIST(ACID|ACIDS DATA(*datatype*(s)) TYPE(USER|PROFILE|DCA) DEPARTMENT(*acid*)
DESCRIPT	Specify a description displayed with the LIST command function. Add a description to an existing calendar	TSS ADDTO(SDT) [CALENDAR(*cal-name*)] DESCRIPT(*descript-name*) [MAP(*map-name*)] [MASK(*mask-name*)] [RLP(*record-name*)] [SELECT(*select-name*)] [TIMEREC(*time-name*)]
DFLTGRP	Assign a default group to an ACID operating under OpenEdition z/OS.	TSS ADDTO(*acid*) DFLTGRP(*groupname*)
DFLTSLBL	Associate a default MLS SECLABEL label with a selected ACID.	TSS ADD|REMOVE(*acid*) SECLABEL(*label1*[,..,5]) [DFLTSLBL(*labeld*)]
DIGICERT	Identify a digital certificate.	TSS COMMAND(*acid*) DIGICERT(*name*) [DCDSN(*dsname*)]

Keyword	Use to	Syntax
DISPLAY	Define, change, or list the display value for the field in the FDT Record. Identify the field name associated with a given display value.	TSS ADDTO(FDT) DISPLAY(*fieldname*) FDTNAME(*field name*) FDTCODE(*hex code*) TSS LIST(FDT) DISPLAY('*display value*')
DIVISION	List data about ACIDs in a specific division Assign an ACID to a division	TSS CREATE(*dept acid*|VCA *acid*) TYPE(DEPARMENT|VCA) NAME('VCA or *Dept name*') DIVISION(*acid*) TSS LIST(ACID|ACIDS) DATA(*dataType*(s))
DSA	Specify that the key pair is generated using the Digital Signature Algorithm instead of the RSA algorithm.	TSS GENCERT(acid) DIGICERT(*8-byte name*) SUBJECTN(*subject-name*) [LABLCERT(*label name*)] [DSA] [TRUST|NOTRUST] [ICSF/PCICC]
DUFUPD	Add or remove the DUFUPD attribute to an ACID.	TSS ADDTO(*acid*) DUFUPD
DUFXTR	Add or remove the DUFXTR attribute to an ACID.	TSS ADDTO(acid) DUFXTR
EIMDOMAIN	Create an EIM profile on the SDT.	TSS ADDTO(SDT) EIMPROF(*eim-profile-name*) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXBINDDN(*name*) PRXBINDPW(*password*)
EIMLOCREG	Create an EIM profile on the SDT.	TSS ADDTO(SDT) EIMPROF(*eim-profile-name*) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXBINDDN(*name*) PRXBINDPW(*password*) TSS DELETE(SDT) EIMPROF(*eim-profile-name*)

Keyword	Use to	Syntax

EIMOPTION	Specify whether or not new connections may be established with the specified EIM domain.	`TSS ADDTO(SDT) EIMPROF(`*eim-profile-name*`)`
		`EIMOPTION(ON|OFF)`
		`EIMDOMAIN(`*name*`)`
		`EIMLOCREG(`*name*`)`
		`PRXLDAPHST(`*name*`)`
		`PRXBINDDN(`*name*`)`
		`PRXBINDPW(`*password*`)`
		
		`TSS DELETE(SDT) EIMPROF(`*eim-profile-name*`)`
		`EIMOPTION(ON|OFF)`
		`EIMDOMAIN(`*name*`)`
		`EIMLOCREG(`*name*`)`
		`PRXLDAPHST(`*name*`)`
		`PRXBINDDN(`*name*`)`
		`PRXBINDPW(`*password*`)`

EIMPROF	Specify the EIM profile name for the acid's EIM and PROXY user information.	`TSS ADDTO(SDT) EIMPROF(`*eim-profile-name*`)`
		`EIMOPTION(ON|OFF)`
		`EIMDOMAIN(`*name*`)`
		`EIMLOCREG(`*name*`)`
		`PRXLDAPHST(`*name*`)`
		`PRXBINDDN(`*name*`)`
		`PRXBINDPW(`*password*`)`
		
		`TSS DELETE(SDT) EIMPROF(`*eim-profile-name*`)`
		
		`TSS LIST(SDT) EIMPROF(`*eim-profile-name*`)`
		
		`TSS REMOVE(`*acid*`) EIMPROF`

ENCRYPT	Enable or disable levels of encryption.	`TSS ADD(SDT) REALM(KERBDFLT|`*f_realm*`)`
		`REALMNAME(`*realmname*`)`
		`ENCRYPT('[DES|NODES][DES3|NODES3]`
		`[DESD|NODESD][AES128|NOAES128]`
		`[AES256|NOAES256]')`
		`KERBPASS(`*password*`)`
		`CHKADDRS`
		
		Note: CHKADDRS is used only with the local realm.
		
		`TSS ADD(`*acid*`) KERBNAME(`*kerbname*`)`
		`ENCRYPT('[DES|NODES][DES3|NODES3]`
		`[DESD|NODESD][AES128|NOAES128]`
		`[AES256|NOAES256]')`

Keyword	Use to	Syntax

ENCRYPT	Override the value of ENCRYPT for the local REALM and set the certificate encryption level available to a particular user.	`TSS ADDTO(SDT) REALM(KERBDFLT|f_realm)`
		`REALMNAME(realmname)`
		`KERBPASS(password)`
		`[ENCRYPT('[DES|NODES][,DES3|NODES3]`
		`[,DESD|NODESD] [AES128|NOAES128]`
		`[AES256|NOAES256]')]`
		`CHKADDRS`
		Note: CHKADDRS is used only with the local realm.
		`TSS ADDTO(acid) KERBNAME(kerbname)`
		`[ENCRYPT('[DES|NODES][,DES3|NODES3]`
		`[,DESD|NODESD] [AES128|NOAES128]`
		`[AES256|NOAES256]')]`
		`[MAXTKTLF(ticket-life)]`

EXCLUDE	Add, remove, or replace a list of dates that are specifically excluded from the calendar record in the SDT Record.	`TSS ADD(SDT) CALENDAR(cal-name)`
		`[YEAR(yyyy)]`
		`[DAYS(days)]`
		`[INCLUDE(mm/dd,...]`
		`[EXCLUDE(mm/dd,...)]`

EXPIRE	Remove an expiration that had been set using the FOR or UNTIL parameters.	`TSS REMOVE(acid) EXPIRE`

FACILITY	Specify which facility or facilities an ACID may or may not access
	Give or remove administrators authority to administer the use of facilities
	Permit an ACID to have access to a resource through the specified facility
		`TSS ADMIN(acid) FACILITY(facility name(s))`
		`TSS ADDTO(ACID|ALL)`
		`FACILITY(fac,fac,.. | ALL)`
		`TSS PERMIT(acid) resource(prefix(es))`
		`FACILITY(facility name)`

FDTCODE	Allow the administrator to list data from the FDT Record
	Add user-defined field names to the FDT Record
		`TSS LIST(FDT) FDTCODE(code)`
		`TSS ADDTO(FDT) FDTNAME(field name)`
		`FDTCODE(hex code)`
		`MAXLEN(nnnnn)`

FDTNAME	List data from the FDT Record about how the specified field is processed
	Add or remove user-defined field names to or from the FDT Record
		`TSS LIST(FDT)`
		`FDTNAME(field name)`
		`TSS ADDTO(FDT) FDTNAME(fieldname)`
		`FDTCODE(hex code)`
		`MAXLEN(nnnnn)`

FIRST	Enable an administrator to add a profile to the beginning of a profile list.	`TSS ADDTO(acid) PROFILE(new profile)` `FIRST`

Keyword	Use to	Syntax
FOR	Specify the number of days that an ACID may be used before it expires Specify a period of time during which an ACID is suspended Specify the number of days that an ACID is permitted to access a resource	`TSS PERMIT|ADDTO(acid) FOR(day-count)`

FORCER	Bypass checks and perform the rollover unconditionally.	`TSS ROLLOVER(acid) DIGICERT(TEST)`
		`NEWDIGIC(NEWTEST)`
		`FORCER`

FORMAT	Specify the output format when exporting a digital certificate to an output data set.	`TSS EXPORT(acid) DIGICERT(name)`
		`DCDSN(dsname)`
		`FORMAT(format-type)`
		`PKCSPASS(PK12 password)`

GAP	Specify that a profile is, or will cease to be, globally administered.	`TSS ADDTO(profile acid) GAP`

GID	Assign a numeric value to an ACID of type GROUP for security within USS.	`TSS MODIFY(OMVSTABS)`
		`TSS ADD(acid) GID(USS_group_id)`
		`TSS ADD(acid GID(?)`
		`[RANGE(low-gid,high-gid)]`

GROUP	Add or remove groups from an ACID.	`TSS ADDTO(acid) GROUP(group acid,...)`
HOME	Add or remove a HOME (subdirectory) to an ACID.	`TSS ADDTO(acid) HOME(subdirectory)`

ICSF	Indicate that the generated private key is placed in ICSF.	`TSS GENCERT(ACID) DIGICERT(8-BYTE NAME)`
		`ICSF`
		`TSS REKEY(acid) DIGICERT(8-byte name)`
		`DCDSN(dsname)`
		`ICSF`

IDNFILTR	Specify the significant portion of the issuer's distinguished name used as a filter when associating an ACID with a digital certificate.	`TSS ADDTO(acid) CERTMAP(recid)` `IDNFILTR('issuer-dnfilter')`
IESF1	Assign attributes to an interactive user interface.	`TSS ADDTO(acid) IESFL1(BAT,PSL,COD,VSAM)`
IESF2	Assign attributes to an interactive user interface.	`TSS ADDTO(acid)` `IESFL2(BQA,ESC,COU,CMD,OLPD,XRM)`

Keyword	Use to	Syntax
IESINIT	Assign an application profile name initiated when the interactive interface user signs on.	`TSS ADDTO(acid) IESINIT(profname)`
IESSYNM	Assign an interactive user interface ID used as a model for synonyms.	`TSS ADDTO(acid) IESSYNM(userid)`
IESTYPE	Assign a user type to an Interactive user Interface.	`TSS ADDTO(acid) IESTYPE(USERTYPEx,NEW,SELECT)`
IESVCAT	Assign a default VSAM user catalog for an Interactive User Interface user.	`TSS ADDTO(acid) IESVCAT(usercat)`

IMPORT	Import certificate from PKCS #11 token	`TSS P11TOKEN IMPORT LABLCTKN(token name)`
		`TOKNDATA(userid,digicert)`
		`SEQNUM(nnnnnnnn)`
		`[WITHLABL(certificate label)]`
		`[PCICC(pkds label)]`
		`[ICSF(pkds label)]`

IMSMSC	Determine the level of security in effect for inbound transactions in an IMS Multiple Systems Coupling (MSC) environment.	`TSS ADDTO(region acid)` `IMSMSC('MSClink(acid|+USER|+DEFAULT),.')`

INCLUDE	Add, remove, or replace the list of dates that are specifically included in the calendar record in the SDT Record.	`TSS ADD(SDT) CALENDAR(cal-name)`
		`[YEAR(yyyy)]`
		`[DAYS(days)]`
		`[INCLUDE(mm/dd,...]`
		`[EXCLUDE(mm/dd,...)]`

INSTDATA	Record or remove information about an ACID.	`TSS ADDTO(acid) INSTDATA('install data')`
ISSUERDN and SERIALNUMs	Identify a digital certificate	`TSS LIST(ACID) SERIALNUM(serial-number)` `ISSUERDN('issuer-dist-name')`
JOBNAME	Allow a specific data set to be brought into hyperspace if accessed by one of the jobs in the JOBNAME list.	`TSS ADDTO(DLF) DSNAME(SYS1.)` `JOBNAME(job1,job2,...)`

KERBLINK	Define Kerberos foreign principal users to the Secureway Server Network Authentication Service
	Map foreign principal names to user IDs on local z/OS system
		`TSS ADDTO(SDT) KERBLINK(link_name)`
		`LINKNAME(fully-qualified-name)`
		`KERBUSER(local_acid)`

Keyword	Use to	Syntax
KERBNAME	Specify local principals as CA Top Secret users.	TSS ADDTO(*acid*) KERBNAME('*kerberos-pname*') [ENCRYPT('[DES|NODES][,DES3|NODES3] [,DESD|NODESD] [AES128|NOAES128] [AES256|NOAES256]')] [MAXTKTLF(*max-ticket-life*)]
KERBPASS	Use as a password which must be supplied by a foreign system when the network authentication service connection is initiated.	TSS ADD(SDT) REALM(KERBDFLT|foreign_realm) REALMNAME(*realmname*) ENCRYPT('[DES|NODES][DES3|NODES3] [DESD|NODESD][AES128|NOAES128] [AES256|NOAES256]') KERBPASS(*password*) CHKADDRS **Note:** CHKADDRS is used only with the local realm.
KERBPASS	Specify the value of the REALM record password and is applicable to all REALM (local and foreign) SDT definitions.	TSS ADDTO(SDT) REALM(KERBDFLT) REALMNAME('*kerberos-realm*') MINTKTLF(*min-ticket-life*) MAXTKTLF(*max-ticket-life*) DEFTKTLF(*def-life*) KERBPASS(*kerberos-password*) CHKADDRS TSS ADDTO(SDT) REALM(*realm-label*) REALMNAME('*qualified-name*') KERBPASS(*password*)
KERBSEGM	SDT record created when a Kerberos principal user is defined.	TSS LIST(SDT) KERBSEGM(*acid*|ALL)
KERBUSER	Map foreign principal names to individual user IDs.	TSS ADDTO(SDT) KERBLINK(*label-name*) LINKNAME('*qualified-name*') KERBUSER(*userid*)
KERBVIO	Count unsuccessful to use a Network Authentication Service key.	TSS REMOVE(*acid*) KERBVIO
KEYRING	Add a key ring to an individual user. List information about a keyring.	TSS ADDTO(acid) KEYRING(*8-byte-ring-name*) TSS LIST(SDT) KEYRING(ALL)
KEYSIZE	Specify the size of the private encryption key in decimal bits.	TSS REKEY(*acid*) KEYSIZE(*keysize*)
KEYSMSTR	Provide a key name to encrypt and decrypt passwords.	TSS ADD(SDT) KEYSMSTR(LDAP.BINDPW.KEY DCENCRY(*CCCCCCCCCCCCCCC*) [KEYMASK|KEYENCRY]

Keyword	Use to	Syntax
KEYUSAGE	Specify the appropriate values for the KeyUsage certificate extension, of which of the values might be coded.	TSS GENCERT(*acid*) KEYUSAGE(HANDSHAKE|DATAENCRYPT|DOCSIGN |CERTSIGN)
LABLCERT	Specify a label associated with a certificate.	TSS ADDTO(*acid*) DIGICERT(*name*) DCDSN(*dsname*) LABLCERT(*label name*)
LABLCMAP	Specify the label associated with the digital certificate filter.	TSS ADDTO(*acid*) CERTMAP(*recid*) SDNFILTR('*subject-dfilter*') IDNFILTR('*issuer-filter*') LABLCMAP('*32-byte label*')
LABLPKDS	Specify a label associated with the certificate private or public key being stored into the ICSF storage facility.	TSS ADDTO(*acid*) LABLPKDS(*PKDSlabelname/**)
LABLRING	Specify a 237 byte label to associate with the key ring.	TSS LIST(acid) {KEYRING(*8-byte ring name*)} {LABLRING(*237-byte ring label*)}
LANGUAGE	Assign or remove a language preference code passed to the message processing Installation Exit.	TSS ADDTO(*acid*) LANGUAGE(*c*)
LDAPDEST	Add, remove, or replace nodes to the LDAP node list of an ACID record.	TSS ADDTO(*acid*) LDAPDEST(*node,node,,*) TSS REMOVE(*acid*) LDAPDEST(*node,node,,*) TSS REPLACE(*acid*) LDAPDEST(*node,node,,*)

Keyword	Use to	Syntax
LDAPNODE	Define LDAP nodes to the CA Top Secret database as NDT node elements.	TSS ADDTO(NDT) LDAPNODE(*node_name*) ACTIVE(YES|NO) ADMDN(*LDAP admin d name*) ADMPSWD(*LDAP admin password*) APPLNAME(*application name*) BITDEFLT(*bit field format*) BROADCAST(YES|NO) CHILDELETE(YES/NO) DATEFMT(*date format*) DEBUG(YES/NO) EXTENDED(YES/NO) LABLCERT(*label name*) USERDNS(*D Name suffix*) JOURNAL(YES|NO) RECOVERY(YES/NO) SYNCADD(YES|NO) SYNCDEL(YES|NO) SYNCUPD(YES|NO) OBJCLASS(*LDAP object class*) PSWDASIS(YES|NO) SYSID(*sysid1,sysid2,,,*) URL(*UResource Locator*) XREF(*ACIDfield1,LDAPattrib1Name,* *LDAPattrib1FieldType,* *LDAPattrib1DataFormat,* *LDAPattribLength*)
LDS	Add or remove the LDS attribute to or from an ACID record.	TSS ADDTO|REMOVE(*acid*) LDS
LDSYSID	Define LDS global options to the database as NDT LDSYSID elements.	TSS ADDTO(NDT) LDSYSID(*system smfid*) DEBUG(YES/NO) RETRY(*nnn*) TIMEOUT(*nnn*) JOURNAL(YES/NO) JOURNALDSN(*dsname*) KEYRING(*ring_name*)
LIBRARY	Specify libraries or library prefixes in which a privileged program must reside.	TSS PERMIT(*acid*) DSNAME(*p-fix*) PRIVPGM(*p-fix*) LIBRARY(*p-fix*)
LINKID	Identify which LUs can be used for APPC conversation processing.	TSS ADDTO(APPCLU) LINKID(*netid.loclu.remlu*) SESSKEY(*nnnnnnnn*) INTERVAL(*nnnnn*) CONVSEC(NONE|ALREADYV|CONV |PERSISTV|AVPV) [SESSLOCK]

Keyword	Use to	Syntax
LINKNAME	Specify the fully qualified names of both the foreign realm name and the foreign principal name in a trust relationship.	TSS ADDTO(SDT) KERBLINK(*label-name*) LINKNAME('*qualified-name*') KERBUSER(USERID)
LINUXNAM	Add, remove, or replace the Linux user name to an acid.	TSS ADDTO|REMOVE|REPLACE(*acid_name*) LINUXNAM(*linux_username*)
LINUXNODE	Add, remove, or replace Linux nodes to the NDT node list of an ACID record.	TSS ADD|REMOVE|REPLACE(NDT) LINUXNODE(*name*) [IPADDR(*ip_address*) FACILITY(*name*) ACTIVE(YES|NO)]
LNXENTS	Provide signon information onto an acid for LINUX in addition to the LINUXNAM.	TSS ADDTO(*acid*) LNXENTS(*fac*,UID|?,*hm*,*shell*,*grp acid*) RANGE(*xxx*,*xxx*) TSS ADDTO(*acid*) LNXENTS(*facility*,GID|?) RANGE(*xxx*,*xxx*) TSS REMOVE(*acid*) LNXENTS(*facility*)
LTIME	Specify how long (in minutes) until a user's terminal will lock if CA-Top Secret does not detect activity.	TSS ADDTO(acid) LTIME(*nnn*)[,*facility*])
MAPDATA	Add, remove, or replace a MAPDATA field in the MAP record of the SDT Record.	TSS ADDTO(SDT) MAPREC(*map-name*) MAPDATA(*field-definition*)
MAPREC	Provide a name CA-Top Secret references a MAP record in the SDT Record by PERMIT or REVOKE a MAP record associated with an OTRAN or PPT resource.	TSS ADDTO(SDT) MAPREC(*map-name*) DESCRIPT(*descript-name*) MAPDATA(*field-definition*) TSS PERMIT(*acid*) {OTRAN(*oper*)|PPT(*oper*)} MAPREC(*map-name*) SELECT(*sel-name*)
MASKDATA	Add, remove, or replace a MASKDATA field in the MASK record of the SDT Record.	TSS ADDTO(SDT) MASKREC(*mask-name*) MASKDATA(*field-definition*)
MASTFAC	Override the default facility, controlled by a batch or started task ACID, that is associated with a multi-user facility such as IMS or CICS.	TSS ADDTO(*region acid*) MASTFAC(*facility*)

Keyword	Use to	Syntax
MASKREC	Provide a name for a MASK record which CA-Top Secret uses in the SDT Record PERMIT or REVOKE a MASK record together with a SELECT statement associated with an FCT.	TSS ADDTO(SDT) MASKREC(*mask-name*) MASKDATA(*field-definition*)
MASKREC	Overlay the values on file for an FCT and thus provide field-level protection under Record Level Protection (RLP).	TSS PERMIT(*acid*) FCT(*oper*) ACCESS(*access-level*) MASKREC(*mask-name*) SELECT(*selread*)
MAXLEN	Define or change the number of bytes allowed to be entered for the user-defined FDT entry.	TSS ADDTO(FDT) MAXLEN(*nnnnn*)
MAXLEN	Define the maximum permission length for the user resource class being created.	TSS ADDTO(RDT) RESCLASS(*resource name*) RESCODE(*hex code*) MAXLEN(*maxpermit*)
MAXTKTLF	Specify the maximum ticket life in the KERBDFLT REALM record in the SDT, or when defining local principals in the user's security record.	TSS ADDTO(SDT) REALM(KERBDFLT) REALMNAME('*kerberos-realm*') MINTKTLF(*max-ticket-life*) MAXTKTLF(*max-ticket-life*) DEFTKTLF(*deflt-ticket-life*) KERBPASS(*password*) CHKADDRS TSS ADDTO(*acid*) KERBNAME('*principal*') MAXTKTLF(*max-ticket-life*)
MCSALTG	Assign an alternate group used in recovery. The IBM equivalent is ALTG.	TSS ADDTO(*acid*) MCSALTG(*groupname*)
MCSAUTH	Authorize the operator commands that can be entered from the console. The IBM equivalent to this field is AUTH.	TSS ADDTO(*acid*) MCSAUTH(INFO|MASTER|SYS|IO|CONS|ALL)
MCSAUTO	Specify whether the AUTO keyword is assigned to this console.	TSS ADDTO(*acid*) MCSAUTO(YES|NO)
MCSCMDS	Specify the system commands from this console are sent to.	TSS ADDTO(*acid*) MCSCMDS(*|*sysname*)
MCSDOM	Specify which delete operator messages (DOM) this console is to receive.	TSS ADDTO(*acid*) MCSDOM(NORMAL|ALL|NONE)

Keyword	Use to	Syntax
MCSHC	Receive hardcopy message set	`TSS ADDTO(acid) MCSLOGC(YES|NO)`
MCSINTIDS	Receive messages for console ID=0	`TSS ADDTO(acid) MCSINTDS(YES|NO)`
MCSKEY	Assign a KEY keyword to this console. The IBM equivalent to this field is KEY.	`TSS ADDTO(acid) MCSKEY(keyword)`
MCSLEVL	Specify the messages to be received by this console.	`TSS ADDTO(acid)` `MCSLEVL(ALL|NB|R|I|CE|E|IN)`
MCSLOGC	Specify whether command responses are logged in the hard copy log.	`TSS ADDTO(acid) MCSLOGC(YES|NO)`
MCSMFRM	Specify the display format for console messages.	`TSS ADDTO(acid) MCSMFRM(M|J|S|T|X)`
MCSMGID	Specify whether a one-byte migration ID is to be assigned to this console.	`TSS ADDTO(acid) MCSMGID(YES|NO)`

MCSMON	Specify how selected system events are monitored.	`TSS ADDTO(acid)`
		`MCSMON(JOBNAMES|JOBNAMES-T`
		`|SESS|SESS-T|STATUS)`

MCSROUT	Specify the routing codes assigned to the console.	`TSS ADDTO(acid)` `MCSROUT(:hp5.NONE:ehp5.|ALL|nnn,...)`
MCSSTOR	Specify the amount of storage, in megabytes, to be used for message queuing.	`TSS ADDTO(acid) MCSSTOR(nnnn)`
MCSUD	Specify whether this console is to receive undelivered action messages and WTOR messages.	`TSS ADDTO(acid) MCSUD(YES|NO)`
MCSUNKNIDS	Receive messages for unknown console IDs	`TSS ADDTO(acid) MCSUNKNIDS(YES|NO)`
MEMLIMIT	Specify the maximum number of bytes of non-shared memory space that this user can allocate.	`TSS ADD(TESTID) MEMLIMIT(value)`

MINTKTLF	Specify the minimum ticket life in the KERBDFLT REALM record in the SDT.	`TSS ADDTO(SDT) REALM(KERBDFLT)`
		`REALMNAME('kerberos-realm')`
		`MINTKTLF(min-ticket-life)`
		`MAXTKTLF(max-ticket-life)`
		`DEFTKTLF(default-ticket-life)`
		`KERBPASS(kerberos-password)`
		`CHKADDRS`

Keyword	Use to	Syntax
MISC1	Give or to remove an eadministrator's authority to perform administrative functions.	`TSS ADMIN(acid) MISC1(authority level(s))`
MISC2	Give or remove an administrator's authority to perform administrative functions.	`TSS ADMIN(acid) MISC2(authority level(s))`
MISC3	Give or remove an administrator's authority to perform additional functions.	`TSS ADMIN(acid) MISC3(authority level(s))`
MISC4	Give or remove an administrator's authority to perform additional functions	`TSS ADMIN(acid) MISC4(authority level(s))`
MISC5	Give or remove an administrator's authority to perform additional administrative functions	`TSS ADMIN(acid) MISC5(authority level(s))`
MISC8	Give or remove an administrator's authority to perform additional administrative functions	`TSS ADMIN(acid) MISC8(authority level(s))`
MISC9	Give or remove an administrator's authority to perform additional administrative functions	`TSS ADMIN(acid) MISC9(authority level(s))`
MMAPAREA	Specify the maximum amount of dataspace storage (pages) that can be allocated for memory mapping of HFS.	`TSS ADD(acidname) MMAPAREA(nnnnnnnn)`

MODE	Assign ownership of CA-Top Secret operating modes to the master SCA (MSCA)
	Specify an operating MODE for a user, control or profile ACID.
		`TSS ADDTO(sca acid)`
		`MODE(DORM,WARN,IMPL,FAIL)`
		`TSS PERMIT(USER01) MODE(WARN)`
		`FACILITY(BATCH,TSO)`

MODE	Specify an operating MODE for a user, control or profile ACID.	`TSS PERMIT(acid|profile)` `MODE(DORM|WARN|IMPL|FAIL)`

Keyword	Use to	Syntax
MRO	Store or remove user and profile Security Records in Common System Storage (CSA or ECSA) so that security information is accessible to all online regions.	`TSS ADDTO(region acid) MRO`

MULTIPW	Assign or remove multiple password attributes, ACIDs need a different password to access each facility.	`TSS ADD(acid) FAC(facility)`
		`PASSWORD(pswd[,[interval][,EXP]])`
		`MULTIPW`

NADATE and NATIMEs	Specify the effective date and time that the digital certificate expires.	`TSS REKEY(acid) NADATE(mm/dd/yy)` `NATIME(hh:mm:ss)`
NAME	Associate the ACID with a name for further identification.	`TSS CREATE(acid) NAME('character name')`
NBDATE and NBTIMEs	Specify the date and time the digital certificate becomes active.	`TSS REKEY NBDATE(mm/dd/yy)` `NBTIME(hh:mm:ss)`
NEWDIGIC	Specify the name that identifies a digital certificate within an acid record.	`TSS REKEY NEWDIGIC(name)`
NEWLABLC	Specify an optional and case-sensitive label to be associated with the certificate being added to the user.	`TSS ADDTO NEWLABLC(label-name)`
NOADSP	Prevent data sets, created by an ACID, from being automatically secured by z/OS by setting the RACF bit Define an ACID used to create data sets that cannot be automatically protected by CA-Top Secret	`TSS ADDTO(acid) NOADSP`
NOATS	Fail Automatic Terminal Signons.	`TSS ADDTO(acid) NOATS`
NODSNCHK	Specify that no data sets name checks are performed.	`TSS ADDTO(acid) NODSNCHK`
NOLCFCHK	Allow an ACID to execute any command or transaction for all facilities, regardless of LCF restrictions.	`TSS ADDTO(acid) NOLCFCHK`

Keyword	Use to	Syntax

NOPERMIT	Prevent an owner from being automatically permitted access to a resource whose ownership was transferred via the ADDTO command.	`TSS ADDTO(acid) resource(prefix)`
		`UNDERCUT`
		`NOPERMIT`

NOPWCHG	Prevent ACIDs from changing passwords at signon or initiation.	`TSS ADDTO(acid) NOPWCHG`
NOREFRESH	Prevent new logons allocating a new copy of the profile while updates are being made to the profile.	`TSS [ADDTO|REMOVE] (profile) NOREFRESH`
NORESCHK	Allow an ACID to bypass security checking for all owned resources except data sets and volumes.	`TSS ADDTO(acid) NORESCHK`
NOSUBCHK	Allow an ACID to bypass alternate ACID usage as well as all job submission security checking.	`TSS ADDTO(acid) NOSUBCHK`
NOSUSPEND	Allow an ACID to bypass suspension due to violations (VTHRESH).	`TSS ADDTO(acid) NOSUSPEND`
NOVOLCHK	Allow an ACID to bypass volume level security checking.	`TSS ADDTO(acid) NOVOLCHK`
OIDCARD	Prompt ACIDs to insert their identification cards into a batch reader whenever they sign on.	`TSS ADDTO(acid) OIDCARD`
OMVSPGM	Add or remove a program from a specified ACID.	`TSS ADDTO(acid) OMVSPGM(programname)`
OPCLASS	Assign or remove a set of CICS operator classes.	`TSS ADDTO(acid) OPCLASS(nn,nn..)`
OPIDENT	Assign or remove a CICS operator identification value that is equal to the ACID's OPIDENT entry in the CICS SNT (Signon Table)	`TSS ADDTO(acid) OPIDENT(xxx)`
OPPRTY	Assign or remove a CICS operator priority from the associated ACID.	`TSS ADDTO(acid) OPPRTY(0...255)`

Keyword	Use to	Syntax

PASSWORD	Assign a password, along with values that control its use, to a previously defined ACID.	`TSS ADDTO(acid)`
		`PASSWORD(password[,0...255],`
		`[EXPIRED])`
		`[FACILITY(facility) MULTIPW]`
		`TSS ADDTO(acid) PASSWORD(NOPW)`
		`FACILITY(facility) MULTIPW]`
		`TSS REPLACE(acid) PASSWORD(password)`

PCICC	Specify that the key pair is generated using the PCI Cryptographic Coprocessor and that the private key is stored in ICSF PKDS.	`TSS REKEY(acid) DIGICERT(8-byte name)`
		`DCDSN(dsname)`
		`PCICC`

PHRASE	Assign a password phrase as an alternative to PASSWORD.	`TSS ADDTO(acid)` `PHRASE(phrase[,nnn][,EXPIRED])`
PHYSKEY	Support external authentication devices	`TSS ADDTO(acid) PHYSKEY('physkey data')`
PKCSPASS	Specify the password associated with a PKCS#12-formatted digital certificate.	`TSS CHKCERT DCDSN(input-data-set-name)` `PKCSPASS(pkcs#12-password)`

POSIT	Specify the POSIT number associated with the class.	`TSS ADD(RDT) RESCLASS(resource class)`
		`RESCODE(hex code)`
		`POSIT(nnnn)`

PREFIX	Specify that all record matching is performed using the data entered as a partial key.	`TSS LIST(STC) PROCNAME(ASSEM) PREFIX`
		`TSS LIST(SDT)`
		`TSS LIST(RDT)`
		`TSS LIST(FDT)`

PRIVPGM	Specify the full names of the programs in control when a resource is accessed.	`TSS PERMIT(acid) resource(prefix)` `PRIVPGM(program)`

PROCNAME	Define a started task to CA-Top Secret by associating the STC procedure name with an ACID or action.	`TSS ADDTO(STC) PROCNAME(stcname|DEFAULT)`
		`ACID(acid|action)`
		`[STCACT]`

PROCUSER	Specify the maximum number of processes a user can have open at the same time.	`TSS ADD(acidname) PROCUSER(nnnnn)`
PROFILE	Add or remove up to 254 profiles from a specified ACID.	`TSS ADDTO(acid) PROFILE(profile acid,...)`

Keyword	Use to	Syntax
PRXBINDDN	Use as the distinguished name to use when authenticating to the LDAP server.	TSS ADDTO|REMOVE(SDT) EIMPROF(*eim-profile*) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXBINDDN(*name*) PRXBINDPW(*password*)
PRXBINDPW	Authenticate to the LDAP server.	TSS ADDTO|REMOVE(SDT) EIMPROF(*eim-profile*) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXBINDDN(*name*) PRXBINDPW(*password*)
PRXKRBREG	The name of the Kerb registry.	TSS ADDTO(SDT) EIMPROF(*eim-profile-name*) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXKRBREG(*name*) PRX509KRB(*name*) TSS DELETE(SDT) EIMPROF(*eim-profile-name*)
PRXLDAPHST	PRXLDAPHST is the LDAP server and URL and port.	TSS ADDTO|REMOVE(SDT) EIMPROF(eim-profile) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXBINDDN(*name*) PRXBINDPW(*password*)
PRX509REG	The name of the Kerb registry.	TSS ADDTO|DELETE(SDT) EIMPROF(name) EIMOPTION(ON|OFF) EIMDOMAIN(*name*) EIMLOCREG(*name*) PRXLDAPHST(*name*) PRXKRBREG(*name*) PRX509REG(*name*)
PSTKAPPL	Define the application ID.	TSS ADDTO(NDT) PSTKAPPL(*application*) SESSKEY(*abcdef12*)
PSUSPEND	Prevent ACIDs from accessing the system when a violation occurs due to PTHRESH.	TSS REMOVE(*acid*) PSUSPEND

Keyword	Use to	Syntax
PSWDPHR	Allow an ACID to sign on with a password phrase when PPHRASE is set OFF.	`TSS ADDTO(acid) PSWDPHR`

PTKTDATA	Define data resources for PassTickets used with R_GenSec and R_TicketServ callable services.	`TSS ADD(RDT) RESCLASS(PTKTDATA)`
		`ACLST(ALL,READ,UPDATE)`
		`MAXLEN(37)`

RANGE	Specify time range intervals within a calendar day associated with a TIMEREC label. Limit the scope of a search for auto-assignment of UID/GID.	`TSS ADDTO(SDT) TIMEREC(name)` `RANGE(hhmm:hhmm,...)`

REALM	Define the local realm and foreign realms and their trust relationships with each other.	`TSS ADDTO(SDT) REALM(KERBDFLT)`
		`REALMNAME('name')`
		`MINTKTLF(min-ticket-life)`
		`MAXTKTLF(max-ticket-life)`
		`DEFTKTLF(deflt-ticket-life)`
		`KERBPASS(kerberos-password)`
		`CHKADDRS`
		`TSS ADDTO(SDT) REALM(realm-label)`
		`REALMNAME('name')`
		`KERBPASS(PASSWORD)`

REALM(FOREIGN_REALM)	Provides a label for nodes other than for the local TCP/IP node.	`TSS ADD(SDT) REALM(foreign_realm)`
		`REALMNAME(name)`
		`ENCRYPT('[DES|NODES][DES3|NODES3]`
		`[DESD|NODESD] [AES128|NOAES128]`
		`[AES256|NOAES256]')`
		`KERBPASS(password)`

REALM(KERBDFLT)	Name the REALM associated with the local TCP/IP node.	`TSS ADD(SDT) REALM(KERBDFLT)`
		`REALMNAME(local-realm-URL)`
		`ENCRYPT('[DES|NODES] [DES3|NODES3]`
		`[DESD|NODESD] [AES128|NOAES128]`
		`AES256|NOAES256]')`
		`KERBPASS(password)`
		`CHKADDRS`

Keyword	Use to	Syntax

REALMNAME	Describe the relationship of a REALM in the Secureway Security Server Network Authentication Service configuration file to the local REALM.	`TSS ADDTO(SDT) REALM(KERBDFLT)`
		`REALMNAME(`*`local-realm-URL`*`)`
		`ENCRYPT('[DES|NODES] [DES3|NODES3]`
		`[DESD|NODESD] [AES128|NOAES128]`
		`[AES256|NOAES256]')`
		`KERBPASS(`*`password`*`)`
		`CHKADDRS`
		
		`TSS ADDTO(SDT) REALM(`*`foreign_realm`*`)`
		`REALMNAME('/../local_URL/`
		`krbtgt/frgn_URL')`
		`ENCRYPT('[DES|NODES] [DES3|NODES3]`
		`[DESD|NODESD] [AES128|NOAES128]`
		`[AES256|NOAES256]')`
		`KERBPASS(`*`password`*`)`

REALMNAME (Local Realm)	Specify the fully qualified names of a local realm name.	`TSS ADDTO(SDT) REALM(KERBDFLT)`
		`REALMNAME('`*`kerberos-realm`*`')`
		`MINTKTLF(`*`max-ticket-life`*`)`
		`MAXTKTLF(`*`max-ticket-life`*`)`
		`DEFTKTLF(`*`default-ticket-life`*`)`
		`KERBPASS(`*`kerberos-password`*`)`
		`CHKADDRS`

REALMNAME	Specify the fully qualified names of the local and foreign realm names in a trust relationship.	`TSS ADDTO(SDT) REALM(`*`realm-label`*`)`
		`REALMNAME('`*`name`*`')`
		`KERBPASS(`*`password`*`)`

RECDATA	Specify field characteristics associated with a RECORD.	`TSS ADDTO(SDT) RECORD(`*`rlp-name`*`)` `RECDATA(`*`field-definition`*`)`
RECORD	Provide an up to eight-character name associated with each RLP Record in the SDT Record.	`TSS ADDTO(SDT) RECORD(`*`rlp-name`*`)` `RECDATA(defin1,..defin5)`

Keyword	Use to	Syntax
RENEW	Renew a digital certificate.	TSS RENEW {(CERTAUTH|CERTSITE|acid)} DIGICERT(*8-byte-name*) [SUBJECTN('CN="*common-name*" T="*title*" OU="*org-unit-name1,org-unit-name2*" O="*organizational-name*" L="*locality*" ST="*state-or-province*" C="*2–digit–only country code*"')] [NBDATE(*mm/dd/yy*) NBTIME(*hh:mm:ss*)] [NADATE(*mm/dd/yy*) NATIME(*hh:mm:ss*)] [LABLCERT(*label name*)] [ICSF|PCICC] [KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN CERTSIGN)] [ALTNAME('IP=numeric-IP-address DOMAIN=*internet-domain-name* EMAIL=*email-address* URI=*universal-resource-identifier*')] [LABLPKDS(*PKDS-label*|*)]
RESCLASS	Define a resource-class-name that allows one resource-class-name per command.	TSS ADDTO(RDT) RESCLASS(*resource class*) RESCODE(hex code)
resclass(resource)	Associate a resource instance with a SECLABEL and optionally override MLMODE for matching resources.	TSS ADD(MLS) resclass(*resource.instance*) SECLABEL(*label*) [MODE(FAIL|WARN|DORM)]
RESCODE	Supply an internal abbreviation for the RESCLASS resource class in ACID security records and in audit information Find what RESCLASS is associated with a specific resource code	TSS ADDTO(RDT) RESCLASS(*resource Type*) [RESCODE(*hex code*)]
RESOURCE	Give or remove authority for an administrator to issue ADDTO, REMOVE, PERMIT, or REVOKE commands for any resource class in the RDT	TSS ADMIN(acid) RESOURCE(*auth-level*(s)) ACCESS(*access-level*(s))
RESOWNER	Add or remove a User or Control type ACID associated with a data set or an ACID that matches the high level index of the data set that is being allocated for the extraction by SMS.	TSS ADDTO(*acid*) DSNAME(*dataset name*) RESOWNER(*smsacid*)

Keyword	Use to	Syntax
RSTDACC	Prevent users from accessing protected resources they are not specifically authorized to access.	`TSS ADDTO(acid) RSTDACC`
RETAIN	Use with the DLF ACID to leave the data set in hyperspace when the job which bought the data set into hyperspace ends.	`TSS ADDTO(DLF) DSNAME(SYS1.)` `RETAIN`

RINGDATA	Specifies the ACID and certificate name (as specified by DIGICERT) of the digital certificate being added to the user.	`TSS ADDTO(userid) KEYRING(8-byte name)`
		`[LABLRING(ring name)]`
		`{RINGDATA(userid,digicert)}`
		`{RINGDATA(CERTSITE,cert)}`
		`{RINGDATA(CERTAUTH,cert)}`
		`[DEFAULT]`
		`[USAGE(PERSONAL|CERTSITE|CERTAUTH)]`

SCOPE	MSCA allow authority	`TSS ADMIN(lsca) SCOPE({lsca1}`
		`[,{lsca2},...]) {zone1} {zone2}`
		`TSS DEADMIN(dca1|vca1|zca1|lsca1)`
		`SCOPE(profile1)`
		`TSS ADMIN(lsca) SCOPE(lsca1|zone1,...)`
		`TSS ADMIN(admin) SCOPE(profile)`

SCTYKEY	Specify which CICS security keys an ACID may or may not use.	`TSS ADDTO(acid) SCTYKEY(n,n,...)`
SDNFILTR	Specify the significant portion of the subject's distinguished name used as a filter when associating an ACID with a digital certificate.	`TSS ADDTO(acid) CERTMAP(recid)` `SDNFILTR('filter')`

SDTFNAME	Remove a field from a MASK, MAP or RECORD in the SDT Record.	`TSS REMOVE(SDT) [MASKREC(mask-name)]`
		`SDTFNAME(fld1,...fld5)`
		`[MAPREC(map-name)]`
		`RECORD(rlp-name)`

SECLABEL	Define and remove security labels in the MLS record.	`TSS ADDTO(MLS) SECLABEL(seclabel-name)`
		`SECEVEL(level-name)`
		`CATEGORY(category1,…,categoryn)`
		`SYSID(sysid1,…,sysidn)`
		`MLAUDIT(access1,…,accessn)`
		`TSS REMOVE(MLS) SECLABEL(seclabel-name)`

SECLEVEL	Define or remove security levels which are the hierarchical elements of security labels.	`TSS ADDTO(MLS) SECLEVEL(level-number)`
		`LVLNAME(level-name)`
		`TSS REMOVE(MLS) SECLEVEL(level-name)`

Keyword	Use to	Syntax
SEGMENT	Assign fields to a specific segment. You cannot add user-defined fields to system-defined segments. List data about fields in a specific segment.	`TSS ADDTO|LIST(FDT) SEGMENT(segmentname)`

SELDATA	Add, remove, or replace a SELDATA field in the SELECT record of the SDT Record. Specify a (compound) logical condition to decide whether RLP or Screen Level Protection is applicable for an associated SELECT.	`TSS ADDTO(SDT) SELECT(sel-name)`
		`DESCRIPT(desc-name)`
		`SELDATA('IF [NOT] exp AND|OR] exp')`

SELECT	Provide a name by which CA-Top Secret references a SELECT record in the SDT Record.
	Determine whether SLP permission is invoked, and whether RLP read/update permission is invoked (in the “selread” and “selwrite” SELECT names, respectively).
	Permit or revoke a SELECT record associated with an FCT resource.
		`TSS ADDTO(SDT) SELECT(sel-name)`
		`DESCRIPT(descript-name)`
		`SELDATA('IF [NOT]sel-exp`
		`[AND|OR] sel-exp')`
		`TSS PERMIT(acid) FCT(oper)`
		`SELECT(selread,selwrite)`
		`TSS PERMIT(acid)`
		`{OTRAN(tran)|PPT(program)}`
		`SELECT(selread)`

SERIALNUM	Specify the digital certificate's serial number.	`TSS LIST SERIALNUM(serial number)`

SESSKEY	Define the encryption key for the application.
	Display the session keys associated with designated LINKIDs in the APPCLU Record or PassTicket applications in the NDT Record.
		`TSS ADDTO(NDT) PSTKAPPL(application)`
		`SESSKEY(session_key)`
		`TSS ADDTO(APPCLU) LINKID(id)`
		`SESSKEY(session_key)`
		`INTERVAL(num)`
		`TSS LIST(NDT) DATA(SESSKEY)`

SHMEMMAX	Use the SHMEMMAX keyword to specify the maximum number of bytes of shared memory space that this user can allocate.	`TSS ADD(TESTID) SHMEMMAX(value)`
SIGNALG	Specify signing algorithm	`TSS GENCERT` `SIGNALG(SHA1|SHA256)`

Keyword	Use to	Syntax
SIGNMULTI	Allow multiple signons for specific ACIDS in a facility with the SIGN(S) sub-option.	TSS ADDTO(*acid*) FACILITY(*facility*) SIGNMULTI
SIGNWITH	Specify the digital certificate with a private key that is signing the certificate.	TSS GENCERT SIGNWITH(*acid,digicert*)
SITRAN	Specify which CICS transaction CA-Top Secret automatically executes after an ACID successfully signs on to a facility.	TSS ADDTO(*acid*) *SITRAN(transaction[,facility*])
SMASYS and SMANODEs	Define Security Management Architecture optons	TSS ADD(NDT) SMASYS(*sysid*) RECOVERYDSN(*dsname*) RECVDSN(*Recovery* DSN)
SMSAPPL	Add or remove a default SMS application identifier.	TSS ADDTO(*acid*) SMSAPPL(*application*)
SMSDATA	Add or remove a default SMS data class.	TSS ADDTO(*acid*) SMSDATA(*data class name*)
SMSMGMT	Add or remove a default SMS management class.	TSS ADDTO(*acid*) SMSMGMT(*class name*)
SMSSTOR	Add or remove a default SMS storage class.	TSS ADDTO(*acid*) SMSSTOR(*class name*)
SNAME	Map a user identity from Lotus Notes z/OS UNIX to a CA-Top Secret ACID.	TSS ADDTO(acid) SNAME('*name*')
SOURCE	Specify source reader or terminal prefixes through which the associated ACID may enter the system.	TSS ADDTO(*acid*) SOURCE(*oper,...*)
START	Specify an optional activation date.	TSS ADDTO(*acid*) DIGICERT(*name*) DCDSN(*dsname*) START(*mm/dd/yy*) TSS PERMIT(USER01) DSN(****.FILE) UNTIL('05 01 02')
STCACT	Invoke operator accountability.	TSS ADDTO(STC) PROCNAME(*stcname*|DEFAULT) ACID(*acid*|*action*) [STCACT]

Keyword	Use to	Syntax

SUBJECTN	Specify the ACID's distinguished name in a digital certificate.	`TSS GENCERT SUBJECTN{('CN="common-name"`
		`T="title"`
		`OU="name1, name2"`
		`O="organizational-name"`
		`L="locality"`
		`ST="state"`
		`C="country"')}`

SUSPEND	Prevent ACIDs from accessing the system when a violation occurs.	`TSS ADDTO(acid) SUSPEND`

SYSID	Identify the system to which the authorization applies.	`TSS ADDTO(acid) {FACILITY(facility)}`
		`SYSID(sysid)`
		`{CRITMAP(recid)}`

TARGET	Specify which CA-Top Secret nodes receive commands and how the local node processes it
	Assign nodes associated with ACIDs
		`TSS ADDTO(acid) keyword(s)`
		`TARGET(node,node,...)`
		`TSS LIST(ACID) TARGET(*|LOCAL|nodename)`

TIMEREC	Provide a name to reference a TIMEREC record in the SDT Record.
	Permit or revoke a time restriction on any resource.
	Add, remove, replace, or list TIME records in the SDT Record.
		`TSS ADDTO(SDT) TIMEREC(time-name)`
		`DESCRIPT(descript-name)`
		`RANGE(hhmm:hhmm,...)`
		`TSS PERMIT(acid) RESCLASS(resource-name)`
		`TIMEREC(time-name)`

TIMES	Assign a range of hours during which a facility or resource may be accessed.	`TSS ADDTO(acid) FACILITY(facility)`
		`TIMES(00,24)`
		`TSS PERMIT(acid) resource(prefix(es))`
		`TIMES(00,24)`

TOKENADD	Create PKCS #11 token	`TSS P11TOKEN TOKENADD LABLCTKN(token name)`
TOKENDEL	Delete PKCS #11 token	`TSS P11TOKEN TOKENDEL LABLCTKN(token name)` `[FORCE]`
TOKENLIST	Display PKCS #11 token information	`TSS P11TOKEN TOKENLST LABLCTKN(token name)`
TRACE	Activate a diagnostic trace on all ACID activity (initiations, resource access, violations, user's security mode).	`TSS ADDTO(acid) TRACE`

Keyword	Use to	Syntax
TRANSACTIONS	Confine ACIDs to using a specific transaction, or subset of the transactions, available within that facility.	`TSS ADDTO(acid) TRANSACTIONS(fac,(trans[(G)])`
TRUST	Associate a digital certificate with a user. NOTRUST is the default.	`TSS ADDTO(acid) DIGICERT(name) TRUST|NOTRUST|HITRUST`
TSOCOMMAND	Provide a default command issued at TSO logon.	`TSS ADDTO(acid) TSOCOMMAND(nnn)`
TSODEST	Provide a default destination identifier for TSO generated JCL for TSO users.	`TSS ADDTO(acid) TSODEST(id)`
TSOHCLASS	Assign a default hold class for TSO generated JCL for TSO users.	`TSS ADDTO(acid) TSOHCLASS(class)`
TSOJCLASS	Assign a default job class for TSO generated job cards from TSO users.	`TSS ADDTO(acid) TSOJCLASS(class)`
TSOLPROC	Provide a default proc to be used for TSO logon.	`TSS ADDTO(acid) TSOLPROC(proc)`
TSOLSIZE	Assign a default region size for TSO.	`TSS ADDTO(acid) TSOLSIZE(nnnnnnn)`
TSOMCLASS	Assign a default message class for TSO generated JCL for TSO users.	`TSS ADDTO(acid) TSOMCLASS(class)`
TSOMPW	Support multiple TSO UADS passwords, on a user-by-user basis.	`TSS ADDTO(acid) TSOMPW`
TSOMSIZE	Define the maximum region size that a TSO user may specify at logon.	`TSS ADDTO(acid) TSOMSIZE(nnnnnnn)`
TSOOPT	Assign default options that a TSO user may specify at logon.	`TSS ADDTO(acid) TSOOPT(option,...)`
TSOSCLASS	Assign a default SYSOUT class for TSO generated JCL for TSO users.	`TSS ADDTO(acid) TSOSCLASS(class)`
TSOUDATA	Assign a site-defined data field to a TSO user.	`TSS ADDTO(acid) TSOUDATA(data field)`
TSOUNIT	Assign a default unit name for dynamic allocations under TSO.	`TSS ADDTO(acid) TSOUNIT(name)`

Keyword	Use to	Syntax
TYPE	Specify the type of ACID.	TSS CREATE(acid) TYPE(USER|PROFILE|GROUP |DEPARTMENT|DIVISION|ZONE |DCA|VCA|ZCA|LSCA|SCA) NAME('*name*') ... TSS LIST(ACIDS) DATA(dataType(s)) TYPE(USER|PROFILE|GROUP|DCA|VCA |SCA|ZCA|LSCA|DEPARTMENT |DIVISION|ZONE)
TZONE	Specify an ACID's physical time zone in relation to the CPU's time zone.	TSS ADDTO(*acid*) TZONE([-]nn)
UID	Specify a numeric UID value to each user for security within USS.	TSS MODIFY(OMVSTABS) TSS ADD(*acid*) UID(*USS_user_id*) TSS ADD(*acid*) UID(?) [RANGE(*low-uid,high-uid*)]
UNAME	Map a user identity from Novell Directory Services to an ACID.	TSS ADDTO(*acid*) UNAME('*uname*')
UNBIND	Remove certificate from PKCS #11 token	TSS P11TOKEN UNBIND LABLCTKN(name) SEQNUM(nnnnnnnn)|LABLCERT(cert label) TOKNUSER(userid) LABLCTKN(token name) FORCE
UNDERCUT	Transfer resource ownership from one ACID to another.	TSS ADDTO(*acid*) resource(prefix) UNDERCUT
UNTIL	Assign or remove the specific date: On which an ACID expires. When permission to access a resource expires.	TSS ADDTO(*acid*) UNTIL(mm/dd/yy) TSS PERMIT(*acid*) resource(*prefix*(es)) UNTIL(*mm/dd/yy*)
USAGE	Indicate the trust level for a digital certificate being added to a key ring.	TSS ADDTO(*acid*) KEYRING(*8-byte name*) [LABLRING(*237-byte ring name)]* *{RINGDATA(acid,digicert)}* {RINGDATA(CERTSITE,*digicert*)} {RINGDATA(CERTAUTH,*digicert*)} [DEFAULT] [USAGE(PERSONAL|CERTSITE|CERTAUTH)]
USER	Grant or remove access to unownable, installation-defined resources.	TSS ADD(*acid*) USER(*class,value*)

Keyword	Use to	Syntax
USERNL1 and USERNL2s	Set the National Language code for CTS sign ons. USERNL1 is the primary and USERNL2 is the secondary.	TSS ADDTO(*acid*) [USERNL1(*code*)|USERNL2(*code*)]
USING	Create an ACID of the same type using an existing ACID as a model.	TSS CREATE(*newacid*) USING(*modelacid*)
VSUSPEND	Remove the suspension of an ACID suspended for access violation reasons.	TSS REMOVE(*acid*) VSUSPEND
WAACCNT	Provide an account number for z/OS APPC processing.	TSS ADDTO(*acid*) WAACCNT(*accntname*)
WAADDRn	Indicate up to four additional lines of SYSOUT delivery information.	TSS ADDTO(*acid*) WAADDR1(*info*) WAADDR2(*info*) WAADDR3(*info*) WAADDR4(*info*)
WABLDG	Indicate the building SYSOUT information is delivered to.	TSS ADDTO(*acid*) WABLDG(*name*)
WADEPT	Iindicate the department SYSOUT information is delivered to.	TSS ADDTO(*acid*) WADEPT(*deptname*)
WAIT	Indicate whether a CA-Top Secret command is processed synchronously or asynchronously.	TSS *function*(*acid*) *keyword*(s) WAIT(YES|NO)
WANAME	Indicate who SYSOUT information is delivered to.	TSS ADDTO(*acid*) WANAME(*name*)
WAROOM	Indicate the room SYSOUT information is delivered to.	TSS ADDTO(*acid*) WAROOM(*roomname*)
XCOMMAND	Prevent ACIDs from using a specified command or subset of commands available within that facility.	TSS ADDTO(*acid*) XCOMMAND(*facility*,(*cmdname*[(G)]))
XSUSPEND	Suspend an ACID suspended by the installation exit.	TSS REMOVE(*acid*) XSUSPEND
XTRANSACTIONS	Restrict ACIDs from using a specific transaction, or subset of the transactions, available within that facility.	TSS ADDTO(*acid*) XTRANSACTIONS(*fac*,(*transac*[(G)]))

Keyword	Use to	Syntax

YEAR	Add, remove, replace or list a year field in the calendar record of the SDT Record.	`TSS ADD(SDT) CALENDAR(`*cal-name*`)`
		`[YEAR(`*yyyy*`)]`
		`[DAYS(`*days*`)]`
		`[INCLUDE(`*mm/dd*`,...]`
		`[EXCLUDE(`*mm/dd*`,...)]`

ZONE	Assign an ACID to a zone
	List data about ACIDs in a specific zone
		`TSS CREATE(`*divacid*`|`*ZCAacid*`)`
		`TYPE(DIVISION|ZCA)`
		`NAME('`*ZCA or Division name*`')`
		`ZONE(`*acid*`)`
		`TSS LIST(ACID|ACIDS) DATA(`*datatype*`(s))`
		`TYPE(`*acidtype*`)`
		`ZONE(`*acid*`)`

Chapter 3: Control Options

This section contains the following topics:

Control Options

Option	Use to:	Sub options
ADABAS	Specify SVC's used by ADABAS (Release 4.8-4.9) security.	N/A
ADMINBY	Control auditing of permits and facilities added to a user.	NOADMINBY|ADMINBY
ADSP	Control global automatic data set protection.	YES|NO|ALL
AUDIT(SWITCH)	Force an immediate switch to the top of the ATF or to the alternate ATF.	N/A
AUTH	Control the order of precedence for the ALL, PROFILES, and USER records.	OVERRIDE,ALLOVER
AUTOEDSN	Turn on the AUTOERASE feature for selected data sets only.	ADD|REM
AUTOERASE	Control autoerase feature necessary to meet NCSC requirements.	YES|NO|ALL
BACKUP	Control automatic security file backup.	blank|*hhmm*|OFF
CACHE	Specify amount of virtual storage within the CA Top Secret address space for caching.	*nnnn*|CLEAR|STATUS|OFF
CANCEL	Allow CA Top Secret to be canceled via the O/S CANCEL command.	N/A
CATADELPROT	Prevent dataset deletion	YES|NO
CHOWNURS	Allow users to use the CHOWN function to change file ownership for files that they own.	ON|OFF
CMDNUM	The number of command processors initiated at startup of the CA Top Secret address space.	Range: 1 to 10 Default: 5
CPF	Control startup of Command Propagation Facility.	ON|OFF|KILL|REFRESH|INACTIVE

Option	Use to:	Sub options
CPFAUTOGID	Transmit assigned GID value (not ?) when using Command Propagation Facility.	YES|NO
CPFAUTOUID	Transmit assigned UID value (not ?) when using Command Propagation Facility.	YES|NO
CPFNODE	Change the status and attributes of a CPF node after CA Top Secret has initialized and CPF is activated.	STOP|START|REFRESH
CPFNODES	Identify remote nodes TSS commands can be transmitted to.	S,C|S,P|S,GW|S,P,GW||S,C.GW|R|R,GW|NB
CPFRCVUND	Identify if the local node can receive commands transmitted from remote nodes that have not be defined to the CPFNODES list.	YES|NO
CPFSTAT	Provide the current settings for the CPF control options, CPF, and nodes.	YES|NO
CPFTARGET	Default for TSS command TARGET keyword.	LOCAL|AUTO|*
CPFWAIT	Default for TSS command WAIT keyword.	YES|NO
DATE	Date display format.	*yy/dd/mm*
DB2FAC	Control DB2 subsystem protection.	N/A
DEBUG	Debugging feature. Use as directed by CA support only.	ON|OFF
DFLTRNGU	Default range for auto UID feature.	*nnn*,*nnn* Range: 1 to 2,147,483,647
DFLTRNGG	Default range for auto GID feature.	*nnn*,*nnn* Range: 1 to 2,147,483,647
DIAGTRAP	Produce a diagnostic dump. Use as directed by CA support only.	
DISPMASK	Allow the attribute of MASK on a maskable resource to be displayed on a permit.	ON|OFF
DL1B	Protection of DBD and PSB for DL/1 batch programs.	YES|NO
DOWN	Action taken when CA Top Secret address space is inactive.	B|S|T|O,W|B|F|N Default: BW,SB,TW,OW
DRC	Modify or list DRC attributes.	*nnn*,*option* Range: 1 to 159
DUFPGM	Identify programs allowing for extraction or update of INSTDATA.	*program*|RESET

Option	Use to:	Sub options
DUMP	Produce a dump of control blocks in the address space and common system storage. Use as directed by CA support only.	
ETRLOG	Send mainframe security events to CA Audit.	ON|OFF
ETROPTS	The monitor sends to CA Audit.	ADD|REM, VIO,LOG,START,INIT,USS,CMDADM,CONTROL
EXIT	Control installation exit (TSSINSTX).	ON|OFF
EXPDAYS	Display commands beyond the expiration date.	*nn* Range: 1 to 30 Default: 0
FACILITY	Control facility processing.	*facility*|ALL
GOSETGID	Alter the way the makeFSP SAF callable service works.	ON|OFF
HFSACL	Provide more control over the HFS file system than native HFS security.	ON|OFF
HFSSEC	Turn HFS security ON or OFF	ON|OFF
HPBPW	Honor previous batch password.	*n* Range: 0 to 9 Default: 0
IMS	Set global options for IMS security processing.	[NO] NOIMS61SUB NOIMSATSDF NOIMSATSLG IMSLCFMG IMSDBDVL IMSPSBVL
INACTIVE	Control users that have been inactive for a specified period.	0|*nnn* LASTUSED Range: 1 to 255
INSTDATA	Alter global installation data field.	0|*hhhh*
IOTRACE	Control CA Top Secret I/O trace.	OFF|ON|SR
JCT	Identify JES2 JCT offsets.	INDEV=*nnnn*, ROUTE=*nnnn*, NJHDR=*nnnn*
JES	Identify JES2/JES3 subsystems.	SSID=*cccc* TYPE=JES2|JES3 LEVEL RELEASE *n.n* VERIFY|NOVERIFY
JESNODE	Identify the local JES node.	*nodename*
JOBACID	Control ACID identification for batch jobs.	A|U|J|R,n, Default: A,1,0
KERBLVL	Highest available encryption level available for Kerberos certificates.	0|1

Option	Use to:	Sub options
LDAPNODE	Change the status, trace and recovery options of an LDAP node after CA Top Secret has initialized and LDS is activated.	*nodename*, ACTIVE(YES|NO) ,TRACE(ON|OFF) ,RECOVERY(YES|NO)
LDS	Enable LDAP processing for the TSS region.	ON|OFF
LDSRETRY	Retry count for failed LDS send operations.	*nnn* Default: 003
LDSTIMEOUT	Set timeout interval value for the LDS server.	*nnn* Default: 005
LDSTRACE	Control tracing of LDS outbound processing.	ON|OFF
LMPCHECK	Verify that LMP encryption key is being used.	N/A
LOG	Control incident recording for all facilities.	ACTIVITY, ACCESS, MSG,SMF,INIT,SEC9 |NONE|ALL
LUUPDONCE	Enforce the daily update of the last-used statistics within the user's security file record	YES|NO
MAXKEYSIZE	Specify the maximum private key size for digital certificates.	2048|4096
MLACTIVE	Specify whether Multilevel Security checking will be performed.	YES|NO
MLFSOBJ	Specify whether UNIX files/directories are required to have security labels.	YES|NO
MLIPCOBJ	Specify whether UNIX IPC objects are required to have security labels.	YES|NO
MLMODE	Select the security mode in which Multilevel Security checking will be performed.	DORMANT|WARN|FAIL
MLNAME	Restrict the display of names of datasets, and UNIX Files/directories to only those for which the user is authorized to read.	YES|NO
MLSECAUD	Specify whether Seclabel Auditing is to be performed.	YES|NO
MLSLBLRQ	Specify if security labels are required for all users, datasets, and resources in an MLS environment	YES|NO
MLWRITE	Allow or prevent the write down of data.	YES|NO
MODE	Control the default processing mode set for facilities at CA Top Secret initiation.	WARN|FAIL|IMPL|DORM

Option	Use to:	Sub options
MSG	Alter characteristics of CA Top Secret violation messages.	*nnnn,option*
MSUSPEND	Allow MSCA to be suspended if password violation occurs.	YES|NO
NEWPHRASE	Characteristics of the password phrase.	[MA=*nn*],[MN=*nn*],[ID],[MAX=*nnn*], [MIN=*nn*],[MINDAYS=*nn*],[NR=*nn*], [NU],[SC=*nn*],[WARN=*nn*]
NEWPW	New password specification rules.	([FA],[FN],[ID],[MASK=*mask*], [MASK=*nnn*],[MC],[MAX=*n*],[MIN=*n*],[MIN DAYS=*nn*],[NM],[NO],[NR=*n*], [NU],[NV],[RN],[RS],[SC],[SW],[UC],[TS], [WARN=*nn*])
NJEUSR	Default ACID used in the Store-and-Forward nodes.	*acid*
NPPTHRESH	Maximum number of password phrase reverification attempts.	Range: 1 to 99 Default: 2
NPWRTHRESH	Maximum threshold for new passwords to be verified before complete logon sequence needs restarting.	Range: 1 to 99 Default: 2
OMVSGRP	Acid used to provide the OMVS segment for an extract for any group that does not have an OMVS segment.	Default: The field DFLTGRP from the acid specified in OMVSUSR
OMVSTABS	Refreshes internal UID and GID tables for Open z/OS security.	
OMVSUSR	The acid used to provide the OMVS segment for an extract for any user who does not have an OMVS segment.	*acid*
OPTIONS	Replaces several optional apars.	*n,n*
PASSCHAR	Special characters for passwords.	NONE
PDSPROT	Identify PDS protected at the member level. Enable/disable member-level protection.	ON|OFF ADD|REMOVE DSN(*dsn*), *VOL(vol)*, CLASS(*class*)
PPEXP	The number of days before a password expires.	Range: 0 to 255 Default: 30
PPHIST	The number of days the password phrase stays in the history file.	Range: 1 to 64 Default: 3
PPSCHAR	Characters allowed in password phrases.	*c,c,c,c,c,c,c,c,c,c,c,c,c,c,c,c,c,c*
PRODUCTS	Specify special products installed.	TSO/E, ACF/2, CA-Tape,TSO,NONE

Option	Use to:	Sub options
PROFINTERVAL	How long a profile cannot be refreshed for.	Range: 0 to 9999
PPHRASE	Specify if users can use password phrases.	ON|OFF
PTHRESH	Password violation threshold.	0|*nnn* Range: 1 to 254 Default: 4
PTKRESCK	Specify if FASTAUTH is performed before a Pass Ticket is generated.	YES|NO
PWEXP	Password expiration interval.	Range: 1 to 255 Default: 30
PWHIST	Number of previous passwords maintained in history file.	Range: 1 to 64 Default: 3
PWVERIFY	Verify old password before accepting new password	YES|NO
RCACHE	Specify if hardening is allowed.	YES|NO
RCQNAME	Specify which caches can be hardened.	ADD|REM R*ccccccc*
RECOVER	Control change recovery.	ON|OFF
REFRESH	Request CA-SAF module reinitialization after maintenance.	blank|SAF|*modabbrv*
REINIT	Request module reinitialization after maintenance.	K|E|M|1|2|3|S|R
RESETEOD	Reset an “end-of day” shutdown condition.	N/A
RESETSTATS	Reset all statistics.	N/A
RPW	Modify and list contents of restricted password list.	LIST|RESET|(ADD|REM,*password)*
SECCACHE	Provide a cache for security records that reflect the status of a user following a RACROUTE VERIFY request	SECCACHE(SIZE=*mmmm*,INDEX=*nnnnnn*, EXP=*hhh*,WARN=*ppp*) SECCACHE(CLEAR,EXP=*hhh*|*acidname*) SECCACHE(STATUS) SECCACHE(OFF)
SECTRACE	Control security diagnostic trace.	WTO|WTL|OFF|ACT,WTO|WTL|ON
SHRFILE	Specify ifCA Top Secret files are shared.	NO|(YES[SECURITY), AINDXPER
SHRPROF	Display shared profile table percentage used.	*jobname*
SMA	Control communication with the remote SMA host.	ON|OFF

Option	Use to:	Sub options
SMFTYPE	Change the SMF record type for SAF trace records from 231 to another type	SMFTYPE(*nnn*)
ST	Generate combined STATS, STATUS, and VERSION display.	N/A
STATG	Gather statistics.	ON|OFF
STATGINT	Time interval for statistics gathering.	Range: 1 to 60 Default: 15
STATREC	Specify the types of statistics processed.	(CACHE, COMMAND, CPF, IOSTATS, RACROUTE, SECCACHE, SYSPLEX, WORKLOAD, ALL)
STATS	Display statistics counts.	N/A
STATSLOG	Specify the name of a pre-allocated dataset statistics are written to.	*dsname*
STATUS	Display control option settings.	BASE,CPF,FACMODE, JES, LDS, PASSWORD, PHRASE, SYSPLEX, VERSION
SUBACID	Control online job submission of jobs and started tasks without explicit USER parameters, submitted to INTRDR.	J|U,*n* Default: 7
SVCDUMP	Produce a system dump of the CA Top Secret system.	N/A
SWAP	Control CA Top Secret address space swapping.	YES|NO
SYNCH	Synchronize global resource authorization tables.	N/A
SYSOUT	Spin off CA Top Secret activity log, specifies class and destination.	*class,dest* Default: A,LOCAL
SYSPLEX	Enable XCF and XES processing with CA Top Secret.	(*connect*|*group*|*structure*) |(DISCONNECT[XES]) |TRACE(ON|OFF))
TAPE	Control tape processing.	OFF|DEF|DSNAME
TEMPDS	Control temporary data set protection.	YES|NO
TEXTTSS	Characters to replace the string 'CA Top Secret' in messages and reports.	*text* Range: Up to 24 characters Default: CA Top Secret)
TIMELOCK	Interval at which CA Top Secret will attempt to obtain the Security File lock or enqueue.	*n1,n2,n3,n4* Default: 25,64,128,1200

Option	Use to:	Sub options
TIMER	Timer control interval.	*nnn* Range: 10 to 300 Default: 15
TNGMON	Set and activate error messages sent to a Unicenter console.	(ON|OFF) | (ADDTO|REMOVE, *ipaddress*[,DEBUG])
TSS	Allow use of TSS command at the O/S console.	N/A
TSSCMDOPTION	Default settings for TSS command specific options.	ADMINBY|NOADMBY, TERSE|VERBOSE
UNIXOPTS	Control USS auditing and the maximum number of supplemental groups supported	UNIXOPTS(MAXSGRPS=nnnn,DIRACC,DIRSCH ,FSOBJ,FSSEC,IPOBJ,PROCACT,PROCESS)| (None)
VERSION	Display CA Top Secret version and maintenance level.	N/A
VSAMCAT	Bypass user catalog volume checks on VSAM data set creation	YES|NO
VTHRESH	Violation threshold and action.	*(nn*,[NOT],[CAN],[WARN]) ,[SUS],[RES],[WARN], RES Range: 0 to 254 Default: 05,NOT
XCF(*)	Route information to remote systems in the SYSPLEX.	N/A