CA-Top Secret®

Command Functions Guide
Release 3.0
VSE

SP1

Second Edition, September 2000

Contents

About This Guide

Purpose

This guide provides inexperienced CA-Top Secret administrators with detailed information on how to use TSS command functions to administer security. Experienced administrators may find this guide useful as a quick reference aid.

Prerequisite Reading

Security administrators should read the *User Guide* and the respective *Implemention Guides* prior to using this guide.

Organization

Chapter	Description
1	Describes the purpose, syntax, entry methods, and processing of TSS command functions. Explanation of rules and procedures which govern the use of TSS command functions.
2	Describes the purpose of the Resource Descriptor Table (RDT) Record, how to manage and modify the RDT, and detailed reference pages on each applicable keyword.
3	Describes the purpose of the Field Descriptor Table (FDT) Record, how to manage and modify the FDT, and detailed reference pages on each applicable keyword.
4	Describes the purpose of the Static Data Table (SDT) Record, how to manage and modify the SDT, and detailed reference pages on each applicable keyword.
5	Describes the purpose of the TSS ADDTO/REMOVE command function, instructions on use, entry methods, and detailed reference pages on each applicable keyword.
6	Describes the purpose of the TSS ADMIN/DEADMIN command function, instructions on use, entry methods, and detailed reference pages on each applicable keyword.
7	Describes the purpose of the TSS CREATE command function, instructions on use, and entry methods.
8	Describes the purpose of the TSS DELETE command function, instructions on use, and entry methods.
9	Describes the purpose of the TSS HELP command function, instructions on use, and entry methods.
10	Describes the purpose of the TSS LIST command function, instructions on use, and entry methods.
11	Describes the purpose of the TSS LOCK/UNLOCK command function, instructions on use, and entry methods.
12	Describes the purpose of the TSS MODIFY command function, instructions on use, and entry methods.
13	Describes the purpose of the TSS MOVE command function, instructions on use, and entry methods.
14	Describes the purpose of the TSS PERMIT/REVOKE command function, instructions on use, entry methods, and detailed reference pages on each applicable keyword.
15	Describes the purpose of the TSS REFRESH command function, instructions on use, and entry methods.

Chapter	Description
16	Describes the purpose of the TSS RENAME command function, instructions on use, and entry methods.
17	Describes the purpose of the TSS REPLACE command function, instructions on use, entry methods, and detailed reference pages on each applicable keyword.
18	Describes the purpose of the TSS WHOHAS command function, instructions on use, and entry methods.
19	Describes the purpose of the TSS WHOOWNS command function, instructions on use, and entry methods.
20	Describes the purpose of the TSS WHOAMI command function, instructions on use, and entry methods.
21	Describes the purpose, standard formats and rules governing the use of the Command Propagation Facility (CPF).
22	Describes the purpose of each resource and provides detailed examples using both the ADDTO/REMOVE and PERMIT/REVOKE command functions.
Appendix A	Provides a list of prefixed resources.

CA-Top Secret Publications

The following publications are supplied with CA-Top Secret:

Title	Contents
Installation Guide	CA-Top Secret installation for VSE, including: installation and maintenance steps, startup and shutdown considerations, backup and recovery procedures, and Security File conversion.
Command Functions Guide	Comprehensive reference to the TSS command and CA-Top Secret resources.
Control Options Guide	Comprehensive reference of CA-Top Secret control options.
Implementation: BATCH, STC and APPC Guide	Provides for setting up security in Batch, STC and APPC environments.
Implementation: CICS Guide	Provides for setting up security in a CICS environment.
Messages and Codes Guide	Provides all CA-Top Secret messages and codes.
Planning Guide	General guide for planning a successful CA-Top Secret security implementation and describing the latest enhancements to CA-Top Secret.
Report and Tracking Guide	Details the use of TSSUTIL, TSSTRACK, TSSAUDIT, TSSCFILE and TSSCPR and provides sample reports.
Troubleshooting Guide	Includes CA-Top Secret debugging options and facilities, information to be prepared prior to contacting Technical Support, and an explanation of customer support.
User Guide	Conceptual overview of CA-Top Secret architecture and capablilities. Also includes implementation instructions that span all facilities, including: implementation how to's, customization, and the CA-Top Secret utilities.

All guides are updated as required. Instructions accompany each update package.

Related Publications

The common component services formerly known as CA90s have been enhanced and renamed CA Common Infrastructure Services, CA-CIS. All the documentation for the services exists in the following publications supplied by Computer Associates:

Name	Contents
CA-CIS Administrator Guide	A guide for system administrators.
CA-CIS CAICCI User Guide	Describes how to use the communication protocols needed for cross-system communication.
CA-CIS Installation Guide	Tells how to install the CA-CIS.
CA-CIS Message Guide	Lists messages and codes for CA-CIS.
CA-CIS Reference Guide	Describes how to access and use the VSE common components.
CA-CIS Systems Programmer Guide	Details the programming requirements for command, security, and signon exits.

The following publications relate to CA-Top Secret and are available from Computer Associates:

Title	Operating System
CA-EARL Reference Guide	MVS/VM/VSE
CA-EARL User Guide	MVS/VM/VSE
CA-EARL Systems Programmer Guide	VSE
CA-EARL Examples Guide	MVS/VM/VSE

Command Notation

Enter the following exactly as they appear in command descriptions:

UPPERCASE	identifies commands, keywords, and keyword values which must be coded exactly as shown.
MIXEDcase	identifies acceptable command abbreviations. The UPPER-CASE letters represent the minimum abbreviation possible. The lowercase letters of the command may be entered for further clarification **Note:** In some cases, the command processor may require a more detailed abbreviation due to user-defined resource being the same as a command abbreviation. In these cases, either enter the complete command or code a national or numeric character in one of the first four positions of the user-defined resource.
underlining	identifies default operands. These operands do not need to be entered to take effect.
Symbols	"" / * # () , must be coded exactly as shown.

The following items clarify command syntax; do not type when they appear:

lowercase	indicates keyword values which you must supply.
[ ]	identifies optional keywords.
|	separates alternative keywords or values; choose one.
{ }	indicates that you must enter one of the keywords.
...	means the preceding value may be repeated more than once.

The following table indicates the appropriate command format.

Sample Command	Explanation
TSS PER(acid) DSN(dsname)	You must supply a value for the ACID and for the data set name.
MODE(DORM|IMPL|WARN|FAIL)	You must choose **only** one of the keywords.

`TSS {ADDto  } (acid) MCSAUTH {(INFO)  }`
`    {REMove }                {(MASTER)}`
`    {REPlace}                {(SYS)   }`
`                             {(IO)    }`
`                             {(CONS)  }`
`                             {(ALL)   }`
	You must select a command function, enter the name of an ACID, enter the MCSAUTH keyword, and select an operand from the list.

Chapter 1. CA-Top Secret Command Functions Overview

This overview defines the purpose of CA-Top Secret command functions, and explains the entry methods used to issue the functions. Inexperienced security administrators should read this overview prior to entering CA-Top Secret command functions.

1.1 CA-Top Secret Command Functions

Security administrators use command functions to communicate their administrative requirements to CA-Top Secret. These requirements may range from the creation of an ACID to the definition of resource ownership.

CA-Top Secret command functions are independent of the system facility. The security administrator will use command functions in the same manner, regardless of whether the facility is CICS or BATCH.

1.1.1 CA-Top Secret Function List

Security administrators, and in some cases, users, may enter the following TSS functions. TSS command abbreviations appear in parentheses after the function name.

Table 1-1. TSS Function List

Function	Description
ADDTO (ADD)	Adds resource ownership and attributes to an ACID.
REMOVE (REM)	Removes resource ownership or attributes from an ACID.
ADMIN (ADM)	Grants administrative authorities to an administrator.
DEADMIN (DEA)	Removes administrative authorities from administrator.
CREATE (CRE)	Defines a new ACID to CA-Top Secret.
DELETE (DEL)	Deletes an ACID from the Security Record.
HELP *	Requests information about a CA-Top Secret function.
LIST (LIS)	Displays security data about an ACID(s).
LOCK (LO) *	Locks an online terminal. (OS/390 and VSE)
UNLOCK (UNL) *	Unlocks an online terminal. (OS/390 and VSE)
MODIFY (MODI) *	Displays or alters CA-Top Secret control options.
MOVE	Moves an ACID from one division or department to another.
PERMIT (PER)	Grants permission for ACIDs to access resources.
REVOKE (REV)	Revokes a resource permission.
RENAME (REN)	Changes the ACCESSOR ID assigned to an ACID.
REPLACE (REP)	Changes values of an attribute assigned to an ACID.
WHOHAS (WHOH)	Displays ACIDs who have access to resources.
WHOOWNS (WHOO)	Displays ACIDs who own resources.
WHOAMI *	Displays an individual ACID's security environment.

***** indicates those TSS commands which cannot be routed through the security network using the Command Propagation Facility (CPF).

The HELP and MODIFY commands will generate a TSS0299E KEYWORD KEYWORD ILLEGAL FOR FUNCTION message. LOCK, UNLOCK, and WHOAMI commands will generate a response from the local node instead. This occurs even when a TARGET keyword is used or if CPFTARGET is set to * or AUTO.

1.2 Command Syntax

In addition to command functions, there are other components that comprise a TSS command. All command syntax components are described in Figure 1 and Table 1-2.

```
TSS FUNCTION(acid | ACIDS | STC | AUDIT | RDT | DLF | ALL) KEYWORD(OPERAND)
 1     2                              3                          4        5
```

Figure 1. TSS Command Syntax

Table 1-2. TSS Command Syntax

Component	Description	Rules
1	TSS Command Name	Command must always begin with TSS.
2	Name of the function CA-Top Secret will perform (see Table 1-1)	A) Must immediately follow TSS. B) Only one function entered per TSS command. C) One or more spaces must be entered between TSS and the function.
3	Specifies the ACID being affected by the function.	See "Adding Resources" in the ADDTO/REMOVE section for details on the different ACID names.
4	Specifies the resource type or security attribute being processed by the function.	A) Keywords may be entered in any order. B) Online: Keywords may be entered from line to line without special action. C) Batch: The last keyword on a continuing line must be followed by a blank and a dash. The next Keyword can be entered on the next input line. D) Operand data can be continued on the following line by putting a + on the current line. The + lets you string data from one line to the next.
5	Enter the specific prefix, resource name, or the required value or name for a security attribute.	A) Refer to the specific function overview for details of each TSS Command function. B) Operands must be provided and () is required to indicate no value. If an operand is missing, any following keyword is ignored.

1.3 Entry Methods

CA-Top Secret functions may be entered freeform onto the command screen of an online terminal, or as input to the batch utility TSSCMNDB. The TSSCMNDB utility can process multiple commands.

Command Syntax:

```
TSS CREATE(USER01) TYPE(USER) NAME('H.PARKER') PASSWORD(1234,30,EXPIRE)
    SOURCE(GRAF0076) PROFILE(BUDGET,TAXES,CRIME) DSN(SYS.01)
    DEPT(DEPTB01)
```

Figure 2. Command Syntax

1.3.1 TSSCMNDB Batch Utility

TSSCMNDB reads multiple TSS input commands and passes them to command processors active in the TSSMNGR address space. The input to the utility, along with the result from the command processor, is displayed as SYSLST output. If any commands fail, TSSCMNDB will issue a non-zero return code.

Input to TSSCMNDB can be entered in two ways:

1. Eighty column card image statements immediately following the EXEC TSSCMNDB statement are accepted as SYSRDR input. This is the default method.
2. A sequential disk file with a filename to TSSCMDS will be accepted as input when UPSI 01 is set. The file should contain 80-character records and be in fixed/unblocked format.

Note: Only one of these methods can be active for each execution of TSSCMNDB.

Sample TSSCMNDB JCL

```
// JOB TSSCMNDB  ***  TSS Batch Command Utility  ***
// ID USER=SYSA,PWD=SYSA
*
*  This utility accepts input from either SYSRDR or a
*  sequential disk file based on the following UPSI setting
*
*  UPSI 00 - Accept input from SYSRDR
*  UPSI 01 - Accept input from sequential disk
*
// UPSI 00
// ASSGN SYS010,DISK,VOL=vvvvvv,SHR
// DLBL TSSCMDS,'CAI.TOP.SECRET.COMMAND.INPUT',,SD
// EXTENT SYS010,vvvvvv,1,0,xx,yy
// EXEC TSSCMNDB
TSS ...
TSS ...
TSS ...
/*
/&
```

1.4 Online and Batch Processing of Commands

After an ACID enters a TSS command function, CA-Top Secret will edit the entry for the correct syntax, and then determine if the ACID contains the proper administrative authority to enter the command function (refer to Rules and Procedures). If the command was entered properly, it will immediately be recognized by all systems and take effect.

1.4.1 Command Response Messages

Entry of TSS command functions causes CA-Top Secret to issue a variety of messages, all detailed in the *Messages and Codes Guide*. If a command is successful, CA-Top Secret will issue the message:

```
TSS0300I   xxxx FUNCTION SUCCESSFUL.
```

Failed Commands and Return Codes:

If the command failed, CA-Top Secret will issue the message:

```
TSS0301I   xxxx FUNCTION FAILED, RETURN CODE = XX
```

Note: Message TSS0301I will be followed by a message in the TSS0200 series that explains the cause of the problem.

Return Codes: XX will be of the following values:

Code	Definition
4	Syntax Error
8	Functional Error (such as data set not found)
16	Unexpected Error (Message TSS0390E will also be issued)

1.5 Rules and Procedures

The following rules and procedures govern the use of all TSS command functions.

1.5.1 Administrative Authority

CA-Top Secret will process only the command functions (with the exceptions of HELP and WHOAMI) issued by ACIDs who have administrative authority. This administrative authority is limited by the scope of the administrator. The chapter called "How to Use ADMIN/DEADMIN" provides more detailed information about administrative authority and administrative scope.

1.5.2 Scope

A security administrator generally has authority over resources and ACIDs that fall under his functional area of administration, such as a zone, department, division, or the entire installation.

Table 1-3 shows an example of how an organization might define its security administrators to CA-Top Secret, and the scope that would result. The table also provides examples of what administrators would and would not be able to do within their scope. The table is not all-inclusive, and depends on specific administrative authorities granted.

Table 1-3. Administrative Scope

Title	Scope	Example
MSCA	Entire installation	The master SCA (MSCA) can create all CA-Top Secret administrators, including SCAs, LSCAs, ZCAs, DCAs, VCAs, and auditors.
SCA	Entire installation	An SCA's scope of authority depends on the administrative authorities that were granted to him. An SCA can create ZCAs, DCAs, VCAs, Profile, and User ACIDs, but not other SCAs.
LSCA	A zone or LSCA	An LSCA can have all the authority of an SCA, but unlike the SCA, the LSCA must have a scope of authority assigned to it. This scope of authority can be one or more LSCAs and/or zones.
ZCA	A zone	A zone security administrator can permit access to resources that are owned by his zone, all connected divisions, departments and users within that zone, and may define profiles and perform maintenance for ACIDs that are within his scope. A ZCA can permit ACIDs in other zones to access his zone's resources, but cannot perform maintenance for ACIDs in other zones.
VCA	A division	A divisional security administrator can permit access to resources that are owned by his division, all departments and users within that division, and may define profiles and perform maintenance for ACIDs that are within his scope. A VCA can permit ACIDs in other divisions to access his division's resources, but cannot perform maintenance for ACIDs in other divisions.
DCA	A department	The department administrator has the same scope over a department that a VCA has over a division.

1.5.3 CA-Top Secret Administrator

There can be several types of security administrators with varying degrees of authority. All administrators are defined to CA-Top Secret, and therefore, have the capability to enter TSS command functions. There are cases, however, where the person who has the authority to approve security administration is not the same person who actually enters the command functions.

Chapter 2. Using the RDT Record

This chapter describes how to administer the Resource Descriptor Table (RDT) Record. In order to manage the RDT, the administrator must have MISC1(RDT) authority so that he can specify attributes, access levels, default access level as well as list the RDT Record itself. An administrator can be given MISC8(LISTRDT) authority to limit his RDT administrative functions to listing the RDT Record.

2.1 Purpose

The RDT Record is a table in the CA-Top Secret Security File. The RDT stores predefined resources, such as volumes, data sets, and terminals. User-defined resources can be added to the RDT by using the TSS ADD(RDT) command.

2.1.1 Modifying the RDT

The user may have one or several reasons for updating or modifying the RDT. These reasons can be divided into two main categories:

- **Modifying Existing Resource Classes**

  The user may want to modify an existing resource class to change its attributes. For example, the user can add default protection by assigning the DEFPROT attribute to the resource class. DEFPROT and the other attributes are discussed later in this chapter.

  Note: For predefined resource classes, only EXIT, DEFPROT, MERGE, ALLMERGE, and GENERIC attributes can be changed.

- **Defining New Resource Classes**

  The user may want to define non CA-Top Secret resource classes in the following situations:

  – IBM products that have requirements for a non-fixed or installation-defined resource class name.

    Under normal circumstances CA-Top Secret will have anticipated the use of standard IBM resource classes, however, there are exceptions.

  – OEM software or other vendor software packages have unique resource class names that are not defined by CA-Top Secret. While many security interfaces are predefined to CA-Top Secret, there are exceptions where the user must supply the resource class names.

  – Users must also define resource class names for installation-written security with its own resource classes, and any other customized site applications with resources and security of its own.

    Note that installation-written security may require separate naming conventions and access levels which are described later in this chapter.

2.1.2 Implementing the RDT

Sample Commands:

TSS command functions that relate to the RDT are shown below.

To define a new resource class to the RDT, enter:

```
TSS ADDTO(RDT) RESCLASS(resource class name) RESCODE(hex code) MAXLEN(nnn)
    [ATTR(attribute list)] [ACLST(access level list)]
    [DEFACC(default access level)]
```

To change the values of previously-defined resource classes, enter:

```
TSS REPLACE(RDT) RESCLASS(resource class name)
    [ATTR(attribute list)] [ACLST(access level list)]
    [DEFACC(default access level)]
```

To remove a previously-defined resource class definition, enter:

```
TSS REMOVE(RDT) RESCLASS(resource class name)
```

To list the entire RDT Record, enter:

```
TSS LIST(RDT)
```

To list a specific resource class or resource code defined to the RDT, enter:

```
TSS LIST(RDT) RESCLASS(resource type)
   -or-
TSS LIST(RDT) RESCODE(resource code)
```

Note: When LISTing the RDT, a MASK or NOMASK attribute will appear in the output signifying whether the resource supports masking.

MISC1(RDT) authority or MISC8(LISTRDT) authority is acceptable for the administrator to use the TSS LIST(RDT) command.

The two keywords RESCLASS and RESCODE are **required** when adding a resource to the RDT Record. Only RESCLASS is required for modifying, listing and removing a particular resource class name.

2.2 Applicable Keyword List

The following keywords are used with the RDT reserved ACID and may be used with the ADDTO(RDT) and REPLACE(RDT) command functions. The reference pages that follow contain detailed documentation for each keyword.

```
ACLST
ATTR
DEFACC
MAXLEN
RESCLASS
RESCODE
```

2.3 ACLST

Operating System: VSE, OS/390, and VM

Description: Administrators can define, change or remove access levels for the resource in the RDT (Resource Descriptor Table) Record.

TSS Commands: The following TSS commands can be used with the ACLST keyword: **ADDTO, REPLACE.**

Syntax:

```
TSS ADD(RDT) RESCLASS(resource type) RESCODE(hex code)
    [ACLST(access level list)]
```

The access level list can consist of any combination of any user- or CA-Top Secret-defined access levels. Common CA-Top Secret-defined access levels and their hexadecimal values follow:

ALL(FFFF)
AUTOLOG(4000)
BLP(8000)
BROWSE(0200)
CONTROL(0400)
CREATE(1000)
DELETE(1000)
FEOV(0200)
FETCH(8000)
FIND(1000)
GRPLOGON(1000)
LOGON(8000)
MREAD(4400)
MWRITE(2400)
MULTI(0400)
NOCREATE(0100)
NONE(0000)
NONSHR(2000)
PURGE(0100)
READ(4000)
REPL(0800)
SCRTCH(0800)
SHR(4000)
SUROGATE(2000)
UPDATE(8000)
WRITE(2000)

For more information concerning the RDT Record, refer to the *User Guide*.

Note:

- Access levels within the ACLST should be unique and in descending hexadecimal order so that permits with multiple access levels display the highest possible access level. For example, if the list specifies READ,UPDATE(6000); the UPDATE implies READ and a permit is issued for UPDATE access. The TSS LIST command will show that the permit includes READ access and will display READ instead of UPDATE. The access level will be displayed correctly if the ACLST is specified as UPDATE(6000),READ.
- All hexadecimal values must be unique. You cannot specify two different access levels with the same hexadecimal value.
- When using ACLST with a TSS REPLACE command, the entire access list is replaced by the values specified in the command.

Authority: CA-Top Secret administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE resource classes in the RDT Record.

Types: The ACLST keyword is only used with the **RDT** ACID.

Examples:

To add a new resource called #PRODUCT to the RDT Record with READ and WRITE access levels, the administrator enters:

```
TSS ADD(RDT) RESCLASS(#PRODUCT) ACLST(READ,WRITE)
```

Note: To add new access levels to a resource class that is already defined in the RDT Record, use the REPLACE function, as in the following example:

```
TSS REP(RDT) RESCLASS(#PRODUCT) ACLST(READ,WRITE)
```

If the administrator wants his own unique access levels, which would be more applicable to the resource, he must specify the hexadecimal values associated with each access level:

```
ACLST(CALL=4200,ANSWER=8400)
```

or combine predefined values with his own unique access levels:

```
ACLST(READ,ANSWER=8400)
```

To remove an access level list, the administrator uses the REPLACE command function and specifies ATTR(NOACCESS). For example:

```
TSS REP(RDT) RESCLASS(#PRODUCT) ATTR(NOACCESS)
```

2.4 ATTR

Operating System: VSE, OS/390, and VM

Description: To define or change a resource to the RDT (Resource Descriptor Table) Record with one or more attributes.

TSS Commands: The following TSS commands can be used with the ATTR keyword: **ADDTO, REPLACE.**

Syntax:

```
TSS ADD(RDT) RESCLASS(resource type) RESCODE(hex code)
    ATTR(attribute list)
```

Operand Descriptions: The following operands can be used with the ATTR keyword:

Operand	Description
EXIT	Calls the installation exit for this resource.
NOEXIT	Deactivates the installation exit.
DEFPROT	Protects this resource by default.
NODEFPROT	Deactivates default protection.
PRIVPGM	Supports PRIVPGMs for this resource.
NOPRIVPGM	Deactivates PRIVPGM support.
LIB	Supports LIB with PRIVPGM for this resource.
NOLIB	Deactivates support for LIB with PRIVPGM.
LONG	Supports 44 character permissions.
SHORT	Supports 8 character permissions.
MASK	Supports masking characters in a TSS PERMIT.
NOMASK	Turns off previously changed MASK attribute.
MERGE	Uses AUTH(MERGE) for access checking of this resource.
NOMERGE	Deactivates AUTH(MERGE) option for access checking.
ALLMERGE	Uses AUTH(ALLMERGE) for access checking of this resource class.
NOALLMERGE	Deactivates AUTH(ALLMERGE) option for access checking.
VMUSER	Supports VMUSER for this resource.
NOVMUSER	Deactivates VMUSER support.

GENERIC Defines a similar set of resources as one generic prefix.

NONGENERIC Changes a generic attribute to a non-generic one. A non-generic attribute only supports general resources. That is, resources that do not support masking. It treats the specific resources within the resource class as fully qualified names. Refer to the chapter called "How to Use PERMIT/REVOKE" for further information on generic prefixing. EXIT, DEFPROT, MERGE, ALLMERGE and GENERIC are the only site modifiable attributes which can be changed for predefined resources.

Note:

- All of the operands used to deactivate an attribute can only be used with a TSS REPLACE(RDT) command function.
- The following default attributes are in effect when adding user-defined resource classes to the RDT unless the corresponding overriding attribute is specified: NOEXIT|EXIT, NODEFPROT|DEFPROT, NOPRIVPGM|PRIVPGM, NOLIB|LIB, SHORT|LONG, MASK|NOMASK, NOMERGE|MERGE, NOALLMERGE|ALLMERGE, NOVMUSER|VMUSER, GENERIC|NONGENERIC.
- If you defined a resource as maskable, all those currently signed on users with that permitted resource type will start to fail. Those users will have to refresh their security environments. The change to the RDT not only sets up for the new permissions but causes all of the security validations to treat that class as maskable. Those that logged on before the switch have the wrong internal record format and are required to refresh or log off and log on.

Authority: Administrators must have MISC1(RDT) authority, via the ADMIN function, to ADD or REMOVE resource classes in the RDT Record.

Types: The ATTR keyword is used only with the **RDT** ACID.

Examples:

To add #PRODUCT to the RDT Record and give it default protection, the administrator enters:

```
TSS ADD(RDT) RESCLASS(#PRODUCT)
    RESCODE(02) ATTR(DEFPROT)
```

To remove an attribute that he has attached to a specific resource class, the administrator uses the REPLACE command function and prefixes the attribute with NO. For example, to remove default protection from resource class #PRODUCT:

```
TSS REP(RDT) RESCLASS(#PRODUCT)
    ATTR(NODEFPROT)
```

To remove the LONG attribute which is already attached to a specific resource class, specify ATTR(SHORT).

Note: For PRIVPGM, LIB and VMUSER the security driver must also support these features. For all predefined CA-Top Secret resource classes (such as DATASET and VOLUME), only the DEFPROT, EXIT, MERGE, ALLMERGE and GENERIC attributes may be altered through the TSS REPLACE(RDT) command function.

2.5 DEFACC

Operating System: VSE, OS/390, and VM

Description: To assign the default access to be used on a TSS PERMIT for a resource that has been added to the RDT (Resource Descriptor Table) Record.

TSS Commands: The following TSS command can be used with the DEFACC keyword: **REPLACE, ADDTO.**

Syntax:

```
TSS ADD(RDT) RESCLASS(resource type) RESCODE(hex code)
    [DEFACC(default access list)]
```

If not specified, the default access is NONE.

The following are predefined CA-Top Secret access levels, with their associated hexadecimal values.

ALL(FFFF)
AUTOLOG(4000)
BLP(8000)
BROWSE(0200)
CONTROL(0400)
CREATE(1000)
DELETE(1000)
FEOV(0200)
FETCH(8000)
FIND(1000)
GRPLOGON(1000)
LOGON(8000)
MREAD(4400)
MULTI(0400)
MWRITE(2400)
NOCREATE(0100)
NONE(0000)
NONSHR(2000)
PURGE(0100)
READ(4000)
REPL(0800)
SCRTCH(0800)
SHR(4000)
SUROGATE(2000)
UPDATE(8000)
WRITE(2000)

For more information concerning the RDT Record, refer to the *User Guide.*

Note: The access level specified by DEFACC must match the applicable access levels indicated by the ACLST entries for that resource. If they do not match or, if no ACLST was specified, you will receive a TSS0282E error message.

When creating a user-defined resource class, if the access level is not one that is known to CA-Top Secret, you must specify the hex value in the DEFACC as well as the ACLST fields. For example:

```
TSS ADD(RDT) RESCLASS(NEWRES) RESCODE(01) ACLST(ALLOW=4000)
    DEFACC(ALLOW=4000)
```

Authority: Administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE resource classes in the RDT Record.

Types: The DEFACC keyword is used with the RDT ACID only.

Examples:

To establish a TSS PERMIT default access level of READ to the #PRODUCT resource, the administrator enters:

```
TSS ADD(RDT) RESCLASS(#PRODUCT) RESCODE(02)
    DEFACC(READ)
```

Now, when any #PRODUCT resource is permitted to a user and the ACCESS keyword is omitted from the PERMIT, a default access level of READ will be used.

2.6 MAXLEN

Operating System: VSE, OS/390, and VM

Description: To define the maximum permission length for the user resource class being created.

TSS Commands: The following TSS command can be used with the MAXLEN keyword: **ADDTO.**

Syntax:

```
TSS ADDTO(RDT) RESCLASS(resource name) RESCODE(hex code) MAXLEN(nnn)
```

Command length — decimal value from 1 to 255

Operand Descriptions: The following operand can be used with the MAXLEN keyword:

Operand	Description
nnn	Is a decimal value between 1 and 255.

Authority: Administrators must have MISC1(RDT) authority, via the ADMIN function, to ADD fields in the RDT Record.

Types: The MAXLEN keyword is used only with the **FDT** and **RDT** records.

Examples:

To define an RDT field length of 17 use the following command:

```
TSS ADD(RDT) RESCLASS(#PRODUCT) RESCODE(3F) MAXLEN(17)
```

2.7 RESCLASS

Operating System: VSE, OS/390, and VM

Description: To add or remove user-defined resource classes to or from the RDT (Resource Descriptor Table) Record when RDT is the target ACID name. The TSS command, logging, and the security interface honor this name. The TSS LIST command is used with RESCLASS to list data from the RDT Record.

TSS Commands: The following TSS commands can be used with the RESCLASS keyword: **REPLACE, LIST, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(RDT) RESCLASS(resource type) RESCODE(hex code)
```

Keyword length — 1-8 characters.

Capacity of list — 1 resource class per command. RESCLASS and RESCODE are required when adding a resource to the RDT Record.

For more information concerning the RDT Record, refer to the *User Guide*. For information about predefined RDT resources, refer to Chapter 22, “Summary of Resources” on page 22-1.

Note: To avoid any possibility of a dynamically-defined resource conflicting with a predefined CA-Top Secret resource class, we recommend that the dynamically-defined resource class have a national (@,#,$) or numeric (0-9) in one of the first four characters of the name. The first four characters of all resource class names must be unique and cannot conflict with any dynamically-defined or predefined resource class name.

Any number of resource classes may be added to the RDT up to RESCODE 3F. The resource class will immediately be usable with all RACF macros. For new resource classes, there is a limitation of 10 that may be added between IPLs for purposes of RACROUTE REQUEST=STAT or (RACSTAT). Any resource classes, beyond the limit of 10, that are added between IPLs will not be found by RACSTAT until after the next IPL.

Authority: Administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE resource classes in the RDT Record. Administrators may have MISC1(RDT) or MISC8(LISTRDT) authority, via the TSS ADMIN function, to LIST resource classes in the RDT Record.

Types: The RESCLASS keyword is used with the RDT only.

Examples:

To add #PRODUCT to the RDT Record, the administrator enters:

```
TSS ADD(RDT) RESCLASS(#PRODUCT) RESCODE(3F)
```

To remove #PRODUCT from the RDT Record, the administrator enters:

```
TSS REMOVE(RDT) RESCLASS(#PRODUCT)
```

Note: Removing a resource class from the RDT Record requires that all ownership of the resource class is previously removed.

To list data concerning how FCTs will be processed, the administrator enters:

```
TSS LIST(RDT) RESCLASS(FCT)
```

2.8 RESCODE

Operating System: VSE, OS/390, and VM

Description: To add user-defined resource classes to or from the RDT (Resource Descriptor Table) Record when RDT is the target ACID name. The LIST command is used to list data from the RDT Record (i.e., resource class, access level, attributes) about how a specifed resource code was processed.

TSS Commands: The following TSS commands can be used with the RESCODE keyword: **ADDTO, LIST.**

Syntax:

```
TSS ADD(RDT) RESCLASS(resource type) RESCODE(hex code)
```

Keyword length — a two-digit hexadecimal code ranging from 01 - 3F (due to TSS ADMIN restrictions).

Capacity of list — 1 resource code per command.

RESCODE (as well as RESCLASS) is required when adding a resource to the RDT Record.

RESCODE is the two-digit hexadecimal code (01-3F) which is passed to FRACHECK to indicate the type of resource.

For more information concerning the RDT Record, the administrator should refer to the *User Guide.*

Authority: Administrators must have MISC1(RDT) authority, by the TSS ADMIN function, to ADD resource classes in the RDT Record. Administrators may have MISC1(RDT) or MISC8(LISTRDT) authority, by the TSS ADMIN function, to LIST resource classes in the RDT Record.

Types: The RESCODE keyword is used with the RDT ACID only.

Examples:

To add #PRODUCT to the RDT Record, the administrator enters:

```
TSS ADD(RDT) RESCLASS(#PRODUCT) RESCODE(3F)
```

To remove #PRODUCT from the RDT Record, the administrator enters:

```
TSS REMOVE(RDT) RESCLASS(#PRODUCT)
```

To list data concerning how resource code 3F will be processed, the administrator enters:

```
TSS LIST(RDT) RESCODE(3F)
```

2.9 Resource Masking

The resource masking feature lets you do the following:

- Change existing non-maskable resources to support masking by simply entering the following command

  ```
  TSS REPLACE(RDT) RESCLASS(resclass) ATTR(MASK)
  ```

  which will convert the resource to support masking although the maximum number will remain at eight.

  If you have an existing resource that you want to own which is longer than eight characters, you must revoke and remove all users of that resource class, remove the resclass from the RDT, and re-create the resource class using the method described in the next item.

- Create user-defined resources to support ownership longer than eight characters by specifying the following:

  ```
  TSS ADD(RDT) RESCLASS(resclass) ATTR(MASK)
  ```

- List the resource class to show several new features such as: a MASKABLE or NOMASK resource, a MAXOWN(nn) attribute displaying the maximum value for an ownable resource, and a MAXPERMIT(nnn) attribute displaying the maximum value for a permitted resource.

- Define lengths up to 255 characters with the MAXLEN(nnn) keyword. In prior releases, ATTR(LONG) implies MAXLEN(44).

The following example illustrates how the new attributes are listed for a resource:

```
TSS LIST(RDT) RESCLASS(TERMINAL)

ACCESSORID = *RDT*     NAME       = RESOURCE DEFINITIONS

RESOURCE CLASS = TERMINAL
RESOURCE CODE = X'E3'
     ATTRIBUTE = NOMASK,MAXOWN(08),MAXPERMIT(008)
TSS0300I  LIST     FUNCTION SUCCESFUL
```

There are some situations that can occur when changing resources between maskable and non-maskable. First of all, any resource that can be owned at more than eight characters cannot have masking turned off. Second, users should be careful when turning masking on for an existing resource with permits. Any permit containing a masking character (*,+,%,-) will not have existing permits work as if masked. This means you may want to revoke all of those permissions to avoid confusion. If a permit containing a masking character was executed prior to the RDT change to support masking, then a listing of this permission would show ATTRIB = NONMASK to signify that it won't be treated as a mask. You might experience some difficulty if a masking character is used in the first

byte of ownership. Because of internal requirements, a mask in the first byte is stored in an altered state from a non-masked situation. An example of this situation follows.

Assume resclass OTRAN is non-maskable as is the default. If you take ownership of a resource such as OTRAN(TST*) then it can be permitted. However, if you then turn on masking for OTRAN using the following command, you have redefined what has been owned.

```
TSS REPL(RDT) RESCLASS(OTRAN) ATTR(MASK)
```

If you now try to permit OTRAN(TST*), it would fail for resource not owned, although you had previously owned it. Now, with mask on, you own OTRAN(TST*) again which works. Assuming you gave ownership to the same department. If you list that department DATA(RESOURCE) you will now see the OTRAN TST* all owned twice. This is because internally they are different although externally they will look the same. To eliminate any possibility of such confusion, it is recommended that before turning masking on for any existing resource, you inspect all existing permissions and ownerships for that resource class and eliminate any that contain masking characters.

Note: If you defined a resource as maskable, all those currently signed on users with that permitted resource type will start to fail. Those users will have to refresh their security environments. The changed to the RDT not only sets up for the new permissions but causes all of the security validations to treat that class as maskable. Those that logged on before the switch have the wrong internal record format and are required to refresh or log off and log on.

Chapter 3. Using the FDT Record

This chapter describes how to administer the Field Descriptor Table (FDT) Record. In order to manage the FDT, the administrator must have MISC1(RDT) authority so that he can add to, remove from, and list the FDT Record itself. MISC8(LISTRDT) authority may be given to an administrator to limit his authority to listing the FDT Record only.

3.1 Purpose

The FDT Record is a table in the CA-Top Secret Security File. The FDT stores predefined fields, such as those included in SEGMENT CICS and SEGMENT CA-PC. User-defined fields can be added to the FDT by using the TSS ADD(FDT) command.

3.1.1 Modifying the FDT

The user may have one or several reasons for updating or modifying the FDT. These reasons can be divided into two main categories:

- **Modifying Existing Field Classes**

  The user may want to modify an existing field to change its attributes. For example, the user may wish to change the display of a field when a user is LISTed. Fields predefined by CA-Top Secret cannot be modified by the user.

- **Defining New Fields**

  The user may want to use non CA-Top Secret fields to define installation information (by user ACID) that can be maintained or extracted by application programs. Applications can extract and update this user information using the RACROUTE macro. Extract of the FDT may only be performed from the USER record of an ACID.

3.1.2 Implementing the FDT

Sample FDT Commands:

The following TSS command functions relate to the FDT.

To define a new field to the FDT, enter:

```
TSS ADD(FDT) FDTNAME(fieldname) FDTCODE(hex code)
    SEGMENT(segmentname) MAXLEN(nn) DISPLAY(fieldname)
```

To change the values of user-defined fields, enter:

```
TSS REPLACE(FDT) FDTNAME(fieldname)
    SEGMENT(segmentname) MAXLEN(nn) DISPLAY(fieldname)
```

To remove a user-defined field, enter:

```
TSS REMOVE(FDT) FDTNAME(fieldname)
```

Listing the FDT: The administrator can list the **entire** FDT Record by entering:

```
TSS LIST(FDT)
```

The administrator can list a specific field name, field code, segment, or display value defined to the FDT by entering one of the following commands:

```
TSS LIST(FDT) FDTNAME(field type)
- or -
TSS LIST(FDT) FDTCODE(hex code)
- or -
TSS LIST(FDT) SEGMENT(segment name)
- or -
TSS LIST(FDT) DISPLAY('current display name')
```

Note:

- MISC1(RDT) authority or MISC8(LISTRDT) authority is required for the administrator to use the TSS LIST(FDT) command.
- The TSS LIST(FDT) FDTCODE(hex code) command can only be used to list user-defined fields.

3.2 Applicable Keyword List

The following keywords are used with the FDT reserved ACID and may be used with the ADDTO(FDT) and REPLACE(FDT) command functions. The reference pages that follow contain detailed documentation for each keyword.

```
ATTR
DISPLAY
FDTCODE
FDTNAME
MAXLEN
SEGMENT
```

The FDTCODE, FDTNAME, and MAXLEN keywords are **required** when adding a resource to the FDT Record. Only FDTNAME is required for modifying, listing and removing a particular field name.

3.3 ATTR

Operating System: VSE, OS/390, and VM

Description: Administrators can add or replace attributes to a field in the FDT (Field Descriptor Table) Record.

TSS Commands: The following TSS commands can be used with the ATTR keyword: **ADDTO, REPLACE.**

Syntax:

```
TSS ADD(FDT) FDTNAME(field name) FDTCODE(hex code)
    MAXLEN(40) ATTR(attribute list)
```

Operand Description: The following operands can be used with the ATTR keyword:

Operand	Description
MIXED	Allows display of mixed case data for a field in the FDT Record.
NONDISP	Prohibits display of a field when an administrator issues a TSS LIST command on the ACID. The data can be extracted or modified using the Application Interface or the RACROUTE macro, but not displayed using TSS LIST.

For more information concerning the FDT Record, refer to the *User Guide*.

Authority: CA-Top Secret administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE fields in the FDT Record.

Types: The ATTR keyword is used with the **RDT** and **FDT** records.

Examples:

To add $TAX information to an ACID in mixed case, the administrator enters:

```
TSS ADD(FDT) FDTNAME($TAX) FDTCODE(44) MAXLEN(40) ATTR(MIXED)
```

If ATTR(MIXED) is not given, the information will be added to the user in uppercase.

3.4 DISPLAY

Operating System: VSE, OS/390, and VM

Description: Administrators can define, change or list the display value for the field in the FDT (Field Descriptor Table) Record.

TSS Commands: The following TSS commands can be used with the DISPLAY keyword: **ADDTO, LIST, REPLACE.**

Syntax:

```
TSS ADD(FDT) DISPLAY(fieldname) FDTNAME(field name)
    FDTCODE(hex code)
```

Field length — 1-11 characters

For more information concerning the FDT Record, refer to the *User Guide*.

Authority: CA-Top Secret administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE fields in the FDT Record.

Types: The DISPLAY keyword is only used with the **FDT** record.

Examples:

To add a new field called $PERS to the FDT Record with a DISPLAY value of EMPLOY, the administrator enters:

```
TSS ADD(FDT) FDTNAME($PERS) FDTCODE(1E) SEGMENT(PERSDEPT)
    MAXLEN(11) DISPLAY('EMPLOY')
```

If the DISPLAY value in not given, it will default to the same value specified for FDTNAME.

3.5 FDTCODE

Operating System: VSE, OS/390, and VM

Description: To add user-defined field names to the FDT (Field Descriptor Table) Record when FDT is the target ACID name.

TSS Commands: The following TSS command can be used with the FDTCODE keyword: **ADDTO, LIST.**

Syntax:

```
TSS ADD(FDT) FDTNAME(field name) FDTCODE(hex code)
    MAXLEN(nnnnn)
```

Keyword length — a unigue two-digit hexadecimal code ranging from 01 - FF.

- FDTCODE (as well as MAXLEN and FDTNAME) is required when adding a resource to the FDT Record.
- For more information concerning the FDT Record, the administrator should refer to the *User Guide*.

Authority: Administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD field names in the FDT Record. Administrators may have either MISC1(RDT) or MISC8(LISTRDT) authority, via the TSS ADMIN function, to LIST the FDT Record.

Types: The FDTCODE keyword is used with the FDT ACID only.

Examples:

To add PERSDEPT to the FDT Record, the administrator enters:

```
TSS ADD(FDT) FDTNAME($PERSDEPT) FDTCODE(3F) MAXLEN(40)
```

To remove $PERSDEPT from the FDT Record, the administrator enters:

```
TSS REMOVE(FDT) FDTNAME($PERSDEPT)
```

3.6 FDTNAME

Operating System: VSE, OS/390, and VM

Description: To add or remove user-defined field names to or from the FDT (Field Descriptor Table) Record when FDT is the target ACID name.

TSS Commands: The following TSS commands can be used with the FDTNAME keyword: **REPLACE, LIST, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(FDT) FDTNAME(fieldname) FDTCODE(hex code)
    MAXLEN(nnnnn)
```

Keyword length — 1-8 characters.

- FDTNAME, FDTCODE, and MAXLEN are required when adding a resource to the FDT Record.
- To prevent any possibility of your field name conflicting with any future CA-Top Secret resources, include either a numeric (0-9) or a national ($ # @) in the FDTNAME name.
- The first four characters of all field names must be unique and cannot conflict with any dynamically-defined or predefined field name.
- For more information concerning the FDT Record, refer to the *User Guide*.

Authority: Administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE field names in the FDT Record. Administrators may have either MISC1(RDT) or MISC8(LISTRDT) authority, via the TSS ADMIN function, to LIST the FDT Record.

Types: The FDTNAME keyword is used with the FDT only.

Examples:

To add $PERSDEPT to the FDT Record, the administrator enters:

```
TSS ADD(FDT) FDTNAME($PERSDEPT) FDTCODE(3F) MAXLEN(11)
```

To remove $PERSDEPT from the FDT Record, the administrator enters:

```
TSS REMOVE(FDT) FDTNAME($PERSDEPT)
```

Note: Fields can be removed from the FDT even if a user ACID contains those fields. If a new FDT entry is defined using the same FDTCODE, the results are unpredictable. A TSS LIST of a user ACID will remove any field information no longer in the FDT.

3.7 MAXLEN

Operating System: VSE, OS/390, and VM

Description: To define or change the number of bytes that will be allowed to be entered for the user-defined FDT entry.

TSS Commands: The following TSS command can be used with the MAXLEN keyword: **ADDTO, REPLACE.**

Syntax:

```
TSS ADD(FDT) MAXLEN(nnnnn)
```

Command length — decimal value from 1 to 32767

Operand Descriptions: The following operand can be used with the MAXLEN keyword:

Operand	Description
nnnnn	Is a decimal value between 1 and 32767.

Authority: Administrators must have MISC1(RDT) authority, via the ADMIN function, to ADD or REPLACE fields in the FDT Record.

Types: The MAXLEN keyword is used only with the **FDT** and **RDT** records.

Examples:

To change an FDT field length from 8 to 17 on the following command:

```
TSS ADD(FDT) FDTNAME($PERS) MAXLEN(8) SEGMENT(PERSDEPT)
    FDTCODE(1E) DISPLAY('PERSDEPT')
```

the administrator enters:

```
TSS REP(FDT) FDTNAME($PERS) MAXLEN(17)
```

Note: 32,767 is the total number of bytes available for **all** user-defined fields.

3.8 SEGMENT

Operating System: VSE, OS/390, and VM

Description: To assign fields to a specific segment. You cannot add user-defined fields to system-defined segments.

TSS Commands: The following TSS commands can be used with the SEGMENT keyword: **REPLACE, ADDTO, LIST.**

Syntax:

```
TSS ADD(FDT) SEGMENT(segmentname)
```

Command length — 1-8 characters

If not specified, the default segment is BASE.

The following are predefined CA-Top Secret segments:

ALL
BASE
CA-PC
CICS
DFP
DLFDATA
IESIS
LANGUAGE
OMVS
OPERPARM
TSO
WORKATTR

For more information concerning the FDT Record, refer to the *User Guide*.

Authority: Administrators must have MISC1(RDT) authority, via the TSS ADMIN function, to ADD or REMOVE segments in the FDT Record.

Examples:

To include a field called $ACCTS in a segment named TAXINFO, the administrator enters:

```
TSS ADD(FDT) FDTNAME($ACCTS) FDTCODE(1E) SEGMENT(TAXINFO)
    MAXLEN(12) DISPLAY('SALARY ACCT')
```

To find all field names that are in the TAXINFO segment, the administrator enters:

```
TSS LIST(FDT) SEGMENT(TAXINFO)
```

Chapter 4. Using the SDT Record

This chapter describes how to administer the Static Data Table (SDT) Record. To manage the SDT, the administrator must have MISC3(SDT) authority so that he can add to, remove, or list the SDT Record.

Note: MISC8(LISTSDT) authority can be used to limit the administrator's authority to only listing the SDT Record.

4.1 Purpose

The SDT Record is a reserved ACID and a Security File repository for internal, non-volatile data which is used with various PERMIT administrative functions. The SDT stores six distinct record elements which include:

CALENDAR records
MAP records (MAPREC)
MASK records (MASKREC)
RLP records (RECORD)
SELECT records
TIME records (TIMEREC)

These unique user-defined record IDs can be added to the SDT using the TSS ADD(SDT) command function.

At CA-Top Secret initialization, the currently-defined elements are loaded into memory and are used as part of your security environment.

4.1.1 Modifying the SDT

Modifications to the SDT are not reflected automatically in the in-core storage copy of any modified element, since the administrator often requires several commands to building or modify an SDT Record element. When completed, the administrator can refresh the elements in in-core storage with a TSS MODIFY command, as follows:

```
TSS MODIFY(SDTTABLE)
TSS MODIFY(SDTTABLE(RECORD))
```

Refer the *Control Options Guide* for additional syntax of SDTTABLE refresh.

4.1.2 Implementing the SDT

The SDT record elements are created as they are needed using the TSS ADD(SDT) command. Existing records are then maintained using the TSS REPLACE(SDT), TSS REMOVE(SDT), and TSS DELETE(SDT) commands. Once defined, most record elements can be combined with the PERMIT command to further refine your security environment.

The detailed procedures for implementing Record Level Protection (RLP) and Screen Level Protection (SLP) can be found in Chapters 4 and 12 of the *Implementation: CICS Guide*.

The remainder of this section contains sample commands for defining, replacing, removing, deleting, and listing the record elements of the SDT and their associated fields.

Sample SDT Commands for CALENDAR Records:

To define a new CALENDAR record to the SDT, enter:

```
TSS ADD(SDT) CALENDAR(cal-name) DESCRIPT(descript-name)
             YEAR(yyyy) DAYS(days,...)
             EXCLUDE(mm/dd,mm/dd,...) INCLUDE(mm/dd,mm/dd,...)
```

To replace an existing CALENDAR record with new dates, enter:

```
TSS REPLACE(SDT) CALENDAR(cal-name)
                 YEAR(yyyy) DAYS(days,...)
                 EXCLUDE(mm/dd,mm/dd,...) INCLUDE(mm/dd,mm/dd,...)
```

To remove only specified dates from an existing CALENDAR record, enter:

```
TSS REMOVE(SDT)  CALENDAR(cal-name)
                 YEAR(yyyy) DAYS(days,...)
                 EXCLUDE(mm/dd,mm/dd,...) INCLUDE(mm/dd,mm/dd,...)
```

To delete a specified CALENDAR record from the SDT, enter:

```
TSS DELETE(SDT) CALENDAR(cal-name)
```

To list all or only a specified CALENDAR record from the SDT, enter:

```
TSS LIST(SDT) CALENDAR(ALL|cal-name)
```

Sample SDT Commands for MAP Records:

For complete details on SDT MAP administration, refer to Chapter 8, "Maintaining Special Security Records", in the CA-Top Secret *User Guide*.

To define a field in a new or existing MAP record to the SDT, enter:

```
TSS ADD(SDT) MAPREC(map-name) DESCRIPT(descript-name)
             MAPDATA(fieldname,type,row,column,length)
```

To replace an existing MAP record with a new field, enter:

```
TSS REPLACE(SDT) MAPREC(map-name)
                 MAPDATA(fieldname,type,row,column,length)
```

To remove up to five fields from an existing MAP record, enter:

```
TSS REMOVE(SDT) MAPREC(map-name)
                SDTFNAME(mapdata-fld1,...mapdata-fld5)
```

To delete a specified MAP record from the SDT, enter:

```
TSS DELETE(SDT) MAPREC(map-name)
```

To list all or only a specified MAP record from the SDT, enter:

```
TSS LIST(SDT) MAPREC(ALL|map-name)
```

Sample SDT Commands for MASK Records:

For complete details on SDT MASK administration, refer to Chapter 8, "Maintaining Special Security Records", in the CA-Top Secret *User Guide*.

To define a new MASK record to the SDT, enter:

```
TSS ADD(SDT) MASKREC(mask-name) DESCRIPT(descript-name)
             MASKDATA(fieldname,type,offset,length,mask-value-literal)
```

To replace an existing MASK record with a new field, enter:

```
TSS REPLACE(SDT) MASKREC(mask-name)
              MASKDATA(fieldname,type,offset,length,mask-value-literal)
```

To remove up to five fields from an existing MASK record, enter:

```
TSS REMOVE(SDT) MASKREC(mask-name)
                SDTFNAME(maskdata-fld1,...maskdata-fld5)
```

To delete a specified MASK record from the SDT, enter:

```
TSS DELETE(SDT) MASKREC(mask-name)
```

To list all or only a specified MASK record from the SDT, enter:

```
TSS LIST(SDT) MASKREC(ALL|mask-name)
```

Sample SDT Commands for RLP Records:

For complete details on SDT RLP administration, refer to Chapter 12, "Implementing Security", in the CA-Top Secret *Implementation: CICS Guide*.

To define a new RLP record to the SDT, enter:

```
TSS ADD(SDT) RECORD(rlp-name) DESCRIPT(descript-name)
             RECDATA(fieldname,type,offset,length)
```

To replace an existing RLP record with a new field, enter:

```
TSS REPLACE(SDT) RECORD(rlp-name)
                 RECDATA(fieldname,type,offset,length)
```

To remove up to five fields from an existing RLP record, enter:

```
TSS REMOVE(SDT) RECORD(rlp-name)
    SDTFNAME(recdata-fld1,...recdata-fld5)
```

To delete a specified RLP record from the SDT, enter:

```
TSS DELETE(SDT) RECORD(rlp-name)
```

To list all or only a specified RLP from the SDT, enter:

```
TSS LIST(SDT) RECORD(ALL|rlp-name)
```

Sample SDT Commands for SELECT Records:

To define a new SELECT record to SDT, enter:

```
TSS ADD(SDT) SELECT(sel-name) DESCRIPT(desc-name)
             SELDATA('IF sel-expression

              [AND] sel-expression...')
              [ OR]
```

To replace an existing SELECT record with a new sel-expression statement(s), enter:

```
TSS REPLACE(SDT) SELECT(sel-name)
                 SELDATA('IF sel-expression

                 [AND] sel-expression...')
                 [ OR]
```

To delete a specified SELECT record from the SDT, enter:

```
TSS DELETE(SDT) SELECT(sel-name)
```

To list all or only a specified SELECT from the SDT, enter:

```
TSS LIST(SDT) SELECT(ALL|sel-name)
```

Sample SDT Commands for TIME Records:

To define a new TIME record to the SDT, enter:

```
TSS ADD(SDT) TIMEREC(time-name) DESCRIPT(descript-name)
             RANGE(hmm,hhmm,...)
```

To replace an existing TIME record with a new range, enter:

```
TSS REPLACE(SDT) TIMEREC(time-name) RANGE(hhmm:hhmm,...)
```

To remove only specified times from an existing TIME record, enter:

```
TSS REMOVE(SDT) TIMEREC(time-name)
```

To delete a specified TIME record from the SDT, enter:

```
TSS DELETE(SDT) TIMEREC(time-name)
```

To list all or only a specified TIME record from the SDT, enter:

```
TSS LIST(SDT) TIMEREC(ALL|time-name)
```

4.2 Applicable Keyword List

The following keywords can be used with the six types or record elements in the SDT reserved ACID. These keywords can be used with the ADDTO(SDT) and REPLACE(SDT) command functions. The following pages list each keyword in alphabetical order with a detailed description of each one.

Applicable Keywords for CALENDAR Records:

CALENDAR
DAYS
DESCRIPT
DAYS
EXCLUDE
INCLUDE
YEAR

Applicable Keywords for MAP Records:

DESCRIPT
MAPREC
MAPDATA
SDTFNAME

Applicable Keywords for MASK Records:

DESCRIPT
MASKREC
MASKDATA
SDTFNAME

Applicable Keywords for RLP Records:

DESCRIPT
RECDATA
RECORD
SDTFNAME

Applicable Keywords for SELECT Records:

DESCRIPT
SDTFNAME
SELDATA
SELECT

Applicable Keywords for TIMEREC Records:

DESCRIPT
RANGE
SDTFNAME
TIMEREC

4.3 CALENDAR

Operating System: VSE, OS/390, and VM

Description: Administrators can provide an up to eight-character name by which CA-Top Secret references a CALENDAR record.

TSS Commands: The following TSS commands can be used with the CALENDAR keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT) CALENDAR(cal-name)
```

Operand Description: The following operand can be used with the CALENDAR keyword:

Operand	Description
cal-name	Specifies an eight-character, user-defined record ID that must be unique for each calendar. It can contain letters, numbers, and special characters.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT. MISC8(LISTSDT) authority only gives the administrator the ability to list calendars in the SDT.

Types: The CALENDAR keyword is used with the SDT Record, exclusively.

Examples:

To create a calendar for the present year called CAL1, enter:

```
TSS ADD(SDT) CALENDAR(CAL1)
```

Note: The calendar created by this command selects no days whatever from the current year. To select days to include within the calendar, some combination of DAYS, INCLUDE or EXCLUDE must be used.

For more information concerning the SDT Record, refer to the *User Guide*.

4.4 DAYS

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace the days of the week in a calendar in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the DAYS keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT) CALENDAR(cal-name) DAYS(days,...)
```

Operand Description: The following operand can be used with the DAYS keyword:

Operand	Description
days	Replace with: SUNDAY, MONDAY. TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, WEEKDAYS, WEEKENDS.

Default: None.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The DAYS keyword is used with the SDT Record, exclusively.

Examples:

To create a calendar for the present year with every Monday, Wednesday, Thursday and Friday enabled, enter:

```
TSS ADD(SDT) CALENDAR(CAL1) DAYS(MON,WED,THUR,FRI)
```

This keyword also adds DAYS to an existing CALENDAR.

For more information concerning the SDT Record, refer to the *User Guide*.

4.5 DESCRIPT

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a users-description field in any of the six record types in the SDT Record.

TSS Commands: The following TSS commands can be used with the DESCRIPT keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT) [CALENDAR(cal-name) ] DESCRIPT(descript-name)
             [MAP(map-name)      ]
             [MASK(mask-name)    ]
             [RLP(record-name)   ]
             [SELECT(select-name)]
             [TIMEREC(time-name)]
```

Operand Description: The following operands can be used with the DESCRIPT keyword:

Operand	Description
descript-name	Allows an optional 32-character, user-description field that permits the administrator to apply a logical name to this particular record. If the description field contains blanks, you must enclose it in single quotes.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The DESCRIPT keyword is used with the SDT Record, exclusively.

Examples:

To create a calendar for the present year with a user-description field called PAYROLL CALENDAR, enter:

```
TSS ADD(SDT) CALENDAR(CAL1) DESCRIPT('PAYROLL CALENDAR')
```

This keyword also adds a description to an existing calendar which has a different description.

For more information concerning the SDT Record, refer to the *User Guide*.

4.6 EXCLUDE

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a list of dates that are specifically excluded from the calendar record in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the EXCLUDE keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT) CALENDAR(cal-name) EXCLUDE(mm/dd,...)
```

Operand Description: The following operand can be used with the EXCLUDE keyword:

Operand	Description
mm/dd	Lists specific dates that are excluded in addition to the ones specified with the DAYS keyword.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The EXCLUDE keyword is used with the SDT Record.

Examples:

To create a calendar for the present year with April 16 disabled, enter:

```
TSS ADD(SDT) CALENDAR(CAL1) EXCL(04/16)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.7 INCLUDE

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace the list of dates that are specifically included in the calendar record in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the INCLUDE keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT) CALENDAR(cal-name) INCLUDE(mm/dd,...)
```

Operand Description: The following operand can be used with the INCLUDE keyword:

Operand	Description
mm/dd	Lists specific dates that are included in addition to the ones specified with the DAYS keyword.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function to ADD or REMOVE records or fields in the SDT.

Types: The INCLUDE keyword is used with the SDT Record.

Examples:

To create a calendar for the present year with April 22 and April 29 enabled, enter:

```
TSS ADD(SDT) CALENDAR(CAL1) INCL(04/22,04/29)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.8 MAPDATA

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a MAPDATA field in the MAP record of the Static Data Table (SDT) Record.

MAP records are used to support Screen Level Protection (SLP) records.

TSS Commands: The following TSS commands can be used with the MAPDATA keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT)  MAPREC(map-name)  MAPDATA(mapdata-fld)
```

Operand Description: The following operands can be used with the MAPDATA keyword:

Operand	Description
mapdata-fld	Supports one entry list with five subfields:
	fld-name Specifies an up to 24-character field name unique within this MAP record that can contain letters, numbers, and special characters.
	type Indicates a field type that must be one of the following: CHAR (character), BIN (binary), PACKED, ZONED, or HEX (hexadecimal). A description of each type follows.
	CHAR Specifies any of the EBCDIC characters, left-justified and padded with blanks.
	BIN Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
	PACKED Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
	ZONED Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
	HEX Specifies up to 256 hexadecimal digits (0-F) left-justified and padded with nulls (X"00").

row	Specifies a numeric row of the data field.
column	Specifies a numeric column of the data field.
length	Specifies the length of the data field (optional).

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The MAPDATA keyword is used with the SDT Record.

Examples:

To add a MAPDATA field to the MAP record ENG1 that contains a salary field in character format called PAY which is in in the fifth row and sixth column, and has a length of eight characters, enter:

```
TSS ADD(SDT) MAPREC(ENG1) MAPDATA(PAY,CHAR,5,6,8)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.9 MAPREC

Operating System: VSE, OS/390, and VM

Description: Administrators can provide an up to eight-character name by which CA-Top Secret references a MAP reocrd in the the Static Data Table (SDT) Record.

MAP records are used to support Screen Level Protection (SLP) records for OTRAN and PPT resources. The screen being protected through SLP is a one-for-one relationship to the transaction (OTRAN) or program (PPT). In other words, you are only allowed to protect **one** screen per OTRAN or PPT resource.

TSS Commands: The following TSS commands can be used with the MAPREC keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT)  MAPREC(map-name) MAPDATA(mapdata-fld)
```

Operand Description: The following operand can be used with the MAPREC keyword:

Operand	Description
map-name	Specifies an eight-character, user-defined record ID that must be unique for each MAP record that can contain letters, numbers, and special characters.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The MAPREC keyword is used with the SDT Record.

Examples:

To create a MAP record called ENG1 in the SDT, enter:

```
TSS ADD(SDT) MAPREC(ENG1) MAPDATA(PAY,5,6,8)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.10 MASKDATA

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a MASKDATA field in the MASK record of the Static Data Table (SDT) Record.

Note: If using Record Level Protection (RLP), you must perform the following:

1. You must add the RLP record to the SDT.
2. Give the RECDATA layout and create the necessary SELECT criteria.
3. Add the MASK record and MASKDATA to the SDT.

TSS Commands: The following TSS commands can be used with the MASKDATA keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT)  MASKREC(mask-name) MASKDATA(maskdata-fld)
```

Operand Description: The following operand can be used with the MASKDATA keyword:

Operand	Description
maskdata-fld	Supports one entry list with five subfields:
	fld-name Specifies an up to 24-character field name that must be unique for each MASK record, and can contain letters, numbers, and special characters.
	type Indicates a field type that must be one of the following: CHAR (character), BIN (binary), PACKED, ZONED, or HEX (hexadecimal). A description of each type follows.
	CHAR Specifies any of the EBCDIC characters, left-justified and padded with blanks.
	BIN Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
	PACKED Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
	ZONED Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.

HEX Specifies up to 256 hexadecimal digits (0-F) left-justified and padded with nulls (X"00").

offset Indicates an up to five-digit offset value that must not exceed the record length.

length Indicates a decimal value, ranging from one to 44, for the length of the masked field.

mask Indicates an up to 44-character mask value that can contain letters, numbers, and special characters. However, the mask value must match the field's data type. See the table below for specific rules.

Authority: CA-Top Secret admininstrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The MASKDATA keyword is used with the SDT Record.

The following table illustrates a mask-field type and its respective mask-field literal type:

Field Type	Literal Format	Literal Character-Set	Left Sign
CHAR	"quoted-string"	Alphanumeric	No
BIN	unquoted-string	{0,1}	Yes
HEX	X"quoted-string"	0-F	No
PACKED	unquoted string	0-9	Yes
ZONED	unquoted string	0-9	Yes

Examples:

To add a MASKDATA field to the MASK record CRYPT1 that contains a salary field in character format called ADDR, masked field with an asterisk (*), having an offset value of 50 and a length of 20 characters, enter:

```
TSS ADD(SDT) MASKREC(CRYPT1) MASKDATA(ADDR,CHAR,50,20,********************)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.11 MASKREC

Operating System: VSE, OS/390, and VM

Description: Administrators can provide an up to eight-character name for a MASK record which CA-Top Secret uses in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the MASKREC keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT)  MASKREC(mask-name) MASKDATA(maskdata-fld)
```

Operand Description: The following operand can be used with the MASKREC keyword:

Operand	Description
mask-name	Specifies an eight-character, user-defined record ID that must be unique for each MAP record that can contain letters, numbers, and special characters.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The MASKREC keyword is used with the SDT Record.

Examples:

To create a MASK record called CRYPT1 in the SDT, enter:

```
TSS ADD(SDT) MASKREC(CRYPT1) MASKDATA(ADD,CHAR,50,20,********************)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.12 RANGE

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a RANGE field in the TIME record of the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the RANGE keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT)  TIMEREC(time-name) RANGE(hhmm:hhmm,...)
```

Operand Description: The following operand can be used with the RANGE keyword:

Operand	Description
hhmm:hhmm	Specifies a list of one or more entries in the format hhmm:hhmm for the starting and ending times of a range. You can indicate up to 53 ranges per command. End time must be greater than start time. Each time is denoted in hours (hh) and minutes (mm) based on a 24-hour day. Values for minutes must be 00, 15, 30, or 45, designating 15-minute increments of a range. For example, specifying 00 for minutes includes minutes 00 to 14 in the range. Therefore, RANGE(1200:1300) signifies 12 noon through 1:14 p.m. If you only want noon to 1 p.m., then specify RANGE(1200:1245) to designate those four quarter hours. A single time range in the list can not include midnight. For example, to specify 11 p.m. until 1 a.m., enter: `RANGE(2300:0045,0000:0045) not RANGE(2300:0045)` which would be invalid.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The RANGE keyword is used with the SDT TIMEREC Record.

Examples:

To add a time period from 1 p.m. o 5 p.m. to the RANGE field of the TIME record called TEMP1 in the SDT, enter:

```
TSS ADD(SDT) TIMEREC(TEMP1) RANGE(1300:1645)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.13 RECDATA

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a RECDATA field in the RLP record of the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the RECDATA keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT)  RECORD(rlp-name)
              RECDATA(recdata-fld)
```

Operand Description: The following operands can be used with the RECDATA keyword:

Operand	Description		
recdata-fld	Suppors one entry with four subfields:		
	fld-name	Specifies an up to 24-character field name unique to this RLP record that contains letters, numbers, and special characters.	
	type	Indicates a valid field type: CHAR (character), BIN (binary), PACKED, ZONED or HEX (hexadecimal). A description of each type follows.	
		CHAR	Specifies any of the EBCDIC characters, left-justified and padded with blanks.
		BIN	Specfies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
		PACKED	Specifies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
		ZONED	Specifies up to 16 decimal digits with optional sign. If no sign is specified, a positive value is assumed.
		HEX	Specifies up to 256 hexadecimal digits (0-F) left-justified and padded with nulls (X"00").
	offset	Specifies a five-digit offset of the data field.	

length Specifies an up to 44-character length of the data field (optional).

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The RECDATA keyword is used with the SDT Record.

Examples:

To add a RECDATA field to the RLP record PROLL1 that contains a name field in character format called NAME, having an offset of 20 and a length of 30 characters, enter:

```
TSS ADD(SDT) RECORD(PROLL1) RECDATA(NAME,CHAR,20,30)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.14 RECORD

Operating System: VSE, OS/390, and VM

Description: Administrators can provide an up to eight-character name associated with each RLP Record in the Static Data Table (SDT) Record. RLP records are associated with CICS FCT entries by name.

TSS Commands: The following TSS commands can be used with the RECORD keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT)  RECORD(rlp-name)
              RECDATA(recdata-fld1,...recdata-fld5)
```

Operand Description: The following operand can be used with the RECORD keyword:

Operand	Description
rlp-name	Specifies an eight-character, user-defined record ID that must be unique for each RLP record that can contain letters, numbers, and special characters. The specified rlp-name must match the name of the FCT being protected by the RLP feature.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The RECORD keyword is used with the SDT Record.

Examples:

To create an RLP record called PROLL1, and a RECDATA field that contains salary information in character format with a length of six characters and an offset of 48, enter:

```
TSS ADD(SDT) RECORD(PROLL1) RECDATA(PAY,CHAR,48,6)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.15 SDTFNAME

Operating System: VSE, OS/390, and VM

Description: Administrators can remove a field from a MASK, MAP or RLP record in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the SDTFNAME keyword: **REMOVE only.**

Syntax:

```
TSS REMOVE(SDT)  [MASKREC(mask-name)] SDTFNAME(data-fld1,...data-fld5)
                 [MAPREC(map-name)]
                 [RECORD(rlp-name)]
```

Operand Description: The following operand can be used with the SDTFNAME keyword:

Operand	Description
data-fld	Any data field associated with the MAPDATA, MASKDATA, RECDATA and SELDATA fields.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to REMOVE these fields from the SDT.

Types: The SDTFNAME keyword is used with the SDT Record.

Examples:

To remove a MASKDATA field called MASK1 from the PAYMASK SDT MASK record, enter:

```
TSS REM(SDT) MASKREC(PAYMASK) SDTFNAME(MASK1)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.16 SELDATA

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace a SELDATA field in the SELECT record of the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the SELDATA keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT) SELECT(sel-name) DESCRIPT(desc-name)
 SELDATA('IF [NOT] sel-expression  [AND|OR] sel-expression')
```

Operand Description: The following operands can be used with the SELDATA keyword:

Operand	Description
IF	Signals the beginning of a select expression. You must specify IF, and the entire SELDATA must be enclose in a single quote.
NOT	Specifies a negative relationship for the following sel-expression.
sel-expression	Specifies the logic behind which records the user is restricted to. The sel-expression is coded in a Boolean logic format, which must contain a left-hand side (LHS) field name, a relational operator, and a right-hand side (RHS) comparison data value. A sel-expression consists of Boolean expressions modified by NOT, surrounded by parentheses, and joined by conjunctions, AND and OR. Parentheses are used to destermine the order of evaluation. There is no priority applied to AND, OR, and NOT when parentheses are not supplied.
	Left-hand side Specifies the field name (as defined in the SDT RECORD) that you want CA-Top Secret to compare. If the field name is not defined to CA-Top Secret via the SDT RECORD, access to the requested record will be denied.
	Logical operator Select one of these logical operators: EQ (equal to), NE(not equal to), LT (less than GT (greater than), GE (greater then or equal to) LE (less than or equal to).
	Right-hand side Specifies the value that you want CA-Top Secret to compare against the contents of the record's LHS field.

Depending on the LHS field data-type (CHAR, PACKED, ZONED, BIN, or HEX) determines how to input the RHS data value. Make sure the RHS data-type matches the LHS field's data-type. If not, access to the requested record maybe denied.

For data-type of CHAR, you MUST enclose the data value in double quotes. For example,

```
SELDATA('IF dept EQ "HR1000"')
```

where dept is defined in the SDT RECORD with the data-type of CHAR.

Values 0-9, A-Z, and special characters are accepted. However, CA-Top Secret uses the character of * as a wildcard match, similar to data set masking. For example,

```
SELDATA('IF dept EQ "H**100"')
```

If the LHS field dept contains a value that begins with H, and ends with 100, this would result in a match or a true expression.

For data-types of PACKED, ZONED, or BIN, you MUST enter only decimal digits (0-9) without quotes and a maximum of 16 decimal digits. For example,

```
SELDATA('IF salary LT 50000')
```

where salary is defined in the SDT RECORD with the data-type of PACKED, ZONED, or BIN.

If the decimal value needs to be a negitive number, you **MUST** proceed the digits with a minus sign (-). For example,

```
SELDATA('IF total LE -1000')
```

where total is defined in the SDT RECORD with the data-type of PACKED, ZONED, or BIN. You also want to match on field total a value less then or equal to negitive 1000.

For data-type of HEX, you **MUST** precede the double quotes with an X, followed by the hexadecimal data value. Max is 256. For example,

```
SELDATA('IF table EQ X"FFFFFFFF"')
```

where table is defined in the SDT RECORD with the data-type of HEX.

AND/OR Used to link multiple sel-expressions together. Use AND when **both** sel-expressions are true; use OR when **either** statement is true.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The SELDATA keyword is used with the SDT Record.

Examples:

To add a SELDATA field to the SELECT record called PROBE1 for all the first names of employees that begin with Mike in departments 100 and above, enter:

```
TSS ADD(SDT) SELECT(PROBE1) SELDATA('IF DEPT GE "100" AND "MIKE" ')
```

For more information concerning the SDT Record, refer to the *User Guide*.

Using Parentheses in SELDATA Clauses

Use parentheses in complex expressions to indicate how you want CA-Top Secret to evaluate the clause. Parentheses group the left- and right-hand sides of an expression and they express order, that is, which part of a complex expression is the left-hand side and which side is the right-hand side.

Consider the following:

```
IF CODE = "3A"
```

How can you tell what is the left-hand and what is the right-hand when there are three parts? The following example shows one way to define the tests you want to evaluate using parentheses.

If you want CA-Top Secret to find a true condition when CODE equals 3A, or CODE equals 3B and SALARY is less than $25,000, then you need to use parentheses as shown below:

```
SELDATA=('IF ((CODE = "3A") OR  ((CODE = "3B") AND (SALARY LT 25000)))')
```

The expression above evaluates as true when CODE equals 3A, or CODE equals 3B and SALARY is less than $25,000.

```
SELDATA=('IF (((CODE = "3A") OR  (CODE = "3B") AND (SALARY LT 25000)))')
```

The expression above evaluates as true when CODE equals 3A and SALARY is less than $25,000 or when CODE equals 3B and SALARY is less than $25,000. The parentheses clearly define the left- and right-hand sides.

You must specify parentheses when you use NOT in an expression.

4.17 SELECT

Operating System: VSE, OS/390, and VM

Description: Administrators can provide an up to eight-character name by which CA-Top Secret references a SELECT record in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the SELECT keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT) SELECT(sel-name) DESCRIPT(desc-name)
    SELDATA('IF [NOT] sel-expression  [AND|OR] sel-expression')
```

Operand Description: The following operand can be used with the SELECT keyword:

Operand	Description
sel-name	Specifies an eight-character, user-defined record ID that must be unique for each SELECT record. It can contain letters, numbers, and special characters.
descript-name	Designates an optional 32-character, user-description field that will be used as a logical name for this record. If the description field contains blanks, you must enclose it in single quotes.

Refer to the SELDATA keyword previously discussed for an explanation of all of its operands.

Authority: CA-Top Secret admininstrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The SELECT keyword is used with the SDT Record.

Examples:

To create a SELECT record called PROBE1 in the SDT, selecting departments ranging from 200 through 299, enter:

```
TSS ADD(SDT) SELECT(PROBE1)
             SELDATA('IF DEPT GE "200" AND DEPT LE "299" ')
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.18 TIMEREC

Operating System: VSE, OS/390, and VM

Description: Administrators can provide an up to eight-character name by which CA-Top Secret references a TIMEREC record in the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the TIMEREC keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT) TIMEREC(time-name) DESCRIPT(descript-name)
             RANGE(hhmm:hhmm,...)
```

Operand Description: The following operand is used with the TIMEREC keyword:

Operand	Description
time-name	Specifies an eight-character *time-name* that is user-defined and can contain letters, numbers or special characters.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records in the SDT Record.

Types: The RECORD keyword is used with the SDT Record.

Examples:

To add a TIME record called TEMP1 to the SDT, enter:

```
TSS ADD(SDT) TIMEREC(TEMP1)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.19 YEAR

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, replace or list a year field in the calendar record of the Static Data Table (SDT) Record.

TSS Commands: The following TSS commands can be used with the YEAR keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT) CALENDAR (cal-name) YEAR(yyyy)
```

Operand Description: The following operand can be used with the YEAR keyword:

Operand	Description
yyyy	Specifies a year in which to apply a calendar record. If not specified, the current year is used.

Default: If omitted, the defaults to the current year.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The YEAR keyword is used with the SDT Record.

Examples:

To create a 1996 calendar named FIN96, enter:

```
TSS ADD(SDT) CALENDAR(FIN96) YEAR(1996)
```

For more information concerning the SDT Record, refer to the *User Guide*.

4.20 Applicable Keywords Used With PERMIT

The following keywords, associated with the SDT, are used with TSS PERMIT:

```
CALENDAR
MAPREC
MASKREC
SELECT
TIMEREC
```

Each of the keywords is described in alphabetical order on the following pages.

4.20.1 CALENDAR

Once defined to the SDT, this keyword can be used is association with any resource to PERMIT or REVOKE a CALENDAR to an ACID. The PERMIT syntax is shown below.

Syntax:

```
TSS PER(acid) RESCLASS(resclass- name)  ACCESS(access-level)
              CALENDAR(calendar-name)
```

Capacity of list — One CALENDAR record per TSS command

Authority: The administrator must have MISC3(SDT) authority granted by the TSS ADMIN function, to PERMIT or REVOKE access to a CALENDAR associated with a resource that is owned within their scope.

Access Levels: Available access levels are determined by the RDT resource class being permitted.

If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to CALENDAR records: **Expiration, Facility, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The CALENDAR keyword associated with a resource is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Note: CALENDAR and DAYS are mutually exclusive on a PERMIT.

Examples:

To permit a user to update the inventory master file data set INV.MASTER.FILE with the personnel department's CALENDAR CAL1, the administrator enters:

```
TSS PERMIT(USR01) DSN('INV.MASTER.FILE') ACCESS(UPDATE)
                  CALENDAR(CAL1)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USR01) DSN('INV.MASTER.FILE')
```

4.20.2 MAPREC

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a MAP record associated with an OTRAN or PPT resource. A MAP record is used to support Screen Level Protection (SLP). The PERMIT syntax is shown below.

Syntax:

```
TSS PER(acid) OTRAN(oper)|PPT(oper) MAPREC(map-name)
```

Capacity of list — One MAP record per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE access to MAP records that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels that are associated with OTRANs and PPTs: **ALL, INQUIRE, SET, EXECUTE, ALL, NONE, UPDATE**

The only exception for OTRAN access is UPDATE.

If ACCESS is not specified, CA-Top Secret defaults to EXECUTE access for both OTRAN and PPT.

Access Controls: The administrator can use any of the following methods to control access to MAP records: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The MAPREC keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To permit a user ALL access to a CICS transaction called PAYR with a MAP record ENG1, the administrator enters:

```
TSS PERMIT(USR01) OTRAN(PAYR) ACCESS(ALL) MAPREC(ENG1)
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) OTRAN(PAYR)
```

4.20.3 MASKREC

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a MASK record together with a SELECT statement that is associated with an FCT. The PERMIT syntax is shown below.

Syntax:

```
TSS PER(acid)  FCT (oper) ACCESS(access-level)
               MASKREC(mask-name)  SELECT(selread)
```

mask-name Specifies the SDT MASKREC name applied to the PERMIT.

selread Specifies the SDT SELECT name used as the selection process for all file accesses.

Capacity of list — One MASKREC and SELECT statement per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE access to MASKRECs associated with an FCT that are owned within their scope.

Access Levels: The administrator can specify the same access levels associated with an FCT resource: **SET, INQUIRE, ALL, BROWSE, DELETE, NONE, READ, UPDATE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access : **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The MASKREC keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To permit a user ALL access to the FCT file called PAY with the MASK record CRYPT1 and selecting all departments 100 and above from the input record, and all the employees named Mike from the output record, the administrator enters:

```
TSS ADD(SDT) SELECT(ISDEPT)
             SELDATA('IF DEPT GE "100" AND NAME EQ "MIKE" ')
```

```
TSS PERMIT(USR01) FCT(PAY) ACCESS(ALL) MASKREC(CRYPT1)
                  SELECT(ISDEPT)
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) FCT(PAY)
```

4.20.4 SELECT

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a SELECT record associated with an FCT resource. The PERMIT syntax is shown below.

Syntax:

```
TSS PER(acid) FCT(oper) SELECT(selread,selwrite)
TSS PER(acid) OTRAN(tran)|PPT(program) SELECT(selread)
```

selread Specifies the SDT SELECT record used as the selection process file accesses of READ and BROWSE.

selwrite Specifies the SDT SELECT record used as the selection process for file acesses of UPATE(WRITE, REWRITE, DELETE).

Note: It is not necessary to have both a selread and selwrite record for a SELECT statement. If selwrite is omitted, then the SELECT record specified by the selread is given both READ and UPDATE accesses.

Capacity of list — One SELECT statement per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE SELECT records associated with an FCT that are owned within their scope.

Access Levels: The administrator can specify any or all of the access levels associated with an FCT: **SET, INQUIRE, ALL, BROWSE, DELETE, NONE, READ, UPDATE.:** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls:: The administrator can use any of the following methods to control access to SELECT records: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The SELECT keyword in association with an FCT is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To permit a user to access all data from an FCT called PAY and select all records so that departments 1000 through 1999 are chosen, but limit user only to update DEPT 1500, the administrator enters:

```
TSS ADD(SDT) SELECT(READDEPT)
               SELDATA('IF DEPT GE "1000" AND DEPT LT "2000" ')

TSS ADD(SDT) SELECT(UPDTDEPT)
               SELDATA('IF DEPT EQ "1500" ')
```

```
TSS PERMIT(USR01) FCT(PAY)  ACCESS(ALL)
                    SELECT(READDEPT,UPDTDEPT)
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) FCT(PAY)
```

4.21 TIMEREC

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a TIME record associated with any resource. The PERMIT syntax is shown below.

Syntax:

```
TSS PER(acid) RESCLASS(resclass-name) TIME(time-name)
```

Capacity of list — One TIMEREC per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE access to TIME records associated with a resource owned within their scope.

Access Levels Available access levels are detemined by the RDT resource class being permitted.**:** If ACCESS is not specified, CA-Top Secret defaults to READ access.

If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to TIME records: **Expiration, Facility, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The TIME keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Note: The TIMEREC and TIMES keywords are mutually exclusive on a PERMIT.

Examples:

To permit a user to update a data set with a prefix of SFT and using a department's TIME record named TIME1, the administrator enters:

```
TSS PERMIT(USR01) DSN(SFT.)  ACCESS(ALL) TIMEREC(TIME1)
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) DSN(SFT.)
```

Chapter 5. How to Use ADDTO/REMOVE

This chapter presents the standard formats and rules that govern the ADDTO and REMOVE command functions for attributes and data fields. The resources that are defined and subsequently removed using the ADDTO and REMOVE command functions are defined in Chapter 22, "Summary of Resources".

5.1 Purpose

5.1.1 ADDTO

The ADDTO command function has three main purposes:

- assigns resource ownership or special attributes to a defined ACID
- defines started tasks to CA-Top Secret
- adds to the Audit Record a resource that CA-Top Secret will audit.

In addition, the ADDTO function:

- authorizes an ACID to use specific facilities
- connects profiles to users
- grants access to unownable installation-defined resources
- prohibits an ACID from using a specific set of commands or transactions, or confines an ACID to a specific set of commands or transactions
- adds new resource classes to the Resource Descriptor Table (RDT)
- adds new fields to the Field Descriptor Table (FDT)
- assigns PassTickets and VAX-related UAF, Node, NETUAF and volume records to the Node Descriptor Table (NDT)
- identifies which LUs can participate in APPC conversations by adding them to the APPCLU Record.

5.1.2 REMOVE

The REMOVE function removes ownership of the keyword specified in the ADDTO function. Note that ownership cannot be REMOVEd until PERMITted access is REVOKEd, if applicable. REMOVE is the functional opposite of ADDTO. Rules and examples unique to the REMOVE function are presented with the applicable keyword.

5.2 Assigning Resource Ownership

Resource ownership means that the user, profile, or control ACID has an access level of ALL. Since it may not be desirable to grant unlimited access to individual users or profiles, CA-Top Secret administrators should assign resource ownership to department or division ACIDs using the ADDTO command function. Then, full or restricted resource access may be authorized for other ACIDs (non-owners) via the PERMIT command function. Assigning resource ownership can have either of the following results:

If Resource is:	**ADDTO Function will:**
New (undefined)	Define the resource by assigning ownership to the ACID (preferably a department or division ACID) specified in the command function. For example, `TSS ADD(ACID1) DSN(USER)`

Owned by another ACID	Transfer ownership to the ACID specified in the command function, and automatically PERMIT the old owner to have full access to the resource.
	
	For example, to transfer ownership of data set USER01 from ACID1 to ACID2, the administrator enters:
	
	`TSS ADD(ACID2) DSN(USER) UNDERCUT`
	
	To prevent automatic permission with the NOPERMIT keyword, he would enter:
	
	`TSS ADD(ACID2) DSN(USER) UNDERCUT NOPERMIT`
	
	Refer to the UNDERCUT keyword for details.

5.3 Assigning an Attribute

Adding an attribute to a user or profile ACID assigns special authorities or restrictions to that ACID. A security administrator can, for example, give a user the ability to modify control options by adding the CONSOLE attribute: TSS ADD(USER2) CONSOLE.

5.4 Maintaining the STC, AUDIT, RDT, FDT, NDT, DLF, APPCLU, and ALL Records

The command syntax as shown in the introduction requires a target ACID after the function, as in

```
TSS FUNCTION(acid)
```

with the ACID usually being a user ACID or similar unique ACID name such as those given to departments, profiles, or control ACIDs. ADDing resources or ADMINistering authorities to an ACID of this type is clearly defined by the command functions as they are described in their individual chapters.

However, certain commands use other ACID names as the target of the function:

- STC
- AUDIT
- RDT
- FDT
- NDT
- DLF
- APPCLU
- ALL

The STC, AUDIT, RDT, FDT, NDT, DLF, APPCLU and ALL Records are special ACIDs pre-defined to CA-Top Secret. You use their names as the ACIDs in the commands when you define resources or attributes to these records.

5.4.1 STC Record

The ADDTO function is used to define an OS/390 started task command (STC) to CA-Top Secret. Only two keywords apply to the command using the STC ACID: PROCNAME and STCACT. See those pages in this section for details on how and why to use them.

5.4.2 AUDIT Record

AUDIT allows an administrator to audit the use of a specific resource with the command:

```
TSS ADD(AUDIT) resource class(resource name)
```

which ADDs a resource to the Audit Record. AUDIT can be both a target ACID name and keyword; see the AUDIT page for more details on both.

5.4.3 RDT Record

The RDT (Resource Descriptor Table) Record is a table in the CA-Top Secret Common Storage Area. The RDT stores resources--predefined, such as volumes, data sets, and terminals; and user-defined, which are any resources you add with TSS ADD.

5.4.3.1 RDT Record Functions

The functions used to administer the RDT Record are:

- TSS LIST(RDT) to list the contents of the RDT Record.
- TSS ADD/REMOVE(RDT) to add or remove a resource from the RDT Record.
- TSS REPLACE(RDT) to replace certain access levels and attributes of an existing RDT Record entry.
- TSS ADMIN(acid) MISC1(RDT) to give the user the MISC1 authority needed to administer the RDT.

Refer to “Sample Commands” on page 2-3, for examples of RDT-related commands.

5.4.3.2 RDT Record Keywords

The following keywords are used with the RDT functions. Refer to their respective pages in the appropriate chapters for more information.

ACLST Used with ADDTO/REMOVE or REPLACE, ACLST is optional to add, remove, or change access levels for the RDT resources.

ATTR Used with ADDTO/REMOVE or REPLACE, ATTR is optional to define resources to the RDT Record with various attributes.

DEFACC DEFACC is optional, and allows you to add a default access to a resource. Use with ADDTO/REMOVE and REPLACE.

RESCLASS RESCLASS, along with RESCODE, is a required keyword when defining resources to the RDT Record. It specifies the resource in question. Use it with ADDTO/REMOVE(RDT), LIST(RDT), and REPLACE(RDT). List all the resources defined to the RDT Record with:

```
TSS LIST(RDT) DATA(ALL)
```

RESCODE RESCODE is also a required keyword, used with ADDTO or LIST. RESCODE is a hexadecimal code that indicates the resource type.

5.4.4 FDT Record

The FDT (Field Descriptor Table) Record is a table in the CA-Top Secret Common Storage Area. The FDT stores fields--predefined and user-defined, which are any fields you add with TSS ADD.

5.4.4.1 FDT Record Functions

The functions used to administer the FDT Record are:

- TSS LIST(FDT) to list the contents of the FDT Record.
- TSS ADD/REMOVE(FDT) to add or removes a field from the FDT Record.
- TSS REPLACE(FDT) to replace certain access levels and attributes of an existing FDT Record entry.
- TSS ADMIN(acid) MISC1(RDT) to give the user the MISC1 authority needed to administer the FDT.

5.4.4.2 FDT Record Keywords

The following keywords are used with the FDT functions. Refer to their respective pages in the appropriate chapters for more information.

DISPLAY Used with ADDTO, LIST, or REPLACE, DISPLAY will add, list, or change the field name of the FDT resource.

MAXLEN Used with ADDTO or REPLACE, MAXLEN will define the length of the data that can be added to the user.

SEGMENT SEGMENT allows you to group fields together. Use with ADDTO/REMOVE, LIST, and REPLACE.

FDTNAME FDTNAME, along with FDTCODE, is a required keyword when defining fields to the FDT Record. It specifies the field in question. Use it with ADDTO/REMOVE(FDT), LIST(FDT), and REPLACE(FDT). List all the fields defined to the FDT Record with:

```
TSS LIST(FDT)
```

FDTCODE FDTCODE is also a required keyword, used with ADDTO. FDTCODE is a hexadecimal code that indicates the field type.

5.4.5 NDT Record

The Node Descriptor Table (NDT) contains data for assigning PassTickets and Session Keys to applications. It also contains VAX-related data such as: UAF, Node, NETUAF and Volume records. For example:

```
TSS ADD(NDT) PSTKAPPL(KA180987) SESSKEY(A1B2C3)
```

assigns a Session Key of A1B2C3 to application KA180987 in the Node Descriptor Table.

```
TSS ADD(NDT) VXNODE(USDC01)
```

assigns the VAX node USDC01 to the Node Descriptor Table.

5.4.6 DLF Record

The DLF Record defines those data sets which are eligible for the IBM Data Lookaside Facility. This facility is only available under OS/390/ESA 3.1.3 and above.

```
TSS ADD(DLF) DSN(data set name)
```

5.4.6.1 DLF Record Keywords

The following keywords are used with the DLF functions. Refer to their respective pages in this chapter.

JOBNAME Used with ADDTO/REMOVE, JOBNAME allows a specific data set to be brought into hyperspace if accessed by one of the jobs in the JOBNAME list.

RETAIN Used with ADDTO/REMOVE, RETAIN leaves the data set in hyperspace when the job which brought that data set into hyperspace ends.

5.4.7 APPCLU Record

The APPCLU record identifies which logical units (LUs) can establish a link for the purposes of processing APPC transactions and conversations.

5.4.7.1 APPCLU Record Keywords

The following keywords are used with the APPCLU Record. In addition to their detailed reference pages, you can also refer to the *Implementation: Batch, STC and APPC Guide* for more information on the APPCLU record.

LINKID Identifies the two LUs being targeted by the command. *You must supply a valid LINKID when using any of the following additional keywords to update the APPCLU record.*

CONVSEC Indicates the type of security validation that will occur when an APPC conversation link is established between two LUs.

INTERVAL Indicates how often the SESSKEY for a particular LU-LU link must be changed. **Required when a SESSKEY is specified.**

SESSKEY Identifies a "session key" or password that is verified by VTAM when a conversation is initiated between two LUs.

SESSLOCK Identifies two LUs which *cannot* establish a link for the purposes of a TP-TP conversation.

5.4.8 ALL Record

The ALL Record identifies resources that are globally accessible to all users.

```
TSS PERMIT(ALL) resource(operand) ACCESS(ALL)
```

is an example which uses ALL as both an ACID type and as an access level. Assuming there are no other PERMITs, this command function gives ALL users ALL access to the resource entered.

Note: The ALL Record is not used with the TSS ADDTO/REMOVE command function.

5.5 Entry Methods

CA-Top Secret administrators may enter TSS ADDTO/REMOVE command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

5.5.1 Command Syntax

Figure 3 and Table 3-1 show how command functions are entered freeform at an online terminal.

```
TSS ADD(acid) keyword(operand)
         ↓        ↓        ↓
         1        2        3
```

Figure 3. Command Syntax

Table 3-1. Command Syntax

Field	Description
1	ACID to which resource or attribute is being assigned.
2	TSS keyword that identifies type of resource or attribute being assigned.
3	Specific prefix, name, or value of resource or attribute.

5.6 Authority

CA-Top Secret administrators must have the appropriate RESOURCE(OWN) authority, via the TSS ADMIN command function, to ADD or REMOVE ownership of resources from ACIDs within their scope. Note that RESOURCE(OWN) allows administrators to ADD or REMOVE ownership of **all** resource types from ACIDs within their scope.

Administrators must have MISC1, MISC2 or MISC9 authority to assign many of the security attributes to ACIDs within their scope. ACID authorities determine the levels at which administrators can manage ACIDs within their scope. Authority requirements are specified on the reference page for each attribute.

Note: All resources that are defined to CA-Top Secret are described in detail in the chapter entitled: "Summary of Resources."

5.7 Applicable Keyword List

The following keywords may be used with the TSS ADDTO/REMOVE command functions for CA-Top Secret VSE. The reference pages that follow contain detailed documentation for each keyword.

ACTION	IESFL2	NORESCHK	TIMEREC
AFTER|BEFORE	IESINIT	PASSWORD	TIMES
ASUSPEND	IESSYNM	NOSUBCHK	TRACE
AUDIT	IESTYPE	NOSUSPEND	TRANSACTIONS
CONSOLE	IESVCAT	NOVOLCHK	TZONE
CONVSEC	INSTDATA	OPCLASS	UNDERCUT
DAYS	INTERVAL	OPIDENT	UNTIL
DEFNODES	LANGUAGE	OPPRTY	USER
DFLTGRP	LTIME	PASSWORD	USERNL1
DUFUPD	MASTFAC	PROFILE	USERNL2
DUFXTR	MODE	PSTKAPPL	VSECATBT
EXPIRE	MULTIPW	SCTYKEY	VSEMCON
FACILITY	NOATS	SESSKEY	VSERDD
FIRST	NODES	SESSLOCK	VSESVSAD
FOR	NODSNCHK	SITRAN	XTRANSACTIONS
GAP	NOLCFCHK	SOURCE	
HOME	NOPERMIT	SUSPEND	
IESFL1	NOPWCHG	TARGET	

Note: All resources defined to the RDT can also be used with the ADDTO/REMOVE command function. For an explanation of these keywords, refer to the chapter "Summary of Resources."

The following keywords do not apply to VSE. See the CA-Top Secret OS/390 *Command Functions Guide* for an explanation of these keywords.

COMMAND	MCSSTOR	SMSAPPL	TSOOPT
GID	MCSUD	SMSDATA	TSOSCLASS
GROUP	MRO	SMSMGMT	TSOUDATA
IMSMSC	NOADSP	SMSSTOR	TSOUNIT
JOBNAME	NOVMDCHK	STCACT	UID
LINKID	OIDCARD	TSOCOMMAND	WABLDG
MCSALTG	OMVSPGM	TSODEFPRFG	WAACCNT
MCSAUTH	PCADMIN	TSODEST	WAADDR1
MCSAUTO	PCDSDAYS	TSOHCLASS	WAADDR2
MCSCMDS	PCIDLE	TSOJCLASS	WAADDR3
MCSDOM	PCLGTYPE	TSOLACCT	WAADDR4
MCSKEY	PCMINPWD	TSOLPROC	WADEPT
MCSLEVL	PCOPTS	TSOLSIZE	WAIT
MCSLOC	PHYSKEY	TSOMCLASS	WANAME
MCSMFRM	PROCNAME	TSOMPW	WAROOM
MCSMGID	RESOWNER	TSOMSIZE	XCOMMAND
MCSMON	RETAIN		
MCSROUT	ROSRES		

5.8 ACTION

Operating System: VSE, OS/390, and VM

Description: To assign action(s) to an ACID which CA-Top Secret will take when access to a FACILITY is attempted.

TSS Commands: The following TSS command can be used with the ACTION keyword: **ADDTO.**

Syntax:

```
TSS ADDTO(acid) FAC(facility)
    ACTION(AUDIT,NOTIFY,DENY)
```

Authority: The CA-Top Secret administrator must be authorized to administer a specific facility, via the ADMIN function, before he can authorize access to ACIDs within his scope.

Types: The ACTION keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Operands: The following operands can be used with the ACTION keyword:

Action	Description
AUDIT	CA-Top Secret will audit the ACID when logged on to the facility. For example, to audit an ACID accessing CICSTEST, the administrator enters: `TSS ADD(USER01) FAC(CICSTEST) ACTION(AUDIT)`
NOTIFY	CA-Top Secret will notify the security console that the ACID is signing onto the facility.
DENY	CA-Top Secret will deny access to a facility even though it was specified in the ACID's PROFILE. For example, if a user attempts to logon to a facility and the administrator wishes to deny access to that facility. the administrator enters: `TSS ADD(USER01) FAC(CICSPROD) ACTION(DENY)`

Examples:

To indicate that the user is allowed to sign on to CICS and everything the ACID does is audited:

```
TSS ADD(acid) FAC(CICS) ACTION(AUDIT)
```

5.9 AFTER|BEFORE

Operating System: VSE, OS/390, and VM

Description: To add a profile to a specific location in the order of profiles.

TSS Commands: The following TSS command can be used with the AFTER|BEFORE keyword: **ADDTO.**

Syntax:

```
TSS ADD(acid) PROFILE(new profile)
    AFTER|BEFORE(existing profile)
```

ACID length — 1-8 characters

Capacity of list — 1 existing profile.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to connect profiles to ACIDs within their scope.

Types: The AFTER or BEFORE keyword can be used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

Assume profiles PROF01 through PROF04 already exist for ACID USER01, and PROF05 is to be added between PROF02 and PROF03. You would enter:

```
TSS ADD(USER01) PROF(PROF05) AFTER(PROF02)

                or

TSS ADD(USER01) PROF(PROF05) BEFORE(PROF03)
```

in either case, the order of profiles for ACID USER01 will be: PROF01, PROF02, PROF05, PROF03, PROF04.

5.10 ASUSPEND

Operating System: VSE, OS/390, and VM

Description: To remove the suspension of an ACID that was suspended for administrative reasons.

TSS Commands: The following TSS command can be used with the ASUSPEND keyword: **REMOVE.**

Syntax:

```
TSS REM(acid) ASUSpend
```

Authority: Administrators must have MISC8(REMASUSP) authority, via the ADMIN function, to REMOVE the ASUSPEND attribute from ACIDs within their scope.

Types: The ASUSPEND keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Limiting Suspensions: Administrators may add the FOR or UNTIL keywords onto an ASUSPEND entry to remove a suspension that was added with the FOR or UNTIL keywords. This entry will unsuspend USER01 if it was suspended with FOR(5).

```
TSS REM(USER01) ASUS FOR(5)
```

This entry will unsuspend USER01 if it was suspended with UNTIL(12/17/94).

```
TSS REM(USER01) ASUS UNTIL(12/17/94)
```

Examples:

To remove the ASUSPEND attribute from an ACID, the administrator enters:

```
TSS REMOVE(ACARP) ASUS
```

To remove a temporary suspend, ASUS UNTIL(date), the administrator enters:

```
TSS REMOVE(ACARP) ASUS UNTIL(date)
```

5.11 AUDIT

Operating System: VSE, OS/390, and VM

Description: To allow an audit of ACID activity.

Note: AUDIT is a reserved ACID name.

```
TSS ADD(AUDIT) resource class(resource name)
```

ADDs a specific resource(s) to the Audit Record for auditing purposes.

TSS Commands: The following TSS command can be used with the AUDIT keyword: **CREATE ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) AUDIT
```

Capacity of list — 1-5 resource names per TSS command.

Authority: The administrators must have ACID(AUDIT) authority to ADD or REMOVE the AUDIT attribute from ACIDs within their scope. When using AUDIT as a reserved ACID name, administrators must have RESOURCE-AUDIT authority.

Types: The AUDIT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

To audit USER01's activities, the administrator adds the AUDIT attribute by entering:

```
TSS ADD(USER01) AUDIT
```

To remove the AUDIT attribute from USER01, the administrator enters:

```
TSS REMOVE(USER01) AUDIT
```

5.12 CALENDAR

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, replace, or list an existing calendar in the SDT (Static Data Table) Record.

TSS Commands: The following TSS commands can be used with the CALENDAR keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT) CALENDAR(cal-name)
```

Operand Description: The following operand can be used with the CALENDAR keyword:

Operand	Description
cal-name	Specifies an eight-character, user-defined record ID that must be unique for each calendar. It can contain letters, numbers, and special characters.

Authority: CA-Top Secret admininstrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT. MISC8(LISTSDT) authority only gives the administrator the ability to list calendars in the SDT.

Types: The CALENDAR keyword is used with the SDT Record, exclusively.

Examples:

To create a calendar for the present year called CAL1, enter:

```
TSS ADD(SDT) CALENDAR(CAL1)
```

For more information concerning the SDT Record, refer to the *User Guide*.

5.13 CONSOLE

Operating System: VSE, OS/390, and VM

Description: To grant or remove an ACID's ability to modify control options. For VM, options are modified via the TSS MODIFY command only. With VSE and OS/390, options are modified at the O/S console or via the TSS MODIFY command function.

TSS Commands: The following TSS command can be used with the CONSOLE keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) CONSOLE
```

Authority: CA-Top Secret administrators must have MISC9(CONSOLE) authority, via the TSS ADMIN function, to ADD or REMOVE the CONSOLE attribute.

Types: The CONSOLE keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To give user GABVCA the ability to enter protected control options at the console, or through the TSS MODIFY command, the administrator enters:

```
TSS ADD(GABVCA) CONSOLE
```

To remove the CONSOLE attribute:

```
TSS REMOVE(GABVCA) CONSOLE
```

5.14 DAYS

Operating System: VSE, OS/390, and VM

Description: To restrict access to a specific day(s) of the week.

TSS Commands: The following TSS commands can be used with the DAYS keyword: **ADDTO, PERMIT, REPLACE.**

Syntax:

```
TSS ADD(acid) resource(prefix) FAC(facility name)
    DAYS(day-list)
```

"day-list" is composed of one or more of the following entries for the days of the week:

Entry	Description
MON	Monday
TUE	Tuesday
WED	Wednesday
THU	Thursday
FRI	Friday
SAT	Saturday
SUN	Sunday
WEEKDAYS	Includes Monday, Tuesday, Wednesday, Thursday, and Friday.
WEEKENDS	Includes Saturday and Sunday only.

Default: If the DAYS keyword is omitted, CA-Top Secret allows access on every day of the week.

Authority: Administrators must have MISC9(DAYS) authority, via the TSS ADMIN function, to ADD or REPLACE the DAYS attribute.

Types: The DAYS keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL Record.**

Examples:

To give user MICHVCA the ability to access the CICSPROD facility on Monday and Tuesday, the administrator enters:

```
TSS ADD(MICHVCA) FAC(CICSPROD) DAYS(MON,TUE)
```

To change the DAYS attribute on MICHVCA's access to the CICSPROD facilty from Monday and Tuesday to Wednesday and Thursday, the administrator enters:

```
TSS REPLACE(MICHVCA) FAC(CICSPROD) DAYS(WED,THU)
```

To remove all access to the CICSPROD facility from MICHVCA, the administrator enters:

```
TSS REMOVE(MICHVCA) FAC(CICSPROD)
```

Note: You cannot remove the DAYS keyword from a facility, you must remove the facilty from the ACID.

5.15 DAYS (For Calendars)

Operating System: VSE, OS/390, and VM

Description: Administrators can add, remove, or replace the days of the week in a calendar in the SDT (Static Data Table) Record.

TSS Commands: The following TSS commands can be used with the DAYS keyword: **ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(SDT) CALENDAR(cal-name) DAYS(days,...)
```

Operand Description: The following operand can be used with the DAYS keyword:

Operand	Description
days	Replace with: SUNDAY, MONDAY. TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, WEEKDAYS, WEEKENDS.

Authority: CA-Top Secret admininstrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records or fields in the SDT.

Types: The DAYS keyword is used with the SDT Record, exclusively.

Examples:

To create a calendar for the present year with every Monday, Wednesday, Thursday and Friday enabled, enter:

```
TSS ADD(SDT) CALENDAR(CAL1) DAYS(MON,WED,THUR,FRI)
```

For more information concerning the SDT Record, refer to the *User Guide*.

5.16 DEFNODES

Operating System: VSE, OS/390, and VM

Description: To assign default remote node IDs for an ACID. An ACID's DEFNODES list will *only* be searched *if* the CPFTARGET control option is set to AUTO *and* no TARGET has been specified on the command.

TSS Commands: The following TSS command can be used with the DEFNODES keyword: **ADDTO, CREATE, REMOVE, LIST, REPLACE.**

Syntax:

```
TSS ADD(acid) DEFNODES(oper,oper,...)
```

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to replace the default CPF node list for ACIDs within their scope.

Types: The DEFNODES keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To define the default CPF nodes used in the TARGET keyword when administering ACID USER01, the administrator enters:

```
TSS ADD(USER01) DEFNODES(NYC,CHI,DET)
```

To remove the CHI nodes from USER01's DEFNODES list, the administrator enters:

```
TSS REMOVE(USER01) DEFNODES(CHI)
```

Both the NYC and DET nodes will remain in USER01's DEFNODES list. To issue a completely new set of DEFNODES, you would use the TSS REPLACE command. TSS REPLACE deletes the existing DEFNODES list in its entirety and substitutes a new list.

5.17 DUFUPD

Operating System: VSE, OS/390, and VM

Description: To add or remove the DUFUPD attribute to an ACID. DUFUPD enables an ACID to use the CA-Top Secret Application Interface to update the installation data (INSTDATA) or field data from a Security Record. DUFUPD is a component of the CA-Top Secret Dynamic Update Facility (DUF).

TSS Commands: The following TSS command can be used with the DUFUPD keyword: **CREATE ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) DUFUpd
```

The DUFUPD keyword is only applicable when installation or field data used for customization is entered into the Security File.

Authority: Administrators must have MISC1(INSTDATA) authority, via the TSS ADMIN function, to ADD and REMOVE the DUFUPD attribute from ACIDs within their scope.

Use With DUFXTR: DUFXTR and DUFUPD may be entered together to provide full use of the Dynamic Update Facility:

```
TSS ADD(ACID) DUFXTR DUFU
```

Types: The DUFUPD keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To give user PRS001 the ability to update installation data, the administrator enters:

```
TSS ADD(PRS001) DUFU
```

To remove the DUFUPD attribute, the administrator enters:

```
TSS REMOVE(PRS001) DUFU
```

5.18 DUFXTR

Operating System: VSE, OS/390, and VM

Description: To add or remove the DUFXTR attribute to an ACID. DUFXTR enables an ACID to use a RACROUTE REQUEST=AUTH (RACHECK) macro or the CA-Top Secret Application Interface to extract installation data (INSTDATA) or field data from a Security Record. DUFXTR is a component of the CA-Top Secret Dynamic Update Facility (DUF).

INSTDATA and the Dynamic Update Facility are described in the *User Guide*.

TSS Commands: The following TSS command can be used with the DUFXTR keyword: **CREATE ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) DUFXtr
```

The DUFXTR keyword is only applicable when installation or field data used for customization is entered into the Security File.

Authority: Administrators must have MISC1(INSTDATA) authority, via the TSS ADMIN function to ADD and REMOVE the DUFXTR attribute from ACIDs within their scope.

Use With DUFUPD: DUFXTR and DUFUPD can be entered together to provide full use of the Dynamic Update Facility.

```
TSS ADD(ACID) DUFX DUFU
```

Types: The DUFXTR keyword can be used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To give user PRS001 the ability to extract installation data, the administrator enters:

```
TSS ADD(PRS001) DUFX
```

To remove the DUFXTR attribute, the administrator enters:

```
TSS REMOVE(PRS001) DUFX
```

5.19 EXPIRE

Operating System: VSE, OS/390, and VM

Description: Used with the REMOVE command function to remove an expiration that had been set using the FOR or UNTIL parameters.

TSS Commands: The following TSS command can be used with the EXPIRE keyword: **REMOVE**

Syntax:

```
TSS REM(acid) EXPIRE
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function to un-EXPIRE ACIDs within their scope.

Types: The EXPIRE keyword can be used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

The CA-Top Secret administrator created a temporary AUDIT01 ACID that was set to expire on 4/5/94 via the UNTIL parameter. On 4/6/94, the user still needs access to that ACID. The administrator enters the following command:

```
TSS REM(AUDIT01) EXPIRE
```

5.20 FACILITY

Operating System: VSE, OS/390, and VM

Description: To specify which facility or facilities an ACID may or may not access.

TSS Commands: The following TSS commands can be used with the FACILITY keyword: **CREATE, PERMIT, ADMIN, DEADMIN, ADDTO, REMOVE, REPLACE, WHOHAS.**

Syntax:

```
TSS ADD(acid|ALL) FACility(fac,fac,.... | ALL)
```

Facilities listed as operands must reside in the site's Facilities Matrix Table. This is done by specifying the ACTIVE suboption of the FACILITY control option for that facility. For more information, refer to the *Control Options Guide*.

Authority: The CA-Top Secret administrator must be authorized to administer a specific facility or facilities, via the ADMIN command function, before he can authorize access to ACIDs within his scope.

Controls: These controls are similar to access controls used with a TSS PERMIT command. The controls that can be used with FACILITY are:

Control	Keyword
Expiration	FOR or UNTIL
Time/Day	TIME and/or DAY; TIMEREC and/or CALENDAR
Actions	FAIL, NOTIFY, AUDIT, DENY

For more details on these controls, refer to the respective keyword in this chapter.

Types: The FACILITY keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL Record.**

Note: You can also control mode by facility for an individual user by using the FACILITY keyword on a TSS PERMIT command. For example:

```
TSS PERMIT(USER01) MODE(WARN) FAC(BATCH,CICSPROD)
```

Examples:

To authorize user NJ014 to access both VM and CICSPROD, the administrator enters:

```
TSS ADD(NJ014) FAC(VM,CICSPROD)
```

To authorize USER05 to sign on to CICS on Monday, Wednesday, and Friday from the hours of 9 A.M. to 5 P.M. for the next 10 days and to audit the ACID's activity, the administrator enters:

```
TSS ADD(USER05) FAC(CICS) DAYS(MON,WED,FRI)
    TIMES(9,17) FOR(10) ACTION(AUDIT)
```

To authorize a user or users to access all facilities currently active in the installation:

```
TSS ADD(acid) FAC(ALL)
```

Note: This authorization also gives the user access to all subsequently added facilities.

To remove access to a facility:

```
TSS REMOVE(NJ014) FAC(CICSPROD)
```

Note: If NJ014 had been authorized to access all facilities via TSS ADD(acid) FAC(ALL), this command would not remove access to the CICSPROD facility. Instead, you would need to use ACTION(DENY).

To authorize a user to access all facilities except CICSPROD:

```
TSS ADD(acid) FAC(ALL)
TSS ADD(acid) FAC(CICSPROD) ACTION(DENY)
```

To PERMIT all users to access the CICSPROD facility between the hours of 9 a.m. and 5 p.m., the following command must be issued:

```
TSS ADD(ALL) FAC(CICSPROD) TIME (09,17)
```

5.21 FIRST

Operating System: VSE, OS/390, and VM

Description: To add a profile as the first in the order of profiles.

TSS Commands: The following TSS command can be used with the FIRST keyword: **ADDTO.**

Syntax:

```
TSS ADD(acid) PROFILE(existing-profile) FIRST
```

Prefix length — 1 to 8 characters

Capacity of list — 1 existing profile.

Authority Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to connect profiles to ACIDs within their scope**.:**

Types The FIRST keyword can be used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

Assume the profile called PROF05 is to be added to USER01 as the first in the search order. You would enter:

```
TSS ADD(USER23) PROF(PROF05) FIRST
```

5.22 FOR

Operating System: VSE, OS/390, and VM

Description: To set the number of days that the associated ACID (Accessor ID) may be used before it expires. FOR may also be used with SUSPEND to specify a period of time during which an ACID will be suspended.

TSS Commands: The following TSS commands can be used with the FOR keyword: **CREATE, PERMIT, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) FOR(day-count)
```

"day-count" may equal 0 to 255 days (where 0 = no expiration).

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign the FOR keyword to ACIDs within their scope.

Note: When used with SUSPEND, administrators must also have MISC1(SUSPEND) authority.

Related Keywords:

- The UNTIL keyword is used to set a specific date that an ACID will expire. FOR and UNTIL are mutually exclusive; CA-Top Secret will not accept UNTIL and FOR within the same TSS command.
- The SUSPEND keyword may be used with FOR to specify a time period during which an ACID will be suspended.
- If you wish to REMOVE the expiration interval and are unsure of whether you specified FOR or UNTIL on the TSS ADD, you can use the following syntax:

  ```
  TSS REMOVE(acid) EXPIRE
  ```

- You cannot REMOVE the FOR attribute from a facility, you must remove the facility from the ACID:

  ```
  TSS REMOVE(acid) FAC(facility)
  ```

Types: The FOR keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To force an ACID to expire after 5 days, the administrator enters:

```
TSS ADD(USER23) FOR(5)
```

After an ACID expires, it cannot be used until the time limit is removed. The following entry will totally remove the expiration limit from USER23 and thus reactivate the ACID:

```
TSS REM(USER23) FOR(5)
```

The following entry will also remove the expiration:

```
TSS ADD(USER23) FOR(0)
```

If the FOR keyword is ADDed to an ACID in combination with the SUSPEND keyword, the ACID is temporarily suspended for the specified number of days and can then be used again. In the following example, USER23 is suspended for 14 days:

```
TSS ADD(USER23) SUSPEND FOR(14)
```

The FOR keyword may also be used when adding PROFILE ACIDs and FACILITY(s) to a user.

```
TSS ADD(USER23) FAC(TSO) FOR(5)
 -or-
TSS ADD(USER23) PROFILE(PROF23) FOR(5)
```

Note:

- When used with a PROFILE or FACILITY, the use of that profile or facility expires, not the ACID itself.
- For examples of the use of FOR with SUSPEND, see the SUSPEND keyword.

5.23 GAP

Operating System: VSE, OS/390, and VM

Description: To specify that a profile will become, or will cease to be, globally administrable.

TSS Commands: The following TSS command can be used with the GAP keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(profile acid) GAP
```

Authority: Only an administrator with the same scope of authority as the administrator who CREATED the profile can assign the GAP attribute to that profile.

Types: The GAP keyword is used with the following ACID types: **Profile.**

Examples:

An SCA created profile ADMACT as shown below:

```
TSS CRE(ADMACT) TYPE(PROFILE) NAME('ACTPROJECT') DEPT(ACCTD)

TSS PER(ADMACT) DSN(*.ACCTS) ACCESS(READ)
```

Since many users in several departments required access to profile ADMACT, the SCA decided to ADD the GAP attribute to the profile, thus allowing CA-Top Secret administrators in all departments to administer the profile:

```
TSS ADD(ADMACT) GAP
```

Global Administration is removed from a profile when no longer required by entering:

```
TSS REMOVE(ADMACT) GAP
```

5.24 IESFL1

Operating System: VSE

Description: Used to assign attributes to an Interactive Interface user. These attributes include: submit to batch authority, PRIMARY sublibrary assignment, POWER and ICCF delete confirmation, and alter/allocate VSAM resource authorization. These attributes correspond to user profile data stored in the VSE Control File.

TSS Commands: The following TSS commands can be used with the IESFL1 keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) IESFL1(BAT,PSL,COD,VSAM)
```

Operand	Description
BAT	Authorizes the II user to submit jobs to the VSE batch environment.
PSL	Assigns the II user a primary sublibrary named PRIMARY.acid.
COD	Requires the II user to give confirmation when deleting POWER jobs or ICCF members.
VSAM	Authorizes the II user to: define files, libraries, and alternate indexes; process catalogs; define/delete VSAM space.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign IESFL1 values to ACIDs within their scope.

Types: The IESFL1 keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To give the II user authority to submit jobs to VSE batch, and to require delete confirmation for POWER jobs and ICCF members, the administrator enters:

```
TSS ADD(SYSA) IESFL1(BAT,COD)
```

To remove the above attributes, the administrator enters:

```
TSS REMOVE(SYSA) IESFL1(BAT,COD)
```

5.25 IESFL2

Operating System: VSE

Description: Used to assign attributes to an Interactive Interface user. These attributes include: the authority to manage all POWER jobs, allow escape to a native CICS session, display all messages on the console, master console and command authorization, allow delete of OLPD incident records, and maintain profile authorization. These attributes correspond to user profile data stored in the VSE Control File.

TSS Commands: The following TSS commands can be used with the IESFL2 keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) IESFL2(BQA,ESC,COU,CMD,OLPD,XRM)
```

Operand	Description
BQA	Authorizes the II user to manage all VSE/POWER jobs.
ESC	Permits the II user to escape to a native CICS session.
COU	Displays all messages on the console for the II user. Without this attribute, shows only messages related to this user.
CMD	Authorizes the II user to get a master console and enter all commands.
OLPD	Authorizes the II user to delete OLPD incident records.
XRM	Authorizes the II user to maintain resource profiles within the Interactive Interface. These resource profiles include the user, application, and selection profiles.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign IESFL2 values to ACIDs within their scope.

Types: The IESFL2 keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To give the II user authority to maintain Interactive Interface profiles and to permit escape to a native CICS session, the administrator enters:

```
TSS ADD(SYSA) IESFL2(ESC,XRM)
```

To remove the above attributes, the administrator enters:

```
TSS REMOVE(SYSA) IESFL2(ESC,XRM)
```

5.26 IESINIT

Operating System: VSE

Description: Used to assign an eight-character selection or application profile name that should be initiated when the Interactive Interface user signs on. This attribute corresponds to user profile data stored in the VSE Control File.

TSS Commands: The following TSS commands can be used with the IESINIT keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) IESINIT(profname)
```

Operand	Description
profname	A profile name that is one to eight characters in length. It should match an existing profile name defined to the Interactive Interface.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign IESINIT values to ACIDs within their scope.

Types: The IESINIT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign a profile name of IESEADM to be initiated when the II user signs on, the administrator enters:

```
TSS ADD(SYSA) IESINIT(IESEADM)
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) IESINIT
```

5.27 IESSYNM

Operating System: VSE

Description: Used to assign an Interactive Interface user ID to be used as a model for synonyms. This attribute corresponds to user profile data stored in the VSE Control File.

TSS Commands: The following TSS commands can be used with the IESSYNM keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) IESSYNM(userid)
```

Operand	Description
userid	A user ID that is four to eight characters in length. It should match an existing user ID defined to the Interactive Interface.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign IESSYNM values to ACIDs within their scope.

Types: The IESSYNM keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign a user ID of OPER to be used as a model for synonyms, the administrator enters:

```
TSS ADD(SYSA) IESSYNM(OPER)
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) IESSYNM
```

5.28 IESTYPE

Operating System: VSE

Description: Used to assign a user type to an Interactive Interface user. Also used to assign attributes for new item display and the initial action profile type. These attributes correspond to the user profile data stored in the VSE Control File.

TSS Commands: The following TSS commands can be used with the IESTYPE keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) IESTYPE(USERTYPEx,NEW,SELECT)
```

Operand	Description
USERTYPEx	Defines the overall user characteristics. Replace *x* with one of the following values: **1** VSE system administrator (includes access to ICCF) **2** Programmer/Operator (includes access to ICCF) **3** General application user
NEW	System displays news items to the II user.
SELECT	Interprets initial action name as a selection profile. If not specified, interprets the action as an application profile.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign IESTYPE values to ACIDs within their scope.

Types: The IESTYPE keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To make the II user a system administrator, have news items displayed, and the initial action a selection profile, the administrator enters:

```
TSS ADD(SYSA) IESTYPE(USERTYPE1,NEW,SELECT)
```

To remove the above attributes, the administrator enters:

```
TSS REMOVE(SYSA) IESTYPE(USERTYPE1,NEW,SELECT)
```

5.29 IESVCAT

Operating System: VSE

Description: Used to assign a default VSAM user catalog for an Interactive Interface user. This attribute corresponds to user profile data stored in the VSE Control File.

TSS Commands: The following TSS commands can be used with the IESVCAT keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) IESVCAT(usercat)
```

Operand	Description
usercat	A VSAM user catalog name that is one to eight characters in length. It should match an existing VSAM user catalog definition.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign IESVCAT values to ACIDs within their scope.

Types: The IESVCAT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign VSESPUC as the default VSAM catalog for the current II dialogs, the administrator enters:

```
TSS ADD(SYSA) IESVCAT(VSESPUC)
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) IESVCAT
```

5.30 INSTDATA

Operating System: OS/390, VM and VSE

Description: To record or remove information about an ACID. Up to 255 characters of information about an associated ACID may be used for convenient record keeping, or for interrogation by a user-written Installation Exit.

TSS Commands: The following TSS commands can be used with the INSTDATA keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) INSTdata('installation data')
```

CA-Top Secret adds additional installation data to the end of any existing data. The new data will be concatenated, but cannot extend beyond 255 characters.

When INSTDATA is added to an ACID which previously contained no data, the full 255 character space is available.

Authority: CA-Top Secret administrators must have MISC1(INSTDATA) authority, via the ADMIN function, to use the INSTDATA keyword for ACIDs within their scope.

Types: The INSTDATA keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA, DEPARTMENT, DIVISION, ZONE**

Examples:

To add INSTDATA to ACID QO66, enter:

```
TSS ADD(QO66) INST('JUNE 90')
```

The data, 'JUNE 90', will be added to the end of the INSTDATA which exists for QO66.

CA-Top Secret administrators may remove the entire INSTDATA field for an ACID, but cannot remove specific portions.

```
TSS REMOVE(QO66) INST
```

removes ALL INSTDATA for QO66.

Note: Use TSS REPLACE (INSTDATA) to totally replace old data with new data.

5.31 LANGUAGE

Operating System: VSE, OS/390, and VM

Description: To assign or remove a language preference code which will be passed to the message processing Installation Exit. Refer to the *Customization Guide* for VM and the *Auditor's Guide* for VSE and OS/390 regarding detailed information on the Installation Exit.

TSS Commands: The following TSS commands can be used with the LANGUAGE keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) LANGuage(c)
```

Prefix length — (c) must equal a user-defined, one-character language preference code.

Capacity of list — 1 LANGUAGE code per TSS command.

Customization: The site must write an Installation Exit for message translation to allow association of the language preference code with the language of preference. CA-Top Secret passes this code to the Installation Exit for message translation.

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, via the ADMIN function, to assign a LANGUAGE preference to ACIDs within their scope.

Types: The LANGUAGE keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA**

Examples:

To indicate that a user in Quebec requires error messages in French (and the administrator has defined F as the code for French), the administrator enters:

```
TSS ADD(userque) LANG(F)
```

To remove a language preference, the administrator enters:

```
TSS REMOVE(userque) LANG(F)
```

5.32 LTIME

Operating System: VSE, OS/390, and VM

Description: To specify how long (in minutes) until a user's terminal will lock if CA-Top Secret does not detect activity at that user's terminal.

TSS Commands: The following TSS commands can be used with the LTIME keyword: **CREATE, REPLACE**

Syntax:

```
TSS ADD(acid) LTIme(0...120  [,facility])
```

Value: LTIME may equal 0 to 120 minutes (where 0 = do not lock).

Authority: CA-Top Secret administrators must have MISC1(LTIME) authority, via the ADMIN function, to assign the LTIME keyword to ACIDs within their scope.

Override Control Option: A user's LTIME will override the facility LOCKTIME that may be set as a suboption of the FACILITY control option.

Facility Differences: There are differences in how CA-Top Secret detects the inactivity of terminals connected to various facilities. Refer to the appropriate facility implementation guide for details.

Types: The LTIME keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To cause a signed-on user's terminal to lock if unused after 15 minutes, the administrator enters:

```
TSS ADD(QQ35R10) LTI(15)
```

While issuing:

```
TSS ADD(QQ35R10) LTI(15,CICS)
```

will cause the signed on user's terminal to lock if unused after 15 minutes on CICS only.

To remove the LTIME value from an ACID:

```
TSS REMOVE(QQ35R10) LTI(15)
```

To deactivate automatic terminal locking for an ACID, the administrator enters:

```
TSS REMOVE(QQ35R10) LTI(0)
```

5.33 MASTFAC

Operating System: VSE and OS/390 (VM description is in the OS/390 *Command Functions Guide*)

Description: To override the default facility, controlled by a batch or started task ACID, that is associated with a multi-user facility such as CICS. (By default, CICS uses the CICSPROD facility. MASTFAC allows use of other defined facilities such as CICSTEST.)

TSS Commands: The following TSS commands can be used with the MASTFAC keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(region ACID) MAStfac(facility)
```

Authority: CA-Top Secret administrators must have MISC9(MASTFAC) authority, via the ADMIN function, to assign the MASTFAC attribute to ACIDs within their scope.

Application: The following describes when the MASTFAC attribute is valid.

1. MASTFAC is only of value to the BATCH or STC ACID that controls the region, not to the ACIDs that will sign on.
2. MASTFAC is valid only for online multi-user regions such as CICS and CA-IDMS.

Facility Matrix: The facility name used as an operand for MASTFAC must be defined to CA-Top Secret in the systems Facilities Matrix.

Additional facilities can be defined via the NAME suboption of the FACILITY control option. Refer to one of the following guides for details on how to associate facilities with region control ACIDs:

Implementation: CICS Guide
Implementation: Other Interfaces Guide

Types: The MASTFAC keyword is used with the **User** ACID type.

Examples:

To indicate that facility CICSTEST is controlled by ACID CICST1 the administrator enters:

```
TSS ADD(CICST1) MAS(CICSTEST)
```

This example assumes that the administrator had already CREATED the batch or started task ACID (CICST1).

To remove the relationship between a region and a facility, the administrator enters:

```
TSS REM(CICST1) MAS(CICSTEST)
```

5.34 MODE

Operating System: VSE, OS/390, and VM

Description: To assign ownership of CA-Top Secret operating modes to the master SCA (MSCA).

TSS Commands: The following TSS commands can be used with the MODE keyword: **CREATE, PERMIT, REVOKE, WHOOWNS, WHOHAS, ADDTO, REMOVE**

Syntax:

```
TSS ADD(sca acid) MODE(DORM,WARN,IMPL,FAIL)
```

Authority: The MSCA must own all modes before they can be specified, via the PERMIT function, for an ACID. Assigning MODE ownership to the MSCA is usually done just once at the time of installation.

Types: The MODE keyword can be used with the following ACID types: **SCA.**

Note: You can also control mode by facility for an individual user by using the FAC keyword in a TSS PERMIT. For example:

```
TSS PER(USER01) MODE(WARN) FAC(BATCH,CICSPROD)
```

5.35 MULTIPW

Operating System: VSE, OS/390, and VM

Description: To assign or remove multiple password attributes, which means ACIDs need a different password to access each facility.

TSS Commands: The following TSS command can be used with the MULTIPW keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) MULTIPW
```

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, via the ADMIN function, to administer the MULTIPW attribute to ACIDs within their scope.

Types: The MULTIPW keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA.**

Examples:

To indicate that USER99 may have a different password to access each facility, the administrator enters:

```
TSS ADD(USER99) PASSWORD(TAQRAC)
        FAC(CICS) MULTIPW
```

This allows the following entries for USER99:

```
TSS ADD(USER99) PASSWORD(BUZWRD) FAC(CICS)

TSS ADD(USER99) PASSWORD(SUPAV1) FAC(CICS)
```

To remove the MULTIPW attribute:

```
TSS REMOVE(USER99) MULTIPW
```

5.36 NOATS

Operating System: OS/390 and VSE

Description: To prevent an ACID in CICS and CA-IDMS from signing on via ATS (Automatic Terminal Signon).

TSS Commands: The following TSS command can be used with the NOATS keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOATS
```

Intended Use: There is a security concern in environments where ATS is allowed (CICS and CA-IDMS). When a terminal ID is identical to a CA-Top Secret administrator's ID, and ATS is used, then the person signing on automatically becomes an administrator without supplying any form of identification. The NOATS attribute will deter this type of security exposure.

Authority: CA-Top Secret administrators must have MISC1(NOATS) authority, via the ADMIN function, to ADD or REMOVE the NOATS attribute from ACIDs within their scope. Note that an administrator already defined to CA-Top Secret will, by default, *not* have the NOATS administrative authority.

Types: The NOATS keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

This entry:

```
TSS ADD(USER01) NOATS
```

will prevent USER01 from signing on via ATS.

Administrators can remove the NOATS attribute by entering:

```
TSS REMOVE(USER01) NOATS
```

5.37 NODSNCHK

Operating System: VSE, OS/390, and VM

Description: To specify that no data set name check will be performed. That is, CA-Top Secret will bypass all data set access security checks. All data set access will be audited.

TSS Commands: The following TSS command can be used with the NODSNCHK keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NODSnchk
```

Authority: CA-Top Secret administrators must have MISC9(BYPASS) authority, via the ADMIN function, to assign the NODSNCHK attribute to ACIDs within their scope.

Intended Use: NODSNCHK is intended to only be applied to special products, such as DASD space managers, which access many data sets. CA-Top Secret administrators should avoid applying NODSNCHK to user ACIDs.

Types: The NODSNCHK keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

This entry:

```
TSS ADD(BYPACID) NODSnchk
```

enables BYPACID to bypass security for data sets, and thus access any data set at the installation.

Administrators can remove the NODSNCHK attribute by entering:

```
TSS REMOVE(BYPACID) NODSnchk
```

5.38 NOLCFCHK

Operating System: VSE and OS/390

Description: To allow an ACID to execute any command or transaction for all facilities, regardless of LCF (Limited Command Facility) restrictions. No auditing is done.

TSS Commands: The following TSS command can be used with the NOLCFCHK keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOLcfchk
```

Authority: CA-Top Secret administrators must have MISC9(BYPASS) authority, via the ADMIN function, to assign the NOLCFCHK attribute to ACIDs within their scope.

Note that if the NOLCFCHK attribute is added to an ACID, then that ACID's terminal cannot be LOCKed.

Types: The NOLCFCHK keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To allow a user to execute all commands and programs, the administrator enters:

```
TSS ADD(Q2004) NOL
```

To remove the NOLCFCHK attribute, the administrator enters:

```
TSS REMOVE(Q2004) NOL
```

5.39 NOPERMIT

Operating System: VSE, OS/390, and VM

Description: To prevent an owner from being automatically PERMITted access to a resource whose ownership was transferred via the ADDTO command function.

TSS Commands: The following TSS command can be used with the NOPERMIT keyword: **CREATE, ADDTO.**

Syntax:

```
TSS ADD(acid) resource(prefix) UNDERCUT NOPEpmit
```

Authority: CA-Top Secret administrators must have resource(OWN) authority, via the ADMIN function, to ADD or REMOVE ownership of resources from ACIDs within their scope.

Types: The NOPERMIT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA,SCA, MSCA.**

Examples:

A CA-Top Secret administrator transfers ownership of data set SYS.01 from user OLDOG to user NWDOG as shown:

```
TSS ADD(NWDOG) DSN(SYS.01) UNDERCUT
```

CA-Top Secret automatically PERMITs OLDOG to access the data set, even though ownership was transferred to NWDOG.

To prevent this automatic permission, the administrator enters:

```
TSS ADD(NWDOG) DSN(SYS.01) NOPE UNDERCUT
```

5.40 NOPWCHG

Operating System: VSE, OS/390, and VM

Description: To prevent ACIDs from changing passwords at either signon or initiation.

TSS Commands: The following TSS command can be used with the NOPWCHG keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOPWchg
```

Authority: CA-Top Secret administrators must have ACID(CREATE) authority, via the ADMIN function, to assign the NOPWCHG attribute to ACIDs within their scope.

Types: The NOPWCHG keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To prevent a group of users from changing their passwords, the CA-Top Secret administrator ADDs the NOPWCHG attribute to their profile:

```
TSS ADD(GROUPA) NOPW
```

To remove the NOPWCHG attribute, the administrator enters:

```
TSS REMOVE(GROUPA) NOPW
```

5.41 NORESCHK

Operating System: VSE, OS/390, and VM

Description: To allow an ACID to bypass security checking, including auditing, for all owned resources except data sets and volumes.

TSS Command: The following TSS command can be used with the NORESCHK keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOReschk
```

Authority: CA-Top Secret administrators must have MISC9(BYPASS) authority, via the ADMIN function, to assign the NORESCHK attribute to ACIDs within their scope.

Types: The NORESCHK keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

This entry:

```
TSS ADD(BYUSER) NOR
```

allows BYUSER to bypass security checks for resource access (except data sets and volumes).

To remove the NORESCHK attribute, the administrator enters:

```
TSS REMOVE(BYUSER) NOR
```

5.42 NOSUBCHK

Operating System: VSE, OS/390, and VM

Description: To allow an ACID to bypass alternate ACID usage as well as all job submission security checking. Thus, associated ACIDs may submit all jobs regardless of the (derived) ACID on the job card being submitted.

Note: For OS/390, the USER= keyword must still be inserted onto the job card prior to OS/390 submission.

TSS Commands: The following TSS command can be used with the NOSUBCHK keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOSUBchk
```

Authority: Administrators must have MISC9(BYPASS) authority, via the TSS ADMIN function, to assign the NOSUBCHK attribute to ACIDs within their scope.

Types: The NOSUBCHK keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To allow a Production Controller to submit a job on behalf of any accessor, the administrator enters:

```
TSS ADD(PRDCTL1) NOSUB
```

To remove the NOSUBCHK attribute, the administrator enters:

```
TSS REMOVE(PRDCTL1) NOSUB
```

5.43 NOSUSPEND

Operating System: VSE, OS/390, and VM

Description: To allow an ACID to bypass suspension due to violations (VTHRESH).

TSS Command: The following TSS command can be used with the NOSUSPEND keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOSUSpend
```

Authority: CA-Top Secret administrators must have MISC9(BYPASS) authority via the ADMIN function to assign the NOSUSPEND attribute to ACID within their scope.

Types: The NOSUSPEND keyword is used with the following ACID types: **User, DCA, VCA, SCA, LSCA, MSCA.**

Note: The CREATE and REMOVE command functions can only be issued for USER type ACIDs.

Examples:

The ACID assigned as the CICS default user is an example of an ACID shared by many users that should never suspend as a result of violations. In this example, CICS DFLTUSER=TOPSMAN is allowed to bypass being suspended due to violations:

```
TSS ADD(TOPSMAN) NOSUSPEND
```

To remove the NOSUSPEND attribute, the administrator enters:

```
TSS REMOVE(TOPSMAN) NOSUSPEND
```

5.44 NOVOLCHK

Operating System: VSE, OS/390, and VM

Description: To allow an ACID to bypass volume level security checking.

TSS Commands: The following TSS command can be used with the NOVOLCHK keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) NOVOLCHK
```

Authority: Administrators must have MISC9(BYPASS) authority, via the TSS ADMIN function, to assign the NOVOLCHK attribute to ACIDs within their scope.

Types: The NOVOLCHK keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the NOVOLCHK attribute to an ACID within his scope, the administrator enters:

```
TSS ADD(USER01) NOVOLCHK
```

To allow use of volumes that are not globally allowed for data set creation, the administrator enters:

```
TSS ADD(USER01) NOVOLCHK NODSNCHK
```

Note: NOVOLCHK does not necessarily give access to data sets on the volume. Administrators must enter the NODSNCHK keyword along with NOVOLCHK if they want to allow total access to an entire volume when individual data sets are also being accessed.

To remove the NOVOLCHK attribute, the administrator enters:

```
TSS REMOVE(USER01) NOVOLCHK
```

5.45 OPCLASS

Operating System: VSE and OS/390

Description: To assign or remove a set of CICS operator classes. These values replace those normally found in an ACID's SNT (Signon Table) entry. The OPCLASS values are placed into an ACID's TCT (Terminal Control Table) entry at signon.

TSS Command: The following TSS command can be used with the OPCLASS keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) OPCLass(nn,nn..)
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign OPCLASS values to ACIDs within their scope.

Types: The OPCLASS keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To add OPCLASS values to user CLRK55, the administrator enters:

```
TSS ADD(CLRK55) OPCL(1,4,7)
```

To remove a user's OPCLASS values, the administrator enters:

```
TSS REMOVE(CLRK55) OPCL(1,4,7)
```

5.46 OPIDENT

Operating System: VSE and OS/390

Description: To assign or remove a CICS operator identification value that is equal to the ACID's OPIDENT entry in the CICS SNT (Signon Table). The OPIDENT value is placed into the ACID's TCT at signon.

TSS Commands: The following TSS commands can be used with the OPIDENT keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) OPIdent(xxx)
```

Prefix length — 1-3 characters

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign OPIDENT values to ACIDs within their scope.

Types: The OPIDENT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign an OPIDENT to user BLAS19, the administrator enters:

```
TSS ADD(BLAS19) OPI(XYZ)
```

To remove the user's OPIDENT, the administrator enters:

```
TSS REMOVE(BLAS19) OPI
```

Note: Do not imbed blank spaces to substitute characters. For example:

```
TSS ADD(BLAS19) OPI(X Y)
```

is not a valid entry.

5.47 OPPRTY

Operating System: VSE and OS/390

Description: To assign or remove a CICS operator priority from the associated ACID. The OPPRTY value is placed into the ACID's TCT (Terminal Control Table) at signon.

TSS Commands: The following commands can be used with the OPPRTY keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) OPPrty(0...255)
```

Prefix length — 0-255 (where 0 = no special priority).

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign OPPRTY values to ACIDs within their scope.

Types: The OPPRTY keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign an OPPRTY of 10 to USER01, the administrator enters:

```
TSS ADD(USER01) OPP(10)
```

To remove the OPPRTY assignment, the administrator enters:

```
TSS REMOVE(USER01) OPP(10)
```

5.48 PASSWORD

Operating System: VSE, OS/390, and VM

Description: To assign a password, along with values that control its use, to a previously defined ACID.

TSS Commands: The following TSS commands can be used with the PASSWORD keyword: **CREATE, REPLACE, ADDTO.**

Syntax:

```
TSS ADD(acid) PASsword(password[,0...255], [EXPIRED])
TSS ADD(acid) PASsword(NOPW)
```

Operand	Value	Description
Password	User-defined	MANDATORY Administrator must enter a four- to eight-character password for the associated ACID. This entry might not appear when typed into the PASSWORD field of the ADDTO/REMOVE panel. It will appear as entered freeform on the screen.
	NOPW	Indicates that ACID does not require a password.
Expiration Interval	0...255	OPTIONAL DEFAULT PWEXP value = 30-DAY EXPIRATION INTERVAL Administrator may set the expiration interval to equal 0 to 255 days. If no entry is made, CA-Top Secret uses a default interval set by the PWEXP control option (30 days). When REPLACE is used to change the password and no interval is specified, the user's existing password interval is retained.

Operand	Value	Description
Automatic Expiration	EXPIRED	OPTIONAL Causes ACID's password to automatically expire, forcing the ACID to enter a new password at signon. When the CA-Top Secret administrator does a TSS LIST against the ACID that was set to automatically expire, he will receive a password expiration date of 01/01/80, but with a correct expiration interval. This date is meant to alert the administrator that the user must change his password on the first logon.

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, via the ADMIN function, to assign the PASSWORD attribute to ACIDs within their scope.

Note: A password specified by the ADDTO command function will replace the ACID's previous password.

Types: The PASSWORD keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

The following entry indicates that CA-Top Secret will replace USER56's previous password with WORK, and prompt him to change his password immediately during his first signon. He will be forced to change his password every nine days.

```
TSS ADD(USER56) PAS(WORK,9,EXP)
```

An administrator may also enter:

```
TSS ADD(USER56) PAS(WORK)
```

USER56 will then sign on with this password until it expires in 30 days (or the default set by the PWEXP control option) or until he changes it on his own. This assumes that the NEWPW control option was not set to NU, which would prevent USER56 from changing his own password.

Note: The NOPWCHG attribute also prevents an ACID from changing his password.

A password cannot be removed. An administrator can, however, change an ACID's password via the REPLACE or ADDTO command function.

5.49 PROFILE

Operating System: VSE, OS/390, and VM

Description: To add or remove up to 254 profiles from a specified ACID. Refer to the *General Concepts Guide* for a basic definition of profiles. The *User Guide* describes the use of profiles.

TSS Commands: The following TSS command can be used with the PROFILE keyword: **CREATE ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid)
    PROFile(profile acid,profile acid,...)
```

ACID length — 1-8 characters

Capacity of list— 5 PROFILE ACIDs per TSS command.

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to connect profiles to ACIDs within their scope.

Types: The PROFILE keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

This entry indicates that profile WRIT01 is now connected to USER02.

```
TSS ADD(USER02) PROF(WRIT01)
```

Administrators can designate the order of a new profile using either the AFTER or BEFORE keywords with the profile name. This entry indicates that PROF03 should follow PROF01. For more details, refer to the AFTER and BEFORE keyword in this section.

```
TSS ADD(acid) PROF(PROF03) AFTER(PROF01)
```

If you use the FOR or UNTIL keywords with PROFILE, you will be able to see the expiration date(s) if you enter:

```
TSS LIST(acid) DATA(EXP)
```

To remove the connection between a profile and an ACID:

```
TSS REMOVE(USER02) PROF(WRIT01)
```

5.50 PSTKAPPL

Operating System: VSE and OS/390

Description: Defines the application ID. Depending on the application, the secured signon function uses a specific method to determine the application ID:

- For CICS or APPC applications, the application ID is defined using the standard naming conventions you use to define these applications in a VTAM APPL statement.
- For OS/390 batch jobs that include CA-Top Secret passwords in the JCL, you can replace the password with a PassTicket. The application ID for batch jobs is defined by prefacing the SMF identifier of the system with the characters OS/390. For example, MVSXE05 is the application ID for all batch jobs on machine MVXE05.
- For VSE batch jobs that include CA-Top Secret passwords in the JCL, you can replace the password with a PassTicket. The application ID for batch jobs is defined by prefacing the VSE System Adapter cpuid (Can be displayed with CAISERV Report, or CA? AR Command on Console) of the system with characters "VSE". For Example VSEA is the application ID for all batch jobs on a system with CA System Adapter cpuid A.

TSS Commands: The following TSS commands can be used with the PSTKAPPL keyword: **ADDTO, REMOVE, LIST, REPLACE.**

Syntax:

```
TSS ADD(NDT) PSTKAPPL(application) SESSKEY(abcdef12)
```

SESSKEY is a 1 to 16-byte hexadecimal "password" that is unique to each application assigned as a PassTicket. A SESSKEY is required for each PassTicket.

For more information on SESSKEY. Refer to the *User Guide*.

Authority: Administrators must have MISC1(NDT) authority to administer the NDT Record.

Types: The PSTKAPPL keyword only applies to the NDT Record.

Examples:

To indicate that the session key for KA180987 is A1B2C3, the administrator enters the following command:

```
TSS ADD(NDT) PSTKAPPL(KA180987) SESSKEY(A1B2C3)
```

5.51 SCTYKEY

Operating System: VSE and OS/390

Description: To specify which CICS security keys an ACID may or may not use.

TSS Commands: The following TSS command can be used with the SCTYKEY keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) SCTYKEY(n,n,...)
```

Capacity of list — up to 256 CICS security keys per TSS command. (CICS only recognizes up to 64 security keys per TSS command.)

Authority: Administrators must have ACID(MAINTAIN) authority, with the TSS ADMIN function, to specify SCTYKEYs for ACIDs within their scope.

Security keys are available in all modes except FAIL.

Types: The SCTYKEY keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To specify security keys for user VCA14, the administrator enters:

```
TSS ADD(VCA14) SCTYKEY(1,5,7,11)
```

Administrators may remove security keys by entering:

```
TSS REMOVE(VCA14) SCTYKEY(1,5,7)
```

5.52 SITRAN

Operating System: VSE and OS/390

Description: To specify which CICS transaction CA-Top Secret will automatically execute after an ACID successfully signs on to a facility.

Note: If a SITRAN is ADDed to an ACID that already has a CICS transaction defined, the transaction is REPLACEd.

TSS Commands: The following TSS commands can be used with the SITRAN keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid)
    SITran(CICS transaction name [,facility])
```

Name length — 1-8 characters.

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, via the ADMIN function, to ADD or REMOVE SITRAN values from ACIDs within their scope.

Types: The SITRAN keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To force execution of the CICS transaction PAY6 for a profile ACID, regardless of the facility logged on, the administrator first enters:

```
TSS ADD(PROF3C) SIT(PAY6)
```

Then issuing the following command causes CA-Top Secret to invoke the transaction PAY6 only when logged on to the CICSTEST facility.

```
TSS ADD(PROF3C) SIT(PAY6,CICSTEST)
```

To remove the SITRAN value, the administrator enters:

```
TSS REM(PROF3C) SIT(PAY6)
```

5.53 SOURCE

Operating System: VSE, OS/390, and VM

Description: To specify source reader or terminal prefixes through which the associated ACID may enter the system.

Terminal restriction can be used to restrict Automatic Terminal Signon ACIDs from being used at another terminal.

TSS Commands: The following TSS command can be used with the SOURCE keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) SOUrce(oper,...)
```

Prefix length — 1-8 characters.

Capacity of list — 1-5 prefixes per TSS command.

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, with the ADMIN function, to ADD or REMOVE SOURCE prefixes from ACIDs within their scope.

Types: The SOURCE keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To force a user to initiate all jobs from remote 5, the administrator enters:

```
TSS ADD(R5USR1) SOU(R5)
```

To remove the SOURCE assignment, the administrator enters:

```
TSS REMOVE(R5USR1) SOU(R5)
```

5.54 SUSPEND

Operating System: VSE, MVS, and VM

Description: Prevents ACIDs from accessing the system when a violation occurs.

TSS Commands: The following TSS command can be used with the SUSPEND keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) SUSpend
```

Authority: Administrators must have MISC1(SUSPEND) authority, via the ADMIN function, to ADD or REMOVE the SUSPEND attribute from ACIDs within their scope.

Types: The SUSPEND keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Limiting Suspensions: Administrators may add the FOR or UNTIL keywords onto a SUSPEND entry to limit the number of days the suspension will be enforced. The entry shown below will suspend USER01 for five days.

```
TSS ADD(USER01) SUS FOR(5)
```

This entry suspends USER01 until December 17, 1996.

```
TSS ADD(USER01) SUS UNTIL(12/17/96)
```

When SUSPEND is used with either FOR or UNTIL, the TSS LIST output for the suspended ACID will contain the following:

```
SUSPEND =  UNTIL mm/dd/yy
```

Examples:

USER02 is on leave until November 10, 1996. To prevent someone from signing on using his ACID, the administrator enters:

```
TSS ADD(USER02) SUS UNTIL(11/10/96)
```

Note: If an ACID is suspended administratively, the ASUSPEND keyword must be used to remove the suspension.

To remove a temporary SUSPEND (SUS UNTIL(DATE)), the administrator enters:

```
TSS REMOVE(ACARP) ASUS UNTIL
```

To remove the SUSPEND attribute from an ACID, or to unsuspend an ACID that was **automatically** suspended due to a violation, the administrator enters:

```
TSS REMOVE(ACARP) SUS
```

Note: If an ACID is suspended administratively, the ASUSPEND keyword must be used to remove the suspension.

To remove a temporary suspend (SUS UNTIL(date)), the administrator enters:

```
TSS REMOVE(ACARP) SUS UNTIL
```

5.55 TARGET

Operating System: VSE, MVS, and VM

Description: Specifies which CA-Top Secret nodes receive commands and how the local node processes it.

Note: When administering commands against a user-defined resource class, the resource class must be defined on the sending node or the node where the resource class was defined.

TSS Commands: The following TSS command can be used with the TARGET keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, REPLACE, RENAME, ADMIN, DEADMIN, WHOOWNS, WHOHAS, MOVE, LIST, DELETE.**

Syntax:

```
TSS ADD(acid) keyword(s) TARGET(node,node,...)
```

Authority: Administrators must have MISC2(TARGET) authority, via the ADMIN function, to use the TARGET keyword to override the default CPF routing command.

Types: The TARGET keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To add data sets beginning with SYS1. to the Accounting Department and transmit them to all nodes whose names start with R, the administrator enters:

```
TSS ADD(ACCDPT)  DSN(SYS1.) TARGET(R*) WAIT(Y)
```

To remove the data sets the administrator enters:

```
TSS REMOVE(ACCDPT) DSN(SYS1.) TARGET(R*) WAIT(Y)
```

5.56 TIMEREC

Operating System: VSE, MVS, and VM

Description: Administrators can add, remove, replace, or list TIME records in the SDT (Static Data Table) Record.

TSS Commands: The following TSS commands can be used with the TIMEREC keyword: **ADDTO, REMOVE, REPLACE, LIST.**

Syntax:

```
TSS ADD(SDT) TIMEREC(time-name) DESCRIPT(descript-name)
             RANGE(hhmm,hhmm,...)
```

Operand Description: The following operand is used with the TIMEREC keyword:

Operand	Description
time-name	Specifies an eight-character *time-name* that is user-defined and can contain letters, numbers or special characters.

Authority: CA-Top Secret administrators must have MISC3(SDT) authority, granted by the TSS ADMIN function, to ADD or REMOVE records in the SDT Record.

Types: The RECORD keyword is used with the SDT Record.

Examples:

To add a TIME record called TEMP1 to the SDT, enter:

```
TSS ADD(SDT) TIMEREC(TEMP1)
```

For more information concerning the SDT Record, refer to the *User Guide*.

5.57 TIMES

Operating System: VSE, MVS, and VM

Description: To assign a range of hours during which a facility may be accessed.

TSS Commands: The following TSS command can be used with the TIMES keyword: **ADDTO, PERMIT, REVOKE, REMOVE.**

Syntax:

```
TSS ADDTO(acid) FACILITY(facility) TIMES(00,24)
```

Time Ranges: The first two digits in the TIME operand specify the hour at which (CPU time) CA-Top Secret permits access to the facility. The second pair of digits specify the hour through which CA-Top Secret permits access. Thus, CA-Top Secret permits access from the first minute of the hour specified in the first operand, until the first minute of the hour specified in the second operand.

Range: To specify an inclusive range, set the start time to a lesser number than the stop time. The entry,

```
TSS ADDTO(USER01) FAC(CICS) TIMES(06,12)
```

The following entry allows USER01 to access the CICS facility from 8 p.m. until 10 a.m. the following day.

```
TSS ADDTO(USER01) FAC(CICS) TIMES(20,10)
```

Specific Hour: To assign access for one hour (10 a.m. to 11 a.m.), the administrator enters:

```
TSS ADDTO(ACID) FAC(CICS) TIMES(10,11)
```

Authority: Although no specific authority is required, CA-Top Secret administrators must have facility administrative authority, via the TSS ADMIN function, to ADD facilities to an ACID.

Types: The TIMES keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

5.58 TRACE

Operating System: VSE, MVS, and VM

Description: To activate a diagnostic trace on all ACID activity (initiations, resource access, violations, user's security mode, etc.)

TSS Commands: The following TSS command can be used with the TRACE keyword: **CREATE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) TRACE
```

Authority: CA-Top Secret administrators must have MISC9(TRACE) authority, via the ADMIN function, to specify the TRACE attribute for ACIDs within their scope.

Activation of TRACE: TRACE is usually activated at the request of CA-Technical Support, or whenever an administrator requires its use for problem diagnosis.

Where CA-Top Secret records trace information depends on the settings of the SECTRACE control option. Refer to SECTRACE in the *Control Options Guide* for details.

Types: The TRACE keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To activate a diagnostic trace to solve an authorization problem, the CA-Top Secret administrator uses the following procedure:

1. Enter:

```
TSS ADD(USER01) TRACE
```

2. Enter:

```
TSS MODIFY('SECTRACE(ACT|WTO|WTL)')
```

ACT Activates the trace.

WTO Sends trace information to the security console.

WTL Sends trace information to syslog.

3. When USER01 runs a job, trace information will be sent to the destination(s) specified in step 2.
4. Refer to Diagnostic Trace in the *Troubleshooting Guide* for details on how to interpret the resulting trace information.

To remove the TRACE attribute, the administrator enters:

```
TSS REMOVE(USER01) TRACE
```

5.59 TRANSACTIONS

Operating System: VSE and MVS

Description: To confine ACIDs to using a specific transaction, or subset of the transactions, available within that facility.

TSS Commands: The following TSS command can be used with the TRANSACTIONS keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) TRANSactions(fac,(trans[(G)])
```

Transaction name — 1-8 characters.

Capacity of list — 1-30 transaction names or prefixes per TSS command.

Inclusive vs. Exclusive: The TRANSACTIONS keyword is inclusive in that it confines an ACID to using specific transactions for a facility. Refer to the XTRANSACTIONS keyword to determine how to allow an ACID to use *all but* a specific list of transactions for a facility.

Authority: CA-Top Secret administrators must have MISC1(LCF) authority, via the ADMIN function, to ADD or REMOVE TRANSACTIONS from ACIDs within their scope.

Types: The TRANSACTION keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL Record.**

Examples:

To confine a group of CICS clerks to a set of transactions, the administrator enters:

```
TSS ADD(PROF1) TRANS(CICSP,(CPO1,CPO2,CPO3))
```

The letter G next to the transaction prefix indicates that the ACID is confined to using transactions beginning with the prefix specified. The following command indicates that ACID EJ001 is confined to using transactions prefixed by CPO.

```
TSS ADD(EJ001) TRANS(CICSP,(CPO(G)))
```

The letter V next to the transaction prefix indicates that the ACID may use the transaction, however, CA-Top Secret will first re-verify the ACID's password before the transaction is executed.

To remove the TRANSACTIONS restriction, the administrator enters:

```
TSS REMOVE(EJ001) TRANS(CICSP,(CPO(G)))
```

5.60 TZONE

Operating System: VSE, MVS, and VM

Description: To specify an ACID's physical time zone in relation to the CPU's time zone. This forces all date and time rules to be based on the ACID's local date and time, not on the CPU's date and time.

TSS Commands: The following TSS commands can be used with the TZONE keyword: **CREATE, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) TZONE([-]nn)
```

Range of values for nn can equal from -12 to +12.

Authority: CA-Top Secret administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to specify TZONE for ACIDs within their scope.

Examples:

The CPU is located in New York and user ZAP99 is located in San Diego. To ensure that all date and time checking is based on ZAP99's Pacific Coast Time and not the CPU's Eastern Standard Time, the CA-Top Secret administrator enters:

```
TSS ADD(ZAP99) TZONE(-3)
```

To allow the user's timezone to revert back to the CPU's timezone, the administrator enters:

```
TSS REMOVE(ZAP99) TZONE(0)
```

5.61 UNDERCUT

Operating System: VSE, MVS, and VM

Description: To transfer resource ownership from one ACID to another.

TSS Commands: The following TSS command can be used with the UNDERCUT keyword: **CREATE, ADDTO.**

Syntax:

```
TSS ADD(acid) resource(prefix) UNDERCUT
```

Undercutting: Undercutting (transfer of ownership) occurs when an administrator ADDS a prefix which is shorter than another resource prefix which is already owned. The use of the UNDERCUT keyword indicates that the transfer is intentional. If the UNDERCUT keyword is omitted, CA-Top Secret issues the following message:

```
TSS0351E SPECIFY 'UNDERCUT' TO TRANSFER OWNERSHIP
```

This prevents CA-Top Secret administrators from unintentionally transferring or undercutting ownership.

Result of Transfer: When resource ownership is transferred from one owner to another, CA-Top Secret automatically PERMITs the old owner to have full access to the resource. To prevent the old owner from having full access to resources they no longer own, NOPERMIT can be entered as part of the ADDTO command function:

```
TSS ADD(NEWOWNER) DSN(SYS.01) UNDERCUT NOPERMIT
```

Generic Prefixing: A data set defined as SYS.01 is owned by ACID2. Since CA-Top Secret supports generic prefixing, it will consider SYS.01 and SYS.01.02 to be generic prefixes for the *same* data set. Thus the following entry transfers ownership of SYS.01.02 from ACID2 to ACID1.

```
TSS ADD(ACID1) DSN(SYS.01) UNDERCUT
```

Rules for Transfer

- An administrator can only undercut prefixes within his scope of authority.
- Undercutting only applies to prefixes, not to full resource names. Therefore, if USER. and USER01. were full minidisk names they could exist as separate minidisks.
- Undercutting only applies to prefixes of the same resource type. Thus USER could exist as a minidisk, and USER01 could exist as a program.

Authority: CA-Top Secret administrators must have RESOURCE(OWN) authority, via the TSS ADMIN function, to ADD or REMOVE ownership of resources from ACIDs within their scope.

Types: The UNDERCUT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

5.62 UNTIL

Operating System: VSE, MVS, and VM

Description: To assign or remove the specific date on which an ACID will expire.

The format for date entries is determined by the settings for the DATE control option. Determine these settings before entering a date with the UNTIL keyword. The default is MM/DD/YY.

Any year (YY) entered as 70 or above is considered by CA-Top Secret to be a 20th century date. Any year below 70 is considered to be a 21st century date. For example, 68 would be processed as being 2068 not 1968.

TSS Commands: The following TSS commands can be used with the UNTIL keyword: **CREATE, PERMIT, REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) UNTil(mm/dd/yy)
```

Authority: No specific administrative authority is needed to ADD or REMOVE the UNTIL keyword.

Types: The UNTIL keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples

Note: The following examples assume the date format is MM/DD/YY.

To allow use of an ACID until December of 1997, the administrator enters:

```
TSS ADD(YURGO) UNT(12/01/97)
```

ACID YURGO will now expire on 12/01/97. The ADDTO function may also be used to replace or change an expiration date. The following entry changes YURGO's expiration date from 12/01/97 to 07/04/98.

```
TSS ADD(YURGO) UNT(07/04/98)
```

The same change could have been made with the REPLACE function. Expiration dates may be removed by entering:

```
TSS REMOVE(YURGO) UNT
```

If you wish to REMOVE the expiration interval and are unsure of whether you specified FOR or UNTIL on the TSS ADD, you can use the following syntax.

```
TSS REMOVE(acid) EXPIRE
```

To reactivate an expired ACID, the administrator may either enter:

```
TSS ADD(ACID56) UNT(mm/dd/yy)
    - or -
TSS ADD(USER56) FOR(0)
```

The UNTIL keyword may also be used in conjunction with the FACILITY and PROFILE keywords:

```
TSS ADD(USER56) FAC(CICSPROD) UNTIL(07/04/97)
TSS ADD(USER56) PROF(CICSPROD) UNTIL(07/04/97)
```

Specifying the UNTIL keyword with PROFILE, allows you to see the expiration date(s) by entering:

```
TSS LIST(profacid) DATA(EXP)
```

The UNTIL keyword cannot be used to REMOVE an expiration date from a facility or profile. For example, the following TSS command will not remove the expiration date from the profile, but will remove the profile from the user record:

```
TSS REM(USER56) PROF(TECHPROF) UNTIL
```

To remove an expiration date from a facility or profile, the facility or profile must be removed from the ACID and then added again to the ACID without the expiration date.

Note: For examples of the use of UNTIL with SUSPEND, see the SUSPEND keyword.

5.63 USER

Operating System: VSE, MVS, and VM

Description: To grant or remove access to unownable, installation-defined resources.

The *General Concepts Guide* defines installation-defined resources, and the contrasts between ownable and unownable resources.

TSS Commands: The following TSS command can be used with the USER keyword: **CREATE ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) USEr(class,oper,...)
```

Prefix length — 1 character.
Capacity of list — 1-8 characters per TSS command.

Authority: CA-Top Secret administrators must have MISC1(USER) authority, via the ADMIN function, to ADD or REMOVE the USER keyword from ACIDs within their scope.

The installation must customize the application programs so they will call CA-Top Secret to verify access to installation-defined resources. The installation may define up to 40 unowned resource classes. Refer to the respective MVS and VM *Implemention Guide* for details.

Types: The USER keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL Record.**

Examples:

To allow a user to access several unowned user resources, the administrator enters:

```
TSS ADD(GENU8) USE(U,WELL,OIL,GAS)
```

To remove access to unowned installation-defined resources, the administrator enters:

```
TSS REMOVE(GENU8) USE(U,WELL)
```

5.64 USERNL1

Operating System: VSE and OS/390

Description: Used to assign or remove a primary national language attribute to an ACID. This attribute matches the three character CICS language codes that support unique end-user messages in the CICS Transaction Server environment.

TSS Commands: The following TSS commands can be used with the USERNL1 keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) USERNL1(xxx)
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign USERNL1 values to ACIDs within their scope.

Types: The USERNL1 keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the CICS primary national language code for German, the administrator enters:

```
TSS ADD(SYSA) USERNL1(DEU)
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) USERNL1
```

5.65 USERNL2

Operating System: VSE and OS/390

Description: Used to assign or remove a secondary national language attribute to an ACID. This attribute matches the three character CICS language codes that support unique end-user messages in the CICS Transaction Server environment.

TSS Commands: The following TSS commands can be used with the USERNL2 keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) USERNL2(xxx)
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign USERNL2 values to ACIDs within their scope.

Types: The USERNL2 keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the CICS secondary national language code for US English, the administrator enters:

```
TSS ADD(SYSA) USERNL2(ENU)
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) USERNL2
```

5.66 VSECATBT

Operating System: VSE

Description: Used to assign the VSE special right to catalog B-transients. This attribute corresponds to the RIGHT attribute of the DTSECTAB.

TSS Commands: The following TSS commands can be used with the VSECATBT keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) VSECATBT
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign VSECATBT values to ACIDs within their scope.

Types: The VSECATBT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the VSE special right to catalog B-transients, the administrator enters:

```
TSS ADD(SYSA) VSECATBT
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) VSECATBT
```

5.67 VSEMCON

Operating System: VSE

Description: Used to assign the VSE special right to open the master console. This attribute corresponds to the MCON attribute of the DTSECTAB.

TSS Commands: The following TSS commands can be used with the VSEMCON keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) VSEMCON
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign VSEMCON values to ACIDs within their scope.

Types: The VSEMCON keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the VSE special right to open the master console, the administrator enters:

```
TSS ADD(SYSA) VSEMCON
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) VSEMCON
```

5.68 VSERDD

Operating System: VSE

Description: Used to assign the VSE special right to read directories. This attribute corresponds to the READDIR attribute of the DTSECTAB.

TSS Commands: The following TSS commands can be used with the VSERDD keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) VSERDD
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign VSERDD values to ACIDs within their scope.

Types: The VSERDD keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the VSE special right to read directories, the administrator enters:

```
TSS ADD(SYSA) VSERDD
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) VSERDD
```

5.69 VSESYSAD

Operating System: VSE

Description: Used to assign the VSE special right of security administrator. This attribute corresponds to the AUTH attribute of the DTSECTAB.

TSS Commands: The following TSS commands can be used with the VSESYSAD keyword: **CREATE, ADDTO, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) VSESYSAD
```

Authority: Administrators must have ACID(MAINTAIN) authority, via the TSS ADMIN function, to assign VSESYSAD values to ACIDs within their scope.

Types: The VSESYSAD keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To assign the VSE special right of security administrator, the administrator enters:

```
TSS ADD(SYSA) VSESYSAD
```

To remove the above attribute, the administrator enters:

```
TSS REMOVE(SYSA) VSESYSAD
```

5.70 XTRANSACTIONS

Operating System: VSE and MVS

Description: To restrict ACIDs from using a specific transaction, or subset of the transactions, available within that facility.

TSS Commands: The following TSS command can be used with the XTRANSACTIONS keyword: **CREATE REPLACE, ADDTO, REMOVE.**

Syntax:

```
TSS ADD(acid) XTRANSactions(fac,(trans[(G)]))
```

Prefix length — 1-8 characters. Entries are treated as a prefix only if the generic indicator (G) follows the entry.

Capacity of list — 1-30 transaction names or prefixes per TSS command.

Authority: Administrators must have MISC1(LCF) authority, via the ADMIN function, to ADD or REMOVE the XTRANSACTIONS keyword from ACIDs within their scope.

The XTRANSACTIONS keyword is exclusive in that it allows an ACID to use ***all but*** a specific transaction(s) for a particular facility. Refer to the TRANSACTIONS keyword to determine how to confine ACIDs to using transactions for a given facility.

Types: The XTRANSACTIONS keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL Record.**

Examples:

To prohibit a group of CICS clerks from using a set of transactions, the administrator enters:

```
TSS ADD(PROF1) XTRANS(CICSP,(CPO1,CPO2,CPO3))
```

The letter G next to the transaction prefix indicates that the user is prohibited from using transactions that begin with the prefix specified. The following entry indicates that user EJ001 is prohibited from using transactions prefixed by CPO.

```
TSS ADD(EJ001) XTRANS(CICSP,(CPO(G)))
```

To remove the XTRANSACTIONS restriction, the administrator enters:

```
TSS REMOVE(EJ001) XTRANS(CICSP,(CPO(G)))
```

Chapter 6. How to Use ADMIN/DEADMIN

This chapter discusses the standard formats and rules for assigning and removing administrative authorities from a control ACID.

Security administrators should read the information on Security Administration and Auditing in the *User Guide* prior to using this guide. Refer to the respective *Implemention Guide* and *Planning Guide* for guidelines and examples of how to organize the security administration function.

6.1 Purpose

6.1.1 ADMIN

Given the proper administrative authority, security administrators with any type of control ACID may use the ADMIN function to assign administrative capabilities to subordinate CA-Top Secret administrators that fall within their scope.

6.1.2 DEADMIN

The DEADMIN function is used to remove administrative capabilities. All formats, rules, and restrictions that apply to the ADMIN function also apply to the DEADMIN function.

6.2 Components of ADMIN and DEADMIN Functions

The security administrator must provide CA-Top Secret with two pieces of information via the ADMIN or DEADMIN function: **Authority Type,** and **Authority Level.**

6.2.1 Authority Types

CA-Top Secret administrators may give other CA-Top Secret administrators the authority to administer the following CA-Top Secret authority types:

Authority	Keyword or Examples
Resource	Allows administrators to give authority to issue TSS commands for all resource types owned within their administrative scope. An administrator can also give authority for a specific resource (like DSNAME). For detailed information on each resource, see Chapter 22, "Summary of Resources." All specific resources have the same authority levels, OWN, XAUTH, AUDIT, REPORT, INFO and ALL. The access keyword, which is a subset of RESOURCE, is used with XAUTH to specify access levels. Access level operands depend on the type of resource to which access is being PERMITted. Some examples might include: NONE, READ, WRITE, UPDATE, SCRATCH, BROWSE, MULTI, MREAD, MWRITE.
ACID	Used to specify the authority levels, such as MAINTAIN, REPORT, AUDIT, and CREATE, at which administrators can manage ACIDs within their scope.
Facility	Any active facility contained in the Facility Matrix, such as VM, TSO, IMS, CICSTEST, CA-Roscoe, etc.
Data	Information that the administrator may display using the TSS LIST function: BASIC, RESOURCE, XAUTH, LCF, SOURCE, PROFILE, INSTDATA, CICS, ADMIN, NAMES, PWVIEW, PASSWORD, WORKATTR, SESSKEY, and ALL. **Note:** An administrator can display all of the above information, *except* PWVIEW and SESSKEY, using the TSS LIST command function. Refer to Chapter 10, "How to USE LIST," if further details are required.
MISC1	Low-level administrative functions: LCF, INSTDATA, USER, LTIME, SUSPEND, NOATS, RDT, TSSSIM, ALL.
MISC2	DLF, TARGET, NDT, TSO, SMS, APPCLU, PC, WORKATTR, ALL.
MISC3	SDT, ALL.
MISC8	LISTRDT, LISTSTC, MCS, REMASUSP, ALL.

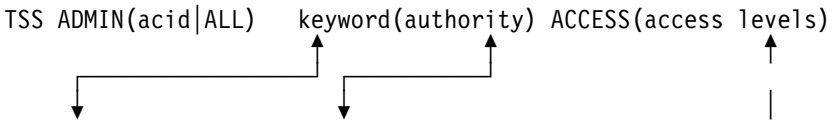
MISC9 High-level administrative functions: BYPASS, TRACE, CONSOLE, STC, MASTFAC, MODE, GLOBAL, GENERIC, ALL.

SCOPE Used to define the scope for the LSCA

6.2.2 Authority Levels

With each authority type, except facility, the administrator may specify several *levels* of authority. Each authority level specifies exactly how much authority an administrator will have over the authority type. The following figure shows each authority type and its corresponding levels of authority.

Authority Levels:



Keyword	Authority Level	ALL
RESOURCE	OWN,XAUTH,AUDIT,INFO, REPORT,ALL	BROWSE CONTROL
ACID	XAUTH,AUDIT,CREATE,INFO, DEFNODES,REPORT,MAINTAIN,ALL	DELETE FETCH
DATA	BASIC,RESOURCE,XAUTH,LCF, SOURCE,INSTDATA,CICS, PROFILE,ADMIN,NAMES,ACID WORKATTR,SESSKEY, PASSWORD, PWVIEW, ALL	FIND LOAD MULTI MREAD MWRITE
MISC1	LCF,INSTDATA,USER,LTIME,RDT, SUSPEND,NOATS,TSSSIM,ALL	PURGE READ
MISC2	SMS,TSO,NDT,DLF,TARGET, PC,WORKATTR,APPCLU,ALL	SCRATCH UPDATE
MISC3	SDT,ALL	
MISC8	LISTRDT,LISTSTC,MCS, REMASUSP, ALL	
MISC9	BYPASS,TRACE,CONSOLE,STC, MASTFAC,MODE,GLOBAL, GENERIC,ALL	
FACILITY	Specific Facilities	
SCOPE	Define scope for LSCA	

Refer to the detailed reference pages for more information on access levels.

6.3 Entry Methods

CA-Top Secret administrators enter TSS ADMIN/DEADMIN command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

6.3.1 Command Syntax

The following example shows how TSS command functions are entered freeform at an online terminal.

```
TSS ADMIN(acid) keyword(authority level) ACCESS(access level)
          1      2           3                  4
```

Field	Description
1	The ACID of the administrator being granted ADMIN authority.
2	The authority type that the administrator is being authorized to manage.
3	The authority level(s) at which the administrator will manage the authority type.
4	The access levels (i.e., FETCH, WRITE, etc.) for which the administrator is authorized to PERMIT RESOURCE(XAUTH) resource access. If no entry is made, CA-Top Secret usually assigns a default level based on the resource type.

6.3.2 Sample Entries

The entry:

```
TSS ADD(VCA1) DSNAME(OWN,AUDIT)
```

indicates that security administrator VCA1 assigns ownership of data sets by adding them to the Audit Record. Thus VCA1 could enter:

```
TSS ADD(DEPT1) DSNAME(XYZ.DATA.CRASH)
```

and

```
TSS ADD(AUDIT) DSNAME(XYZ)
```

to audit the specified data set.

To remove VCA1's authority to assign the AUDIT attribute for DSNAMEs, the administrator enters:

```
TSS DEADMIN(VCA1) DSNAME(AUDIT)
```

Note that VCA1 still has the authority to assign ownership of DSNAMEs to ACIDs within his scope.

To totally remove VCA1's authority for DSNAMEs, the administrator enters:

```
TSS DEADMIN(VCA1) DSNAME(ALL)
```

6.4 General Rules

The following general rules apply to all ADMIN and DEADMIN entries. Specific rules are documented with the applicable keyword.

6.4.1 Authority

An administrator can only assign authority type keywords and authority level operands for which he has the authority. For example, an SCA cannot grant an administrator MISC9(ALL) authority, unless he himself has MISC9(ALL) authority.

6.4.2 Scope

CA-Top Secret administrators can only assign administrative authorities to subordinate administrators within their scope. For example, VCAs (divisional administrators) *cannot* assign administrative authorities to other VCAs, even if they are in the same division. They *can,* however, assign administrative authorities to DCAs (departmental administrators), or User ACIDs, or auditors within the divisions they control.

Only the MSCA, who is defined to CA-Top Secret during the installation process, can CREATE and assign administrative authorities to SCAs.

6.4.3 Limitations

Administrative authority cannot be assigned to zones, division, department, or profile ACIDs.

6.4.4 Granting Authority to All Users

Administrative authority may be granted to all users within the organization by entering:

```
TSS ADMIN(ALL)
```

6.5 Applicable Keyword List

The following keywords are used with the TSS ADMIN and DEADMIN functions. The reference pages that follow contain detailed documentation for each keyword.

```
ACID
DATA
FACILITY
MISC1
MISC2
MISC3
MISC8
MISC9
RESOURCE
resource
SCOPE
```

Note: The keyword that is listed as "resource" can be used as an archetype for any resource defined to the RDT. All resources defined to the RDT can also be used with the ADMIN/DEADMIN command function. For an explanation of these keywords, refer to the chapter entitled: "Summary of Resources."

6.6 ACID

Operating System: VSE, OS/390, and VM

Description: To give CA-Top Secret administrators the authority (or to remove their authority) to specify the authority level(s) at which they can manage ACIDs within their scope.

TSS Commands: The following TSS commands can be used with the ACID keyword: **CREATE, DELETE, ADDTO (STC only), PERMIT, REVOKE, RENAME, WHOHAS LIST.**

Syntax:

```
TSS ADMIN(acid) ACID(authority level(s))
```

Authority Level: The CA-Top Secret administrator may specify any or all of the following authority levels.

ALL Grants all of the ACID type authorities.

CREATE Gives an administrator the authority to CREATE and DELETE ACIDs.

XAUTH Gives the authority to PERMIT or REVOKE ACIDs used for job submissions.

AUDIT Allows an administrator to attach the AUDIT attribute to ACIDs within his scope. This authority level is likewise required to be able to report on the AUDIT attribute. Thus, an administrator without ACID(AUDIT) may not run TSSAUDIT and will not be able to see the AUDIT attribute through TSS LIST.

REPORT Grants the administrator the authority to use the TSSUTIL and TSSCHART utilities to prepare customized reports showing the security activity for ACIDs within his scope.

INFO Allows administrators to use the WHOHAS function to determine who has access to specific ACIDs used for job submissions.

MAINTAIN Allows administrators to perform TSS command functions for ACIDs within their scope, including:

RENAME: Renames an ACID.

MOVE: Moves an ACID from one department or division to another. MOVE will work only if both the source organization and the destination are within the administrator's scope. MOVE authority is ***not*** valid if assigned to users or DCAs.

REPLACE: Replaces the NAME of an ACID.

REPLACE: Replaces the ACID's password information.

REPLACE: Replaces the expiration date for an ACID via the FOR keyword.

REPLACE: Replaces the CICS OPIDENT, OPPRTY, OPCLASS, and/or SITRAN values for an ACID.

ADDTO: Adds the SOURCE from which an ACID may initiate.

ADDTO: Adds the profiles to which an ACID is connected.

DEFNODES The ability to ADD, REMOVE, and REPLACE DEFNODES on an ACID record.

Types: The ACID keyword is used with the following ACID types: **User, DCA, VCS, ZCA, LSCA, SCA, MSCA.**

Examples:

To give the Payroll Department's auditor the authority to generate TSSUTIL reports regarding ACID activity, and the authority to see who has access to the department's job submission ACIDs, via the WHOHAS function, the administrator enters:

```
TSS ADMIN(PAYAUD) ACID(REPORT,INFO)
```

To give the Payroll Department's auditor the authority to prepare customized reports showing security activity, the administrator enters:

```
TSS ADMIN(PAYAUD) RESOURCE(REPORT)
```

To give a DCA the authority to create, delete, and maintain the department's ACIDs, and to permit users in the department to use job submission ACIDs to submit jobs; the administrator enters:

```
TSS ADMIN(TECHDCA) ACID(CREATE,MAINTAIN,XAUTH)
```

To remove TECHDCA's authority for ACIDs, the administrator enters:

```
TSS DEADMIN(TECHDCA) ACID(CREATE,MAINTAIN,XAUTH)
```

6.7 DATA

Operating System: VSE, OS/390, and VM

Description: To give CA-Top Secret administrators the authority, or to remove their authority, to list information via TSS LIST from the Security File.

Note: When an ACID is given any type of DATA administration authority, DATA(NAMES) is always implied.

TSS Commands: The following TSS command can be used with the DATA keyword: **LIST, ADMIN, DEADMIN.**

Syntax:

```
TSS ADMIN(acid) DATA(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify any or all of the following authority levels:

BASIC Authorizes administrators to list an ACID to see the name associated with the ACID, the ACID's type, facilities he is permitted to access, profiles he is associated with, and when the ACID was created, modified, and last used.

RESOURCE Authorizes administrators to list resources owned by an ACID within their scope.

XAUTH Authorizes administrators to list resources which may have been PERMITted by an ACID within their scope, the level at which the ACID may access the resource, and the owner of the resource.

LCF Authorizes administrators to list the commands and/or transactions that an ACID is confined to (via TRANS/CMD) or restricted from (via XTRANS/XCMD).

SOURCE Authorizes administrators to list the device from which an ACID must initiate.

INSTDATA Authorizes administrators to list the installation data for an ACID.

CICS Authorizes administrators to list values for CICS operator fields: OPCLASS, OPIDENT, OPPRTY

TSO Authorizes administrators to list an AICD's default TSO data.

SMS Authorizes administrators to list an ACID's default SMS data.

PROFILE Allows administrators to list contents of all profiles connected to an ACID.

ADMIN Allows administrators to list an ACID's administrative authority.

NAMES Allows administrators to list an ACID's name, and the associated Department or Division names.

Note: When an ACID is given any type of DATA administration authority, DATA(NAMES) is always implied.

ACIDS Allows administrators to list all ACIDS connected to the ACID entered in the LIST command.

PASSWORD Allows administrators to display the ACID's password expiration date and interval, *not* the actual password.

PWVIEW Authorizes administrators to display the ACID's actual password, plus the expiration date, and interval. If the PWVIEW control option is set to NO, it will override the PWVIEW authority level.

PCDATA Authorizes administrators to display the PC group information associated with that ACID. This includes PCIDLE, PCOPTS, PCMINPWD, PCDSDAYS, PCLGTYPE and PCADMIN.

SESSKEY Authorizes administrators to display the SESSKEYs associated with each LINKID in the APPCLU Record.

WORKATTR Authorizes administrators to display the SYSOUT account and delivery attributes associated with a particular ACID. This includes WAACCNT, WABLDG, WADEPT, WAADDR1, WAADDR2, WAADDR3, WAADDR4, WANAME and WAROOM.

ALL Allows administrator to list everything except PASSWORD, SESSKEY and PROFILE contents.

Rules:

1. Secondary administrators and auditors may be given the ability to request all portions of a Security Record with the ***exception*** of passwords and profile contents by issuing the following ADMIN command function:

   ```
   TSS ADMIN(acid) DATA(ALL)
   ```

2. If it is desired that an administrator have the ability to list every field of a user security record, ***including*** the password field(s) and the contents of profiles connected to the ACID, then the administrator must be explicitly given that ability with the following command:

   ```
   TSS ADMIN(acid) DATA(ALL,PWVIEW,PROFILE)
   ```

Types: The DATA keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To give divisional administrator TECHVCA the authority to list every possible DATA field and the contents of profiles, *excluding* the password itself and any applicable SESSKEYs, the administrator enters:

```
TSS ADMIN(TECHVCA) DATA(ALL,PASSWORD,PROFILE)
```

To remove TECHVCA's authority for DATA:

```
TSS DEADMIN(TECHVCA) DATA(ALL,PASSWORD,PROFILE)
```

Note: Because DATA(PWVIEW) implicitly includes the administrative authorities granted by DATA(PASSWORD); namely, to view the password expiration interval and date, TSS ADMIN/DEADMIN of one of these DATA authorities may affect the other one as follows:

1. TSS ADMIN(acid) DATA(PWVIEW) grants the ACID DATA(PASSWORD) as well as DATA(PWVIEW). However, TSS ADMIN(acid) DATA(PASSWORD) does not grant the ACID DATA(PWVIEW).
2. If an ACID has both DATA(PASSWORD) and DATA(PWVIEW), TSS DEADMIN(acid) of either one of these authorities removes the other one as well.

   To remove only DATA(PWVIEW) from the ACID, therefore, the administrator should first issue TSS DEADMIN(acid) DATA(PWVIEW), and then execute TSS ADMIN(acid) DATA(PASSWORD).

6.8 FACILITY

Operating System: VSE, OS/390, and VM

Description: To give TSS administrators the authority, or to remove their authority, to administer the use of a specific facility (VM) or facilities (in VSE and OS/390).

TSS Commands: The following TSS commands can be used with the FACILITY keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, REPLACE, ADMIN, DEADMIN.**

Syntax:

```
TSS ADMIN(acid) FACility(facility name(s))
```

Authority: CA-Top Secret administrators may only assign facilities which they have been authorized to within their scope.

Authority Levels: Not applicable

General Use: Facility authority is generally used to restrict the facilities that an administrator may specify using the ADDTO or CREATE function.

Types: The FACILITY keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

If an SCA wants to give an administrator the authority to create and maintain ACIDs for CICS users, the administrator enters:

```
TSS ADMIN(BOSSVCA) ACID(CREATE,MAINTAIN)
    FAC(CICSPROD,CICSTEST)
```

This entry allows the TSS administrator to create ACIDs for CICS users or profiles, and would allow the administrator to use various TSS functions (ADDTO, MOVE, RENAME, etc.) to maintain those ACIDs.

CA-Top Secret does not check an administrator's facility authority when the administrator specifies a FACILITY within a TSS PERMIT function.

Note: Specifying ALL will give the security administrator the authority to add *any* facility to an ACID within their scope.

6.9 MISC1

Operating System: VSE, OS/390, and VM

Description: To give or to remove a CA-Top Secret administrator's authority to perform one or more administrative functions.

TSS Commands: The following TSS commands can be used with the MISC1 keyword: **ADMIN, DEADMIN only.**

Syntax:

```
TSS ADMIN(acid) MISC1(authority level(s))
```

Authority Level: The CA-Top Secret administrator may specify any or all of the following MISC1 authorities:

LCF Authorizes administrators to assign LCF command and transaction restrictions ((X)COMMAND and (X)TRANSACTION) to ACIDs within their scope.

INSTDATA Authorizes administrators to associate installation data with ACIDs within their scope. It also authorizes administrators to ADD Dynamic Update Facility attributes, DUFXTR and DUFUPD, to ACIDs within their scope.

USER Authorizes administrators to administer the use of unownable installation-defined resources (USERx).

LTIME Authorizes administrators to set time intervals that determine when CA-Top Secret will lock an unused terminal for ACIDs within their scope.

SUSPEND Authorizes administrators to administer the SUSPEND attribute to ACIDs within their scope.

NOATS Authorizes administrators to prevent ACIDs within their scope (in CICS and CA-IDMS) from signing on via ATS (Automatic Terminal Signon).

RDT Authorizes the administrator to maintain and list the RDT Record (Resource Descriptor Table) and the FDT (Field Descriptor Table) Record.

TSSSIM Authorizes administrators to use the TSSSIM utility.

ALL Authorizes administrators to use all of the authorities.

Types: The MISC1 keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

This entry allows the administrator to suspend and unsuspend ACIDs within his scope.

```
TSS ADMIN(AMCDCA) MISC1(SUSPEND)
```

This entry removes all lower level administrative authorities from AMCDCA.

```
    TSS DEADMIN(AMCDCA) MISC1(ALL)
```

6.10 MISC2

Operating System: VSE, OS/390, VM, and VAX

Description: To give, or to remove, a CA-Top Secret administrator's authority to perform one or more administrative functions.

TSS Commands: The following TSS command can be used with the MISC2 keyword: **ADMIN, DEADMIN only.**

Syntax:

```
TSS ADMIN(acid) MISC2(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify any or all of the following MISC2 authorities:

SMS Authorizes an administrator to ADD, REMOVE, and REPLACE the following SMS fields to an ACID within his scope: **SMSAPPL, SMSDATA, SMSMGMT,** and **SMSSTOR.**

TSO Authorizes an administrator to ADD, REMOVE, and REPLACE the following TSO UADS fields for an ACID within his scope: TSOCOMMAND, TSODEST, TSODEFPRFG, TSOSCLASS, TSOHCLASS, TSOJCLASS, TSOLACCT, TSOLPROC, TSOLSIZE, TSOMCLASS, TSOMSIZE, TSOOPT, TSOUDATA, and TSOUNIT.

NDT Used for NDT (Node Descriptor Table). For more information on VAX resources, please refer to the CA-Top Secret/SECMAN for VAX *Command Reference Guide*.

DLF Gives the ability to ADD and REMOVE data sets from the DLF (Data Lookaside Facility) Record.

PC Authorizes the administrator to ADD, REMOVE or REPLACE the following PC group attributes from an ACID's Security Record: PCADMIN, PCDSDAYS, PCIDLE, PCLGTYPE, PCMINPWD, and PCOPTS.

APPCLU Authorizes the administrator to maintain the APPCLU Record, and PERMIT users to access one of the following APPCLU resources: APPCPORT, APPCSCI and APPCSI.

MISC2(APPCLU) also authorizes the administrator to ADD, REPLACE and REMOVE, the following SYSOUT account and delivery attributes for a user: WAACCNT, WABLDG, WADEPT, WAADDR1, WAADDR2, WAADDR3, WAADDR4, WANAME and WAROOM.

TARGET Give the ability to administer nodes associated with ACIDs.

Types: The MISC2 keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

To authorize an administrator to set SMS data fields for users within his scope, enter:

```
TSS ADMIN(acid) MISC2(SMS)
```

To remove MISC2 authority, enter:

```
TSS DEADMIN(acid) MISC2(ALL)
```

6.11 MISC3

Operating System: VSE, OS/390, and VM

Description: To give, or to remove, a CA-Top Secret administrator's authority to perform one or more additional administrative functions.

TSS Commands: The following TSS command can be used with the MISC3 keyword: **ADMIN, DEADMIN only.**

Syntax:

```
TSS ADMIN(acid) MISC3(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify the following MISC3 authorities:

SDT Authorizes an administrator to maintain and list the SDT (Static Data Table) record.

Types: The MISC3 keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

To authorize an administrator to define record elements to the SDT and PERMIT them to users within his scope, enter:

```
TSS ADMIN(acid) MISC3(SDT)
```

To remove MISC3 authority, enter:

```
TSS DEADMIN(acid) MISC3(SDT)
```

6.12 MISC8

Operating System: VSE, OS/390, and VM

Description: To give, or to remove, a CA-Top Secret administrator's authority to list the contents of the RDT, FDT or STC or to use the ASUSPEND administrative function.

TSS Commands: The following TSS commands can be used with the MISC8 keyword: **ADMIN, DEADMIN only.**

Syntax:

```
TSS ADMIN(acid) MISC8(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify any or all of the following MISC8 authorities:

LISTRDT Authorizes an administrator to list the RDT and FDT Records but **not** to change them. MISC1(RDT) authority is required to maintain the RDT and FDT Records.

LISTSTC Authorizes the administrator to list the contents of the Started Task Table but **not** to change it. MISC9(STC) authority is required to define started tasks to the Started Task Table.

LISTSDT Authorizes the administrator to list the contents of the Static Data Table (SDT) but **not** to change it. MISC3(SDT) authority is required to maintain the SDT records.

MCS Authorizes the administrator to issue the Multiple Console Support (MCS) commands for ACIDs within their scope.

REMASUSP Authorizes the administrator to issue the TSS REMOVE(acid) ASUSPEND command for ACIDs within their scope.

ALL Authorizes the administrator to use all of the authorities.

Types: The MISC8 keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

The following entry gives the administrator the authority to remove an administrative suspension from an ACID within his scope.

```
TSS ADMIN(TECHSCA) MISC8(REMASUSP)
```

The following entry gives TECHVCA the authority to list the RDT Record.

```
TSS ADMIN(TECHVCA) MISC8(LISTRDT)
```

To remove all MISC8 authority, the administrator enters:

```
TSS DEADMIN(acid) MISC8(ALL)
```

6.13 MISC9

Operating System: VSE, OS/390, and VM

Description: To give, or to remove, a TSS administrator's authority to perform one or more high-level administrative functions.

TSS Commands: The following TSS command can be used with the MISC9 keyword: **ADMIN, DEADMIN only.**

Syntax:

```
TSS ADMIN(acid) MISC9(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify any or all of the following MISC9 authorities:

BYPASS Authorizes an administrator to associate the following bypass attributes with ACIDs within his scope: NODSNCHK, NOVOLCHK, NORESCHK, NOLCFCHK, and NOSUBCHK.

TRACE Authorizes the administrator to associate the TRACE attribute with ACIDs within his scope.

CONSOLE Authorizes the administrator to administer the CONSOLE attribute.

MASTFAC Authorizes the administrator to associate a region control ACID with a multiuser address space facility.

MODE Authorizes the administrator to associate any CA-Top Secret owned security mode with an ACID within his scope.

STC Authorizes the MSCA/SCA to define a started task to the CA-Top Secret Started Task Table, and authorizes the administrator to list the contents of the Started Task Table.

GLOBAL Authorizes the administrator to use LCF and administrative authorities for all users via the ALL record.

GENERIC Authorizes the administrator to use the WHOOWNS function to obtain a list of all resources owned within his administrative scope. RESOURCE(INFO) authority only allows an ACID to obtain data on specific resources.

ALL Authorizes the administrator to use all of the authorities.

Types: The MISC9 keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

To authorize an administrator to set security modes for users within his scope, the administrator enters:

```
TSS ADMIN(TECHSCA) MISC9(MODE)
```

CA-Top Secret administrator TECHVCA is authorized to assign the NOSUBCHK attribute to job submission ACIDs via the entry:

```
TSS ADMIN(TECHVCA) MISC9(BYPASS)
```

An administrator in the Software Development Department is given the following authority so that he can define region control ACIDs for CICS:

```
TSS ADMIN(DEVDCA) MISC9(MASTFAC,STC)
```

To remove MISC9 authority, the administrator enters:

```
TSS DEADMIN(acid) MISC9(ALL)
```

6.14 RESOURCE

Operating System: VSE, OS/390, and VM

Description: To give CA-Top Secret administrators the authority, or to remove their authority, to issue CA-Top Secret command functions for all resource types owned within their administrative scope.

TSS Commands: The following TSS command can be used with the RESOURCE keyword: **ADMIN, DEADMIN only.**

Syntax:

```
TSS ADMIN(acid) RESOUrce(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify any or all of the following authority levels:

OWN Gives administrators the authority to use ADDTO and REMOVE functions to assign ownership of resources to ACIDs within their scope.

XAUTH Gives administrators the authority to use PERMIT and REVOKE functions to grant **any** ACID access to resources that are owned within their scope.

The CA-Top Secret administrator may grant any or all of the following access level keywords which may subsequently be used by other CA-Top Secret administrators as part of the PERMIT command function.

DEFAULT If ACCESS is not specified, CA-Top Secret grants the administrator the authority to PERMIT access to resources at the DEFACC access level defined by the RDT.

ALL Resource may be accessed in any manner.

CONTROL VSAM data set that had a control password may be used.

CREATE User may create a data set.

DELETE User may delete a record from a database.

FEOV User may use Force End Of Volume.

FETCH Programs from library can only be executed, not read.

NONE User has no access to the resource.

PURGE User may purge the entire queue of records.

READ Dataset can be read. FETCH is implied.

REPLACE User may replace a record.

SCRATCH User may scratch a data set.

UPDATE User may update a data set. READ is implied.

WRITE User may write to data set.

AUDIT Authorizes an auditor or administrator to globally audit the use of a resource by ADDing it to the Audit Record:

```
TSS ADD(AUDIT) RESOU(prefix(es))
```

This authority level is required when using the TSSAUDIT utility.

REPORT Grants an administrator the authority to use TSSUTIL utility to prepare customized reports showing security activity for resources. It also allows an auditor or administrator to use the TSSTRACK, TSSAUDIT, TSSCPR and TSSCHART utilities.

INFO Authorizes administrators to use WHOOWNS and WHOHAS functions to determine ownership of and permission to a specific resource.

ALL Grants administrators all of the authorities.

Types: The RESOURCE keyword is used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

To authorize an administrator to PERMIT users to update any resource owned within his scope, and to determine who owns and who has access to those resources, the administrator enters:

```
TSS ADMIN(SUPSCA) RESOU(XAUTH,INFO) ACCESS(U)
```

To remove SUPSCA's authority for resources, the administrator enters:

```
TSS DEADMIN(SUPSCA) RESOU(XAUTH,INFO)
```

6.15 resource

Operating System: VSE, OS/390, and VM

Description: To give CA-Top Secret administrators the authority, or to remove their authority, to issue command functions for a specific resource class owned within their administrative scope.

TSS Commands: The following TSS command can be used with resource: **ADDTO, REMOVE, PERMIT, REVOKE, WHOHAS, WHOOWNS, ADMIN, DEADMIN.**

Syntax:

```
TSS ADMIN(acid) resource(authority level(s))
```

Authority Levels: The CA-Top Secret administrator may specify any or all of the following authority levels:

OWN Gives administrators the authority to use ADDTO and REMOVE functions to assign ownership of a specific resource to ACIDs within their scope.

XAUTH Gives administrators the authority to use PERMIT and REVOKE functions to grant ***any*** ACID access to resources that are owned within their scope.

The CA-Top Secret administrator may grant any or all of the following access level keywords which may subsequently be used by other CA-Top Secret administrators as part of the PERMIT command function.

DEFAULT If ACCESS is not specified, CA-Top Secret grants the administrator the authority to PERMIT access to resources at the DEFACC access level defined by the RDT.

ALL Resources may be accessed in any manner.

NONE User has no access to the resource.

Note: Access levels are set by the RDT definition for the resource. For further information about resources and their access levels, refer to the chapter called "Summary of Resources."

AUDIT Authorizes an auditor or administrator to globally audit the use of a resource by ADDing it to the Audit Record:

```
TSS ADD(AUDIT) resource(resource(s))
```

REPORT Grants an administrator the authority to use TSSUTIL utility to prepare customized reports showing security activity for resources. It also allows an auditor or administrator to use the TSSTRACK, TSSCPR, TSSCHART and TSSAUDIT utilities.

INFO Authorizes administrators to use WHOOWNS and WHOHAS functions to determine ownership of and permission to a specific resource.

ALL Grants administrators all of the authorities.

Types: A resource can be used with the following ACID types: **User, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

Using the TERMINAL resource class, a system network administrator can be set up to define and authorize protected terminals:

```
TSS ADMIN(NETMNGR) TERM(ALL)
```

To remove this administrative capability, the administrator enters:

```
TSS DEADMIN(NETMNGR) TERM(ALL)
```

6.16 SCOPE

Operating System: VSE, OS/390, and VM

Description: To give CA-Top Secret administrators the authority, or to remove their authority, to assign the SCOPE of an LSCA.

TSS Commands: The following TSS command can be used with the SCOPE keyword: **ADMIN, DEADMIN.**

Syntax:

```
TSS ADMIN(lsca) SCOPE(lsca(s),zone(s))
```

Authority Levels: Only the MSCA may assign an LSCA's SCOPE.

Examples:

This entry would give LSCA01 administrative authority over LSCA02 and ZONE1.

```
TSS ADMIN(LSCA01) SCOPE(LSCA02,ZONE1)
```

To remove an ACID or ACIDs from the LSCA's scope, use the DEADMIN command function and specify each ACID that is being removed. For example, the following entry removes all lower level administrative authorities from LSCA01.

```
TSS DEADMIN(LSCA01) SCOPE(LSCA02,ZONE1)
```

Chapter 7. How to Use CREATE

This chapter presents the standard formats and rules governing the use of the CREATE function.

7.1 Purpose

Given the proper administrative authority, the CA-Top Secret administrator uses the TSS CREATE command function to define new ACIDs to CA-Top Secret. The CA-Top Secret administrator can also assign resource ownership and/or security attributes while creating the ACID.

7.2 Entry Methods

CA-Top Secret administrators may enter TSS CREATE command functions free-form onto an entry screen, or as input to the batch utilities TSSCMNDB.

7.2.1 Entry Screen Syntax

The entry for the CREATE function varies depending on the type of ACID being created, and the authority of the administrator performing the CREATE. The following list shows the command syntax used to CREATE each ACID type. Refer to the TYPE keyword for details about each of the ACID types.

SCA

TSS CREATE(acid) NAME('user name') TYPE(SCA)
PASSWORD(password[,0...255][,EXP])

LSCA

TSS CREATE(acid) NAME('user name') TYPE(LSCA)
PASSWORD(password[,0...255][,EXP])

ZONE

TSS CREATE(acid) NAME('zone name') TYPE(ZONE)

ZCA

TSS CREATE(acid) NAME('user name') TYPE(ZCA)
PASSWORD(password[,0...255][,EXP]) ZONE(acid)

DIV

TSS CREATE(acid) NAME('division name') TYPE(DIVISION)

VCA

TSS CREATE(acid) NAME('user name') TYPE(VCA)
PASSWORD(password[,0...255][,EXP]) DIVISION(acid)

DEPT

TSS CREATE(acid) NAME('department name') TYPE(DEPARTMENT)
[DIVISION(acid)]

DCA

TSS CREATE(acid) NAME('user name') TYPE(DCA)
PASSWORD(password[,0...255][,EXP]) DEPARTMENT(acid)

PROFILE

TSS CREATE(acid) NAME('group name') DEPT(acid)
TYPE(PROFILE)

GROUP

TSS CREATE(acid) NAME('group name') DEPT(acid)
TYPE(GROUP)

USER

TSS CREATE(acid) NAME('user name') TYPE(USER)
PASSWORD(password[,0...255][,EXP]) DEPARTMENT(acid)

7.2.2 Identification Keywords

The NAME must be entered as part of all CREATE functions since this keyword specifies the name of the user, job, administrator, profile, department, or division, that the ACID represents.

Depending on the type of ACID being created, the TYPE keyword as well as the DEPARTMENT and/or DIVISION keywords are also specified.

7.3 General Rules

The following general rules and procedures apply to all CREATE entries. Specific rules are documented with the applicable keyword.

7.3.1 Authority

1. The administrator must have ACID(CREATE) authority, via the TSS ADMIN function, to CREATE ACIDs under their administrative scope.
2. The administrator must have RESOURCE(OWN) authority, via the TSS ADMIN function, to assign resource ownership to ACIDs within their scope.
3. MISC1, MISC2 and MISC9 authorities are required, via the TSS ADMIN function, to assign many of the security attributes.

7.3.2 Use of DEPARTMENT, DIVISION and ZONE

SCA SCAs must enter the ZONE, DIVISION or DEPARTMENT keyword with all TSS CREATE entries which require these keywords.

LSCA LSCAs must enter the ZONE or DIVISION keyword with all TSS CREATE entries which require these keywords.

ZCA ZCAs cannot enter the ZONE keyword in their CREATE entries. CA-Top Secret automatically assigns the ACID to the ZCA's zone. The ZONE keyword *is* required if the person entering the command function is an SCA.

VCA VCAs cannot enter the DIVISION keyword in their CREATE entries. CA-Top Secret automatically assigns the ACID to the VCA's division. The DIVISION keyword *is* required if the person entering the command function is an SCA.

DCA DCAs cannot enter the DEPARTMENT keyword in their CREATE entries. CA-Top Secret automatically assigns the ACID to their department. The DEPARTMENT keyword *is* required if the person entering the command function is not a DCA.

7.4 Applicable Keyword List

The CA-Top Secret administrator may incorporate the following keywords, within the CREATE function, to assign resources and attributes to the ACID(s) they are creating. Most of these keywords are documented in Chapter 5 (ADDTO/REMOVE) and Chapter 22 (Summary of Resources) of this guide, and therefore are not repeated in this chapter.

ABSTRACT	IESTYPE	PHYSKEY	TSOCLASS	WRITER
APPLICATION	IESVCAT	PPT	TSOUDATA	XCOMMAND
AREA	INSTDATA	PROCNAME	TSOUNIT	XTRANSACTIONS
ASUSPEND	IUCV	PROFILE	TST	ZONE
AUDIT	JCT	PROGRAM	TYPE	
COMMAND	JESJOBS	PROPCNTL	TZONE	
CONSOLE	JESPOOL	PSB	UNDERCUT	
CPCMD	LANGUAGE	PSFMPL	UNTIL	
CACMD	LTIME	SCTYKEY	UR1/UR2	
CPU	MASTFAC	SDSF	USER	
DATABASE	MGMTCLAS	SITRAN	USERCLASS	
DBD	MODE	SMESSAGE	USERNL1	
DB2	MRO	SMSAPPL	USERNL2	
DB2BUFFP	MULTIPW	SMSDATA	USING	
DB2COL	NAME	SMSMGMT	VMCF	
DB2DBASE	NOADSP	SMSSTOR	VMDIAL	
DB2PKG	NOATS	SOURCE	VMMACH	
DB2PLAN	NODES	SPI	VMDISK	
DB2STOGP	NODSNCHK	STCACT	VMNODE	
DB2SYS	NOLCFCHK	STORCLAS	VMRDR	
DB2TABLE	NOPERMIT	SUBSCHEM	VOLUME	
DB2TABSP	NOPWCHG	SUSPEND	VSECATBT	
DCSS	NORESCHK	TARGET	VSEKIB	
DCT	NOSUBCHK	TERMINAL	VSEMCON	
DEVICES	NOSUSPEND	TRACE	VSEMEMBER	
DIAGNOSE	NOVMDCHK	TRANSACTIONS	VSEPART	
DIVISION	NOVOLCHK	TSOACCT	VSERDD	
DLISEG	OIDCARD	TSOAUTH	VSESLIB	
DSNAME	OPCLASS	TSOCOMMANDS	VSESYSAD	
DUFUPD	OPCMD	TSODEFPRFG	VSEUSER	
DUFXTR	OPERCMDS	TSODEST	VTAMAPPL	
FACILITY	OPIDENT	TSOHCLASS	VXDEVICE	
FCT	OPPRTY	TSOJCLASS	VXFILE	
FIELD	OTRAN	TSOLACCT	WAACCNT	
FOR	PANEL	TSOLPROC	WABLDG	
GAP	PASSWORD	TSOLSIZE	WAADDR1	
GROUP	PCADMIN	TSOMCLASS	WAADDR2	
IBMFAC	PCDSDAYS	TSOMPW	WAADDR3	
IBMGROUP	PCIDLE	TSOMSIZE	WAADDR4	
IESFL1	PCLGTYPE	TSOOPT	WADEBP	
IESFL2	PCMINPWD	TSOPRFG	WAIT	
IESINIT	PCOPTS	TSOPROC	WANAME	
IESSYNM			WAROOM	

7.5 DEPARTMENT

Operating System: VSE, OS/390, and VM

Description: To assign a new ACID to a department.

TSS Commands: The following TSS commands can be used with the DEPARTMENT keyword: **LIST, MOVE, CREATE**

Syntax:

```
TSS CREATE(user|profile|DCA acid) NAME('name')
    FACILITY(fac name) PASSWORD(password) DEPT(acid)
```

Use By DCAs: Since a DCA can only create ACIDs in his own department, TSS automatically assigns the new ACID to the DCA's department. CA-Top Secret will not accept the DEPARTMENT keyword when entered by a DCA, even if the DCA specifies his own department ACID. The DEPARTMENT keyword is only required when the person entering the command is not a DCA.

Types: The DEPARTMENT keyword is used with the following ACID types: **User, Profile, DCA.**

Examples:

To create a new CICS user for the TECH Department, the DCA enters:

```
TSS CREATE(TECH10) NAME('TECH USER') FAC(CICS) PAS(XXXX,15,EXP)
    TYPE(USER)
```

In this example, when TECH10 signs on using XXXX as his password, he will automatically be prompted for a new password which will expire in 15 days, and every 15 days thereafter.

The same entry from a TSS administrator, other than the DCA, would be entered as:

```
TSS CREATE(TECH10) NAME('TECH USER')
    FAC(CICS) PAS(XXXX,15,EXP)
    DEPT(TECHDEP) TYPE(USER)
```

7.6 DIVISION

Operating System: VSE, OS/390, and VM

Description: To assign an ACID to a division.

TSS Commands: The following TSS commands can be used with the DIVISION keyword: **LIST, MOVE, CREATE.**

Syntax:

```
TSS CREATE(dept acid|VCA acid) TYPE(DEPT|VCA)
    NAME('VCA or Department name') DIVision(acid)
```

Use By VCAs: Since a VCA may only create ACIDs for his own division, TSS automatically assigns the new ACID to the VCA's division. CA-Top Secret will not accept the DIVISION keyword when entered by a VCA, even if the VCA specifies his own divisional ACID. The DIVISION keyword is only required when the person entering the command is an SCA.

Types: The DIVISION keyword is used with the following ACID types: **LSCA, ZCA, VCA, Zone, Department.**

Examples:

To create a new Accounting Department to be placed in the Parts Division, the CA-Top Secret administrator enters:

```
TSS CREATE(ACCT01) NAME('ACCT DEPT')
    TYPE(DEPT) DIV(PARTDIV)
```

7.7 NAME

Operating System: VSE, OS/390, and VM

Description: To associate the ACID with a name for further identification.

TSS Commands: The following TSS command can be used with the NAME keyword: **REPLACE, CREATE.**

Syntax:

```
TSS CREATE(acid) NAME('1 to 32 character name') ...
```

The NAME keyword may contain from 1 to 32 characters.

The entire name must be delimited by single quotes if it contains blanks or special characters.

If the name contains an apostrophe (i.e., a single quote character), use two single quotes within the name; for example: NAME('Patrick O''Neil').

Usage: The NAME field is provided for reporting and documentation purposes. CA-Top Secret displays the NAME field as part of message TSS7000I when a user signs on to a facility. NAME is also displayed in the TSSUTIL report for initiation or signon records.

Types: The NAME keyword may be used to identify any of the following ACIDs: **User, Profile, DEPT, DIV, ZONE, DCA, VCA, ZCA, LSCA, SCA.**

Examples:

To assign a name to a division's ACID, the administrator enters:

```
TSS CREATE(SHIPDIV) NAME('SHIPPING DIVISION')...
```

7.8 TYPE

Operating System: VSE, OS/390, and VM

Description: To specify what type of ACID is being created.

TSS Commands: The following TSS command can be used with the TYPE keyword: **LIST, MOVE, CREATE.**

Syntax:

```
TSS CREATE(acid name)
    TYPE(USER|PROFILE|GROUP|DEPT|DIV|ZONE|DCA|
    VCA|ZCA|LSCA|SCA) NAME('name') ...
```

Types: The TYPE keyword may be used to identify any of the following ACIDs: **User, Profile, Group, DEPT, DIV, ZONE, DCA, VCA, ZCA, LSCA, SCA.**

Default: If the administrator fails to enter the TYPE keyword, CA-Top Secret will automatically default to TYPE(USER).

Examples:

To create a new department to be placed in the PARTS Division, the CA-Top Secret administrator enters:

```
TSS CREATE(PART10) NAME('PARTS RETURN')
    TYPE(DEPT) DIV(PARTSDIV)
```

7.9 USING

Operating System: VSE, OS/390, and VM

Description: To create an ACID of the same type using an existing ACID as a model.

TSS Commands: The following TSS commands can be used with the USING keyword: **CREATE.**

Syntax:

```
TSS CREATE(acid) USIng(modelacid)
```

Authority: All rules of scope and administrative authority are supported. If the model ACID is outside the scope of the administrator and/or the model ACID has any information field which requires an ADMIN authority that the administrator does not have, the CREATE function will fail.

Usage: The "model acid" information that is available from a TSS LIST(modelacid) DATA(BASIC,TSO) will be copied to the ACID in the CREATE USING command along with the TSO DFLT, SMS, CICS and WORKATTR DATA information. Any existing ACID can be used as the model, but the model must exist **before** attempting to create copies from it.

Note: In addition to the information from TSS LIST DATA(BASIC), the TSO DFLT DATA information will be copied.

Types: The USING keyword may be used with the following ACID types: **User, Profile, DEPT, ZONE, DCA, VCA, ZCA, LSCA, SCA, MSCA**

Examples:

To create a new ACID (USER02) which is modeled after an existing ACID (USER01) including USER01's name and password, enter:

```
TSS CREATE(USER02) USING(USER01)
```

Administrators usually CREATE new ACIDs with their own unique name and password values to override those in the model. Such as,

```
TSS CREATE(USER02) USING(USER01)
    NAME('JOHN SMITH') PAS(SMIJO01,7,EXP)
```

This will give USER02 a name of John Smith with an initially expired password of SMIJO01 that will expire every 7 days.

To omit an information field from the new ACID, enter the keyword with no value specified in the parentheses. In this example, we wish to omit the INSTDATA keyword from USER02, enter:

```
TSS CREATE(USER02) USING(USER01) INSTDATA()
```

All ACID attributes in USER01 which are not desired in USER02 must be explicitly REMOVEd from USER02 after the CREATE. ACID attributes (i.e., SUSPEND, NORESCHK) have no values to nullify with () string values and therefore cannot be nullified within the CREATE syntax. Information that is not copied by CREATE USING (such as PERMITs) must be explicitly granted to the new ACID after the CREATE.

7.10 ZONE

Operating System: VSE, OS/390, and VM

Description: To assign an ACID to a zone.

TSS Commands: The following TSS commands can be used with the ZONE keyword: **LIST, MOVE, CREATE.**

Syntax:

```
TSS CREATE(div. acid|ZCA acid) TYPE(DIV|ZCA)
    NAME('ZCA or Division name') ZONe(acid)
```

Use By ZCAs: Since a ZCA may only create ACIDs for his own zone, TSS automatically assigns the new ACID to the ZCA's zone. CA-Top Secret will not accept the ZONE keyword when entered by a ZCA, even if the ZCA specifies his own zonal ACID. The ZONE keyword is only required when the person entering the command is an SCA.

Types: The ZONE keyword is used with the following ACID types: **Division, ZCA**

Examples:

To create a new Accounting Division to be placed in the Parts Zone, the CA-Top Secret administrator enters:

```
TSS CREATE(ACCT01) NAME('ACCT DIV')
    TYPE(DIV) ZON(PARTZON)
```

Note: To add a new department to a zone you must add that department to a division. Departments *cannot be directly added* to a zone.

Chapter 8. How to Use DELETE

This chapter presents the standard formats and rules governing the use of the DELETE function. There are no detailed reference pages for the DELETE chapter.

8.1 Purpose

Given the proper administrative authority, the administrator may enter the TSS DELETE command function to remove an ACID's definition from the Security Record.

8.2 Entry Methods

Administrators may enter the TSS DELETE command function freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

8.2.1 Entry Screen Syntax

The basic entry for the DELETE command function is:

```
TSS DELETE(acid)
```

where **acid** is the ACID being deleted.

8.2.1.1 Sample Entry

To remove the TSS definition for ACID CLRK99, the administrator enters:

```
TSS DELETE(CLRK99)
```

8.3 General Rules and Procedures

The following rules and procedures apply to the entry of all DELETE command functions.

8.3.1 Authority/Scope

CA-Top Secret administrators must have ACID(CREATE|ALL) authority, via the ADMIN function, to DELETE ACIDs within their scope.

8.3.2 Processing of DELETE

CA-Top Secret actually performs the following three functions when an ACID is deleted:

1. Disconnects the deleted ACID from all profiles to which it is connected.
2. REVOKEs any access permissions that the ACID was granted.
3. REMOVEs any resources that the ACID owns.

8.3.2.1 Failure of a DELETE Function

Organizational ACIDs:

CA-Top Secret will not allow the deletion of an ACID which has other ACIDs connected to it. Therefore, division, department, and/or profile ACIDs cannot be deleted if other ACIDs are connected to them.

To DELETE a department or division ACID, the CA-Top Secret administrator must use the TSS MOVE function to transfer all ACIDs out of the department or division being deleted. Refer to the TSS MOVE chapter for details.

To DELETE a profile ACID, the CA-Top Secret administrator must use the TSS REMOVE function to remove the profile from any connected user ACIDs. Refer to the "How to Use ADDTO/REMOVE" chapter for details.

Acids That Own Resources:

The DELETE function will also fail if the ACID being deleted owns resources that are PERMITted to other ACIDs.

Special ACIDs:

CA-Top Secret will not allow the deletion of special ACIDs such as ALL, STC, AUDIT, DLF, RDT, or the MSCA's ACID.

Chapter 9. How to Use HELP

This chapter presents the standard formats and rules which govern the use of the HELP function. There are no detailed reference pages for the HELP chapter.

9.1 Purpose

The HELP function provides basic information about the use of each TSS command function.

9.2 Entry Methods

Administrators may obtain HELP when entering command functions onto an entry screen, or as input to the batch utility TSSCMNDB.

9.2.1 Entry Screen Syntax

Enter the following to obtain HELP while entering command functions on the screen:

```
TSS HELP OPERAND(function)
```

Note: The HELP command cannot be routed through the security network using the Command Propagation Facility (CPF).

The **function** must equal one of the following CA-Top Secret command functions:

```
ADDTO      LIST       REMOVE     WHOOWNS
ADMIN      LOCK       RENAME     WHOHAS
CREATE     MODIFY     REPLACE    WHOAMI
DEADMIN    MOVE       REVOKE
DELETE     PERMIT     UNLOCK
WHOOWNS
WHOHAS
WHOAMI
```

When the HELP command function is entered onto the screen, CA-Top Secret responds with a list of all keywords that may be used with the command function entered in the command.

9.2.2 Sample Entry

To obtain information concerning the ADMIN function, the administrator enters:

```
TSS HELP OPERAND(ADMIN)
```

CA-Top Secret will respond with the following display:

TSS HELP Response

```
TSS HELP OPERAND(ADMIN)


ABSTRACT,ACID,APPLICATION,AREA,CACMD,CPCMD,CIMS,CPU,DATA,
DBD,DB2,DB2BUFFP,DB2COLL,DB2DBASE,DB2PKG,DB2PLAN,DB2STOGP,DB2SYS,
DB2TABLE,DB2TABSP,DCSS,DCT,DEVICES,DIAGNOSE,DSNAME,FACILITY,FCT,
FIELD,IBMFAC,IBMGROUP,JCT,JESJOBS,JESSPOOL,MGMTCLAS,MISC1,MISC2,MISC9,
OPCMD,OPERCMDS,OTRAN,PANEL,PPT,PROGRAM,PROPCNTL,PSB,PSFMPL,RESOURCE,
SDSF,SMESSAGE,STORCLAS,SUBSCHEM,TERMINAL,TSOACCT,TSOAUTH,TSOPROC,
TSOPRFG,TST,UR1,UR2,VMDIAL,VMMACH,VMMDISK,VMNODE,VMRDR,VOLUME,VTAMAPPL,
VXDEVICE,VXFILE, WRITER

TSS0300I  HELP        FUNCTION SUCCESSFUL
```

Chapter 10. How to Use LIST

This chapter presents the standard formats and rules which govern the use of the LIST function.

10.1 Purpose

Given the proper administrative authority, the CA-Top Secret administrator may enter the LIST command function for CA-Top Secret to display data from the:

- Security Record of a specific ACID.
- Security Record of all ACIDs that match a specific prefix.
- Security Record of all ACIDs of a specific type.
- Security Record of all ACIDs in a department, and/or division.
- AUDIT, STC, NDT, RDT, FDT, DLF, APPCLU and/or ALL Records.

10.2 Entry Methods

Administrators may enter TSS LIST command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

10.2.1 Entry Screen Syntax

TSS LIST entries vary depending on the type of data being requested and from which Security Record the data is obtained. The basic commands for each type of data request are as follows:

To obtain all the data about a specific ACID and contents of all profiles connected to that ACID, the administrator enters:

```
TSS LIST(acid) DATA(PROFILE,ALL)
```

To obtain all the data about the ACIDs starting with a specific prefix and the contents of all profiles connected to those ACIDs, the administrator enters:

```
TSS LIST(acid) ACIDPRFX(acid-prefix) DATA(PROFILE,ALL)
```

Note: Prefixes can be from one to eight characters long.

To obtain data about all ACIDs of a specific type, the administrator enters:

```
TSS LIST(ACIDS) TYPE(USER | PROFILE | GROUP | DCA | VCA | DEPT |
    DIV | SCA | LSCA | ZONE | ZCA)
    DATA(BASIC,RESOURCE,XAUTH,LCF,SOURCE,INSTDATA,CICS,ADMIN,NAMES,
    TSO,ACIDS,EXPIRE,PASSWORD|ALL[,PROFILE,PASSWORD,EXPIRE])
```

To obtain data about all ACIDs in a department, the administrator enters:

```
TSS LIST(ACIDS) DEPT(dept. acid) DATA(BASIC,RESOURCE,XAUTH,LCF,SOURCE,TSO,
  INSTDATA,CICS,ADMIN,NAMES,ACIDS,PASSWORD|ALL [,EXPIRE,PASSWORD,PROFILE])
```

To obtain data about all ACIDs in a division, the administrator enters:

```
TSS LIST(ACIDS) DIV(div. acid) DATA(BASIC,RESOURCE,XAUTH,LCF,SOURCE,TSO,
  INSTDATA,CICS,ADMIN,NAMES,ACIDS,PASSWORD|ALL [,EXPIRE,PASSWORD,PROFILE])
```

To obtain data about all ACIDs in a zone, the administrator enters:

```
TSS LIST(ACIDS) ZON(zon. acid) DATA(BASIC,RESOURCE,XAUTH,LCF,SOURCE,TSO,
    INSTDATA,CICS,ADMIN,NAMES,ACIDS,PASSWORD|ALL [,EXPIRE,PASSWORD,PROFILE])
```

To obtain data about the contents of the DLF record, the administrator enters:

```
TSS LIST(DLF)
```

To obtain data about the contents of the ALL record, the administrator enters:

```
TSS LIST(ALL)
```

To obtain data about the contents of the AUDIT record, the administrator enters:

```
TSS LIST(AUDIT)
```

To obtain data about the contents of the STC record, the administrator enters:

```
TSS LIST(STC)
```

To obtain data about the contents of the RDT record, the administrator enters:

```
TSS LIST(RDT)
```

To obtain data about the contents of the FDT record, the administrator enters:

```
TSS LIST(FDT)
```

To obtain data about the contents of the NDT record, the administrator enters:

```
TSS LIST(NDT)
```

To obtain data about the contents of the APPCLU record, the administrator enters:

```
TSS LIST(APPCLU)
```

10.2.2 Sample Entry

To LIST CICS definitions for all profiles in the Payroll Department, the administrator enters:

```
TSS LIST(ACIDS) DATA(CICS) DEPT(PAYROLL) TYPE(PROFILE)
```

10.3 General Rules and Procedures

The following rules and procedures apply to the entry of all LIST functions. Specific rules are documented with the applicable CA-Top Secret keyword.

10.3.1 Authority

CA-Top Secret administrators must have been granted explicit authority via the ADMIN - DATA function to LIST TSS data types.

10.3.2 Scope

CA-Top Secret will only display data concerning ACIDs within the administrator's scope. Thus, an MSCA or an authorized SCA could obtain LIST data for the entire site. A VCA may list data for his division and all subordinate departments, and a DCA may list data for his department.

10.3.3 Hard Copy Listings

Hard copy listings are obtained by using the batch utlity TSSCMNDB in VSE, batch TMP of TSSCFILE in OS/390, and the batch utility TSSCRIPT in VM.

10.3.4 Order of Display

ACIDs are listed first by division, then by the department within the division. User and profile ACIDs are listed in alphabetical order within an organizational grouping.

10.3.5 ACID Types

Use the following list to translate the ACID types that appear on the output of a TSS LIST command.

Code	ACID Type
DC	DCA
D	Department
V	Division
LC	LSCA
P	Profile
SC	SCA
ZC	ZCA
VC	VCA
Z	Zone

10.3.6 SORTing for Profiles

When a TSS LIST(acid) DATA(PROFILES) command is issued, the profiles associated with that ACID will be listed alphabetically. If you want to view the profiles in the order in which they will be processed, you need to specify DATA(PROFILES,NOSORT). An example is shown next.

```
TSS LIST(USER01) DATA(PROFILES,NOSORT)
```

This example produces a list of the profile ACIDs associated with USER01. Those ACIDs will be listed in the order in which they will be searched by the Security Algorithm.

10.3.7 LISTing for Acids

When a TSS LIST(acid) DATA(BASIC) command is issued, the output associated with that ACID will be sorted alphabetically (i.e., LOCK TIME will come before TIME ZONE).

When a TSS LIST(acid) SEGMENT(ALL) command is issued, the segments, and the fields within the segments, will be sorted alphabetically.

Groupings are identified by the segment which they are in, not a header line. For example, groupings that were separated by a header line such as **TSO DATA** and **PC DATA** are now identified as **SEGMENT TSO** and **SEGMENT CA-PC**.

10.4 Applicable Keyword List

The following keywords may be used with the TSS LIST command function. Refer to the detailed reference pages that follow for descriptions, examples, and definitions of each keyword.

```
DATA
DEPARTMENT
DISPLAY
DIVISION
FDTNAME
FDTCODE
LINKID
PSTKAPPL
RESCLASS
RESCODE
SEGMENT
SESSKEY
TARGET
TYPE
UID
WAIT
ZONE
```

10.5 DATA

Operating System: VSE, OS/390, and VM

Description: To specify which portion of a Security Record will be listed.

TSS Commands: The following TSS commands can be used with the DATA keyword: **ADMIN, DEADMIN, LIST, WHOHAS.**

When used with the TSS WHOHAS function, the DATA keyword can only be used with the MASK, LITERAL and NOPREFIX operands. Conversely, these operands cannot be used when the DATA keyword is issued on a function other than WHOHAS. For more information on using the DATA keyword on a TSS WHOHAS command, refer to Chapter 18, "How to Use WHOHAS" on page 18-1.

Syntax:

```
TSS LIST (acid|ACID) DATA(datatype(s))
    TYPE(USER|PROFILE|DEPT|DIV|ZONE|SCA|LSCA|ZCA|VCA|DCA)
```

Data Types: The CA-Top Secret administrator may request any or all of the following DATA types. If a DATA type is not selected, CA-Top Secret defaults to BASIC.

Type	Causes CA-Top Secret to Display
BASIC	The ACID, the name associated with the ACID, the ACID's type, facilities that the ACID is allowed to access, profiles with which the ACID is associated, groups with which the ACID is associate including the default group, special attributes attached to the ACID, the date that the ACID was created/modified and last used, and the language preference and TZONES, if used. **Note:** The AUDIT attribute is only displayed if the user performing the TSS LIST has the ACID(AUDIT) administrative attribute.
RESOURCE	A list of resources owned by an ACID within its scope. **Note:** The RESCLASS keyword may be used with RESOURCE to list the resources that are owned by the acid.
XAUTH	A list of resources that may be accessed by the ACID shown in the command, the level at which the ACID may access the resource, and the owner of the resource. **Note:** The RESCLASS keyword may be used with XAUTH to list the resources to which the acid is permitted.
LCF	The commands and transactions that an ACID is confined to (via TRANS/CMD) or restricted from (via XTRANS/XCMD).
SOURCE	Devices from which an ACID must initiate.

INSTDATA The installation data for an ACID.

CICS A list of values for CICS operator fields: OPCLASS, OPIDENT, OPPRTY, SCTYKEY.

PROFILES Contents of all profiles connected to the ACID in the LIST function. The content of the display will be based on the other DATA suboptions entered in the LIST command. For example,

```
TSS LIST(PSGEDJ) DATA(BASIC,PROFILE)
```

will produce a list of BASIC data for PSGEDJ, and BASIC data for each profile connected to PSGEDJ. While,

```
TSS LIST(PSGEDJ) DATA(NAMES,PROFILE)
```

will product a list of the PSGEDJ ACID, and the name connected to that ACID. This will be followed by the ACID and name of all profiles connected to PSGEDJ.

Unless you specify DATA(PROFILES,NOSORT), the profiles will be listed alphabetically rather than by order of processing.

ADMIN An ACID's administrative authority.

When TSS LIST displays the MISC1-MISC9 authorities, the designation MISCx(*ALL*) is used to indicate that all of the available authorities in the current release have been assigned to this ACID. If one or more of the authorities available has not been assigned, a listing of the assigned authorities is provided. For example,

```
MISC8(LISTRDT,LISTSTC,LISTSDT)
```

shows that three of the five MISC8 authorities in Release 3.0 have been assigned.

NAMES An ACID name, and the associated owner's name.

ACIDS All ACIDs connected to the ACID entered in the LIST function. This keyword applies to lists of division, department and profile ACIDs.

TSO List TSO "UADS" data fields for an ACID.

PASSWORD The ACID's password *expiration date and interval.* The password itself is also displayed only if the administrator has PWVIEW authority via the TSS ADMIN DATA command function, ***and*** the PWVIEW control option is set to YES.

EXPIRE A list of all profile ACIDs and applicable expiration dates.

If the EXPIRE keyword is omitted, attached profiles containing expiration dates will be indicated by an asterisk(*).

SESSKEY The session keys associated with designated LINKIDs in the APPCLU Record **or** PassTicket applications in the NDT Record. To view session keys, the administrator must have DATA(SESSKEY) authority and either MISC2(APPCLU) or MISC1(NDT) authority depending on the keys designated.

WORKATTR The SYSOUT delivery and account information specified by the following attributes: WAACCNT, WABLDG, WAADDR1-4, WADEPT, WANAME, and WAROOM.

PCDATA The PC attributes associated with an ACID. These include: PCADMIN, PCDSDAYS, PCIDLE, PCLGTYPE, PCMINPWD, and PCOPTS.

ALL All data types except PASSWORD, PROFILE, and expiration of temporary profiles.

Authority: CA-Top Secret administrators must have been granted explicit authority, via the ADMIN DATA function, to LIST any or all of the TSS data types.

Types: The DATA keyword is used with the following ACID types: **User, Profile, DEPT, DIV, ZONE, DCA, VCA, ZCA, LSCA, SCA, MSCA, ACIDS**

Examples

To list all data concerning a specific ACID, the administrator enters:

```
TSS LIST(CATSTC1) DATA(ALL)
```

This entry provides the administrator with all LIST data about the ACID or ACIDS, **except** password information, expiration dates of temporary profiles, associated SESSKEYs and will not list in detail any connected profiles.

```
TSS LIST(acid | ACIDS) DATA(ALL)
```

To obtain all LIST data including the password information (i.e., password, expiration date, interval), expiration dates of any connected profiles, as well as a detailed list of each connected profile, the administrator enters:

```
TSS LIST(acid|ACIDS) DATA(ALL,PASSWORD,PROFILE,EXPIRE)
```

10.6 DEPARTMENT

Operating System VSE, OS/390, and VM

Description: To allow CA-Top Secret administrators to list data about ACIDs in a specific department.

TSS Commands: The following TSS commands can be used with the DEPARTMENT keyword: **CREATE, MOVE, LIST.**

Syntax:

```
TSS LISt(acid|ACIDS DATA(datatype(s)) TYPE(USER|PROFILE|DCA)
    DEPartment(acid)
```

Authority: CA-Top Secret will only display data concerning ACIDs within the administrator's scope. Thus, an MSCA or an authorized SCA could obtain LIST data for the entire site. A VCA may list data for his division and all subordinate departments. A DCA may not specify the DEPARTMENT keyword.

Types: The DEPARTMENT keyword is used with the following ACID types: **User, Profile, DCA.**

Examples

To list the names of all users in the TECH Department, the administrator enters:

```
TSS LIST(ACIDS) DATA(NAMES) DEPARTMENT(TECH)
```

10.7 DISPLAY

Operating System: VSE, OS/390, and VM

Description: To allow TSS administrators to identify the field name associated with a given display value.

TSS Commands: The following TSS commands can be used with the DISPLAY keyword: **ADDTO, REPLACE, LIST.**

Syntax:

```
TSS LIST(FDT) DISplay('display value')
```

Authority: CA-Top Secret administrators must have MISC1(RDT) authority, via the ADMIN function, to LIST data from the FDT Record.

Types: The DISPLAY keyword is used with the following ACID type: **FDT.**

Examples

To find the field name associated with the LOCKTIME= value shown when LISTing an ACID, the administrator enters:

```
TSS LIST(FDT) DISPLAY('LOCK TIME')
```

it will identify LTIME as the associated field.

10.8 DIVISION

Operating System: VSE, OS/390, and VM

Definition: To allow CA-Top Secret administrators to list data about ACIDs in a specific division.

TSS Commands: The following TSS commands can be used with the DIVISION keyword: **CREATE, MOVE, LIST.**

Syntax:

```
TSS LIST(acid|ACIDS) DATA(data type(s)) TYPE(acidtype)
    DIVision(acid)
```

Authority: CA-Top Secret will only display data concerning ACIDs within the administrator's scope. Thus, an MSCA or an authorized SCA could obtain LIST data for the entire site. A VCA cannot specify the DIVISION keyword.

Types: The DIVISION keyword is used with the following ACID types: **Division, Zone, VCA, ZCA, LSCA, ACIDS.**

Examples

To list the names of all users in the TECH Division, the administrator enters:

```
TSS LIST(ACIDS) DATA(NAMES) DIV(TECH)
```

10.9 FDTNAME

Operating System: VSE, OS/390, and VM

Description: Allows the TSS administrator to list data from the FDT Record (i.e., fieldcode, access level, and attributes) concerning how the specified field(s) is processed.

TSS Commands: The following TSS commands can be used with the FDTNAME keyword: **ADDTO, REMOVE, LIST.**

Syntax:

```
TSS LIST(FDT)
FDTName(field name)
```

Capacity of list - 1 resource class per TSS command

Authority: Administrators must have MISC1(RDT) or MISC8(LISTRDT) authority, via the ADMIN function, to list data from the FDT Record.

Types: The FDTNAME keyword is used with the following ACID types: **FDT.**

Examples

To list data concerning the contents of the $ACCT field, the administrator enters:

```
TSS LIST(FDT) FDTNAME($ACCT)
```

10.10 FDTCODE

Operating System: VSE, OS/390, and VM

Description: Allows the TSS administrator to list data from the FDT Record (field name, access level, and attributes) concerning how a specified field code(s) is processed.

TSS Command: The following TSS commands can be used with the FDTCODE keyword: **ADDTO, LIST.**

Syntax:

```
TSS LIST(FDT) FDTCode(code)
```

Capacity of list - 1 field code per TSS command

Authority: Administrators must have MISC1(RDT) or MISC8(LISTRDT) authority, via the ADMIN function, to list data from the FDT Record.

Types: The FDTCODE keyword is used with the following ACID types: **FDT.**

Examples

To list data concerning how field code 3F will be processed, the administrator enters:

```
TSS LIST(FDT) FDTCODE(3F)
```

10.11 SEGMENT

Operating System: VSE, OS/390, and VM

Description: To allow TSS administrators to list data about fields in a specific segment.

TSS Commands: The following TSS commands can be used with the SEGMENT keyword: **ADDTO, REPLACE, LIST.**

Syntax:

```
TSS LIST(acid) SEGMENT(ALL|segmentname)
```

Authority: CA-Top Secret administrators must have MISC1(RDT) authority, via the ADMIN function, to LIST data from the FDT Record.

Types: The SEGMENT keyword is used with the following ACID type: **ACID, FDT, USER.**

Examples

To list the names of all fields in the TAXINFO Segement, the administrator enters:

```
TSS LIST(ACIDS) SEGMENT(TAXINFO)
```

10.12 TYPE

Operating System: VSE, OS/390, and VM

Description: Allows the CA-Top Secret administrator to specify the type of ACID for which he is requesting data.

TSS Commands: The following TSS command can be used with the TYPE keyword: **CREATE, MOVE**

Syntax:

```
TSS LIST(ACIDS) DATA(data type(s))
    TYPE(USER|PROFILE|GROUP|DCA|VCA|SCA|ZCA|LSCA|DEPT|DIV|ZONE)
```

Authority: CA-Top Secret will only display data concerning ACIDs within the administrator's scope. Thus, an MSCA or an authorized SCA could obtain LIST data for the entire site. A VCA may list data for his division and all subordinate departments, and a DCA may list data for his department.

Default: If no operand for the TYPE keyword is entered, CA-Top Secret will list all acids within the administrator's scope.

Types: The TYPE keyword is used with the following ACID types: **ACIDS, User, Profile, Group, Department, Division, Zone, VCA, ZCA, LSCA, SCA.**

Examples

To request all security information for DCA's in the TECH Division, the administrator enters:

```
TSS LIST(ACIDs) DATA(ALL) DIVISION(TECH) TYPE(DCA)
```

10.13 ZONE

Operating System: VSE, OS/390, and VM

Definition: To allow CA-Top Secret administrators to list data about ACIDs in a specific zone.

TSS Commands: The following TSS commands can be used with the ZONE keyword: **CREATE, MOVE, LIST**

Syntax:

```
TSS LIST(acid|ACIDS) DATA(datatype(s)) TYPE(acidtype) ZONe(acid)
```

Authority: CA-Top Secret will only display data concerning ACIDs within the administrator's scope. Thus, an MSCA, an authorized SCA or an authorized LSCA, could obtain LIST data for the entire site. A ZCA cannot specify the ZONE keyword.

Types: The ZONE keyword is used with the following ACID types: **Zone, ZCA, LSCA, ACIDS.**

Examples

To list the names of all users in the TECH Zone, the administrator enters:

```
TSS LIST(ACIDS) DATA(NAMES) ZON(TECH)
```

Chapter 11. How to Use LOCK/UNLOCK

This chapter presents the standard formats and rules that govern the use of the LOCK and UNLOCK functions. Note that the LOCK/UNLOCK functions are disabled if the NOLCFCHK attribute is attached to the ACID.

There are no detailed reference pages for the LOCK/UNLOCK functions.

11.1 Purpose

LOCK allows any ACID to LOCK his terminal so it cannot be used when unattended. UNLOCK allows an ACID to UNLOCK his terminal.

11.2 Entry Methods

Administrators may enter TSS LOCK or UNLOCK command functions freeform onto an entry screen.

The entry for the LOCK function is: TSS LOCK

The entry for the UNLOCK function is: TSS UNLOCK

11.3 General Rules and Procedures

The following rules and procedures apply to the entry of the LOCK and UNLOCK functions.

LOCK/UNLOCK is valid for CICS and CA-IDMS.

In CICS and CA-IDMS/DC, the ACID is prompted for his password if he attempts to use a locked terminal. If the password is valid, the request is executed; if not, the request is terminated.

Note: The LOCK and UNLOCK commands cannot be routed through the security network using the Command Propagation Facility (CPF).

Chapter 12. How to Use MODIFY

This chapter presents the standard formats and rules which govern the use of the MODIFY function.

There are no detailed reference pages for the MODIFY function. Refer to the *Control Options Guide* for information on CA-Top Secret control options.

12.1 Purpose

Given the CONSOLE attribute, the CA-Top Secret administrator may enter the MODIFY function to:

- display the status of the global security environment
- enter, change, or display CA-Top Secret control options.

12.2 Entry Methods

Administrators may enter the TSS MODIFY command function freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

12.3 Displaying Status

To display the status of the site's security environment, the administrator enters:

```
TSS MODIFY
```

In response to the above command, CA-Top Secret will provide a display containing the following information, depending on whether the system is VSE, OS/390, or VM.

VM:

- Number of events written to Audit/Tracking File
- Number of batch jobs processed in the server machine
- Number of CP commands validated
- Number of changes made to Security File
- Number of diagnoses validated
- Number of logons processed
- Number of writes to the Security File
- Number of reads to the Security File
- Number of IUCV requests received
- Number of IUCV requests processed
- Number of recovery records written
- Number of security checks made in the server
- Number of security file requests processed
- Number of violations
- Listing of control options and their settings
- Percentage of Security File being used.

VSE or OS/390:

- Job initiations validated
- Cross-memory requests processed
- VSE or OS/390 security calls processed
- SMF security records logged
- Program executions validated
- Number of changes made to the Security File
- Number of changes saved in the Recovery File
- Number of Security File input requests
- Number of Security File output operations since IPL on this CPU
- Number of audit events recorded in the Audit/Tracking File
- Listing of most control options and their current settings
- Percentage of Security File being used
- Statistics on how CACHE is being used.

12.4 Entering/Changing Control Options

To enter or change control options, the administrator enters:

```
TSS MODIFY(control option!(suboption-list)+)
```

The maximum character length of the TSS MODIFY subfield is 50 characters.

There are specific authorization rules which govern who may enter or change CA-Top Secret control options. Refer to the *Control Options Guide* for detailed descriptions of all control options and entry methods.

12.5 General Rules and Procedures

The following rules and procedures apply to the entry of all MODIFY command functions.

12.5.1 Authority

Under VM, if the ACID issuing the TSS MODIFY command does not have the CONSOLE attribute, this message is displayed:

```
TSS0802A:  Enter Password For Function
```

In response to message TSS0802A, the administrator must enter the MSCA's previous password, or an ACID/password combination for an ACID which has CONSOLE authority.

In VSE, CA-Top Secret will only process MODIFY requests issued by ACIDs with the CONSOLE attribute.

12.5.2 Source

MODIFY requests must be made from an online terminal (i.e., CICS) in a VSE environment. In a VM environment, MODIFY requests must be made from a logged-on user ID.

Note: The MODIFY command cannot be routed through the security network using the Command Propagation Facility (CPF).

Chapter 13. How to Use MOVE

This chapter presents the standard formats and rules which govern the use of the MOVE function. There are no detailed reference pages for this function.

13.1 Purpose

Given the proper administrative authority, the CA-Top Secret administrator may enter the MOVE function to move an ACID from one department, division or zone to another, or to change a user, ZCA, DCA and/or VCA into an SCA. If you use TYPE, you can promote or demote the type of ACID.

13.2 Entry Methods

Administrators may enter TSS MOVE function freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

13.2.1 Entry Screen Syntax

The basic entry for the MOVE function is as follows:

```
TSS MOVE(acid) --DEPARTMENT(acid)|DIVISION(acid)-- ZONE(acid)--TYPE(acid)-
          1          2         3    4      5     6     7      8
```

Field	Description
1	Enter the ACID that is being moved.
2 **4** **6**	Enter DEPARTMENT if the ACID is being moved into a department, enter DIVISION if the ACID is being moved into a division, or enter ZONE if the ACID is being moved into a zone.
3 **5** **7**	Enter the department, division or zone ACID of the destination. Not entering a department, division or zone makes the ACID (user, DCA, VCA, ZCA, LSCA) an SCA.
8	Enter the ACID type to which you are moving.

13.2.1.1 Sample Entry

To move a user (ACT4T) from the Accounts Receivable Department to the Accounts Payable Department (DACTPAY), the administrator enters:

```
TSS MOVE(ACT4T) DEPT(DACTPAY)
```

13.3 General Rules and Procedures

The following rules and procedures apply to the entry of the MOVE command function.

13.3.1 Authority

CA-Top Secret administrators must have authority, via ADMIN - ACID(MAINTAIN|ALL), to move ACIDs within their scope.

13.3.2 Effects of MOVE if the TYPE Keyword is Omitted

The movement of an ACID from one organization to another may change the ACID type of the ACID being moved. The following table shows how each type of ACID is changed when moved into another department, division or zone.

Table 13-1. Effects of MOVE Function

ACID Type	When moved into a DEPT:	When moved into a DIV:	When moved into a ZONE:	When moved with no destination:
USER	Remains User	Becomes VCA	Becomes ZCA	Becomes SCA
PROF	Remains Profile	N/A	N/A	N/A
DCA	Remains DCA	Becomes VCA	Becomes ZCA	Becomes SCA
VCA	Becomes DCA	Remains VCA	Becomes ZCA	Becomes SCA
ZCA	Becomes DCA	Becomes VCA	Remains ZCA	Becomes SCA
LSCA*	Becomes DCA	Becomes VCA	Becomes ZCA	Becomes SCA
SCA	Becomes DCA	Becomes VCA	Becomes ZCA	N/A
DEPT	N/A	Connected ACIDs and resources are moved with the department to a new division.	N/A	Remains DEPT with no division
DIV	N/A	N/A	Connected ACIDs and resources are moved with the division to a new zone	Remains DIV with no zone

* An LSCA can only be moved once his scope of authority has been removed. For example:

```
TSS DEADMIN(LSCA01) SCOPE(ZONE01,LSCA02)
```

Note: The following considerations apply when performing a MOVE:

- Only the MSCA can move a USER to an SCA
- Only the MSCA, SCA or ZCA (within scope) can move a DIV or VCA
- Only the MSCA, SCA, or VCA (within scope) can move a DEPT or DCA
- Only the MSCA, SCA, or DCA (within scope) can move a USER or PROFILE
- Only the MSCA can move an LSCA

13.3.3 Effects of MOVE Using the TYPE Keyword

With the TYPE keyword, an administrator can move an ACID from its original type to a new targeted type. A DEPT or DIVISION will only be specified if the new targeted ACID type requires it. See the chart below for details.

```
   TYPE            Keyword
Specification      Required
```

SCA	N/A
LSCA	N/A
ZCA	ZONE
VCA	DIVISION
DCA	DEPARTMENT
USER	DEPARTMENT

A VCA will move a DCA (DCA01) into a new financial department (FINDEPT) and demote this DCA to a TYPE(USER) by issuing the command:

```
TSS MOVE(DCA01) DEPT(FINDEPT) TYPE(USER)
```

The following command would leave a TYPE(USER) in the same department but promote it to a DCA:

```
TSS MOVE(USER01) TYPE(DCA)
```

Chapter 14. How to Use PERMIT/REVOKE

This chapter presents the standard formats and rules governing use of the PERMIT and REVOKE command functions. Those resources which are permitted or revoked through the PERMIT/REVOKE command functions, may be found in Chapter 22 entitled "Summary of Resources."

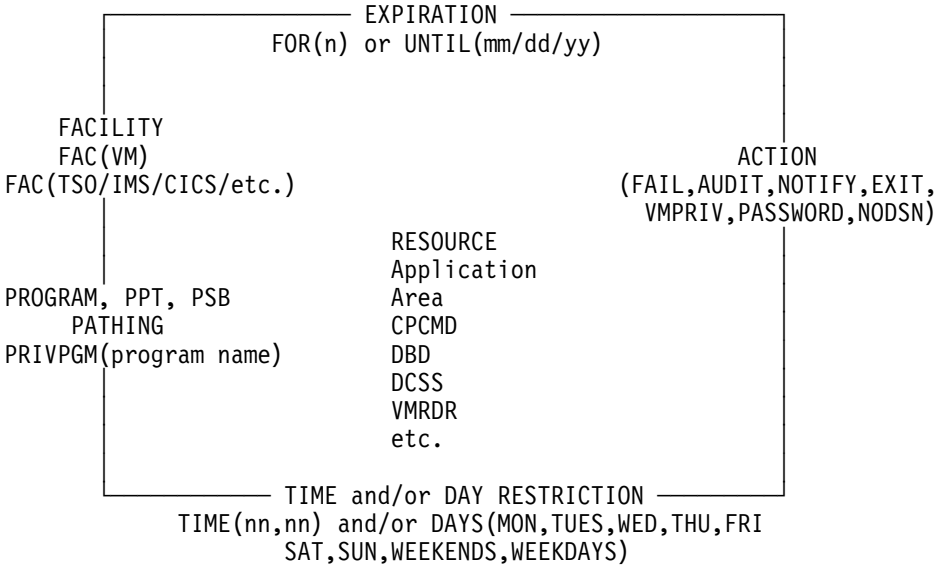
14.1 Purpose

14.1.1 PERMIT

Resource ownership means that the user, profile, or control ACID has an access level of ALL. Since it may not be desirable to grant unlimited access to individual users or profiles, CA-Top Secret administrators should assign resource ownership to department or division ACIDs using the ADDTO command function. Then, full or restricted resource access may be authorized for other ACIDs (non-owners) via the PERMIT command function.

Controlling Access to Resources: The CA-Top Secret administrator may use the PERMIT function to dictate not only who may access a resource, but how, when, and/or at what level, the resource may be accessed. Additionally, the administrator may specify the ACTION that CA-Top Secret will take when access to a resource is attempted.

Controlling Access:



14.1.2 REVOKE

Access to ownable resources may be REVOKEd when no longer needed, or when the access restrictions (i.e. levels and/or controls) need to be changed. In order to change a resource access restriction, the administrator must first REVOKE access and then reissue the PERMIT command function. Since REVOKE is the functional opposite of PERMIT, all entry methods and rules that apply to PERMIT also apply to REVOKE.

Note: All optional parameters that can be coded on the PERMIT command can also be coded on the REVOKE command. Although a resource may be PERMITted with optional parameters, the optional parameters cannot be REVOKEd from the resource individually. The resource must be REVOKEd and then re-PERMITted with any desired parameters.

14.2 Entry Methods

Administrators may enter TSS PERMIT or REVOKE command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

14.2.1 Command Syntax

The following figure shows how the PERMIT function is entered, freeform, onto an entry screen.

```
TSS PERMIT(acid) keyword(p-fix) ACCESS(level) keyword(oper)
          1      2      3      4      5      6
```

Field	Description
1	ACID of user or job for whom access is being PERMITted or REVOKEd
2	Keyword for type of resource to which access is being PERMITted or REVOKEd (i.e., DSNAME, VOL, etc.)
3	Prefix or resource name
4	A specific level of ACCESS to the resource, if applicable; if no entry is made, CA-Top Secret usually assigns a default access level based on the resource type. For example, the default for data set is READ
5	Access level = the manner in which a resource can be used once accessed (NONE, READ, WRITE, etc.)
6	Additional access keywords and their associated options. For example: DAYS(WEEKENDS), ACTION(FAIL)

After the ENTER key is pressed, CA-Top Secret displays the following message if the PERMIT or REVOKE was correct:

```
TSS0300I <    > FUNCTION SUCCESSFUL
```

An error message is displayed if the function was entered incorrectly.

14.3 General Rules

What follows are general rules and procedures that apply to all PERMIT and REVOKE command functions. Specific rules are documented with the applicable keyword.

14.3.1 Authority

CA-Top Secret administrators must have the appropriate resource(XAUTH) authority, via the TSS ADMIN command function, to PERMIT or REVOKE access to owned resources within their administrative scope. Note that RESOURCE(XAUTH) allows administrators to PERMIT or REVOKE access to ***all*** owned resources within their administrative scope. Administrators must also have explicit authority to use each access level keyword.

14.3.2 Scope of Authority

Given the proper administrative authority, a CA-Top Secret administrator may allow *any* ACID to access a resource, even if the ACID is outside of the administrator's scope. The resource, however, must be within the administrator's scope of authority.

14.3.3 Ownership

A resource must be owned before access can be PERMITted.

14.3.4 Application

Resources may not be PERMITted to department or division ACIDs.

14.3.5 Multiple PERMITs

CA-Top Secret allows the use of prefixing and masking for resource identification. Therefore, an administrator can enter multiple permissions to the same resource for the same user. A REVOKE command can remove a single or multiple permissions. CA-Top Secret uses a security validation algorithm to determine whether a resource access request should be granted or denied. This algorithm is further discussed in the *User Guide.*

14.4 Duplicate Permissions

In CA-Top Secret Release 3.0 no duplicate permissions are stored in the CA-Top Secret Security File. If a permission is issued to a user or profile that exactly matches an existing permission, CA-Top Secret will issue PERMIT FUNCTION SUCCESSFUL. No error messages are issued since the administrator requested that the permit be stored with the the user or profile, and CA-Top Secret verified that this request was accomplished.

The matching criteria is that all fields coded on the new permit exactly match the existing permission. If the new permit or existing permission has extra parameters, this would not constitute a match and the new permit would be stored on the Security File.

What follows is a brief summary of the algorithm as it applies to the PERMIT command function.

14.4.1.1 Best Match

CA-Top Secret will search a user's entire Security Record before making an access determination. This determination is, in part, based on the permission that contains a resource name or prefix that is the "best match" for the resource name or prefix being requested. This best match is based on the length of the prefix. Thus, if USER01 requests access to data set 'AB.CD' and CA-Top Secret encounters the following entries during its security validation search:

```
TSS PERMIT(USER01) DSN(AB.C) ACCESS(UPDATE)

TSS PERMIT(USER01) DSN(AB)
```

Then CA-Top Secret will grant access to the PERMIT containing AB.C since this data set prefix is the best match for the requested 'AB.CD'.

14.4.1.2 Equal Prefix Lengths

If CA-Top Secret encounters two matching PERMITs with equal prefix lengths while searching a Security Record, the access determination is based on the following procedure:

1. The first PERMIT containing a matching prefix is considered the "current best match." If no other PERMITS in the Security Record contain a matching prefix, CA-Top Secret will base its access decision on this PERMIT command function.
2. If the PERMIT in step 1 ***authorizes*** access, contains the ACCESS(NONE) restriction, or has the ACTION(DENY) attribute, CA-Top Secret ignores all subsequent PERMITs that contain resource prefixes of equal length. CA-Top Secret will, however, examine PERMITs containing matching prefixes of greater length.

3. If however, the PERMIT found in step 1 does not allow access, does not contain the ACCESS(NONE) restriction, or does not have the ACTION(DENY) attribute, then subsequent PERMITs of equal prefix lengths will be searched.

14.4.2 Revoking Multiple PERMITs

A REVOKE command can remove a single or multiple permissions. When multiple permissions are defined, a single REVOKE command function removes all definitions that match the resource name or prefix specified in the command function.

14.4.3 Using the GENERIC-NONGENERIC Attribute

The RDT attribute, NONGENERIC, causes a general resource to be treated as a fully qualified name rather than as a generic prefix.

Note: The GENERIC/NONGENERIC attribute affects security resource checks, it has no effect on CICS Bypass List processing.

The NONGENERIC attribute can support both long and short resource classes. This attribute does not, however, support the resources that support masking characters. For a complete list of these resources, refer to Appendix A: *Prefixed Resources*.

As an example, an administrator can permit a user to resource OTRAN(PSRV), which would allow access to PSRV as well as PSRVTEST or any other OTRAN whose first four characters match the prefix, PSRV. If the NONGENERIC attribute is activated, a permit to OTRAN(PSRV), however, only allows the user to execute transaction PSRV and not PSRVTEST. In order for the user to be allowed to issue either transaction, the permit must be done to OTRAN(PSRV(G)).

To alter a particular general resource class to conform to the non-generic attribute, the administrator enters:

```
TSS REPLACE(RDT) RESCLASS(OTRAN) ATTR(NONGENERIC)
```

where the OTRAN keyword is the resource class to be altered. To remove the NONGENERIC attribute, the administrator enters:

```
TSS REPLACE(RDT) RESCLASS(OTRAN) ATTR(GENERIC)
```

When changing the resource class from GENERIC to NONGENERIC, or from NONGENERIC to GENERIC, the security validation behavior for all existing definitions is preserved. However, resources will list differently and administrative commands which follow will have a different effect.

For example, if an attribute of a resource class is changed from GENERIC to NONGENERIC, any resource permitted prior to the change will display with a (G) to indicate the cross-authorization remains GENERIC.

Also, attempts to revoke such a permit may fail, with either TSS0384E: "RESOURCE NOT FOUND IN SECURITY RECORD", (if the (G) is not included on the REVOKE statement), or TSS0244E: "INVALID SUBFIELD LENGTH FOR KEKYWORD - KEYWORD" (if the (G) is included).

In this case, the attribute of the resource class should be temporarily changed back from NONGENERIC to GENERIC (when no other administration is taking place). The REVOKE (without the (G)) should then succeed, and the resource attribute may again be changed to NONGENERIC.

The NONGENERIC attribute applies to the following OS/390/VM resources **by default:**

IUCV
VMCF
VMDIAL
VMMACH
VMRDR

14.4.4 Masking and Prefixing for Other Resources

Resource masking is a technique which allows administrators to group resources with similar characteristics. Special characters are specified to represent variations between resource names. Prefixing allows administrators to group similar resources to be defined by CA-Top Secret simultaneously.

A list of resources that support masking characters and prefixing can be found in Appendix A: *Prefixed Resources*.

Note:

- When LISTing the RDT, a MASK or NOMASK attribute will appear in the output signifying whether a resource supports masking characters.
- *ALL* can be used with any RDT resource.

14.4.5 Prefixing for Data Sets

Prefixing allows the CA-Top Secret administrator to group a set of similar data sets together, and define them by a 2-26 character prefix. For example, all data sets used by the Publications Department could be prefixed by TECHPUBS. Then, the administrator could PERMIT a user to access any data set prefixed by TECHPUBS.

```
TSS PERMIT(USER01) DSN(TECHPUBS.)
```

This eliminates the need to permit access to 'TECHPUBS.PROD.SCEDS' and 'TECHPUBS.GRAPHICS.SCEDS'.

A prefix may span several data set name index levels. For example, DSN(TECHPUBS.PR).

14.4.5.1 Resource Masking

Resource masking is another method of reducing the number of resource definitions required to implement widespread protection. Masking allows administrators to group resources with similar characteristics, and use special characters to represent variations between resource names. Those resources which support masking characters are indicated in Chapter 22 called "Summary of Resources."

The following is a description of the five types of masks.

14.4.5.2 Floating "-"

The character "-" represents a variable number of characters.

ENTRY:	MATCHES:	BUT NOT:
ACCT-VEND	ACCTPAY.VENDOR	ACC.VEND
	ACCTVEND	AP.ACC.VEND

Explanation: In this case, the entry indicates that a matching prefix must begin with the characters ACCT, followed by a variable number of characters represented by a "-", and must end with the characters VEND.

The prefix ACC.VEND does not begin with ACCT and therefore does not match the entry.

Floating characters can cross node (also called qualifier or index) boundaries. Floating characters cannot be used with other mask types.

14.4.5.3 Variable "*"

The asterisk "*" can be used to represent zero to eight characters.

ENTRY:	MATCHES:	BUT NOT:
ACCT*M.DATA	ACCTPAYM.DATA	ACCTPAYD.DATA
*LAB	LAB	NEW.JERSEY.LAB
*RAT	TESTRAT.LAB	TRAP.ALL.RATS

Explanation: In the first entry, the asterisk is used to represent zero to eight characters between ACCT and M; thus the entry matches ACCT.PAYM but not ACCTPAYD. In the second entry, *LAB does not match NEW.JERSEY.LAB since NEW.JERSEY. is

more than eight characters long. Multiple asterisks can be listed in series to equal up to 44 characters; thus **LAB would match NEW.JERSEY.LAB.

14.4.5.4 Index ".*."

The characters ".*." or "*." appearing at the beginning of the data set name are used to represent a one to eight character index.

```
  ENTRY:            MATCHES:              BUT NOT:

*.BALL             BASKET.BALL           BALL.GAME

CICS.*.*.F         CICS.RUM.TSS.FIL      CICS.FEATURES
```

Explanation: The index mask is an extension of the variable mask that allows the CA-Top Secret administrator to specify where index levels must appear in a data set name. The first entry specifies that .BALL must be prefixed by 1 to 8 characters; thus, the data set BALL.GAME does not match this definition. The second entry specifies that two indexes must appear between CICS. and .F. CICS.FEATURES contains no indexes between CICS. and .F and therefore does not match the mask.

14.4.5.5 Fixed Position "+"

The character "+" is used to represent any single character within a data set name.

```
  ENTRY:            MATCHES:            BUT NOT:

A123+.TSO          A1234.TSO           A123.TSO
```

14.4.5.6 ACID "%"

The character "%" represents the ACID of the user specified in the TSS command.

If: TSS PER(USER52) DSN(%.MAIL) ACCESS(ALL)

Then: USER52 will have full access to the data set named USER52.MAIL.

This capability can be used to permit all TSO users full access to data sets prefixed by their ACID.

1. The MSCA must own the "%." character. Note that only the MSCA can own a special character.
2. TSS ADD(MSCA acid) DSN(%.)
3. A CA-Top Secret Administrator may now PERMIT all TSO users to have all access to any data set prefixed by an ACID.

   ```
   TSS PER(ALL) DSN(%.) FAC(TSO) ACC(ALL)
   ```

CA-Top Secret recognizes a special technique to specify a portion of the userid to be used as a mask. The special technique uses the % character in conjunction with values identifying the start and length of the userid being entered. For example, to permit TUSER01 access to dataset USER01 the administrator enters:

```
TSS PER(TUSER01) DSN(%26%)
```

14.4.5.7 Combinations

All masking characters, **except** the floating mask, may be combined.

ENTRY:	MATCHES:	BUT NOT:
MAR++.*.SUM	MAR86.A.SUM	MARCH.SUM

14.4.5.8 Illegal Combinations

What follows is an example of an illegal combination.

CSSY.*-83 BOTL-WORK+++.COMP

Remember, floating characters "-" may not be combined with other masking characters.

14.5 Applicable Keyword List

The following keywords may be used with the TSS PERMIT/REVOKE command functions. The reference pages that follow contain detailed documentation for each keyword.

```
ACID
ACTION
CALENDAR
DAYS
FACILITY
FOR
IMSMSC
LIBRARY
MAPREC
MASKREC
MODE
PRIVPGM
SELECT
TIMEREC
TIMES
UNTIL
VMUSER
```

Note: All resources defined to the RDT can also be used with the PERMIT/REVOKE command function. For an explanation of these keywords, refer to the chapter entitled: "Summary of Resources."

14.6 ACID

Operating System: VSE, OS/390, and VM

Description: To cross authorize an ACID to submit jobs under another ACID.

TSS Commands: The following TSS command can be used with the ACID keyword: **PERMIT** only.

Syntax:

```
TSS PERMIT(acid) ACID(acidid)
```

Types: The ACID keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

Examples:

To allow user WYLMI01 to submit a job under SMITH01, the administrator enters:

```
TSS PERMIT(WYLMI01) ACID(SMITH01)
```

14.7 ACTION

Operating System: VSE, OS/390, and VM

Description: To specify which action(s) CA-Top Secret will take when access to a resource is attempted.

TSS Commands: The following TSS command can be used with the ACTION keyword: PERMIT, REVOKE(ACTION(ADMIN) **only** for REVOKE).

Syntax:

```
TSS PERMIT(acid) resource(prefix)
    ACTION(FAIL,AUDIT,NOTIFY,DENY,VMPRIV,
    PASSWORD,NODSNCHK,ADMIN)

TSS REVOKE(acid) resource(prefix) ACTION(ADMIN)
```

Authority: Although no specific authority is required, administrators must have resource(XAUTH) authority, via the TSS ADMIN function, to specify ACTION for resources that are owned within their scope.

Types: The ACTION keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

Operands: The following operands can be used with the ACTION keyword:

Action	Description
FAIL	If this permission is used by CA-Top Secret as the "best fit" for the resource, CA-Top Secret will process the request as if the user were in FAIL mode. To be more specific, CA-Top Secret will fail any unauthorized access to the resource, and conversely, allow authorized access (superseding, for example, native password protection on data sets and minidisks). **Note:** FAIL can be used with resources that have access levels, whereas DENY is used with resources that do not have access levels.
AUDIT	CA-Top Secret will audit the access.
NOTIFY	CA-Top Secret will notify the security console of resource access via the message TSS7299W.
EXIT	If the PERMIT is granted, CA-Top Secret issues the EXIT call to invoke the TSS Installation Exit for data sets and volumes only in OS/390 and VSE and for all VM resources.

DENY Valid for all resources which do not support access levels, ACTION(DENY) will fail any attempted access to the resource defined in the PERMIT.

This ACTION effectively provides ACCESS(NONE) to the resource. The ACID's mode is still honored.

VMPRIV (VMPRIVILEGE) The privileged form of CP commands and DIAGNOSE instructions.

PASSWORD FOR DATASETS ONLY:

If the PERMIT is granted, CA-Top Secret returns control to VM for password protection. This assumes that a link password exists for the minidisk.

Note: Any data set checks which occur as a result of the allocation of an SMS-managed data set will not be prompted for a data set password. This is a normal function of SMS.

NODSN FOR VOLUMES ONLY

Only volume checking will be performed. All data set restriction is bypassed, and the minimum and maximum access levels to all data sets will be controlled by the PERMITted volume access.

ADMIN Under normal circumstances, CA-Top Secret allows an administrator to PERMIT and REVOKE only those resources which fall under his scope. When specifying ACTION(ADMIN), the administrator gives authority to another administrator requesting the ability to PERMIT and REVOKE resources outside of his scope. If an access level is not specified, CA-Top Secret will permit the default access level for that resource class.

Note: ACTION(ADMIN) is not valid for Profile type ACIDs.

Examples:

USER01 is in WARN mode, and is *not* connected to PROF01, which allows access to MASTER.PAYROLL.FILE. Ordinarily, if USER01 attempted to access the MASTER.PAYROLL.FILE, he would be warned, but not failed. To ensure that CA-Top Secret will fail USER01 if he attempts to access the MASTER.PAYROLL.FILE, the administrator enters:

```
TSS PERMIT(USER01) DSN('MASTER.PAYROLL.FILE') ACTION(FAIL) ACCESS(NONE)
```

If the administrator wants CA-Top Secret to create an audit record every time USER01 updates the PERS.PAY data set, he would issue the following command:

```
TSS PER(USER01) DSN(PERS.PAY) ACTION(AUDIT) ACC(UPDATE)
```

If the administrator enters:

```
TSS PERMIT(USER01) DSN('PERS.PAYROLL') ACC(R) ACT(NOTIFY)
```

CA-Top Secret will issue message TSS7299I whenever USER01 accesses PERS.PAYROLL.

USER01 is connected to a profile (PROF01) that allows him to access all terminals in the Accounting Department:

TSS PER(PROF01) TERMINAL(K06L1234)

There are two terminals, however, that USER01 may not access (K06L4567 and K06L1233) To deny USER01 access to these terminals, the TSS administrator enters:

```
TSS PER(USER01) TERM(K06L4567,K06L1233)
    ACTION(DENY)
```

To ensure that the denied access will result in a failure in any mode, the administrator enters:

```
TSS PER(USER01) TERM(K06L4567,K06L1233)
    ACTION(FAIL,DENY)
```

This command allows USER05 to permit or revoke access to this resource to other users-although the resource itself is not owned within his scope.

```
TSS PER(USER05) DSN(SYS1.) ACTION(ADMIN)
```

This command removes authority from USER05 to permit or revoke access to this resource. the resource itself is not owned within his scope.

```
TSS REV(USER05) DSN(SYS1.) ACTION(ADMIN)
```

Note: If the FACILITY keyword had been specified on the above command, the command would have been processed without an error. However, FACILITY restrictions will not be in effect.

14.8 CALENDAR

Once defined to the SDT, this keyword can be used is association with any resource to PERMIT or REVOKE a CALENDAR to an ACID.

Operating System: VSE and OS/390

Syntax:

```
TSS PER(acid) RESOURCE(resource- name)  ACCESS(access-level)
              CALENDAR(calendar-name)
```

Capacity of list — One CALENDAR record per TSS command

Authority: The administrator must have MISC3(SDT) authority granted by the TSS ADMIN function, to PERMIT or REVOKE access to a CALENDAR associated with a resource that is owned within their scope.

Access Levels: The administrator can specify any or all of the access levels of their respective resource. For example, a data set would have the following access levels: **ALL, CREATE, CONTROL, FETCH, NONE, READ, SCRATCH, UPDATE, WRITE.**

If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to CALENDAR records: **Expiration, Facility, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The CALENDAR keyword associated with a resource is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Note: CALENDAR and DAYS are mutually exclusive on a PERMIT.

Examples:

To permit a user to update the inventory master file data set INV.MASTER.FILE with the personnel department's CALENDAR CAL1, the administrator enters:

```
TSS PERMIT(USR01) DSN('INV.MASTER.FILE') ACCESS(UPDATE)
                  CALENDAR(CAL1)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USR01) DSN('INV.MASTER.FILE')
```

14.9 FACILITY

Operating System: VSE, OS/390, and VM

Description: To permit an ACID to have access to a resource through the specified facility.

TSS Commands: The following TSS commands can be used with the FACILITY keyword: **ADDTO, REMOVE, CREATE, REPLACE, ADMIN, DEADMIN, PERMIT.**

Syntax:

```
TSS PERMIT(acid) resource(prefix(es)) FAcility(facility name)
```

Capacity of list— 1-5 facility names per TSS command

Refer to the PERMIT/REVOKE chapter introduction for general rules and procedures. Specific rules and procedures that apply to the FACILITY keyword are shown below.

Default Facility: If the FACILITY keyword is not specified in a PERMIT function, CA-Top Secret allows the user to access the resource from any facility authorized for that user.

Authority: Use of the PERMIT function does NOT require that the administrator have authority to grant an ACID signon ability to the facility. Therefore, an administrator may enter,

```
TSS PERMIT(PAY10DM) DSN(PAYROLL) FAC(CICS)
```

even though the administrator does not have authority for CICS. However, in this case, the administrator must have DSNAME(XAUTH) authority.

Types: The FACILITY keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

Examples:

To allow user ED001 to have READ access (default) to tutorial data sets through both CICS and BATCH, the administrator enters:

```
TSS PER(ED001) DSN(TUTOR) FAC(CICS,BATCH)
```

14.10 FOR

Operating System: VSE, OS/390, and VM

Description: To specify the number of days that the ACID is permitted to access the resource.

TSS Commands: The following TSS commands can be used with the FOR keyword: **ADDTO, REMOVE, CREATE, REPLACE, PERMIT, REVOKE.**

Syntax:

```
TSS PERMIT(acid) resource(prefix(es)) FOR(1-255 days)
```

Refer to the PERMIT/REVOKE chapter introduction for general rules and procedures. Specific rules and procedures that apply to the FOR keyword are shown below.

Expired Access: When a resource permission expires, the permission is ignored by the CA-Top Secret search algorithm. The TSS LIST function will automatically remove the expired resource permission.

UNTIL Keyword: The UNTIL keyword sets a specific date when the resource permission will expire. FOR and UNTIL are mutually exclusive; CA-Top Secret will not accept FOR and UNTIL within the same PERMIT command function.

Types: The FOR keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

Examples:

To indicate that USER01 is allowed READ access (default) to any data set suffixed by .FILE for one day (i.e., for the rest of today), the administrator enters:

```
TSS PERMIT(USER01) DSN(***.FILE) FOR(1)
```

To revoke USER01's access, the administrator enters:

```
TSS REVOKE(USER01) DSN(***.FILE)
```

14.11 MAPREC

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a MAP record associated with an OTRAN or PPT resource. A MAP record is used to support Screen Level Protection (SLP).

Syntax

```
TSS PER(acid) OTRAN(oper)|PPT(oper) MAPREC(map-name)
```

Capacity of list — One MAP record per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE access to MAP records that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels that are associated with OTRANs and PPTs: **ALL, INQUIRE, SET, EXECUTE, ALL, NONE, UPDATE**

The only exception for OTRAN access is UPDATE.

If ACCESS is not specified, CA-Top Secret defaults to EXECUTE access for both OTRAN and PPT.

Access Controls: The administrator can use any of the following methods to control access to MAP records: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The MAPREC keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To permit a user ALL access to a CICS transaction called PAYR with a MAP record ENG1, the administrator enters:

```
TSS PERMIT(USR01) OTRAN(PAYR) ACCESS(ALL) MAPREC(ENG1)
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) OTRAN(PAYR)
```

14.12 MASKREC

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a MASK record together with a SELECT statement that is associated with an FCT.

Syntax:

```
TSS PER(acid)  FCT (oper) ACCESS(access-level)
               MASKREC(mask-name)  SELECT(selin,selout)
```

selin Specifies the input select record.

selout Specifies the output select record.

Note: It is not necessary to have both an input and output record for a SELECT statement.

Capacity of list — One MASKREC and SELECT statement per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE access to MASKRECs associated with an FCT that are owned within their scope.

Access Levels: The administrator can specify the same access levels associated with an FCT resource: **SET, INQUIRE, ALL, BROWSE, DELETE, NONE, READ, UPDATE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

selin Can have an access level of: **READ, BROWSE**

selout Can have an access level of: **WRITE, UPDATE, DELETE**

Note: If only an input record is used on the SELECT statement, it would be permitted UPDATE access.

Access Controls: The administrator can use any of the following methods to control access : **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The MASKREC keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To permit a user ALL access to the FCT file called PAY with the MASK record CRYPT1 and selecting all departments 100 and above from the input record, and all the employees named Mike from the output record, the administrator enters:

```
TSS PERMIT(USR01) FCT(PAY) ACCESS(ALL) MASKREC(CRYPT1)
                  SELECT('IF DEPT GE "100" AND NAME EQ "MIKE" ')
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) FCT(PAY)
```

14.13 MODE

Operating System: VSE, OS/390, and VM

Description: To specify an operating MODE for a user, control or profile ACID.

TSS Commands: The following TSS commands can be used with the MODE keyword: **ADDTO, REMOVE, WHOOWNS, WHOHAS, ADMIN, DEADMIN, PERMIT, REVOKE.**

Syntax:

```
TSS PERMIT(acid|profile) MODE(DORM|WARN|IMPL|FAIL)
```

Refer to the PERMIT/REVOKE chapter introduction for general rules and procedures. Rules that apply to the MODE keyword are shown below.

Overrides: A user or profile MODE will override the global and facility MODES.

DORMANT mode: CA-Top Secret allows administrators to PERMIT DORMANT mode, but this practice is not suggested because a user or profile operating in DORMANT mode bypasses CA-Top Secret security. Generally, administrators should only upgrade the mode (i.e., WARN to IMPL, etc.).

Authority: The master SCA (MSCA) must own all modes before they can be PERMITted. Modes can only be administered by an SCA ACID with MISC9(MODE) authority, via the TSS ADMIN function.

Types: The MODE keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To force a user to run in IMPL mode, the administrator enters:

```
TSS PERMIT(PAYUSER) MODE(IMPL)
```

To change this specification to FAIL mode, the administrator enters:

```
TSS REVOKE(PAYUSER) MODE(IMPL)
TSS PERMIT(PAYUSER) MODE(FAIL)
```

14.14 PRIVPGM

Operating System: VSE and OS/390

For VSE: Use with DLBL cards; the privileged program specified in the PERMIT function must be executed iwth the following JCL keyword:

```
// EXEC program
```

Description: To specify the full names of the programs that must be in control when a resource is accessed. A privileged program specification restricts the use of a resource to a control path.

TSS Commands: The following TSS command can be used with the PRIVPGM keyword: **PERMIT** only.

Syntax:

```
TSS PERMIT(acid) resource(prefix(es))
    PRIvpgm(program)
```

Prefix length— 1-8 characters
Capacity of list— 1-5 program names

Refer to the PERMIT/REVOKE chapter introduction for general rules and procedures. Specific rules and procedures that apply to the PRIVPGM keyword are shown below.

Use with DSNAMEs: The privileged program specified in the PERMIT function must be executed via the following JCL keyword:

EXEC PGM=program

OR via a program executed through LINK, LOAD, ATTACH, or XCTL.

Technically, the program must be associated with either the top-most or bottom-most PRB.

Authority: Although no specific authority is required, administrators must have resource(XAUTH) authority, via the TSS ADMIN function, to specify PRIVPGM for resources that are owned within their scope.

Types: The PRIVPGM keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

Examples:

To permit access to SMF data sets SYS1.MANX and SYS1.MANY specifically through a link-listed program, the administrator enters:

```
TSS PER(SYS92) ACC(CONTROL) DSN(SYS1.MAN+)
    PRI(SMFMNGR)
```

To permit access to the personnel data set, but allow any program beginning with the characters PRSP, the administrator enters:

```
TSS PER(PAY100K) DSN(PERS.*.MASTER) PRI(PRSP(G))
```

To permit access to a CICS file, but only if the CICS program in control is PCC505, the administrator enters:

```
TSS PER(CLK505P) FCT(PARTS) PRI(PCC505)
```

Examples for VSE:

To permit access to dataset VSE.PRD2.BASE from program DITTO, the administrator enters:

```
TSS PER(SYS92) ACCESS(UPDATE) DSN(VSE.PRD2.BASE) PRI(DITTO)
```

14.15 SELECT

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a SELECT record associated with an FCT resource.

Syntax:

```
TSS PER(acid) FCT(oper) SELECT(selin,selout)
```

selin Specifies the input select record.

selout Specifies the output select record.

Note: It is not necessary to have both an input and output record for a SELECT statement.

Capacity of list — One SELECT statement per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE SELECT records associated with an FCT that are owned within their scope.

Access Levels: The administrator can specify any or all of the access levels associated with an FCT: **SET, INQUIRE, ALL, BROWSE, DELETE, NONE, READ, UPDATE.:** If ACCESS is not specified, CA-Top Secret defaults to READ access.

selin Can have an access level of: **READ, BROWSE**

selout Can have an access level of: **WRITE, UPDATE, DELETE**

Note: If only an input record is used on the SELECT statement, it would be permitted UPDATE access.

Access Controls:: The administrator can use any of the following methods to control access to SELECT records: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The SELECT keyword in association with an FCT is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To permit a user to access all data from an FCT called PAY and select all records so that departments 1000 through 1999 are chosen, the administrator enters:

```
TSS PERMIT(USR01) FCT(PAY)  ACCESS(ALL)
                  SELECT('IF DEPT GE "1000" AND DEPT LT "2000" ')
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) FCT(PAY)
```

14.16 TIMEREC

Once defined to the SDT, this keyword can be used to PERMIT or REVOKE a TIME record associated with any resource.

Syntax:

```
TSS PER(acid) RESOURCE(resource-name) TIME(time-name)
```

Capacity of list — One TIMREC per TSS command

Authority: The administrator must have MISC3(SDT) authority, granted by the TSS ADMIN function, to PERMIT or REVOKE access to TIME records associated with a resource owned within their scope.

Access Levels: The administrator can specify any or all of the access levels associated with a particular resource. For example, a data set would have the following access levels: **ALL, CREATE, CONTROL, FETCH, NONE, READ, SCRATCH, UPDATE, WRITE.**

If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to TIME records: **Expiration, Facility, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The TIME keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Note: The TIMEREC and TIMES keywords are mutually exclusive on a PERMIT.

Examples:

To permit a user to update a data set with a prefix of SFT and using a department's TIME record named TIME1, the administrator enters:

```
TSS PERMIT(USR01) DSN(SFT.)  ACCESS(ALL) TIMEREC(TIME1)
```

To revoke access the administrator enters:

```
TSS REVOKE(USR01) DSN(SFT.)
```

14.17 TIMES

Operating System: VSE, OS/390, and VM

Description: To specify a range of hours during which users may access a resource.

TSS Commands: The following TSS commands can be used with the TIMES keyword: **ADDTO, PERMIT.**

Syntax:

```
TSS PERMIT(acid) resource(prefix(es)) TIMES(00,24)
```

Time Ranges: The first two digits in the TIME operand specify the hour at which (CPU time) CA-Top Secret permits access to the resource. The second pair of digits specify the hour through which CA-Top Secret permits access. Thus, CA-Top Secret permits access from the first minute of the hour specified in the first operand, until the first minute of the hour specified in the second operand.

Note: When the time range wraps around midnight, access is permitted until one minute before the "second" hour expires. For example if the range is (10,20), the user will be permitted access from 10 a.m. until 8 p.m. If the range is (20,10), indicating that it wraps around midnight, then the user can access that resource from 8 p.m. until 10:59 a.m. on the following morning.

Inclusive Range: To specify an inclusive range, set the start time to a lesser number than the stop time. This entry permits USER01 to open the data set between 0600 hours (6:00 am) and 1200 hours (noon).

```
TSS PERMIT(USER01) DSN(**.+COPS) TIMES(06,12)
```

Wrap Around Range: To indicate a range that wraps around the 24-hour clock, set the start time greater than the stop time. This entry permits USER01 to access the data set between 8:00 p.m. in the evening and 8:59 a.m. on the *following* morning.

```
TSS PERMIT(USER01) DSN(**.+COPS) TIMES(20,08)
```

To permit access for one hour (10 am to 11 am), the administrator enters:

```
TSS PERMIT(ACID) DSN(**.PREFIX) TIMES(10,11)
```

Authority: Although no specific authority is required, CA-Top Secret administrators must have resource(XAUTH) authority, via the TSS ADMIN function, to specify TIMES for resources that are owned within their scope.

Types: The TIMES keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

14.18 UNTIL

Operating System: VSE, OS/390, and VM

Description: To assign a specific date when permission to access a resource will expire.

TSS Commands: The following TSS commands can be used with the UNTIL keyword: **CREATE, ADDTO, REMOVE, REPLACE, PERMIT, REVOKE.**

Syntax:

```
TSS PERMIT(acid) resource(prefix(es)) UNTil(mm/dd/yy)
```

Format for Dates: The format for date entries is determined by the settings for the DATE control option. Determine these settings before entering a date with the UNTIL keyword. The default is mm/dd/yy.

Expired Access: When a resource permission expires, the permission is ignored by the CA-Top Secret search algorithm. The TSS LIST function automatically removes the expired resource permission.

FOR Keyword: The FOR keyword may be used to set the *number of days* that a user may access a resource. FOR and UNTIL aer mutually exclusive; CA-Top Secret only accepts one of the keywords within the same PERMIT command function.

Authority: No specific authority is required to assign the UNTIL keyword.

Types: The UNTIL keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA, ALL.**

Examples:

This entry permits USER01 to READ (default) to any data set suffixed by .FILE until May 1, 1991 (i.e., until 11:59:59 pm on April 30, 1991).

```
TSS PERMIT(USER01) DSN(****.FILE) UNT(05/01/94)
```

Chapter 15. How to Use REFRESH

This chapter presents the standard formats and rules that govern the use of the REFRESH function. There are no detailed reference pages for REFRESH.

15.1 Purpose

REFRESH allows a CA-Top Secret administrator to renew the ACIDs in any address space in the security environment. This command is especially useful in multi-user address spaces like CICS and IMS, where an ACID can have multiple instances of signed on users.

Issuing the REFRESH command against a target region refreshes all occurrences of an ACID. As a result, the user does not need to log off and log back on for administrative changes to take effect.

15.2 Entry Methods

CA-Top Secret administrators may enter TSS REFRESH command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

15.2.1 Command Syntax

The following sample shows the basic entry for the REFRESH function.

```
TSS REFRESH[(acid)] [JOBNAME(job|*)]
```

no operands Refreshes one's own security environment.

acid Refreshes all occurrences of a specified ACID in the address space where the command is issued.

JOBNAME Refreshes either one of the following:

- **job** Refreshes all occurrences of a specified ACID in the address space of a given jobname.
- ***** Refreshes all occurrences of a specified ACID in all address spaces

15.2.2 Sample Entry

To get a new copy of the security administrator's own machine, he would enter:

```
TSS REFRESH
```

15.3 General Rules and Procedures

What follows are rules and procedures that apply to the entry of all REFRESH command functions.

15.3.1 Authority

All users are allowed to refresh their own security environment.

15.3.2 Scope

The ACID being REFRESHd must be within the administrator's scope.

Chapter 16. How to Use RENAME

This chapter presents the standard formats and rules which govern the use of the RENAME function. There are no detailed reference pages for RENAME.

16.1 Purpose

RENAME allows a CA-Top Secret administrator to change the ACcessor ID of any ACID.

16.2 Entry Methods

CA-Top Secret administrators may enter TSS RENAME command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

```
TSS RENAME(acid) ACID(new acid)
           1     2       3
```

Field	Description
1	Enter the ACID to be RENAMEd.
2	Enter the ACID keyword.
3	Enter the new ACID.

16.2.1 Sample Entry

To change the ACID of the MSCA from TSSREC to BIGBOSS, the administrator enters:

```
TSS RENAME(TSSREC) ACID(BIGBOSS)
```

16.3 General Rules and Procedures

What follows are rules and procedures that apply to the entry of all RENAME command functions.

16.3.1 Authority

CA-Top Secret administrators must have authority, via the ADMIN - ACID(MAINTAIN | ALL) function, to rename an ACID.

16.3.2 Scope

The ACID being RENAMEd must be within the administrator's scope.

16.3.3 Permitted Use of the ACID

An ACID cannot be renamed if it is currently permitted to another ACID.

16.3.4 Global Records

The ALL, AUDIT, STC, NDT, RDT, DLF records cannot be renamed.

Example:

CA-Top Secret will **not** accept the entry:

```
TSS RENAME(ALL) ACID(GLOBAL)
```

Chapter 17. How to Use REPLACE

This chapter presents the standard formats and rules governing use of the REPLACE function.

17.1 Purpose

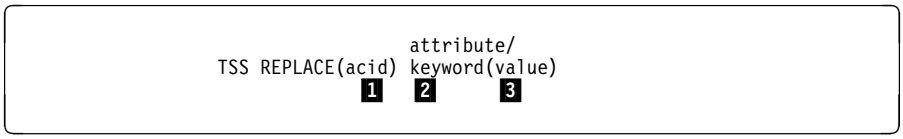
Given the proper administrative authorities, the CA-Top Secret administrator may use the REPLACE function to change the values, names, or data of CA-Top Secret attributes or keywords assigned to ACIDs within his scope.

17.2 Entry Methods

Administrators may enter TSS REPLACE command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

17.2.1 Command Syntax

The following sample shows the basic entry for the REPLACE function:



Field	Description
1	Enter the ACID that will be affected by the REPLACE function.
2	Enter the attribute or keyword to be changed by the REPLACE function.
3	Enter the new attribute or keyword's value, name, or data that will REPLACE the current information.

17.2.1.1 Sample Entry

To change a user's password, the administrator enters:

```
TSS REPLACE(USER77) PASSWORD(QUACK)
```

17.3 Authority

Full use of the REPLACE function requires a combination of administrative authorities. Refer to the specific attribute or keyword in the detailed reference pages for the appropriate administrative authority.

17.3.1 Scope

Administrators can use the REPLACE function only to maintain ACIDs under their administrative scope.

17.4 Applicable Keyword List

The following keywords may be used with the REPLACE function. For more information about these keywords, refer to the reference pages in the "How to Use ADDTO/REMOVE" chapter.

ACLST	MCSCMDS	PCOPTS	TSOMSIZE
ATTR	MCSDOM	PHYSKEY	TSOOPT
CONVSEC	MCSKEY	PSTKAPPL	TSOSCLASS
DEFNODES	MCSLEVL	RESCLASS	TSOUDATA
DEFACC	MCSLOGC	SCTYKEY	TSOUNIT
FACILITY	MCSMFRM	SESSKEY	TZONE
FOR	MCSMGID	SESSLOCK	UID
GID	MCSMON	SITRAN	UNTIL
IESFL1	MCSROUT	SMSAPPL	VSECATBT
IESFL2	MCSSTOR	SMSDATA	VSEMCON
IESINIT	MCSUD	SMSMGMST	VSERODIR
IESSYNM	NAME	SMSSTOR	VSESYSAD
IESTYPE	OPCLASS	TARGET	WAACCNT
IESVCAT	OIDCARD	TSOCOMMAND	WABLDG
IMSMSC	OPIDENT	TSODEFPRFG	WAADDR1
INSTDATA	OPPRTY	TSODEST	WAADDR2
LANGUAGE	PASSWORD	TSOHCLASS	WAADDR3
LTIME	PCADMIN	TSOJCLASS	WAADDR4
MASTFAC	PCDSDAYS	TSOLACCT	WAADEPT
MCSALTG	PCIDLE	TSOLPROC	WAIT
MCSAUTH	PCLGTYPE	TSOLSIZE	WANAME
MCSAUTO	PCMINPWD	TSOMCLASS	WAROOM

Note: All resources defined to the RDT can also be used with the REPLACE command function. For an explanation of these keywords, refer to the chapters called: RDT Administration, How to Use ADDTO/REMOVE, and Summary of Resources.

Chapter 18. How to Use WHOHAS

This chapter presents the standard formats and rules governing the use of the WHOHAS function.

18.1 Purpose

Given the proper administrative authority, the CA-Top Secret administrator may enter the TSS WHOHAS command function to display:

- all ACIDs, within the administrator's scope, that have access (via the PERMIT function) to a specified resource
- all ACIDs, within the administrator's scope, that have access (via the ADDTO function) to a specified facility
- all ACIDs, within the administrator's scope, that operate under a specific CA-Top Secret mode due to a TSS PERMIT-MODE command function
- all ACIDs, within the administrator's scope, which have access to a specific job submission ACID. CA-Top Secret also displays the owner of the job submission ACID or resource, and the level of access (READ, UPDATE, CONTROL, etc.) that the ACID has to the resource.

18.2 Entry Methods

CA-Top Secret administrators may enter TSS WHOHAS command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

Note: Only one resource keyword and prefix may be specified per command.

18.2.1 Command Syntax

```
TSS WHOHAS keyword(prefix|mode|acid) DATA(options)
           1                 2            3
```

Field	Description
1	If resource access information is required, enter the resource class for the CA-Top Secret keyword. To determine ACIDs which are functioning in a specific security mode, enter MODE. To determine who has access to a specific job submission ACID, enter ACID.
2	Enter the specific resource prefix, CA-Top Secret mode, or ACID for which access information is required.
3	Optionally designate LITERAL, MASK, and/or NOPREFIX to determine how CA-Top Secret should interpret the resource (i.e., as a mask or as an actual resource name).

18.2.1.1 Sample Entry

To determine who has access information for datasets prefixed with "SFT.CICS.," the auditor enters:

```
TSS WHOHAS DSN(SFT.CICS)
```

CA-Top Secret will respond by displaying the ACIDs and the access information (see Figure 13 following).

```
RESOURCE      =       SFT.CICS.                   OWNER(SFTDEPT)
  XAUTH       =       SFT.CICS.                   ACID(SFTUSR1)
    ACCESS    =       UPDATE
  XAUTH       =       SFT.CICS.LOAD               ACID(SFTUSR2)
    ACCESS    =       UPDATE,CONTROL
  XAUTH       =       SFT.                        ACID(SFTMNGR)
    ACCESS    =       READ
  XAUTH       =       SFT.*.TEST                  ACID(SFTMNGR)
    ACCESS    =       UPDATE,CONTROL
```

Figure 13. TSS Response to WHOHAS

18.2.2 Obtaining Resource Access Information

Resource access information can be obtained by specifying a prefix, fully qualified name (within quotes), or a pattern containing masking characters. Not all resources support masking characters. See Chapter 13 under "Masking and Prefixing for Other Resources."

The amount of information displayed by the WHOHAS function can be voluminous depending upon the number of PERMITs defined. The DATA(option) keyword can be used to limit the display.

If, if you now issue the WHOHAS command for SYS, it will return the OWNER for SYS1, then all of the authorizations under the owner. Next, you will get the owner for SYS2 and all of those authorizations until the list is completed.

18.2.3 Obtaining Facility Access Information

Facility access information can be obtained by specifying a fully qualified facility name; no prefix or masking is supported.

Because facility information is not maintained as a resource, the amount of work required to obtain this information is dependent on the scope of the administrator requesting it. For a ZCA or lower, it is reasonably quick; however, for an SCA or an LSCA, it can require much longer to complete. Therefore, you might consider using batch processing to execute this command as an SCA. The amount of time required will be similar to the time required to execute the TSS LIST(ACIDS) DATA(BASIC) command.

If the administrator needed a list of all ACIDs that have the facility CICSPROD, the entry would be:

```
TSS WHOHAS FACility(CICSPROD)
```

18.3 Rules and Procedures

The following rules and procedures apply to all WHOHAS functions.

18.3.1 Authority

Resources

CA-Top Secret administrators must have RESOURCE(INFO) authority, via the ADMIN function, to obtain access information for all resources.

Facility

CA-Top Secret administrators must have FACILITY(facname) or FACILITY(ALL) authority, via the ADMIN function, to obtain access information for FACILITY.

Modes

The administrator must have MISC9(MODE) authority, via the ADMIN function, to obtain access information for MODES.

ACIDs

The administrator must have ACID(INFO) authority, via the ADMIN function, to obtain access information for job submission ACIDs.

18.3.2 Scope

Resources

Administrators may only obtain access information for resources or job ACIDs owned within their scope.

Facility

Administrators may only obtain FACILITY information for ACIDs within their scope.

Modes

Administrators may only obtain MODE information for ACIDs within their scope.

18.4 Applicable Keyword List

The following resource keywords may be used with the TSS WHOHAS command function. Refer to the chapter How to Use PERMIT/REVOKE and the Summary of Resources for descriptions, examples, and definitions of each keyword.

ABSTRACT	DB2DBASE	MGMTCLAS	TSAF	WAIT
ACID	DB2PKG	MODE	TSOACCT	WRITER
APPCPORT	DB2PLAN	NODES	TSOAUTH	
APPCSI	DB2STOGP	OPCMD	TSOPRFG	
APPCTP	DB2SYS	OPERCMDS	TSOPROC	
APPLICATION	DB2TABLE	OTRAN	TST	
AREA	DB2TABSP	PANEL	USRCLASS	
CAADMIN	DCSS	PPT	UR1/UR2	
CACCFDSN	DCT	PROGRAM	VMANAPPL	
CACCFMEM	DEVICES	PROPCNTL	VMCF	
CACMD	DIAGNOSE	PSB	VMDIAL	
CALIBMEM	DSNAME	PSFMPL	VMMACH	
CAREPORT	DLFCLASS	RECIPID	VMMDISK	
CATAPE	DLISEG	SCHEDULE	VMNODE	
CAVAPPL	FCT	SDSF	VMRDR	
CIMS	FIELD	SMESSAGE	VOLUME	
CPCMD	IBMFAC	SPI	VSELIB	
CPU	IBMGROUP	STATION	VSEPART	
DATABASE	IUCV	STORCLAS	VSEMEMBR	
DBD	JCT	SUBSCHEM	VSESLIB	
DB2	JESINPUT	SYSCONS	VSEUSER	
DB2BUFFP	JESJOBS	TARGET	VTAMAPPL	
DB2COLL	JESSPOOL	TERMINAL	VXDEVICE	
	JOBNAME		VXFILE	

Additional resource keywords may be used by an installation that has defined new resource classes in the RDT Record.

The following non-resource keyword may be used with the TSS WHOHAS command function. Refer to the chapter "How to Use ADDTO/REMOVE" for descriptions, examples, and definitions of this keyword.

FACILITY

18.5 DATA

Operating System: VSE, OS/390, and VM

Description: When issued with the TSS WHOHAS function, the DATA keyword is used to indicate how CA-Top Secret should interpret the resource name in question (i.e., should it be taken literally or treated as a mask).

TSS Commands: The following TSS commands can be used with the DATA keyword: **ADMIN, DEADMIN, LIST, WHOHAS**

Note: When used with the TSS WHOHAS function, the DATA keyword can only be used with the MASK, LITERAL and NOPREFIX operands. Conversely, these operands cannot be used when the DATA keyword is issued on a function other than WHOHAS.

Syntax:

```
TSS WHOHAS resclass(resname)
    DATA(LITERAL|MASK|NOPREFIX)
```

Data Types: The CA-Top Secret administrator may request any or all of the following DATA types on a TSS WHOHAS command. If no DATA options are specified, all matching prefixes will be displayed and any masks coded on the command will not be expanded.

Type	Causes CA-Top Secret To Display
LITERAL	Permits with resource names which match exactly the resource name name entered on the TSS WHOHAS command. Masking characters entered on the TSS WHOHAS command are treated as literals. Thus, permits with resource names containing masking characters are displayed only if they match exactly the resource name of the TSS WHOHAS command.
MASK	Permits which match the pattern coded in the resource name in the TSS WHOHAS command. This keyword should be used only if the resource name on the TSS WHOHAS command contains masking characters. **Note:** Not all resources support masking characters. Refer to Chapter 14 for more information.
NOPREFIX	Permits of either fully qualified resources (contained within single quotes) or of resource names equal in length to, or longer than the resource name in the TSS WHOHAS command. Permits with shorter resource names are not displayed. A masking character in the resource name of a permit is treated as a mask, but is always counted as one for the purpose of determining the length of that resource name. Thus, permits with resource names containing masking characters will be displayed provided that the resource names satisfy the length requirement for DATA(NOPREFIX).

Examples:

1. TSS WHOHAS without a DATA keyword shows all permits:

TSS WHOH DSN(SYS2.)

```
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.*                                          ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.++                                         ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARMLIB                                    ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARM                                       ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
```

2. TSS WHOHAS with DATA(LITERAL) shows all permits that match exactly the resource name entered on the TSS WHOHAS command:

TSS WHOH DSN(SYS2.PARM) DATA(LITERAL)

```
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.PARM                                       ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
```

TSS WHOH DSN(SYS2.*) DATA(LITERAL)

```
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.*                                          ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
```

3. TSS WHOHAS with DATA(MASK) shows all permits that match the masking pattern of the resource name entered on the TSS WHOHAS command:

TSS WHOH DSN(SYS2.*) DATA(MASK)

```
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.*                                          ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.++                                         ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARMLIB                                    ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARM                                       ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
```

4. TSS WHOHAS with DATA(NOPREFIX) shows all permits with prefixes that are equal to or longer than the resource name entered on the TSS WHOHA command. Shorter permits are ignored:

TSS WHOH DSN(SYS2.P) DATA(NOPREFIX)

```
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.*                                          ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.++                                         ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARMLIB                                    ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARM                                       ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
TSS WHOH DSN(SYS2.PARM) DATA(NOPREFIX)
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.PARMLIB                                    ACID(USER0
ACCESS  = READ
XAUTH     = SYS2.PARM                                       ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
TSS WHOH DSN(SYS2.PARMLIB) DATA(NOPREFIX)
DATASET    = SYS2.                                          OWNER(DEPT2
XAUTH     = SYS2.PARMLIB                                    ACID(USER0
ACCESS  = READ
TSS0300I  WHOHAS   FUNCTION SUCCESSFUL
```

Chapter 19. How to Use WHOOWNS

This chapter presents the standard formats and rules which govern use of the WHOOWNS function. There are no detailed reference pages for WHOOWNS. Refer to Summary of Resources for more information about owned resource keywords.

19.1 Purpose

Given the proper administrative authority, the TSS administrator may enter TSS WHOOWNS functions to display the ACID that owns a specific resource, or the ACIDs that own each resource of a specific type.

Additional resource keywords may be used by an installation that has defined new resource classes in the RDT Record.

19.2 Entry Methods

CA-Top Secret administrators may enter TSS WHOOWNS command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

Note: Only one resource keyword and prefix may be specified per command.

19.2.1 Command Syntax

The following example shows how WHOOWNS command functions are entered freeform at an online terminal.

```
TSS WHOOWNS keyword(prefix|TSS mode|*)
                   1       2        3
```

Field	Description
1	If information is required for resource ownership, enter the TSS keyword for that resource. If information is required for a security mode, enter MODE.
2	Enter the specific resource prefix, or CA-Top Secret mode for which ownership identification is required.
3	Enter an asterisk (*) to obtain a listing of all owners for all resources of this type.

19.2.1.1 Sample Entry

To determine who owns the SFT.CICS. data set, the auditor enters:

```
TSS WHOOWNS DSN(SFT.CICS)
```

CA-Top Secret will respond by displaying all ACIDs that have ownership of the data set, and each ACID's access level to the data set.

```
RESOURCE      =       SFT.CICS.                    OWNER(SFTDEPT)
TSS0300I WHOOWNS FUNCTION SUCCESSFUL
```

In the preceding example, CA-Top Secret displays ownership information for all data sets prefixed by SFT.CICS.

To determine the owners of all of the division's data sets, the VCA would enter:

```
TSS WHOOWNS DSN(*)
```

19.3 Rules and Procedures

The following rules and procedures apply to all WHOOWNS functions.

19.3.1 Authority

Resources

CA-Top Secret administrators must have RESOURCE(INFO) authority, via the ADMIN function, to identify owners of resources.

The administrator must have MISC1(GENERIC) authority, via the ADMIN function, to use the WHOOWNS keyword(*) command function.

19.3.2 Scope

Administrators may obtain information only for resources owned within their scope.

19.3.3 WHOOWNS Display

When WHOOWNS functions are entered for a resource, CA-Top Secret will display all resource prefixes which generically match the requested resource prefix. All resources will be displayed in alphabetical order.

19.3.4 Modes

The administrator must have MISC9(MODE) authority, via the ADMIN function, to obtain ownership information for MODES.

19.4 Applicable Keyword List

The following resource keywords are used with the TSS WHOOWNS function. Refer to the How to Use PERMIT/REVOKE and Summary of Resources reference pages for descriptions, examples, and definitions of each keyword.

ABSTRACT	DB2STOGP	NODES	TSOPRFG
APPCPORT	DB2SYS	OPCMD	TSOPROC
APPCSI	DB2TABLE	OPERCMDS	TST
APPCTP	DB2TABSP	OTRAN	USRCLASS
APPLICATION	DCSS	PANEL	UR1/UR2
AREA	DCT	PPT	VMCF
CACMD	DEVICES	PROGRAM	VMDIAL
CAPCLU	DIAGNOSE	PSB	VMMACH
CIMS	DSNAME	PSFMPL	VMMDISK
CPCMD	FCT	SDSF	VMNODE
CPU	FIELD	SMESSAGE	VMRDR
DATABASE	IBMFAC	SPI	VOLUME
DBD	IBMGROUP	STORCLAS	VTAMAPPL
DB2	IUCV	SUBSCHEM	VXDEVICE
DB2BUFFP	JCT	SYSCONS	VXFILE
DB2DBASE	JESJOBS	TARGET	WAIT
DB2COLL	JESSPOOL	TERMINAL	WRITER
DB2PKG	MGMTCLAS	TSOACCT	
DB2PLAN	MODE	TSOAUTH	

Chapter 20. How to Use WHOAMI

This chapter presents the standard formats and rules governing the use of the WHOAMI function. There are no detailed reference pages for the WHOAMI function.

20.1 Purpose

Any ACID defined to CA-Top Secret may enter WHOAMI at an online terminal to display their current security environment.

20.1.1 WHOAMI Display

CA-Top Secret provides the following information in response to the WHOAMI command function:

- ACID
- ACID TYPE (i.e. USER, DCA, VCA, ZCA, LSCA, SCA)
- Security Mode (DORMANT, WARN, IMPL, FAIL)
- Facility
- Terminal Name
- Lock Time
- Logging Options
- Installation Data (OS/390 only)
- Security Bypass Attributes (NOVOLCHK, NODSNCHK, etc.)
- Current identification of CPU
- If the ACID is undefined
- If the virtual machine is currently running under a surrogate ACID. (VM only)

20.2 Entry Methods

Users may enter TSS WHOAMI command functions freeform onto an entry screen, or as input to the batch utility TSSCMNDB.

20.2.1 Command Syntax

The basic entry for the WHOAMI function is:

```
TSS WHOAMI
```

Note: The TSS WHOAMI command function cannot be routed through the security network using CPF.

Chapter 21. Command Propagation Facility

This chapter presents the command syntax and rules governing the use to the Command Propagation Facility (CPF).

21.1 Keywords Used With CPF

Once the appropriate CPF control options are set, the new CPF keywords **— TARGET, WAIT** and **DEFNODES** — can be used with the TSS command to specify which CA-Top Secret nodes a command will be propagated to and how the local node will process that command.

The TARGET Keyword: The TARGET keyword identifies the nodes to which a command should be routed. TARGET is used to override the CPFTARGET control option which sets up default routing instructions for the entire installation.

There are four different ways of specifying an operand for TARGET. They are:

TARGET(*)	Causes the command to be transmitted to the local node and to all nodes defined in the CPFNODES control option.
TARGET(=)	Restricts command execution to the local node only.
TARGET(node1,node2,...)	Identifies each node to which a command is transferred.
TARGET(n...n*,n...n*,...)	Causes all commands to be transmitted to the CPF nodes whose names begin with the indicated string. The string can range from one to seven characters.

In the event CPF is active and a command is issued **without** specifying a TARGET, CA-Top Secret will propagate the command according to the instructions set by CPFTARGET. If CPFTARGET is set to AUTO, the command will be routed based on the DEFNODE keyword.

The WAIT Keyword: The WAIT keyword is used to indicate whether or not the terminal on the CPF node issuing the command is locked until a response is received from the targeted node(s). WAIT is used to override the default set by the CPFWAIT control option.

There are two values that can be specified for the WAIT keyword. They are:

WAIT(Y) Selects synchronous processing whereby a response will be sent to the terminal where the command was issued. Until a response is received that terminal will be locked. When this type of processing is in effect, the CPF Recovery File is not used to save transmitted commands.

WAIT(N) Selects asynchronous processing whereby a response is returned only to the CPF Journal File for that node. Consequently, the terminal keyboard will be freed up as soon as the command is accepted. When this type of processing is in effect, the CPF Recovery File **is** used to save transmitted commands. Commands targeted only for the local machine, however, are **not** saved.

To better understand how TARGET and WAIT are used with a command, consider the following examples:

```
TSS WHOHAS  DSN(PAYROLL.)  TARGET(CPU1,CPU2,=)  WAIT(Y)
```

displays the users on CPU1, CPU2 and the local node that have access to the PAYROLL dataset prefix.

```
TSS ADD(DEPT01)  DSN(SYS1.)  TARGET(R*)  WAIT(Y)
```

causes all data sets beginning with SYS1. that are added to DEPT01 to be transmitted to all nodes whose names start with R.

The DEFNODES Keyword: The DEFNODES keyword is used to maintain a list of default routing nodes for an individual ACID. The only time that this list is consulted is when:

1. The CPFTARGET control option is set to AUTO **and**
2. no TARGET is specified when the command is issued.

Unlike the TARGET and WAIT keywords, the DEFNODES keyword is only used when the list itself is being designated (either through the initial TSS CREATE for the ACID or through a subsequent TSS ADD) or updated. Otherwise, the list is consulted by default when **both** of the above conditions apply.

Note: If CPFTARGET is set to AUTO and no TARGET is specified but the ACID has no DEFNODES, the command will propagate to those nodes identified by the CPFNODES control option.

The DEFNODES list can be assigned to an ACID from the initial CREATE statement or it can be ADDed later. Later, the list can be maintained using TSS REPLACE (which completely deletes the current list), TSS REMOVE (which selectively deletes certain nodes on that list) and TSS ADD (which selectively adds certain nodes to that list).

In order to display a user's DEFNODES, the administrator needs to specify TSS LIST DATA(DEFNODES).

To better understand the implications of DEFNODES lists, consider the following examples:

The administrator responsible for the Accounting Department needs to define a new user for that department. This new user will require an initial DEFNODES list that includes: New York, Chicago and Detroit. The administrator enters:

```
TSS CREATE(ACCT01) NAME('ACCT USER') FAC(VM,TSO) PAS(xxxx)
    TYPE(USER) TARGET(NYC,CHI,DET)
```

Note: The administrator also has the option of using a Model ACID, which would contain all the default access rights and restrictions — including DEFNODES — for all users in the Accounting Department. In this case, he or she would then specify the USING keyword along with the TSS CREATE.

To add DEFNODES Baltimore and Atlanta to that user, the administrator enters:

```
TSS ADD(USER01) DEFNODES(BAL,ATL)
```

The list for USER01 now consists of NYC, CHI, DET, BAL, ATL.

To remove Houston from the list, the administrator enters:

```
TSS REM(USER01) DEFNODES(HOU)
```

To completely replace the current list with a new list consisting of Houston and Boston, the administrator enters:

```
TSS REP(USER01) DEFNODES(HOU,BOS)
```

For more information on implementing CPF, refer to the *User Guide*

21.2 Applicable Keyword List

The following resource keywords may be used with the CPF command function.

```
DEFNODES
TARGET
WAIT
```

21.3 DEFNODES

Operating System: VSE, OS/390, and VM

Description: To define a list of default remote routing nodes for an ACID. An ACID's DEFNODES are only consulted when the CPFTARGET control option is set to AUTO and no TARGET has been specified on a command.

TSS Commands: The following TSS commands can be used with the DEFNODES keyword: **ADDTO, CREATE, REMOVE, REPLACE.**

Syntax:

```
TSS ADD(acid) DEFNODES(oper,oper,...)
```

You can specify up to 5 nodes per command.

Authority: TSS administrators must have ACID(DEFNODES) authority, via the TSS ADMIN function, to replace the default CPF node list for ACIDs within their scope.

Types: The DEFNODES keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

To define the default routing nodes of NYC, CHI and DET for the USER01 ACID, the administrator would enter:

```
TSS ADD(USER01) DEFNODES(NYC,CHI,DET)
```

Therefore, if a command is issued against USER01, under the proper conditions (CPFTARGET set to AUTO and no TARGET specified on the command), that command will automatically be propagated to the NYC, CHI and DET nodes.

To completely remove this list, the administrator would enter:

```
TSS REMOVE(USER01) DEFNODES(NYC,CHI,DET)
```

21.4 TARGET

Operating System: VSE, OS/390, and VM

Description: Specifies to which CA-Top Secret nodes a command will be propagated.

TSS Commands: The following TSS commands can be used with the TARGET keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS, RENAME, REPLACE.**

Syntax:

```
TSS function(acid) keyword(s) TARGET(node,node,...)
```

A description of your options for specifying the TARGET nodes is included at the beginning of this chapter.

Authority: CA-Top Secret administrators must have MISC2(TARGET) authority, via the TSS ADMIN function to use the TARGET keyword to override the default CPF routing command. Refer to the *Implementation Guides* for VSE, OS/390, and VM for further information regarding CPF.

Types: The TARGET keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

21.5 WAIT

Operating System: VSE, OS/390, and VM

Description: Indicates whether a TSS command should be processed synchronously or asynchronously.

TSS Commands: The following TSS commands can be used with the WAIT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS, RENAME, REPLACE.**

Syntax:

```
TSS function(acid) keyword(s) WAIT(Y|N)
```

where:

Y specifies synchronous processing (CPF will wait for a response from all remote nodes before processing resumes).

N Specifies asynchronous processing (CPF will not wait for a response).

Authority: No explicit authority is required. For CPF routed commands, the WAIT keyword indicates whether the command should be processed synchronously or asynchronously. This option overrides the default CPFWAIT control option setting.

Types: The WAIT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Chapter 22. Summary of Resources

This chapter provides detailed reference pages for each resource class. The keywords are arranged in alphabetical order and include: the operating systems affected, a clear and concise description of each keyword, what TSS command functions can be used with that keyword, and technical information, as well as examples for the ADDTO/REMOVE and PERMIT/REVOKE command functions.

All resources in this chapter (with the exception of data sets, minidisks, DB2 databases, DB2 tables, and DB2 table spaces) honor the NONGENERIC attribute which can protect a resource by its fully qualified name rather than its prefix.

22.1 Resources

The following is a list of resources discussed in this chapter:

ABSTRACT	FIELD	SUBSCHEM	VSESLIB
ACID	IBMFAC	SURROGAT	VSEUSER
AREA	JCT	TERMINAL	
CACMD	NODES	TST	
CPU	OTRAN	UR1/UR2	
DBD	PANEL	USRCLASS	
DCT	PPT	VOLUME	
DLISEG	PROGRAM	VSELIB	
DSNAME	PSB	VSEPART	
FCT	SPI	VSEMEMBR	

22.1.1 Resource Class: ABSTRACT

Operating System: VSE and OS/390

Description: Used to secure installation-defined resource classes.

TSS Commands: The following TSS commands can be used with the ABSTRACT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) ABStract(oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have ABSTRACT(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of ABSTRACT resources from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The ABSTRACT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) ABSTRACT(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have ABSTRACT(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to ABSTRACT resources that are owned within their scope.

Access Controls: The administrator can use any of the following methods to control access to ABSTRACT resources: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The ABSTRACT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

An organization wants to protect linkage editor setcode by using the CA-Top Secret reorganized name of AC1. AC1 will be owned by the Corporate Department by entering:

```
TSS ADD(CORPORAT) ABS(AC1)
```

The administration may now PERMIT access to users or profiles that require access.

Ownership can be removed by entering:

```
TSS REMOVE(CORPORAT) ABS(AC1)
```

TSS PERMIT/REVOKE

The administrator wants to permit users in the Technical Services Department to access AC1 on Fridays only:

```
TSS PERMIT(TECHPROF) ABS(AC1) DAYS(FRIDAY)
```

The administrator wants to permit users in the Technical Services Department to access XDT98000:

```
TSS PERMIT(TECHPROF) ABS(XDT98000)
```

To revoke access, the administrator enters:

```
TSS REVOKE(TECHPROF) ABS(AC1)
```

22.1.2 Resource Class: ACID

Operating System: VSE, OS/390, and VM

Description: Used to secure special ACcessor IDs, such as those used to submit jobs.

TSS Commands: The following TSS commands can be used with the ACID keyword: **PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) ACID(acid)
```

ACID length — 1-8 characters

Capacity of list — 1-5 ACIDs per TSS command.

Authority: The administrator must have ACID(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE ACIDs that are owned within their scope.

Access Controls: The administrator can use any of the following methods to control the use of job submission ACIDs: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The ACID keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect the ACID, AUDITING, the administrator assigns ownership to the Payroll Department by entering:

```
TSS ADD(PAYDEPT) ACID(AUDITING)
```

To remove ownership of the ACID, the administrator enters:

```
TSS REM(PAYDEPT) ACID(AUDITING)
```

22.1.3 Resource Class: AREA

Operating System: VSE and OS/390

Description: Used to secure CA-IDMS database areas.

TSS Commands: The following TSS commands can be used with the AREA keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) AREA(prefixes(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have AREA(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of AREAs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The AREA keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) AREA(prefix(es)) ACCESS(access levels)
```

Prefix length — 1-44 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have AREA(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to AREAs that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **NONE, READ, ALL, UPDATE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to AREA resources: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The AREA keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Personnel Department ownership of the AREA for the Corporate Personnel Database (PERDB), the administrator enters:

```
TSS ADD(PERSDP) AREA(PERDB)
```

Ownership can be removed by entering:

```
TSS REMOVE(PERSDP) AREA(PERDB)
```

TSS PERMIT/REVOKE

To permit USER01 to have ALL access to PAYFILE, the administrator enters:

```
TSS PERMIT(USER01) AREA(PAYFILE) ACCESS(ALL)
```

To revoke USER01's access to PAYFILE, the administrator enters:

```
TSS REVOKE(USER01) AREA(PAYFILE)
```

22.1.4 Resource Class: CACMD

Operating System: VSE, OS/390, and VM

Description: Used to secure other CA Product commands and programs.

Refer to the CA product specific documentation for descriptions of CACMD names used by the individual product.

TSS Commands: The following TSS commands can be used with the CACMD keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) CACMD(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have CACMD(OWN) authority via the TSS ADMIN function, to ADD or REMOVE authority to control access of CA product specific commands owned within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The CACMD keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) CACMD(prefix(es))
```

Prefix length — 1-44 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have CACMD(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE the authority to CA product specific commands, functions and programs.

Access Controls: The administrator can use any of the following methods to control access to CACMD resources: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The CACMD keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

PRDCNTL would like ownership of the CA-1 command named LOINQUIR, the administrator enters:

```
TSS ADD(PRDCNTL) CACMD(LOINQUIR)
```

Ownership can be removed by entering:

```
TSS REMOVE(PRDCNTL) CACMD(LOINQUIR)
```

TSS PERMIT/REVOKE

To permit ACID, TAPELIB, the ability to use the CA-1 command, CATALOG, the administrator enters:

```
TSS PERMIT(TAPELIB) CACMD(CATALOG)
```

To enable all users to issue the CA-1 command INQUIRE, the administrator enters:

```
TSS PERMIT(ALL) CACMD(INQUIRE)
```

22.1.5 Resource Class: CPU

Operating System VSE, OS/390, and VM

Description: Used to secure an ACID's access to a particular CPU. Also used to force an ACID to enter the system only through a particular CPU.

TSS Commands: The following TSS commands can be used with the CPU keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) CPU(smfid|id from DMKSYS)
```

Prefix length — 1-4 characters for VSE and OS/390, 1-8 characters for VM

Capacity of list — 1-5 CPU IDs per TSS command.

Authority: The administrator must have CPU(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of CPU from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The CPU keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) CPU(smfid)
```

Prefix length — 1-4 characters for OS/390, 1-8 characters for VM

Capacity of list — 1-5 CPU IDs per TSS command.

Authority: The administrator must have CPU(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to CPUs that are owned within their scope.

Access Controls: The administrator can use any of the following methods to control access to CPUs: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The CPU keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect the CPU, SYSA, the administrator assigns ownership to Department 01 by entering:

```
TSS ADD(DEPT01) CPU(SYSA)
```

The administrator may now PERMIT access to users or to profiles that require access.

The administrator may remove ownership by entering:

```
TSS REMOVE(DEPT01) CPU(SYSA)
```

TSS PERMIT/REVOKE

To permit the day shift to execute BATCH jobs on CPU-SYSA, the administrator enters:

```
TSS PERMIT(DAYPROF) CPU(SYSA) FAC(BATCH)
```

To revoke access to SYSA, the administrator enters:

```
TSS REVOKE(DAYPROF) CPU(SYSA)
```

22.1.6 Resource Class: DBD

Operating System: VSE

Description: Used to secure a VSE DL/I database descriptor name.

TSS Commands: The following TSS commands can be used with the DBD keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) DBD(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 DBD names per TSS command

Authority: The administrator must have DBD(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of DBD names from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The DBD keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) DBD(prefixes) ACCESS(access-levels)
```

Prefix length — 1-8 characters per prefix

Capacity of list — 1-5 DBD names or prefixes per TSS command.

Authority: The administrator must have DBD(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to DBD names that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, DELETE, REPLACE, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to DBD names: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The DBD keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Personnel Department ownership of the DBD resource for the corporate personnel database (PERSFILE), the administrator enters:

```
TSS ADD(PERSDPT) DBD(PERSFILE)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PERSDPT) DBD(PERSFILE)
```

TSS PERMIT/REVOKE

To permit user PERSF1 to update DBDs used by the Personnel Department, the administrator enters:

```
TSS PERMIT(PERSF1) DBD(PERS44,PERS51,PERS07) ACCESS(U)
```

To revoke access, the administrator enters:

```
TSS REVOKE(PERSF1) DBD(PERS44,PERS51)
```

Now, user PERSF1 may only update PERS07.

22.1.7 Resource Class: DCT

Operating System: VSE and OS/390

Description: Used to secure transient data entries in the CICS Destination Control l Table (DCT).

TSS Commands: The following TSS commands can be used with the DCT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) DCT(oper,oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 CICS destinations per TSS command

Authority: The administrator must have DCT(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of DCTs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The DCT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) DCT(prefix(es)) ACCESS(access levels)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have DCT(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to DCTs that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, ALL, FEOV, NONE, PURGE, READ, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to DCTs: **Expiration, Facility, Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The DCT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect a CICS destination, the administrator assigns ownership to the Corporate Level Division (CORPCICS) by entering:

```
TSS ADD(CORPCICS) DCT(PRT6)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(CORPCICS) DCT(PRT6)
```

TSS PERMIT/REVOKE

To permit a user full access to the installation's DCTs, the administrator enters:

```
TSS PERMIT(USER05) DCT(DCT1) ACCESS(ALL)
```

To revoke access the administrator enters:

```
TSS REVOKE(USER05) DCT(DCT1)
```

22.1.8 Resource Class: DLISEG

Operating System: VSE

Description: Used to secure a VSE DL/I database segment.

TSS Commands: The following TSS commands can be used with the DLISEG keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) DLISEG(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 segment names per TSS command

Authority: The administrator must have DLISEG(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of segments from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The DLISEG keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) DLISEG(prefixes) ACCESS(access-levels)
```

Prefix length — 1-8 characters per prefix

Capacity of list — 1-5 segment names or prefixes per TSS command.

Authority: The administrator must have DLISEG(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to segments that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, DELETE, REPLACE, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to segment names: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The DLISEG keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of the segment called PERSEG to the Personnel Department, the administrator enters:

```
TSS ADD(PERSDPT) DLISEG(PERSEG)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PERSDPT) DLISEG(PERSEG)
```

TSS PERMIT/REVOKE

To permit user PERSF1 to update the segments used by the Personnel Department, the administrator enters:

```
TSS PERMIT(PERSF1) DLISEG(PERSEG) ACCESS(UPDATE)
```

To revoke access, the administrator enters:

```
TSS REVOKE(PERSF1) DLISEG(PERSEG)
```

22.1.9 Resource Class: DSNAME

Operating System: VSE, OS/390, and VM

Description: Used to secure data sets. You can identify each data set separately or in groups of like-named data sets (using generic prefixing and masking techniques).

TSS Commands: The following TSS commands can be used with the DSNAME keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) DSName(oper,...)
```

Prefix length — 2-26 characters

Capacity of list — 1-5 data set names or prefixes per TSS command

Generic prefixing allows the administrator to group a set of similar data sets together, and define them by one generic prefix. The chapter on "How to Use PERMIT/REVOKE," provides excellent guidelines and examples for preparing a resource naming standard.

Authority: The administrator must have DSNAME(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of data sets from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The DSNAME keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) DSName(prefix(es)) ACCESS(access levels)
```

Prefix length — 2-44 characters

Capacity of list — 1-5 data sets names, prefixes, or masks per TSS command.

Note: A fully qualified data set name can be PERMITted to an ACID by enclosing in single quotation marks. This will indicate that it is defined to CA-Top Secret, not as a prefix, but by its fully qualified name.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, CREATE, CONTROL, FETCH, NONE, READ, SCRATCH, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to data sets: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Masking: Data set masking is another method of reducing the number of data set definitions to implement widespread data set protection. Refer to the chapter on "How to Use PERMIT/REVOKE" for a discussion on the five types of masks used with data sets.

Types: The DSNAME keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Inventory Department (INVDEPT) ownership of a data set known as UNSOLD.INV.MASTER.FILE, the administrator enters:

```
TSS ADD(INVDEPT) DSN('UNSOLD.INV.MASTER.FILE')
```

The administrator may remove ownership by entering:

```
TSS REMOVE(INVDEPT) DSN('UNSOLD.INV.MASTER.FILE')
```

TSS PERMIT/REVOKE

The administrator can have USER01 access any data set prefixed by SFT by entering:

```
TSS PERMIT(USER01) DSN(SFT.)
```

This eliminates the need to permit access to 'SFT.IMS.PROD' and 'SFT.IMS.SCEDS' —refer to the chapter on "How to Use PERMIT/REVOKE" for examples on how to use the different types of masks used with data sets.

To revoke USER01's access to all data sets beginning with the prefix SFT the administrator enters:

```
TSS REVOKE(USER01) DSN(SFT.)
```

22.1.10 Resource Class: FCT

Operating System: VSE and OS/390

Description: Used to secure File Control Table entries (dd names) in CICS.

TSS Commands: The following TSS commands can be used with the FCT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) FCT(oper,oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 FCT prefixes per TSS command

Authority: The administrator must have FCT(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of FCTs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The FCT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) FCT(prefix(es)) ACCESS(access levels)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have FCT(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to FCTs that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **SET, INQUIRE, ALL, BROWSE, DELETE, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to FCTs: **Expiration, Facility, PPT Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The FCT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of an FCT prefix to a department ACID, the administrator enters:

```
TSS ADD(PAYDEPT) FCT(PAY)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PAYDEPT) FCT(PAY)
```

TSS PERMIT/REVOKE

To permit a group of users to read and browse two CICS files, the administrator enters:

```
TSS PERMIT(PERPROF) FCT(SKILLS,PENSION) ACCESS(READ,BROWSE)
```

To revoke access the administrator enters:

```
TSS REVOKE(PERPROF) FCT(SKILLS,PENSION)
```

22.1.11 Resource Class: FIELD

Operating System: VSE and OS/390

Description: Used to secure installation-defined database fields.

TSS Commands: The following TSS commands can be used with the FIELD keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) FIEld(oper,oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 FIELD prefixes per TSS command

Authority: The administrator must have FIELD(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of FIELDs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Protection: Fields are not automatically protected by CA-Top Secret, even when defined via the ADDTO command function. An application program must perform the security check by calling CA-Top Secret via FRACHECK or the application high-level language interface.

Types: The FIELD keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) FIEld(prefix(es)) ACCESS(access levels)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have FIELD(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to FIELDs that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to FIELDs: **Expiration, Facility, Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The FIELD keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect a group of fields for a CICS application, the administrator enters:

```
TSS ADD(DEPTC) FIE(A100,A200,A300)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(DEPTC) FIE(A100,A200,A300)
```

TSS PERMIT/REVOKE

To permit CICS clerks to update fields daily from 8:00 am until 5:00 pm, but only through a specific CICS application program (on behalf of a transaction), the administrator enters:

```
TSS PERMIT(PRFCLRK) FIE(A1006,A3002) TIMES(08,17) DAYS(WEEKENDS)
    PRIVPGM(ISPTASK1) ACCESS(U)
```

To revoke access the administrator enters:

```
TSS REVOKE(PRFCLRK) FIE(A1006,A3002)
```

22.1.12 Resource Class: IBMFAC

Operating System: VSE and OS/390

Description: Equivalent resource class to RACF class FACILITY. Used to determine who has ownership or control over catalog, IDCAMS, FMS, DFDSS and other IBM Facilities.

TSS Commands: The following TSS commands can be used with the IBMFAC keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) IBMFAC(facility,...)
```

Prefix length — 1-8 characters

Capacity of list — 5 facilities per TSS command

Authority: The administrator must have IBMFAC(OWN) authority via the TSS ADMIN function, to protect user access to IBM facilities. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The IBMFAC keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) IBMFAC(facility,...)
```

Prefix length — 1-44 characters

Capacity of list — 5 facilities per TSS command.

Authority: The administrator must have IBMFAC(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to IBM facilities that are owned within their scope.

Access Controls: The administrator can use any of the following methods to control access to IBMFAC: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to NONE access.

Types: The IBMFAC keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To add an IBMFAC of IDC.DIAG, the administrator enters:

```
TSS ADD(DEPT02) IBMFAC(IDC.DIAG)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(DEPT02) IBMFAC(IDC.DIAG)
```

TSS PERMIT/REVOKE

To allow an ACID to use IBMFAC, the administrator enters:

```
TSS PERMIT(DEPT02) IBMFAC(facility,...)
```

To revoke access the administrator enters:

```
TSS REVOKE(DEPT02) IBMFAC(facility,...)
```

22.1.13 Resource Class: JCT

Operating System: VSE and OS/390

Description: Used to secure entries in the CICS Journal Control Table (JCT).

TSS Commands: The following TSS commands can be used with the JCT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) JCT(oper,oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 JCT prefixes per TSS command

Authority: The administrator must have JCT(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of JCTs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The JCT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) JCT(prefix(es)) ACCESS(access levels)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 JCT prefixes per TSS command.

Authority: The administrator must have JCT(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to resources that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, ALL, NONE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to JCTs: **Expiration, Facility, PPT Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The JCT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of a JCT, the administrator adds the JCT to Department 1 by entering:

```
TSS ADD(DEPT1) JCT(J03)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(DEPT1) JCT(J03)
```

TSS PERMIT/REVOKE

To permit a user all access to a predefined journal through the CICSTEST facility, the administrator enters:

```
TSS PERMIT(GKM75) JCT(JC03) ACCESS(ALL) FAC(CICSTEST)
```

To revoke access the administrator enters:

```
TSS PERMIT(GKM75) JCT(JC03)
```

22.1.14 Resource Class: NODES

Operating System: OS/390 and VM

Description: Used to control incoming NJE jobs and SYSOUT, and optionally, to assign a userid as the owner of the job or SYSOUT on this system.

TSS Commands: The following TSS commands can be used with the NODES keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) NODES (node,...)
```

Prefix length — 2-26 characters

Capacity of list — 1-5 nodenames or prefixes per TSS command

Generic prefixing allows the administrator to group a set of similar nodes together, and define them by one generic prefix. The chapter on "How to Use PERMIT/REVOKE," provides excellent guidelines and examples for preparing a resource naming standard.

Authority: The administrator must have NODES(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of nodes from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The NODES keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax

```
TSS PER(acid) NODES(node(s)) ACCESS(levels) [NJEACID(acid)]
```

Prefix length — 2-44 characters

Capacity of list — 1-5 nodes per TSS command.

Note: A fully qualified node can be PERMITted to an ACID by enclosing in single quotation marks. This will indicate that it is defined to CA-Top Secret, not as a prefix, but by its fully qualified name.

Access Levels: The administrator can specify any or all of the following access levels: **CONTROL, NONE, READ, UPDATE.** If ACCESS is not specified, CA-Top Secret defaults to ALL access.

Access Controls: The administrator can use any of the following methods to control access to data sets: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Masking: Node masking is another method of reducing the number of node definitions to implement widespread node protection. Refer to the chapter on "How to Use PERMIT/REVOKE" for a discussion on the five types of masks.

Types: The NODES keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give USER01 ownership of jobs submitted from ALPHA2.USERJ*, the administrator enters:

```
TSS ADD(USER01) NODES(ALPHA.USERJ*)
```

The administrator may remove ownership by entering:

```
TSS REM(USER01) NODES(ALPHA.USERJ*)
```

TSS PERMIT/REVOKE

If node ALPHA is not allowed to execute jobs on node ALPHA.USERJ, the administrator enters:

```
TSS PER(ALL) NODES(ALPHA.USERJ.) ACCESS(NONE)
```

If an exception is to be made for userid X123, the administrator enters:

```
TSS PER(ALL) NODES(ALPHA.USERJ.X123) ACCESS(UPDATE)
```

If any job submitted from node BETA is to run without any password checking, the administrator enters:

```
TSS PER(ALL) NODES(BETA.USERJ) ACCESS(CONTROL)
```

22.1.15 Resource Class: OTRAN

Operating System: VSE and OS/390

Description: Used to secure ownable transactions for CICS, IMS, and CA-IDMS that are protected by OTRAN.

TSS Commands: The following TSS commands can be used with the OTRAN keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) OTRAN(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 transaction per TSS command

Authority: The administrator must have OTRAN(OWN) authority via the TSS ADMIN function, to ADD or REMOVE OTRAN from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The OTRAN keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) OTRAN(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 transactions per TSS command

Authority: The administrator must have OTRAN(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to transactions that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, EXECUTE, ALL, NONE.** If ACCESS is not specified, CA-Top Secret defaults to EXECUTE access.

Access Controls: The administrator can use any of the following methods to control access to the OTRAN resource: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The OTRAN keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect the CICS transaction, PAYR, the administrator assigns ownership to the Payroll Department (PAYDEPT)by entering:

```
TSS ADD(PAYDEPT) OTRAN(PAYR)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PAYDEPT) OTRAN(PAYR)
```

TSS PERMIT/REVOKE

To permit an ACID, PAYPROG, to access the transaction PA01 through CICS only, the administrator enters:

```
TSS PERMIT(PAYPROG) OTRAN(PA01) FAC(CICS)
```

To revoke access the administrator enters:

```
TSS REVOKE(PAYPROG) OTRAN(PA01)
```

22.1.16 Resource Class: PANEL

Operating System: VSE, OS/390, and VM

Description: Used to secure authority to ISPF, CICS and REXX panels.

Refer to the CA product specific documentation for descriptions and PANEL names used by the individual product.

TSS Commands: The following TSS commands can be used with the PANEL keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) PANEL(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have PANEL(OWN) authority via the TSS ADMIN function, to ADD or REMOVE authority to control access to CA product specific panels within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The PANEL keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) PANEL(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have PANEL(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE the authority to CA product specific panels within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, NONE, READ, WRITE, UPDATE, CONTROL, SCRATCH.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to PANEL resources: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The PANEL keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

PRDCNTL would like ownership of the CA-1 panel named LOABCDE, the administrator enters:

```
TSS ADD(PRDCNTL) PANEL(LOABCDE)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PRDCNTL) PANEL(LOABCDE)
```

TSS PERMIT/REVOKE

To permit ACID, TAPELIB, the ability to use the READ functions of CA-1 panel, LOABCDE, the administrator enters:

```
TSS PERMIT(TAPELIB) PANEL(LOABCDE) ACCESS(READ)
```

To revoke access the administrator enters:

```
TSS REVOKE(TAPELIB) PANEL(LOABCDE) ACCESS(NONE)
```

22.1.17 Resource Class: PPT

Operating System: VSE and OS/390

Description: Used to secure program entries in the CICS Program Propagation Table (PPT).

TSS Commands: The following TSS commands can be used with the PPT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) PPT(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 CICS PPTs per TSS command

Authority: The administrator must have PPT(OWN) authority via the TSS ADMIN function, to ADD or REMOVE PPTs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The PPT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) PPT(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have PPT(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to transactions that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, EXECUTE, ALL, NONE, UPDATE.** If ACCESS is not specified, CA-Top Secret defaults to EXECUTE access.

Access Controls: The administrator can use any of the following methods to control access to PPTs: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The PPT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of a PPT name, CP12388, to a department, the administrator enters:

```
TSS ADD(CICSCORP) PPT(CP12388)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(CICSCORP) PPT(CP12388)
```

TSS PERMIT/REVOKE

To permit a test CICS user access to a program, APPLPROG, the administrator enters:

```
TSS PERMIT(GKM75) PPT(APPLPROG)
```

To revoke access the administrator enters:

```
TSS REVOKE(GKM75) PPT(APPLPROG)
```

22.1.18 Resource Class: PROGRAM

Operating System: VSE and OS/390

Description: Used to secure system programs and utilities.

TSS Commands: The following TSS commands can be used with the PROGRAM keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) PROGram(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have PROGRAM(OWN) authority via the TSS ADMIN function, to ADD or REMOVE PROGRAMs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Protection: Programs which can be protected include: TSO commands, and those specified by 'EXEC PGM=program' in JCL statements; all programs executed internally via CALL, LINK, LOAD, XCTL, ATTACH, EXECUTE and CA-IDMS programs.

Types: The PROGRAM keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) PROGram(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes or names per TSS command

Authority: The administrator must have PROGRAM(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to transactions that are owned within their scope.

Access Controls: The administrator can use any of the following methods to control access to PROGRAMS: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The PROGRAM keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect the use of all system utilities, IEH5000 and IEASSST, the administrator assigns ownership to the Corporate Department ACID, and can subsequently PERMIT restricted access to users or profiles by entering:

```
TSS ADD(CORPRAT) PROG(IEH,IEASSST)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(CORPRAT) PROG(IEH,IEASSST)
```

TSS PERMIT/REVOKE

To permit use of the SUPERZAP program from Batch only, the administrator enters:

```
TSS PERMIT(SYSAU2) PROG(IMASPZAP) FAC(BATCH)
```

To revoke access the administrator enters:

```
TSS REVOKE(SYSAU2) PROG(IMASPZAP) FAC(BATCH)
```

22.1.19 Resource Class: PSB

Operating System: VSE

Description: Used to secure VSE DL/I Program Specification Block.

TSS Commands: The following TSS commands can be used with the PSB keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) PSB(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 PSB names per TSS command

Authority: The administrator must have PSB(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of PSB names from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The PSB keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) PSB(prefixes) ACCESS(access-levels)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 PSB names or prefixes per TSS command

Authority: The administrator must have PSB(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to PSB names that are within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, DELETE, REPLACE, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to PSB names: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The PSB keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of the PSB PERSDB to the Personnel Department, the administrator enters:

```
TSS ADD(PERDEPT) PSB(PERSDB)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PERDEPT) PSB(PERSDB)
```

TSS PERMIT/REVOKE

To permit user PERSF1 to access the department's PSBs, the administrator enters:

```
TSS PERMIT(PERSF1) PSB(PERSDB)
```

To revoke access the administrator enters:

```
TSS REVOKE(PERSF1) PSB(PERSDB)
```

22.1.20 Resource Class: SPI

Operating System: VSE and OS/390

Description: Used to secure the following:

- CEMT INQUIRE, SET, and PERFORM
- EXEC CICS INQUIRE and CICS
- EXEC CICS ENABLE, DISABLE, and EXTRACT
- EXEC CICS SPOOLOPEN

TSS Commands: The following TSS commands can be used with the SPI keyword (Systems Programmer Interface): **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) SPI(COMMAND KEYWORD)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have SPI(OWN) authority via the TSS ADMIN function, to ADD or REMOVE SPI resources to ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The SPI keyword is used with the following ACID types: **User, Profile, Department, Division, Zone.**

Note: For detailed information on the syntax and usage of IBM CEMT and EXEC CICS commands, refer to IBM's *CICS-Supplied Transactions* and *CICS Customization* guides. For additional information, refer to the *Implementation: CICS Guide.*

Equivalents for CEMT INQUIRE and SET

SPI Keyword	Description
SYSTEM	indicates system parameters.
AUTOINST	automatic installation of terminals.
AUXTRACE	indicates whether auxiliary trace is active, which auxiliary data set traces are active and whether on not auxiliary trace data sets are open or closed.

CONNECTI contains the 4-character "sysid" used in the TCT (Terminal Control Table) for Intersystem Communication (ISC) or Interregion Communication (IRC).

CONTROL is the control unit associated with a terminal.

DATASET is the 8-character name used in the FCT (File Control Table).

DLIDATBA is the 8-character name used for DL/I (DDIR control block).

DUMP indicates whether the dump data set is opened or closed.

DUMPOPTI selects system dump.

IRBATCH identifies the batch job sharing data with & icics. for batch regions connected to CICS via IRC (Interregion communication).

IRC indicates whether the IRC facility is active.

JOURNAL is the journal number.

LINE is the name of any line terminal.

MODENAME is the 8-character name for a group of sessions.

NETNAME is the name defining the remote system to the network.

PITRACE indicates whether program isolation trace is active.

PROGRAM is the 8-character program name defined in the PPT (Program Control Table).

QUEUE indicates the 4-character queue name used in the DCT (Destination Control Table).

TASK indicates the number of the task identifier.

TCLASS indicates the class to which the task belongs.

TERMINAL is the 4-character terminal used in the TCT (Terminal Control Table).

TRACE indicates whether or not the trace is active.

TRANSACT is the 4-character transaction name used in the PCT (Program Control Table).

VOLUME is the 6-character volume serial number.

VTAM indicates a connection with CICS.

SPI Equivalents for CEMT PERFORM

SPI Keyword	Description
RECONNEC	indicates that CICS is to be reconnected after a failure.
RESET	synchronizes the system date and time with your CICS date and time.
SHUTDOWN	indicates that CICS is to be shutdown.
SNAP	gives a picture of your CICS system.

SPI Equivalents for CEMT ADD and REMOVE

SPI Keyword	Description
VOLUME	is the 6-character volume serial number.

SPI Equivalents for EXEC CICS INQUIRE and SET

SPI Keyword	Description
CONNECTI	contains the 4-character "sysid" used in the TCT (Terminal Control Table), for Intersystem Communication (ISC) or Interregion Communication (IRC).
DATASET	is the 8-character name used in the FCT (File Control Table).
FILE	is the 8-character data set name in the FCT.
MODENAME	is the 8-character name for a mode group defined for a specific system connection.
PROGRAM	is the 8-character program name defined in the PPT (Program Control Table).
SYSTEM	indicates the current values of your system parameters.
TERMINAL	is the 4-character terminal name used in the TCT (Terminal Control Table).
TRANSACT	is the 4-charcter transaction name used in the PCT (Program Control Table).

SPI Equivalents for EXEC CICS ENABLE, DISABLE, EXTRACT

SPI Keyword	Description
ENABLE	specifies that all or part of the enable sequence for an exit program is to be performed.
DISABLE	specifies that all or part of the disable sequence for an exit program is to be performed.
EXTRACT	indicates that data is to be extracted from CICS control blocks.

SPI Equivalents for EXEC CICS SPOOLOPEN

SPI Keyword	Description
JESSPOOL	opens a spool report for input to CICS and reads existing spool data sets using external writer names for the userid.

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) SPI(COMMAND KEYWORD)
    ACCESS(ACTION KEYWORD(s))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have SPI(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to SPI resources that are owned within their scope.

Types: The SPI keyword is used with the following ACID types: **User, Profile, Department, Division, Zone.**

Note: For detailed information on the syntax and usage of IBM CEMT and EXEC CICS commands, refer to IBM's *CICS-Supplied Transactions* and *CICS Customization* guides. For additional information, refer to the *Implementation: CICS Guide.*

SPI Access Levels for CEMT INQUIRE and SET

CEMT Action	SPI Access Level
ADD	SET
INQUIRE	INQUIRE
PERFORM	PERFORM
REMOVE	REMOVE
SET	SET

SPI Access Levels for EXEC CICS INQUIRE and SET

EXEC CICS Command	SPI Access Level
INQUIRE	INQUIRE
SET	SET

SPI Access Levels for EXEC CICS ENABLE, DISABLE, EXTRACT

Command Function	SPI Access Level
ENABLE	SET
DISABLE	SET
EXTRACT	READ

SPI Access Levels for EXEC CICS SPOOLOPEN

Command Options	SPI Access Level
INPUT	READ
OUTPUT	WRITE

Examples:

TSS ADDTO/REMOVE

To add the SPI SYSTEM resource to a user, the TSS administrator enters:

```
TSS ADDTO(acidname) SPI(SYSTEM)
```

To add the equivalent SPI CONNECTION keyword to a user (using the CICS CEMT command) the TSS administrator enters:

```
TSS ADDTO(acidname) SPI(CONNECTION)
```

To add the equivalent SPI ENABLE keyword to a user (using the EXEC CICS command) the TSS administrator enters:

```
TSS ADDTO(acidname) SPI(ENABLE)
```

To add the equivalent SPI SPOOLOPEN keyword to a user (using the EXEC CICS command) the TSS administrator enters:

```
TSS ADDTO(acidname) SPI(JESSPOOL)
```

TSS PERMIT/REVOKE

To permit access to the SPI SYSTEM resource, the TSS administrator enters:

```
TSS PERMIT(acidname) SPI(SYSTEM) ACCESS(INQUIRE)
```

To permit access to the SPI CONNECTION resource, (using the CICS CEMT command) the TSS administrator enters:

```
TSS PERMIT(acidname) SPI(CONNECTION) ACCESS(SET)
```

To permit access to the SPI ENABLE resource (using the EXEC CICS command) the TSS administrator enters:

```
TSS PERMIT(acidname) SPI(ENABLE) ACCESS(SET)
```

To permit access to the SPI SPOOLOPEN resource (using the EXEC CICS command) the TSS administrator enters:

```
TSS PERMIT(acidname) SPI(JESSPOOL) ACCESS(READ)
```

22.1.21 Resource Class: SUBSCHEM

Operating System: VSE and OS/390

Description: Used to secure CA-IDMS subschema names.

TSS Commands: The following TSS commands can be used with the SUBSCHEM keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) SUBschem(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have SUBSCHEM(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of SUBSCHEMs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The SUBSCHEM keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) SUBschem(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have SUBSCHEM(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to SUBSCHEMs that are owned within their scope.

Access Controls: The administrator can use any of the following methods to control access to SUBSCHEMs: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The SUBSCHEM keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of the subschema, PERDB, to the Personnel Department, the administrator enters:

```
TSS ADD(PERSDP) SUB(PERDB)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PERSDP) SUB(PERDB)
```

TSS PERMIT/REVOKE

To allow USER01 access to the division's subschema, the administrator enters:

```
TSS PERMIT(USER01) SUB(PAYFILE)
```

To revoke access the administrator enters:

```
TSS REVOKE(USER01) SUB(PAYFILE)
```

22.1.22 Resource Class: SURROGAT

Operating System: VSE, OS/390, and VM

Description: Used to restrict installation of pre-set security for terminals to specifc ACIDs. SURROGAT can only be used with terminals running under CICS 4.1.

TSS Commands: The following TSS commands can be used with the SURROGAT keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) SURRogat(acidname.DFHINSTAL)
```

Prefix length — 2-17 characters

Authority: The administrator must have SURROGAT(OWN) authority via the TSS ADMIN function, to ADD or REMOVE terminals from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The SURROGAT keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) SURRogat(acidname.DFHINSTAL)
```

Prefix length — 2-17 characters

Authority: The administrator must have SURROGAT(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to terminals that are owned within their scope.

The SURROGAT keyword is used to establish access authorizations and restrictions.

Access Controls: The administrator can use any of the following methods to control access to surrogate terminals: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The SURROGAT keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To install a terminal with a pre-set userid of WAREHOUS, an ACID named WAREHOUS must be defined to CA-Top Secret with permission to the CICS Facility and any appropriate resources:

```
TSS ADD(CICSDEPT) SURROGAT(WAREHOUS.DFHINSTAL)
```

TSS PERMIT/REVOKE

To permit the user defining the terminal access to the SURROGAT resource for WAREHOUS, the administrator enters:

```
TSS PERMIT(CICSADM) SURROGAT(WAREHOUS.DFHINSTL) ACC(READ)
```

22.1.23 Resource Class: TERMINAL

Operating System: VSE, OS/390, and VM

Description: Used to secure terminal IDs and PCs used to access the mainframe.

Terminal restriction can be used to restrict Automatic Terminal Signon ACIDs from being used at another terminal.

TSS Commands: The following TSS commands can be used with the TERMINAL keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) TERMinal(oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-8 prefixes per TSS command

Authority: The administrator must have TERMINAL(OWN) authority via the TSS ADMIN function, to ADD or REMOVE terminals from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Defining Terminals: Terminals come in a variety of forms. The following tables provide instructions and examples on how to specify prefixes for each type of terminal.

Table 22-1. Terminal Definitions for VM

Type	Prefix	Example
Locally attached	GRAF plus four-character local address	TSS ADD(BUDDEPT) TERM(GRAF02BA)
Remotely attached VM-controlled network terminals	NETW plus four-character resource id	TSS ADD(CORP) TERM(NETW0301)
Logical devices	LDEV plus four-character address of logical device which is arbitrarily defined.	TSS ADD(CORPNET) TERM(LDEV1234)
VTAM/SNA	8-character LU name	TSS ADD(FINDEPT) TERM(xxxxxxxx)

Note: The four-character address for logical devices is arbitrarily assigned by CP when a product such as VM/PASSTHRU or CA-VTERM requests such a device. 'LDEV' is the only practical prefix when specifying a logical device with TSS ADDTO or PERMIT.

Jes Readers: Use names known to JES, as shown in the following table.

Table 22-2 (Page 1 of 2). Terminal Definitions for OS/390

Type	Prefix	Example
RJE	REMOTE #@ READER# Rnn.RDnn	TSS ADD(BUDDEPT) TERM(R12.RD1) Assigns remote 12, reader 1 to the Budget Department
NJE	Symbolic Name Node # @ Remote # Nnn.Rnn	TSS ADD(CORPNET) TERM(PHILA) TSS ADD(CORPNET) TERM(N2.R4)
Local	READER1	TSS ADD(CORPNET) TERM(READER1)

Table 22-2 (Page 2 of 2). Terminal Definitions for OS/390		
Type	**Prefix**	**Example**
Terminals	Use the name known to TCAM or VTAM via TP monitor definitions. *ALL*	To protect VTAM terminals (cluster name TSONxxx), enter: TSS ADD(CORP) TERM(TSON) To allow a user to access all protected terminals, perform the following: 1. Assign ownership of *ALL* to the MSCA: TSS ADD(MSCA) TERM(*ALL*) 2. PERMIT the user to access all terminals: TSS PER(user) TERM(*ALL*)

Table 22-3. Terminal Definitions for PCs		
Type	**Prefix**	**Example**
PC	8-character LU name	TSS ADD(DEVDEPT) TERM(xxxxxxxx)

Types: The TERMINAL keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) TERMinal(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-8 prefixes per TSS command

Authority: The administrator must have TERMINAL(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to TERMINALs that are owned within their scope.

The TERMINAL keyword is used to establish access authorizations and restrictions.

Access Controls: The administrator can use any of the following methods to control access to TERMINALs: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Note: All terminals can be protected by setting DEFPROT on the resource class TERMINAL.

Types: The TERMINAL keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Finance Department, (FINDEPT), ownership of a local terminal in the personnel office (address K61L1234), the administrator enters:

```
TSS ADD(FINDEPT) TERM(K61L1234)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(FINDEPT) TERM(K61L1234)
```

TSS PERMIT/REVOKE

To permit all users connected to the PAYROLL profile (PAYPROF1) access to a local terminal in the personnel office (address K61L1234), from 7:00 to 11:00 am the administrator enters:

```
TSS PERMIT(PAYPROF1) TERM(K61L1234) TIMES(07,11)
```

To revoke access the administrator enters:

```
TSS REVOKE(PAYPROF1) TERM(K61L1234)
```

22.1.24 Resource Class: TST

Operating System: VSE and OS/390

Description: Used to secure CICS Temporary Storage Table names.

TSS Commands: The following TSS commands can be used with the TST keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) TST(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have TST(OWN) authority via the TSS ADMIN function, to ADD or REMOVE TSTs from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The TST keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) TST(prefix(es)) ACCESS(access levels)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have TST(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to TSTs that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **INQUIRE, SET, ALL, NONE, PURGE, READ, REPLACE, WRITE.** If access in not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to TSTs: **Expiration, Facility, Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The TST keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of a TST to Department 5, the administrator enters:

```
TSS ADD(DEPT5) TST(XCOM7)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(DEPT5) TST(XCOM7)
```

TSS PERMIT/REVOKE

To permit a CICS user to access restricted temporary storage when using the CICSTEST facility, the administrator enters:

```
TSS PERMIT(SYST3) TST(XCOM7) ACC(ALL) FAC(CICST)
```

To revoke access the administrator enters:

```
TSS REVOKE(SYST3) TST(XCOM7)
```

22.1.25 Resource Class: UR1/UR2

Operating System: VSE, OS/390, and VM

Description: Used to secure general installation-defined resource restrictions as account codes.

TSS Commands: The following TSS commands can be used with the UR1 and UR2 keywords: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) UR1(oper,oper,...)|UR2(oper,oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have UR1/UR2(OWN) authority via the TSS ADMIN function, to ADD or REMOVE UR1/UR2 resources from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Customization: Use of the UR1 or UR2 keyword requires prior customization of application programs or system exits to invoke the VM/OS/390/VSE security interface so it will call CA-Top Secret to verify access to installation-defined resources.

Resource Class: An installation-defined resource type, such as account codes, can be identified as being a class 1 (UR1) or a class 2 (UR2) user owned resource.

Ownership: Once the resource classes are defined, the administrator can use the UR1 keyword to assign ownership of up to five UR1 resource prefixes.

Types: The UR1/UR2 keywords are used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA. TSS PERMIT/REVOKE**

Syntax:

```
TSS PER(acid) UR1(p-fix)|UR2(p-fix) ACCESS(access levels)
```

Prefix length — 1-44 characters

Capacity of list — 1-5 prefixes per TSS command

Authority: The administrator must have UR1/UR2(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to UR1/UR2 resources that are owned within their scope.

Customization: Use of the UR1 or UR2 keyword requires prior customization using the OS/390/VM security interface such that it calls CA-Top Secret to verify access to installation-defined resource. Refer to Customization in *Implementation: General Guide* for details.

Resource Classes: An installation-defined resource type, such as account codes, can be identified as being a class 1 (UR1) or a class 2 (UR2) user owned resource.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, NONE, READ, WRITE, UPDATE.** If access is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to user-defined resources: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The UR1/UR2 keywords are used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of an account number to Corporate, the administrator enters:

```
TSS ADD(CORPORAT) UR1(ACCT788I)
```

The administer may now PERMIT access to users or profiles that require access.

The administrator may remove ownership by entering:

```
TSS REMOVE(CORPORAT) UR1(ACCT788I)
```

TSS PERMIT/REVOKE

To permit a group of users all access to a set of account numbers, the administrator enters:

```
TSS PERMIT(CLKPROF) UR2(ACCT7889,ACCT4567) ACCESS(ALL)
```

To revoke access, the administrator enters:

```
TSS REVOKE(CLKPROF) UR2(ACCT7889,ACCT4567)
```

22.1.26 Resource Class: USRCLASS

Operating System: VSE, OS/390, and VM

Description: Used to secure resource classes used by other CA Product interfaces.

Refer to the CA product specific documentation for descriptions of USRCLASS names used by the individual product.

TSS Commands: The following TSS commands can be used with the USRCLASS keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) USRCLASS(prefix(es))
```

Prefix length — 1-8 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have USRCLASS(OWN) authority via the TSS ADMIN function, to ADD or REMOVE authority to control access of CA product specific resources owned within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The USRCLASS keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) USRCLASS(prefix(es))
```

Prefix length — 1-44 characters

Capacity of list — 1-5 prefixes per TSS command.

Authority: The administrator must have USRCLASS(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE the authority to CA product specific commands, functions and programs.

Access Controls: The administrator can use any of the following methods to control access to USRCLASS resources: **Expiration, Facility, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The USRCLASS keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

SYSPRG would like ownership of the USRCLASS named BACKUP, the administrator enters:

```
TSS ADD(SYSPRG) USRCLASS(BACKUP)
```

Ownership can be removed by entering:

```
TSS REMOVE(SYSPRG) USRCLASS(BACKUP)
```

TSS PERMIT/REVOKE

To permit ACID, USER01, the ability to use the USRCLASS BACKUP, the administrator enters:

```
TSS PERMIT(VMUSER1) USRCLASS(BACKUP)
```

To enable all users to issue the USRCLASS RESTORE, the administrator enters:

```
TSS PERMIT(ALL) USRCLASS(RESTORE)
```

22.1.27 Resource Class: VOLUME

Operating System: VSE, OS/390, and VM

Description: Used to secure DASD or tape volumes.

TSS Commands: The following TSS commands can be used with the VOLUME keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) VOLume(entries)
```

Length of entries — 2-6 characters.

Entries are treated as prefixes only if the generic indicator (G) follows each entry.

Capacity of list — 1-30 entries per TSS command

Generic prefixing allows the administrator to group a set of similar resource names together, and define them by on generic prefix. The chapter on "How to Use PERMIT/REVOKE," provides excellent guidelines and examples form preparing a resource naming standard.

Authority: The administrator must have VOLUME(OWN) authority via the TSS ADMIN function, to ADD or REMOVE volume ownership from ACIDs within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Vol/Ser Attributes: The volume serial number or prefix must be followed by a (G) to indicate a generic volume prefix.

Note: The use of attributes is an administrative way to document that the volume relates to a disk or tape. CA-Top Secret will honor the rule for both disk and tape access requests if they occur.

Types: The VOLUME keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA. TSS PERMIT/REVOKE**

Syntax:

```
TSS PER(acid) VOLume(oper,oper,...) ACCESS(access levels)
```

Length of entries — 2-6 characters. Entries are treated as prefixes only if the generic indicator (i.e.,(G)) is suffixed to the entry.

Capacity of list — 1-30 entries per TSS command

Authority: The administrator must have VOLUME(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to VOLUMEs that are owned within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, BLP, CONTROL, CREATE, NOCREATE, NONE, READ, SCRATCH, UPDATE.**

If access in not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to VOLUMEs: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The VOLUME keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To protect all tape volumes with the generic prefix of 10000, the administrator assigns ownership to the Corporate Department by entering:

```
TSS ADD(CORP4) VOL(10000(G))
```

The administrator may now PERMIT access to users or profiles that require access. Administrators can remove ownership of by entering:

```
TSS REMOVE(CORP4) VOL(10000(G))
```

TSS PERMIT/REVOKE

To permit all users to access storage volumes, the administrator enters:

```
TSS PERMIT(ALL) VOL(STOR01,STOR02,STOR03) ACCESS(CREATE)
```

To revoke access to storage volumes, the administrator enters:

```
TSS REVOKE(ALL) VOL(STOR01,STOR02,STOR03)
```

22.1.28 Resource Class: VSELIB

Operating System: VSE

Description: Used to secure access to VSE libraries. You can identify each library separately, or in groups of like-named libraries using generic prefixing and masking techniques.

TSS Commands: The following commands can be used with the VSELIB keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOHAS, WHOOWNS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) VSELIB(oper,...)
```

Prefix length — 1-26 characters

Capacity of list — 1-5 library names or prefixes per TSS command

Generic prefixing allows the administrator to group a set of similar libraries together and define them using one generic prefix. The chapter "How to Use PERMIT/REVOKE" provides excellent guidelines and examples for preparing resource naming standards.

Authority: The administrator must have VSELIB(OWN) authority via the TSS ADMIN function, to ADD or REMOVE ownership of libraries from ACIDs within their scope. Refer to the chapter "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The VSELIB keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) VSELIB(prefix) ACCESS(access levels)
```

Prefix length — 1-26 characters

Capacity of list — 1-5 library names or prefixes per TSS command

Note: A fully qualified library name can be PERMITted to an ACID by enclosing it in single quotation marks. The single quotation marks indicate that it is defined to CA-Top Secret by its fully qualified name, not as a prefix.

Authority: The administrator must have VSELIB(XAUTH) authority via the TSS ADMIN function, to PERMIT or REVOKE access to VSE libraries that are within their scope.

Access Levels: The administrator can specify any or all of the following access levels: **ALL, ALTER, NONE, READ, UPDATE, WRITE.** If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to the libraries: **Expiration, Facility, Program Pathing, Time/Day, Actions.** Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Masking: Library masking is another method of reducing the number of library definitions required to implement widespread library protection. Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The VSELIB keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Payroll Department (PAYDEPT) ownership of a VSE library called PAYLIB located in a VSE Dataset called VSE.PAYROLL.LIBRARY, the administrator enters:

```
TSS ADD(PAYDEPT) VSELIB(VSE.PAYROLL.LIBRARY.PAYLIB)
```

The administrator may remove ownership by entering:

```
TSS REMOVE(PAYDEPT) VSELIB(VSE.PAYROLL.LIBRARY.PAYLIB)
```

TSS PERMIT/REVOKE

The administrator can give USER01 read and update access to the VSE library called PAYLIB, located in dataset VSE.PAYROLL.LIBRARY by entering:

```
TSS PERMIT(USER01) VSELIB(VSE.PAYROLL.LIBRARY.PAYLIB)
ACCESS(READ,UPDATE)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USER01) VSELIB(VSE.PAYROLL.LIBRARY.PAYLIB)
```

22.1.29 Resource Class: VSEMEMBR

Operating System: VSE

Description: Used to secure VSE library members. You can identify each member separately, or in groups of like-named members using generic prefixing and masking techniques.

TSS Commands: The following commands can be used with the VSEMEMBR keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) VSEMEMBR(oper,...)
```

Prefix length — 1-26 characters

Capacity of list — 1-5 member names or prefixes per TSS command

Generic prefixing allows the administrator to group a set of similar members together and define them using one generic prefix. The chapter "How to Use PERMIT/REVOKE" provides excellent guidelines and examples for preparing resource naming standards.

Authority: The administrator must have VSEMEMBR(OWN) via the TSS ADMIN function to ADD or REMOVE ownership of members within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The VSEMEMBR keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) VSEMEMBR(prefixes) ACCESS(access-levels)
```

Prefix length — 1-34 characters **Capacity of List —** 1-5 member names or prefixes per TSS command

Note: A fully qualified member name can be PERMITted to an ACID by enclosing it in single quotation marks. The single quotation marks indicate that it is defined to CA-Top Secret by its fully qualified name, not as a prefix.

Authority: The administrator must have VSEMEMBR(XAUTH) authority via the TSS ADMIN function to PERMIT or REVOKE access to VSE members that are within their scope.

Access Levels: The administrator can specify any or all of the following access levels: ALL, ALTER, EXECUTE, NONE, READ, UPDATE, WRITE. If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to members: Expiration, Facility, Program Pathing, Time/Day, Actions. Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Masking: Member masking is another method of reducing the number of member definitions that may be required to implement widespread member protection. Refer to the chapter "How to Use PERMIT/REVOKE" for a discussion on the types of masks used with members.

Types: The VSEMEMBR keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Payroll Department (PAYDEPT) ownership of a VSE member called PAYPROG that resides in the VSE library PAYLIB, the administrator enters:

```
TSS ADD(PAYDEPT) VSEMEMBR('PAYLIB.PAYSUBL.PAYPROG')
```

To remove ownership, the administrator enters:

```
TSS REMOVE(PAYDEPT) VSEMEMBR('PAYLIB.PAYSUBL.PAYPROG')
```

TSS PERMIT/REVOKE

To give USER01 read and execute access to the VSE member called PAYPROG, the administrator enters:

```
TSS PERMIT(USER01) VSEMEMBR(PAYLIB.PAYSUBL.PAYPROG)
         ACCESS(READ,EXECUTE)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USER01) VSEMEMBR(PAYLIB.PAYSUBL.PAYPROG)
```

22.1.30 Resource Class: VSEPART

Operating System: VSE

Description: Used to secure VSE batch partition IDs.

TSS Commands: The following commands can be used with the VSEPART keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) VSEPART(oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 partition IDs or prefixes per TSS command

Authority: The administrator must have VSEPART(OWN) authority via the TSS ADMIN function to ADD or REMOVE ownership of partition IDs from ACIDS within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The VSEPART keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA**

TSS PERMIT/REVOKE

Syntax:

```
TSS PER(acid) VSEPART(prefixes)
```

Prefix length — 1-2 characters

Capacity of List — 1-5 partition IDs or prefixes per TSS command

Authority: The administrator must have VSEPART(XAUTH) authority via the TSS ADMIN function to PERMIT or REVOKE access to VSE partition IDs that are within their scope.

Access Controls: The administrator can use any of the following methods to control access to partitions: Expiration, Facility, Program Pathing, Time/Day, Actions. Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The VSEPART keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To give the Operations Department (OPSDEPT) ownership of a VSE batch partition called BG, the administrator enters:

```
TSS ADD(OPSDEPT) VSEPART(BG)
```

To remove ownership, the administrator enters:

```
TSS REMOVE(OPSDEPT) VSEPART(BG)
```

TSS PERMIT/REVOKE

To give USER01 access to the VSE batch partition called BG, the administrator enters:

```
TSS PERMIT(USER01) VSEPART(BG)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USER01) VSEPART(BG)
```

22.1.31 Resource Class: VSESLIB

Operating System: VSE

Description: Used to secure VSE sublibraries. You can identify each sublibrary separately, or in groups of like-named sublibraries using generic prefixing and masking techniques.

TSS Commands: The following commands can be used with the VSESLIB keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) VSESLIB(oper,...)
```

Prefix length — 1-16 characters

Capacity of list — 1-5 sublibrary names or prefixes per TSS command

Generic prefixing allows the administrator to group a set of similar sublibraries together and define them using one generic prefix. The chapter "How to Use PERMIT/REVOKE" provides excellent guidelines and examples for preparing resource naming standards.

Authority: The administrator must have VSESLIB(OWN) authority via the TSS ADMIN function to ADD or REMOVE ownership of sublibraries from ACIDS within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The VSESLIB keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA TSS PERMIT/REVOKE**

Syntax:

```
TSS PER(acid) VSESLIB(prefixes) ACCESS(access-levels)
```

Prefix length — 1-16 characters

Capacity of List — 1-5 sublibrary names or prefixes per TSS command

Note: A fully qualified sublibrary name can be PERMITted to an ACID by enclosing it in single quotation marks. The single quotation marks indicate that it is defined to CA-Top Secret by its fully qualified name, not as a prefix.

Authority: The administrator must have VSESLIB(XAUTH) authority via the TSS ADMIN function to PERMIT or REVOKE access to VSE sublibraries that are within their scope.

Access Levels: The administrator can specify any or all of the following access levels: ALL, ALTER, NONE, READ, UPDATE, WRITE. If ACCESS is not specified, CA-Top Secret defaults to READ access.

Access Controls: The administrator can use any of the following methods to control access to sublibraries: Expiration, Facility, Program Pathing, Time/Day, Actions. Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Masking: Member masking is another method of reducing the number of sublibrary definitions that may be required to implement widespread sublibrary protection. Refer to the chapter "How to Use PERMIT/REVOKE" for a discussion on the types of masks used with libraries

Types: The VSESLIB keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples: TSS ADDTO/REMOVE

To give the Payroll Department (PAYDEPT) ownership of a VSE sublibrary called PAYSUB that resides in the VSE library PAYLIB, the administrator enters:

```
TSS ADD(PAYDEPT) VSESLIB('PAYLIB.PAYSUBL')
```

To remove ownership, the administrator enters:

```
TSS REMOVE(PAYDEPT) VSESLIB('PAYLIB.PAYSUBL')
```

TSS PERMIT/REVOKE

To give USER01 read and update access to the VSE sublibrary called PAYSUBL, the administrator enters:

```
TSS PERMIT(USER01) VSESLIB(PAYLIB.PAYSUBL) ACCESS(READ,UPDATE)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USER01) VSESLIB(PAYLIB.PAYSUBL)
```

22.1.32 Resource Class: VSEUSER

Operating System: VSE

Description: Used to secure VSE user-defined resources.

TSS Commands: The following commands can be used with the VSEUSER keyword: **CREATE, ADDTO, REMOVE, PERMIT, REVOKE, ADMIN, DEADMIN, WHOOWNS, WHOHAS.**

TSS ADDTO/REMOVE

Syntax:

```
TSS ADD(acid) VSEUSER(oper,...)
```

Prefix length — 1-8 characters

Capacity of list — 1-5 user-defined resources or prefixes per TSS command

Authority: The administrator must have VSEUSER(OWN) authority via the TSS ADMIN function to ADD or REMOVE ownership of user-defined resources from ACIDS within their scope. Refer to the chapter on "How to Use ADMIN/DEADMIN" for details on administrative authorities and levels.

Types: The VSEUSER keyword is used with the following ACID types: **User, Profile, Department, Division, Zone, DCA, VCA, ZCA, LSCA, SCA, MSCA TSS PERMIT/REVOKE**

Syntax:

```
TSS PER(acid) VSEUSER(prefixes)
```

Prefix length — 1-8 characters

Capacity of List — 1-5 user-defined resources or prefixes per TSS command

Authority: The administrator must have VSEUSER(XAUTH) authority via the TSS ADMIN function to PERMIT or REVOKE access to VSE user-defined resources that are within their scope.

Access Controls: The administrator can use any of the following methods to control access to user-defined resources: Expiration, Facility, Program Pathing, Time/Day, Actions. Refer to the chapter "How to Use PERMIT/REVOKE" for more details on each of the access control methods.

Types: The VSEUSER keyword is used with the following ACID types: **User, Profile, DCA, VCA, ZCA, LSCA, SCA, MSCA.**

Examples:

TSS ADDTO/REMOVE

To assign ownership of a special account number to the CORPORAT department, the administrator enters:

```
TSS ADD(CORPORAT) VSEUSER(ACCT9999)
```

To remove ownership, the administrator enters:

```
TSS REMOVE(CORPORAT) VSEUSER(ACCT9999)
```

TSS PERMIT/REVOKE

To give USER01 access to the special account number, the administrator enters:

```
TSS PERMIT(USER01) VSEUSER(ACCT9999)
```

To revoke access, the administrator enters:

```
TSS REVOKE(USER01) VSEUSER(ACCT9999)
```

Note: Use of the VSEUSER resource keyword requires prior customization using the VSE security interface so that it calls CA-Top Secret to verify acces to user-defined resources. Refer to customization in the *User Guide* for details.

Appendix A. Prefixed Resources

CA-Top Secret manages two distinct types of resources: general and prefixed. Prefixed resources are those that support masking characters, and are listed below.

APPCID
APPCLU
APPCSI
APPCTP
DB2BASE
DB2COLL
DB2PKG
DLFCLASS
DSNAME
DTADMIN
DTSYSTEM
DTTABLE
DTUTIL
JESJOBS
JESSPOOL
MQCONN
MQNLIST
MQPROC
MQQUEUE
NODES
OPERCMDS
PANAPT
SDSF
VMMDISK
VSESLIB
VSEMEMBR
WRITER

Prefixed resources have an attribute of MASK when the RESCLASS is displayed using the TSS LIST(RDT) RESCLASS(resource class) command.

Index

A

B

C

D

E

F

G

H

M

N

O

P

R

S

T

U

V

W

X

Y

Z

User Registration Form

If you are interested in registering as a user of Computer Associates software, please complete the information below. Send it to the following address:

Computer Associates International, Inc.
ATTN: User Registration
One Computer Associates Plaza
Islandia, NY 11749

Registration entitles you to receive such items as:

- newsletters
- product release announcements
- information about User Groups
- information about CA conferences
- client questionnaires

You *do not* have to be the primary contact for CA software within your company or organization. All you have to be is interested in CA software, how it is used, and where it is headed.

Product(s): _____

_____

_____

_____

Site ID: _____
(Enter UNKNOWN if you do not know your Site ID.)

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

I would like additional information on: _____

Demand Analysis Request Form

Please use this form to make suggestions for product improvement. Send it to the following address.

Computer Associates International, Inc.
ATTN: Demand Analysis Requests
One Computer Associates Plaza
Islandia, NY 11749

Be sure to print your name and address below if you would like a reply.

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

Is DAR from a User Group? (Yes/No) ___ User Group ID: _____

Priority: _____

Description of Requested Item:

_____

_____

_____

_____

_____

_____

_____

_____

_____

CA Account Manager:	CA Office:
Input by:	Date:

Reader Comment Form

CA-Top Secret Command Functions Guide

Release 3.0 VSE

Document Number: R101TS30CME

Please use this form to tell us how you use this manual and to make suggestions for improvement. Send it to the following address. (To request additional publications, call 1-800-841-8743 or check the CA home page (http://www.cai.com) on the Internet. To ask questions about the functionality of CA products, contact your CA representative.)

Computer Associates International, Inc.
ATTN: Reader Comment Form
One Computer Associates Plaza
Islandia, NY 11749

Be sure to print your name and address below if you would like a reply.

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

Years of experience with this CA product: _____

Overall Rating

	Good	Fair	Poor	Why?
Accuracy				
Organization				
Clarity				

Reference Aids

	Good	Fair	Poor	Why?
Contents				
Index				
Glossary				
Reference to Other Manuals				

Clarity

	Good	Fair	Poor	Why?
Instructions and Procedures				
Examples				
Graphics				

How Manual Is Used:

How do you use this manual in your job?

How often do you use this manual in a week?

Suggestions:

What do you like about this manual?

What do you dislike about this manual?

What would you like us to change?

Additional Comments: