# CA Top Secret® for z/VM

## User Guide

r12

# Contact CA Technologies

**Contact CA Support**

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

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

**Provide Feedback**

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

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

# Contents

# Chapter 1: Introduction

This section contains the following topics:



## About this Guide

This guide is a comprehensive look at what users need to know about their company's security. It is targeted to the security administrator who is assigned the task of developing a company User guide.

## Why Use CA Top Secret?

Security is a global concern. It affects not only corporate personnel assigned to administer and audit security, but also end users at every level. To ensure that your security policies and procedures remain sound, ensure that all users understand the following: security is a team effort.

CA Top Secret is an important component in the CA family of integrated security solutions, designed to streamline security administration, enable single-point user signon, and provide auditing capabilities.

CA Top Secret offers a unique hierarchical security configuration similar to the organizational structure of your corporate environment. Administrative tools, reporting options and automatic logging capabilities help ensure the integrity and security of your corporate assets.

## Purpose

The purpose of security software is to minimize the risks of accidental or intentional corruption, destruction, or disclosure of data. The integrity of the information kept in the computing environment is essential. CA Top Secret provides that integrity.

Through individual accountability, access permissions, and a comprehensive audit trail, CA Top Secret controls and monitors who can access and change data. Until permissions are issued to control how new data is shared, that data is protected by default.

Additional advanced technology within CA Top Secret provides further assurance of data integrity. Also, CA Top Secret is fully SAF-compliant, providing controlled mechanisms for access to security information.

## Components and Features

The following CA Top Secret components and features ensure your environment's integrity and security:

- Encompasses RACF Functions—As with RACF, CA Top Secret provides system entry validation, resource control, auditability, accountability, administrative control, and SAF compatibility. Unlike RACF, CA Top Secret has a user-oriented architecture, which means that the focus of security is on the individual user rather than on the resource. This type of architecture offers less overhead, more efficiency, and better overall implementation.
- System Entry Validation—CA Top Secret requires that the user have a valid ACID (ACcessor ID) and password before entering the system. Other system entry validations are optional and can be tailored to meet your environment. For example, you can restrict a particular user by entering the system through a specific facility, such as VM.
- Resource Protection—A resource is any component of the computing or operating system required by a task. CA Top Secret protects a wide variety of resources by default, and provides the capability of also protecting site-defined resources.
- User Information Repository—As part of building your security database, you must identify each user to CA Top Secret by using ACIDs. The attributes and resource access permissions you associate with each ACID comprise the ACID's Security Record which, in turn, becomes part of the overall Security File.
- CA-CIS Architecture—CA-CIS enables CA to deliver Systems Management Software solutions that perform better, are more deeply integrated, exhibit greater reliability, and are consistent across hardware platforms. These benefits enable you to make significant strides in achieving total data center automation, in meeting service-level requirements, and in controlling costs while maximizing the return on investment.
- Distributed Security—The security area is a good example of the cross-platform capability of CA-CIS. Distributed security in CA Top Secret coordinates multi-system security by using the following component of the Integration Services of CA-CIS architecture:
  - CAISSF—(Standard Security Facility) provides an easy-to-use application interface for CA and non-CA products to obtain and use CA Top Secret security information.
  - CAICCI—(Common Communication Interface) is a common communications facility that enables CA Top Secret secured nodes to communicate with one another. This facility provides the VTAM facilities needed to transmit and receive TSS commands, when using the Command Propagation Facility (CPF).

Within CA Top Secret, distributed security can include the following:

Command Propagation Facility (CPF) is a major part of distributed security in CA Top Secret that can route security administration to all or selected nodes either synchronously or asynchronously, resulting in single point administration. Changes made to ACIDs, passwords, or access levels, for example, can be propagated to all nodes to which the user is defined. For example, USER01 is defined to two nodes, with NODE A as his local node and NODE B as his remote node. If he changes his password on NODE A, CPF will automatically propagate the change to NODE B. Through the use of command function keywords, you can specify which node receives these commands and how the local node processes them.

## System Entry Protection

Once ACIDs have been defined to CA Top Secret, users must pass at least two tests to enter the system:

- They must have a valid ACID.
- They must have a valid password.

As part of a flexible approach to security administration, CA Top Secret supports a wide variety of password security policies by using password protection controls and options. Some of these controls and options are:

- Restricting how passwords can be defined and changed
- Setting expiration intervals
- Maintaining password history
- Selecting a password violation threshold

In addition to these password controls, an ACID can also be restricted to:

- A particular terminal or CPU
- Access only on particular days of the week or during certain hours
- Access through particular facility such as TSO and CICS

## Types of ACIDs

ACIDs are the ACcessor IDs by which users are identified to CA Top Secret. An ACID can be up to eight alphanumeric characters long, which normally corresponds with the user's system userid. With CA Top Secret, you have the option of using the same ACID for all facilities or using a different ACID for each facility (that is, TSO, CICS, VM, and so on).

CA Top Secret recognizes several different types of ACIDs, ranging from a user to an entire zone. Together, these types comprise the basic hierarchical structure of your CA Top Secret security database. Each of these ACID types is then associated with a set of resource access authorizations.

The simplest, and generally, the most useful way to build your security database is to create a security hierarchy that mirrors your actual corporate structure. However, CA Top Secret does not limit you to this approach. The basic function of the corporate structure defined to CA Top Secret is to serve as a coordinating framework for security administration at your installation. Therefore, its design should be fundamentally dictated by what will best facilitate security implementation and maintenance.

The CA Top Secret hierarchy is constructed from seven ACID types:

- User
- Profile
- Group
- Department
- Division
- Zone
- Control

These ACID types fall into one of two categories:

- Functional
- Organizational

Functional ACIDs see User, Profile, Group, and Control ACIDs, and are used to perform specific tasks. Organizational ACIDs are Department, Division, and Zone ACIDs, and are used to construct the upper levels of your security hierarchy.

Functional ACIDs report to organizational ACIDs, while organizational ACIDs report to other organizational ACIDs. Organizational ACIDs never report to functional ACIDs.

## User ACIDs

At times, the difference between a user and a User ACID can be confusing. Just remember that a user is a person. A User ACID designates a specific employee in a department—the lowest level of the CA Top Secret organizational hierarchy. Individuals are associated with User ACIDs or Control ACIDs.

Every User ACID must be associated with a single Department ACID.

## Profile ACIDs

When a group of users need to use a set of identical resources in the same way (the users perform similar or related job functions), it is convenient to define this set of access authorizations once and then associate the entire set with each of the users in the group. In CA Top Secret this set of common resource access characteristics is termed a Profile. Every profile is assigned a unique Profile ACID. Once a profile is defined it can be associated with any number of users (at the same or different levels in the hierarchy), thereby eliminating the need to define each resource access authorization separately for every user.

Every Profile ACID must be associated with and defined to a single Department ACID.

## Group ACIDs

CA Top Secret supports the concept of Groups in the IBM OpenVM environment. A Group is similar to a Profile in that it is a collection of users who can share access authorities for protected resources; however, Groups are recognized by IBM OpenMVS while Profiles aren't.

## Department ACIDs

At any installation, users typically work for a particular department. CA Top Secret recognizes this logical separation by requiring each User ACID to be associated with one Department ACID.

## Division ACIDs

CA Top Secret lets you optionally define multiple divisions within your corporate security structure. Each division can be composed of one or more departments. (A department does not have to be associated with a division). Every division is assigned a unique Division ACID, and resources can be assigned to a Division just as they can be assigned to a Department, Profile, or User.

## Zone ACIDs

A Zone ACID is another optional organizational level in your corporate security structure. A zone can be used to group two or more divisions. Every Zone is assigned a unique Zone ACID and—as with Users, Profiles, Departments, and Divisions—resources can be assigned to a zone as well.

## Control ACID

Control ACIDs are used for administrative purposes and define security administrators that are associated with various structural levels within the CA Top Secret security database. A Control ACID, like an ordinary User ACID, can be a regular user of system facilities. A Control ACID can issue subsystem commands and perform other functions—such as access data sets and submit jobs.

Initially, CA Top Secret knows of only one Security Administrator—the MSCA ACID. This ACID is defined to CA Top Secret during the installation process; other Control ACIDs are created later.

Each type of Control ACID performs administrative tasks for the structural level it is associated with. To enable the Control ACID to perform these tasks, each one is assigned a scope of authority and administrative authorities within that scope.

## Concept Of Scope

Once you define your security administrator ACIDs, you need to consider for which part of your security hierarchy they will be responsible. This is called the security administrator's scope of authority. CA Top Secret provides you with several different levels of Control ACID scope, and each level corresponds to a level in your corporate structure. For example, a Division Control ACID, or VCA, is responsible for administering security for all the ACIDs within a particular Division (including ACIDs assigned to Departments associated with that Division). The VCA responsible for the Finance Division would also be responsible for the ACIDs within the Payroll and Accounting Departments.

## Concept Of Authority

In addition to scope of authority, the Security Administrator must also be assigned particular types of administrative authorities. These authorities define the security functions the Control ACIDs can perform for ACIDs within their scope.

Upper level security administrators can grant administrative authorities to lower level administrators within their scope, provided the higher level administrators already possess the appropriate authorities.

The following illustration shows a typical corporate structure and the ACIDs related to each structural element.

The following table shows how the CA Top Secret ACIDs correspond to elements within the corporate structure shown in the previous illustration:

| Corporate Element | Corresponding ACID |
|---|---|
| Data Security Manager/Chief | MSCA is a control ACID |
| Data Security Administrator | SCA is a Control ACID |
| Princeton Office | PRNZON is a Zone ZCID |
| Finance Division<br>R & D Division | xxxDEPT are Department ACIDs |
| Payroll Department<br>Accounting Department<br>Research Department<br>Marketing Department | xxxDEPT are Department ACIDs |
| Payroll Functions<br>Accounts Receivable Functions<br>Accounts Payable Functions | xxxPROF are Profile ACIDs |
| Clerks | USRxx are User ACIDs |

## Role of the Security Administrator

The security administrator (or security administrators, depending on your ACID hierarchy) is the focal point of security for your site. He needs to understand how CA Top Secret works and how to best implement security for your system. He may not necessarily be responsible for installing or maintaining the CA Top Secret product, but he acts as the liaison between CA Top Secret security and the users who need to access the facilities and resources it secures. The security administrator's actual role is determined by a number of factors, among them:

- His scope of authority (is he responsible for the entire installation or a single department within that installation).
- His designated administrative authorities (can he create ACIDs, run reports, change control options).
- Security needs of the site.

For example, you might design one security administrator whose sole purpose is ACID creation and maintenance, and another security administrator who is responsible for maintaining resources and the Resource Descriptor Table (RDT). For more details on the RDT, see your Command Functions Guide. Or, like many installations, you might create a "backup MSCA" by assigning full authority to one SCA.

Regardless of his specific role or area of control, each security administrator must first possess the appropriate administrative authority.

## Types of Administrators

The CA Top Secret administrative hierarchy has seven levels:

- Master Security Control ACID (MSCA)
- Central Security Control ACID (SCA)
- Limit Central Security Control (LSCA)
- Zonal Control Acid (ZCA)
- Divisional Control ACID (VCA)
- Departmental Control ACID (DCA)
- User ACID

The first six levels represent types of ACIDs—that is, ACIDs whose primary function is to control security administration. (The MSCA is frequently referred to as the Master Central security administrator, the SCA as a Central security administrator, and so on.) While users can be given administrative authority (limited to themselves), their primary function is to perform work (for example, production processing). Likewise, Control ACIDs can perform work, but this should be a secondary function for them.

## Types of Administrative Authorities

An ACID's authority determines what he can do with respect to the administration of ACIDs, resources, facilities, the displaying of security database information, and so on. An administrator can confer only those administrative authorities she already possesses herself.

The different types of administrative authorities are:

- ACID
- DATA
- RESOURCE
- FACILITY
- MISC1
- MISC2
- MISC3
- MISC8
- MISC9
- SCOPE

Each of these types of authority roughly corresponds to a different set of security environment control and maintenance functions (for example, ACID maintenance or resource maintenance). In addition, a group of operands is associated with each type of authority. Each operand designates a very specific functional authority. For example, ACID(CREATE) authority allows the Control ACID to create and delete ACIDs within her scope, while RESOURCE(INFO) allows her to perform certain inquiries for any resource within her scope.

Administrative authorities cannot be assigned to a Division, Department, or Profile ACID.

## Establishing Global Authorities

To give every ACID the ability to perform specified administrative functions, the administrator can assign the administrative authority to the ALL Record. For example, assigning MISC1(LTIME) to the ALL Record gives every ACID the authority to set his own terminal lock time interval. The ALL Record can also contain resources access levels.

## Logon/Logoff

Because logon/logoff procedures are site dependent, each organization must provide their user community with both the operating system requirements as well as CA Top Secret requirements for logon/logoff procedures.

The procedures serve as step-by-step instructions including all system responses such as the CA Top Secret Last-Used and Status messages

## New User Logon Procedure

For a new user to logon to the operating system the security administrator must assign a userid, an CA Top Secret ACID, and a password. Typically, the userid and ACID are the same. If the logon procedure is different for new users, we recommend that you outline a separate logon procedure and develop a New User form.

The New User form is used to notify central security that they must set up a new account. It must contain all necessary access requirements. A sample New User form can be found in the Sample User Guide" chapter.

Note: Care must be taken when assigning the userid and CA Top Secret password. To ensure confidentiality, the assignment is communicated directly to each user by their security administrator. Also, users must be informed of all password rules and regulations.

## Passwords

Password use and validation are the most fundamental mechanisms for protecting ACIDs from unauthorized use. CA Top Secret requires that all ACIDs be password protected by default. A security administrator assigns the first password. The user associated with the ACID can then either change the password immediately, or later when it expires.

Password assignment is controlled by certain CA Top Secret control option values. These values are set and stored within CA Top Secret; however, they can be changed to fit your site's security requirements at any time.

Password assignment can be controlled in these ways:

- By following rules for changing passwords
- By setting password expiration intervals
- By using password violation thresholds
- By using random password generation

## Rules for Changing Passwords

The following rules demonstrate some of the options you can apply to all users of CA Top Secret security:

- The minimum length of a password can be set. New passwords must be at least four characters in length and cannot be exactly the same as, or even a close variant of, the user's previous password (for instance, ninth and tenth could be considered close variants because they differ by only two letters).
- Passwords can only be changed after a specific interval of time has elapsed (the system default is one day).
- Passwords cannot contain repeating characters and can be required to conform to a mask.
- Passwords that match the userid or the first four characters of any word in the associated (personal) name field, as well as passwords that match entries in a restricted password list, are not allowed.

## Password Expiration Intervals

A password expiration interval is the number of days before CA Top Secret forces a user to change his password.

## Password Violation

To prevent unauthorized system entry by password guessers, CA Top Secret recognizes a password violation threshold that is enforced system-wide. Once this threshold is exceeded, CA Top Secret automatically suspends the ACID.

## Random Generation

Random password generation is a feature that lets CA Top Secret automatically generate a random set of characters for a password. A security administrator can instruct CA Top Secret to generate a random password for a user whose password has expired, or the user himself can instruct CA Top Secret to automatically generate a password.

## ACID and Password Validation

Because of their importance in the CA Top Secret security environment, ACIDs are validated in many different ways to protect against unauthorized use. First, CA Top Secret checks the Security File to determine whether a designated ACID has been defined (by seeing if a Security Record exists for it). Second, if the ACID is undefined, CA Top Secret responds based on the initial control option settings for the security mode and various system options.

Password validation occurs when the user signs on, supplying his ACID and its associated password. CA Top Secret verifies that the supplied password is correct by checking it against the ACID/password combination stored within CA Top Secret. If the supplied ACID/password combination matches, the user is allowed to continue; if it does not match, the user is denied access to the system. By combining password assignment and validation in this way, CA Top Secret lets you secure your environment by controlling who can access it.

## Modes

Mode is the level of security under which CA Top Secret operates. There are four modes: DORMANT, WARN, IMPL, and FAIL.

These security modes are an invaluable tool when planning a phased or gradual implementation of your security environment. They can be set to apply to the entire installation, a particular facility, or even a particular user or group of users.

Note: Passwords are validated in all modes.

**DORMANT**

CA Top Secret is installed, but is not actively validating. The TSS command is fully supported and can be used.

**WARN**

CA Top Secret is active, but violations generate warning messages rather than the requests being failed.

**IMPL**

CA Top Secret is active, and fails any unauthorized access requests. Users not defined to CA Top Secret can operate normally but are restricted from accessing protected resources.

**FAIL**

CA Top Secret is in full control of access requests. All users must be defined and all resources protected.

## What is a Facility?

A facility is a way of grouping options and associating them with a particular service that users sign on to. VM is an example of a facility. CA Top Secret provides security for many facilities, including:

- VM
- CICS
- Advantage CA-Roscoe
- IMS
- Advantage CA-IDMS
- BATCH
- TSO
- STC

As delivered, CA Top Secret comes with many facilities already defined in what is known as the Facilities Matrix Table. You can customize this table by adding facilities and changing existing ones.

## What is a Resource?

As was discussed previously, a resource is any component of the computing or operating system required by a task. CA Top Secret protects a wide variety of computer resources, but to protect them it must know about them. Computer resources are secured through ownership and authorization.

### Types of Resources

The types of resources (such as data sets, volumes, terminals and minidisks) that CA Top Secret protects are listed in what is called the Resource Descriptor Table (RDT). Many resource types are already automatically defined to the RDT at installation; however, additional resource types (including site-defined resources) can be added.

### Ownership And Authorization

Securing resources is a two step process. Once the resource type, or class, is defined in the RDT, then each resource must be:

- Owned by an individual or department ACID
- Permitted to additional ACIDs (if necessary)

Ownership of a resource automatically implies full access to that resource. For other ACIDs to have access to that resource, they must be authorized, or permitted, to use it.

### Security Validation Algorithm

Once all resources have been defined to CA Top Secret and their access levels specified, any future request to access those resources is processed through the CA Top Secret Security Validation Algorithm. The Security Validation Algorithm is the formula that CA Top Secret uses to determine whether an ACID has the appropriate authorizations to access a particular resource.

## What is a Field?

A field resides in the data area of the ACID's Security Record which holds information to be used by system and security level applications.

### Security Record Segments and Fields

Each Security Record is broken down by segments as defined in the IBM External Security Interface (RACROUTE) Guide.

Fields and segments of the ACID Record are defined in a special Reserved Record of the Security File known as the Field Descriptor Table (FDT). Some fields and segments are pre-defined by CA Top Secret at installation; however, additional fields and segments can be added. For more details, see the Command Functions Guide.

### Administrative Authority

Manipulation of the Field Descriptor Table (FDT) requires special administrative authority.

### Assigning Values for Defined Fields

After fields and segments are defined to the FDT, the field name becomes a keyword in CA Top Secret. Values are assigned, replaced and removed using standard CA Top Secret commands. Fields in an ACID Security Record can be modified by anyone with administrative authority over the ACID.

## Control Options and Command Functions

Control options and command functions are used to communicate with CA Top Secret. The basic distinction between control options and command functions is that control options define your security environment and command functions are used to maintain the integrity of the security database.

## What are Control Options?

Control options are used to customize the security environment of a particular installation. Control options are typically set during installation, and are stored in the Parameter File. One of the most important control options is MODE, which determines how CA Top Secret reacts to a particular resource access request or violation. Many control options can be temporarily changed using the TSS MODIFY command function.

The following example tells CA Top Secret to modify the FACILITY control option so that users on the VM facility will be in IMPL mode.

```
TSS MODIFY(FAC(VM=MODE=IMPL))
```

## What are Command Functions?

Command functions are the primary tool of the security administrator and are always preceded by the letters TSS. A command function is used to define ACIDs, assign attributes, and determine resource access.

For example, the following TSS command will assign a specific date on which an ACID will expire.

```
TSS ADD(USER01) UNTIL(04/06/04)
```

All command syntax components are described in the following examples:

```
1   2         3          4      5

TSS FUNCTION { (acid)  } KEYWORD(OPERAND)
             { (ACIDS) }
             { (AUDIT) }
             {(RDT)    }
             {(FDT)    }
             {(ALL)    }
```

| Component | Description | Rules |
|---|---|---|
| 1 | TSS command name | Command must always begin with TSS. |
| 2 | Name of the function CA Top Secret will perform | Must immediately follow TSS.<br>Only one function entered per TSS command.<br>One or more spaces must be entered between TSS and the function. |
| 3 | Specifies the ACID being affected by the function. | ACID names can be up to eight characters in length and must conform to the restrictions established by your site. |

| Component | Description | Rules |
|---|---|---|
| 4 | Specifies the resource type or security attribute being processed by the function. | Keywords can be entered in any order.<br>Online: Keywords can be entered from line to line without special action.<br>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. |
| 5 | Enter the specific prefix, resource name, or the required value name for a security attribute. | Operands must be provided and parentheses are required to indicate no value. If an operand is missing, any following keyword is ignored. |

## Entry Methods

CA Top Secret functions can be entered freeform onto the command screen of an online terminal or into any of the CA Top Secret full-screen administration panels.

## Freeform

The following screen illustrates how commands are entered freeform onto the command screen:

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

## Administration Panels

TSS command functions can be entered and changed through CA Top Secret's full-screen administration panels, if the administrator is running under CMS. These panels provide the administrator with a fill-in-the-blank application for the TSS command.

The following example demonstrates the procedure for accessing the CA Top Secret selection panel. The initial panel is invoked by entering the command CATSS.

- If you have not already done so, link to either CAIMAINT Test (291) or Production (391) minidisk.
- Enter CATSS and press ENTER. The system displays the CA Top Secret Selection Panel.

```
CAKV-A000  Top Secret Selection Menu  CA-TOP-SECRET
====>
Enter the number of your selection and press the ENTER key:

  1  Create          - Define a new ACID
  2  Acid(S)         - Delete, Move, and/or Rename ACID(S)
  3  Add/Remove      - Add/Remove ACID Resources and Attributes
  4  Replace         - Change ACID Attributes
  5  Permit/Revoke   - Permit/Revoke Resource Access Permissions
  6  Admin/Deadmin   - Remove/Assign Administration Authorities
  7  WhoAmI          - Display current ACID's status
  8  WhoHas/WhoOwns  - Display Resource access/ownership information
  9  List            - List ACID(S) Security Records
 10  Status          - Display TSS System Status
 11  Modify          - Perform TSS Modify
 12  Security Tables - Modify Security tables (RDT,STC,etc)

PF1=Help    2=    3=End    4=Return    5=    6=
PF7=        8=    9=       10=         11=   12=Cursor
```

# Distributed Security Processing

As discussed earlier, distributed security processing can include Command Propagation Facility (CPF). This section focuses on the major component of distributed security processing—the Command Propagation Facility (CPF).

With the Command Propagation Facility, distributed security processing allows you to administer security across multiple VTAM nodes. For example, with the appropriate authorization a security administrator on one node can make modifications to the Security File on another node. The Command Propagation Facility allows centralized control of the whole network or even a smaller portion of that network.

## What is the Command Propagation Facility?

The Command Propagation Facility (CPF) provides the security environment with:

- Routing of security administration to all or selected nodes within the security network.
- Optional synchronous or asynchronous remote command execution. The basic difference between the two types of command execution is that synchronous waits for the command response to return from the remote node before continuing, while asynchronous does not have to wait for a response before resuming processing.
- TSS command execution with most CA Top Secret commands.
- Automatic update of passwords on all connected systems if changed by the user at logon.
- Propagation of user-initiated suspensions for exceeding password and violation threshold limits.
- Optional Journal Files (virtual printers) to log commands transmitted to, and responses received from, remote nodes.
- Optional collection of asynchronous commands in a Recovery File so that they can be retransmitted in case of network outage.

## Synchronizing Information Across Nodes

CPF allows you to automatically synchronize Security Administration on multiple nodes through the propagation of TSS commands, as well as user-initiated changes, such as suspension and password changes. Security administration propagation can be either implicit or explicit. Implicit uses the CPF control options to set system-wide propagation rules; while explicit uses CPF command keywords to set propagation rules on a command-by-command basis.

## Controlling Access From Remote Nodes

When CPF transmits a command to a remote destination, it records the command image on the Journal File for that node and associates an ID with that command. A Journal File provides an historical record of the command traffic to and from CA Top Secret. When a response is received from the remote node, CPF journals the response and the ID number so that the response can be matched to the command that prompted it. When the response is sent back, it is journalled with the ID and remote destination name. By examining the appropriate Journal File, an auditor can see exactly what came in, what went out, and the results of the action taken.

# How Does CA Top Secret Work?

The purpose of CA Top Secret is to control access to resources by limiting system entry (through passwords and terminal restrictions, for example) and limiting how, when, and which resources a user can access once he enters the system.

As part of using CA Top Secret to secure your installation, the security administrator must design the security database. The following terms and their distinctions are important to understand the basics of CA Top Secret:

**Security Administrator**

The person who is primarily responsible for implementing and maintaining system security by defining users, resources, access levels, and facilities.

**Security Database**

A systemized collection of data containing information on user and resource definitions, and access permissions and system entry conditions stored for immediate use.

**Security File**

An encrypted security database consisting of the Security Records, which contain all user and resource permissions and restrictions.

**Security Record**

A part of the Security File that contains a set of user and profile records, including such information as which resources a user can access, and how he can use them.

In addition, the security administrator is also responsible for the following:

- Controlling the security environment through the use of control options and TSS commands.
- Control options provide a mechanism allowing CA Top Secret to customize the environment.
- Control options are typically set during installation, and are stored in what is called the Parameter File.
- One of the most important control options is MODE, which determines how CA Top Secret will react to a particular resource access request or violation.
- TSS commands are used primarily to define ACIDs and to establish resource access. Many control options can be temporarily modified using the TSS command.
- Monitoring resource access violations through the CA Top Secret auditing, tracking, and reporting options.

CA Top Secret also provides the means for securing subsystems and facilities (such as VM, CICS, Advantage™ CA-Roscoe® Interactive Environment, Advantage™ CA-IDMS®, IMS and TSO), as well as for maintaining security across multiple VTAM-connected nodes through the Command Propagation Facility.

# Where is Information Stored?

Information for CA Top Secret is stored among many files and records which work together to provide an integrated security software package.

## CA Top Secret Files

The files used by CA Top Secret to secure an environment are:

- Security File
- Parameter File
- Audit/Tracking File (optional alternate file)
- Backup File
- Recovery File
- Command Propagation Files

### Security File

This file is an encrypted security database consisting of the Security Records that contain all user and resource permissions and restrictions. When a user initiates a job or signs on to an online facility in a VM, MVS, or VSE environment, CA Top Secret obtains the user's Security Record from the Security File, and places it in the user's address space for the duration of the session.

### Parameter File

This file stores and defines control options at initialization, and sets up the operating environment for CA Top Secret. As was discussed earlier, control options are the tools that allow you to modify and customize the security environment.

### Facility Matrix Table

This table contains all the facilities defined to CA Top Secret. Each entry contains information about the specific attributes associated with a particular facility (like VM, TSO, and so on), and can be viewed and modified with the FACILITY control option.

### Audit/Tracking File

This file records security-related events and can be shared among CPUs. These events include violations, job and session initiation, and resource access. You can also designate an optional, alternate Audit/Tracking File to increase the amount of information that can be stored before the file fills up and begins to wrap.

## Backup File

This file stores the automatic daily backup of the Security File to ensure complete integrity of the security environment. The backup file is an exact copy of the Security File, as it existed at the time of last backup, and can be used if the Security File device becomes unavailable.

## Recovery File

This file is a wraparound file that stores recent administrative commands depending on the size of the file allocated. The backup Security File with the application of select recovery file commands can completely restore a damaged Security File.

## Command Propagation Files

The are two distinct types of files that are associated with the Command Propagation Facility (CPF): the Recovery File and the Journal File. These files must be dedicated to a single CPU.

## CPF Recovery File

This file is a disk file used by the Command Propagation Facility to save transmitted commands until a response to those commands has been received from remote nodes. There is one Receive journal to record commands and their response from other nodes. There can be a Send journal for each connected node to record commands and responses.

## CPF Journal Files

These files provide an historical record of the command traffic to and from a particular CA Top Secret CPF node.

## Special Security Records

CA Top Secret has several reserved or special ACIDs that are pre-defined and maintain resource and attribute information. These records include:

**ALL Record**

Identifies resources that are globally accessible to all signed on users.

**Audit Record**

Stores the resource names that are to be audited.

**Resource Descriptor Table**

(RDT) Contains pre-defined resource classes. Each resource class is identified by a unique keyword and has certain attributes associated with it.

**Field Descriptor Table**

(FDT) Defines fields (classes) that can be attached to ACIDs within the Security File. Each field description contains a field name, field code, and field attributes.

**Node Descriptor Table**

(NDT) Contains all PassTicket application and session key-related node information.

A PassTicket is a dynamically generated, one-time-only, password substitute with a limited lifespan. For more details about PassTickets, see the Implementation Guide.

The NDT is a global record similar to the Resource Descriptor and Field Descriptor Tables.

**Static Data Table**

(SDT) The SDT is a new Security file repository and reserve acid for internal, non-volatile data that is used with various PERMIT administrative functions.

# Chapter 2: Sample User Guide

The following is provided as a sample User guide for a fictional corporation called ANY COMPANY. ANY COMPANY runs under two facilities, VMTEST and VMPROD, and has implemented the use of New User and Resource Access Request forms.

This section contains the following topics:

# New User Form

ANY COMPANY - REQUEST FOR NEW USER

User Name: _____

Dept/Div: _____

Effective date: From: _____ To: _____

User Access Class: _____

Facility(s): _____

UserID: _____ Call Extension 200

First Password: _____ Call Extension 200

Approvals: SCA _____

DCA _____

# Resource Access Request Form

ANY COMPANY - RESOURCE ACCESS REQUEST

Requester's Name: _____

Dept/Div: _____

Effective date: From: _____ To: _____

Purpose of Request: _____

_____

Resource Type: _____

Requested Access Level: _____

Approvals: SCA _____

DCA _____

# Security Policy and Structure

This section discusses security-related issues and offers samples.

## Security Reference Card

ANY COMPANY CORPORATE DATA SECURITY

REFERENCE CARD

In an effort to protect this company's valued data processing resources, the CA-Top Secret data security product has been implemented. CA-Top Secret controls who can access what resources, and how and when those resources can be accessed. Each employee is responsible for maintaining security within their scope. This entails:

- Keeping all accounts confidential
- Revising account passwords at regular intervals
- Notifying the appropriate person(s) if abuse of accounts are suspected
- Actively supporting all company security procedures.

A copy of the Company Security Policy can be obtained through your supervisor.

## Security Glossary

The following are security-related terms you should know:

**access**

The way in which a resource can be used.

**ACID**

An acronym for ACcessor ID which identifies a user to CA-Top Secret.

**administrator**

A person designated and authorized to grant users permission to access resources.

**error message**

A system response that displays to inform the user that the entered transaction is not valid; usually providing the reason for invalidity.

**facility**

The various facilities supported by the central computer, such as VM, TSO, CICS, CA-ROSCOE, BATCH.

**mode**

The security implementation stage which determines the manner in which CA-Top Secret processes resource access requests. The four modes are: DORMANT, IMPLEMENT, WARN, and FAIL.

**ownership**

The state of being a protected resource. The "owner" of the resource has full access to the resource.

**password**

A unique string of characters associated with a particular ACID. Logon cannot be successful if an incorrect password is supplied.

**permission**

Authorization for access to an owned resource.

**profile**

A collection of identical resource permissions associated with a group of users performing the same job function.

**resource**

Something protected by CA-Top Secret such as a minidisk, data set, or terminal.

**userid**

See ACID

**violation**

An illegal attempt to access a resource.

## Security Structure

The following chart illustrates how this company's security is structured. You may want to jot down the name and extension of your immediate department security administrator.

## Secure Logon Procedures

Your security administrator has assigned to you a unique userid and password. Your userid/password combination identifies you to CA-Top Secret and allows you access to the resources required to perform your job. It is imperative that you safeguard your userid/password. Abide by the following guidelines:

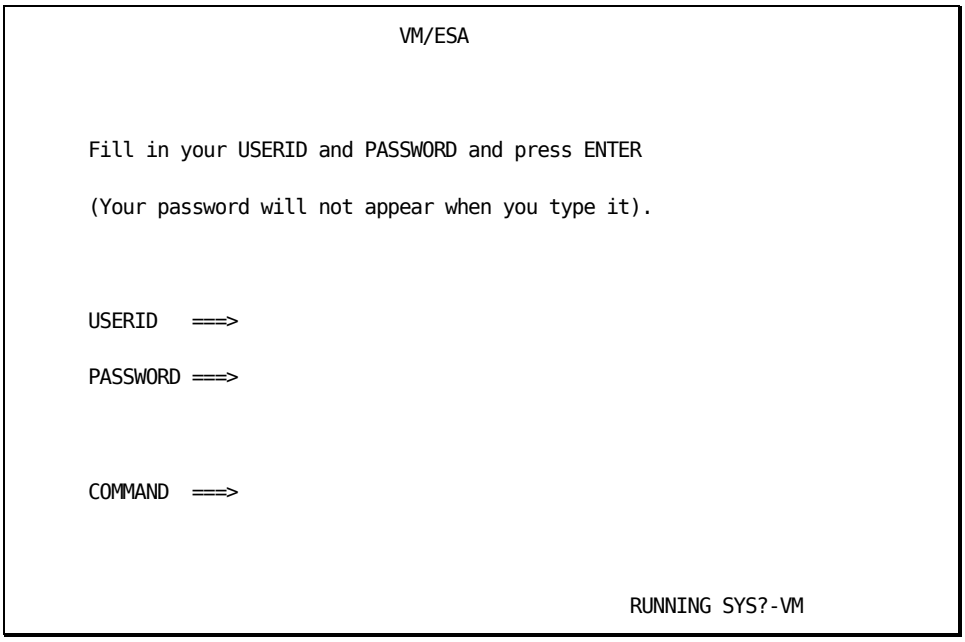
- MEMORIZE your userid/password upon receipt.
- All written records of your password must be DESTROYED.
- DO NOT post your userid or password near the video terminal, disks, cabinets, bulletin boards, or other areas accessible to unauthorized individuals.
- DO NOT maintain your password in an unprotected data set or CMS file where others might view it.
- DO NOT share your ACID or password with anyone. Personnel requesting the use of another's ACID or password may be directed to the appropriate security administrator.
- Inform your security administrator IMMEDIATELY if you suspect that your ACID or password has been compromised and request a password change.

# New User Logon

If you are a new user, your security administrator assigns a userid/password to you through the New User form. The form lists your userid, a first time password, and the facility to which your userid is authorized. To log on to the system the Standard Signon Procedure must be followed. Read through the Standard Logon and Password Change procedures for your facility before attempting to log on to the system. If questions arise, ask your supervisor for help.

# Standard Logon

CA-Top Secret changes the appearance of the logon process to a user logging onto a virtual machine.




To log on, enter the following:

- your userID
- your password

Press enter.

The following message displays:

```
TSS0130I Accessorid LAST-USED date time SYSTEM=logid FACILITY=fac

TSS0131I COUNT=nnnnn MODE=mode NAME=name

R;
```

When the R; prompt displays you have successfully logged on.

## First Time Logon

If you are logging on for the first time, you may receive the following CA-Top Secret message:

```
TSS0144E Password has expired. New password missing

TSS0102A Enter new_password, new_password/verify, or RANDOM
```

Choose one of the following procedures:

- Enter a new_password and press Enter. If the following message displays:

  ```
  TSS0120A Reenter new password for verification
  ```

  then enter your new password again.

- Enter a new_password/verify and press Enter. The following message displays:

  ```
  TSS0136I Password Changed
  ```

- Enter RANDOM and press Enter. The following message displays:

  ```
  TSS01341 Your new password is newpassword
  ```

## Password Change

Passwords automatically expire every 30 days. Each user is authorized (but not encouraged) to change the password at logon prior to the 30 day expiration. To change your CA-Top Secret password, perform the following procedure:

1. Enter LOGOFF or DISCONN and press Enter. Begin the LOGON process.
2. Enter Logon userid and press Enter. The following message displays:

   ```
   TSS0100A Enter password, LOGOFF, or HELP (it will not appear when typed):
   ```

3. Enter old_password/new_password and press Enter. If the following message displays:

   ```
   TSS0120A Reenter new password for verification
   ```

   Enter your new password again and press Enter.

4. Enter your new password and press Enter. The following message displays:

   ```
   TSS0130I Accessorid LAST-USED date time SYSTEM=logid FACILITY=fac

   TSS0131I COUNT=nnnnn MODE=mode NAME=name

   TSS0136I Password Changed

   R;
   ```

   When the R; prompt displays you have successfully logged on.

## New Password Rules

Use the following rules when selecting your new CA-Top Secret password:

- Password must be four to eight characters in length.
- You cannot repeat a character, for example, "bonnzo" is not acceptable.
- You can use a mix of alpha and numeric characters.
- You cannot use any of your last three previous passwords.

## Expired/Aging Passwords

Approximately five days prior to the automatic password expiration date, CA-Top Secret displays the following message each time you log on to a facility:

```
TSS0132I Password will expire soon on mm/dd/yy
```

Where: mm/dd/yy displays the month, day, and year that your password expires.

## Forgotten Passwords

If you forget your password, CA-Top Secret does not allow you to access a facility. Do not attempt to guess at your password. Notify your supervisor immediately. This supervisor contacts the Security administrator who is authorized to assign you a new password.

## Reporting Problems

If you experience a problem, perform the following steps:

1. When violation messages display, do not clear the messages from the screen.
2. Record all CA-Top Secret messages, IBM message numbers and accompanying text, or both.
3. Record all entries prior to receiving the messages.
4. Report the problem immediately to your supervisor.

## Requesting Resource Access

If CA-Top Secret is prohibiting you access to any resource that is necessary to perform your job, inform your supervisor immediately. You or your supervisor must fill out a Resource Access Request form. Central Security reviews your request and authorization may be granted.

## Emergency Access

In the case that a resource access is needed immediately, contact your Security Administrator. Security administrators are authorized to grant emergency access to users on a limited time basis. To acquire unconditional access, you must submit a Resource Access Request form.

## Off-Hours System Access

Off Hour Access is defined as non-business hours after 8.00 p.m. or before 6.00 a.m. during regular working days (including Saturdays) and at all times during holidays and Sundays.

Off Hour Access is granted when it is deemed necessary to meet business requirements. Contact your Security administrator. A minimum notice of 24 hours is mandatory.

# CA Top Secret Messages

The following lists CA Top Secret password-related messages.

**TSS0100A Enter password, LOGOFF or HELP (it will not appear when typed):**

**Reason:**

Informational message.

**Action:**

Enter your password, LOGOFF, or HELP and press enter.

**TSS0101A Please enter your current password. You may optionally change it.**

**Reason:**

You are being asked if you want to change your current password

**Action:**

Enter one of the following:

- To change your password, enter your current password, a forward slash, your new password, and press Enter:

  `password/new_password`

- To change your password and have the change verified, entere your current password, a forward slash, your new password, the word VERIFY, and press Enter.

  `password/new_password/VERIFY`

- To have the system change your password to a new, randomly generated password, enter your password, a forward slash, the word RANDOM, and press Enter.

  `password/RANDOM`

**TSS0102A Enter: new_password, new_password/verify, or RANDOM**

**Reason:**

Your current password has expired and CA-Top Secret is requesting that you enter a new one.

**Action:**

Follow the action detailed in message TSS0101A.

**TSS0130I acid LAST-USED date time SYSTEM=system FACILITY=facility**

**Reason:**

This informational message informs you when, on what system, and under which facility your ACID was last used.

**Action:**

None.

**TSS0142E FACILITY facility NOT AUTHORIZED FOR YOUR USE**

**Reason:**

You are not authorized to access the named facility.

**Action:**

None.

**TSS0143E PASSWORD IS INCORRECT**

**Reason:**

The password you entered is not correct.

**Action:**

Reenter your password. If you continue to experience problems, see your supervisor.

**TSS0144E PASSWORD HAS EXPIRED. NEW PASSWORD MISSING.**

**Reason:**

Your current password has expired.

**Action:**

Enter a new password.

**TSS0149E USE OF ACCESSOR ID SUSPENDED.**

**Reason:**

Your ACID is no longer valid due to an automatic or explicit suspension.

**Action:**

Contact your supervisor.

**TSS0152E ACCESSOR ID HAS BEEN INACTIVE TOO LONG**

**Reason:**

Your ACID is no longer valid due to inactivity.

**Action:**

Contact your supervisor.

**TSS0403E MINIDISK|DATA SET NOT ACCESSIBLE - name**

**Reason:**

An attempt was made to access the named minidisk or data set to which you are not authorized.

**Action:**

None.

**TSS0404E ACCESS NOT GRANTED TO MINIDISK|DATA SET**

**Reason:**

A requested function requires a minidisk or data set access level which you do not possess.

**Action:**

None.

# Security Features

You can monitor security using the following CA-Top Secret security features:

**TSS Last-Used Message**

CA-Top Secret displays the Last-Used message (TSS0130I). This message informs you when, on which System, and through which facility your ACID was last used. It enables you to detect illegal use of your ACID.

**TSS Status Message**

This message informs you how your session is processed regarding security. It also contains a current count of the number of times your ACID was used to submit batch jobs.

**TSS WHOAMI**

This message displays CA-Top Secret message number TSS0303I. This message contains information, such as user's facility, terminal id, system id, and mode, that can be helpful when reporting possible security problems.