CA Top Secret® for z/VM

Installation Guide

r12

Fifth Edition

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Examples of Commands to Build a CP Nucleus (see page 43)—Added an example for building a CP nucleus named TSSCP630; added note information to indicate that CAXABLD and CTLZ630 are required keywords prior to the VMFBLD command for z/VM 6.3.0.
- Task KVC0I099—Generate CMS Nucleus (see page 46)—Added a note about where to find information about generating a zCMS operating system; described what *prodid* value to use in the CAKVBLD command if your z/VM release z/VM 6.3.0; indicated that you must you must supply the ZCMSLOAD as the buildlist parameter (to build the zCMS operating system (z/VM R6.2.0 and above).
- Change Messages for z/VM 6.3.0 (see page 80)—Added this topic.

More Information:

CA Activator (see page 13)
Match an Activator Account to the MSCA ACID (see page 90)

Contents

Chapter 1: Preparing for Installation

This section describes what you need to know and do before you install the product.

This section contains the following topics:

Hardware Requirements

CA Top Secret for z/VM requires the following minimum hardware configuration:

- A z/Series, System/390, or compatible processor complex
- One tape drive, required to load the product tape
- Real or virtual unit record equipment (if you want messages to be printed)
- An IBM 3270 compatible terminal with at least 24 displayable lines

Software Requirements

CA Top Secret for z/VM includes support for z/VM Release 5.2.0 and above.

Read the Product Information Bulletins (PIBs) or Product Maintenance Letters (PMLs) accompanying the installation tape for information on IBM service prerequisites and special considerations for your specific IBM maintenance level, if any.

Server Machine DASD Requirements

CA Top Secret for z/VM requires permanent disk space as detailed in the following chart. The amount of space outlined in the chart will result in a disk usage of approximately 85%. All units are in cylinders, except for FBA devices, which are allocated blocks.

Not all of the devices listed are supported by all releases of z/VM.

Disk Type	Server SYSRES Files (0100, 0101, 0102, 0103) Minimum	Security File (0200) and Backup File (0500) Minimum using default blocksize	Audit File (0300) Recommended Audit2 File (0301) Optional	Recovery File (0400) Recommended	CPF Recovery (0600) Recommended
3330	7	39	16	14	25
3340	15	110	44	28	50
3350	5	20	8	5	18
3375	5	28	10	7	14
3380	3	14	6	5	10
3390	3	14	5	5	10
9345	3	14	7	6	12
FBA*	4096	14260	5580	5208	10002

* Fixed-block architecture (FBA) devices include 3310, 3370, 9332, and 9335.

Security and Backup File sizes assume the default of 5000 ACIDs. An Audit File of recommended size will hold approximately 14,500 violation records. A Recovery File of recommended size will hold approximately 10,000 Security File change records.

If you use the Command Propagation Facility (CPF), define a CPF Recovery File (0600). The size of this file should be a minimum of 10 3390 cylinders or equivalent. However, you should increase the size of this file if you are defining a large number of CPF nodes, if you expect CPF traffic to be heavy, or if some CPF nodes could be inactive for long periods of time.

Storage

CA Top Secret for z/VM installation requires a virtual machine storage size of at least 32 MB (32M).

The CA Top Secret for z/VM service machine has a recommended default storage size of 24 MB. The minimum recommended virtual storage size is 8 MB, although the efficient free storage management routines will result in a very small working set if less storage is actually required. For very large systems this may be expanded as needed.

CA Activator DASD Space Requirements

CA-Activator requires additional permanent disk space as detailed in the following chart. Approximate allocations are shown for disks formatted with a blocksize of 4 KB.

	Work Disk (191)	Test Disk (291)	Production Disk (391)	Production Generation (322)
Blocks	2000	8800	3000	1800

You should over-allocate all CMS-formatted disks by 30% to accommodate future maintenance.

Chapter 2: Implementing CA-CIS

This section contains the following topics:

About CA-CIS

CA-CIS is an architecture to promote the sharing of software services among applications and to provide the most efficient and effective processing of information across the enterprise.

When you install CA Top Secret, there are also components available through CA-CIS that provide added benefits and features to the product.

The options that CA-CIS offers with CA Top Secret include:

- CA-Activator
- Advantage™ CA-Earl®
- CAI Common Communications Interface (CAICCI)
- CA-ESM/VM

CA Activator

CA-Activator s required to install CA Top Secret.

The CA-Activator features include:

- Interactive, full-screen dialogs and HELP panels
- Customization steps that let you keep control of software installation
- Automatic incorporation of options during installation
- Recording of all software-solution options whenever needed

- Validation and demonstration of software installation

  Note: The CA Activator account must match the MSCA ACID to run product demonstration.

- Error-free maintenance

For information, see the CA-Activator *Reference Guide* and *Supplement*.

More information:

Match an Activator Account to the MSCA ACID (see page 90)

Advantage CA-Earl Reporting Service

The Advantage CA-Earl Reporting Service is a user-friendly report definition facility with the power of a comprehensive programming system. This component is required.

CAICCI

CAICCI, the Common Communications Interface, enables CA Top Secret to communicate with other CA products. This optional facility provides a layer that isolates application software from the specifics of the communications environment.

Some of CAICCI's features are:

- Single point of control
- Multiple platform support
- Performance optimization
- Program-to-program communication
- Dynamic installation configuration
- Ease of customization
- Error handling

Some of CAICCI's benefits are:

- Improved portability
- Supports complex distributed applications
- Eases operational burdens

CAICCI is an optional component and should only be installed if your site chooses to use the Command Propagation Facility (CPF).

When identifying CAICCI nodes using CPF, we suggest specifying a minimum MAXRU of 1024 or more, although a value of at least 4096 is recommended if it can be supported by your network configuration. If necessary, you can specify a MAXRU as small as 256, although a value this small may impact command response time, particularly when synchronous commands with large amounts of output are propagated over non-channel attached connections.

Regardless of what value you specify, that value must be consistent between all CAICCI nodes.

For information on MAXRU, see the CA-CIS *Reference Guide*.

CA-ESM/VM

CA-ESM/VM is the External Security Manager for z/VM, enabling CA Top Secret security to be extended to IBM Shared File System files, directories and administrative commands. This component is required if you are securing SFS resources or using the RACROUTE security interface.

For information on CAKVSFS EXEC, see the appendix “SFS Grant Authority Conversion Utility”.

For information on CA-ESM/VM, see the CA-CIS *Reference Guide*.

Chapter 3: Installation Procedures

This section contains the following topics:

Installation Tapes

CA Top Secret for z/VM is distributed on a single labeled tape. In addition, a CA-CIS for z/VM tape is distributed which contains the latest genlevel of CA-Activator as well as the latest genlevels of the other CA-CIS services.

One tape unit is required to install the product. CA-Activator automatically locates the components necessary to install the product and transfers them from tape to disk.

Several days before installation, check with your CA regional office or central support office to ensure that you have all Program Temporary Fixes (PTFs) beyond the base genlevel.

Define the CA-Activator Machine

If this is the initial installation of CA Top Secret at your site, you must designate a CA product maintenance virtual machine from which the product is installed and maintained. For information, see the *CA-CIS CA-Activator Reference Guide*.

You may already have installed other products using Common Infrastructure Services, at which time you defined a common CA-CIS product maintenance ID (such as CAIMAINT). Use this virtual machine to maintain this product. Sensitive files and non-public object code are migrated to a separate Production Generation disk when the product is moved to Production.

The Production System disk can safely be made available to decentralized administrative personnel and users of other CA products installed on the same disk. However, these non-public files is present on the Test System minidisk. For this reason, you may wish to install CA Top Secret on a separate maintenance user ID, particularly if many users have access to the Test system minidisk for administration and use of other products.

If you have already defined a CA product maintenance virtual machine for this product (or want to share an existing one), the only required steps are to increase the minidisks by the recommended sizes and to define a Production Generation minidisk (322).

These tasks are described in the CA-CIS *CA-Activator Reference Guide:*

- Define the CA-Activator product maintenance virtual machine.
- For CAIMAINT, CA Top Secret for VM installation requires a virtual machine storage size of at least 32 MB (32M).
  - CA-Activator requires additional permanent disk space as detailed in the following chart. Approximate allocations are shown for disks formatted with a blocksize of 4 KB.

	work disk (191)	test desk (291)	production disk (391)	production Generation disk (322)
Blocks	2000	8800	3000	1800

  - You should over-allocate all CMS-formatted disks by 30% to accommodate future maintenance.
  - The 191 disk (A-disk) holds the CA-Activator files.
  - The 291 disk holds all files loaded for the Test System.
  - The 391 disk holds Production System copies of administrative applications, tools, and public files.
  - The 322 disk holds the Production System copies of sensitive object code and system generation tools.

  As an additional safeguard, CA-Activator checks to be sure enough disk space is available before installing a new product.
- Load the CA-Activator files from the CA-CIS for z/VM tape to the A-disk.
- Customize CA-Activator's profile.

CA recommends that you define a new CA-Activator CAIMAINT machine for the r12 installation. This allows you to preserve your current CA-Activator environment during the conversion process.

Password Considerations

CA Top Secret replaces the logon password prompt interface and redefines the slash (/) character to separate the current logon password and optional new password. Do not enter a password with an imbedded slash (/) because CA Top Secret interprets it as two entries.

When implementing CA Top Secret, undefined users and users running in DORMANT or WARN modes are required to enter their CP directory password. If the user's password contains an imbedded slash, it is parsed incorrectly and logon is not allowed.

CP Level OS/DOS Data Set Considerations

In DORMANT mode with the SIOCHK option specified, CP level OS/DOS data set protection might deny access to a resource (or fail an I/O request) if it is unable to determine the resource being accessed. Test this feature with potentially incompatible applications before it is enabled in production. Some guest systems will require ACIDs with special attributes when this option is selected.

For information on the SIOCHK option, see the *Implementation Guide*.

VMCF and IUCV Protection

To enable IUCV security, see the OPTIONS control option in the *Control Options Guide*.

APPC Connection Security

To enable APPC security, see the OPTIONS control option in the *Control Options Guide*.

Migration Considerations

When planning your migration, consider:

- Moving CPF control options to NDT
- If using CPF, the CPF recovery file must be re-formatted using TSSMAINT prior to turning on CPF with r12 for the first time

Minimum Genlevels for File Sharing

To be compatible with CA Top Secret for z/VM r12, other systems must be at or above the following genlevels:

- CA Top Secret for z/OS, r5.3 SP01
- CA Top Secret z/VSE, r3 SP05
- CA Top Secret for z/VM r1.6

When sharing TSSVM with TSSVSE, note the following requirements:

- Operating System Requirements when using Options(22):
  - CA Top Secret for z/VM operation system r5.2 and above
  - CA Top Secret z/VSE r3.0
- Sharing requires maintenance on both CA Top Secret for z/VM, which is included on the SP2 genlevel tape, and CA Top Secret for z/VSE; therefore, contact Customer Support to obtain these solutions.

Installation Phases

Each CA product installation (initial or subsequent) involves the phases:

- Loading the product files from the distribution tape to the Test minidisk
- Generating the Test System from the loaded tape files
- Generating the Production System from the Test System

CA-Activator Installation Task Selection Menu

With system, test, or production, CA-Activator displays a list of tasks on the dynamic CA-Activator Installation Task Selection Menu (CACT-2121). The Installation Task Selection Menu appears whenever a task is executed or ended. The Task Selection Menu includes product and task information.

Possible task statuses are:

OPEN

Task is ready to be executed.

COMPLETE

Task has been successfully executed.

INCOMPLETE

Part of the task has not been successfully executed.

HAS PREREQ

Task cannot be opened because a prerequisite task has not been successfully executed.

O (OPTIONAL)

Execution of task is optional, dependent on previous task selection.

Use the Task Selection Menu to select tasks, enter:

- 1 to select a task for execution
- 2 to view list of task PREREQUISITES

When you install CA Top Secret using CA-Activator, the Installation Task Selection Menu lists the tasks to complete the installation.

To begin, select OPEN tasks to complete, in the order shown by entering 1 in the Option field.

Chapter 4: Generating the Test System

This section contains the following topics:

Task KVC0I90S—Select CA-CIS Services

This task selects the services used by CA Top Secret.

Follow these steps:

1. From the Task Selection Menu, select panel KVC0-I90S.
2. Specify the required CA-CIS services:

   Advantage CA-Earl

   A required service that is always selected.

   CAICCI

   Allows sites to administer multiple security files across VTAM-networked, TCPIP LV4, and TCPIP LV6 systems using CPF.

   CA ESM

   Support for Shared File Systems (SFS) external security and the RACROUTE macro.

3. Press F2

   The message "Action complete" appears when the CA-CIS services have been selected.

4. Press F3.

Note: If you receive message CACT015A on panel CACT-2121 indicating that CA-CIS services are required, load the required services from tape and complete installation of these services before continuing with the installation.

Task KVC0I000—Operating System Parameters

This task specifies the:

- z/VM operating system version and release level
- Processor configuration generated for
- z/VM user ID of the virtual machine used for maintenance of CP and CMS and that of the CA Top Secret server
- Virtual address for the Production Generation minidisk.

The information provided determines the installation task behavior and the selection of software modules. If you upgrade or reconfigure your z/VM system, update this information. It may be necessary to include different CA Top Secret object modules in your CP nucleus or to repeat installation tasks.

To specify the operating environment

1. From the Task Selection Menu, select panel KVC0-I000.
2. Specify the z/VM version and release level of your operating system.

   Each selection can describe more than one product or release level.

3. Enter the user ID (one to eight characters) of the virtual machine used for installation and maintenance of CP and CMS. Typically, this is a user ID named MAINT.
4. Enter the user ID to designate as the CA Top Secret server, for example TSSVM.

   If you are reinstalling the product, you may have already defined this user in the CP directory. This user is defined in a subsequent installation task.

5. Enter the user ID of the virtual machine to receive CA Top Secret server SYSOUT/VMDUMPS.
6. Define the Production Generation minidisk. The default is displayed, to define a different virtual address type over the default.

7. Press F2..

   The task executed.

8. Press F3.

Task KVC0I012—Select Shared Database

This task indicates if you are sharing your security database with another CA Top Secret security system. If the security database is shared, this task specifies the system that performs Security File backups. Record-locking features help ensure database integrity.

If your Security, Audit/Tracking, Recovery, and Backup files currently exist (on minidisks or on real OS volumes), you must provide appropriate CP directory control statements for the CA Top Secret server to gain access to these files. For information, see Task KVC0I030.

If you are planning to use the Single System Image feature of Z/VM 6.2 and later, we recommend all Top Secret servers within the cluster share the security database. This sharing complements the intent of this feature of a logical single image.

CA Top Secret for z/VM cannot share security files with:

- CA Top Secret for z/VM prior to 1.6
- CA Top Secret for z/OS prior to release 5.3
- CA Top Secret for z/OS security files that use VSAM

  Note: If you are sharing the security file between MVS and VM and the security file under MVS has been created with the AESENCRYPT option, this security file can no longer be shared between MVS and VM.

- CA Top Secret for VSE prior to 3.0

SHRFILE other than NO causes the server to ensure minidisk caching is turned off for the server files at start up.

To share your security database with another CA Top Secret security system

1. From the Task Selection Menu, select panel KVC0-I012.
2. Enter one of the following:
   - 2 for NO and press F2 to enter the information
   - 1 for YES and do one of:
     - If this system will backup the Security File, enter 1 and press F2.
     - If another system will backup the Security File, enter 2 and press F2.
3. Press F3.

Task KVC0I020—Select Optional Features

This task selects optional features for your CA Top Secret security system.

CP-level OS/DOS Volume and Data Set Protection

(Optional) This feature provides OS/DOS data set and volume protection from access by virtual machines, regardless of the guest operating system. This protection is implemented through the interception of virtual machine input and output operations by CA Top Secret's CP component.

If you select this feature, use the (NO)SIOCHK suboption of the FACILITY control option to activate or deactivate CP-level OS/DOS data set/volume protection.

Caution should be used when initially implementing this feature. In DORMANT mode with the SIOCHK option specified, CP level OS/DOS data set protection may deny access to a resource (or fail an I/O request) if it is unable to determine the resource being accessed.

CP level OS/DOS data set and volume protection may be installed concurrently with the CMS level database and volume protection feature.

To have CP-level OS/DOS volume and data set protection for z/VM 5.2.0 and above, put Options(19) in the Startup Parameter file.

RACF Compatibility Mode

This feature provides a mode in which the CA Top Secret server can be activated for creation of the CA Top Secret Security File only, while your current security software continues to protect your z/VM system.

To select optional features for your CA Top Secret security system

1. From the Task Selection Menu, select panel KVC0-I020.
2. Select CP-level OS/DOS data set/volume protection:
   - To select this feature, enter 1 and press F2
   - If this feature is not to be implemented, enter 2 and press F2

   Panel KVC0-I021 appears.
3. Select RACF Compatibility Mode requirement:
   - To select this feature, enter 1 and press F2
   - If this feature is not to be implemented, enter 2 and press F2
4. Press F3.

Task KVC0I025—Generate Utility Modules

This task generates the executable CA Top Secret utility and support modules.

To generate executable CA Top Secret utility and support modules

1. From the Task Selection Menu, select panel KVC0-I025.
2. Press F2

   The modules are generated.
3. Press F3.

Task KVC0I030—Define the Server

This task defines the server as a user in the z/VM CP directory.

This task contains the panels:

- KVC0-I030—Define the CA Top Secret Server
- KVC0-I031—Modify Prototype Directory
- KVC0-I032—Update CP Directory

For 3380 DASD models, the minimum number of cylinders for the Security/Backup Files is 14. The Audit and Recovery Files require at least one cylinder each.

The security database files are maintained on OS-formatted DASD volumes. If you have previously installed CA Top Secret, you may have allocated the security database files on real OS DASD volumes using the TSSMAINT utility.

If the security database files are not allocated on OS DASD volumes, each file (Security, Audit/Tracking, Recovery, Backup and CPF Recovery) must be placed (created) on its own minidisk and formatted during this task.

Important! Do not place the Security File on the same volume as the Backup or Recovery Files.

CA Top Secret z/VSE or z/OS cannot access Security database files formatted by this task.

When defining minidisks 100 to103 to the server, use RR as the link type. This link type allows the parameter file and the LMP key file to be updated from another machine while the CA Top Secret server is active.

For information about the server DASD requirements, see Server Machine DASD Requirements (see page 9).

To define the CA Top Secret server

1. From the Task Selection Menu, select panel KVC0-I030.
2. To define the CA Top Secret server using a prototype directory entry:
   a. Enter 1 and press F2

      Panel KVC0-I031 appears with a prototype directory.

   b. Match the prototype directory entry to your installation's requirements. Fields in lowercase require modification.

      Note: Panel KVC0-I031 may consist of two pages; press F8 to go to the next page.

      Note: XEDIT does not verify the accuracy or consistency of the answers. Use the program that updates your directory for this type of verification.

   c. Press F2

      The sample directory is saved in the file "*userid* DIRECT B," where *userid* is the CA Top Secret server ID specified in Task KVC0I000.

      Panel KVC0-I032 appears.

   d. Update the CP directory with the CA Top Secret server definitions. The panel automatically displays the file ID.
3. If the CA Top Secret server is already been defined
   a. Enter 2 and press F2.

   b. Exit this task or use another terminal to access the current CP directory source file and insert the sample directory entry with CA Top Secret server definitions.

   c. Issue the appropriate command to update the online CP directory. When the update is completed, reenter this task and press F2 to confirm action.
4. Press F3.

Software Requirements

CA Top Secret for z/VM includes support for z/VM Release 5.2.0 and above.

Read the Product Information Bulletins (PIBs) or Product Maintenance Letters (PMLs) accompanying the installation tape for information on IBM service prerequisites and special considerations for your specific IBM maintenance level, if any.

Task KVC0I035—Format Server SYSRES

Use this task to format or verify formatting of the CA Top Secret server's system residence (SYSRES) minidisk (100, 101, 102, or 103).

Formatting the CA Top Secret server's SYSRES minidisk:

- Links to the CA Top Secret server's SYSRES minidisk in WRITE mode. Before attempting to execute this task, make sure that no other machine has a WRITE link to this minidisk.

  Note: The CA Top Secret server only requires a READ link to this minidisk while CA Top Secret is active.

- Reserves space for the CA Top Secret server nucleus.

To format or verify formatting of the CA Top Secret server's sysres minidisk

1. From the Task Selection Menu, select panel KVC0-I035.
2. Enter the number preceding the minidisk you want to format and press F2.

   The SYSRES minidisk.is formated.
3. (Optional) If the minidisk selected is already formatted a message appears. If:
   - The disk label is TSSRES, and you do not want to reformat the minidisk, enter NO.
   - The disk label is not TSSRES or if it reads TSSRES but you still want to reformat the disk, enter YES.
   - You are upgrading from one release of CA Top Secret to another reformat the disk (after making a copy of your CA Top Secret PARMS and LMP files).
4. Press F3.

Task KVC0I042—Define Security Database Files

This task:

- Defines the data set name and ID for the files
- Formats the minidisk with WRITE password (if applicable)
- Creates the Security File with all the correct parameters.

If you are using existing CA Top Secret security database files, this task uses the existing information and does not format the minidisks.

This task contains the panels:

- KVC0-I042—Define Security Database Files (1 of 2)
- KVC0-I043—Security File Parameters
- KVC0-I044—Define Security Database files (2 of 2).

You can share the Security/Backup files, as well as the Audit/Recovery files with Release 1.2 and above of CA Top Secret for z/VM, and Release 4.3 and above of CA Top Secret for MVS (including CA Top Secret for z/OS Release 5.1). However, to provide auditing of greater than 44 byte resources, you must format a new Audit file that can only be shared with another 1.6 (or CA Top Secret for MVS Release 5.2 or CA Top Secret for z/OS Release 5.3) system and CA Top Secret for VSE 3.0 and above.

If this file will support mixed case passwords, run TSSXTEND after CA Top Secret is running. For information, see the appendix "Creating, Converting, or Extending The Security File".

To define your CA Top Secret security database files

1. From the Task Selection Menu, select panel KVC0-I042.

   The panel is displayed with default data set names.

2. Type over the existing characters. Entries are case-sensitive.

   File and vCUU

   No entry required. Security database files and device addresses are displayed.

   Data Set name

   Enter the OS-format data set names assigned to the CA Top Secret security database files or accept the default values.

   Range: Up to 44 characters

   Format MDISK and data set?

   Enter:

   - 1 to indicate that this file is to be newly created and formatted.
   - 2 if the security database files already exist or if you intend to format them using CA Top Secret for z/OS or VSE.

   If the CA Top Secret security database files are shared files, answer NO. If you answer NO, the data set names for the security database files specified must match already existing files on another system.

If yes, write password

If a WRITE password is necessary, enter the link password for the minidisk. The WRITE password may not be required, for instance if CA Top Secret is active from a previous installation and allows WRITE access. If it is required, you are prompted for it.

3. Files that do not appear on panel KVC0-I042 appear on panel KVC0-I044 after completion of panel KVC0-I042.
4. Press F2 .

   Panel KVC0-I043 is displayed..

   If the minidisk appears to already be formatted, you receive a message.
5. Enter YES.

   The Security File, Audit/Tracking File and Recovery File are each formatted independently.
6. Panel KVC0-I043, Security File Parameters

   To format the CA Top Secret Security File as part of the CA Top Secret security database, use this panel to specify or change parameters. The panel displays default and minimum values. Note that the data set names and ID entered on the previous panel are also displayed. Make the appropriate entries in each of the fields. Data specified for the Security File is used to automatically format the Backup File.

   ACCESSORS

   Indicates the maximum number of users, profiles, departments, divisions and zones defined in the CA Top Secret Security File. The five-digit value entered here determines the amount of Security File space allocated to hold ACID-related information.

   Minimum: 1000

   Default: 1000.

   BLOCKS

   Indicates the number of blocks for the Security File. Enter a five-digit value. There is no default. If you do not specify a number, then a value is calculated based on the values given for the ACCESSORS and VOLUMES parameters.

   BLOCKSIZE

   Indicates the block size for the Security File based on the type of file on which it is resident. Enter a four-digit value that must be a multiple of 256.

   Minimum: 8192

   DSN

   Indicates the data set name assigned to the Security File. The default is CAI.TOP.SECRET.SECURITY.FILE.

ID

Defines a name for the Security File.

Range: 1 to 8 characters

Default: PRIMARY

PIEBLOCKS

Specifies the number of blocks reserved for the PIE index. PIEs are used for ownership of maskable resources. Normally this value is not set and the number is calculated based on the value of the ACCESSORS= keyword.

Range: 1 to 9999

Default: Calculated by system

RESBLOCKS

Specifies the number of blocks reserved for the RIE index. RIEs are used for ownership of non-maskable resources.

Range: 1 to 9999

Default: 10

SCA/PASSWORD

This parameter identifies the ACID and password for the MSCA to CA Top Secret. Initially, it is the only ACID defined to CA Top Secret. The format is *msca*/*password* where *msca* is a one- to eight-character MSCA ACID and *password* is a four- to eight-character password assigned to that ACID. The password expires after the initial logon and can be changed at that point. However, the user can issue the TSS REPLACE function to specify a time interval for the MSCA's new password. If the user does not specify a time, the default expiration for that password is five days. There is no default for the SCA; it must be specified.

```
TSS REPLACE (MSCA) PASSWORD(PASSWORD|*[,0...255]
```

SDTBLOCKS

Specifies the number of blocks reserved for the special SDT record on your system.

Range: 2 to 256

Default: 2

MAXACIDSIZE

Allows a site to determine larger than normal ACID sizes. Values are in 1024 increments.

Range: 256 to 512

Default: 256

VOLUMES

Indicates the number of volumes/prefixes defined to CA Top Secret. This six-digit value determines the amount of Security File space allocated to hold volume-related information.

Default: 500

7. Press F2

   Panel KVC0-I044 is displayed.

8. Complete this panel and press F2.

   The task executes.

9. Press F3.

Task KVC0I050—Set Customer Encryption Key

Use this task to assign the customer encryption key. The encryption key is unique to your installation and is used to encrypt information in the Security File.

If you are installing CA Top Secret in a shared security environment, make certain that the encryption key you specify is identical in all systems sharing the Security File.

The encryption key is permanent. Information in the Security File is encrypted using this key beginning with the first access by CA Top Secret after formatting. Subsequently, you can change it only by beginning again from Task KVC0I042 and reformatting the Security File.

Important! The encryption key is stored permanently in the file TSSVMI TEXT, on CA-Activator's Test or Production Generation minidisks. Use caution in granting user access to these minidisks.The encryption key is unique to your site. A high-level security administrator should keep it in a safe place. It is needed in the future for recovery procedures

To assign the encryption key

1. From the Task Selection Menu, select panel KVC0-I050.
2. Do one of the following:
   - Enter an eight-character string. This is automatically translated into 16-digit hex. These entries are case-sensitive.
   - Enter a 16-character hexadecimal string. Valid entries include: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.
3. Press F2.

   The encryption key is displayed.
4. Press F3.

Task KVC0I055—Select/Retrieve Installation Exit

Use this panel to indicate whether you are using the CA Top Secret Installation Exit. When this task is executed, the Installation Exit is retrieved and copied to the Test minidisk (291).

The CA Top Secret Installation Exit must be in place prior to executing this task.

To indicate whether you are using the CA Top Secret Installation Exit

1. From the Task Selection Menu, select panel KVC0-I055.
2. Do one of the following:
   - To use the CA Top Secret Installation Exit:
     a. Enter 1
     b. Enter the user ID (one to eight characters) of the minidisk where the CA Top Secret Installation Exit text resides.
     c. Enter the device address of the minidisk in the vdev field.
     d. (Optional.) If the minidisk containing the CA Top Secret Installation Exit requires a READ password, you are prompted for the password. Enter the READ password (one to eight characters) for the minidisk.
     e. Press F2 to execute this task.

        The CA Top Secret Installation Exit is copied to the Test minidisk (291).
   - If the CA Top Secret Installation Exit is not used, enter 2 and press F2.
3. Press F3.

Task KVC0I061—Generate Server Nucleus

Use this task to:

- Generate the CA Top Secret server operating system nucleus. The nucleus is then written to the CA Top Secret server's SYSRES minidisk (100, 101, 102, or 103).
- Regenerate the operating system nucleus any time you update the CA Top Secret Installation Exit or apply APAR maintenance to any of the server modules.

When the server nucleus is written to the SYSRES minidisk, you must re-IPL CMS. When the system is successfully IPLed, reenter this task to verify generation of the server nucleus.

This task consists of the panels:

- KVC0-I061—Generate Server Nucleus
- KVC0-I062—Load Server Nucleus

- KVC0-I063—Verify Server Nucleus Generation

READ/WRITE access to the CA Top Secret server's SYSRES minidisk is required and requested using a selected MULTI-READ link. You may need to specify the server's SYSRES minidisk MULT password.

To generate the CA Top Secret server operating system nucleus

1. From the Task Selection Menu, select panel KVC0-I061.
2. Select the target vcuu address to hold the server nucleus.
3. Press F2

   The CA Top Secret nucleus is generated. A server load deck is created and resides in your virtual reader.
4. If prompted, enter the MULT password for the server SYSRES minidisk chosen previously.

   Note: Although the MULT password is requested, this procedure does not link in MULTI-WRITE mode. Rather, a MULTI-READ link is requested to obtain exclusive WRITE access while tolerating existing READ-only links.
5. From panel KVC0-I062, do one of the following:
   - Press F2 to IPL the reader. Go to Step 6.
   - Press F3 to quit.

   Note: This panel automatically closes and the CMS terminal session is lost. The IPL is done at the CP level. This only affects your virtual machine user ID, not the real z/VM system.
6. If the IPL is successfully completed, the following message appears:

   ```
   HCPGIR450W CP ENTERED; DISABLED WAIT PSW 000A0000 00000000
   ```

   - You must receive this message for a successful IPL and to continue this task. If the above message is received, IPL CMS, reenter CA-Activator.
   - If you do not receive this message, or if it appears in a different form, or with a value other than zeros (00000000) in the last word, then the server nucleus was not generated successfully. Consult the list of server wait state codes in the *Messages and Codes Guide*.
   - The PSW code list includes invalid codes, reasons for the error, and an action to rectify the error. Review the list and make the appropriate action to correct the problem.
   - Reenter CA-Activator and reopen panel KVC0-I061. Repeat this procedure beginning with Step 1, to generate the server nucleus.

   Panel KVC0-I063 lets you verify that the server nucleus has been generated. As a result, a server load map now resides in your virtual reader. The CA Top Secret server load map is also checked for errors at this time.

7. Enter **1** for CONFIRM and press F2.

   The server load map is saved and inspected for errors. The following message appears:

   ```
   Load map has been saved in file 'TSSNUC MAP'
   Checking map for errors...Please wait
   ```

   If errors are found in the server load map, one of the following error messages appears:

   ```
   Error - undefined external references detected
   ```

   ```
   Errors detected in load map. Task not completed. Press ENTER to return to
   CA-Activator.
   ```

   Correct the error and enter **2** for RESTART and press F2 to restart the procedure to regenerate the server nucleus. Go to Step 1.

   The task is completed. The server nucleus is generated.

8. Press F3.

Task KVC0I065—Enter LMP Key

Use this task to enter a new, or update an existing LMP key. The LMP KEY must be placed on each server SYSRES volume that is used (100, 101, 102, or 103). This task is independent of the generation of the server nucleus and can be used annually to update the file with the site's new key. It can be done while the server is running. When it is placed on the currently active server SYSRES, the updated key is used for the next LMP key check by the server.

CA Top Secret is an LMP key-controlled product. A valid LMP key must be supplied to run the product cleanly.

READ/WRITE access to the CA Top Secret server’s SYSRES minidisk is required. It is requested using a selected MULTI-READ link. You may need to specify the server’s MULT password.

Use this task any time the LMP key file needs to be created or updated. Make sure that the updated key is placed on every SYSRES minidisk that is used in your environment. This task can be selected multiple times to update all the disks required.

To enter a new, or update an existing LMP key

1. From the Task Selection Menu, select panel KVC0-I065.
2. Select the target vCUU address to receive the updated LMP key and press F2

   The LMP key file on the selected minidisk is updated.

3. If prompted, enter the MULT password for the server SYSRES minidisk selected in the previous step.

   Note: Although the MULT password is requested, this procedure does not link in MULTI-WRITE mode. Rather a MULTI-READ link is requested to obtain exclusive WRITE access while tolerating existing READ-ONLY links.

4. The file CAILMP KEYS is opened using XEDIT. It will contain the contents of an already existing file or a single-line dummy entry. Comment records can be added to the file by putting an * in column one of a line.

   Note: If sharing a server 100 disk across multiple CPU's you may include all keys in this file. Each CPU will look for it's match key during LMP key processing

5. When the file has been updated, type FILE.

   The task completes.

CAIRIM KEYS dd File Record Coding Conventions

The CAIRIM KEYS dd is a file comprised of 80-byte records. These records may be broken into four logical fields:

- The first is in position 1. If an "*" is found in this field, then the record is treated as a comment.
- The second field is located in positions 2 through 71 of the record, and contains the CALMP Control Statement data.
- The third field is in position 72. If a "-" is found here then this Control Statement is continued on the next record.
- The fourth field is in positions 73 through 80 and may be used for numbering the records.

With the introduction of SITEID processing, it is necessary to allow Control Statements to be broken in the middle of a verb. This is accomplished by coding a " +" (blank space and the plus sign) at the point in the verb data that you wish to break the verb and by adding a "-" (minus sign) in position 72. The data is then continued on the next record.

If you are attempting to break the data in a verb at a space then the space must be included followed by the " +" so that the last 3 characters of the verb look like " +" (2 spaces and a plus) followed by a "-" in position 72.

The Control Statements are not case sensitive, they may be all upper case, all lower case, or a mixture of both.

Examples:

```
1xxxxxxxx1xxxxxxxxx2xxxxxxxxx3xxxxxxxxx4xxxxxxxxx5xxxxxxxxx6xxxxxxxxx7xxxxxxxx8
*                                                                       00010000
*  CALMP KEYS FOR CAIRIM                                                00020000
*                                                                       00030000
SITEID(00123456) SITECODE(ETH2PHQZTXQPXGXRK7ZPT)                       -00050000
   NAME(SUPER DUPER LONG CLIENT NAME AND THIS ONE IS BIG  +             -00060000
                ENOUGH)                                                 00070000
*   SITEID(98765432) SITECODE(AFM3XC43BPASTBG0FUUY8)                   -00090000
*      NAME(THIS IS A LONG CLIENT NAME)                                 00100000
PRODUCT(SO) DATE(19JUL12)                                              -00140000
      CPU(3090-****/ +                                                 -00150000
             071966) LMPCODE(42E2LZA66ZC7RZDD)                          00160000
PRODUCT(SO) DATE(12DEC12)                                              -00170000
      CPU(3090-****/071966) LMPCODE(22E2LZA  +                         -00180000
             663Z7RZDE)                                                00190000
PRODUCT(L0) DATE(12DEC12)                                              -00200000
      CPU(3090-****/071966) LMPCode(HHGHP8DRRC81T8LG)                  00210000
EKG(35575167)                                                          00220000
PROD(L0) DATE(25DEC11)                                                 -00230000
      CPU(3090-****/456789) LMPCODE(8HGHERW1DC91T8L6)                  00240000
```

```
*    PROD(KO) DATE(05MAR10)                                          -00250000
*       CPU(SITE-****/123456) LMPCODE(HEETFYCEP4QED75B)               00260000
PROD(KO) DATE(11NOV12)                                               -00270000
      CPU(SITE-****/123456) LMPCODE(9EE5CYCEPBB8D75T)                 00280000
```

Records 00060000, 00150000, and 00180000 show that the operand was continued on another record by coding a " +" (blank followed by a plus sign) as the last 2 characters of the operand on the record to be continued and by adding a "-" in column 72.

Records 00060000, and 00180000 show that in order to break at a blank you must code that blank along with the " +" (blank followed by a plus sign) so that in the Control Statement there is a " +" (2 blanks followed by a plus sign) at the end of the verb data which is followed by the "-" in position 72.

Records 0060000, and 00090000 show that only one SITEID Control Statement may appear in the KEYS dd file, and it must be the first Control Statement aside from comments in the File. The multiple SITEID Control Statements in the example are examples of different formats.

Records 0090000, 00250000, and 00260000 are examples of a commented out Control Statement.

Records 00250000 and 00280000 are examples of a Product Execution Key using SITEID processing.

Task KVC0I070—Customize Startup Parameters

Use this task to specify or change CA Top Secret control options in the Startup Parameter File. The Startup Parameter File (CA Top Secret PARMS) is created during the installation process. This task writes the modified CA Top Secret PARMS file on the CA Top Secret server's SYSRES minidisk. If you are working in a shared security environment, this task will access the existing CA Top Secret PARMS file for modifications.

This task consists of the panels:

- KVC0-I070—Customize Startup Parameters. This panel provides instructions for the task.
- KVC0-I071—Startup Parameter File. This panel provides a prototype CA Top Secret PARMS file for modifications.

Specifying or changing the data in the CA Top Secret PARMS file defines the control options that is in effect as of the next IPL or server restart. These control options control the CA Top Secret security environment and operation.

If you have previously installed an CA Top Secret product, or you are working in a shared environment, the existing CA Top Secret PARMS file is accessed. The control options specified for the previous installation is checked for consistency against the specifications for this installation. This task lets you select automatic correction of entries in the existing CA Top Secret PARMS file.

To specify or change control options in the Startup Parameter File

1. From the Task Selection Menu, select panel KVC0-I070.
2. Press F2

   Panel KVC0-I071 displays a prototype CA Top Secret PARMS file.
3. Make the appropriate entries in each field and press F2

   The entries are saved on the server's SYSRES disk as specified in KVC0I061.
4. Press F3.

The CA Top Secret PARMS file being updated should be saved to the same vcuu selected to hold the server nucleus in task KVC0I061.

Important! The default mode setting for CA Top Secret is MODE(FAIL). You may change this to MODE(DORM) before starting CA Top Secret for the first time.

Task KVC0I075—Send CAKVBLD to System Maintenance Machine

Task KVC0I079 and Task KVC0I099 require the addition of CA Top Secret modules to the system load list. These modules must be accessible in the system maintenance machine during the build of the nucleus. To accomplish this, CA Top Secret provides an additional utility called CAKVBLD. This EXEC must be loaded permanently into the system maintenance user's 191 minidisk.

This task consists of the panels:

- KVC0-I075
- KVC0-I076

To send CAKVBLD to your system maintenance machine

1. From the Task Selection Menu, select panel KVC0-I075.
2. Press F5.

   The SENDFILE command is invoked and CAKVBLD EXEC is sent to the system maintenance user for CP and CMS.
3. Press F3.

   The task closes.

4. Log on to the appropriate system maintenance machine and enter:

   ```
   QUERY RDR * ALL
   ```

   A response similar to the following displays:

   ```
   ORIGINID FILE CLASS RECORDS CPY HOLD DATE TIME NAME TYPE DIST
   CAIMAINT 1234 A PUN 00000xx 001 NONE mmdd hhmmss CAKVBLD EXEC ????
   ```

5. Locate the entry for the CAKVBLD EXEC in your RDRLST and note the spool ID number (under the second column of the header above).

6. Enter:

   ```
   ACCESS 191 A
   RECEIVE NNNN = = A
   ```

7. Reenter CA-Activator, if necessary, and from panel KVC0-I075, press F2 to confirm that all instructions on the panel have been successfully completed.

8. Press F3.

Task KVC0I079—Rebuild the CP Nucleus

When applying z/VM maintenance, you must perform the following activities:

- Regenerate the CP nucleus with the CA Top Secret CP modules
- Point to the current CP IBM maintenance mini disk

Use this task to rebuild your current CP nucleus with CA Top Secret CP modules.

Rebuilding the CP nucleus consists of the following panels:

- KVC0-I079
- KVC0-I085

Important! To build the required CA Top Secret modules into the CP nucleus, the most current version of these modules must be accessible to the z/VM service EXECs and the current IBM z/VM maintenance disks during the build. If you applied IBM z/VM CP maintenance, you must rebuild the CP nucleus with the CA Top Secret modules.

The CP nucleus module generation resembles the standard IBM VMFBLD process but includes a CAXABLD prefix that precedes the VMFBLD EXEC.

To rebuild your current CP nucleus with CA Top Secret CP modules:

1. Create a copy of the CP nucleus on the CP parameter disk (for system recovery if a problem occurs with the new CP nucleus).
2. From the Task Selection Menu, select task ID KVC0-I079.

   You are transferred to the appropriate panel, based on your operating system selection.
3. Log on to your CP system maintenance machine.

   You can disconnect from your current terminal to perform the logon (if you do not have access to more than one terminal) or use another terminal.
4. Perform any IBM required steps prior to VMFBLD.

   Examples of what might be needed are VMFSETUP and VMFPF EXECs.
5. Perform one of the following steps (depending on whether you are regenerating a test system or production system):
   - (TEST module generation) Link to and access CAIMAINT virtual machine's 291 disk.
   - (PRODUCTION module generation) Link to and access CAIMAINT virtual machine's 391 and 322 disks.
6. Generate the CP nucleus module, using the supplied CAXABLD EXEC to prefix the standard VMFBLD EXEC.

   By default, the CP modules are placed on the 493 disk and must be moved to the CP parameter disk CF1. Both 493 and CF1 are defaults only and may be redefined by your system.
7. Save the CP LOAD map and the CAXALOAD SUMMARY A1. CA Support might need this information to debug problems.

Examples of Commands to Build a CP Nucleus

This example builds a CP nucleus named TSSCP520 containing CA Top Secret:

```
CAXABLD CTLZ520 VMFBLD PPF ZVM CP CPLOAD * NUCTARG MODULE MODNAME TSSCP520 (ALL
```

This example builds a CP nucleus named TSSCP530 containing CA Top Secret:

```
CAXABLD CTLZ530 VMFBLD PPF ZVM CP CPLOAD * NUCTARG MODULE MODNAME TSSCP530 (ALL
```

This example builds a CP nucleus named TSSCP540 containing CA Top Secret:

```
CAXABLD CTLZ540 VMFBLD PPF ZVM CP CPLOAD * NUCTARG MODULE MODNAME TSSCP540 (ALL
```

This example builds a CP nucleus named TSSCP610 containing CA Top Secret:

```
CAXABLD CTLZ610 VMFBLD PPF ZVM CP CPLOAD * NUCTARG MODULE MODNAME TSSCP610 (ALL
```

This example builds a CP nucleus named TSSCP620 containing CA Top Secret:

```
CAXABLD CTLZ620 VMFBLD PPF ZVM CP CPLOAD * NUCTARG MODULE MODNAME TSSCP620 (ALL
```

This example builds a CP nucleus named TSSCP630 containing CA Top Secret:

```
CAXABLD CTLZ630 VMFBLD PPF SERVP2P CP CPLOAD * NUCTARG MODULE MODNAME TSSCP630 (ALL
```

Notes:

- CAXABLD and CTLZ520 are required keywords prior to the VMFBLD command for z/VM 5.2.0.
- CAXABLD and CTLZ530 are required keywords prior to the VMFBLD command for z/VM 5.3.0.
- CAXABLD and CTLZ540 are required keywords prior to the VMFBLD command for z/VM 5.4.0.
- CAXABLD and CTLZ610 are required keywords prior to the VMFBLD command for z/VM 6.1.0.
- CAXABLD and CTLZ620 are required keywords prior to the VMFBLD command for z/VM 6.2.0.
- CAXABLD and CTLZ630 are required keywords prior to the VMFBLD command for z/VM 6.3.0.
- To review information of all keywords after VMFBLD, see the IBM manual *VMSES/E Introduction and Reference*.
- If you did not select OS/DOS data set/volume protection with Task KVC0I020, you see unresolved external references in the CP load map for various entry points with names beginning with TSSVOL and TSSVOM. Ignore these particular unresolved references.

Task KVC0I090—IPL CP System

Use this panel to confirm that all CP and CA Top Secret server components are installed. IPL the z/VM system to load the CP component modules. When the IPL is complete, activate CA Top Secret by AUTOLOGging the CA Top Secret server.

The CP and CA Top Secret modules must be in place before IPLing the z/VM system. This task must be completed before executing Task KVC0I099.

To confirm that all CP and CA Top Secret server components are installed

1. From the Task Selection Menu, select panel KVC0-I090.
2. Read the instructions on the panel and press F2.
3. Press F3.

   The Activator exits.
4. To activate CA Top Secret, AUTOLOG the CA Top Secret server, enter (X)AUTOLOG and the user ID for the CA Top Secret server.

When the installation has been verified, add an (X)AUTOLOG command to the PROFILE EXEC of your AUTOLOG1 virtual machine so that the next time the system is IPLed, CA Top Secret is activated automatically.

The supplied WAIT4TSS EXEC, found on CA-Activator's Test or Production minidisk, is useful for suspending AUTOLOG1 operation until CA Top Secret is fully initialized.

Task KVC0I092—SFS ESM Modifications

CA-CIS Task 3711I010 (CA-ESM z/VM Module Generation) must be completed before executing this task.

Use this task to confirm that the CP directory entry for each SFS service has been updated to allow it to connect through IUCV to the CA Top Secret service machine and to link to the CA-Activator disk containing the RPIUCMS module. A similar IUCV statement must be added to each SFS service machine entry that is utilizing external security. The CA Top Secret service machine's CP directory entry must have a corresponding IUCV statement for the SFS machines that is utilizing its service for ESM. The last file that needs to be modified prior to turning on external security is the SFS DMSPARMs file. This file holds a parameter that must be changed from NOESECURITY to ESECURITY to activate SFS ESM.

To confirm that the CP directory entry for each SFS server has been updated

1. From the Task Selection Menu, select panel KVC0-I092.
2. Read the instructions on the panel and make the necessary changes to the appropriate files.
3. Press F2.
4. Press F3.

   CA-Activator exits.

Task KVC0I093—Update CAIRPI PARMS File for SFS

This task updates the CAIRPI PARMS parameter file with the user ID of the CA Top Secret service machine. When SFS initializes, the RPIUCMS module reads this file to determine the user ID SFS should IUCV connect to establish external security. You can indicate that the changes needed have been made previously or you can allow them to occur through the panel.

This task consists of the panels:

- KVC0-I093—Update CAIRPI PARMS file for use by SFS
- KVC0-I094—Update CAIRPI PARMS file for use by SFS
- KVC0-I095—Update CAIRPI PARMS file for use by SFS

The CAIRPI PARMS file must reside on the CA-Activator disk used for the installation of CA Top Secret. The user ID defined in task KVC0-I000 as the CA Top Secret server is inserted into the CAIRPI PARMS file. Panel KVC0-I094 displays the updated file and F2 saves it to disk. Panel KVC0-I095 displays the name and location of the parameter file.

Task KVC0I099—Generate CMS Nucleus

Use this task to update your current CMS nucleus load list with CA Top Secret CMS modules.

This task consists of the following panels:

- KVC0-I099—Generate CMS Nucleus
- KVC0-I104—Generate CMS Nucleus Enhanced

To build the required CA Top Secret modules into the CMS nucleus, the system load list must be modified. In addition, the most current version of these modules must be accessible to the z/VM service EXECs during the build.

To accomplish this build in the enhanced z/VM maintenance structure, the CAKVBLD command creates a temporary, updated copy of the system build list and a temporary Product Parameter File (PPF) override file. CAKVBLD passes these files to the standard z/VM service routine to build the nucleus.

The system generation method invoked by this task is dependent on the operating system selected for generating CA Top Secret.

Note: Full support of zCMS started with z/VM 6.2.0. For information about generating a zCMS operating system, please see the appropriate IBM manual.

To update your current CMS nucleus load list with CA Top Secret CMS modules

1. From the Task Selection Menu, select task ID KVC0-I099.

   You are transferred to the appropriate panel, based on your operating system.

2. Access another terminal, and log on to your CMS system maintenance machine.

3. Issue the CAKVBLD command to rebuild the CMS nucleus.

   The general format of the command is as follows:

   CAKVBLD *prodid compname* <*buildlist*> (TEST|PROD <*vmfbld_options*>

   prodid

   Specifies the filename of the Product Parameter File (PPF) normally used to build your CMS system. If you are accustomed to using the VMFBLD command to build your CMS nucleus, use the same **prodid** or PPF for this parameter as you would specify in the VMFBLD command. You may specify an override file here, if applicable.

   If you have previously used the ITASK command to build the CMS nucleus, you should specify the z/VM product number that is the default PPF filename for the product. ITASK uses this default filename when it executes the VMFBLD command. Select the appropriate *prodid* value for your z/VM release as follows:

   - For z/VM 6.3.0, use SERVP2P.
   - For all other z/VM releases, use ZVM.

   compname

   Specifies the component name you usually specify when building your CMS system. You can specify an override component such as CMSOPT. Note that the component name specified here must exactly match those used to generate your CMS system without CA Top Secret as well as the PF filename and build list.

buildlist

(Optional) Specifies the build list name, as in the VMFBLD command. Typically, for CMS, the default CMSLOAD is used.

Important! To build the zCMS operating system (z/VM R6.2.0 and above), you must supply the ZCMSLOAD as the buildlist parameter.

TEST

Indicates that the Test System is generated. If specified, you *cannot* specify PROD.

PROD

Indicates that the Production System is generated. If specified, you *cannot* specify TEST.

vmfbld_options

Specifies any options valid for the VMFBLD command. The specified options are passed to VMFBLD when this command is executed.

Note: The CAKVBLD command supersedes the VMFBLD or ITASK build step in the z/VM installation procedures. You must, however, complete the remaining procedures.

Issuing CAKVBLD performs the following activities:

- Links to the CA-Activator Test System minidisk or the Production Generation minidisk, according to your specification.
- Reads your PPF file, your PPF override file, and the base PPF. Then it generates a temporary PPF override file called $CAKVCMS $PPF. Your original PPF files are not modified. This temporary override file is used to generate your CMS nucleus.

  The temporary override file contains new definitions that supplement your base PPF CMS component to include a new local disk (the CA-Activator Test or Production Generation minidisk) and to define the temporary build list ($CAKVCMS EXEC). If your original CMS component was an override component, it is included in its entirety in the temporary PPF, in addition to the above changes.

- Invokes VMFSETUP to establish the proper disk search order as follows:

  ```
  VMFSETUP $CAKVCMS compname ( ACCESS BLD
  ```

- Creates a temporary build list, $CAKVCMS, by adding CA Top Secret modules to your original build list.
- Invokes VMFBLD to build the nucleus using the temporary PPF and build list. The VMFBLD command will include any *vmfbld_opts* you specified in the CAKVBLD command.

The CA Top Secret generated temporary files are not erased, so you can inspect them in case of build errors.

Note: Usually the CMS and zCMS build process punches the output (which is usually spooled to a reader). IPLing from the reader will cause the process to want to write to the boot sector of the appropriate disk (190 – CMS and 990 – zCMS). Make sure the appropriate disk is linked WRITE for this function.

We recommend saving the load maps of the newly created CMS systems for diagnostic purposes later.

4. Reconnect if necessary, and from panel KVC0-I104, press F2 to finish the task.
5. Press F3.

Task KVC0I110—Install CA-Register Interface

Execute this task to allow registration of users into CA Top Secret through the CA-Register interface.

CA-Register administrators will need to be linked to both the CA-Register and CA Top Secret maintenance disks (if they are not installed on the same maintenance ID) to register users into CA Top Secret.

When the CA-Register interface is installed, the CA-Register server must be recycled to load the CA Top Secret exit program.

To allow registration of users into CA Top Secret

1. From the Task Selection Menu, select panel KVC0-I110.
2. Enter a default prototype ACID if one is desired. The default prototype is an ACID is used as a skeleton for defining attributes of a new user.
3. Enter the user ID of the CA-Register maintenance ID. This is required if CA-Register is not installed on the same user ID as CA Top Secret.

4. Do **one** the following, based on whether CA-Register is installed on the same maintenance ID as CA Top Secret:

   - (CA-Register installed on the CA Top Secret maintenance ID) Press F2 to execute the update of the REGISTER APPLS file for CA-Register. When you complete this task, proceed to step 8.
   - (CA-Register installed on another maintenance ID) Press F9 to set up for updating the REGISTER APPLS file for CA-Register. When you complete this task, continue with step 5.

5. Press F5 to send the CA Top Secret exit program for CA-Register (CAKVRGST EXEC) to the CA-Register maintenance user ID.
6. If necessary, disconnect from the CA Top Secret maintenance user ID then log on to the CA-Register maintenance user ID to perform the following tasks:

   - Receive file CAKVRGST EXEC on to the 291/391 disk.
   - Using CA-Activator, execute CA-Register installation task S510I002 - Define REGISTER APPLS file. Include an entry for CA Top Secret as defined on panel KVC0-I110. Press F2 to save the entry then exit CA-Activator and log off.

7. If necessary, reconnect to the CA Top Secret maintenance user ID and press F2 to confirm installation of CA-Register interface.
8. Press F3.

Chapter 5: Generating the Production System

This section contains the following topics:

About the Production System

Generating the Production System is accomplished through the CA-Activator Product Installation Menu. The procedures take the product components in their validated state and move them to the Production System and Production Generation minidisks. This phase should be completed only after the product genlevel and all maintenance applied to the Test System have been thoroughly tested.

Access the Product Installation Menu

To access the Production Task Selection Menu

1. From the Test System Task Selection Menu, press F3 twice.

   The CA-Activator Product Installation Menu is displayed.

2. From the Product Installation Menu, select option 3.

   The Generate Production System Menu is displayed.

3. Enter 1 to select CA Top Secret.

   The Production Task Selection Menu appears. All tasks are marked as complete except Production Task KVC0P001, Copy Component Files to Production.

TASK KVC0P001—Copy Component Files to Production

This task keeps the Production System minidisk up to date with the current level of software. Use this task to copy all CA Top Secret Test System files, including any software maintenance that has been applied, from the Test minidisk (291) to the Production minidisk (391) and the Production Generation minidisk (322 by default).

The public product files associated with end-user and administrative activities is copied to the Production System minidisk. This minidisk can safely be made available to decentralized security administrators and application systems (for instance, those requiring program access to the Standard Security Facility translator).

Non-public files, including CA Top Secret object code and files containing sensitive information, is copied to the Production Generation minidisk. This minidisk should be protected and only the System Maintenance user ID should be permitted access to it for system generation purposes.

When this task is complete, you can generate the Production CA Top Secret server or CP and CMS using Production System generation tasks. If you do not have a separate Production server or z/VM system, regeneration is unnecessary. The Production System represents the latest validated CA Top Secret software level. To back out of a subsequently updated Test System, recreate the latest proven software configuration using Production System generation tasks.

To copy component files to your production system

1. From the Task Selection Menu, select panel KVC0P001.
2. Press F2

   Test System files are migrated to the Production minidisks.
3. Press F3.

   The Task Selection Menu is displayed.
4. If necessary, repeat any previous tasks to generate the Production System.

After Task KVC0P001

You might need to execute some of the remaining tasks. For instance, if you maintain a second-level z/VM system with its own z/VM software and server for testing the latest CA product maintenance (or an individual APAR) this system should be generated by generating the Test System. After verifying the effect and reliability of the maintenance, you would migrate the Test System software to your Production System and regenerate your first-level system using selected tasks from the Production Task Selection Menu.

You might also have several different production z/VM systems, each with a different hardware or software configuration. In this case, you would execute one or more installation tasks to define a target production system, generate that system (or a portion of it) then repeat this sequence for another target system.

In this case, you should be sure to test the new software with all required configurations before copying to the Production minidisk.

It is possible that your production environment is used, off-hours, for testing new levels of the Test System software. After testing, these generated systems might be moved directly to production use. This is permissible provided that you maintain sufficient controls and testing procedures.

Performance Considerations

After completing Production Task KVC0P001 or after system reconfiguration, the following tasks should be considered in the performance of the remaining product installation:

Specify Operating System Parameters

You may need to update this task before proceeding with additional tasks, if, for example, your target Production operating system is configured differently from your Test System (although good testing practice suggests that the same software configuration be used even if the Test System does not require all of the available features). Similarly, you may need to generate multiple target Production Systems.

Each time the Production Generation minidisk address specification is changed in this task for an enhanced service system release, you must re-execute panel KVC0-I075. The CAKVBLD command contains imbedded minidisk information required for proper system generation.

Shared Database Selection

Your responses in this task influence the defaults for building and checking the CA Top Secret PARMS file in Task KVC0I070. If you need to execute that task, you should update the information here first.

Selection of Optional Features

See the previous two procedures.

Generate Utility Module

See the first procedure in this list.

Define CA Top Secret server

Because of the structure of the z/VM Access Control Interface, it is impossible to AUTOLOG more than one CA Top Secret server at the same time. However, you may wish to maintain a Test server and Production server for ease of testing, or to facilitate second-level testing. Remember that you may deactivate one server and activate another having a different z/VM user ID (that is, TSSVM and TSSVMB).

Note: Be careful when activating servers with different software maintenance levels. Upgrades in server software, especially new product genlevels, may require corresponding service in CP. You should not mix genlevels between the server, CP and CMS.

If you need to define a new CA Top Secret server for the Production System, or to change the definition of the Production server due to software release level requirements, execute this task.

Format server SYSRES

This task must be executed if you have newly created the CA Top Secret server for Production System use.

Define Security Database Files

If you have a separate Test facility, it might have its own CA Top Secret security database or share the Production data base. If necessary, specify or create the Production data base files using this task.

Set Customer Encryption Key

Each time you execute Production Task KVC0P001, the customer encryption key specified for the Test System is carried over to the Production System. If your Test System Security File encryption key differs from that of the Production System, you will need to execute this task.

Select/Retrieve Installation Exit

The Installation Exit module, TSSINS, is copied from the Test System minidisk to the Production Generation minidisk when you copy component files to production. This is done if changes were required to the Installation Exit to support the current software, and to ensure the use of the tested version of your Installation Exit. If this is inappropriate, execute this task to retrieve the required Installation Exit module for production use.

Generate Server Nucleus

If you have separate Test and Production servers, you will need to execute this task to generate the Production server. If, on the other hand, you have only one server and you are testing new server software maintenance, you will have regenerated the server nucleus (using the appropriate Test System generation task). Should it become necessary to fall back to the previous version, regenerate the server using this Production task to reinstate the latest validated level of service.

Customize Startup Parameters

Use this task to create or modify the CA Top Secret PARMS file for your Production System if you have just created the Production server, have specified new options in previous tasks, or need to implement new control options for the Production z/VM facility.

Send CAKVBLD to System Maintenance Machine

Execute this task if you use a different maintenance virtual machine to generate your Production z/VM CP system, or if you have changed the Production Generation minidisk address in Task KVC0I000. The CAKVBLD command contains imbedded minidisk information and must be kept up-to-date on the 191 disk to ensure that CP and CMS are built with Production object code and tools.

Generate CP Nucleus

Execute this task to build a new CP nucleus for Production using the newly validated level of CP modules.

IPL CP System

This task is included to remind you that the Production System is not complete until you have IPLed CP with current software. It should be noted that, unlike generating the Test System, it is not necessary to execute this task To confirm product installation. The Production System is considered to be in place and all Test System APARs are updated to reflect this as soon as you execute Production Task KVC0P001.

Generate CMS Nucleus

Information given above for Task KVC0I079, applies to this task as well.

Install CA-Register Interface

Execute this task if you are enabling the CA-Register interface for the first time or if maintenance has been applied to the CA Top Secret exit program for CA-Register.

TASK HL11P001—Copy CA-HELP Files to Production

Use this task to copy your Test System generated version of the CA-HELP component to your Production System minidisk.

From the Task Selection Menu, select panel HL11P001. The task executes and is marked as complete.

TASK P112P001—Copy Panel Manager Files to Production

Use this task to copy the Test System generated version of the CA-PANEL MANAGER component to your Production System minidisk.

From the Task Selection Menu, select panel P112P001. The task executes and is marked as complete.

Chapter 6: Populating the Security File

This section contains the following topics:

Security Concepts

During the installation a security file is created in which only the Master Security Control Administrator (MSCA) ACID is defined.

The MSCA is the ACID that allows you to begin to define your security environment. Your organization is provided the flexibility to incorporate into your security environment any controls provided by CA Top Secret. Initially, the MSCA ACID is used to accomplish this. For information on establishing a security environment, see the *Planning Guide*.

Each user requiring access to the z/VM system must be assigned an ACID. Users requiring CA Top Secret administrative authorities must be defined as control ACIDs (SCA, DCA, VCA, or ZCA). All other users must be defined as user ACIDs (USER). This process is performed manually, or with the z/VM Directory Conversion Program (CAKVDIR EXEC), which is used to read the CP Source Directory and to generate from input a CA Top Secret command file which may in turn be used to populate the Security File.

The z/VM Directory Conversion Program (CAKVDIR EXEC) creates ACIDs of types DEPARTMENT and USER and resources of type VMMDISK. All other ACID types and all other resource types are defined manually.

If an existing Security File, shared with other systems, is to be used, the output of the z/VM Directory Conversion Program must be carefully edited to remove any commands which would create definitions inconsistent with existing definitions. Duplicate resource definitions must be reviewed. Where necessary, existing permissions may need to be revoked and re-permitted using the SYSID restriction. New permissions may require the addition of a SYSID restriction.

About the Security File

CA Top Secret security information is stored in a single file called the security file. Within the Security File, each user is associated with a unique Security Record that enables CA Top Secret to associate access authorizations with users.

Within a z/VM environment, when a user logs onto a virtual machine, the CA Top Secret server retrieves the Security Record for that user from the Security File. The user's Security Record remains in the server's storage for the life of the session.

The Security File data set name is specified during installation. The default name is CAI.TOP.SECRET.SECURITY.FILE.

The security file, audit/tracking file(s) and recovery file can be shared with other systems.

User ACIDS

A User ACID has a specific meaning in CA Top Secret. To CA Top Secret, a User ACID is an ACID type, like Division ACIDs or Department ACIDs. Users are associated with User ACIDs or Control ACIDs.

Department, Division, and Zone ACIDs are used to define levels in the CA Top Secret organizational hierarchy. User ACIDs are at the lowest level in the hierarchy. They generally designate a specific employee in a department.

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

Department ACIDs

At many sites, users typically work within a particular department. CA Top Secret recognizes this logical separation, and provides for the establishment of department ACIDs. Each user ACID must be associated with one department ACID only. Resources may be owned by a department ACID in the same fashion as resources owned by a user ACID.

Define an Acids

Use the TSS CREATE command with the appropriate keywords to define ACIDs to CA Top Secret,. For example, to create a Department ACID called PAYDEPT, enter:

```
TSS CREATE(PAYDEPT) Name('PAYROLL DEPARTMENT') TYPE(Dept)
```

Use the CAKVDIR command to associate the users in the CP source directory with User and Department ACIDs.

Populate the Security File

To populate the Security File from the CP source directory

1. (Optional) Determine which z/VM minidisks are to be available to all users.
2. Create a file named CAKVDIR ALL that lists each minidisk and its access level (if applicable). For instructions, see the section Specify Common Resources in this chapter.

   CA supplies a user exit named CAKVDIRE used to determine department and name assignments. You can use it as supplied or you can modify it to make assignments based on requirements at your site. For information, see the section CAKVDIRE Command in this chapter.
3. Obtain the CP source directory file, ensuring that it is located on any accessed minidisk or SFS directory.
4. Execute the CAKVDIR command. Inputs to the command are the CP source directory file and the CAKVDIR ALL file (if used); the output is a TSS command file. This file is named direct_fn TSS A.

   For information, see the section CAKVDIR Command in this chapter.
5. Examine the TSS command file, and if necessary, edit it to meet your installation requirements.
6. Activate CA Top Secret, and log on using the MCSA ACID.
7. (Optional) If the TSS command file is in TSSCRIPT format:
   a. Edit the TSS command file to add to the top of the file:

      ```
      //TSSJOB ACID=msca_acid,PASSWORD=msca_pswd
      //EXEC PGM=TSSCRIPT
      ```

   b. Save the file as direct_fn SCRIPT fm.
   c. Use the SUBTSS command to submit the SCRIPT file to the TSSVM service machine or punch it directly:

      ```
      CP SPOOL PUNCH tssvm_service_machine_id CLASS B
      PUNCH direct_fn SCRIPT fm (NOHEADER
      ```

8. (Optional) If the TSS command file is in REXX EXEC format:

   a. Rename or copy the TSS command field to have a file name of EXEC.

   b. Run the command file by entering the following:

      ```
      EXEC direct_fn
      ```

   The Security File is populated with security records based on the information in the CP source directory.

CAKVDIR Command

Use this command to create a TSS command file, which is then used as input to populate the Security File.

The CAKVDIR command reads a CP source directory and builds a file of TSS commands that CA Top Secret uses to create departments, profiles and users, and to assign minidisk ownership and permissions. By default, the TSS command file is built in TSSCRIPT format, but can instead be built in REXX format.

The name of the TSS command file built by this command is direct_fn TSS A.

As part of its processing, the CAKVDIR command calls the CAKVDIRE user exit to determine how to assign users to departments.

This command has the format:

```
CAKVDIR direct_fn ( REPlace DEPtspec(dept)  MDiskown(owmer) DEFTept(def_name)
Exec ALL MSCA(msca_acid)  FACility(fac_names)
```

direct_fn

Required. Specifies the filename of the CP source directory (the filetype must be DIRECT).

Note: The default name for the IBM source direct file is USER DIRECT.

REPlace

Replaces a currently existing TSS command file (direct_fn TSS A).

DEPtspec(dept ACIGROUP EXIT)

Required. Specifies how User ACIDs are assigned to department ACIDs:

dept

An 8-character Department name to which all User ACIDs is associated.

ACIGROUP

Specifies that the Department ACID is the same as the security group name specified on the ACIGROUP statement in each user's CP directory entry.

If there is no ACIGROUP statement in the directory entry, that user is assigned to the default Department as specified on the DEFDEPT option.

EXIT

Specifies that the CAKVDIRE user exit be used to determine how to associate User ACIDs to Department ACIDs. For information on this user exit, see the section CAKVDIRE User Exit in this appendix.

If a department cannot be determined for a User's CP directory entry, that user is assigned to the default Department as specified on the DEFDEPT option.

MDiskown (DEPT USER)

Specifies which ACID to own a user's minidisks:

DEPT

(Default) Specifies that the Department ACID is to own user minidisks.

USER

Specifies that the users own their own minidisks.

DEFDept(dept_name)

Specifies the default Department ACID to create for user ACIDs not given a department by ACIGROUP or CAKVDIRE user exit. The default value is $direct_fn.

Exec

Specifies that the TSS command file is built in REXX EXEC format (V 255). By default the TSS command file is built in TSSCRIPT format (F 80).

ALL

Specifies that the TSS PERMIT (ALL) commands is included in the TSS command file based on minidisks. And access levels specified in the CAKVDIR ALL file. For information about how to create this file, see the section Specifying Common Resources later in this appendix.

By default, no TSS PERMIT (ALL) commands are included in the TSS command file

MSCA(msca_acid)

If specified, it suppresses the TSS CREATE(msca_acid) command for a TSSVM defined ACID that is also in the CP source directory (direct_fn).

By default, suppression doe not occur, and there is duplicate entries in the TSS command file. This may cause a non-fatal error TSS0315E ACID ALREADY EXISTS.

FACillity(fac_names)

If specified, overrides the default facility that is added to User and Control ACIDs. The default is FAC(VM).

To specify multiple facility names, separate them with a comma. For example:

```
FAC(VMSYS1,VMSYS2,BATCH)
```

CAKVDIR Return Codes

Return Code	Meaning
0	Successful completion
12	Invalid option on command
16	No department specification given
20	MSCA ACID does not exist in USER DIRECT*
28	File does not exist
32	Duplicate / invalid definition for CA Top Secret for VM
36	EXECIO error
40	No ACID given to user exit
44	Invalid user exit function

Specify Common Resources

With CA Top Secret, you can protect logons, as well as ownable CA Top Secret resources such as the CP DIAL command, minidisks, z/VM readers, DCSSs, RSCS nodes, CP commands, diagnose codes, IUCV, VMCF, OS/DOS data sets, DASD volumes, and CPUs.To allow access to specific ownable minidisks (VMMDISK) that are common to all users, create a file name CAKVDIR ALL. The file contains the permission information for each minidisk (VMMDISK).

Entries in the CAKVDIR ALL File

When the ALL option is specified on the CAKVDIR command, the CAKVDIR command checks the statements in the CP source directory against the ALL records in the CAKVDIR ALL file to determine whether a PERMIT command is required. A PERMIT is required only if the access mode is not allowed by the ALL record, or if the ALL record denies access.

Based on the results of the CAKVDIR check, the resulting TSS command file will contain a TSS PERMIT (ALL) command for each minidisk in the CAKVDIR ALL file.

The format of entries in the CAKVDIR ALL file is:

```
VMMDISK(perfix) ACCESS(access_level)
```

(prefix)

The prefix or the mdisk name (owner.vaddr).

ACCESS(access_level)

A specific level of access to the resource, if applicable. If no entry is made, CA Top Secret usually assigns a default access level baed on the resource type. For example, the default for mdisk (VMMDISK) is READ.

The access_level is the manner in which a resource can be used one accessed. For example: NONE, READ, WRITE.

For example, to specify a minidisk resource, the format is:

```
VMMDISK(owner.vaddr) ACCESS(access_level)
```

Example: CAKVDIR ALL File

This example allows all users access to MAINT 190, 19D, and 19E:

```
VMMDISK(MAINT.0190)  ACCESS(READ)
VMMDISK(MAINT.019D)  ACCESS(READ)
VMMDISK(MAINT.019E)  ACCESS(READ)
```

When the ALL option is specified on the CAKVDIR command, the following commands are included in the TSS command file:

```
TSS PERMIT (ALL)  VMMDISK(MAINT.0190)  ACCESS(READ)
TSS PERMIT (ALL)  VMMDISK(MAINT.019D)  ACCESS(READ)
TSS PERMIT (ALL)  VMMDISK(MAINT.019E)  ACCESS(READ)
```

CAKVDIRE

The CAKVDIRE user exit is called as part of CAKVDIR command processing. It enables your organization to:

- Determine the name to define for a Department, Profile, or User ACID
- Optionally define a method for determining the Department ACID to assign to a User or profile ACID

The CAKVDIRE user exit is always called to first determine the NAME value for a Department, Profile, or User ACID. It is called a second time to determine the Department ACID only if the DEPTSPEC(EXIT) option is specified on the CAKVDIR command.

There are three tokens:

- *function* which can be either NAME or DEPT
- The ACID name being created
- The default department ACID specified on the DEFDEPT option (where *function* is DEPT)

When function is NAME, the value returned from the CAKVDIRE user exit is the human name to assign to the Department, Profile, or User ACID.

You must modify the CAKVDIRE user exit to get the Human name.

If the option is specified on the CAKVDIR command, the CAKVDIRE user exit is called again. In this case, function is DEPARTMENT, and the value returned from CAKVDIRE is the Department ACID to associate with the Profile or User ACID. If the CAKVDIRE user exit does not return a Department ACID, the department specified on the option of the CAKVDIR command is used as the Department ACID.

Sample TSS Command File Creation Scenario

The following scenario illustrates the process of populating the Security File.

Determine Common Resources

For all users to have access to some common minidisks, create a CAKVDIR ALL file like this:

```
VMMDISK(MAINT.0190) ACCESS(READ)
VMMDISK(MAINT.019D) ACCESS(READ)
VMMDISK(MAINT.019E) ACCESS(READ)
```

Obtain the CP Source Directory

The CP source directory (USER DIRECT) looks like this:

```
DIRECTORY 0123 3390 DIRECT
USER $ALLOC$ NOLOG 256K 1M * 64 ON ON ON ON
OPTION MAXCONN 64
MACHINE ESA
POSIXOPT QUERYDB SYSDEFAULT EXEC_SETIDS SYSDEFAULT
MDISK 0 3390 0 END SPACE R
MDISK 1 3390 0 END T-DISK R
MDISK 2 3390 0 END SPOOL R
MDISK 3 3390 0 END PAGING R
MDISK 4 3390 0 END DIRECT R
MDISK 5 3390 0 END PARM R
MDISK 6 3390 0 END SPOOL2 R
USER CAIMAINT CAIMAINT 8M 24M G 64
IPL CMS
CONSOLE 009 3215
SPOOL 00C 2540 READER D
SPOOL 00D 2540 PUNCH A
SPOOL 00E 1403 A
LINK MAINT 190 190 RR
LINK MAINT 19D 19D RR
LINK MAINT 19E 19E RR
MDISK 191 3390 12 8 SPACE MR
MDISK 291 3390 20 30 SPACE MR
MDISK 391 3390 50 10 SPACE MR
MDISK 322 3390 45 15 SPACE2 MR
USER MAINT MAINT 35M 64M ABCDEFG 64 ON ON ON ON
ACCOUNT 1 SYSPROG
OPTION MAXCONN 64 MAINTCCW LNKS LNKE LNKNOPAS
AUTOLOG AUTOLOG1 MAINT
NAMESAVE GCS VTAM HELP HELPINST CMSFILES CMSVMLIB
MACHINE XA
IPL CMS
POSIXOPT QUERYDB SYSDEFAULT EXEC_SETIDS SYSDEFAULT
CONSOLE 9 3215 T
SPOOL C READER *
SPOOL D PUNCH A
SPOOL E PRINTER A
LINK $PARM$ 5 CF1 MR
LINK $ALLOC$ 4 123 MR
MDISK 191 3390 1 1 SPACE MR READ
MDISK 190 3390 0 END MNT190 RR ALL
MDISK 193 3390 0 END MNT193 RR ALL
MDISK 19D 3390 0 END MNT19D RR ALL
MDISK 19E 3390 0 END IBMPRD RR ALL
USER OPERATOR OPERATOR 24M 32M ABCDEFG 64 ON ON ON ON
ACCOUNT 2
```

```
OPTION MAXCONN 64 MAINTCCW LNKNOPAS
AUTOLOG AUTOLOG1 MAINT
MACHINE XA
IPL CMS PARM AUTOCR
POSIXOPT QUERYDB SYSDEFAULT EXEC_SETIDS SYSDEFAULT
CONSOLE 9 3215 T
SPOOL C READER *
SPOOL D PUNCH A
SPOOL E PRINTER A
LINK MAINT 190 190 RR
LINK MAINT 19E 19E RR
LINK MAINT 19D 19D RR
MDISK 191 3390 2 1 SPACE RR
USER TSSVM TSSVM 16M 64M G 64
MACHINE ESA
IUCV *RPI PRIORITY MSGLIMIT 100
IPL 100 PARM 'SYSOUT SYSTEM'
CONSOLE 009 3215
SPOOL 00C 2540 READER *
SPOOL 00D 2540 PUNCH A
SPOOL 00E 1403 A
MDISK 100 3390 1 3 SPACE2 RR TSSVMR TSSVMW TSSVMM
MDISK 200 3390 4 15 SPACE2 MR TSSVMR TSSVMW TSSVMM
MDISK 300 3390 34 6 SPACE2 MR TSSVMR TSSVMW TSSVMM
MDISK 400 3390 40 5 SPACE2 MR TSSVMR TSSVMW TSSVMM
MDISK 500 3390 19 15 SPACE2 MR TSSVMR TSSVMW TSSVMM
USER CMSBATCH CMSBATCH 4M 4M G 64
MACHINE ESA
IPL CMS PARM AUTOCR
CONSOLE 009 3215
SPOOL 00C 2540 READER *
SPOOL 00D 2540 PUNCH A
SPOOL 00E 1403 A
MDISK 191 3390 35 3 SPACE2 RR
```

Create the TSS Command File

In the resulting CA Top Secret command file, to have the Command File following conditions apply:

- You want all User ACIDs to be assigned to the VMDEVO Department ACID.
- Users own their own minidisks.
- The TSS command file is to be built in REXX format.
- Common minidisks are included.

- The TSS create command is not generated for the MSCA.
- Use the default facility name FAC(VM).

Execute the CAKVDIR command with the following options:

```
CAKVDIR USER ( DEPTSPEC(VMDEVO) MDISKOWN(USER) EXEC ALL MCSA(msca_acid)
```

Check the Console

As the CAKVDIR command runs, it writes messages to the console. Check for successful completion (return code = 0):

```
cakvdir USER ( deptspec(vmdevo) mdiskown(user) exec all msca(msca_acid)
CAIKVD001I CA-TOP SECRET z/VM Directory Conversion Utility starting pass 1. CAIKVD001I
CA-TOP SECRET z/VM Directory Conversion Utility starting pass 2. CAIKVD001I CA-TOP
SECRET z/VM Directory Conversion Utility starting pass 3. CAIKVD002I CA-TOP SECRET
z/VM Directory Conversion Utility ended. RC= 0. Ready:
```

Examine the TSS Command File

The resulting TSS command file is shown below:

```
/* Build TopSecret Security File */
"TSS CREATE(VMDEV0) NAME('VMDEV0') TYPE(DEPARTMENT)"
"TSS CREATE($ALLOC$) NAME('$ALLOC$') DEPT(VMDEV0) PASS(NOLOG) TYPE(USER)"
"TSS ADDTO($ALLOC$) VMMDISK($ALLOC$.)"
"TSS ADDTO(msca_ACID) VMMDISK(msca_ACID.)"
"TSS CREATE (MAINT) NAME('MAINT') DEPT(VMDEVO) PASS(MAINT) TYPE(USER) FAC(VM)"
"TSS ADDTO(MAINT) VMMDISK(MAINT.)"
"TSS CREATE(OPERATOR) NAME('OPERATOR') DEPT(VMDEVO) PASS(OPERATOR)",
"TYPE(USER) FAC(VM)"
"TSS ADDTO(OPERATOR) VMMDISK(OPERATOR.)"
"TSS CREATE(TSSVM) NAME('TSSVM') DEPT(VMDEVO) PASS(TSSVM) TYPE(USER) FAC(VM)"
"TSS ADDTO(TSSVM)) VMMDISK(TSSVM.)"
"TSS CREATE(CMSBATCH) NAME('CMSBAYCH') DEPT(VMDEVO0 PASS(CMSBATCH)",
"TYPE(USER) FAC(VM)"
"TSS ADDTO(CMSBATCH)"
"TSS PERMIT(ALL) VMMDISK(MAINT.0190) ACCESS(READ)"
"TSS PERMIT(ALL) VMMDISK(MAINT.019D) ACCESS(READ)"
"TSS PERMIT(ALL) VMMDISK(MAINT.019E) ACCESS(READ)"
"TSS PERMIT(MAINT) VMMDISK($PARM$.0005) ACCESS(MREAD)"
"TSS PERMIT(MAINT) VMMDISK($ALLOC$.0004) ACCESS(MREAD)"
```

Appendix A: Creating, Converting or Extending The Security File

This section contains the following topics:

About TSSXTEND and TSSXTEND

Enlarging or reducing the size of the Security File is a three-step process performed by the MSCA:

- Create a new, larger or smaller Security File using the TSSMAINT utility
- Add the new Security File to the CA Top Secret service machine directory
- Copy the old Security File to the newly created one using the TSSXTEND utility

Special Considerations

There are some important considerations in making a smooth transition from the existing Security File to the new larger or smaller Security File.

- Creating a new backup Security File—When you have created a larger Security File, you must create a Backup File (with the same control cards used for the new Security File) using TSSMAINT.
- Changing the encryption key—TSSXTEND has the capability of changing your company's Security File encryption key. Ordinarily, your company's encryption key should **never** be changed. However, if it is suspected that the integrity of your key has been violated, a new key can be supplied using TSSXTEND. If you change your encryption key, you must rerun the ACTIVATOR steps for applying the encryption key, prior to bringing up the server on the new security file.
- Deletion of old files—You should **not** delete the old Security File and Backup files until your installation is sure that the file enlargement or replacement was successful.

Create the New Security File

If the Security File is to be shared with CA Top Secret for z/OS then the file must be created and extended using the z/OS product and not CA Top Secret for z/VM. If sharing with VSE, then extend on the VSE system.

Note: If you are sharing the security file between MVS and VM and the security file under MVS has been created with the AESENCRYPT option, the security file can no longer be shared between MVS and VM.

To create a new Security File

1. Define the minidisk that will contain the new Security File to the CA Top Secret server directory as the 201 disk.
2. Define new backup security file to the CA Top Secret server as 501 disk.

   Note: Make this the same size as the new 201 disk.
3. Place the directory online.
4. Enter the command:

   ```
   TSS MODIFY(SHUTDOWN)
   ```
5. (X)AUTOLOG the server.

   The server is refreshed with new 201 and 501 mini disks.

6. From the CA-Activator machine:
   a. Issue CP DETACH 200.

      You will normally receive a message that it does not exist.

   b. Issue CP LINK *serverid* 201 200 MW

      serverid

      The name of your CA Top Secret server.

   a. Issue TSSCATDK 200 SECFIL.
   b. Create file SECURITY MAIDATA A as needed for your new Security File. For information on the control statements, see the chapter “Generating the Test System” .

      The is a sample of SECURITY MAIDATA:

      ```
      CREATE SECURITY
      DSN=CAI.TOP.SECRET.SECURITY.FILE
      VOLUMES=1000
      BLOCKSIZE=8192
      SDTBLOCKS=2
      ACCESSORS=5000
      SCA=mscaacid/mscapass
      id=PRIMARY
      ```

   c. Issue TSSMAINT SECURITY
   d. Issue CP DETACH 200
7. Have the MSCA submit the TSSXTEND batch job using the JCL described in TSSXTEND JCL.
8. (Optional) If the Security File encryption key has been changed, rerun the KVC0I050 and KVC0I061 installation tasks.

9. Create a new Backup File on the CA-Activator machine:
   a. Issue CP DETACH 500.

      You will most likely get a message that it does not exist.

   b. Issue CP LINK *serverid* 501 500 MW

      serverid

      The name of your CA Top Secret server.

   a. Issue TSSCATDK 500 BCKFIL.
   b. Create file BACKUP MAIDATA A as needed for your Backup File. Use the same parameters used to create the current Security File, with the exception of CREATE (CREATE BACKUP), DSN= (select a new data set name) and (ID=BACKUP).
   c. Issue TSSMAINT BACKUP.
   d. Issue CP DETACH 500.
10. (Optional) If the new Security File has a different data set name update the data set name in the Parameter File on the CA Top Secret server's 100 disk.

    If the new backup file has a different data set name update the data set name in the Parameter File on the CA Top Secret server's 100 disk.
11. Change the CA Top Secret service machine directory
    a. Change the 200 disk to another value (old security file).
    b. Change the 500 disk to another value (old backup security file).
    c. Change 201 disk to the 200 disk.
    d. Change 501 disk to the 500 disk.
    e. Place the directory online.

    Note: Do not delete your old Security and backup files until you have verified that the extend function has successfully completed.
12. Issue a TSS MODIFY(SHUTDOWN)
13. Re-(X)AUTOLOG the server

    The directory is refreshed and comes up on the new Security File.
14. Issue a TSS MODIFY(BACKUP).

    A current copy of the Security File is created on the new backup file.

TSSXTEND JCL

Use the following JCL to copy the contents of the old Backup File into the new Security File. Use the Backup File, and not the current Security File, as input to TSSXTEND. Otherwise, changes made to the current Security File during the execution of TSSXTEND could corrupt the new Security File. If you do need to copy the current Security File, replace COPY BACKUP in the sample below, with COPY SECURITY.

```
//TSSJOB ACID=mscaacid,PASSWORD=mscapass
//EXEC  PGM=TSSXTEND
COPY BACKUP
OLDKEY=xxxxxxxxxxxxxxx
NEWKEY=xxxxxxxxxxxxxxx
NEWDSN=new.file.data set.name
NEWPWBLOCK**OPTIONAL**
```

Notes:

- If you are sharing the security file between MVS and VM and the security file under MVS has been created with the AESENCRYPT option, the security file can no longer be shared between MVS and VM.
- This job can only be submitted using the MSCA's ACID.
- NEWKEY card is always required. If you are not changing the Security File encryption key, then the NEWKEY and OLDKEY fields must be identical.
- The OLDKEY and NEWKEY fields must be 16-character hexadecimal values. The first 8 characters of an encryption key cannot be identical to the last 8 characters. There can be no embedded commas or spaces, and comments cannot be placed on these fields.
- Use the optional NEWPWBLOCK keyword to add mixed case password support to the security file. If the security file will be shared with a previous release of CA Top Secret, do not use the NEWPWBLOCK keyword until you verify that the previous release supports NEWPWBLOCK. For information, contact CA Support.

Important! Safeguard your key.

Move the Security File

Note: If you are sharing the security file between MVS and VM and the security file under MVS has been created with the AESENCRYPT option, the security file can no longer be shared between MVS and VM.

To move the Security File from one system or device to another

1. If the Security File is already accessible on z/VM (for example, it is shared with a z/OS system and you want to create a separate Security File on z/VM, or it is a 3380 DASD device and you want to move it to a 3390), skip to Step 3.
2. If the Security File exists on a z/OS system, and you want to create a separate Security File on z/VM, with no shared DASD between the systems, use DFDSS or DDR to backup to tape the entire pack containing the Security File. Then, use the same utility to restore the pack on z/VM. Define this pack (a full-pack minidisk) as 200 in the CA Top Secret server's directory entry.
3. If you have a Backup File on z/VM, skip to Step 4. If you do not have a Backup File:
   a. Create a new Backup File. (Follow the instructions in Creating the New Security File.)
   b. Enter:

      ```
      TSS MODIFY(SHUTDOWN)
      ```

   c. Enter the data set name of the new Backup File in the Parameter File on the CA Top Secret server's 100 disk. Re-(X)AUTOLOG the server to refresh the directory.
4. Enter:

   ```
   TSS MODIFY(BACKUP).
   ```

   A copy of the Security File is created.
5. Enter:

   ```
   TSS MODIFY(BACKUP(OFF))
   ```

   The BACKUP function does not interfere with TSSXTEND.
6. Follow the instructions in Creating the New Security File, to create a new Security File and copy the contents of the Backup File.

Messages and Codes

The User Abend codes generated by an unsuccessful execution of TSSXTEND are listed in the *Messages Guide*.

Appendix B: SFS Grant Authority Conversion Utility

Prior to turning SFS ESM protection on the rules in place, using GRANT AUTHORITY, existing SFS commands should be transformed into CA Top Secret commands. Do this by executing the CAKVSFS EXEC. The CAKVSFS EXEC is installed on the CA-Activator disk that was specified as the disk that will contain CA Top Secret.

This exec must be invoked by an SFS administrator for each filepool to be ESM protected. It will generate one file for each filepool owner and that file will contain commands to be given to CA Top Secret to add external security protection to the directories and files in the filepools. The file name of each file is equal to the user ID of the directory owner; the file type is TSSCMDS. These command files should be reviewed for accuracy prior to being given to CA Top Secret. The value used for the ACID in each TSS ADD command defaults to SFSOWN. This can be changed if necessary.

This EXEC has the following format:

```
CAKVSFS AP outmode SFSOWN
```

AP

Indicates the name of the SFS filepool to be examined.

outmode

Specifies the accessed disk to which the TSS commands is written.

SFSOWN

Specifies the ACID to be used for TSS ADD commands.

Appendix C: Signon Messages

This section contains the following topics:

Default Messages

You can change certain signon-related messages to whatever text or language you want. In TSSVM MACLIB, there are members that let you modify the following default messages texts:

TSS0100A

Enter password, LOGOFF, or HELP (it will not appear when typed).

TSS0101A

Please enter your current password. You may optionally change it. Format is password/new_password or password/new_password/verify. To request a random password, enter password/RANDOM.

TSS0102A

Enter new_password/verify or RANDOM.

TSS0115E

New password verification failed.

TSS0120A

Reenter new password for verification.

Change Messages for z/VM 6.2.0 and Below

You can change messages.

Follow these steps:

1. Enter the following command:

   `XEDIT TSSVM MACLIB (MEMBER <member>`

   member

   The name of the desired member.
2. Make your changes to the member.
3. Enter the following command:

   `FILE [set the File Name variable] ZAP A`

   filename

   A name of your choosing, such as T0100A.

   Note: The first character of the filename must be T.
4. At the ready prompt, enter the following command:

   `CACT 2.2.5.`

   The APAR Administration panel is displayed.
5. Select 3 APAR Create/Modify.
6. Set the following:
   - APAR NUMBER to the filename you used above.
   - Format to 3.
   - Component code to AKVC0.
   - Member to TSSKMTH.
   - CSECT to HCPKV9.
   - Object type to TEXT.
   - File type to Text.
   - Description to anything you want.

   Press Enter to see the modified zap.
7. Press F2
8. Press F3.

   Panel CACT-A000 is displayed.
9. Select **5** APAR APPPLY to see your zap in the list.

10. Enter **1** next to your fix and apply the zap.
11. Press F3.
12. Generate a new CP nucleus with the modified TSSKMTH text deck.
13. Set OPTION(7) in the CA Top Secret PARMS file on the server 100 disk.
14. IPL the new CP nucleus.

    You should now see the modified messages.

To go back to the default text, turn the option off. You do not need to remove the zap to go back to the default text.

Change Messages for z/VM 6.3.0

A separate module (TSSUMT) exists where you can modify the signon messages. Having all the messages in this one module allows a greater degree of message modification.

Important! If you perform this procedure and then perform a reinstall or service level update, the shipped TSSUMT text deck replaces your modified deck on CAIMAINT 291. If the CA-supplied source has changed since the last time you made your modifications or changed from the source level on which your modifications are based, perform this entire procedure again. If CA-supplied source has *not* changed, simply copy your text deck again.

Follow these steps:

1. Enter the following command from any ID that has access to the CAIMAINT 291 disk:

   ```
   XEDIT TSSUMT ASSEMBLE
   ```

   The TSSUMT ASSEMBLE file should be found on the CAIMAINT 291 disk.

2. Make message changes as necessary.

   Important! The module includes instructions about which information is modifiable. You must follow these instructions (to avoid invalidating the message table and causing a CP ABEND at execution time).

3. Enter the following command to save your change:

   ```
   FILE TSSUMT ASSEMBLE fm
   ```

   fm

   Specifies a secure user disk where this file can be maintained (should not be the CAIMAINT 291 disk).

4. Assemble your message changes:

   ```
   ASSEMBLE TSSUMT
   ```

   Ensure that you are picking up the modified version of the module. If the assembly produces a return code of zero, you should find the LISTING and TEXT deck on your "A" disk. We recommend placing these output files on the same disk as the source.

5. Copy your text deck:

   ```
   COPYFILE  TSSUMT TEXT fm = = fm291 (OLDD REPL
   ```

   fm

   Specifies the user's secured disk.

   fm291

   Specifies the filemode for the CAIMAINT virtual machine's test disk (291), which holds all files loaded for the test system.

   Issuing this command copies the updated module from your disk to disk 291.

6. Return to task KVC0I079 (see page 42) to perform the task of generating a new CP module with your message changes.
7. Set OPTIONS(7) in the CA Top Secret PARMS file on the server 100 disk.

   This PARMS file setting specifies to use TSSMUT user-supplied messages for SIGNON processing.
8. IPL the new CP nucleus.

   You should now see the modified messages.

To go back to the default messages, remove OPTION(7) from the PARMS file. You do not need to remove the text deck.

Appendix D: CA LMP

This section contains the following topics:

About CA LMP

CA LMP (CA License Management Program) provides a standardized and automated approach to the tracking of licensed software. CA LMP uses common real-time enforcement software to validate the user's configuration and to report on activities regarding the licensing and usage of CA software.

CA LMP enforcement software is designed to operate smoothly and efficiently, whether you are using one CA solution on one physical processor or multiple CA solutions on several processors.

Operation

Periodically during the operation of each CA solution, the CA LMP common enforcement software is automatically invoked. This software compares the Execution Key with the actual, real-time execution environment. If there is a discrepancy between the Execution Keys and the environment, the enforcement software generates messages that are designed to help you resolve the situation and avoid any interruption in solution execution.

Enforcement software messages are written to the system console and the service machine console. When the appropriate messages have been issued, the CA solution continues normal operation.

The enforcement software ensures that solution software under the control of CA LMP is not interrupted because of expiration dates, improper execution keys, or changes in the CPU on which it is running.

Using CA LMP

CA LMP provides a standardized and automated approach to the tracking of licensed software. CA LMP support is available for all CA LMP-supported CA solutions. When a CA software solution has been enabled to take advantage of CA LMP, you receive a Key Certificate with your CA solution installation or maintenance tape.

Defining Product LMP Keys

The CA LMP execution key, provided on the Key Certificate, must be added to the CALMP KEYS member on the service machine's 100 disk.

The LMP product key is in the following format:

PROD(*pp*) DATE(*ddmmmyy*) CPU(*tttt-mmmm/ssssss*) LMPCODE(*kkkkkkkkkkkkkkkkkkkkkkkkkkkk*)

pp

(Required) The two-character product code. For CA Top Secret VM, it is K4.

ddmmmyy

The CA LMP licensing agreement expiration date. For example, 14JUL08.

tttt-mmmm

The CPU type and model (for example, 9672-R83) on which the CA LMP software solution is to run.

ssssss

The serial number of the CPU on which the CA LMP software solution is to run.

kkkkkkkkkkkkkkkkkkkkkkkkkkkk

The execution key needed to run the CA LMP software solution. This is provided on the Key Certificate shipped with each CA LMP software solution.

Execution

When the service machine is started, the software solution will periodically "wake up" to verify the continued validity of the current LMP key. If the key is not valid (for example, if it has just expired), a message is written to the system's operator console and the software solution rereads the key after a short time interval to see if it has been updated to a valid key. If not, the cycle continues.

Loading New LMP Key

It may be necessary to load a new LMP key after the service machine has been started. Replacing the LMP key does not require a CA Top Secret service machine restart.

To replace the LMP key

1. Update the CALMP KEYS member on the service machine's 100 disk to insert the new key.

   This member should contain all the valid keys for all CPU's sharing the service machine's 100 disk. LMP key checking stops on the first key found in the file. If your old key gives you a "key will expire in *xx* days" message and you add the new key after the old one, you will see the countdown on the old key until that key is no longer valid, at which time the new key would be used. To avoid this, insert the new key before the old key in the file.

2. Enter the command:

   ```
   TSS MODIFY(LMPCHECK)
   ```

   The service machine checks the new LMP key immediately.

EKG Keyword

In emergency situations, such as disaster recovery, the Emergency Key Generator (EKG) can be used to quickly and efficiently activate all software in the mainframe site. It is not necessary to implement EKG to activate software in a disaster recovery situation, since CA LMP lets your CA solutions to run uninterrupted regardless of the CPU on which they are running. You will, however, receive many console messages. To suppress these messages, contact CA LMP support and, in an emergency, request an EKG code.

When you have obtained an EKG code, it should be placed as the first record in the CALMP KEYS file.

In all cases, the EKG device code is only good for ten days, based on G.M.T.

Appendix E: CA Activator

This section contains the following topics:

Install Process (Initial)

You must install CA Activator to use it with CA Top Secret for z/VM.

Follow these steps:

1. Attach a tape drive to the CAIMAINT user ID as addr 18n where n is 1, 2, 3, or 4.
2. Mount the CA-CIS for z/VM (formerly known as CA90 Services for VM) GENLEVEL 0704 or higher tape on the drive attached in step 1.
3. Load CA-Activator for z/VM files from the CA-CIS for z/VM tape by doing the following:

   ```
   TAPE REW (TAPn)
   TAPE FSF 4 (TAPn)
   TAPE LOAD * * A (TAPn)
   ```

   Substitute for n the last digit of the tape addr attached in Step 1.
4. Type CACT to enter CA-Activator. You should see in the upper right corner of the panel:

   ```
   GENLEVEL: xxxxIHyy  where xxxx is the CA-Activator GENLEVEL
   and yy is the CA-Activator release
   ```
5. Mount the CA product tape on VDEV 18*n* where *n* is 1, 2, 3, or 4.
6. From the PRIMARY MENU select:
   - Product Administration
   - Product Install/Upgrade
   - Load from CA Product Install Tape
   - Enter vaddr in field and press enter key to execute
7. Press F2 to confirm and start load process. When process ends, press F3 until you reach the Product Install/Upgrade Panel. From here select Generate Test System From Loaded Tape Components.
8. Enter 1 in option field next to product Task Retrieval in Process

   Complete ***ONLY*** CA90S TASK:

9. Loading CA-CIS for VM
    a. Press F3 to Product Install/Upgrade Panel
    b. Mount CA-CIS for z/VM tape on same VDEV
    c. Load from CA Product Install tape.
    d. Enter vaddr in field and press the enter key.
    e. Press F2 to confirm load process
    f. CA-CIS will now be loaded. After process ends, press F3 until you are at Product Install/Upgrade Panel. From here select: Generate Test System from Loaded Tape Components
    g. Enter 1 in option field next to CA-CIS Services Task Retrieval in Progress
    h. Complete ALL CA-CIS tasks.

       CA-CIS Test System is generated.
10. Generating Test System for Products
    a. Press F3 for Product Install/Upgrade Panel
    b. Generate test system from loaded tape components
    c. Enter 1 in option field next to product Task Retrieval in Progress.
    d. Complete ALL non-optional tasks.

Refresh Process

Follow these steps during the refresh process:

1. Attach a tape drive to the CAIMAINT user ID as VDEV 18*n* where *n* is 1, 2, 3, or 4.
2. Mount the CA-CIS for z/VM GENLEVEL 0704 or higher tape on the drive attached in step 1.
3. Enter **CACT** to enter CA-Activator. From the Primary Menu select:
    - Product Administration
    - Product Maintenance
    - Load from CA Product Refresh Tape
    - Enter vaddr in field and press enter
4. Press F2 to confirm
5. Follow prompts to refresh CA-Activator

6. Enter **CACT** to enter CA-Activator. The following appears in the upper right corner of the panel:

   GENLVEL: *xxxx*IH*yy*

   xxxx is the CA-Activator GENLEVEL

   yy is the CA-Activator release

7. Mount product tape on VDEV 18n where n is 1, 2, 3, or 4.

8. From the Primary Menu select:

   - Product Administration
   - Product Maintenance
   - Load from CA Product Refresh Tape
   - Enter vaddr in field and press enter

9. Press F2 to confirm and start load process. When process ends, press F3 until you reach the Product Maintenance Panel. From here select Regenerate Test System from Refreshed Tape Components

10. Enter **1** in option field next to product Task Retrieval in Process

    COMPLETE ***ONLY*** CA90S TASK:

11. Refreshing CA-CIS for VM

    a. Press F3 to Product Maintenance Panel

    b. Mount CA-CIS for z/VM tape on same VDEV

    c. Load From CA Product Refresh Tape

    d. Enter vaddr in field and press enter

    e. Press F2 to confirm load process

    f. CA-CIS for z/VM will now be refreshed. After process ends, press F3 until you are at Product Maintenance Panel. From here select: Regenerate Test System from Refreshed Tape Components

    g. Enter 1 in the option field next to CA-CIS Services Task Retrieval in Progress…

    h. Complete ALL CA-CIS tasks

    CA-CIS test system is now regenerated.

12. Regenerating Test System for Products

    a. Press F3 to Product Maintenance Panel

    b. Regenerate Test System from Refreshed Tape Components

    c. Enter 1 in option field next to product TASK RETRIEVAL IN PROGRESS…

    d. Complete ALL non-optional tasks

    You now have regenerated your test system.

Match an Activator Account to the MSCA ACID

For product demonstration to run properly, the CA Activator account must match the CA Top Secret MSCA ACID. Perform this procedure if the CA Activator account does not match the MSCA ACID.

Follow these steps:

1. Access panel CACT2410.
2. Run the following batch job:

```
//TSSJOB ACID=MASTER,PASSWORD=your sites password
//EXEC PGM=TSSCRIPT
TSS CREATE(CAIMAINT) TYPE(SCA) NAME('CA PRODUCT MAINT ACCOUNT')
 PASS(CAIMAINT,,EXPIRE) FACILITY(ALL)
TSS ADMIN(CAIMAINT) RESOURCE(ALL) ACCE(ALL)
TSS ADMIN(CAIMAINT) ACID(ALL) ACCE(ALL)
TSS ADMIN(CAIMAINT) FAC(ALL) ACCE(ALL)
```

   The CAIMAINT ACID is defined to the TSSVM security data set.
3. Log out from CAIMAINT.
4. Log in to CAIMAINT and enter a new password.
5. Run the product demonstration.

More information:

CA Activator (see page 13)

Appendix F: Installation Questions

The following questions must be answered during the initial installation process of CA Top Secret. This list does not include the optional installation steps. These are provided to allow the decision process to take place prior to actually doing the installation to expedite the process.

KVC0I90S

Installing CAICCI? **Note:** CAICCI is required if you is using CPF.
Installing CA-ESM? **Note:** CAESM 1.1 is required for RACROUTE use including SFS external security.

KVC0I000

What release of the CP operating system are you installing?
What user ID is used for CP generation? (such as MAINT)
What is the name of the TSS virtual machine? Default is TSSVM.
What user ID should receive TSS SYSOUT/VMDUMPs?
What ACTIVATOR disk contains product system files? (Normally use the default of 391)
What ACTIVATOR disk contains generation files? (Normally use the default of 322)

KVC0I012

Will the security database files be shared with another system?
If above is yes, does this system do the automatic backup?

Will the security database files be shared with another system?
Will you be using alternate SYSRES for TSSVM machine? If yes, be prepared to identify if using 101/102/103 disks.
Will you be using the alternate Audit file (301)?

KVC0I020

Will you be using CP level OS/VSE Data set protection?

KVC0I030

Do you need to define the CA Top Secret Service Machine? If yes then have the minidisk information available for required files.

KVC0I042

Specify the OS/VSE style data set names for the security database.

If shared with an OS/VSE system, these files must be created on that system prior to starting CA Top Secret.

Security file:
Audit file:
Audit2 file:
Recovery file:
Backup file:
CPF Recovery:

KVC0I050

What will your 8-byte customer encryption key be? (Entered in character or hex).

KVC0I055

Will you be using an installation exit? If yes, give the user ID and the virtual disk where the exit exists.

KVC0I061

Which virtual machine SYSRES do you wish to create? (CUU)

KVC0I065

Which virtual machine SYSRES do you wish to add an LMP key to? (CUU) (Likely same as above)

KVC0I070

Which server nucleus disk do you wish to build the PARM file for? (CUU) (Likely the same as above)

Important! At the completion of the installation this form should be secured or destroyed. It will contain your unique customer encryption key that should be kept secure. You will need the key again in the future when enlarging the file or installing a new release.