

CA Top Secret® for z/OS

Installation Guide

r15



Sixth Edition

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the "Documentation"), is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This documentation set references the following CA products:

- CA Top Secret® for z/OS (CA Top Secret)
- CA Top Secret® Workstation Option (CA Top Secret Workstation Option)
- CA Chorus™ Software Manager (CA CSM)
- CA ACF2™ for z/OS (CA ACF2)
- CA Common Services for z/OS (CA Common Services)
- CA Earl™ (CA Earl)
- CA IDMS™ (CA IDMS)
- CA Roscoe® Interactive Environment (CA Roscoe)
- eTrust Audit
- CA ASM2® Backup and Restore (CA ASM2 Backup and Restore)

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

We have made the following documentation updates to the fourth edition of this documentation:

- [\(Optional\) Install ENF Data Control Modules](#) (see page 76)—Added instructions for installing ENF DCMs when working with CA Common Services 12 (and higher); added a cross-reference to CA Common Services documentation for more information about DCM configuration in the ENF parameter file.
- [Copy the BDAM and VSAM Files](#) (see page 117)—Updated instruction for how to change the SECOVSM DD when editing TSSXTEND.
- Run the TSSXTEND Utility—Updated the SECOVSM DD statement definition in the JCL; added information about how to address unsuccessful TSSXTEND executions.

We made the following documentation updates to the third edition of this documentation:

- [Create the Security File](#) (see page 87)—Added information about the new ORGACIDSIZE parameter, which lets you set size limits specifically for organizational ACIDs.
- [Increase ACID Size](#) (see page 91)—Added this procedure to describe how to increase the maximum size of organizational ACIDs or increase the maximum size of all ACIDs.

Contents

Chapter 1: Overview 11

Audience	11
How the Installation Process Works.....	11

Chapter 2: Preparing for Installation 13

Hardware Requirements	13
Disk Space Requirements for Data Sets	13
Disk Space Requirements for the Target Libraries	14
Disk Space Requirements for the Distribution Libraries	14
Software Requirements	15
Minimum Compatibility Levels.....	16
Software Prerequisites.....	16
CA Common Services Requirements	16
CA Common Services Considerations	17
MAXRU Size.....	17
Defining the CA LMP Execution Key	18
Security Requirements	19
Storage Requirements.....	20
Calculate Extended CSA Requirements (Optional).....	20
Configuration Requirements	21
VSAM File Considerations	21
Sharing a Security File	21
Coupling Facility	22
ACID Names.....	22
Multi-CPU Environments.....	23
SMF	23
JES2	24
Concurrent Releases	25
Concurrent Releases	25

Chapter 3: Installing Your Product Using CA CSM 27

How to Install Your Product Using CA CSM	27
Access CA CSM Using the Web-Based Interface	29
Acquire a New Product	29
Install a Product	30
Maintain the Installed Products.....	32

Deploy the Product to the Destination System.....	33
Configure the Deployed Product.....	34

Chapter 4: Installing Your Product from Pax-Enhanced ESD 37

How to Install a Product Using Pax-Enhanced ESD	37
How the Pax-Enhanced ESD Download Works	39
ESD Product Download Window	39
USS Environment Setup	42
Allocate and Mount a File System.....	43
Copy the Product Pax Files into Your USS Directory	46
Download Using Batch JCL	47
Download Files to Mainframe through a PC	50
Create a Product Directory from the Pax File	51
Sample Job to Execute the Pax Command (Unpackage.txt)	52
Copy Installation Files to z/OS Data Sets.....	52
Receiving the SMP/E Package	53
(Optional) Clean Target and Distribution Libraries	54
How to Install Products Using Native SMP/E JCL	54
Prepare the SMP/E Environment for Pax Installation	55
Component Installation	56
Run the Installation Jobs for a Pax Installation	56
Clean Up the USS Directory.....	57
Apply Maintenance	58
HOLDDATA	59
System HOLDDATA.....	59
External HOLDDATA	61

Chapter 5: Installing Your Product from Tape 63

Unload the Sample JCL from Tape	64
How to Install Products Using Native SMP/E JCL	65
Prepare the SMP/E Environment for Tape Installation.....	65
Component Installation	66
Run the Installation Jobs for a Tape Installation	67
Apply Maintenance	67
HOLDDATA	68
System HOLDDATA.....	68
External HOLDDATA	70

Chapter 6: Starting Your Product 73

How to Complete Configuration With CA CSM	73
---	----

Assign the Key	74
Authorize Product Libraries	75
Authorize TSS Commands	75
Set Up SAF SECTRACE (Optional).....	76
(Optional) Install ENF Data Control Modules	76
How to Edit the Started Task	78
How to Update the TSSB Backup Started Task Procedure	78
Edit Commands to Initiate and Follow CA Top Secret Initiation	79
Create the Parameter File	81
Upgrade the Existing Security File (Optional)	83
Creating the Security File	84
Create a Backup Security File on DASD (Optional)	92
(Optional) Define the Mirror Security File (BDAM and VSAM Components)	93
Create the Recovery File (Optional)	94
Create an Audit/Tracking File (Optional)	95
Create Alternate Audit/Tracking File (Optional)	97
Create a CPF Recovery File	97
Create the RCACHE VSAM Cluster (Optional)	98
CICS Installation Considerations.....	99
Define the Security Console (Optional).....	99
Set Up Backup, Restore, and Recovery Procedures	99
CA Top Secret ADMIN Menus	102
Set Up Installation Exits.....	103
Customize Facility Security.....	103
CA Top Secret as a Subsystem.....	103
How to Configure Without CA CSM	107
Startup and Shutdown Sequence	108
Start CA Top Secret	108
Activate CA Top Secret	109
Verifying Installation (Optional)	109
Restarting CA Top Secret.....	110
CA Top Secret Shutdown.....	111

Appendix A: TSSXTEND - Extend the Security File **113**

How to Change the Security File Size or Encryption Key	113
TSSXTEND Considerations	115
Convert SDT Records to VSAM	116
Convert Triple-DES Encryption to AES Encryption	117
Copy the BDAM and VSAM Files	117
Copy the VSAM File	118
Run the TSSXTEND Utility	118

Messages and Codes	119
--------------------------	-----

Appendix B: CA Top Secret Health Checks	121
--	------------

Appendix C: OPMAT Member Locations	123
---	------------

About OPMAT Member Locations	123
SOURCE Library	124
CLIST Library	125
MACRO Library	126
ISPF PROFILE Library	126

Appendix D: TSSXVSDT Digital Certificate Backout	127
---	------------

About TSSXVSDT	127
VSAM Digital Certificate Backout	127

Index	133
--------------	------------

Chapter 1: Overview

This guide describes how to acquire, install, and implement CA Top Secret for z/OS to make it available to the staff who customize and use the product.

This section contains the following topics:

[Audience](#) (see page 11)

[How the Installation Process Works](#) (see page 11)

Audience

This guide details CA Top Secret installation procedures for general mainframe users. We strongly recommend that you read this entire document before starting an installation.

How the Installation Process Works

CA Technologies has standardized product installations across all mainframe products. Installation uses the following process:

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Creates an SMP/E environment and runs the RECEIVE, APPLY, and ACCEPT steps. The software is untailored.
- Deployment—Copies the target libraries to another system or LPAR.
- Configuration—Creates customized load modules, bringing the software to an executable state.

[CA Chorus™ Software Manager \(CA CSM\)](#) - formerly known as CA Mainframe Software Manager™ (CA MSM) - is an intuitive web-based tool that can automate and simplify many CA Technologies product installation activities on z/OS systems. This application also makes obtaining and applying corrective and recommended maintenance easier. A web-based interface enables you to install and maintain your products faster and with less chance of error. As a best practice, we recommend that you install mainframe products and maintenance using CA CSM. Using CA CSM, someone with limited knowledge of JCL and SMP/E can install a product.

Note: If you do not have CA CSM, you can download it from the Download Center at <http://ca.com/support>. Follow the installation instructions in the CA Chorus Software Manager documentation bookshelf on the CA Chorus Software Manager product page.

You can also complete the standardized installation process manually using pax files that are downloaded from <http://ca.com/support> or a product DVD.

To install your product, do the following tasks:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Verify that you acquired the product using one of the following methods:
 - Download the software from <http://ca.com/support> using CA CSM.
 - Download the software from <http://ca.com/support> using Pax-Enhanced Electronic Software Delivery (Pax ESD).
 - Order a product DVD. To do so, contact your account manager or a CA Technologies Support representative.
3. Perform an SMP/E installation using one of the following methods:
 - If you used CA CSM to acquire the product, start the installation process from the SMP/E Environments tab in CA CSM.
 - If you used Pax ESD to acquire the product, you can install the product in the following ways:
 - Install the product manually.
 - Complete the SMP/E installation using the Add Product option in CA CSM.
 - If you used a DVD, install the product manually.

Note: If a CA Recommended Service (CA RS) package is published for your product, install it before continuing with deployment.
4. Deploy the target libraries using one of the following methods:
 - If you are using CA CSM to configure your products, a CA CSM deployment is required.
 - If you are using a manual configuration process, a manual deployment is an optional step.

Note: Deployment is considered part of starting your product.
5. Configure your product using CA CSM or manually.

Note: Configuration is considered part of starting your product.

Chapter 2: 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](#) (see page 13)

[Software Requirements](#) (see page 15)

[CA Common Services Requirements](#) (see page 16)

[Security Requirements](#) (see page 19)

[Storage Requirements](#) (see page 20)

[Configuration Requirements](#) (see page 21)

[Concurrent Releases](#) (see page 25)

[Concurrent Releases](#) (see page 25)

Hardware Requirements

This section details disk space requirements for DASD, target libraries, and distribution libraries.

Disk Space Requirements for Data Sets

Sufficient space on DASD must be available to install CA Top Secret and CA SAF. The following table provides estimated space requirements for the data sets. The actual block size that you allocate depends on your site requirements.

Data Set Name	Block Size	3390 Cylinders	Directory Blocks
CAKOLINK	6144	35	100
CAKOLPA	6144	1	10
Security File	8192	*	---
Backup Security File	8192	*	---
Recovery File	1280	*	---
Audit Tracking File	6144	*	---
CPF Recovery File	6000	*	---

An asterisk (*) indicates user-defined values.

Disk Space Requirements for the Target Libraries

The following table provides the estimated space requirements for the target libraries:

Data Set Name	Block Size	Blocks	Directory Blocks	Type
CAI.TSS150.CAKOCLS0	3120	840	25	Clist
CAI.TSS150.CAKOMSG0	6144	400	10	Messages
CAI.TSS150.CAKOPNL0	3120	3875	305	Panels
CAI.TSS150.CAKOTBL0	3120	100	20	ISPF tables
CAI.TSS150.CAKOLINK	6144	35 cylinders	100	Load
CAI.TSS150.CAKODATA	3120	100	20	ISPF profile
CAI.TSS150.CAKOLPA	6144	1 cylinder	10	LPA modules
CAI.TSS150.CAKOSRC0	3120	475	10	Source
CAI.TSS150.CAKODBRM	3120	100	20	SAF DBRM
CAI.TSS150.CAKOXML	32760	17 trks	16	XML data
CAI.TSS150.CAKOSIDE	3120	6 trks	16	
CAI.TSS150.CAKOSAMP	32720	17 trks	16	
CAI.TSS150.CAKOOOPTN	32720	5 trks	25	CIA Datacom
CAI.TSS150.CAKODDTR	32720	5 cyls	25	CIA Datacom
CAI.TSS150.CAKOJCL0	32720	87 trks	80	Sample JCL
CAI.TSS150.CAKOMAC0	3120	6300	305	Macros
CAI.TSS150.CAKOMENU	6144	400	100	Messages

Disk Space Requirements for the Distribution Libraries

The following table provides the estimated space requirements for the distribution libraries:

Data Set Name	Block size	Blocks	Directory Blocks	Type
CAI.TSS150.AAKOMOD0	6144	20	200	Load
CAI.TSS150.AAKOCLS0	3120	475	20	Clist

Data Set Name	Block size	Blocks	Directory Blocks	Type
CAI.TSS150.AAKOMAC0	3120	2100	75	Macros
CAI.TSS150.AAKOPNL0	3120	2000	75	Panels
CAI.TSS150.AAKOMSG0	3120	30	5	Messages
CAI.TSS150.AAKOSRC0	3120	250	5	Source
CAI.TSS150.AAKOTBL0	3120	20	5	ISPF tables
CAI.TSS150.AAKODATA	3120	20	5	ISPF Profile
CAI.TSS150.AAKOMOD1	6144	1000	100	SAF
CAI.TSS150.AAKOMENU	6144	600	100	SAF
CAI.TSS150.AAKOMOD2	6144	2000	30	SAF C
CAI.TSS150.AAKODBRM	3120	20	5	SAF DBRM
CAI.TSS150.AAKOSAMP	3120	20	5	
CAI.TSS150.AAKOOPTN	32720	5 trks	25	CIA Datacom

CAI.TSS150.AAKOMOD3	6144	19 trks	43	IMS
CAI.TSS150.AAKOMOD4	6144	3 trks	16	IDMS
CAI.TSS150.AAKOMOD5	6144	35 trks	35	ROSCOE
CAI.TSS150.AAKOJCL0	32720	87 trks	80	Sample JCL
CAI.TSS150.AAKODDTR	32720	5 cyls	25	CIA Datacom
CAI.TSS150.AAKOXML	32760	17 trks	16	XML Data
CAI.TSS150.AAKOSIDE	3120	6 trks	16	

Software Requirements

This section details compatibility requirements and where to locate software prerequisites.

Minimum Compatibility Levels

The following is a list of minimum required releases and gen levels:

Product	Release	Minimum Gen Level
CA Top Secret for z/OS	r15	SP00
CA Top Secret for z/VM	NA	NA
CA Top Secret for z/VSE	NA	NA

Software Prerequisites

For information on the software prerequisites for IBM and CA Technologies software, see the Product Information Bulletin (PIB).

CA Common Services Requirements

CA Top Secret uses the following CA Common Services components. For information on installing these components, see the CA Common Services documentation.

Component	FMID	Required for:
CAIENF	CW11000 CW11001	Protecting CICS and using CPF, CA Top Secret Workstation Option
CAIENF/CICS	CW31000 CW31001	Protecting CICS and using CPF, CA Top Secret Workstation Option
CAIENF/USS	CRR1000	CA Technologies HFS Security
CAIENF/DB2	CW51000	CA Technologies DB2 Security
CAICCI	CW41000	Using CPF
CAIRIM	CS91000	Protecting CICS, using CPF and CA LMP
CA Earl	CXE6000	Report writing
CA-C Runtime	CF33000	Using Administration panels

CA Common Services Considerations

To coordinate system security (particularly in the event of CICS, DB2, or the Command Propagation Facility (CPF) being used), CA Top Secret relies on the following CA Common Services:

CAIRIM

This component is an initialization program. CA Top Secret requires CAIRIM for CA LMP (used to track licensed software) and when securing CA IDMS r13 and above.

Note: CA Top Secret does not initialize properly without CA LMP.

CAIENF

This component provides a common operating system interface, which offers a simple and flexible approach for CA Technologies products to obtain data from z/OS. (CA Top Secret actually uses a subset of CAIENF components.) CAIENF works with CAIRIM.

Note: To remove CAIENF, you must IPL without CAIENF. Stopping CAIENF does not remove it from the system.

CAICCI

The Common Communication Interface component is required by the CPF.

CAISSF

The Standard Security Facility component is required if you are using another CA Technologies product that also makes security calls.

CA C Runtime

This component runs the administration panels.

CA Earl

(Optional) You can also load CA Earl which is used for report writing.

MAXRU Size

When identifying CAICCI nodes that will use CPF, specify a minimum MAXRU of 1024 KB or more. We recommend that you use 4096 KB or more if your network can support it. A MAXRU of 256 KB is supported, although this may impact command response time, particularly when synchronous commands with large amounts of output are propagated over non-channel attached connections.

The value specified must be consistent between all CAICCI nodes.

Note: For information about MAXRU, see the *CA Common Services Guide*.

Defining the CA LMP Execution Key

CA License Management Program (LMP) is license tracking software provided in CAIRIM.

For instructions on installing CAIRIM and defining the CA LMP execution key to the CAIRIM parameters, see the CA Common Services documentation.

Parameter Key Structure

The parameter structure for the KEYS member has the following format:

PROD(*pp*) DATE(*ddmmyy*) CPU(*tttt-mmmm/sssss*) LMPCODE(*kkkkkkkkkkkkkk*)

pp

Specifies the two-character product code for CA Top Secret. This code should be the same as the code being used by the CAIRIM initialization parameters for earlier genlevels of the product.

ddmmyy

Specifies the CA LMP licensing agreement expiration date (for example, 03JAN10).

tttt-mmmm

Specifies the CPU type and model (for example, 3090-0600) on which the product is to run. If the CPU type, model, or both are fewer than four characters, insert blank spaces for the unused characters.

sssss

Specifies the serial number of the CPU on which the product is to run.

kkkkkkkkkkkkkk

Specifies execution key needed to run the product.

Example: parameter key structure

This example shows a typical parameter key structure:

PROD(X1) DATE(03JAN09) CPU(3090-0600/370623) LMPCODE(5262K06130Z74ZD)

LMP Key Information

The CA LMP Key Certificate contains the following information:

Product Name

Indicates the trademarked or registered name of the designated site and the CPUs on which the product is to be installed.

Product Code

Indicates the two-character code for CA Top Secret.

Supplement

Indicates the reference number of your license for CA Top Secret that may be in the format *nnnnnn - nnn*.

CPU ID

Indicates the code identifying the specific CPU on which CA Top Secret is to be installed.

Execution Key

Indicates an encrypted code required by CA LMP for CA Top Secret initialization. During installation, it is referred to as the LMP code.

Expiration Date

Indicates the date your CA Top Secret license expires.

Technical Contact

Indicates the name of the technical contact at your site that is responsible for the installation and maintenance of this licensed copy of CA Top Secret. This is the person to whom CA Technologies addresses all CA LMP correspondence.

MIS Director

Indicates the name of the Director of MIS (or the person who performs this function at your site). If a person's name is omitted from the certificate, supply the actual certificate when correcting and verifying it.

CPU Location

Indicates the address of the building containing the CPU on which CA Top Secret is installed. Define a CA LMP execution key to the CAIRIM parameters by modifying the member KEYS in the OPTLIB data set.

Security Requirements

To complete the tasks in this guide, you need read, update, and allocate authority for the installation data sets and libraries.

More Information:

[Apply Maintenance](#) (see page 58)

Storage Requirements

CA Top Secret does not use fixed or real storage. The following list summarizes main storage utilization:

Non Extended CSA

175 KB + (security block size) + (audit file size)

Extended CSA

1224KB + (The ALL, SDT and STC Records) + (prefixed resource table)

The space these records use varies from site to site. See the section following to determine space requirements.

CA Top Secret Address Space

4 MB

User Address Space

Requirements vary depending on the size of a user's Security Records. For a single-user address space, typically 1 KB is required per user. The minimum is 464 bytes. In a z/OS environment, the key 3 storage is allocated in extended LSQA above the 16 MB line.

For multi-user address spaces (such as CICS), common profile security records are shared to minimize storage use. The average is 250 bytes per user. The largest portion of data uses key 3 storage, and the rest is in key 0 and the TCB key. User information is freed at sign-off. Profile information is freed when the last user of the profile signs off at address space termination.

Calculate Extended CSA Requirements (Optional)

If you have an existing version of CA Top Secret, you can run TSSFAR to calculate the amount of extended CSA required.

Follow these steps:

1. Run TSSFAR using the control statement of SFSTATS.

The PIE Blocks allocated are displayed.

2. Determine the prefixed resource table size:

$(\text{Pie Blocks} * \% \text{used}) * \text{BLKSIZE}$

Configuration Requirements

This section details configuration-specific requirements for elements of CA Top Secret.

VSAM File Considerations

A VSAM file is mandatory. If you do not implement this file, CA Top Secret will not initialize. The VSAM file stores digital certificates, keyrings, Kerberos records, SDT records, data classification records, SIGVER records, and IDMAP records.

The following VSAM file considerations apply:

- CA Top Secret is compatible with VSAM files that are created on r12 or later.
- The VSAM file may include an alternate index and path file for improved I/O performance in shared file environments.

You can create the VSAM file by using *one* of the following methods:

- Converting a non-VSAM security file
- Copying/extending an existing security file
- Formatting a new security file

More information:

[TSSXTEND - Extend the Security File](#) (see page 113)

[Create the VSAM File](#) (see page 86)

Sharing a Security File

You can share an r15 security file with r12 and r14 unless you have an r15 system with a certificate with a large SDN (subject's distinguished name) or SN.IDN (serial number and issuer's distinguished name). In this case, you cannot share the file with an r12 or r14 system. If you do so, the file will be created by the r15 system.

Important! If a VSAM file is *not* shared between multiple CA Top Secret systems, do *not* create VSAM alternate index and path files. Due to VSAM file requirements, CA Top Secret r15 for z/OS can no longer share secfiles with CA Top Secret for z/VM or CA Top Secret for VSE.

Coupling Facility

The CA Top Secret control option OPTIONS(65) controls the action taken when the structure name of the security file active in the coupling facility is different from the structure name of the local security file.

If this option is:

- On and the structure names are different during CA Top Secret startup—The local system disconnects from the coupling facility and aborts.
- On and CA Top Secret is up—The local system disconnects from the coupling facility and forces other systems to disconnect from the coupling facility.
- Off (default)—CA Top Secret connects to the active structure and overrides the local structure.

The CA Top Secret control option OPTIONS(61) uses the coupling facility to hold the file lock record reducing the number of I/Os to the security file. This behavior increases the amount of CPU used due to the IBM support required for the coupling facility.

The SYSID field contains \$CFLOCK\$, which shows that the system holding the lock is using the lock record in the coupling facility.

ACID Names

ACIDs must not have the same name as any CA Top Secret table (TYPE=GLOBAL acids). If migrating from a previous release, check for ACIDs with the same name as CA Top Secret tables TYPE=GLOBAL ACIDs. If the ACID appears in the following list and it shows a value other than TYPE=GLOBAL, rename the ACID before applying compatibility fixes or installing the new release.

The following list details existing tables for CA Top Secret:

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

Multi-CPU Environments

In a multiple-CPU environment, perform the following actions:

- Place the following CA Top Secret files on a shared DASD volume:
 - Security file
 - Audit/tracking file
 - Recovery file
- If sharing a security file between multiple CPUs, specify the control option SHRFILE(YES) on each CPU.
- Back up the security file from one CPU only. Omit the BACKUP DD statement or code the BACKUP(OFF) control option on all systems but one.
- If “secured” data sets reside on shared DASD volumes and CA Top Secret is being used through one CPU only (usually during transition), system 913 abends might occur. Use program TSSPROT to remove the protection bits from the affected data sets. Set TSS control option ADSP as ADSP(NO) to prevent future data sets from being marked as protected.

Important! Due to VSAM file requirements, CA Top Secret r15 for z/OS can no longer share secfiles with CA Top Secret for z/VM or CA Top Secret for VSE.

SMF

If requested in the LOG control option, CA Top Secret will log security-related activity and incidents to SMF using record type 80.

The normal logging of CA Top Secret to the SMF file does not significantly affect the size of the SMF file, the amount of traffic SMF receives, or the frequency of dump. There are two situations that may warrant changes to either the SMF data set size or procedures:

- When CA Top Secret is in WARN mode
- The Central Security Administrator requests logging of all activity

Generally, SMF logging is discouraged in favor of the CA Top Secret audit/tracking file.

The SMF record number 231 is used for the SAF Trace Report and OMVS logging. If the ACID is being audited, the type 80 records are used. For information, see the *Report and Tracking Guide*.

JES2

Because CA Top Secret does not make any modifications to JES2 (or its control blocks), it makes certain assumptions about the offset of the JCT control block fields:

- JCTINDEV (input device)
- JCTROUTE (NJE input device)
- JCTNJHDR (NJE header)

JCT offsets are determined automatically based on the JES level detected at CA Top Secret initialization. If your installation has made modifications to the JES2 JCT control block which shift the original offsets, the following procedure allows CA Top Secret to correctly locate the source of a batch job:

- Verify the version of primary JES2 running at your installation
- Verify the offsets of the affected JCT fields
- Use the CA Top Secret JCT control option to make adjustments

JES Startup

You can start the CA Top Secret address space prior to JES starting. You can see the \$\$LOG\$\$ spool file after JES is started. There is no need to provide a SYSOUT DD in the JCL. Once JES is up, CA Top Secret allocates a dynamic SYSOUT dataset and starts using it.

CA Top Secret also allows the dynamic allocation of JES files for each CPF node defined in the NDT. The CPF nodes defined via the parameter file are not eligible for spool allocation after JES has started. For CPF nodes defined in the NDT, after JES is started a refresh against those nodes will have to be issued to get the JES spool files allocated. CPF journal files are dynamically allocated once JES is started only if no SYSOUT DD statements exist in the JCL.

If an existing SYSOUT DD is found in the JCL, the following message is issued:

```
TSS9070W SYSOUT UNAVAILABLE, CPF JOURNAL FILE IGNORED FOR nodename
```


Concurrent Releases

You can install this release of CA Top Secret and continue to use an older release for your production environment. If you plan to continue to run a previous release, consider the following points:

- When installing into an existing SMP/E environment, this installation deletes previous releases.
- If you acquired your product from tape or with Pax-Enhanced ESD, select different target and distribution zones (or CSI) for your new release from where your current release is installed. The new zones use different libraries than your current release.

Note: CA CSM installs into a new CSI by default.

- Define DDDEF entries in your new zones to point SMP/E to the proper libraries for installation. Ensure that they point to the new release libraries.

Concurrent Releases

You can install this release of your product and continue to use an older release in another SMP/E environment. If you plan to continue to run a previous release, consider the following points:

- When you install the product into an existing SMP/E environment, this installation deletes previous releases in that environment.
- If you acquired your product with Pax ESD, select different target and distribution zones for your new release from where your current release is installed. The new zones use different libraries than your current release.

Note: CA CSM installs a product into a new SMP/E environment by default. You can select an existing SMP/E environment from your working set. For more information, see the online help that is included in CA CSM.

- Define DDDEF entries in your new zones to point SMP/E to the proper libraries for installation. Ensure that they point to the new release libraries.

Chapter 3: Installing Your Product Using CA CSM

This section contains the following topics:

[How to Install Your Product Using CA CSM](#) (see page 27)

Important! If you use CA CSM to install, deploy, and optionally configure your software, you must use SMP/E (RECEIVE, APPLY, and ACCEPT) to perform some CA Top Secret configuration processes at the Software Installation Services (SIS) level prior to deployment and configuration. For example, the [TSSKEY member](#) (see page 74) uses SMP/E to install an APAR named CRYPTKY that specifies the site security file encryption key. This USERMOD APAR must be installed at the SIS level because this level has an SMP/E environment, unlike the Software Deployment Services (SDS) and Software Configuration Services (SCS) levels used by MSM. If you have other USERMODs to modify CA Top Secret elements (whether site-generated or supplied by CA Technologies), you must use SMP/E to install them at the SIS level.

How to Install Your Product Using CA CSM

As a system programmer, your responsibilities include acquiring, installing, maintaining, deploying, and configuring CA Technologies mainframe products on your system.

CA CSM is an application that simplifies and unifies the management of your CA Technologies mainframe products on z/OS systems. As products adopt the CA CSM services, you can install your products in a common way according to industry best practices.

This scenario describes the steps for a system programmer to acquire, install, deploy, and configure products and maintenance. Not all tasks may apply to your organization. For example, you may decide not to deploy and configure products. In this case, do not perform the product deployment task and the product configuration task.

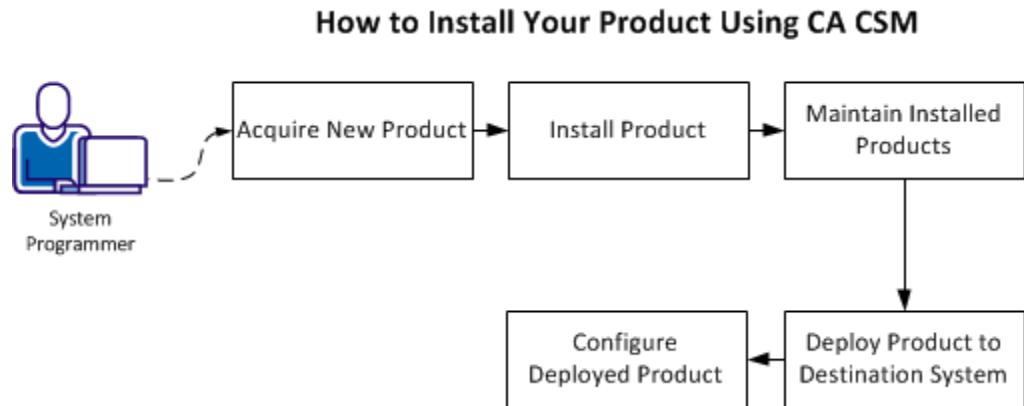
Before you use this scenario, you must have CA CSM installed at your site. If you do not have CA CSM installed, you can download it from the Download Center at <http://ca.com/support>. This web page also contains links to the complete documentation for CA CSM.

You [access CA CSM](#) (see page 29) from a web browser.

Note: This scenario applies to the latest version of CA CSM. If you are using an earlier version, see the appropriate bookshelf on the CA Chorus Software Manager product page.

This scenario is a high-level overview of steps that you perform using CA CSM. For more detailed information, use the online help that is included in CA CSM.

You perform the following tasks to install products and manage them on your system:



1. [Acquire a new product](#) (see page 29).
2. [Install the product](#) (see page 30).
3. [Maintain the installed products](#) (see page 32).
4. [Deploy the product to the destination system](#) (see page 33).
5. [Configure the deployed product](#) (see page 34).

Access CA CSM Using the Web-Based Interface

You access CA CSM using the web-based interface.

You need the URL of CA CSM from the CA CSM administrator.

Follow these steps:

1. Start your web browser, and enter the access URL.

The login page appears.

Note: If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password.

The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).

Note: For more information about the interface, click the online help link at the top right corner of the page.

3. Click New.

You are prompted for the credentials to use on [the CA Support Online website](#).

4. Specify the credentials, click OK, and then click Next.

You are prompted to review your user settings.

Note: These settings are available on the User Settings page.

5. Change the settings or keep the defaults, and then click Finish.

A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

Important! If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

Acquire a New Product

Acquisition allows you to download products and product maintenance from the CA Support Online website at <http://ca.com/support> to a USS directory structure on your system. The products to which your site is entitled and the releases available are displayed in the Available Products section on the Products page.

You perform the following high-level tasks to acquire a product using CA CSM:

1. Set up a CA Support Online account at <http://ca.com/support>.

To use CA CSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, create one on <http://ca.com/support>.

2. Determine the CA CSM URL for your site.

To [access CA CSM](#) (see page 29), you require its URL. You can get the URL from your site CA CSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA CSM account with your credentials that you use to access <http://ca.com/support>. This account enables you to download product packages.

3. Log in to CA CSM and go to the Products page to locate the product that you want to acquire.

After you log in to CA CSM, you can see the products to which your organization is entitled on the Products tab.

If you cannot find the product that you want to acquire, update the product list. CA CSM refreshes the product list through <http://ca.com/support> using the site IDs associated with your credentials.

4. Download the product installation packages.

After you find your product in the product list, you can download the product installation packages. To do so, use the Update Product Release action.

CA CSM downloads (acquires) the packages (including any maintenance packages) from the CA Support Online website.

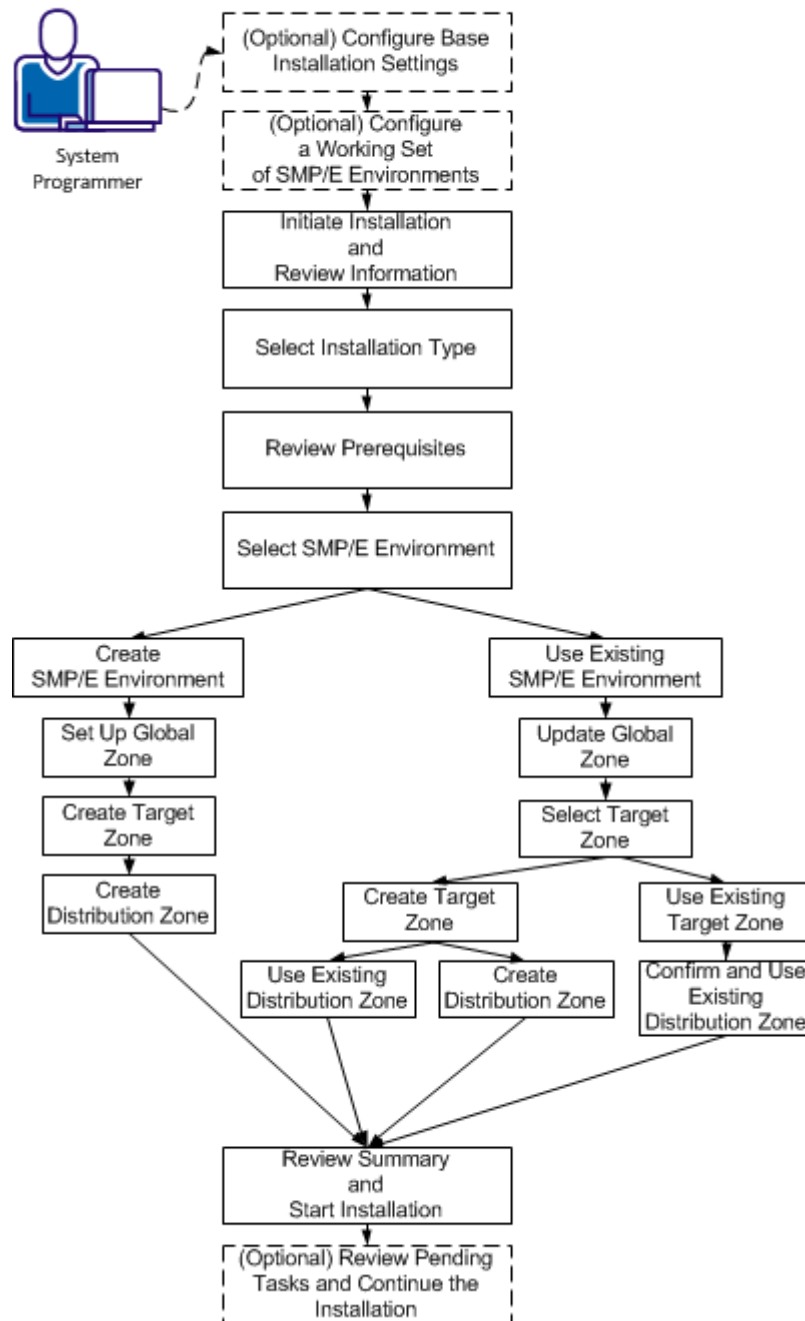
After the acquisition process completes, the product is ready for you to install or apply maintenance.

Install a Product

CA CSM simplifies and manages SMP/E installation tasks. You can browse and install a product that you acquired and that is available in the product list on the Products page. You can also install the maintenance for the products that are currently installed in a managed SMP/E environment on the driving system.

You perform the following high-level tasks to install a product using CA CSM:

How to Install a Product



1. (Optional) On the Settings tab, click Software Installation under System Settings, and configure base installation settings.
2. (Optional) Click the SMP/E Environments tab, and configure a working set of SMP/E environments.
3. Click the Products tab and select a product that you want to install. Start the installation wizard and review product information.
4. Select an installation type.
5. Review installation prerequisites if any are presented.
6. Take *one* of the following steps to select an SMP/E environment:
 - Create an SMP/E environment:
 - a. Set up the global zone.
 - b. Create a target zone.
 - c. Create a distribution zone.
 - Use an existing SMP/E environment from your working set:
 - a. Update the global zone.
 - b. Set up the target zone: Create a target zone or use an existing target zone.
 - c. Set up the distribution zone: Create a distribution zone or use an existing distribution zone.
7. Review the installation summary and start the installation.
8. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. Continue the installation, if applicable.

CA CSM installs the product.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes, there are other steps to perform manually outside of CA CSM before continuing.

Maintain the Installed Products

You can migrate existing SMP/E environments into CA CSM to maintain all your installed products in a unified way from a single web-based interface.

You can use CA CSM to maintain a CA Technologies product.

You perform the following high-level tasks to maintain a product using CA CSM:

1. Verify that CA CSM recognizes the SMP/E environment where your product is installed. If not, migrate the SMP/E environment to CA CSM.

During the migration, CA CSM stores information about the SMP/E environment in the database.

2. From the Product tab, download the latest maintenance for the installed product releases.

If you cannot find the required release, perform the following steps to download the maintenance:

- a. Add the release to the catalog manually.
 - b. Update the added release.
3. Apply the maintenance.

CA CSM applies the maintenance to your product.

After the maintenance process completes, the product is ready for you to deploy to systems that are defined in the system registry.

Deploy the Product to the Destination System

Deployment is a process of copying SMP/E target libraries to a destination system. The destination system could be the local z/OS system, a remote z/OS system, or a sysplex. You identify the destination system, deployed data set names, and the transport mechanism as part of the deployment process. Deploying a product makes it available for configuration.

Important! Before you deploy a product, set up the destination systems and remote credentials in the system registry.

You perform the following high-level tasks to deploy your products using CA CSM:

1. On the Deployments tab, set up methodologies.

Note: You can also set up methodologies when creating a deployment, or use existing methodologies, if you have set up any previously. If you do so, you can skip this step.

2. Start the New Deployment wizard to create a deployment. Complete each of the steps in the wizard. The wizard guides you through choosing deployment settings for your site. At any point, you can save your work and come back to it later.

3. Deploy:
 - a. Take a snapshot of the deployment.
 - b. Transmit the deployment to a destination system.
 - c. Deploy (unpack) to the mainframe environment.CA CSM deploys the product to the destination system.

After the deployment process completes, the product is ready for you to configure.

Configure the Deployed Product

Configuration is a process of copying the deployed libraries to run-time libraries and customizes the product for your site to bring it to an executable state. You can configure CA Technologies products that you have already acquired, installed, and deployed using CA CSM. You cannot use CA CSM to configure a product unless you have already used CA CSM to deploy the product.

You perform the following high-level tasks to configure your products using CA CSM:

1. Select a configurable deployment on the Deployments tab to view details and products for that deployment.
2. Select a product in the deployment and start the Configuration wizard to create a configuration. Complete each of the steps in the wizard. The wizard has multiple levels of detailed instructions and guides you through choosing configuration settings for your site. At any point, you can save your work and come back to it later. Configurations where you have partially completed the steps in the wizard are listed on the Configurations tab. The steps in the wizard include the following:
 - a. Define a configuration name and select a system for the configuration.
 - b. Select configuration functions and options.
 - c. Define system preferences.
 - d. Create target settings.
 - e. Select and edit resources.
3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again. Building the configuration closes the wizard and creates a configuration with all your settings.
4. (Optional) Validate the configuration. Validation verifies access to resources that are going to be used when you implement the configuration.

5. Implement the configuration. You implement a configuration to make your deployed software fully functional. Implementation executes on the destination system, applying the variables, resources, and operations that are defined in the configuration.

CA CSM configures the product.

After the configuration process completes, the product is ready for you to use.

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

[How to Install a Product Using Pax-Enhanced ESD](#) (see page 37)

[Allocate and Mount a File System](#) (see page 43)

[Copy the Product Pax Files into Your USS Directory](#) (see page 46)

[Create a Product Directory from the Pax File](#) (see page 51)

[Copy Installation Files to z/OS Data Sets](#) (see page 52)

[Receiving the SMP/E Package](#) (see page 53)

[Clean Up the USS Directory](#) (see page 57)

[Apply Maintenance](#) (see page 58)

How to Install a Product Using Pax-Enhanced ESD

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced ESD installation. For experienced UNIX users, the *Pax-Enhanced ESD Quick Reference Guide* has sufficient information for subsequent installations.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process.

If you prefer not to involve all CA Technologies product installers with z/OS UNIX System Services, assign a group familiar with USS to perform Steps 1 through 4 and provide the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-Enhanced ESD, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory. To download files, choose one of the following options:

- Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
- FTP the pax files from CA Support Online directly to your USS directory.

Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

3. Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command:

```
pax -rvf pax-filename
```

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory that the pax command created in Step 3 contains a sample JCL to GIMUNZIP the installation package. Edit and submit the UNZIPJCL JCL.
5. Receive the SMP/E package. Use the data sets that GIMUNZIP created in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILES on the RFPREFIX parameter of the RECEIVE command.
6. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.
7. (Optional) Clean up the USS directory. Delete the pax file, the directory that the pax command created, all of the files in it, and the SMP/E RELFILES, SMPMCS, and HOLDDATA data sets.

More Information:

[USS Environment Setup](#) (see page 42)

[Allocate and Mount a File System](#) (see page 43)

[Copy the Product Pax Files into Your USS Directory](#) (see page 46)

[Create a Product Directory from the Pax File](#) (see page 51)

[Copy Installation Files to z/OS Data Sets](#) (see page 52)

How the Pax-Enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-Enhanced ESD:

1. Log in to <https://support.ca.com/>, and click Download Center.

The CA Support Online web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.

The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

For both options, [The ESD Product Download Window](#) (see page 39) topic explains how the download interface works.

Note: For traditional installation downloads, see the *Traditional ESD User Guide*. Go to <https://support.ca.com/>, log in, and click Download Center. A link to the guide appears under the Download Help heading.

4. Perform the steps to install the product based on the product-specific steps.

The product is installed on the mainframe.

ESD Product Download Window

You can download CA Technologies product ESD packages multiple ways. Your choices depend on the size of the individual files and the number of files that you want to download. You can download the complete product with all components, or you can select individual pax and documentation files for your product or component.

How to Install a Product Using Pax-Enhanced ESD

The following illustration shows sample product files. The illustration lists all components of the product. You can use the Download Cart by selecting one or more components that you need, or selecting the check box for Add All to cart. If you prefer to immediately download a component, click the Download link.

CA Earl - MVS

- [Pax Enhanced Electronic Software Delivery \(ESD\) Guide](#)
- [Pax Enhanced Electronic Software Delivery \(ESD\) Quick Reference Guide](#)
- [Traditional Electronic Software Delivery \(ESD\) Guide](#)
- [Learn more about Using pkzip with your Downloaded Mainframe Products](#)
- [Learn more about downloading components of CA product](#)
- [Mounting ISO Images with OpenVMS](#)

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

Note: Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

[View Download Cart](#)

				<input type="checkbox"/> Add All to cart	
Product Components				Add to cart	Download
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	<input type="checkbox"/>	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	<input type="checkbox"/>	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	<input type="checkbox"/>	Download
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	<input type="checkbox"/>	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	10/30/2008	1.85MB	<input type="checkbox"/>	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	01/29/2010	93.92KB	<input type="checkbox"/>	Download
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	<input type="checkbox"/>	Download
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	<input type="checkbox"/>	Download
DATACOM/AD XPRESS INSTALL				<input type="checkbox"/>	Download

Clicking the link for an individual component takes you to the Download Method page.

Download Method

Please choose a download method to complete your download request. [Learn More](#)


HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

HTTP via Internet Browser

If Download Manager cannot be used or fails to start you may access your file(s) via your internet browser.

[View File Link\(s\)](#) 

FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

Depending on the size and quantity of ordered product files, the Download Method screen could also have these options:

Note: For mainframe downloads using this HTTP method, click the Learn More link.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

The Create a Zip File option first creates the zip, and when ready, offers the options that the Zip Download Request examples show in the next illustration.

Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to **'Ready'** a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our [FTP Help document](#)
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP ▾ Alternate FTP ▾

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▾ Alternate FTP ▾
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▾ Alternate FTP ▾

USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a directory for each pax download.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process. The USS file system that is used for Pax-Enhanced ESD must have sufficient free space to hold the directory that the pax command created, and its contents. You need approximately 3.5 times the pax file size in free space to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your ESD directory.

Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for ESD downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

Note: You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

Important! USS commands are case-sensitive.

Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(your_zFS_data_set_name) +
    STORAGECLASS(class) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate your_zFS_data_set_name -compat' )
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
/*
```

- On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAESD DD DSN=yourHFS_data_set_name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSN TYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

The file system is allocated.

Note: Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/  
mkdir CA  
cd CA  
mkdir CAESD
```

Note: This document refers to this structure as *yourUSSESDdirectory*.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(ZFS)  MODE(RDWR)  
      PARM(AGGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(HFS)  MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSESDdirectory/
```

Write access is granted.

Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

Copy the Product Pax Files into Your USS Directory

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up. Use one of the following methods:

- Download the product pax files directly from the CA Support Online FTP server to your z/OS system.
- Download the product pax file from the CA Support Online FTP server to your computer, and upload it to your z/OS system.
- Download the product file from CA Support Online to your computer. If your download included a zip file, unzip the file, and upload the unzipped pax files to your z/OS system.

This section includes a sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system and sample commands to upload a pax file from your computer to a USS directory on your z/OS system.

Important! The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

More Information:

[How the Pax-Enhanced ESD Download Works](#) (see page 39)
[ESD Product Download Window](#) (see page 39)

Download Using Batch JCL

Use this process to download a pax file from the CA Support Product Downloads window by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as *CAtoMainframe.txt* to perform the download.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Note: We recommend that you follow the preferred method as described on CA Support Online. This procedure is our preferred download method; however, we do include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.

The job points to your profile.

3. Replace *YourEmailAddress* with your email address.

The job points to your email address.

4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

You have identified the product component to download.

6. Click Download for the applicable file.

Note: For multiple downloads, add files to a cart.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download.

Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

Preferred FTP

Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

Host Name: ftp://ftpdownloads.ca.com

Alternate FTP

Uses the original download servers that are based on Long Island, New York.

Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

Note: The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

Example: CAtoMainframe.txt, JCL

The following text appears in the attached CAtoMainframe.txt JCL file:

```
//GETPAX   JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* When editing the JCL ensure that you do not have sequence numbers *
/* turned on.                                                    *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                               *
/* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be *
/*    optional at your site. Remove the statements that are not  *
/*    required. For the required statements, update the data set  *
/*    names with the correct site-specific data set names.       *
/* 3. Replace "Host" based on the type of download method.       *
/* 4. Replace "YourEmailAddress" with your email address.        *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS     *
/*    directory used on your system for ESD downloads.           *
/* 6. Replace "FTP Location" with the complete path              *
/*    and name of the pax file obtained from the FTP location   *
/*    of the product download page.                              *
//*****
//GETPAX   EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD  DD   DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD  DD   DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD   SYSOUT=*
//OUTPUT   DD   SYSOUT=*
//INPUT    DD   *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP_location
quit
```

Download Files to Mainframe through a PC

If you download pax or zip files from CA Support Online to your PC, use this procedure to upload the pax file from your PC to your z/OS USS directory.

Follow these steps:

1. Follow the procedures in How the Pax-Enhanced ESD Download Works to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the FTP commands with the following changes:

- a. Replace *mainframe* with the z/OS system IP address or DNS name.
- b. Replace *userid* with your z/OS user ID.
- c. Replace *password* with your z/OS password.
- d. Replace *C:\PC\folder\for\thePAXfile* with the location of the pax file on your PC.
- e. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
- f. Replace *paxfile.pax.Z* with the name of the pax file to upload.

The pax file is transferred to the mainframe.

Example: FTP Commands

This list is a sample of FTP commands to upload the pax file from your PC to your USS Pax-Enhanced ESD directory:

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

Note: If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

Sample Job to Execute the Pax Command (Unpackage.txt)

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSESDdirectory" with the name of the USS *
/* directory used on your system for ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, make *
/* sure the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BPXBATCH,
/* PARM='sh cd /yourUSSESDdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
 - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
 - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:

- a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.

Note: The default Java location is the following:

`/usr/lpp/java/Java_version`

- b. Perform one of the following steps:

- Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically `/usr/lpp/smp/classes/`.
- Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

One of the following occurs: ICSF is active, or you are using Java.

5. Change all occurrences of *yourHLQ* to the high-level qualifier (HLQ) for z/OS data sets that the installation process uses. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for *yourHLQ* as you use for the SMP/E RELFILES.

All occurrences of *yourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

Note: For more information, see the IBM *SMP/E for z/OS Reference (SA22-7772)*.

Receiving the SMP/E Package

If you are installing the package into a new SMP/E environment, use the sample jobs included with the product to set up an SMP/E environment before proceeding.

At this point, complete the SMP/E RECEIVE using files on DASD that the UNZIPJCL job created. Consult the product sample JCL library that contains a sample job customized to receive the product from DASD. Specifically, you must specify the following values:

- DASD data set names for SMPPTFIN and SMPHOLD (if applicable)
- The HLQ that you used in the UNZIPJCL job on the RFPREFIX parameter on the RECEIVE command

(Optional) Clean Target and Distribution Libraries

If you have installed other CA Technologies products using SMP/E, complete this procedure.

To clean up the libraries (r12)

Note: Members KODELCO and KODELCOC are located in the CAIJCL library.

1. If you are installing into a zone that currently has CA Top Secret r12 installed, run KODELCO.
2. If necessary, run a separate UCLIN job to do additional cleanup.
3. Check the contents of CAILIB. If the data set is empty, proceed with the normal installation. If members remain in CAILIB (for example, TSSCAI, TSSCCHEK, and TSSCCTSS), run KODELCOC.

The cleanup process is completed.

To clean up the libraries (r9)

Note: Members KODEL90 and KODEL9OC are located in the CAIJCL library.

1. If you are installing into a zone that currently has CA Top Secret r9 installed, run KODEL90.
2. If necessary, run a separate UCLIN job to do additional cleanup.
3. Check the contents of CAILIB. If the data set is empty, proceed with the normal installation. If members remain in CAILIB (for example, TSSCAI, TSSCCHEK, and TSSCCTSS), run KODEL9OC.

The cleanup process is completed.

How to Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Allocate product data sets and SMP/E data sets.
2. Create SMP/E CSI.
3. Receive base functions.
4. Apply base functions.
5. Accept base functions.
6. Configure the product according to your site requirements.

Prepare the SMP/E Environment for Pax Installation

The members that are used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Top Secret.

For information about the members, see the comments in the JCL.

Follow these steps:

1. Customize the macro TSSSEDIT with your site-specific information and then copy the macro to your SYSPROC location. Replace the rightmost parameters for each ISREDIT CHANGE command. Each time you edit an installation member, type TSSSEDIT on the command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize the *yourHLQ*.SAMPJCL members.

Note: Set the DASD HLQ to the same value specified for *yourHLQ* for the unzip to DASD ESD JCL.

Note: The following steps include instructions to execute the TSSSEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the TSSDALL member.

2. Open the SAMPJCL member TSS1ALL in an edit session and execute the TSSSEDIT macro from the command line.

TSS1ALL is customized.

3. Submit TSS1ALL.

This job produces the following results:

- The target and distribution data sets for CA Top Secret are created.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member TSS2CSI in an edit session and execute the TSSSEDIT macro from the command line.

TSS2CSI is customized.

5. Submit TSS2CSI.

This job produces the following results:

- The CSI data set is defined.
- The SMPPTS and SMPLOG data sets are allocated.
- The global, target, and distribution zones are initialized.
- The DDDEF entries for your product are created.
- The DDDEFs for the required SMP/E data sets are created.

Component Installation

As part of a standard CA Top Secret installation, you can install various components to support the security product. During the following procedure, if you do not want to install any of the following components, comment out the applicable FMID in the RECEIVE job. For details about each component, see <http://ca.com/support>.

The following list identifies and describes each FMID that is part of the RECEIVE job:

CAKOF00

Specifies CA Top Secret MVS base and SAF.

CAKOF01

Specifies CA Top Secret MVS CICS Interface. To protect CICS resources, you must receive this base component.

CAKOF02

Specifies CA Top Secret MVS IMS Base Interface. To protect IMS resources, you must receive this base IMS component and the appropriate release-specific component.

CAKOF03

Specifies CA Top Secret IDMS INTERFACE.

CAKOF04

Specifies CA Top Secret MVS Roscoe Interface. To protect CA Roscoe resources, you must receive this component.

Run the Installation Jobs for a Pax Installation

Submit and run these *yourHLQ*.SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

Follow these steps:

1. Open the SAMPJCL member TSS3RECD in an edit session, and execute the TSSSEDIT macro from the command line.
TSS3RECD is customized.
2. Submit the *yourHLQ*.SAMPJCL member TSS3RECD to receive SMP/E base functions.
Third-Party Software for CA Top Secret is received and now resides in the global zone.
3. Open the SAMPJCL member TSS4APP in an edit session, and execute the TSSSEDIT macro from the command line.
TSS4APP is customized.

4. Submit the *yourHLQ*.SAMPJCL member TSS4APP to apply SMP/E base functions.
Third-Party Software for CA Top Secret is applied and now resides in the target libraries.
5. Open the SAMPJCL member TSS5ACC in an edit session, and execute the TSSSEDIT macro from the command line.
TSS5ACC is customized.
6. Submit the *yourHLQ*.SAMPJCL member TSS5ACC to accept SMP/E base functions.
Third-Party Software for CA Top Secret is accepted and now resides in the distribution libraries.

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

Note: Retain non-SMP/E installation data sets such as *yourHLQ*.INSTALL.NOTES for future reference.

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.
Your view is of the applicable USS directory.
2. Delete the pax file by entering the following command:

```
rm paxfile
```

paxfile

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific_directory
```

product-specific_directory

Specifies the product-specific directory that the pax command created.

The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

Apply Maintenance

CA Support Online has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Follow these steps:

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. If the base release was created recently, no PTFs or HOLDDATA will have been published yet.
2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.

The PTFs and HOLDDATA become accessible to the *yourHLQ.SAMPJCL* maintenance members.
3. The TSSSEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.
4. Open the SAMPJCL member TSS6RECP in an edit session and execute the TSSSEDIT macro from the command line.

TSS6RECP is customized with your JOB statement, CSI location, and zone names.
5. Customize the TSS6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit TSS6RECP.

The PTFs and HOLDDATA are received.
7. Open the SAMPJCL member TSS7APYP in an edit session and execute the TSSSEDIT macro from the command line.

TSS7APYP is customized.

8. Submit TSS7APYP.

The PTFs are applied.

9. (Optional) Open the SAMPJCL member TSS8ACCP in an edit session and execute the TSSSEDIT macro from the command line.

TSS8ACCP is customized.

10. (Optional) Submit *your*HLQ.SAMPJCL member TSS8ACCP.

The PTFs are accepted.

Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for your product:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

EC

Indicates that this SYSMOD requires a hardware engineering change. An EC hold SYSMOD usually does not affect the product unless the EC is present on the hardware device.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

IPL

Indicates that an IPL is required for this SYSMOD to take effect. This is used only when there is no alternative for dynamic activation.

MSGSKEL

Indicates that the SYSMOD contains internationalized message versions that must be run through the message compiler for each language.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SQLBIND

Indicates that a bind is required for a database system other than DB2.

DOWNLD

Indicates that some or all of the elements that this SYSMOD delivers are to be downloaded to a workstation.

Code a BYPASS(HOLDSYS) operand on your APPLY command to install SYSMODs that have internal holds. Code the BYPASS(HOLDSYS) operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. The HOLDDATA resides in a separate file. The HOLDDATA is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA Technologies publishes a SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class that is called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system
- Any resolving SYSMODs that are in RECEIVE status

SMP/E identifies the SYSMOD to apply to correct the situation.

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

[Unload the Sample JCL from Tape](#) (see page 64)

[How to Install Products Using Native SMP/E JCL](#) (see page 65)

[Apply Maintenance](#) (see page 67)

Unload the Sample JCL from Tape

To simplify the process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the UnloadJCL.txt file to view the sample JCL job.

Note: The sample JCL to install the product is also provided in the CAI.SAMPJCL library on the distribution tape.

Follow these steps:

1. Run the following sample JCL:

```
//COPY      EXEC  PGM=IEBCOPY,REGION=4096K
//SYSPRINT  DD   SYSOUT=*
//SYSUT1    DD   DSN=CAI.SAMPJCL,DISP=OLD,UNIT=unitname,VOL=SER=nnnnnnn,
//          LABEL=(1,SL)
//SYSUT2    DD   DSN=yourHLQ.SAMPJCL,
//          DISP=(,CATLG,DELETE),
//          UNIT=sysda,SPACE=(TRK,(15,3,6),RLSE)
//SYSUT3    DD   UNIT=sysda,SPACE=(CYL,1)
//SYSIN     DD   DUMMY
```

unitname

Specifies the tape unit to mount the tape.

nnnnnnnn

Specifies the tape volume serial number.

yourHLQ

Specifies the data set prefix for the installation.

sysda

Specifies the DASD where you want to place the installation software.

The SAMPJCL data set is created and its contents are downloaded from the tape.

2. Continue with one of the following options:
 - If you already have set up the SMP/E environment, go to Run the Installation Jobs for a Tape Installation.
 - If you have *not* set up the SMP/E environment, go to Prepare the SMP/E Environment for Tape Installation.

How to Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Allocate product data sets and SMP/E data sets.
2. Create SMP/E CSI.
3. Receive base functions.
4. Apply base functions.
5. Accept base functions.
6. Configure the product according to your site requirements.

Prepare the SMP/E Environment for Tape Installation

The members that are used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA Top Secret.

For information about the members, see the comments in the JCL.

Follow these steps:

1. Customize the macro TSSSEDIT with your site-specific information and then copy the macro to your SYSPROC location. Replace the rightmost parameters for each ISREDIT CHANGE command. Each time that you edit an installation member, type TSSSEDIT on the command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize your *yourHLQ*.SAMPJCL members.

Note: The following steps include instructions to execute the TSSSEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the TSSDALL member.

2. Open the SAMPJCL member TSS1ALL in an edit session and execute the TSSSEDIT macro from the command line.

TSS1ALL is customized.

3. Submit TSS1ALL.

This job produces the following results:

- The target and distribution data sets for CA Top Secret are created.
- Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

4. Open the SAMPJCL member TSS2CSI in an edit session and execute the TSSSEDIT macro from the command line.

TSS2CSI is customized.

5. Submit TSS2CSI.

This job produces the following results:

- The CSI data set is defined.
- The SMPPTS and SMPLOG data sets are allocated.
- The global, target, and distribution zones are initialized.
- The DDDEF entries for your product are created.
- The DDDEFs for the required SMP/E data sets are created.

Component Installation

As part of a standard CA Top Secret installation, you can install various components to support the security product. During the following procedure, if you do not want to install any of the following components, comment out the applicable FMID in the RECEIVE job. For details about each component, see <http://ca.com/support>.

The following list identifies and describes each FMID that is part of the RECEIVE job:

CAKOF00

Specifies CA Top Secret MVS base and SAF.

CAKOF01

Specifies CA Top Secret MVS CICS Interface. To protect CICS resources, you must receive this base component.

CAKOF02

Specifies CA Top Secret MVS IMS Base Interface. To protect IMS resources, you must receive this base IMS component and the appropriate release-specific component.

CAKOF03

Specifies CA Top Secret IDMS INTERFACE.

CAKOF04

Specifies CA Top Secret MVS Roscoe Interface. To protect CA Roscoe resources, you must receive this component.

Run the Installation Jobs for a Tape Installation

Submit and run these SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

Follow these steps:

1. Open the SAMPJCL member TSS3RECT in an edit session and execute the TSSSEDIT macro from the command line.
TSS3RECT is customized.
2. Submit the *yourHLQ*.SAMPJCL member TSS3RECT to receive SMP/E base functions.
CA Top Secret is received and now resides in the global zone.
3. Open the SAMPJCL member TSS4APP in an edit session and execute the TSSSEDIT macro from the command line.
TSS4APP is customized.
4. Submit the *yourHLQ*.SAMPJCL member TSS4APP to apply SMP/E base functions.
Your product is applied and now resides in the target libraries.
5. Open the SAMPJCL member TSS5ACC in an edit session and execute the TSSSEDIT macro from the command line.
TSS5ACC is customized.
6. Submit the *yourHLQ*.SAMPJCL member TSS5ACC to accept SMP/E base functions.
Your product is accepted and now resides in the distribution libraries.

Note: We recommend that you check for available maintenance; however, you may find that none is available.

Apply Maintenance

CA Support Online has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Follow these steps:

1. Check CA Support Online and download any PTFs and HOLDDATA published since this release was created. If the base release was created recently, no PTFs or HOLDDATA will have been published yet.
2. Transfer the downloaded files to two separate FB 80 sequential data sets. Use one data set to contain the PTFs and the other to contain the HOLDDATA.
The PTFs and HOLDDATA become accessible to the *yourHLQ*.SAMPJCL maintenance members.

3. The TSSSEDIT macro was customized in the installation steps. Verify that you still have the values from the base installation.
4. Open the SAMPJCL member TSS6RECP in an edit session and execute the TSSSEDIT macro from the command line.
TSS6RECP is customized with your JOB statement, CSI location, and zone names.
5. Customize the TSS6RECP SMPPTFIN and SMPHOLD DD statements to reference the FB 80 data sets for the PTFs and HOLDDATA.
6. Submit TSS6RECP.
The PTFs and HOLDDATA are received.
7. Open the SAMPJCL member TSS7APYP in an edit session and execute the TSSSEDIT macro from the command line.
TSS7APYP is customized.
8. Submit TSS7APYP.
The PTFs are applied.
9. (Optional) Open the SAMPJCL member TSS8ACCP in an edit session and execute the TSSSEDIT macro from the command line.
TSS8ACCP is customized.
10. (Optional) Submit *your*HLQ.SAMPJCL member TSS8ACCP.
The PTFs are accepted.
Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for your product:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

EC

Indicates that this SYSMOD requires a hardware engineering change. An EC hold SYSMOD usually does not affect the product unless the EC is present on the hardware device.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

IPL

Indicates that an IPL is required for this SYSMOD to take effect. This is used only when there is no alternative for dynamic activation.

MSGSKEL

Indicates that the SYSMOD contains internationalized message versions that must be run through the message compiler for each language.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SQLBIND

Indicates that a bind is required for a database system other than DB2.

DOWNLD

Indicates that some or all of the elements that this SYSMOD delivers are to be downloaded to a workstation.

Code a BYPASS(HOLDSYS) operand on your APPLY command to install SYSMODs that have internal holds. Code the BYPASS(HOLDSYS) operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. The HOLDDATA resides in a separate file. The HOLDDATA is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA Technologies publishes a SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class that is called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system
- Any resolving SYSMODs that are in RECEIVE status

SMP/E identifies the SYSMOD to apply to correct the situation.

Chapter 6: Starting Your Product

This section contains the following topics:

[How to Complete Configuration With CA CSM](#) (see page 73)

[How to Configure Without CA CSM](#) (see page 107)

[Startup and Shutdown Sequence](#) (see page 108)

[Start CA Top Secret](#) (see page 108)

[Activate CA Top Secret](#) (see page 109)

[Restarting CA Top Secret](#) (see page 110)

[CA Top Secret Shutdown](#) (see page 111)

How to Complete Configuration With CA CSM

The topics in this section describe the manual tasks that you perform when [configuring your product using CA CSM](#) (see page 34).

You must perform the following configuration tasks manually, regardless of whether you are using CA CSM to perform product configuration:

- [Assign your key to the library](#) (see page 74).
- [Authorize the product libraries](#) (see page 75).
- [Authorize TSS commands](#) (see page 75).
- [Set up SAF SECTRACE](#) (see page 76).
- Install ENF DCM.
- [Customize the started task procedure](#) (see page 78).
- [Update the TSSB backup started task](#) (see page 78).
- [Edit commands to initiate and follow CA Top Secret](#) (see page 79).
- [Create the parameter file](#) (see page 81).
- [Upgrade the existing security file](#) (see page 83) or [create a new file](#) (see page 84).
- [Create a backup security file](#) (see page 92).
- [Create a recovery file](#) (see page 94).
- [Create an audit/tracking file](#) (see page 95) and an [alternate audit/tracking file](#) (see page 97).
- [Create a CPF recovery file](#) (see page 97).
- [Create the RCACHE VSAM cluster](#) (see page 98).

- [Define the security console](#) (see page 99).
- [Set up backup, restore, and recovery procedures](#) (see page 99).
- [Modify your ISPF main menu](#) (see page 102).
- [Set up installation exits](#) (see page 103).
- [Customize your facility security](#) (see page 103).
- [Initialize CA Top Secret as a subsystem](#) (see page 103).

Assign the Key

You must assign a unique customer key to the CA Top Secret library to encrypt the security file before you start CA Top Secret. There is no default. The key is a 16-hexadecimal digit string separated into groups of four by commas (,). The first half of the key cannot match the second half.

Follow these steps:

1. Edit the CAKOJCL0 member TSSKEY to conform to your site's standards.
The member matches your standards.
2. Supply your company's key in the ????,???,???,??? field and submit the job.
The key is entered.
3. ACCEPT the APAR so that the key is not left in clear text format in your SMP/E data sets. If your site does not protect job output, delete the output from this step to reduce the chance of the key value being viewed.

Important! You must use an identical key in all future versions of CA Top Secret. Safeguard your key.

More Information:

[TSSXTEND - Extend the Security File](#) (see page 113)

Authorize Product Libraries

Authorizing the product libraries prepares them for APF-authorized programs.

Follow these steps:

1. Edit the PROGxx member in SYS1.PARMLIB to add your CAKOLINK (formerly CAILIB or CAILOAD) and CAKOLPA libraries so they are authorized.

The member is updated.

2. Place the CA Technologies common LINKLIST library CAKOLINK (formerly CAILIB or CAILOAD) in the SYS1.PARMLIB member LNKLISTxx. If a conflict exists with the module, rename the existing module.

The member is updated.

3. Place the CA Technologies common LPALIST library CAKOLPA into the SYS1.PARMLIB member LPALSTxx. If a conflict exists with the modules, rename the existing modules.

The member is updated.

4. Use SYS1.PARMLIB member PROGxx to specify disk volume serial numbers for libraries cataloged in the master catalog.

The member is updated.

Authorize TSS Commands

If you are running RACF, you must authorize CA Top Secret commands before CA Top Secret can run.

To authorize CA Top Secret commands, do *one* of the following:

- Add the TSS command using the AUTHCMD section of the SYS1.PARMLIB(IKJTSOxx). For example, AUTHCMD NAMES (TSS).
- Add the TSS command to the following TSO-authorized tables: IKJEFTE2 and IKJEFTE8.

For information about adding commands to IKJEFTE2 and IKJEFTE8, see IBM's *SPL:TSO Guide*.

Set Up SAF SECTRACE (Optional)

This procedure establishes SYS1.PARMLIB members that can initialize a SAF SECTRACE command during SAF initialization at the earliest possible stages of an IPL. The values do not initiate a SAF trace. If you need to initiate a SAF SECTRACE, CA Support will direct you to do so at the appropriate time.

Follow these steps:

1. Create member CAISEC00 in SYS1.PARMLIB and enter the following line at the beginning of column 1:

```
TRCE(00,NOSTART)
```

The member is created.

2. Create member CAITRC00 in SYS1.PARMLIB and enter the following line at the beginning of column 1:

```
ST DISPLAY,ID=ALL
```

The member is created.

(Optional) Install ENF Data Control Modules

Review the Data Control Modules (DCMs) if your site performs any of the following activities:

- Protects CICS resources
- Uses CPF
- Uses CA Technologies HFS security
- Uses CA Technologies DB2 security
- Uses SAPI

CA Top Secret uses the following DCMs:

KO50DCM2

Is needed to use CA Top Secret support for CICS CTS 2.3 and above. KO50DCM2 does not replace the KO43DCM2 used with earlier releases of CICS. KO50DCM2 specifies a new initialization routine named CAKSCINT.

CARRDCM0

Is needed for HFSSEC security. CARRDCM0 is the ENF DCM for ENF/USS.

J163DCM0

Is needed for HFSSEC security.

DB10DCM1

Is needed for CA Technologies DB2 security.

CAS9DCM4

Is needed for SAPI.

When you work with DCMs, the following considerations apply:

- CA ACF2 and CA Top Secret DCM modules cannot be defined together in the same ENF database or parameter file.
- Having multiple DCMs of the same type simultaneously defined causes performance problems and duplicate CA Top Secret messages.

To install ENF DCMs, perform *one* of the following actions:

- (CA Common Services r12 and above) Edit your ENF parameter file to define the necessary DCMs for your site.

The product installs (or verifies) the DCMs when the CAIENF address space starts.

Note: For more information about DCM configuration in the ENF parameter file, see the CA Common Services documentation.

- (CA Common Services r11 and lower) Edit the TSSENFDC job to install the necessary DCMs into the database, and submit the job.

The product installs the DCMs according to your specifications.

How to Edit the Started Task

Use this process to edit the TSS started task procedure so that you can customize it for your site.

Note: The VSAM file is no longer optional.

1. Edit the TSS member to choose the high-level qualifier for the CA Top Secret security file and optional recovery, backup, and audit files.

The HL parameter is for this purpose.

2. Determine if you will perform the recovery, backup, and audit functions and then comment or delete corresponding DD statements:

- RECFIL for Recovery
- BACKUP for Backup
- AUDIT and AUDIT2 for Audit

Do not DUMMY the files.

3. Choose a data set name for the parameter file and the auto commands file. Use the PARMS parameter to specify these names.
4. Copy the edited file to a procedure library so that TSS can be started from as a system task.

Note: We do not recommend the use of STEPLIB.

How to Update the TSSB Backup Started Task Procedure

Use this process to ensure that the security file is backed up every 24 hours.

Skip this process if you commented or deleted the BACKUP DD statement in the TSS procedure.

1. Update the TSSB parameter HL so that it is identical with that used in TSS.
2. Update the TSSB parameter PARMS so that it is identical with that used in TSS.
3. Update the VSAMFILE, VSAMAIX, and VSMPATH DD statements to point to the VSAMCOPY, AIXCOPY, and PATHCOPY data sets.

Edit Commands to Initiate and Follow CA Top Secret Initiation

You can edit commands to initiate and follow CA Top Secret initiation. If you start CA Top Secret:

- Before JES, place the following command in COMMNDxx:

```
COM='S TSS,SUB=MSTR'
```

After CA Top Secret initiates, the autocommand member TSSAUTO0 contains the following to initiate JES:

```
S JES2 or S JES3
```

All other tasks started by the IPL process follow the start of JES through the CA Top Secret Auto commands.

- After JES, place the following commands in COMMNDxx:

```
COM='S JES2' or 'S JES3'
```

```
COM='S TSS'
```

TSSAUTO0 Command

The format of commands for TSSAUTO0 is the same as a console operator command, starting in column 1. For example, S NET starts VTAM procedure NET.

The AUTOCMDSD DD statement in the TSS STC procedure defines the TSSAUTO0 file for CA Top Secret. CA Top Secret executes the commands upon the first invocation of CA Top Secret on the CPU. If it is restarted, the commands file is ignored. If it abends during initialization and the automatic commands have not yet been issued, it attempts to issue them before terminating.

Initialization Sequence

CA Top Secret initialization must be complete before you start online systems such as CICS, CA Roscoe, and IMS. Complete initialization is indicated by the CA Top Secret message number TSS9000I.

If CA Top Secret is not the first STC procedure started, all tasks that reference *secured* data sets and that do not use the BYPASS security attribute (from the z/OS program properties table) are abended with SE82 or S922 completion codes (default z/OS security).

File Characteristics

The automatic commands file is a standard sequential data set or member of a PDS library (such as SYS1.PARMLIB) with the following DCB attributes:

- LRECL=80
- RECFM=F(B)
- DSORG=PS/PO

File Contents

The automatic commands file holds any O/S commands that may be started as part of the normal IPL procedure. The file can also contain comment cards that must be identified by an asterisk (*) in column 1. The following example shows the content of a typical automatic commands file:

```
*  
* AUTOMATIC IPL COMMANDS  
*  
S IPLPROC,SYS=1  
S NETWORK  
$SI1-10
```

File Location

The automatic commands file does not have to reside in SYS1.PARMLIB. It can reside in any library. Protect this library to avoid possible tampering.

Create the Parameter File

The CA Top Secret control options that define the installation's environment are placed in the CA Top Secret parameter file.

The parameter file can contain any number of records. Control options are processed in the order that they are placed in the parameter file. Options can override previous options. For example, to override specific facilities, the FACILITY control option must be placed after control options such as MODE and LOG.

Follow these steps:

1. Open the CAKOJCL0 member TSSPARM0 for editing and enter the control options anywhere between positions 1 through 70, generally one per line.

Note: You can use free format, with or without commas as separators.

A maximum of 32,768 entries can be made in the parameter file. The recommended initial control options should include:

MODE

Sets global security mode.

Default: FAIL

LOG

Controls recording of security events.

Default: MSG,SEC9,SMF,INIT

DOWN

Selects DOWN options for CA Top Secret

Default: SB,TW,BW,OW

FACILITY

Selects options per facility.

Default: See the *Control Options Guide*.

JOBACID

Locates ACID on BATCH job card.

Default: U,7

NEWPW

Sets specifications for new passwords.

Default: MIN=4,WARN=3 MINDAYS=1 NR=0, NV, ID, RS, TS.

PRODUCTS

Indicates that special products are listed.

Default: TSO/E

SUBACID

Controls derivation of BATCH job ACIDs submitted through the internal reader.

Default: U,7

The control options are specified.

2. Make any comment statements. Comments are identified by an asterisk, (*), in the first position or an asterisk after a control statement.

Comments are specified.

3. Save the parameter file. TSSPARM0 does not have to reside in SYS1.PARMLIB. It can reside in any library protected to avoid possible tampering.

The file is saved.

4. Identify the parameter file to CA Top Secret with the PARMFILE DD statement in the TSS STC procedure.

CA Top Secret can identify the parameter file.

Control Option Overrides (Optional)

Other than in the parameter file, you can specify control options by:

- Placing the control option in the EXEC PARM field of the TSS STC procedure. For example:

```
// EXEC PGM=TSSMNGR4,PARM='list-of-control-options'
```

The maximum length of the field is limited to 100 bytes.

- Using the O/S START command. For example:

```
S TSS,,,list-of-control-options
```

- Using the O/S MODIFY command. For example:

```
F TSS,list-of-control-options
```

- Using the TSS MODIFY command. For example:

```
TSS MODIFY('control option')
```

Upgrade the Existing Security File (Optional)

Skip this section if you are installing CA Top Secret for the first time.

Note: If you are currently running with a BDAM file or an r9 VSAM file, you must upgrade to an r15 VSAM file because r15 does not support BDAM or the r9 VSAM file structure.

Follow these steps:

1. From your previous release of CA Top Secret, run the TSSFAR utility with the SFSTATS option against your existing backup security file.

A file analysis report is generated.

2. Use the file analysis report to determine the minimum parameter values for the current release of the security file.

You have determined the minimum parameter values.

3. Use TSSMAIND and TSSMAINS to allocate all of special blocks directly.

If you use the traditional BLOCKS allocation for the security file, perform the following steps:

- a. Comment the CYLS parameter.
- b. Uncomment the BLOCKS parameter.
- c. Update the BLOCKS parameter with the number reported by TSSMAIND.

With this choice, security data is read with only one block per SIO.

4. Copy your existing security file into the newly allocated security file using the procedures described in the appendix TSSXTEND and TSSRECVR.

Important! If the parameters of the new security file were changed, you must also [create a backup security file on DASD](#) (see page 92).

Your existing security file is copied to the newly allocated security file.

5. Change the SECFILE and BACKUP DD statements in your TSS startup proc to point to the newly allocated security files.

The statements point to the newly allocated security file.

PIEBLOCKS, RESBLOCKS, and SDTBLOCKS

PIEBLOCKS, RESBLOCKS, and SDTBLOCKS are allocated to hold prefixed resource ownership. New user defined resources in CA Top Secret can be defined as either prefixed resources or general resources. RESBLOCKS are allocated to hold general resource ownerships.

SDTBLOCKS hold definitions for SDT records and may be used implicitly for KERBEROS and Digital Certificate support. MLSBLOCKS hold definitions for resources protected with a security label.

RES Blocks allocated:	nnn	% used	mmm
PIE Blocks allocated:	nnn	% used	mmm
SDT Blocks allocated:	nnn	% used	mmm
MLS Blocks allocated:	nnn	% used	mmm

The values listed represent minimum allocations required to successfully copy your old security file into your new security file.

Creating the Security File

The security file contains all security-related information about users, profiles, departments, divisions, zones, and resources.

Important! A pre-r5.2 security file cannot be used with r15. A security file created with r15 cannot be used with r9 or lower.

The size of the security file does not affect CA Top Secret performance. The security file requires contiguous space on DASD. It is organized for direct access and can be located on a 3390 device.

DFSMS Extended Sequential data sets (multi volume data sets) are not supported.

If the security file is extended with the NEWPWBLOCK option, mixed-case passwords, special characters, and long passwords are allowed. Security files initialized with TSSMAINT from the r15 libraries are defined with the NEWPWBLOCK format by default.

More Information:

[CA Top Secret Health Checks](#) (see page 121)

Security File Location

Isolate the security file on a device with nothing else on the disk. This device should be high performance DASD. We recommend that no other data reside on this device. Fill the remaining DASD space on the volume with a dummy data set. This action prevents someone with access to the volume from using the free space. Protect this data from access. If isolating the security file is not an option, ensure that any other data placed on the device is not used during prime time business hours.

Determining the Security File Block Size

Select a block size to match your environment. The default block size must be a multiple of 256 and a minimum of 8192. When calculating the optimal block size, remember that the file contains keyed records with a 17 byte key.

The default parameters allow for 5,000 ACIDs and 1000 (DASD) volumes.

The file structure allows in excess of 3 million ACIDs to be defined in the security file.

Use half-track blocking if you specify more than 2,318,336 ACIDs. The best block size for half-track blocking is 27,648. However, any block size greater than 17,920 results in half-track blocking. With half-track blocking, two physical blocks of data reside on a track of the device. The smaller the block size, the fewer the number of ACIDs that can be defined for each block.

If the block size is not specified, TSSMAINT determines a default based on the type of device the file resides on.

Calculate Required Blocks

This procedure determines the number of blocks needed to create the security file.

Follow these steps:

1. Edit TSSMAIND and SECPARMS to conform to your site's standards.

MLSBLOCKS=?????

(Optional) Each MLS index entry requires one entry with a length of 14 plus the length of the resource name. For information, see the *Multilevel Security Planning Guide*.

2. Specify the name of the dummy run in the SECDUMMY member referenced in TSSMAIND.

3. Set the ID=DUMMY parameter to consist of a maximum of eight characters.
4. Execute a dummy run with the JCL in TSSMAIND.

The number of blocks required is returned.

Note: Running TSSMAIND causes an SD37 ABEND or U1520. This is normal.

Create the VSAM File

To maintain digital certificates, keyrings, and Kerberos KERBSEGM and KERBLINK records in a VSAM data set, use IDCAMS to allocate the data set. Using the VSAM data set allows heavy use of digital certificates. To assign a name to your users, use the Kerberos KERBNAME for your web users. The VSAM data set increases the amount of records that can be stored by converting the records to VSAM.

The r9 VSAM file structure is no longer supported. CA Top Secret only supports the r12 and later VSAM file structure. If you are using the r9 VSAM file structure, allocate an r12 and later VSAM file structure and run TSSXTEND to copy the security file and r9 VSAM file to the new security file.

Note: References to the *VSAM file* in this guide indicate the r12 and later file structure unless noted otherwise.

Follow these steps:

1. Edit the sample JCL provided in VSAMDEF3 to specify the data set name and volume to be allocated.

Note: Do not run STEP 2 if the security file is not shared.

The sample includes your site-specific values.

2. Run VSAMDEF3.

The VSAM base cluster file is defined. If the security file is shared, the alternate index file and path file are defined.

3. Specify this data set on the VSAMFILE DD statement in the jobs that execute TSSMAINT.

The VSAM file is created.

After the VSAM file is created, if you wish to copy in information from an existing security file you must run the TSSXTEND utility. You can copy information from a BDAM only security file or a security file that uses both BDAM and VSAM files.

Create the Security File

You can use the TSSMAINS utility to create the security file for your system. The security file contains all security-related information about users, profiles, departments, divisions, zones, and resources.

Follow these steps:

1. Use the number of blocks [calculated by TSSMAIND](#) (see page 85) to determine the size of the security file in cylinders:

$$\text{CYLS} = 1 + \text{BLOCKS} / (\text{BLKS_PER_TRK} * \text{TRKS_PER_CYL})$$

BLKS_PER_TRK

Specifies the number of physical blocks with the block size you specified that can be placed on a track.

TRKS_PER_CYL

Specifies the number of physical tracks per cylinder.

The size is determined.

2. Edit the CAKOJCL0 member TSSMAINS:
 - a. Specify the security file parameters, line by line, to satisfy your site standards:

ACCESSORS=nnnn

Specifies the maximum number of user, profile, department, division, and zone ACIDs defined to CA Top Secret. The value that you enter for *nnnn* determines the amount of security file space that is allocated to hold ACID-related security information.

Default: 5000

The following formula determines the actual number of allocated ACIDs:

$$(((\# \text{ accessors requested} * 16) / \text{blksize}(\text{quotient only, no remainder})) + 1) * (\text{blksize} / 16)$$

Example:

```
ACCESSORS=7000
BLKSIZE=8192
(((7000 * 16) / 8192) + 1) * (8192 / 16)
((112000 / 8192) + 1) * 512
(13 + 1) * 512
```

The number of allocated accessors would be 7168 (not 7000).

AESENCRYPT

(Optional) Activates AES encryption for passwords and password phrases.

Important! The AES encryption option is specific to CA Top Secret r14 and later; this option is not backwards compatible. If you attempt to start a single r12 system with an r14 or later security file with AES enabled, CA Top Secret does not initialize.

BLOCKSIZE=nnnn

Overrides the default values for the block size of the security file. The *nnnn* value must be a multiple of 256 and a minimum of 8192.

MAXACIDSIZE=nnn

(Optional) Specifies the maximum allowed ACID size (in kilobytes).

Maximum value: 512

Minimum value: 256

Default: 256

ORGACIDSIZE=nnnn

(Optional) Specifies the maximum allowed department organizational ACID size (in kilobytes).

Important! Use this parameter only if you must support an department organizational ACID size that is greater than the MAXACIDSIZE value. CA Top Secret ignores any ORGACIDSIZE value that is less than the MAXACIDSIZE value.

Maximum value: 1024

Minimum value: 513

Default: None

MLSBLOCKS=nnnn

(Optional) Specifies the number of blocks reserved in the security file to hold the MLS index. This index allows quick access to individual MLS record elements.

If you do not specify this keyword, TSSMAINT calculates that two MLS entries are needed for each ACID that is requested on the ACCESSORS keyword.

Note: For more information about MLS security policy support, see the *CA Top Secret Multilevel Security Planning Guide*.

PIEBLOCKS=nnnn

(Optional) Specifies the number of blocks reserved in the security file to hold the PIE index. This index allows quick access to owners of prefixed resources.

If you do not specify this keyword, TSSMAINT calculates that two PIE entries are needed for each ACID that is requested on the ACCESSORS keyword. If you are defining many ACIDs, this calculation significantly increases the number of defined index blocks. The PIEBLOCKS keyword reduces that value, allowing for a smaller security file. Each owned prefix index entry requires one 35-byte entry in the index.

RESBLOCKS=nnnn

(Optional) Specifies the number of blocks allocated to hold the general resources index. Each owned general resource prefix requires one 16-byte entry in the index; thus, each index entry points to the owner of the general resource entity.

Default: 10

SDTBLOCKS=nnn

(Optional) Specifies the number of blocks for holding definitions for Static Data Table (SDT) records. An SDT record is a special system ACID that stores various user-defined static data definitions.

Note: For more information about SDT record elements, see the *CA Top Secret User Guide*.

Valid numbers: 2 to 256

SCA=msca_name/password

Supplies the name and password of the Master Central Security Administrator (MSCA).

msca_name

Specifies a one- to seven-character name for the MSCA.

password

Specifies a four- to eight-character password assigned to the MSCA. The password expires upon initial signon.

Default: SCA=TSSSEC/TORONTO

VOLUMES=nnnn

Specifies the number of volumes and prefixes defined to CA Top Secret. The value that you enter for *nnnn* determines the amount of security file space allocated to hold volume-related security information.

Default: 1000

The following formula determines the actual number of allocated volumes:

$$(((\# \text{ volumes requested} * 16) / \text{blksize}(\text{quotient only, no remainder})) + 1) * (\text{blksize} / 16))$$

- b. Set the VOLSER JCL parameter with the DASD volume serial identifier for your security file.
- c. Set the CYLS parameter.
- d. Set the SECPRIM ID=PRIMARY parameter to identify the name of your security file.

The ID has a maximum of eight characters. Your entry (or the default, PRIMARY) is placed in the master security file and distinguish the master security file from the backup file. CA Technologies suggests ID=PRIMARY for the master file and ID=BACKUP for the backup file.

- e. Set the VSAMFILE DD statement to refer to the VSAM data set that you [previously created](#) (see page 86).
- f. Edit step 2 of the sample JCL by performing *one* of the following actions:
 - To use the VSAM/r15 data set with a shared security file, set the VSAMAIX DD statement to refer to the alternate index VSAM data set.
 - If the security file is not shared, remove step 2 from the JCL.

The member is customized.

3. Run the TSSMAINS utility job.

When the job finishes running, security file creation is complete.

4. (Optional) Perform the following steps if you are using more than one CPU:
 - a. Place the security file on a shared DASD volume that is accessible to all systems.
 - b. Specify the control option SHRFILE(YES) on each CPU.

This control option setting specifies for files that CA Top Secret uses to be shared among other operating systems, CPUs, or both.

Increase ACID Size

Depending on the security policy implementation and required level of protection, certain ACID records might reach the maximum size, at which point administrators cannot add attributes and properties to the records.

You can increase the maximum size of organizational ACIDs or increase the maximum size of all ACIDs. Increasing the size limit avoids the need to redesign the security implementation.

Note: This change can be implemented one security file at a time, does *not* affect the size of the security file, and does *not* affect system performance.

Follow these steps:

1. Allocate a new security file and include any of the following entries:

`MAXACIDSIZE=nnn`

nnn

Specifies a value between 256 and 512 that allows *all* ACIDs to reach a size of more than 256 KB (up to 512 KB). Existing ACIDs do not automatically increase to the new size. However, any existing ACID that reaches the current limit increases to the new maximum size.

`ORGACIDSIZE=nnnn`

nnnn

Specifies a value between 513 and 1024 that allows department organizational ACIDs to reach a size of more than 512 KB (up to 1024 KB). Existing department organizational ACIDs do not automatically increase to the new size. However, any existing department organizational ACID that reaches the current limit increases to the new maximum size.

Important! Use this parameter only if you must support an department organizational ACID size that is greater than the MAXACIDSIZE value. CA Top Secret ignores any ORGACIDSIZE value that is less than the MAXACIDSIZE value.

The product allocates the file.

2. Issue the following command to back up the security file immediately:

`TSS MODIFY BACKUP`

The product copies the current contents of the primary file into an existing backup file.

3. Run the TSSXTEND utility to copy the current backup security file to the newly allocated file.

The product copies the file. Increased ACID size is now available.

Implementing MLS

If you intend to implement MLS, note the following:

- Allocate new security and backup files with sufficient MLSBLOCKS for your use.
- Copy your existing lower-release security file into the new format.

Create a Backup Security File on DASD (Optional)

If you commented or deleted the BACKUP DD in the TSS started task procedure, skip this procedure.

Follow these steps:

1. Edit the CAKOJCL0 member TSSMAINB:
 - The parameters CYLS and BLOCKS must be identical to those employed by TSSMAINS to create the security file.
 - The backup security file must be the same BLKSIZE as the primary security file.
 - Consider using a VOLSER on a separate channel and string, so if a failure occurs on the security file volume, the backup security file remains available.
 - The SECPARMS contents must remain unchanged from the values used in TSSMAINS.
 - The SECBACK member referenced in the TSSMAINB contains the ID=parameter and the default is ID=BACKUP. You can edit the ID= to contain up to eight characters, but the ID=parameter should clearly indicate that this is the backup security file.
 - For the VSAM file, use IDCAMS to create a separate backup VSAM file. Sample JCL is provided in CAKOJCL0 member VSAMDEF6. Specify the backup VSAM file on the VSAMFILE DD statement.

The member is updated.

2. Run TSSMAINB.

The backup security file is allocated. If the VSAMFILE DD was specified, some header fields are initialized in the VSAM file.

3. Use the built-in automatic backup feature to back up the security file. The backup file should not be shared between CPUs. Place the backup file on a DASD that is *not* the same volume, unit, channel path as the security file.

You have obtained a security file backup.

Important! When a security file is shared by multiple CPUs, only one system should be configured for BACKUP.

(Optional) Define the Mirror Security File (BDAM and VSAM Components)

If you are not sharing the security file on multiple systems, you can maintain a mirror copy of the security file and VSAM file (to use them as backups in a recovery situation). To have these copies available for use, define a mirror security file (including the BDAM and VSAM components).

Important! Mirror files are supported only on systems that do *not* share the security file (SHRFILE(NO) control option setting). In this environment, the VSAM file should not be defined with an alternate index. If your current VSAM file is defined with an alternate index, copy the file to a VSAM file without an alternate index before performing this procedure.

Follow these steps:

1. Use the IDCAMS utility to allocate the VSAM mirror file.
The product provides a VSAMDEFM model in CAI.CAKOJCL0.
2. Edit the sample JCL in CAKOJCL0 member TSSMAINM to meet your site's needs.
3. Run the TSSMAINT utility job to allocate a mirror security file (ensuring that your VSAMFILE DD statement points to the defined VSAM mirror file).

Note: TSSMAINT resides in the CA Top Secret CAKOJCL0 data set.

CA Top Secret allocates the mirror security file.

4. Edit the product started task procedure in SYS1.PROCLIB.

Note: You can use the model that is provided in CAI.CAKOJCL0(TSS).

- a. Specify the BDAM file name on the SECMIRR DD statement.
- b. Specify the VSAM file name on the VSAMIRR DD statement.

The following requirements apply to the BDAM and VSAM components:

- These files must *not* be on the same volume of the primary security file. We recommend placing the files on separate channels and separate strings. This way, any physical failure of these devices leaves the other set of files available when the product is restarted.
- The BDAM mirror data set block size must match the block size of the primary security file (SECFIL) data set.
- The VSAM mirror data set must have a maximum record size that matches or exceeds the size of the primary VSAM data set.
- The space allocation and record count for the mirror BDAM data set must match the allocation of the primary BDAM data set.
- The space allocation and record count for the mirror VSAM data set must match the allocation of the primary VSAM data set.

Your new file is now in place. When you activate mirroring, you can begin using the mirror security file.

Create the Recovery File (Optional)

If you commented or deleted the RECFIL DD in the TSS started task procedure, skip this procedure.

The recovery feature stores forward recovery information. The recovery file records changes made to the security file. This file is a *wraparound* file. When the file is full, recording continues at the beginning of the file, overlaying existing data. The default size recovery file can hold approximately 2,000 changes before a wraparound occurs.

The recovery file does not support DFSMS Extended Sequential data sets (multi-volume data sets).

Do not allocate the recovery file on the same volume as the security file in case of loss due to hardware malfunction.

Follow these steps:

1. Edit the TSSMAINT utility to conform to your site's standards.

Note: TSSMAINT resides in the CA Top Secret CAKOJCL0 data set.

The utility is updated.

2. Edit the recovery file parameters one per line, starting in column 1:

CREATE RECOVERY

Requests recovery file initialization.

BLOCKS=???

Specifies the number of blocks to be used for the recovery file. A large recovery file delays initialization of the CA Top Secret address space every time it is started. The size of the recovery file depends on the interval between security file backups. Make the file large enough to record two to three days of changes for every day in the security file backup period. For example, if the security file is backed up at the end of each day, the recovery file should be large enough to accommodate at least two days of changes.

Default: 250

Minimum: 250

Maximum: N/A

The recovery parameters include your site-specific values.

3. Replace lowercase type in the JCL with the appropriate parameters for your site.

Note: The file block size should provide efficient utilization of the track capacity for the device the file resides on. An exact value is not necessary as TSSMAINT rounds the block size down to a multiple of its logical record length. The actual block size may be less than specified on the JCL, but it should be approximate.

The recovery parameters include your site-specific values.

Multiple CPUs

The recovery file may be shared between systems. However, identical sharing must exist for *both* the recovery and security files. Systems that share a recovery file must use the same security file to ensure proper serialization and management of the shared recovery file.

Create an Audit/Tracking File (Optional)

The audit/tracking file is an online file that records security incidents in place of, or in addition to, SMF. The audit/tracking file provides administrators and auditors with a current, online record of system security activity from all CPUs.

We recommend that you use the audit/tracking file instead of SMF because of the following factors:

- SMF recording and reporting can be cumbersome.
- SMF does not provide online display capabilities.
- SMF must be merged from many CPUs for complete reports.

The audit/tracking file is a wraparound file; when the file is full, recording continues at the beginning of the file, overlaying existing data. Optionally, you may use two audit/tracking files. When the first audit/tracking file is full, CA Top Secret automatically switches to the alternate audit/tracking file. When the alternate audit/tracking file is full, recording continues at the beginning of the first audit/tracking file, overlaying existing data.

Note the following audit/tracking file behaviors:

- Cannot span more than one volume
- Does not support DFSMS Extended Sequential data sets (multi volume data sets)

Follow these steps:

1. Edit CAKOJCL0 member TSSMAINA to conform to your site's standards.
The member includes your site-specific values.
2. Edit the JCL parameters one per line, starting in column 1:

CREATE AUDIT

Requests audit/tracking file initialization.

BLOCKS=????

Specifies the number of blocks to be used for the audit/tracking file.

BLOCKSIZE=?????

Specifies the blocksize for the audit/tracking file. The BLOCKSIZE input parameter must be identical to the BLKSIZE JCL parameter of CAKOJCL0(TSSMAINA) when submitted. If you use both a primary and alternate audit/tracking file, the BLOCKSIZE must be identical in both files.

General Value: A multiple of 256 between 512 and 32512

3390 DASD Value: A multiple of 256 between 512 and 27648

ID=AUDIT

Distinguishes one audit/tracking file from the other when using alternating audit/tracking files. You can only specify one of the following values. No other values will be accepted. For the:

- First audit/tracking file use: ID=AUDIT.
- Alternate audit/tracking file use: ID=AUDIT2.

The JCL parameters are edited.

3. (Optional) If you are using an alternate audit/tracking file, code a DDNAME of AUDIT2 in the CA Top Secret STC procedure.

The alternate audit/tracking file is updated.

More Information:

[CA Top Secret Health Checks](#) (see page 121)

Create Alternate Audit/Tracking File (Optional)

CA Top Secret supports the use of an alternate audit/tracking file. When the primary file is full, CA Top Secret writes to the alternate file.

Follow these steps:

1. Edit CAKOJCL0 member TSSMAINA to conform to your site's standards.
2. Edit the DD and ID= statements so that the dataset suffix is AUDIT2, and ID=AUDIT2.
3. Verify the following:
 - The BLOCKSIZE in your JCL is identical to the BLOCKSIZE of your ID=AUDIT file
 - The TSSMAINA JCL parameter BLKSIZE is identical with the BLOCKSIZE in your TSSMAINT input parameter file
4. Submit the job.

Create a CPF Recovery File

The CPF recovery file is used by CPF to save transmitted commands until responses to those commands are received from remote machines.

If you intend to use CPF, format the CPF recovery file through TSSMAINT. The size of each record in the CPF recovery file is 4500 bytes. The block size should be a multiple of this value. One record is written to the CPF recovery file for each node to which the command is sent. The space is reused when a response to the command is received. The CPF recovery file does not support DFSMS Extended Sequential data sets (multi volume data sets).

Important! The CPF recovery file *must never* be shared across multiple systems.

Follow these steps:

1. Edit TSSMAINC to your site's standards.
2. Submit TSSMAINC.

Note: Running TSSMAINC causes an SD37 ABEND. This is normal.

A DD statement must be inserted into the CA Top Secret TSS JCL to define the CPF recovery file. For example:

```
//CPFFILE DD DSN=CAI.tss12.CPFRVRY,DISP=SHR
```

If the CPF recovery file is not defined, command routing through CPF can still occur, but there will be no retransmission of unresponded commands.

If the recovery file becomes temporarily filled, the TSS9803W message is written to the job LOG each time CPF needs to write a message to the file. The CPF operation continues but the command cannot be recovered.

Create the RCACHE VSAM Cluster (Optional)

To implement R_cacheserv hardening for USS, allocate and format a VSAM KSDS. This protects your cache areas from other users. If you do not require R_cacheserv hardening, modify your PARMFILE to RCACHE(NO).

Follow these steps:

1. Edit the CAKOJCL0(INITCSRV) member:
 - Customize the JOBCARD to your site's standards.
 - Change the prefix CAI to your site standards for TSS data files.
 - Change the cluster name to meet site standards (if needed).
2. Submit the job.
3. Uncomment the RCACHE DD statement on the TSS procedure, and edit the dataset name to conform with the name used in INITCSRV.
4. Modify your PARMFILE to:
 - Set RCACHE(YES)
 - Secure up to 150 RCQNAME values

CICS Installation Considerations

For information about running CA Top Secret with CICS, see the *Implementation: CICS Guide*.

Define the Security Console (Optional)

The security console should be a separate operating system console isolated from the rest of your operations staff. It is used solely by the Master Central Security Administrator to control and monitor the security environment if TSSTRACK is used for monitoring. The security console must be defined with ROUTE CODE 9.

To define the security console, place the following command into member TSSAUTO0:

```
VARY cuu,CONSOLE,ROUT=9
```

cuu

Specifies the console address.

Note: A security console is not mandatory. The online tracking feature, TSSTRACK, for the Master Central Security Administrator and Auditor can be used to monitor violations in a real-time manner. For information, see the *Report and Tracking Guide*.

Set Up Backup, Restore, and Recovery Procedures

Important! Set up these backup, restore, and recovery procedures during the installation.

The CA Top Secret distribution tape contains backup, restore, and security file recovery JCL procedures. The JCL procedures described in this step must be tailored to conform to your site's requirements and placed into your PROCLIB so that they are available when they are needed.

TSSXTEND must be used when changing device types. Copy the backup file to make sure no changes are being made.

Automatic Backup to DASD

The security file is a critical resource and should be integrated into your standard backup process. The loss of the security file database necessitates running your system without security until the security file is rebuilt or recovered.

Important! To minimize the possibility of a loss of the database, back up the security file daily.

To ensure that a daily backup is performed, use the CA Top Secret automatic backup feature. Automatic backup requires:

- The presence of the recovery file and backup security file on DASD
- The control option settings, RECOVER(ON) and BACKUP(*hhmm*) where *hhmm* represents the time the backup will occur

Set Up Tape Backup Procedures

All CA Top Secret files must be copied bit-by-bit. Because some standard backup and restore facilities, like DMS, do not copy files bit-by-bit, they cannot be used to back up CA Top Secret files to tape.

Member TSSBCKUP or SMSBCKUP can be used to back up the:

- Security file (not recommended)
- Recovery file
- The entire audit/tracking file

Note: The audit/tracking file can be backed up in its entirety or it can be archived periodically using the TSSARCHI JCL procedure.

To perform the backup, member TSSBCKUP uses the IEHMOVE utility and member SMSBCKUP uses the DFDSS utility. Sites with an SMS environment should use the DFDSS utility or an equivalent utility (for example, CA ASM2 Backup and Restore, FDR) which supports the SMS environment.

Note: If the backup created by job SMSBCKUP is used for disaster recovery, keep in mind that DFDSS does not restore a data set marked as RACF-protected on a system with no security product installed. You can use TSSPROT to turn off the RACF-protect bit on the security file. However, you only need to use TSSPROT once after the file has been initialized using TSSMAINT. Initializing the files turns on the protect bit.

TSSBCKUP or SMSBCKUP should be set up to back up the security file. If it becomes necessary to back up other CA Top Secret files, specify the correct file when executing the task.

Set Up Restore Procedures

Only the CA Top Secret security and recovery files can be restored. CA Top Secret abends if an old copy of the audit/tracking file is restored. If damage to the audit/tracking file is encountered, a new file must be initialized using the TSSMAINT utility.

Restore JCL

The following JCL procedures restore the security and recovery files from tape to DASD:

SMSRESTR

Restores the security or recovery file to DASD over the old file.

TSSRESTN, SMSRESTN

For use with the security file only. Allocates space on DASD, then restores the security file to DASD in the newly allocated space.

TSSRESTN uses the IEHMOVE utility. SMSRESTR and SMSRESTN use the DFDSS utility. Sites with an SMS environment should use the DFDSS utility or an equivalent utility (for example, CA ASM2 Backup and Restore, FDR) which supports the SMS environment.

SMSRESTR should be set up to restore the security file. If it becomes necessary to restore the recovery file, specify the correct file when executing the task.

Set Up Recovery Procedures

The TSSRECV utility provides recovery-processing services for the security file. TSSRECV uses the records kept by the recovery file to recover all changes made to the security file. For TSSRECV to be effective, the recovery control option, RECOVER(ON), must have been in effect. RECOVER(ON) should be specified during installation. It can, however, be specified by an operator O/S MODIFY or TSS MODIFY command.

TSSRECV recovers the security file in two phases: First, TSS commands are generated from the recovery file, then BATCH TMP executes the TSS commands.

TSSRECVR requires that two JCL procedures are setup:

TSSRCVR1

Retrieves changes from the recovery file that occurred after the time and date specified in the EXEC PARM. You must add DATE to the EXEC PARM field before executing TSSRCVR1. The optional TIME parameter can also be added. The correct format is as follows:

```
EXEC PGM=TSSRECVR,PARM=' TIME(hhmm),DATE(yyddd) '
```

or

```
EXEC PGM=TSSRECVR,PARM=' TIME(hhmm),DATE(-nn) '
```

hhmm

Specifies the hour and minute for selecting recovery records. This should be the time of the last security file backup.

yyddd

Specifies the earliest date (in Julian format) for selecting recovery records.

-nn

Is the number of previous days for which you want to retrieve changes from the recovery file.

To use the contents of the entire recovery file, specify TIME(0000),DATE(00000).

TSSRCVR2

Applies the changes to the backup security file.

Note: During installation, the TSSRECVR JCL, TSSRCVR1 and TSSRCVR2, should be setup.

CA Top Secret ADMIN Menus

The administration panels are driven by the CA C Runtime component of CA Common Services.

If you intend to use the CA Top Secret panel system for security administration, modify your ISPF main menu (ISR@PRIM) using the sample menu in CAI.CAKOPNLO. For information, see the *Implementation: Other Interfaces Guide*.

Set Up Installation Exits

Installation exits allow you to bypass, replace, or enhance normal security validation.

Follow these steps:

1. Assemble and link the current version of TSSINSTX into a linklist library. It is the responsibility of the site programmer to place the customized installation code in the appropriate TSSINSTX exit routine.
2. (Optional) If you are using TSSINSTX from a previous release of CA Top Secret, merge your installation code into the current version of TSSINSTX and reassemble the module.

Note: For information about the installation exits and the TSSINSTX module, see the *User Guide*.

Customize Facility Security

If you will be using any of the following, see the following implementation guides for additional required steps:

- CA Top Secret to secure resources for CICS, IMS, CA IDMS or CA Roscoe.
- CA Earl reporting options to run security reports.
- SAF SECTRACE to perform diagnostic traces.

For information about CA Earl reports, see the *Report and Tracking Guide*. For information about SAF SECTRACE, see the *Troubleshooting Guide*.

CA Top Secret as a Subsystem

CA Top Secret lets you start CA Top Secret early in the IPL process as a subsystem using the CAISEC00 parmlib member. This functionality provides an alternative to starting CA Top Secret with SUB=MSTR from the command table SYS1.PARMLIB(COMMNDxx).

When you starting CA Top Secret through CAISEC00, that several members can start the same task with different operands by using the MVS &SYSCONE symbolic substitution.

Note: For CA Top Secret release 15.0, if the TSS procname in SYS1.PROCLIB is TSS, CA Top Secret starts as SUB=MSTR. If you do not want CA Top Secret to start as SUB=MSTR, change the procname to something other than TSS (for example, to TSS15).

How to Initialize CA Top Secret as a Subsystem

This section explains how to use CAISEC00 to start CA Top Secret and CA SAF SECTRACE subsystems automatically. You can initialize CA Top Secret from CAISEC00 or from the command table SYS1.PARMLIB(COMMNDxx).

Note: For first-time installations of CA Top Secret, put a START TSS entry in SYS1.PARMLIB(COMMNDxx) or a TSS(xx START) entry in CAISEC00; otherwise, you must start CA Top Secret manually from the operator console.

1. Create a member called CAISEC00 for your started tasks. In CAISEC00, list each subsystem name, whether it should start automatically, and which members of SYS1.PARMLIB contain additional operands for the START command. For example:

```
EDIT ---- SYS1.PARMLIB(CAISEC00) - 01.01 ----- COLUMNS 001 072 COMMAND
====> SCROLL ====> CSR
***** TOP OF DATA ***** 00000001 TSS(xx
START)
00000003 TRCE(xx START)
00000004 PROMPT
***** BOTTOM OF DATA *****
```

Note: To start some, but not all, of the subsystems listed in the CAISEC00 member, place an asterisk (*) to the left of the name of each subsystem that you do not want to start. Notice that the entry number matches the SYS1.PARMLIB member. For example, TSS(01 START) matches member CAITSS01.

2. Specify the following keyword in the CAISEC00 member. To do so, selecting the CAISECxx suffix by responding to the prompt message:

PROMPT

Indicates that the operator console should be prompted for specification of the CAISEC initialization parameters. During CA SAF initialization, a WTOR message CAS2070I is issued to allow the operator to specify the CA SAF initialization parameters.

3. Specify that CA SAF is to use the CAITSSxx parmlib member by using one of the following options:

```
TSS(xx)
TSS(xx START)
TSS(xx NOSTART)
```


4. Specify the CAISECxx parmlib member suffix by using one of the following options:

SEC=xx or SEC(xx)

This step lets a site maintain multiple CAISECxx parmlib members. CAISEC00 is the initial parmlib member processed during CA SAF startup processing. Within the CAISEC00 member, you can specify any of the valid initialization parameters, including SEC=xx to indicate that an alternate parmlib member should be processed. The last value processed for any of the valid initialization keywords is the value selected for processing. To avoid initialization processing loops, a CAISEC member suffix can be specified only once for processing.

Note the following behaviors:

- To use the CAISEC00 parmlib member as it currently exists, use the U option to cause CA SAF. This value is the default, and it lets you continue processing.
- The U option is available as a response to the prompt at the console only; you cannot use it as a keyword value in CAISEC00. You are unable to specify any other parameters after you specify U.
- If you specify a single parameter or multiple parameters, such as TSS(xx), these replace their counterparts in CAISEC00 or any other CAISECxx member that you specify with the SEC(xx) parameter. All other parameters remain the same.

Note: To use one or more of these options automatically at startup, put them in CAISEC00 and remove the PROMPT keyword.

Using Symbolic Substitution

CA Top Secret supports MVS symbolic substitution in the CAISECxx parmlib member, which you can use to help automate the startup process. For example, use of the &SYSCONE symbolic, which represents the last two characters of the MVS system ID, can allow different startup options to be executed depending on which z/OS system is performing the startup.

The following table demonstrates the following scenario:

- When z/OS system SY01 starts, the &SYSCONE values are set to 01. Members CAISEC00 and CAISEC01 are processed, and startup options from CAITRC00 and CAITSS01 are used.
- When z/OS system SY99 starts, the &SYSCONE values are set to 99. Members CAISEC00 and CAISEC99 are processed. Startup options from CAITRC00 are used, and the operator is prompted for additional input.

Parmlib Member	Parameters
CAISEC00	TRCE(00 NOSTART) SEC(&SYSCONE)
CAISEC01	TSS(&SYSCONE START)
CAISEC99	PROMPT

Specifying Startup Options in CAITSS

The CAITSSxx parmlib member that you specify at the CAISEC prompt contains parameters that apply to that CA Top Secret system. Note the following rules:

- Specify one keyword per line.
- The following control options are allowed and no abbreviations are allowed:

CMDNUM

Determines the number of command processors initiated at startup of the CA Top Secret address space.

EXPDAYS

Sets how many additional days after a FOR or UNTIL clause has expired that an ADD or PERMIT is kept on the security file before deletion.

OPTIONS

Specifies general purpose configuration options. This definition applies to options numbered above 32. Options 1 to 32 replace optional APARs in releases of CA Top Secret prior to r5.1.

PWVERIFY

Forces users to verify their old password before changing to a new password.

SUBSYS

Modifies the TSS subsystem name that defaults to TSS.

- MVS symbolic substitution is supported in the CAITSSxx parmlib member.
- The SUBSYS keyword lets you modify the CA Top Secret subsystem name that defaults to CA Top Secret. The modified subsystem name must be in the format 'TSxx'.

Important! The CA TSS procedure has to match the subsystem name and must be in the system procedure library (SYS1.PROCLIB).

Note: When you stop and start CA Top Secret during an IPL, it uses the options specified on the START command rather than those specified in the CAITSSxx member. If the CAITSSxx member does not exist at IPL time, CA TSS startup parameters are not passed on the automatic start of CA Top Secret. Additionally, no messages are issued.

CAITSSxx Member

The following example shows a CAITSSxx member with specified parameters:

```
EDIT ---- SYS1.PARMLIB(CAITSS01) - 01.01 ----- COLUMNS 001 072 COMMAND ==>
SCROLL ==> CSR

***** TOP OF DATA *****
00000001 CMDNUM(4)
00000002 EXPDAYS(2)
00000003 SUBSYS(TSS5)
*****BOTTOM OF DATA *****
```

How to Configure Without CA CSM

The topics in this section describe the manual tasks you perform if you are not configuring your product using CA CSM.

You must perform the following configuration tasks manually, regardless of whether you are using CA CSM to perform product configuration:

- [Assign your key to the library](#) (see page 74).
- [Authorize the product libraries](#) (see page 75).
- [Authorize TSS commands](#) (see page 75).
- [Set up SAF SECTRACE](#) (see page 76).
- Install ENF DCM.
- [Customize the started task procedure](#) (see page 78).
- [Update the TSSB backup started task](#) (see page 78).
- [Edit commands to initiate and follow CA Top Secret](#) (see page 79).
- [Create the parameter file](#) (see page 81).
- [Upgrade the existing security file](#) (see page 83) or [create a new file](#) (see page 84).
- [Create a backup security file](#) (see page 92).
- [Create a recovery file](#) (see page 94).
- [Create an audit/tracking file](#) (see page 95) and an [alternate audit/tracking file](#) (see page 97).
- [Create a CPF recovery file](#) (see page 97).
- [Create the RCACHE VSAM cluster](#) (see page 98).
- [Define the security console](#) (see page 99).

- [Set up backup, restore, and recovery procedures](#) (see page 99).
- [Modify your ISPF main menu](#) (see page 102).
- [Set up installation exits](#) (see page 103).
- [Customize your facility security](#) (see page 103).
- [Initialize CA Top Secret as a subsystem](#) (see page 103).

Startup and Shutdown Sequence

Regardless of how CA Top Secret is started, all JES devices and initiators should come up drained. They may be started after CA Top Secret initialization with TSSCMDxx.

CA Top Secret should be the last address space brought down at the end of the day.

Start CA Top Secret

CA Top Secret can be started:

- As a subsystem before JES. Specify SUB=MSTR on the O/S START command. TYPE=2 (or JES2) and LEVEL=SP n.n.n must be specified in the JES control option. Failure to do so displays the message TSS9112E-UNABLE TO DETERMINE JES LEVEL.
- During a system IPL after JES initialization. Start CA Top Secret *before* all of the CA Common Services except CAIRIM. CAIRIM must initialize before CA Top Secret.

If the TSS address space is up before JES, the \$\$\$LOG\$\$ spool file is automatically allocated when JES starts. For CPF nodes that require sysout support, the nodes will need to be defined in the NDT and refreshed after JES is up. Spool files for those nodes will then be allocated without restarting the TSS address space. Because of this change, TSS must shut down before JES.

Note: If a subsystem with the same name as a started task exists, the MSTR subsystem is the default for the started task. If no MSTR subsystem exists, the primary JES subsystem is used. In CA Top Secret r15, we established a subsystem with the name TSS. Therefore, if the procname that starts CA Top Secret is TSS, it will start under the master subsystem. To avoid the procname running under MSTR, change the name of the proc.

Activate CA Top Secret

After CA Top Secret has been installed on your system, you can activate it.

Follow these steps:

1. Before starting CA Top Secret for the first time, complete an IPL with the CLPA parameter.
2. If starting CA Top Secret after JES2, enter:

```
S TSS, , ,MODE(DORM)
```

If starting CA Top Secret before JES2, enter:

```
S TSS, , ,MODE(DORMANT) ,SUB=MSTR
```

The START TSS command should be placed in the COMMNDxx member of SYS1.PARMLIB.
3. Enter the following:

```
S TSS
```

A message appears indicating that CA Top Secret is implemented.
4. CA Top Secret should initially be brought up in DORMANT mode. In this mode, you lose password protection for password protected data sets.

To maintain password protection, permit each password protected data set for all facilities and accesses with ACTION(PASSWORD,FAIL). For example:

```
TSS PERMIT(ALL) DSNAME('password.protected.dsname')  
ACCESS(ALL)  
ACTION(PASSWORD,FAIL)
```

Verifying Installation (Optional)

After CA Top Secret has started, log on or sign onto the system.

Note: If you are using TSO, the MSCA must have a valid entry in SYS1.UADS.

CA Top Secret requires a new password. If you are not prompted for a new password, be certain that you have used the ACID that was specified in the TSSMAINT security file creation JCL, for the SCA= parameter.

Restarting CA Top Secret

To restart CA Top Secret after it has been shut down, you can do the following:

- re-IPL
- Enter S TSS. Use this option after a temporary shutdown.
- Enter S TSS,,,REINIT. Only use this method after a temporary shutdown for maintenance to CA Top Secret.

To start CA Top Secret after an inadvertent end of day shutdown

1. Enter the command:

S TSS

Every parameter file option fails. Ignore the resulting in error messages.

2. Enter the commands:

F TSS,RESETEOD

P TSS

S TSS

Notes:

- RESETEOD is a password-protected control option, available only through a modify command, to restart CA Top Secret after an end-of-day shutdown
- When using the START command to start CA Top Secret before JES, add the SUB=MSTR option

CA Top Secret Shutdown

End-of-day shutdown prohibits new initiations in all modes other than DORMANT. New users cannot sign onto any facility and new batch jobs will not execute.

Note the following shutdown behaviors:

- Provided the operator has the authority, an end-of-day shutdown can be reset using the RESETEOD control option.
- To prevent unauthorized mid-day shutdowns, specification of the MSCA's previous password or an ACID/password that has the CONSOLE attribute is required.
- If security is shut down from any mode other than DORMANT, the DOWN options become active.

Follow these steps:

1. Enter the command:

P TSS

CA Top Secret displays the following messages:

```
TSS9072I  ** SELECT TYPE OF SHUTDOWN ** <I> TO IGNORE
TSS9072I  <Z>  END OF DAY;  RE-IPL WILL BE REQUIRED
TSS9072A  <T>  TEMPORARY;   MAY IMPACT THROUGHPUT
```

2. To run:

- a. A normal end-of-day shutdown, enter:

Z

- b. A mid-day shutdown, enter:

T

Appendix A: TSSXTEND - Extend the Security File

This section contains the following topics:

[How to Change the Security File Size or Encryption Key](#) (see page 113)

[TSSXTEND Considerations](#) (see page 115)

[Convert SDT Records to VSAM](#) (see page 116)

[Convert Triple-DES Encryption to AES Encryption](#) (see page 117)

[Copy the BDAM and VSAM Files](#) (see page 117)

[Copy the VSAM File](#) (see page 118)

[Run the TSSXTEND Utility](#) (see page 118)

[Messages and Codes](#) (see page 119)

How to Change the Security File Size or Encryption Key

The TSSXTEND utility lets an MSCA or an authorized user enlarge or reduce the size of the security file or change the security encryption key. TSSXTEND is used in combination with the TSSMAINT utility.

Important! Change your encryption key *only* if you suspect a violation of the integrity of the key. To change the key, run TSSKEY by using the APPLY CRYPTKY control statement, and supply the new key.

A user needs *one* of the following authorizations to run TSSXTEND:

- USE access to the TSSUTILITY.TSSXTEND entity in the CASECAUT resource class for any function except ZAP.

An administrator can grant this level of access by issuing the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSXTEND) ACCESS(USE)
```

- UPDATE access to TSSUTILITY.TSSXTEND entity in the CASECAUT resource class for using the ZAP function.

An administrator can grant this level of access by issuing the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSXTEND) ACCESS(UPDATE)
```

To change the security file size or encryption key:

1. Determine the level of security file usage by issuing the TSS MODIFY(STATUS) command and review security file (NNN%) in message TSS9661I.

NNN%

Represents the percentage of the security file used.

2. Use the TSSMAINT utility to create a new security file.
3. Issue a TSS MODIFY(BACKUP) command to copy the current security file to the current backup security file.
4. Run the TSSXTEND utility to copy the backup security file to a new security file.

TSSXTEND Considerations

To ease the transition from the existing backup file to the new security file, consider the following points:

- **Renaming new files**—When the SECFILE or BACKUP file needs to be copied, the new file has a different DSNAME than the old file. If the old files were created under an earlier release of CA Top Secret, you may need to alter the parameters of TSSMAIND, TSSMAINS, and TSSMAINB to correspond with the new release values resulting from TSSFAR in the new release running against the old file.
 - Run TSSFAR with STEPLIB against the old security file. For details on using SFSTATS report to set ACCESSORS and VOLUMES, see the *Troubleshooting Guide*.
 - Run TSSMAIND to determine the correct number of blocks.
 - Run VSAMDEF3 to allocate a new VSAM file. Run STEP 2 only if the security file is shared.
 - Run TSSMAINS to correctly allocate the new security file. If the security file is shared, run STEP 2 of TSSMAINS.
 - Run TSSXTEND to COPY SECURITY.

- **Creating a new backup security file**—After you have successfully copied the old security file into the newly created security file, format a new backup file capable of accommodating the new security file.

After the security file has been correctly allocated and copied, use TSSMAINB to allocate the backup with identical parameters (except ID=BACKUP).

To assure that the backup file is adequate run TSSXTEND to COPY SECURITY from the new security file to the new backup.

- **Changing the PROC statements**—After the new security and backup files are created, you must change the PROC statements in your JCL procedures (namely, TSS STC, TSSB STC, and backup and recovery procedures) to point to the new files.
- **Changing the encryption key**—You can use TSSXTEND to change your company's security file encryption key. Ordinarily, your company's encryption key should never be changed. However, if you suspect that the integrity of your key has been violated, you can change to a new key. If you change the key, the encryption must be also changed on the CA Top Secret load library. Run member TSSKEY, found in the CAKOJCL0 data set using the APPLY CRYPTKY control statement, and supply the new key so that CA Top Secret can operate correctly.

Important! The encryption key must be the same on the security file and the CA Top Secret load library.

- **Deleting old files**—Do not delete the old security file and backup files until you confirm that the file enlargement/replacement was successful. Provided that you have supplied the names of the new files in all the necessary JCL PROCs, the new and old files can reside on disk without causing CA Top Secret to malfunction.

- **IPL the security file**—When any change is made to the security file using a TSSMAINT/TSSXTEND combination an IPL is required.

Convert SDT Records to VSAM

CA Top Secret will maintain digital certificate, keyring, and KERBSEGM records in a VSAM data set. To improve performance and increase the amount of records that can be stored, convert the records to VSAM.

The VSAM file can be created in the VSAM r12 and later file structure.

Follow these steps:

1. Run TSSFAR to obtain the security file statistics. This data is used to help specify the number of ACIDs, volume, RES, PIE and SDT blocks to allocate in the new BDAM SECFILE.
2. Run TSSMAIND to determine the number of blocks that should be specified in TSSMAINS.
3. Run VSAMDEF3 to allocate the new VSAM/r15 file. Run STEP 2 only if the security file is shared.
4. Edit TSSMAINS:
 - a. Change //VSAMFILE DD to specify the output VSAM data set.
 - b. For the VSAM file, if the security is shared, change //VSAMAIX DD statements in STEP 2 to specify the output VSAM alternate index.
5. Run TSSMAINS. Run STEP 2 only if the security file is shared.

The BDAM file is allocated and the VSAM header record is written.
6. Edit TSSXTEND. Change //SECNVSM DD to specify the output VSAM data set.
7. Run TSSXTEND.
 - TSSXTEND verifies that the timestamps in the new BDAM and new VSAM match or the job fails.
 - TSSXTEND moves selected records from the SDT to the VSAM file.

Note: TSSMAINT allocates the BDAM file and puts a header record into the VSAM file. The BDAM header and VSAM headers have identical time stamps.

More Information

[Create the VSAM File](#) (see page 86)

Convert Triple-DES Encryption to AES Encryption

To convert a security file from Triple-DES encryption to AES encryption:

- Run TSSMAINT to initialize a new security file and to specify the AESENCRYPT option.
- Run TSSXTEND to copy the old security file to the new security file.

Note: AES encryption is a non-shared environment option.

Copy the BDAM and VSAM Files

Use this procedure to copy a security file converted to use VSAM.

Follow these steps:

1. Run VSAMDEF3 to allocate the new VSAM file. Run STEP 2 only if the security file is shared.

IDCAMS creates a new output VSAM file.

2. Edit TSSMAINS by completing the following steps:
 - a. Change //VSAMFILE DD to specify the output VSAM data set.
 - b. For VSAM, if the security is shared change //VSAMAIX DD statements in STEP 2 to specify the output VSAM alternate index.
3. Run TSSMAINS.

Important! Do *not* run STEP 2 if the security file is not shared.

The BDAM file is allocated and the VSAM header is written.

4. Edit TSSXTEND by completing the following steps:
 - a. Change //SECNVSM DD to specify the new VSAM data set.
 - b. Change //SECOVSM DD to specify the old VSAM backup data set.
5. Run TSSXTEND.

The TSSXTEND job:

- Verifies that the timestamp in the new BDAM and new VSAM match
- Verifies that the timestamp in the old BDAM and old VSAM match
- Links TSSVBKUP to copy old VSAM to new VSAM
- Rewrites the VSAM header with the correct new timestamp
- Searches the SDT for records to go to VSAM

Note: TSSMAINT allocates the BDAM file and puts a header record into the VSAM file.

Copy the VSAM File

Use this procedure to copy the VSAM file only.

Note: IDCAMS REPRO copies the old header to the new file so the time stamp that matches the BDAM header is on the file. The copied VSAM file can be used with a BDAM security file that has a matching time stamp only.

Follow these steps:

1. Edit VSAMDEF4 to specify a data set name and volume.
The file includes your site-specific values.
2. Run VSAMDEF4.
The base cluster is copied.
3. (Optional) If the security file is shared, complete the following steps:
 - a. Edit VSAMDEF5 to specify a data set name and volume.
 - b. Run VSAMDEF5.
The new alternate index is built.

Run the TSSXTEND Utility

To run TSSXTEND, submit the following JCL to copy the contents of the old backup security file into the new security file:

```
//jobname JOB USER=msca only
//EXTEND EXEC PGM=TSSXTEND
//MAINTOUT DD SYSOUT=A
//SECFOLD DD DSN=name.of.backup.security.file,DISP=SHR
//SECFNEW DD DSN=name.of.new.security.file,DISP=SHR
//*SECNVSM DD DSN=name.of.vsamfile,DISP=SHR for the output (new) VSAM dataset
//*SECOVSM DD DSN=name.of.vsambackupfile,DISP=SHR for the incoming(old)VSAM backup file
//MAINTIN DD *
COPY SECURITY
OLDKEY=???????????????? ENCRYPTION KEY OF OLD FILE
NEWKEY=???????????????? ENCRYPTION KEY OF NEW FILE
NEWPWBLOCK
/*
```

Note: CA Top Secret r15 provides mixed-case password support by default when you run the TSSMAINT utility to initialize the security file. Therefore, you do not need to use the NEWPWBLOCK keyword when running TSSXTEND with an r15-formatted security file.

The OLDKEY and NEWKEY fields must be a 16-character hexadecimal number. Comments cannot be added to these fields.

Important! Safeguard your key.

When you submit the JCL, the product executes the utility and indicates that the operation was successful.

Note: If the TSSXTEND utility does not execute successfully, use TSSMAINT to format the new security file again. For information about TSSXTEND abend codes, see the *CA Top Secret Message Reference Guide*.

Messages and Codes

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

Note: If the TSSEXTEND utility does not complete successfully, format the new security file again using TSSMAINT.

Appendix B: CA Top Secret Health Checks

This appendix describes health checks for CA Top Secret.

TOP_SECRET_CHK_ATF_SECFILE

Description

Verifies there is no conflict with the placement of the Audit Tracking File and the Security File.

Best Practice

We recommend that you allocate the CA Top Secret Security File on a different DASD volume as the CA Top Secret Audit Tracking File. Performance may degrade as a result of improper placement of these two files.

Reference

For details on how to manage these files, see the *Installation Guide*.

TOP_SECRET_CACHE_STATUS

Description

Verifies that the CA Top Secret CACHE and SECCACHE features are enabled.

Best Practice

We recommend that you enable both of these control options to achieve the best possible performance of the product. The CACHE control option provides an area of memory for CA Top Secret to place frequently used items from the security file. Provision for sufficient CACHE reduces I/O against the security file and increases system performance. The SECCACHE control option provides a cache for CA Top Secret to place security records that reflect the status of a user following a RACROUTE VERIFY request.

Reference

For details to enable these options, see the *Control Options Guide*.

Appendix C: OPMAT Member Locations

This section contains the following topics:

[About OPMAT Member Locations](#) (see page 123)

[SOURCE Library](#) (see page 124)

[CLIST Library](#) (see page 125)

[MACRO Library](#) (see page 126)

[ISPF PROFILE Library](#) (see page 126)

About OPMAT Member Locations

In r14 and later, the CA Top Secret r12 OPMAT data set is no longer included on the installation cart or ESD. Most of the files delivered in OPMAT (at r12) are now installed across various SMP/E supported libraries included with the base CA Top Secret r14 and later installation.

The following sections list CA Top Secret r14 and later library locations for all supported CA Top Secret r12 OPMAT members.

SOURCE Library

This section lists the OPMAT members moved to the SOURCE library.

DSN=&CAI..CAKOSRC0 - SOURCE LIBRARY

AIPGMASM

AIPGMRES

AIPGMSUB

DFSMO1

EXAAICP1

EXAIBA1

EXAIBA2

EXAICA1

EXAICA2

EXAICA3

EXAICC1

EXAIIA1

EXAIIP1

TSSCMMND

TSSCPLC

TSSINSTX

TSSINST1

TSSPGM01

TSSPGM02

TSSCPLA

TSSCPLP

TSSCPLCC

TSSAICC1

TSSAICC2

TSSAICC3

TSSAICC4

SAFHFUSR

S231ASSM

CLIST Library

This section lists the OPMAT members moved to the CLIST library.

DSN=&CAI..CAKOCLS0 - CLIST LIBRARY

BPXWIRAC

EXAICP1

TSSBRWZ

TSSTRACK

TSS2NT

TSS2UNIX

WHOOWNRX

MACRO Library

This section lists the OPMAT members moved to the MACRO library.

DSN=&CAI..CAKOMAC0 - MACRO LIBRARY

\$\$CPFTGT

#AFLAGS

#DFLAGS

#FACMATX

#FEEDBCK

#FLOG

#INSTXPL

#RECOVER

#RFLAGS

#RXTRESP

#SMF80

CFILEREC

EARLOPT

ENFPARM

ENFP0002

ENFP0017

TSSSMFOX

ISPF PROFILE Library

This section lists the OPMAT member moved to the ISPF PROFILE library:

CAKOPROF

Appendix D: TSSXVSDT Digital Certificate Backout

This section contains the following topics:

[About TSSXVSDT](#) (see page 127)

[VSAM Digital Certificate Backout](#) (see page 127)

About TSSXVSDT

TSSXVSDT is a batch utility that assists in backing out of the VSAM digital certificate feature. Due to the VSAM requirement for r15, if digital certificates or keyrings must be backed out from the VSAM file, steps 15-22 of the [VSAM Digital Certificate Backout procedure](#) (see page 127) must be executed using r12 or r14 of CA Top Secret.

Important! If you maintain multiple security files through CPF, prevent CPF from sending the backout commands to multiple nodes. Work with each system and security file as a single entity.

Important! To no longer use the VSAM file, you must use an r14 and earlier release of CA Top Secret.

VSAM Digital Certificate Backout

This procedure is done on a system where the VSAM digital certificate feature is active and digital certificates and keyrings are loaded in the VSAM file.

Follow these steps:

1. Enter the command:

```
TSS LIST(ACIDS) DIGICERT(ALL)
```

A list of all digital certificates added to all users is displayed.
2. Count and record the number of certificates.
3. For each user displayed in the previous list, enter the command:

```
TSS LIST(user) DIGICERT(ALL)
```

Detailed information for all certificates belonging to the user is displayed.

4. Enter the command:

```
TSS LIST(ACIDS) KEYRING(ALL)
```

A list of all keyrings added to all users is displayed.

5. Count and record the number of keyrings.

6. For each user displayed in the previous list, enter the command:

```
TSS LIST(user) KEYRING(ALL)
```

Detail information for all keyrings belonging to the user is displayed.

7. Use the BACKUP control option to create a backup of both the current BDAM security file and the VSAM certificate file. The backups can be used to restore the files in the event of an emergency.

8. Edit the TSSXVSDT batch utility. Enter:

- The existing VSAM file containing the digital certificate and keyring records.
- A new VSAM file that will be defined by IDCAMS and populated by the batch utility.
- A sequential output file that will contain TSS EXPORT commands.
- A sequential output file that will contain TSS ADD commands.
- A SYSIN input statement with the format:

```
DCDSN(XXXXXXXX.XXXXXXXXXX.XXXXXXXXXX)
```

The name specified is used as a prefix to create the DCDSN operand on both the TSS EXPORT and TSS ADD commands created by the utility. The prefix can have a maximum length of 26 characters and must conform to standard MVS data set naming conventions.

- A SYSIN input statements with the format:

```
PKCSPASS(pppppppp)
```

The password specified is used to create the PKCSPASS operand on both the TSS EXPORT and TSS ADD commands created by the utility. The password can have a maximum length of 32 characters.

9. Run the TSSXVSDT batch utility:

The utility generates:

- A new VSAM file with all digital certificate records and keyring records removed, leaving only KERBEROS records if they exist.
- File CMDEXPT containing TSS EXPORT commands for all digital certificate records found in the existing VSAM file.
- File CMDADD containing TSS ADD commands for all digital certificate records and keyring records found in the existing VSAM file.

- A summary report listing the execution results of the utility and any errors found during processing. A non-zero completion code is accompanied by an error message that should be self-explanatory. Correct the error and rerun the utility as often as necessary.

The summary report contains number of:

- VSAM input records.
- VSAM output records.
- Digital certificate records deleted. This should match the number of certificates recorded in step 2.
- Keyring records deleted. This should match the number of keyrings recoded in step 5.

10. Edit TSSXVTMP, enter the CMDEXPT file name created by the batch utility TSSXVSDT. This file holds the TSS EXPORT commands to be executed.

11. Run the batch job TSSXVTMP.

The batch job executes IKJEFT01 to read the TSS command file as input and execute the TSS EXPORT commands. The existing VSAM file is used as input to generate the DCDSN data sets with the certificate data required by the TSS ADD process. A unique data set is allocated and cataloged for each TSS EXPORT command executed, the data set names have the format:

DCDSN(xxxxxxxx.xxxxxxxxx.xxxxxxxxx.aaaaaaa.dddddd)

xxxxxxxx

The prefix specified on the input DCDSN statement.

aaaaaaa

Specifies the ACID that owns the certificate.

ddddddd

Specifies the certificate name.

12. Edit batch job TSSXVOFF, enter:

- The name of the BDAM security file found on the SECFILE DD statement in your current TSS started task procedure.
- A SYSIN input statement with the format:

OFF vvvvvvv

vvvvvvv

Set to either VSAMDCRT or VSAMALL.

To disable all VSAM processing specify VSAMALL. To determine if VSAM is needed review the count of VSAM output records in step 9. If the count is 1 VSAM can be disabled. If the number of output records is greater than 1 you have KERBEROS records stored in VSAM that require continued VSAM processing and you should only disable certificate and keyring VSAM processing.

To disable VSAM digital certificate and keyring processing specify VSAMDCRT on the input statement. This allows the continued VSAM handling of KERBEROS records that have been migrated to VSAM.

13. Run batch job TSSXVOFF

The batch job turns off the appropriate VSAM feature flags located in the BDAM security file to disable VSAM processing.

14. Edit the TSS and TSSB started task procedures to reflect the new processing requirements:

- If you are disabling VSAM processing completely, remove all VSAM related DD statements from the procedures, including VSAMFILE, VSAMBKUP, VSAMAIX, and VSMPATH.
- If you are only disabling VSAM certificate and keyring processing, remove the DD statements for VSAMAIX and VSMPATH and modify the DD statement VSAMFILE to point at the new VSAM file generated by TSSXVSDT.
- If you are sharing the security file make the same modifications to the started task procedures on all systems.

15. Shut down and restart the CA Top Secret address space using the updated procedure. The restart should include the startup parameter:

REINIT (S TSS, , ,REINIT)

If you are sharing the security file shut down and restart the CA Top Secret address space with the updated procedure on all systems as soon as possible to prevent the creation of new certificates and keyrings or the update of existing certificates and keyrings in VSAM that will not be reflected in the backout process.

When the TSS address space is restarted there will be *no* certificates or keyrings available for processing. Any product or process requiring a digital certificate should be quiesced until the certificates are completely restored.

16. Edit TSSXVTMP. Enter the CMDADD file name created by TSSXVSDT, this file holds the TSS ADD commands to be executed.

17. Run TSSXVTMP.

This job executes IKJEFT01 to read the TSS command file as input and execute the TSS ADD commands. The commands use the DCDSN data sets created by the TSS EXPORT commands as input to add the digital certificates to the appropriate users, add digital certificates to keyrings, and add keyrings to users where required.

18. Review the list output from the execution of the commands and make sure they completed successfully.

19. Shut down and restart the CA Top Secret address space using the procedure from step 15. The restart should include the startup parameter:

REINIT (S TSS,,REINIT)

20. Repeat the TSS LIST commands in steps 1 to 6. The TSS LIST(ACIDS) is entered as TSS LIST(SDT) commands since the data is no longer in VSAM.

The commands provide a new directory of digital certificate and keyring objects after they have been restored to the BDAM security file.

21. Compare the TSS LIST command output to verify that all certificates and keyrings have been correctly restored to the BDAM security file. The digital certificate and keyring counts from both steps should match.
22. (Optional) Discard the command files and the DCDSN files generated to support the backout process.

Note: For information on the TSS EXPORT and TSS ADD commands for digital certificates and keyrings, see the *Command Functions Guide* and the *Cookbook*.

Index

A

allocate and mount • 43

C

CA CSM access

login • 29

CA CSM usage scenarios • 27

CAI.SAMPJCL

library • 64

sample jobs • 64

contacting technical support • 4

copy files to USS directory • 46, 47, 50

customer support, contacting • 4

D

download

files using ESD • 39

options • 46

overview • 37

to mainframe through a PC • 50

using batch JCL • 47

E

external HOLDDATA • 59

F

free space • 42

G

GIMUNZIP utility • 52

H

hash setting • 52

high-level qualifier • 52

HOLDDATA • 59

I

IEBCOPY • 64

installing

from Pax-Enhanced ESD • 37

from tape • 63

Integrated Cryptographic Services Facility (ICSF) • 52

internal HOLDDATA • 59

J

Java version support • 52

M

maintenance • 58

P

pax ESD procedure

copy product files • 46

create product directory • 51

download files • 39

set up USS directory • 42

pax file

copy files to USS directory • 46, 47, 50

process overview • 37

product download window • 39

product-level directory • 51

R

read me • 37, 52

S

sample JCL • 64

sample jobs • 47, 51

CAtoMainframe.txt • 47

Unpackage.txt • 51

SMP/E

GIMUNZIP utility • 52

support, contacting • 4

T

tape, installing from • 63

technical support, contacting • 4

U

UNIX System Services (USS)

access requirements • 37, 42

directory cleanup • 57

directory structure • 42

UNZIPJCL • 52

V

VSAM File Structure • 86