CA Top Secret® for z/OS

Release Notes

r15

Eleventh Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus for Security and Compliance Management
- CA Compliance Manager for z/OS
- CA Common Services for z/OS (CA Common Services)
- CA Datacom®/AD (CA Datacom)
- CA Chorus™ Software Manager (CA CSM)
- CA Top Secret® for z/OS (CA Top Secret)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Software Prerequisites (see page 10)—Updated version requirements.
- General Information (see page 10)—Updated version requirements.
- Control Option for Enforcing Rules for Administrative Password Changes (see page 36)—Describes a PWADMIN control option that enforces NEWPW control option restrictions and password interval restrictions when authorized administrators or users perform a password change through a TSS command.

Contents

Chapter 1: Welcome

This section contains the following topics:

Overview

Welcome to the CA Top Secret *Release Notes*. This guide describes enhancements, updates to features, system requirements, installation considerations, upgrade considerations, published solutions, and documentation information.

The information in this chapter applies to r15 and its service packages.

CA Common Services for z/OS Prerequisites

Before you install the CA Top Secret r15 product tape, we recommend that you install *r11 SP8* of CA Common Services for z/OS. The CA Quality Assurance group performed final integration tests at this level.

Note: To use the Serviceability enhancement you will need PTF RO17386. For details, see the Common Services Information Solution RI16.963

Published Fixes

All published fixes are available at Published Solutions on Support Online.

Documentation for r15

The documentation set for CA Top Secret includes the latest technology available for online viewing, keyword searching, book marking, and printing. The documentation set resides in one repository and is available at the CA online product support web site https://support.ca.com. You can view and download all CA product documentation from this central repository. We provide documentation in PDF format and update it on an as-needed basis.

To unload documentation from Support Online

1. On the Web, go to https://support.ca.com.

   The CA Support Online page opens.

2. Type a CA Support Online email address and password, and click Login.

   The CA Support Online page re-opens, and you are logged into CA Support Online.

3. Select Documentation located on the left side.

   The Documentation page opens.

4. Select the following options from the drop-down lists, and click Go.

   - Product = <product-name>
   - Release = <release-number>
   - Language = <language>

   The Product Search Results page opens.

Edition Numbers

Occasionally, we must update documentation outside of a new or updated release. To indicate a minor change to the documentation that does not invalidate it for any releases that it supports, we update the edition number on the cover page.

Release Numbers on Documentation

The release number on the title page of a document might not correspond to the current product release number; however, all documentation delivered with the product, regardless of release number on the title page, supports your use of the current product release. The release number changes only when a significant portion of a document changes to support a new or updated product release. If we do not make substantive changes to a document, we do not change the release number.

Documentation Reorganization

For CA Top Secret r15, we made the following documentation reorganization changes.

The *Auditor Guide* is now called the *Audit Guide*. The *Messages and Codes Guide* is now called the *Message Reference Guide*.

We restructured the *Installation Guide*, which now describes the following methods of installing CA Top Secret:

- CA Chorus™ Software Manager—Simplifies and unifies the management of CA mainframe products on z/OS systems. The services provided by CA Chorus™ Software Manager acquire, install, deploy, and maintain products in a common way.
- Pax-Enhanced Electronic Software Delivery (ESD)—Enables you to download and install CA's mainframe software and maintenance electronically to your own disk.
- Tape—Lets you use sample JCL to install CA Top Secret from tape using the SMP/E RECEIVE-ACCEPT-APPLY method.

We moved the following sections from the *Installation Guide* to the *User Guide:*

- STC Bypass
- Multi-CPU Environments
- Sysplex Coupling Facility
- TSO Online Submission
- OpenEdition z/OS Support
- Using the R_cacheserv Callable Service
- Enterprise Identity Mapping

We moved the following sections from the *Installation Guide* to the *Troubleshooting Guide*:

- TSSRECFR-Security File Recovery
- TSSXVSDT-Digital Certificate Backout

The following sections now appear in the *Installation Guide* and *User Guide*:

- JES2 & JES Startup
- SMF
- VSAM File

Software Prerequisites

Your IBM software must meet the following requirement to use r15:

- Any supported z/OS release (through z/OS 2.1)

If you are running the following software, it must meet specific version requirements to run concurrently with r15:

- IBM CICS Transaction Server for z/OS (CICS TS): You can use any supported release (through CICS TS 5.2).
- IBM Information Management System (IMS): You can use any supported release (through IMS 13.1).
- CA Common Services: You can use any supported release (through CA Common Services 14.1).

General Information

Note the label information located on the CA Top Secret r15 tape. The number 15SP0AKO00 denotes the level of the tape. The volume serial number for this tape is AKOF00 .

This release supports the following IBM software:

- z/OS (all generally supported releases through z/OS 2.1)
- UNIX System Services (USS)
- OpenEdition Distributed Computing Environment (DCE)
- z/OS HTTP Server
- CICS Transaction Server for z/OS (all generally supported releases through CICS TS 5.2)
- IMS (all generally supported releases through IMS 13.1)

An IPL is required after applying this product package.

Chapter 2: New Features

This section contains the following topics:

Support for CA Chorus for Security and Compliance Management Version 03.0.00

Support for handling user-defined fields (UDF) in CA Top Secret Compliance Information Analysis (CIA) has been enhanced.

Note: These enhancements require any existing CIA repositories to be redefined and reloaded (using the updated SAMPJCL jobs provided in the product).

Enhancements are as follows:

- CIA repository tables added/updated to support UDFs (updated data model and data dictionary)
- An updated method available for supporting UDFs in CIA batch unload and load processes
- Support added for different UDFs on multiple systems
- Support added for UDFs in a CIA CA Datacom repository
- CIA SAMPJCL jobs updated

Note: For more information about how to implement CIA and CIA UDF, see the *CA Top Secret Compliance Information Analysis Guide*.

CIA Data Model and Data Dictionary Updates

The CIA data model and data dictionary now support user-defined fields.

The following CIA tables have been added:

- ORGINFO
- UDFCHAR
- UDFNUM
- UDFDATE
- UDFTIME

The following CIA tables have been removed:

- USERFLD
- USERUSER

Important! To successfully implement and use CIA, use the updated SAMPJCL jobs (supplied in the product) to redefine and reload your CIA DB2 or CA Datacom repositories.

UDF Support in CIA Batch Unload and Load Processing

CIA batch unload and load processing now supports user-defined fields. You perform the process as follows:

1. Modify and submit the CIACFILE and CIAUNLD jobs to unload desired data from the security file to a specified UNLOAD file, which is loaded into a CIA DB2 or CA Datacom repository.
2. Use the supplied SAMPJCL jobs to load the data into your CIA DB2 or CA Datacom repository.

Note: For more information, see the *CA Top Secret Compliance Information Analysis Guide*.

CIA SAMPJCL Job Modifications

The following CIA SAMPJCL jobs now support the new method of processing user-defined fields.

- CIAALLOC
- CIADB2
- CIADCOM
- CIADCOMD
- CIALOAD
- CIALOADA

- CIALOADC
- CIAUNLD

The SAMPJCL jobs were modified as follows:

1. (DB2 and CA Datacom) Addition of DD statements to define, update, import, drop, and load data into the following new CIA tables:
   - CAIDB01.ORGINFO
   - CIADB01.UDFCHAR
   - CIADB01.UDFDATE
   - CIADB01.UDFNUM
   - CIADB01.UDFTIME
2. (DB2 and CA Datacom) Removal of DD statements that directly or indirectly reference the following obsolete CIA tables:
   - CIADB01.USERUSER
   - CIADB01.USERFLD
3. Removal of the UNLDUSER DD statement and CIA USERFLD table from the product

New Messages

The following messages have been added to the product:

- TSSC025E - INCOMING PARM USERFIELD( ) CAN'T BE USED WITH OTHER USERFIELDS.
- TSSC026E - USERFIELD(*ALL*) WAS SELECTED BY DEFAULT
- TSSC027E - USERFIELD( ) SELECTED TWICE AS AN INCOMING PARAMETER.
- TSSC028I - GLOBALID FIELD(*ACID*) WAS SELECTED BY DEFAULT.
- TSSC029E - GLOBALID FIELD( ) ALSO HAS TO BE SELECTED AS A USER FIELD.

Support for CA Chorus for Security and Compliance Management Version 02.5.00

The following enhancements support CA Chorus for Security and Compliance Management Version 02.5.00.

CIA Connection Status

CA Top Secret support for CA Chorus Version 02.5.00 includes an enhancement to the CMXREF table which contains CIA real-time status connection information for CIA related events. The status information can be viewed in CA Chorus Investigator.

Note: For more information, see the *Compliance Information Analysis Guide*.

New Messages

The following new messages have been added to support CA Chorus Version 02.5.00:

- CIA0811E—The *keyword* parameter value is invalid. CIA initialization terminated
- CIA0813E—Mutually exclusive values were specified for *keyword* keyword. CIA initialization terminated
- CIA0894E—The CIA repository must be either DB2 or CA Datacom
- CIA0895E—Unable to load module *modname*. CIA update request terminated
- CIA0896E—The *function* of CA Datacom region *mufid* failed. Return: *retcode* Reason: *rsncode*
- CIA0901E—Unable to locate SAF IVT

Simplified CIA Processes

We have simplified several installation, configuration, and usage processes for the CIA feature. Ensure that you carefully review the Configuration chapter of the *Compliance Information Analysis Guide*.

Support for CA Datacom

CA Top Secret now supports the use of CA Datacom for loading and unloading CIA data (in addition to support for DB2 for z/OS). A CIA load data conversion utility converts CA Top Secret security policy and user information in an unload data set from DB2 load format to CA Datacom load format. After processing is completed, the converted data is loaded into a CA Datacom CIA repository. This repository can be used for compliance information analysis purposes. For more information on CA Datacom support and the conversion utility, see the *Compliance Information Analysis Guide*.

Support for CA Chorus for Security and Compliance Management Version 2.0.00

The following enhancements support CA Chorus for Security and Compliance Management r2.0.

CA Chorus for Security and Compliance Management

This release introduces the CA Chorus for Security and Compliance Management role, which lets you simplify security and compliance management. By using a role-based delivery model, the product transforms the way IT staff collaborates with colleagues, interacts with management tools, and leverages the mainframe.

This role offers the following usability features:

- Time Series data graphing
- Real-time reporting
- Real-time access to state and event data
- Security data model extension
- Policy management
- In-context domain documentation
- Hover text
- Object-based navigation for near real-time performance monitoring

This role supports the following security-specific modules:

Alerts module

Displays security alerts based on user-configurable settings.

Command Manager module

Processes commands.

Note: For detailed conceptual and procedural information, see your role-specific *User Guide* available with the CA Chorus documentation set.

This role supports the following common modules and components:

Investigator

Lets you load, edit, and delete complete paths that you have followed while viewing and managing your systems. The *Investigator module* also supports the *Investigator*, which presents you with a cohesive view of your data. The Investigator helps you view and analyze critical information stored in your system by providing multiple work areas to help you manage your data.

Metrics Panel

Provides a visual display of key performance metrics for your monitored systems. The data shows statistics for the last 30-second collection interval. Graphs display the last 15 intervals. System metrics are broken down into data groups or categories.

Notes module

Lets you add a note in the Investigator. A note is private or public information that is related to an object. A note is saved with the entity, metrics, and time and date of creation. The Notes module includes Private Notes and Public Notes tabs.

Knowledge Center

The Knowledge Center is the repository for all documentation in CA Chorus. Examples of Knowledge Center documentation include online help and guides from CA, user-generated documentation, and links to third-party documentation. The Knowledge Center results are based on your location in the product when you click the Help icon. You can also enter specific search text in the Knowledge Center to narrow your results.

Note: For detailed conceptual and procedural information, see the *Product Guide* and your role-specific *User Guide* included with the CA Chorus documentation set.

CIA Real-Time Updates

CA Chorus leverages information from various sources. For many features, it interacts directly with your external security manager.

The real-time nature of processing security and compliance information requires that information in the CIA repository is an accurate reflection of the current information in the security product definitions. Any changes to the information in the security product database must be communicated in real time to the CA Chorus CIA repository. The CIA real-time feature provides that communication, and verifies that the information in the CIA repository reflects the current information in the security product database.

Note: The CIA real-time feature is only available when CA Chorus is installed at your site. When the CIA real-time feature is enabled, it performs an LMP check for the CA Chorus LMP key. Without the key, the CIA real-time feature cannot be enabled.

Control Options

The following control options provide information used by CA Chorus for CIA real-time updates and statistical gathering. For more information on each field see the *Control Options Guide* and *Compliance Information Analysis Guide.*

CHORUSTSFDB

Specifies the CA Chorus Time Series Facility Debug Option

CHORUSTSFSX

Specifies the CA Chorus Time Series Facility Suffix Indicator

CHORUSSTATG

Starts or stops statistics gathering to be sent to CA Chorus Time Series Facility.

CHORUSSTATI

Specifies the time interval for statistics gathering and CA Chorus Time Series Facility record creation.

CIAAUTO

Specifies whether CA Top Secret, at initial start after IPL, will automatically start the CIA real-time processing component started task.

CIAGBLEXIT

Specifies the name of the user globalid exit module that was used by the Unload utility to supply a globalid.

CIAGBLFIELD

Specifies the external name of a character type field in the logonid record that the Unload utility used to supply a globalid.

CIAHOST

Specifies the host name of the DSI server.

CIALOGNAME

Specifies the name of the log stream used by CIA real-time updates.

CIAMAXSTOR

Specifies the maximum size of storage used by the CIA real-time subtask, in megabytes.

CIAPORT

Specifies the port number for the DSI server.

CIAPROCNAME

Specifies the library member name for the CIA real-time processing component started task procedure.

CIART

Specifies CIA real-time updates are active.

CIASYSID

Specifies the SYSID value.

CA Chorus Messages

The following messages have been added to support CA Chorus, CIA real-time updates, and statistical gathering:

- TSS7460E - CPU XXXXXX REQUIRES AN LMP KEY TO RUN PROD(CH) CHORUS
- TSS7461E - CIA real-time Deactivated
- TSS7462E - CIA real-time Subtask not activated. LMP Key not provided
- TSS9693E - CIA REAL-TIME PROCESSING COMPONENT ASCRE ERROR – *RC* = XX *RS* = XX
- TSS9694E - CIA REAL-TIME CANNOT BE ACTIVATED WITHOUT *XXXXXXXX*
- TSS9695E - CIAPROCNAME MUST BE SPECIFIED BEFORE CIAAUTO
- TSS9696E - CIASYSID CAN NOT BE CHANGED WHEN CIA REAL-TIME IS ACTIVE
- TSS9697E - CIAGBLEXIT AND CIAGBLFIELD ARE MUTUALLY EXCLUSIVE
- TSS9698E - CIA REAL-TIME SUBTASK NOT AVAILABLE
- TSS9699E - CIA real-time Subtask not activated. z/OS 1.10 or above required
- TSS9879I - Stats Gathering Activated for Chorus
- TSS9995E - Unable to Write Record - Time Series Facility Not Available
- TSSC104I - LPAR (lpar) was set from (*the system or parameter file*)
- TSSC1051 - Duplicate LPAR skipped - *lpar*
- CIA0133E - Userfield xxxxxxxx not defined to the Top Secret FDT
- CIA0134E - Bad length for type user defined field - xxxxxxxx
- CIA0135E - Invalid field name for Global IDMAP - xxxxxxxx
- CIA0136E - Invalid field length for Global IDMAP - xxxxxxxx
- CIA0240E - Event record is missing or invalid
- CIA0241E - CA Top Secret is not active
- CIA0242E - Unable to locate CIARTCVT
- CIA0243E - CFILE record error
- CIA0244E - CIA Load record error
- CIA0245E - Error building request record list
- CIA0246E - acid type invalid for event
- CIA0247E - GETMAIN/FREEMAIN error
- CIA0248E - Error from call to DSI
- CIA0249E - Invalid plist parameter list
- CIA0251E - Getmain failure for xxxxxxxx

- CIA0252E - Internal processing problem, reason code - xx
- CIA0300I - CIA real-time Logging Task is Initializing
- CIA0301I - CIA real-time Rcvr Queue Allocation: RC=rc RSN=rsn
- CIA0302I - CIA real-time Rcvr Queue Max Entries now nnn cells
- CIA0303I - CIA real-time DASD Log Stream Detected
- CIA0310I - CIA real-time Sys Logger Connect LogStream=name RC=*rc* RSN=*rsn*
- CIA0311I - CIA real-time Log Info LSVERSION=version
- CIA0312I - CIA Real Time Log Info Structure Name=name
- CIA0313I - CIA Real Time Log Info Structure Buf Sizes MAX=*max* AVG=avg
- CIA0314I - CIA Real Time Log Info Diag 1-4: *value1 value2 value3 value4*
- CIA0315I - CIA Real Time Log Info GAPS=*gaps* FLAGS=*flags*
- CIA0320I - CIA Real Time Sys Logger Disconnect LogStream=logstream RC=rc RSN=rsn
- CIA0322I - CIA Real-Time Rcvr now accepting events
- CIA0323I - CIA Real-Time Rcvr no longer accepting events
- CIA0348I - CIA Real-Time Logging Task - Termination Process Complete – Re-initialization is being attempted
- CIA0349I - CIA Real-Time Logging Task - Termination Process Complete - Task will end
- CIA0351E - CIA Real Time Rcvr Queue Deallocation Successful
- CIA0352E - LOAD failed for module name R1=r1 R15=r15
- CIA0354E - CIA Real Time Sys Logger Write Error LogStream=name RC=*rc* RSN=*rsn* Cnt=cnt
- CIA0355W - CIA Real Time Logger Lost Record CIARC=*reason* Count now count
- CIA0356W - CIA Real Time Rcvr Queue cannot be deleted - Receiver Active
- CIA0357I - CIA Real Time Logstream Connection Successful - Awaiting Structure Rebuild
- CIA0358I - CIA Real Time Logstream now disconnected
- CIA0359I - CIA Real Time Logstream - Writes pending
- CIA0360I - CIA Real-Time Logger - Shutdown ordered
- CIA0361I - CIA Real-Time Logger - Attempting connection
- CIA0362I - CIA Real-Time Logger - Waiting for ENF notification
- CIA0363I - CIA Real-Time Logger - Disconnect ordered
- CIA0370E - CIA Real-Time Logger - ENF Exit Storage Error RC=*rc*

- CIA0371I - CIA Real-Time Logger - ENF Event Selected, EVENT=*event*, RSN=*reason*
- CIA0372E - CIA Real-Time Logger - ENF Event Not Freed, RC=*v1*, R0=*v2 xxxxx*
- CIA0373E - CIA Real-Time Logger - ENF Event Queue Error
- CIA0374I - CIA Real-Time Logger - ENFREQ RC=*rc*
- CIA0375I - CIA Real-Time Logger - ENF Event Processing, EVT=nnnnn, RSN=nnnnn
- CIA0376I – CIA Real-Time Logger – ENF Action Selection, EVT=nnnn, RSN=nnnn,, ACT=nnnn
- CIA0380I - CIA Real time Logger - ResMgr Add RC=dd
- CIA0381I - CIA Real Time Logger - ResMgr Completed RC=*dd*
- CIA0385I - CIA Real Time Logger - Connect requested, already connected; attempt Disconnect or Reconnect
- CIA0386I - CIA Real Time Logger - Disconnect Requested, Token=zero, flags reset, attempt Connect
- CIA0401I - CIA/RT Component Activation
- CIA0402I - CIA/RT Component Activation Complete
- CIA0403I - CIA/RT Component Termination
- CIA0404I - CIA/RT Component Termination Complete
- CIA0405I - CIA/RT Component MODIFY Command Complete
- CIA0406I - CIA/RT Component Options Processing
- CIA0407I - CIA/RT Component Options Processing Success
- CIA0408I - CIA/RT Component Communications Task Activation
- CIA0409I - CIA/RT Component Communications Task Termination
- CIA0410I - CIA/RT Component Attaching Permanent Servers
- CIA0411I - CIA/RT Component Detaching Servers
- CIA0415I - CIA/RT Component Event Server Activated
- CIA0416I - CIA/RT Component Event Server Terminated
- CIA0417I - CIA/RT Component Option GTRACE is &status
- CIA0418I - CIA/RT Module Reload Success - &modname reloaded
- CIA0420I - CIA/RT Component Retry Initialization <Y> or <N> ?
- CIA0440I - CIA/RT Status Messages
- CIA0450E - CIA/RT Component Not Authorized
- CIA0451E - CIA/RT Component Storage Obtain Failure
- CIA0452E - CIA/RT Component ESM Subsystem Unavailable
- CIA0453E - CIA/RT Component Already Active – terminating this instance

- CIA0454E - CIA/RT Component Module Load Failure
- CIA0455E - CIA/RT Component ESM Initialization Failure
- CIA0456E - CIA/RT Component Options Failure
- CIA0457E - CIA/RT Component Task Attach Failure
- CIA0458E - CIA/RT Component Command Unrecognized
- CIA0459E - CIA/RT Component Option &option Error, Using Default
- CIA0461E - CIA/RT Component Abend Limit Exceeded
- CIA0462E - CIA/RT Component Control Block &block not found
- CIA0463E - CIA/RT Module Reload Failure - Name not entered
- CIA0464E - CIA/RT Module Reload Failure - Plist or control block in error
- CIA0465E - CIA/RT Module Reload Failure - No match for module &modname
- CIA0466E - CIA/RT Module Reload Failure - &modname RC=&retcode RSN=&rsncode
- CIA0470E - CIA/RT Component Logger &function Failure - RC=&retcode RSN=&rsncode
- CIA0471E - CIA/RT System Logger is Down and needs Restarting
- CIA0476E - CIA/RT Component <DSI or DB2> Processing Failure Condition
- CIA0477E - CIA/RT Correct condition and reply <Y> to continue or <N> to terminate
- CIA0480E - CIA/RT Component – CIASTATS file error, &status
- CIA0481I - CIA/RT Component – CIASTATS file reset - &status
- CIA0490I - CIA/TR Journal File Initialization Complete
- CIA0491E - CIA/RT SYSIN File Open Error
- CIA0492E - CIA/RT Invalid Parameter, BLOCKS= Not Found
- CIA0493E - CIA/RT Invalid Parameter, BLOCKS= Invalid
- CIA0494E - CIA/RT SYSIN File Error - No Parameters Entered
- CIA0495E - CIA/RT Journal File Open Error
- CIA0496E - CIA/RT Error Writing to Journal File
- CIA0497E - CIA/RT Component Journal &function Failure - RC=&retcode RSN=&rsncode
- CIA0500E - Module parameter error
- CIA0501E - Module *modname* routine *rtnname* insufficient storage for execution
- CIA0502E - Module *modname* routine *rtnname* CIASPSQL error - RC=*returncode* RSN=*reasoncode*
- CIA0503E - Module *modname* routine *rtnname* SQL error – SQLCODE=*sqlcode*

- CIA0504E - LOAD failed for module *modname*. R1=*abendcode* R15=*reasoncode*
- CIA0801I - CIA process initialization has begun
- CIA0802I - CIA process initialization complete
- CIA0803E - Unable to load module *modname.* CIA initialization terminated
- CIA0804E - Unable to locate module *modname*. CIA initialization terminated
- CIA0805W - The DB2 subsystem *ssid* is not active
- CIA0809I - CIA process termination complete
- CIA0810E - The *keyword* keyword is not supported. CIA initialization terminated
- CIA0812E - The *parm* parameter is required. CIA initialization terminated
- CIA0821E - CIA/RT SQL ERROR - SQLCODE= *code*
- CIA0890E - Error in *modname* request parameter list
- CIA0891E - Insufficient storage for *modname* execution
- CIA0892E - RRSAF function to DB2 subsystem ssid failed. Return: *retcode* Reason: *rsncode*
- CIA0893E - Error in *modname* - CIA Global area not found

Chapter 3: Enhancements to Existing Features

This section contains the following topics:

Documentation

This section contains topics that are related to documentation enhancements.

CA HTML Bookshelf

This release contains the CA HTML bookshelf, which is an HTML help system that provides access to all deliverables in the product documentation set in both HTML and PDF. HTML provides robust online viewing and search capabilities, while PDF provides a print-friendly option.

The HTML bookshelf features include:

- A single help screen that displays all documentation for this release.
- An all-in-one search tool that searches the entire documentation set and returns matches found in both the HTML and PDF formatted documentation, without the need for a specialized .PDX index file.
- Additional links for using the bookshelf, downloading Acrobat Reader, and contacting CA Technologies.

Note: You must have Adobe Reader 8 or above to view the PDF files in the bookshelf.

Search the Bookshelf

The bookshelf includes a search facility that helps you locate information throughout the set.

To search the bookshelf

1. Enter your search criteria in the Search field in the upper right corner of the bookshelf and press Enter.

   The search returns HTML results listed by topic and PDF results listed by guide. The results are sorted by date so that the most recently updated topics or PDFs appear at the top of the list. To find a topic in a PDF, open the PDF and view the list of topics within the PDF that match the search criteria.

2. (Optional) Click Sort by Relevance.

   The list is reordered so that the HTML topics or PDFs that contain the most matches appear at the top of the list.

Product Enhancements r15

This section describes the enhancements we added to CA Top Secret for r15.

CICS TS 4.2 Support

The following enhancements support CICS TS 4.2.

Password Phrase Support

CICS now supports the use of password phrases as well as standard passwords to authenticate a user ID when signing on to CICS. Because a password phrase can provide an exponentially greater number of possible combinations of characters than a standard password, the use of password phrases can improve system security and enhance usability.

CESL is a new supplied transaction that you can use to sign on to CICS using a password or a password phrase as authorization. Transaction CEDF has been changed to support password phrases.

z/OS 1.12 Support

The following enhancements support z/OS 1.12.

Elliptic Curve Cryptography

z/OS 1.12 introduces support for Elliptic Curve Cryptography (ECC) certificates. The CA Top Secret GENCERT command has been modified to allow ECC certificates to be generated. ECC certificates are regarded as providing stronger cryptography with smaller key sizes than RSA certificates. ECC certificate support has been added to the CHKCERT, ADD, GENREQ, EXPORT, REKEY, P11TOKEN BIND and P11TOKEN IMPORT commands as well.

ECC algorithms supported are the 5 NIST supported prime curves (p192, p224, p256, p384 and p521). Also supported are the Brainpool Curves defined in RFC 5639.

ECC support requires the PKCS 11 support found in the z/OS Integrated Cryptographic Service Facility (ICSF). ICSF must be at the HCR7770 level, at the least.

z/OS 1.12 Messages

The following messages were added to support z/OS 1.12:

TSS0965E KEYUSAGE INDICATES ONLY KEYAGREE – CANNOT INSERT CERTIFICATE UNDER CERTAUTH

TSS1612E INVALID VALUE FOR KEYWORD SIGNALG

TSS1613E ICSF or PCICC was specified but input certificate is NISTECC or BPECC

TSS1614E CANNOT DOWNGRADE PRIVATE KEY FROM ECC

TSS1616 SIGNALG CANNOT BE USED WHEN NISTECC OR BPECC IS SPECIFIED

TSS1617E BPECC and DATAENCRYPT CANNOT BE SPECIFIED TOGETHER; NISTECC and DATAENCRYPT CANNOT BE SPECIFIED TOGETHER

TSS1618E Input certificate contains non-RSA public key. Public key cannot be added to ICSF

The following messages were changed to support z/OS 1.12:

TSS1544E MUTUALLY EXCLUSIVE KEYWORDS SPECIFIED – aaaaaaaa/bbbbbbbb

TSS1545E NISTECC or BPECC was specified but input certificate is not NISTECC or BPECC

The following message was removed to support z/OS 1.12:

TSS1543E ADD/REM RDT FAILS for invalid CHECKVAL value

PKI Services

The R_PKIServ callable service allows applications to request the generation and retrieval of certificate and certificate requests. Support has been added for the following features for this service:

- Multiple Subject Alternate Name values support—parameters AltDomain, AltEmail, AltIPAddr, AltURI may be repeated in the CertPlist for GENCERT, REQCERT, MODIFYREQS, REQDETAILS, CERTDETAILS and VERIFY.
- Elliptic Curve Cryptography (ECC) support—z/OS 1.12 introduces certificates with the Elliptic Curve algorithm instead of the RSA or DSA algorithms. ECC is regarded by the National Security Agency (NSA) as a faster algorithm that requires a smaller key than RSA cryptography. Users can specify the size of the key in bits with the KeySize parameter. Users can also specify the algorithm of the key using the KeyAlg parameter if it is to be generated by PKI Services. Both parameters can be specified on the GENCERT and REQCERT requests.
- Custom extensions—CustomExt is a new parameter that is used to specify a customized extension in the form of a comma separated four part string. This parameter is found in the CertPlist for GENCERT, REQCERT, MODIFYREQS, REQDETAILS and CERTDETAILS.

For more information about this enhancement, see the *Command Functions Guide*.

RACROUTE Extract

The caller's ASID and return address is now being added to the RXTW (extract result work area) for debugging purposes.

REKEY Downgrade Key

A new feature has been added to REKEY and GENCERT commands that prevents the downgrade of a new key from ICSF/PCICC to a database key. Processing has changed to prevent downgrade. If you do not specify any of the following keywords on a REKEY subcommand, CA Top Secret will not take what was used on the original certificate.

- ICSF
- PCICC
- NISTECC
- BPECC

A certificate cannot be downgraded from an ECC type (NISTECC or BPECC) to non-ECC (and conversely). Attempting to do this will produce one of the following messages:

TSS1613E ICSF or PCICC was specified but input certificate is NISTECC or BPECC

TSS1545E NISTECC or BPECC was specified but input certificate is not NISTECC or BPECC

For more information about this enhancement, see the *Command Functions Guide*.

SHA-2 Algorithm

The default signing hash algorithm for certain certificates has changed. SIGNALG is a new parameter on the GENCERT command that allows the user to specify the algorithm that they wish to use.

Valid values for SIGNALG are SHA1 and SHA256. For RSA certificates with key size 2048 or larger, the default is SHA256. Otherwise, the default is SHA1.

Note the following:

- SIGNALG(SHA256) cannot be specified for DSA certificates.
- SIGNALG cannot be specified for ECC certificates.

The following table indicates the default signing algorithm used when SIGNALG is not specified.

Signing Algorithm Used	Keysize (in bit) of Signing Certificate		
	RSA	**NISTECC**	**BPECC**
SHA-1	Less than 2048		
SHA-256	2048 or more	192, 224	160, 192, 224
SHA-256		256	256, 320
SHA-384		384	384
SHA-512		521	512

Note: For more information about this enhancement, see the *Command Functions Guide*.

z/OS 1.13 Support

The following enhancements support z/OS 1.13.

Certificate Key Display Changes

The CHKCERT command has been modified to always display the key size and type of the certificate. If a private key exists for the certificate, the header indicates Private Key Size and Private Key Type. If no private key exists for the certificate being displayed, the header indicates Public Key Bit Size and Public Key Type.

A similar change has been made to the Certificate Utility. Previously, the key size was displayed only when a private key existed for the certificate (or was returned when specifying a key ring). With these changes, a key size is always displayed and the header indicates whether a private key exists or if only a public key exists.

For more information, see the *Report and Tracking Guide* and *Command Functions Guide.*

ECC Keys and ICSF

The GENCERT, REKEY and RENEW command functions have been modified to allow ECC keys to be stored and retrieved from the ICSF PKDS. The GENCERT command can request that ICSF generate the key pair and store the private key. Specify PCICC and LABLPKDS when NISTECC or BPECC is specified to implement these changes. These changes require that ICSF be at the HCR7780 level or higher. If systems that have a back-leveled version of ICSF share the database, the system with the back-leveled ICSF is unable to access the private key.

Note: You no longer are required to specify PCICC to have the hardware generate the key; specifying LABLPKDS is sufficient. This applies to RSA and ECC keys. If you require an RSA key to be in Modulus-Exponent format, specify ICSF.

For additional information, see the *Command Functions Guide.*

IDMAP Cleanup Utility (TSSCHKDN)

We have added the TSSCHKDN batch utility, which identifies invalid distinguished names (DNs) for CA Top Secret IDMAP users implementing secondary distinguished names. The CHKADDRS field allows address checking in tickets for the Kerberos server running on z/OS 1.13 operating system or higher. Use this utility to more efficiently identify IDMAPDN values in IDMAP records that are invalid for z/OS 1.13.

For additional information, see the *Report and Tracking Guide*.

CHKADDRS Support for Kerberos

z/OS 1.13 introduces CHKADDRS, which is a new field in the GSO REALM record. The CHKADDRS field allows address checking in tickets for the Kerberos server running on z/OS 1.13 operating system or higher.

For more information, see the *Command Functions Guide*.

z/OS 1.13 Messages

The following messages have been added to support z/OS 1.13:

TSS1556E Certificate in PKCS 11 token cannot be deleted - error

TSS1558E Error returned from ICSF services. ICSF RC= rc - RSN = rsn

TSS1560E Input certificate contains non-RSA public key. Public key cannot be added to ICSF

TSS1561E Invalid or missing PKDS label. Public key cannot be added to ICSF

TSS1562E Key size of certificate requires PCI Cryptographic Coprocessor. Specify PCICC instead of ICSF

TSS1619E THE IDMAP DISTINGUISHED NAMES ARE INVALID AND MUST BE CORRECTED

TSS1620I Certificate has a private key that cannot be inserted – Certificate inserted without the private key

TSS1621E OPERATION NOT SUPPORTED AT CURRENT LEVEL OF ICSF

z/OS 2.1 Support

The following enhancements support z/OS 2.1.

New CHAIN Parameter for CHKCERT and LIST Commands

The CHKCERT command and the LIST command (with the DIGICERT keyword specified) now accept the CHAIN parameter, which displays information for each certificate in the chain and displays detailed summary information as applicable.

The ADD command (for adding digital certificates to user ACID records) displays message TSS1624I for each certificate added to the user record. The message indicates the record IDs of the CA certificates and end-entity certificate.

The EXPORT command displays message TSS1625I for each certificate added to a certificate package. The messages indicate the record IDs of the end-entity certificate and all signer certificates.

Preventing Certificate Deletion and Rollover after GENREQ

The product now provides the following preventative measures when you are creating a digital certificate based on an existing certificate:

- If you issue the GENREQ command (to generate a request for creating a signed certificate to replace an existing certificate), the product prevents the deletion of the existing certificate until the following process is complete:
  - You have sent the request to a certificate authority and obtained the signed certificate from the authority.
  - The product has inserted the new certificate over the original certificate.

  Retaining the original certificate during the process prevents the loss of a private key when the product replaces the original certificate with the new certificate.

  Note: You can use the FORCE keyword to forcibly remove the original certificate if necessary (for example, if the GENREQ command was issued against this certificate in error).
- If you issue the GENREQ command, then request ROLLOVER processing prior to the signed certificate being returned and replacing the existing self-signed certificate, the product issues an error message. This process prevents the self-signed certificate being moved into the key rings where the original certificate was connected, at which point services using the key ring might not work in the intended manner.

Variable Substitution in the HOME Value for a MODLUSER ACID

When using a model record with BPX.UNIQUE.USER, you do not need to modify the user's OMVS profile record to set the HOME value. You can specify a variable for the HOME value of a MODLUSER ACID. When MODLUSER information is added to a user's ACID record, a user ID value replaces the variable. Substitution occurs as follows:

- Specifying &ACID (or a mixed-case entry) translates to an uppercase user ID value.
- Specifying &acid translates to a lowercase user ID value.

_POSIX_CHOWN_UNRESTRICTED Rule Changes

IBM APAR OA41364 introduced _POSIX_CHOWN_UNRESTRICTED rule changes that tighten the restrictions on non-superusers modifying the ownership of their files.

Prior to the changes, anybody could change the owner and group for their owned files to any UID and GID (when the CHOWNURS control option was turned on). Under the new rules, CHOWNURS is not supported. _POSIX_CHOWN_UNRESTRICTED mode is now in effect when resource CHOWN.UNRESTRICTED is defined in the UNIXPRIV class. User capability depends on level of access to CHOWN.UNRESTRICTED as follows:

- READ access provides the following authorization:
  - Allows a file owner to change the UID of the file to any non-0 UID.
  - Allows a file owner to change the GID of the file to a GID that is not in the owner's supplemental group list.
- UPDATE access allows the file owner to change the UID of the file to UID 0.

Support for CA Top Secret r15

The following enhancements support the initial release of CA Top Secret r15.

New ORGACIDSIZE Parameter for Setting Organizational ACID Size Limits

You can now set size limits specifically for organizational ACIDs. When creating a security file, you can set the following parameter.

Note: For complete information about creating a security file, see the *CA Top Secret Installation Guide*.

ORGACIDSIZE=*nnnn*

(Optional) Indicates the maximum allowed 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

TSSUTIL Support for Reporting on Specific Resources

The TSSUTIL utility can now report on a specific resource. To enable this reporting, you specify the following selection criteria option:

RESOURCE('*resource_name*')

resource_name

Specifies the name of the specific resource.

Limit: 255 characters

Note: You can specify up to eight entries overall for RESOURCE (resource prefixes, resource names, or a combination of both).

Note: For more information about using TSSUTIL to archive and report on security-related activity, see the *CA Top Secret Report and Tracking Guide*.

Example: Report on a Specific Resource Named SampRes

This example produces a report that shows all security incidents related to the resource named SampRes:

```
REPORT EVENT(ALL) LONG RESOURCE('SAMPRES')
```

TSSUTIL Support for Multi-Line Selection Criteria and In-Line Comments

The TSSUTIL utility now supports multi-line selection criteria. For example, a RESOURCE selection criteria option can specify a long resource name that spans more than one line in the JCL. In addition, you can specify +,-, or * characters between control statement options, which allows you to embed in-line comments or provide a visual indication of places where JCL statements occupy more than one line. TSSUTIL ignores any content from the specified character through the end of a current line.

Note: For more information about using TSSUTIL to archive and report on security-related activity, see the *CA Top Secret Report and Tracking Guide*.

Restricting Passwords by String

You can now apply password restrictions based on strings within the passwords. Specifying the RT option in the NEWPW control option prohibits passwords that contain any string that matches an entry from the restricted password list.

Note: The restriction applies regardless of where the string occurs within the password. For complete information about using the NEWPW option to enforce password restrictions (or using the RPW option to manage the restricted password list), see the *CA Top Secret Control Options Guide.*

Example: Deny Password Use Based on a PGMR String

This example prevents a user from specifying a new password that contains one of the entries in the restricted password list. The entry can be any string that occurs within the password.

```
TSS MODIFY NEWPW(MIN=04,MAX=008,WARN=03,MINDAYS=01,NR=0,ID,TS,RT)
```

For this example, the restricted password list contains the entry *PGMR*. Later, a user needs a password change and tries to use the password *STARPGMR*; however, *PGMR* exists in the restricted password list, making the password unacceptable. If the ACID tries *12PGMR34* as the new password, the same rejection occurs.

Support for Comparing All ACID Types

You can now use the TSS COMPARE command function (and the associated USING keyword) to compare all ACID types.

Note: For complete information about using the command and keyword, see the *CA Top Secret Command Functions Guide*.

TSSAUDIT Support for Filtering CHANGES Reports by Times and Date Ranges

TSSAUDIT now includes the following keyword support in the CHANGES control statement:

- The TIME keyword lets you report by selecting records that were produced at a specific time or during a time period.
- The DATE keyword lets you report by selecting records that were produced on a specific date or during a range of dates.

Note: For more information about using TSSAUDIT to monitor security file changes and monitor other sensitive data, see the *CA Top Secret Report and Tracking Guide.*

Security Event Logging for TSSSIM Callable Service

When called as a callable service, the TSSSIM utility now allows CA LDAP to log generated TSSSIM security events to the TSS ATF file.

New FSACCESS Control Option

The new FSACCESS control option lets you enable or disable FSACCESS resource class checks that originate from the SAF component.

The FSACCESS IBM z/OS feature added a security check for the FSACCESS resource class to verify user authority to access the file system objects on z/OS UNIX zFS. This support was added by IBM APARS OA35970/OA35974 at z/OS 1.12 and is included at base z/OS 1.13.

With the IBM feature installed, the resource class checks occur by default many times, so disabling the calls can help significantly reduce overhead.

Note: For a complete description of the FSACCESS control option, see the *Control Options User Guide*.

Control Option for Enforcing Rules for Administrative Password Changes

Control option PWADMIN is now available to enforce NEWPW control option restrictions and password interval restrictions when authorized administrators or users perform a password change through a TSS command. The required authorization is MISC8(PWMAINT) or ACID(MAINTAIN) authority.

Support for Creating a Mirror Security File

A mirror security file is an exact duplicate of the primary security file and provides up-to-the-minute data in the event of a sudden problem with the primary file.

Important! Mirror files are supported only on systems that do not share the security file (SHRFILE(NO) control option setting).

You can use CAKOJCL0 members VSAMDEFM and TSSMAINM to accommodate your site's needs when setting up the mirror file; you can activate mirroring through the MIRROR control option.

ARCHIVE Keyword

The ARCHIVE keyword is a new keyword that generates a list of TSS commands, which are a record of the acid's profile data, including permissions and resources. These commands can later be used to restore the acid. The generated TSS commands can be stored in a PDS dataset using the INTO keyword.

For more information, see the *Command Functions Guide*.

Certificate Utility Enhancements

The Certificate Utility Report now displays the contents of extensions found in a certificate. When the certificate utility can determine the name of the certificate extensions, the certificate name is displayed. When the certificate extension name cannot be determined, a hex dump of the value is now displayed. In previous versions of CA Top Secret, if the utility could not determine the certificate extension, the object ID was displayed.

The following additional fields have been added to a certificate's report:

- Trust status
- Certificate length
- Certificate signing algorithm

Execution of SAFCRRPT now requires a region size of 1500K.

For more information, see the *Report and Tracking Guide*.

COMPARE Command

The COMPARE command function is a new command that compares the security records of two users and displays the differences.

For more information, see the *Command Functions Guide*.

Data Set Name Change

The names of most data sets have been changed for the CA Top Secret product for r15. We recommend that you carefully review the following table and assess any impact these changes may have to your installations z/OS configuration definitions, ISPF configuration/operation procedures, operating procedures, assembly/link-edit customization jobs and procedures, scheduled jobs, and more.

CA Top Secret Distribution Library	r14 Name	r15 Name
Clists	CAI.AAKOCLS0	CAI.AAKOCLS0
ISPF Profile	CAI.AAKOPROF	CAI.AAKODATA
DBRM Modules	CAI.SAF.AAX8DBRM	CAI.AAKODBRM
JCL	CAI.AAKOJCL	CAI.AAKOJCL0
Macros	CAI.AAKOMAC0	CAI.AAKOMAC0
English (ENU) Messages	CAI.SAF.AAX8MENU	CAI.AAKOMENU
Modules	CAI.AAKOLOAD	CAI.AAKOMOD0

CA Top Secret Distribution Library	r14 Name	r15 Name
Modules (SAF)	CAI.SAF.AAX8LOAD, CAI.SAF.AAX8LLE	CAI.AAKOMOD1
Modules (CICS)	CAI.CKOE010.AKO10LLD	CAI.AAKOMOD2
Modules (IMS)	CAI.CKOE02A.AKO2ALLD, CAI.CKOE020.AKO20LLD, CAI.CKOE029.AKO29LLD	CAI.AAKOMOD3
Modules (IDMS)	CAI.CKOE030.AKO30LLD	CAI.AAKOMOD4
Modules (ROSCOE)	CAI.CKOE040.AKO40LLD	CAI.AAKOMOD5
ISPF Messages	CAI.AAKOMSG0	CAI.AAKOMSG0
ISPF Panels	CAI.AAKOPNL0	CAI.AAKOPNL0
Sample Source	CAI.CKOE040.AKO40SRC	CAI.AAKOSAMP
Sidedecks	n/a	CAI.AAKOSIDE
Source	CAI.AAKOSRC0	CAI.AAKOSRC0
ISPF Tables	CAI.AAKOTBL0	CAI.AAKOTBL0
XML Data	CAI.AAKOXML	CAI.AAKOXML

CA Top Secret Target Library	r14 Name	r15 Name
Clists	CAI.CAICLS0	CAI.CAKOCLS0
ISPF Profile	CAI.CAIPROF	CAI.CAKODATA
DBRM Modules	CAI.SAF.CAIDBRM	CAI.CAKODBRM
JCL	CAI.CAIJCL	CAI.CAKOJCL0
Linklist Library	CAI.CAILOAD	CAI.CAKOLINK
LPALIST Library	CAI.CAILPA	CAI.CAKOLPA
Macros	CAI.CAIMAC	CAI.CAKOMAC0
English (ENU) Messages	CAI.SAF.CAIMENU	CAI.CAKOMENU
ISPF Messages	CAI.CAIMSG0	CAI.CAKOMSG0
ISPF Panels	CAI.CAIPNL0	CAI.CAKOPNL0
Sample Source	CAI.CAISRC	CAI.CAKOSAMP
Sidedecks	n/a	CAI.CAKOSIDE

CA Top Secret Target Library	r14 Name	r15 Name
Source	CAI.CAISRC	CAI.CAKOSRC0
ISPF Tables	CAI.CAITBL0	CAI.CAKOTBL0
XML Data	CAI.CAKOXML	CAI.CAKOXML

Data Classification

In the DATACLAS record, a dash (“-“) at the end (or as the only character) of a resource name now indicates that the resource name is a prefix. No other masking is permitted. Any other masking characters are treated as a literal.

DATACLAS tracking records are now stored in the VSAM file.

Logging Limit—MATCHLIM Keyword

Users have several ways to create an audit trail to track access by resource or user. These audit records occur even when access is allowed to the resource. Generally, the number of allowed accesses can be very large and auditing them can hurt performance and potentially impact the system.

The new MATCHLIM keyword can be specified when resource or user auditing is specified. This MATCHLIM keyword limits the number of loggings that will occur for that resource or user to a globally specified value. When the MATCHLIM value is reached, loggings generated because of resource or user auditing stop until the audit counts are reset using the MATCHLIM(CLEAR) or a system IPL.

Audit match limit processing only affects loggings that are generated because of the AUDIT attribute or the AUDIT Record. All other loggings, including those that occur because of violations, bypass authorities, and exits, are not affected by Match Limit processing.

For more information, see the *Control Options* and *Command Functions* guides.

MODEL Command

The MODEL command function is a new command that copies permission for data sets and resources from an existing user acid to another user acid. You can model to existing and new user acids. The MODEL command generates a list of TSS commands, which are then reviewed and executed to create the new acid. You can also use the INTO keyword to write the generated commands to a PDS data set.

Because the MODEL command now exists, abbreviating the CA Top Secret MODIFY command to the first three characters is no longer valid. Use the first four characters (MODI) in the abbreviation for MODIFY.

Note: For more information about the MODEL and MODIFY commands, see the *Command Functions Guide*.

Messages r15

This section lists the new messages in r15.

For detailed information about each message, see the *Messages and Codes Guide*.

ACID Compare Messages

TSS1601E KEYWORD USING IS MISSING

TSS1606E COMPARE ACOMP PROCESSING FAILED - REASON CODE = nn

TSS1607E USING MUST BE TYPE=USER

TSS1608E ACID VALUE FOR KEYWORD USING MISSING

TSS1611E DUPLICATE VALUES NOT ALLOWED FOR COMPARE AND USING ACIDS

Archive Messages

TSS1593E KEYWORD INTO IS MISSING OR INVALID

TSS1594I ARCHIVE FUNCTION SUCCESSFUL

TSS1595I ARCHIVE FUNCTION FAILED IN TSSxxxxxx

TSS1598E ARCHIVE AFILE PROCESSING FAILED – REASON CODE = NN

TSS1600E KEYWORD ARCHIVE IS MISSING

TSS1603E THE INTO DATASET MUST BE A PDS - REASON CODE = 12

TSS1604E OUT OF SPACE - PDS TOO SMALL

Audit Match Messages

TSS7285I Auditing disabled by MATCHLIM for TYPE=<resclass> RSRC=<resname>

TSS7286I Auditing disabled by MATCHLIM for ACID <acidname>

TSS7287E Audit Match Limit Internal Error - Processing deactivated

RENEW Command Messages

TSS1535E PCICC AND ICSF ARE MUTUALLY EXCLUSIVE FOR THIS FUNCTION

TSS1599E Cannot overwrite existing LABLPKDS with RENEW command

Run CA Top Secret as a Subsystem Messages

TSS1610E Not Authorized to use NOPW keyword

TSS2060I Subsystem xxxxxxxx is Waiting for TSS Initialization

TSS2061E Startup override options exceed maximum length and are ignored

TSS2062I Generated start command: <start command>

TSS2063E KEYWORD NOT IN PARM TABLE, KWD: XXXXXXXX

TSS2064E PARMLIB OPERAND ERROR FOR KEYWORD XXXXXXXX

TSS2065E INVALID PARM BUFFER ADDRESS

TSS2066E PARMLIB FILE NAME INVALID, NAME: XXXXXXXX

TSS2067E INVALID VALUE FOR SUBSYSTEM NAME

TSS2068E PARM DATA MOVE FAILED, KWD: XXXXXXXX

TSS2069I Subsystem xxxx is Active

Security File Requirements Messages

TSS1609E UNABLE TO UPDATE VSAM FILE - DRC=XX

TSS9155E VSAMFILE REQUIRED

TSS9156E NEWPWBLOCK FEATURE REQUIRED ON SECFILE

User Modeling Messages

TSS1601E KEYWORD USING IS MISSING

TSS1602E KEYWORD ACID IS MISSING

TSS1603E THE INTO DATASET MUST BE A PDS - REASON CODE = 12

TSS1604E OUT OF SPACE – PDS TOO SMALL

Miscellaneous Messages

TSS0501E INVALID SIGNWITH – USER CERTIFICATE CANNOT BE USED TO SIGN ANOTHER USER'S CERTIFICATE

TSS1558E Error returned from ICSF services. ICSF RC= rc - RSN = rsn

TSS1560E Input certificate contains non-RSA public key. Public key cannot be added to ICSF

TSS1561E Invalid or missing PKDS label. Public key cannot be added to ICSF

TSS1562E Key size of certificate requires PCI Cryptographic Coprocessor. Specify PCICC instead of ICSF

TSS1596E Invalid IDMAP data Rsn = xxxxxxxx

TSS1597E UTF8 Conversion Error, RC=ccc RSN=rrr

Note: The above message supports ID Propagation, a feature of z/OS 1.11.

TSS0341E ACID SPECIFIED IS INVALID FOR CROSS-AUTHORIZATION

Message Updates

The following messages were updated for CA Top Secret r15:

TSS0948E SAFCRCSF ICSF failure – NOT AUTHORIZED FOR CSFKEYS/XCSFKEY

TSS1535E PCICC AND ICSF ARE MUTUALLY EXCLUSIVE FOR THIS FUNCTION

TSS7111E NEW PASSWORD PHRASE CHANGE INVALID - reason

TSS7111E NEW PASSWORD CHANGE INVALID - reason

RENEW Command

The RENEW command function is a new command that renews a certificate.

Previously, renewing a certificate was a multiple-step process that required multiple commands. The RENEW command lets you renew a certificate with only one command, simplifying the process.

Note: The RENEW command can renew only certificates that CA Top Secret creates. RENEW cannot renew certificates that external certificate authorities create.

Because the RENEW command now exists, abbreviating the CA Top Secret RENAME command to the first three characters is no longer valid. Use the first four characters (RENA) in the abbreviation for RENAME.

Note: For more information about the RENAME and RENEW commands, see the *Command Functions Guide.*

Restricted Administrative Authorities

The new CASECAUT resource class allows for additional administrative authorities.

Users with no administrative authorities now can:

- Change certain password related fields for other users within their scope if they have the proper access to TSSCMD.USER.cmd.fieldname in the CASECAUT resource class
- Issue certain digital certificate keyring and token commands for users within their scope if they have proper access to entity TSSCMD.CERTUSER.function in the CASECAUT resource class
- Use the TSSUTIL, TSTRACK, TSSAUDIT, TSSCHART, TSSCFILE, TSSXTEND, TSSSIM, and TSSFAR utilities if they have the proper authority in TSSUTILITY.utilityname in the CASECAUT resource class.

For general information, see the *User Guide*. For more information on the required command and keyword authorities, see the *Command Functions Guide*. For information on required utility authorities see the *Report and Tracking*, *Troubleshooting*, and *Installation* guides.

Run CA Top Secret as a Subsystem

You can now start CA Top Secret early in the IPL process as a subsystem using the CAISEC00 parmlib member. This option is an alternative to starting CA Top Secret with SUB=MSTR from the command table SYS1.PARMLIB(COMMNDxx).

This option lets several members start the same task with different operands using MVS &SYSCLONE symbolic substitution.

For more information, see the *Installation Guide*.

SDN/SN.IDN Size Increase

The serial number and issuer's distinguished name (SN.IDN) field size and the subject's distinguished name (SDN) field size have been increased to accommodate field sizes of up to 1024 bytes. This allows CA Top Secret to handle larger certificates generated by external certificate authorities. 1024 bytes are allowed when the SDNSIZE control option is set to 1024.

For information about the SDNSIZE control option and migration requirements for this feature, see the *Control Options Guide*.

Security File Requirements

The CA Top Secret r12 and later VSAM file structure is now required to run CA Top Secret r15, and all future releases. Due to this VSAM file requirement, z/OS can no longer share secfiles with z/VM or z/VSE.

The NEW_PASSWORD security file feature must be displayed as active in order to use the security file with CA Top Secret r15, and all future releases. This is activated by default for security files created in r14 and later, or in r12 by running TSSXTEND with the NEWPWBLOCK keyword specified.

For more information, see the *Installation Guide*.

Security Call Suspension

CA Top Secret supports a new mechanism that suspends REXX subsystem security calls issued by IBM or third-party subsystems during IPL until CA Top Secret is fully initialized. CA Top Secret places the caller in a queue pending full security system availability. A highlighted message appears on the system console for the duration of the security call suspension. The message includes the name of the waiting subsystem.

Serviceability

CA Top Secret r15 includes a number of enhancements designed to increase serviceability and maintainability. Exploitation of CA Chorus™ Software Manager capabilities simplifies customer procedures for product installation and maintenance. Product serviceability is enhanced through new diagnostic capabilities which provide additional information such as the SMP/E FMID (function modification identifier) and RMID (replacement modification identifier) associated with problem modules. Availability of this information helps streamline the problem diagnosis process with CA Technical Support. Dump title and indicative dump contents have also been enhanced to provide (with accompanying CA Common Services support) greater technical diagnosis information, again, helping to streamline the problem diagnosis process with CA Technical Support.

Note: See common Services Information Solution RI16963 for Common services prerequisites.

Virtual Storage Constraint Relief (VSCR)

Kerberos in-core tables are now allocated in 64 bit storage whenever this option is available. This results in less ECSA storage utilization.