



eTrust CA-Top Secret Security Release 3.0 for VSE

Security, Control, and Audit Solution

eTrust™ CA-Top Secret® Security for VSE is a comprehensive security solution for protecting today's enterprise server environment. Through user validation and resource access control, it ensures a secure operating environment for VSE/ESA, subsystems and applications. eTrust CA-Top Secret employs CA's Standard Security Facility (CAISSF) technology, compliance with the System Authorization Facility (SAF), allowing centralized or decentralized security administration and auditing, through a single security mechanism.

Operating Environment

All IBM Supported releases of VSE/ESA

Highlights:

- Protects data and resources by default
- Easy to understand user-to-resource architecture matches your organization
- Extensive auditing and reporting facilities
- Supports decentralized, centralized, or mixed administration from VSE, VM, and OS/390 environments
- Provides full support for CICS/VSE 2.3 and CICS Transaction Server 1.1
- Provides the ability to protect VSE data sets, including VSAM files from deletion and creation
- Provides the ability to protect DL/1 resources, using external security rules
- Provides the ability to protect VSE system libraries at the member level
- Full database sharing and identical user interface with eTrust™ CA-Top Secret® for z/OS and OS/390 and eTrust™ CA-Top Secret® for VM
- Automatic synchronization of security information across networked processors through the Command Propagation Facility (CPF) allows users to be identified with a single Accessor ID (ACID)
- Automatic synchronization of passwords and user status across eTrust CA-Top Secret and Unicenter® Network and Systems Management systems
- High performance design maximizes efficiency of CPU, storage utilization, and I/O
- The eTrust CA-Top Secret cache facility minimizes memory and I/O usage and improves response time
- Supports IBM PassTicket processing

eTrust CA-Top Secret Security Release 3.0 for VSE

Currently Available – General Availability (GA)

Major Enhancements:

Improvements in Usability

- **Record Level Protection for CICS**

Record Level Protection (RLP) is an extension to FCT Resource Checking, providing the ability to protect records within a CICS file and fields within a record. Boolean logic is available to easily restrict access based upon a value or range of values contained in a field.

- **Screen Level Protection for CICS**

In addition to protecting data at the record and field level, eTrust CA-Top Secret can also protect data from being displayed or updated on a user's terminal with Screen Level Protection (SLP). SLP is used to protect fields within a CICS map.

- **Refresh of the Security Environment**

Single and multi-user address space users no longer have to logoff or restart for security changes to take effect. When authorization changes are made to logged-on users, the security environments can now be immediately updated. In multi-user address space environments, all occurrences of the user ID are refreshed with a single command.

- **CPF Recovery**

Release 3.0 allows you to delete pending commands for a particular node from the CPF Recovery file. This is especially useful to selectively remove commands targeted to test systems that are only occasionally active or systems that have been removed from CPF sharing.

- **Password Re-verification on OTRANS**

Password re-verification is available for ownable transactions (OTRANs). This enhancement facilitates migration from LCF to OTRAN protection of commands and transactions.

- **Application Interface**

Release 3.0 allows the application to specify the size of the return area, allowing greater amounts of information to be returned on RESLIST, FACLIST and FDT calls.

- **Elimination of USERMODS**

The OPTIONS control option streamlines the installation process for those sites who in the past used optional USERMODS. Sites can now easily activate special processing, formerly provided by USERMODS, by simply specifying the appropriate values in the control option. Values and descriptions of special processing and the equivalent USERMOD are fully documented.

Administrative Enhancements

- **Extended Administrative Scope**

Administrators can now be authorized to assign PROFILES outside of their scope. This allows enterprises greater flexibility in implementing eTrust CA-Top Secret and faster response to organizational changes.

- **Adding Profile FIRST**

A FIRST keyword has been added, enabling administrators to add a profile first in the profile list.

- **Selective Revokes**

Release 3.0 allows an administrator to selectively REVOKE PERMITs to the same resource within a record based on entity name and selective criteria, such as allowed access level, source, time of day, and day of week.

- **Duplicate PERMITs Prohibited**

Release 3.0 verifies that an identical authorization within a record does not exist before processing a TSS PERMIT command.

- **PERMIT by SYSID**

The new SYSID keyword may be included on a PERMIT or when adding a FACILITY to a user. This provides granularity by system for all resources and facilities.

- **Masking Enhancements**

In Release 3.0, the security administrator can modify each resource class to support masking. This extension of masking is equivalent to that which is available for data set masking.

- **WHOHAS FACILITY**

A TSS WHOHAS can now be issued for a facility. In addition, information is now returned for all owned resources under a specified prefix.

- **PERMIT Accountability**

ADMINBY is a new control option, which, when in effect, time and date stamps all permissions and all facilities added to a user or PROFILE, identifying the ACID who granted the permission. This information is available to an administrator via the TSS LIST command.

- **Calendar/Time**

Calendars are now provided to restrict access to a specific resource over an entire year. Calendars can be established to reflect site-specific events, such as company holidays. Time is now divided into 15-minute intervals. Multiple time slots can be utilized within a 24-hour period.

- **TSS LIST by Prefix**

The TSS LIST command has been enhanced to list all ACIDs that begin with a specified prefix.

- **Enhanced Status Display**

The STATUS control option has been enhanced to allow a specific option to be displayed when issuing TSS MODIFY(STATUS). Options available are BASE, VERSION, FACMODE, PASSWORD, and CPF.

- **EXPDAYS Control Option**

The EXPDAYS control option causes a TSS ADD or PERMIT command, when used with the FOR and UNTIL parameter, to be displayed beyond the expiration date. This allows a security administrator to see temporary authorizations beyond their expiration dates.

Performance Enhancements

- **Access Check Improvements**

Security File I/O has been reduced making access authorization checking and overall system throughput faster.

- **Additional Command Processors**

The number of available command processors has been increased from 2 to 10, to better manage throughput of command data.

- **ACID Index Performance**

In a shared Security File environment, eTrust CA-Top Secret Release 3.0 reads only those blocks modified by another security system, further reducing I/O and locktime on the Security File.

For more information, please contact your local Computer Associates Client Relationship Manager, or visit us at ca.com.