



## eTrust™ CA-Top Secret® Security r1.6 for VM

eTrust™ CA-Top Secrets Security for VM (eTrust CA-Top Secret) helps you take full advantage of the reliability, scalability and cost-effectiveness of the mainframe by providing innovative, comprehensive security for business transaction environments — including VM, VM minidisks, UNIX System Services for VM, CMS SFS files and mainframe Linux.

### Key Features at a Glance

- Inclusive User Management
- Data and Resource Management
- Auditing and Monitoring
- Separation of Administrative Functions
- Administration Diversity
- Comprehensive Security

### What's New

- Administration Advancement for UNIX
- Extended Security Capabilities for Linux
- Command Propagation Facility Enhancement
- Enhanced Password Controls
- Parameter File Sharing
- License Management Program Enhancement



Computer Associates®

### Enterprise Security Needs

Information security is critical to helping ensure business efficiency and growth, deliver superior customer service and maintain information privacy. Today, almost every organization views technology as a strategic resource. In addition, companies are trying to gain a competitive edge by enabling easier, faster and more reliable access to products and services. There is also an increasing concern about the security issues that arise when establishing web links to valuable mainframe data. Furthermore, many organizations are forced to comply with government regulations, including the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley Act (SOX) and Gramm-Leach-Bliley Act (GLBA), as well as existing corporate policies and industry agreements.

With the introduction of new technologies for the mainframe, including hardware, networks and operating systems, new security concerns are developing at a rapid pace. To stay abreast of today's challenges, organizations must strengthen security, streamline administration and provide enhanced auditing capabilities.

### Security You Can Trust

eTrust CA-Top Secret from Computer Associates International, Inc. (CA) protects your mainframe computer systems and data by controlling access to resources. It maps security closely to your organization through a unique and flexible configuration mechanism that automatically associates users to one or more roles. eTrust CA-Top Secret delivers

flexible, streamlined administration, helping you quickly and efficiently manage users and control resources. In addition, it lets you rapidly respond to changing business needs with minimum overhead.

eTrust CA-Top Secret lets your organization securely take advantage of the latest hardware, networking and operating system components offered for the mainframe. When combined with other eTrust™ Security Management solutions, eTrust CA-Top Secret also provides end-to-end control to help you meet your business and compliance requirements.

eTrust CA-Top Secret is delivered complete with flexible and powerful automatic logging facilities and extensive online monitoring capabilities. Authorized users are provided with a wide range of options for analyzing computer access activities and trends, and evaluating the “who, what and when” of access.

### Distinctive Features and Functionalities

**Inclusive User Management.** Individual accountability is the key to effective information security. Because many government regulations and corporate policies require separation of functions or duties, eTrust CA-Top Secret allows you to decide which policies are relevant. In addition, it enables you to implement the appropriate infrastructure.

- **Users.** eTrust CA-Top Secret provides easy-to-use administration functions that adapt to your organization's structure and procedures, and help you comply with regulations and laws. To eliminate the



```

CAKV-A001                TSS Create (Panel 1 of 5)                CA-TOP-SECRET
=====
ACID   >>>> _____ NAME   >>>> _____
LIST  >>>> -          WAIT   >>>> -          TARGET >>>> _____
PASSWORD >>>> -          TYPE   >>>> _____
DEPT  >>>> _____ DIVISION >>>> _____ ZONE   >>>> _____
FACILITY >>>> _____
PROFILE >>>> _____
FOR   >>>> -          UNTIL  >>>> _____
SOURCE >>>> _____ LT IME  >>>> _____
LANGUAGE >>>> -          TZONE  >>>> _____
USING >>>> _____

Indicate selection of attributes with an 'X'
AUDIT  >>>> -          MULTIPW >>>> -          NORESCHK >>>> -
CONSOLE >>>> -          NOADSP  >>>> -          NOSUBCHK >>>> -
DUPXTR >>>> -          NOATS   >>>> -          NOUMDCHK >>>> -
DUPUPD >>>> -          NODSCHK >>>> -          NOVOLCHK >>>> -
GAP    >>>> -          NOLCFCHK >>>> -          SUSPEND  >>>> -
O IDCARD >>>> -          NOPWCHG >>>> -          TRACE    >>>> -
MRO    >>>> -

```

Figure 1. eTrust CA-Top Secret Resource Administration.

time-consuming efforts needed to help ensure unique definitions for UNIX users, the next available group identification (GID) or user identification (UID) within a specific range can be assigned automatically.

- **Role-Based Security.** Through the use of profiles, eTrust CA-Top Secret allows role-based security to be implemented with little effort. In addition, it provides the flexibility to adapt to your organization’s changes.
- **Individual Accountability.** Each ID is protected by a password. Consistent password policies are enforced throughout your organization, strengthening the effectiveness of passwords and increasing information security.
- **System Entry.** eTrust CA-Top Secret controls entry into virtually all VM entities and applications.

**Data and Resource Management.** Your data center managers are responsible for helping to ensure the integrity of all data and programs stored on their computer systems. The loss of any data can potentially translate into the loss of corporate dollars (see Figure 1).

- **Protection by Mode.** eTrust CA-Top Secret safeguards against loss or abuse by protecting data by default when mode is set to “fail.” Other modes are available to phase in implementation.

- **Controlled Sharing of Data.** eTrust CA-Top Secret requires action to allow access to resources. This process enables you to know and control who has access to what.

**Auditing and Monitoring.** In many countries, several laws have been implemented that require organizations like yours to establish internal controls pertaining to computerized data.

- **Auditing.** eTrust CA-Top Secret generates audit records for virtually any security-related event, including: starts and stops of the security system; commands to modify the running security system; successful or unsuccessful user system entry or exit; failed or audited access; changes to the security databases; and security-related VM events.
- **Reports.** eTrust CA-Top Secret provides a complete set of report generators that let you view and analyze your security event information. Online, real-time monitoring is also available.

**Separation of Administrative Functions.** While the implementation of security is very important, so is the responsibility for security administration. Restricting who can grant access and define your users is one of the cornerstones for effective security.



- **Decentralized or Centralized Administration.** eTrust CA-Top Secret provides several ways for you to separate security administration functions. For example, it provides you with different levels of authority over your users and/or resources. In addition, it can limit authority to security functions, areas or resources.
- **Changes to Security.** Standard reports display updates, additions, changes or deletions of any eTrust CA-Top Secret user or rule or other security records.

**Administration Diversity.** Without proper administration, there can be no guarantee that your security is correctly structured. To help meet your business requirements, eTrust CA-Top Secret includes flexible and powerful administration tools (see Figure 2).

- **Command Processing.** eTrust CA-Top Secret lets you administer security through multiple means.
- **Multiple CPU Security Administration.** In an environment with multiple system images, you can use the eTrust™ CA-Top Secret® Command Propagation Facility (CPF) to administer networked nodes from one single node.

**Comprehensive Security.** eTrust CA-Top Secret provides comprehensive security for VM resources across operating systems, subsystems, OEM software and databases.

- **Operating System Release Support.** eTrust CA-Top Secret supports new operating system versions as they become generally available.
- **Exploitation of New Releases.** eTrust CA-Top Secret takes advantage of new features and functionalities to provide enhanced security administration and management.

### What's New in r1.6

#### Administration Advancement for UNIX.

In each new product release, CA enhances and extends the administrative capabilities of eTrust CA-Top Secret.

- **UID and GID.** To increase the efficiency of defining UID and GID numbers for users within UNIX and mainframe Linux, support has been added to assign unique numbers automatically and to show which numbers are already assigned.

#### Extended Security Capability for Linux.

eTrust CA-Top Secret provides extended and flexible security capabilities for the open source architecture, allowing you to authenticate users primarily on Linux systems.

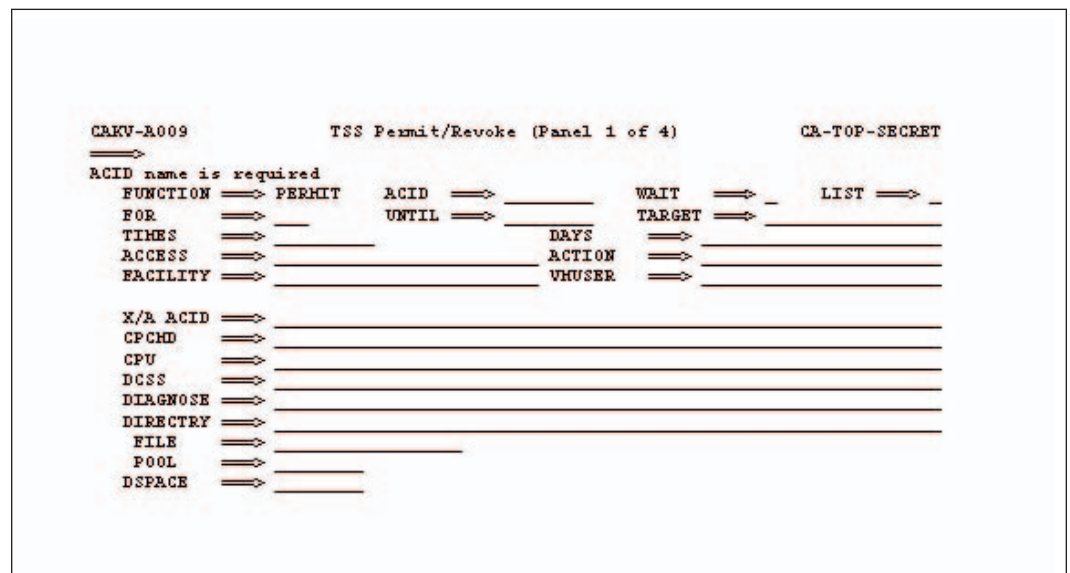


Figure 2: eTrust CA-Top Secret Administrative Panel.



- **Pluggable Authentication Module (PAM) Support.** eTrust CA-Top Secret supports an interface for mainframe Linux users through the use of PAM for user authentication and system access. New Linux user names and Linux nodes can also be administrated. Case-sensitive and long user names are supported, and Linux nodes can be defined to the eTrust CA-Top Secret database as NDT node elements for administration.

**CPF Enhancement.** CPF node definitions can now be defined in the NDT record in the eTrust CA-Top Secret security file. CPF nodes are grouped by system ID. The system ID entry contains the global system defaults for CPF processing. By incorporating CPF global defaults and CPF node definitions into the security file NDT record, CPF nodes can be administered via the TSS command processor instead of being statically defined at startup.

**Enhanced Password Controls.** eTrust CA-Top Secret passwords that were already strong have been further enhanced, enabling you to improve the selection of secure passwords.

- **New Controls for Password Content.** Two new options have been added to the new password (NEWPW) control options to require at least one alphabetic character or at least one numeric character.

**Parameter File Sharing.** Support has been added to use an alternate TSSVM parameter file when sharing a system-resident minidisk among multiple systems. You can now specify an alternate file name to be used for IPL.

**License Management Program (LMP) Enhancement.** License management is important to help ensure only properly licensed products are being utilized. Enhancements to the processing of key validation within the product also help ensure valid keys are established and that the product will initiate properly.

- **LMP Key File.** An enhancement to LMP has been made to allow multiple system keys to exist in a single LMP key file. This allows multiple systems to share a single eTrust™ CA-Top Secret® Security for VM service machine system-resident disk. LMP checking will find the appropriate key for each CPU.

**For more information, visit [ca.com](http://ca.com)**



Computer Associates®