



eTrust® CA-Top Secret® Security r9 for z/OS

eTrust® CA-Top Secret® Security for z/OS (eTrust CA-Top Secret) provides innovative, comprehensive security for business transaction environments, including z/OS UNIX and mainframe Linux—enabling your business to fully realize the reliability, scalability and cost-effectiveness of the mainframe. In conjunction with CA distributed security solutions, eTrust CA-Top Secret helps secure your entire enterprise.

Key Features at a Glance

- Comprehensive Security
- Auditing and Monitoring
- Inclusive User Management
- Data and Resource Management
- Separation of Administration Functions
- Security Information Sharing

What's New

- Multilevel Security (MLS) Auditing
- Statistical Gathering
- Report Enhancements
- Password Features

Supported Environments

- z/OS
- z/OS.e
- z/OS UNIX
- Mainframe Linux

Enterprise Security Needs

Information security is critical to achieving business efficiency and growth, superior customer service and information privacy. Today, organizations view technology as a strategic resource and seek to gain competitive advantage by enabling easier, faster and more reliable access to products and services. There is increased concern about the security issues that arise when establishing web links to valuable mainframe data. Many organizations are also required 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 rapidly developing. 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® protects your mainframe computer systems and data by controlling access to resources. It closely maps security to how you manage your organization using a flexible configuration mechanism unique to CA 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 enables rapid, cost-effective response to changing business needs.

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

eTrust CA-Top Secret is designed to seamlessly integrate with new versions and releases of subsystems (such as CICS, IMS and DB2) and technologies (such as Sysplex) upon their availability, which will protect your investments as your business moves ahead with its objectives and applications.

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

Distinctive Features and Functionalities

Comprehensive Security. eTrust CA-Top Secret provides comprehensive security for z/OS resources across operating systems, sub-systems, OEM software and databases (see Figure 1).

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

Inclusive User Management. Individual accountability is the key to effective information security. Many government regulations and corporate policies require separation of functions or duties. eTrust CA-Top Secret lets you decide what policies are relevant and 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.

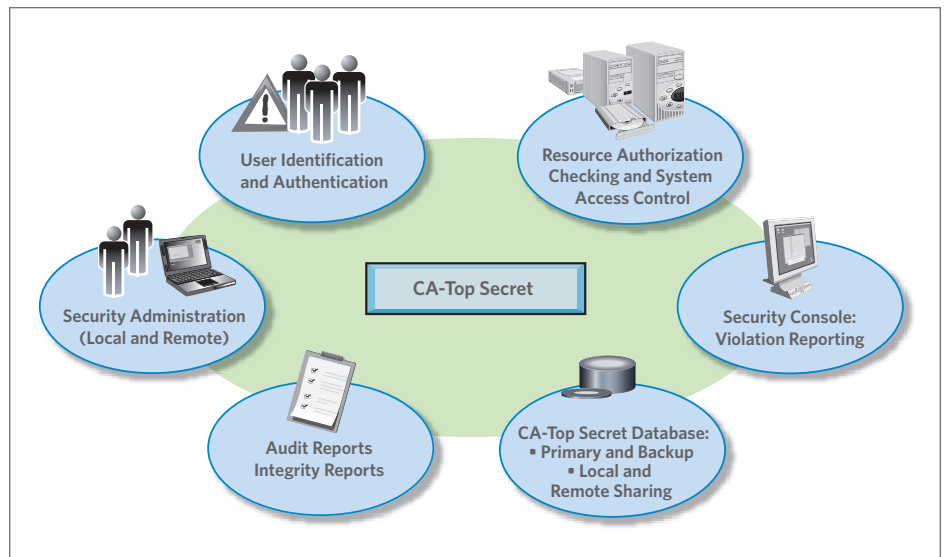


Figure 1. eTrust® CA-Top Secret® Overview.

To eliminate the time-consuming efforts needed to ensure unique definitions for z/OS UNIX users, the next available GID or UID within a specific range can automatically be assigned.

- **Role-Based Security.** Through the use of profiles, eTrust CA-Top Secret allows role-based security to be implemented with little effort and 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 organizations, strengthening the effectiveness of passwords and increasing information security.
- **System Entry.** eTrust CA-Top Secret controls entry into virtually all z/OS subsystems and VTAM applications, including TSO, Batch, z/OS UNIX, CICS, IMS, and DB2 UDB for z/OS. With the CA Pluggable Authentication Module (PAM) support introduced with eTrust CA-Top Secret release 5.3, this control extends to mainframe Linux.

- **Digital Certificate Generation.** To help you reduce the administration time and effort needed to support digital certificates, eTrust CA-Top Secret lets you generate, administer and process certificate requests and export keys.

Data and Resource Management. Your data center managers are responsible for ensuring the integrity of all data and programs stored on their computer systems. Any data loss can potentially translate into financial loss.

- **Protection by Mode.** eTrust CA-Top Secret helps safeguard against loss or abuse by protecting all data sets by default when mode is set to fail. Other modes are available to phase in implementation, i.e. User, Facility, Resource.
- **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.

- **UNIX Access Control List.** A control option called HFSACL allows you to turn support on or off for access control lists.
- **HFSSEC.** Allows for the control of all Hierarchical Files with predefined controls; i.e., TSS permission, instead of the ACL controls of native UNIX.
- **Advanced Data Erasure.** With the use of the AutoErase control option and table, selective datasets are overwritten with binary zeros when deleted. This feature provides true removal of data from DASD.

Auditing and Monitoring. Several laws in many countries require organizations to establish internal controls pertaining to computerized data. eTrust CA-Top Secret includes a variety of audit functions that provide the information and capabilities you need to monitor access and assess the propriety of access rights.

- **Auditing.** eTrust CA-Top Secret generates audit records for virtually any security related event, including start 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 z/OS UNIX events.
- **Reports.** eTrust CA-Top Secret provides a complete set of report generators that allow you to view and analyze your security event information. In addition, online, real-time monitoring is 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 a cornerstone for effective security. eTrust CA-Top Secret provides separation of security administration functions and duties, an additional management control that safeguards your systems and preserves the integrity of your security records.

- **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, and 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 and ease the administration process, eTrust CA-Top Secret includes flexible and powerful administration tools.

- **Command Processing.** eTrust CA-Top Secret allows you to administer security in multiple ways, including TSO, batch, CICS, IMS and eTrust® Admin.
- **Multiple Image Security Administration.** In an environment with multiple system images, you can send eTrust CA-Top Secret commands from one node to single or multiple nodes. This is accomplished via the eTrust CA-Top Secret Command Propagation Facility (CPF).

Security Information Sharing. To help reduce security administration, human error and costs, security information must be shared across a networked environment.

- **eTrust® LDAP Server.** This component provides a single interface for applications to request security services, including adding, updating and retrieving information. In addition, it can be used to securely perform user authentication on behalf of business applications running on z/OS and other platforms connected through TCP/IP.

- **LDAP Directory Services (LDS).** LDS provides flexible integration with existing schema definitions, eliminating the need for specialized interfaces to make security data accessible.
- **eTrust® Distributed Security Integration (eTrust® DSI).** This standalone daemon runs in the z/OS UNIX environment, independent of eTrust LDAP server. In addition, eTrust DSI allows applications on a Windows platform to issue calls to eTrust CA-Top Secret.
- **Linux on z/Series Support.** Pluggable Authentication Modules — (PAM) is an open source architecture that allows eTrust CA-Top Secret to act as an authentication server for one or more Linux systems, eliminating the need for redundant security administration to define users on a system-by-system basis.
- **IBM Policy Director (PDAS).** eTrust CA-Top Secret utilizes the common SAF interface to support customers usage of IBM Policy Director.

What's New in r9

Multilevel Security (MLS) Auditing.

Supporting today's need for more stringent auditing requirements, many of which are based on new government regulations, additional auditing capabilities for MLS now allow additional auditing of SECLABEL-protected data set and resource usage. This auditing can be selected at a global level (i.e., all users), or at a specific SECLABEL level. Further selection granularity is possible based on the access type (i.e., READ, CREATE, WRITE, CONTROL, UPDATE, SCRATCH, FETCH, ALTER).

Increased ACID Size. With an increased ACID size, a user is able to select the maximum size of an ACID at file allocation time. A maximum size of 512K is now allowed and the minimum, default size is 256K.

Statistical Gathering. Timely collection and analysis of performance and usage statistics is important in helping to maintain optimal system performance, operational efficiency, and overall system availability. With this information in hand, the installation can take note of increases in workload, administrative requests, and eTrust CA-Top Secret system usage as a whole and can use it to assist with capacity planning, workload balancing and more. As an option, eTrust CA-Top Secret can gather pertinent statistical information at periodic intervals and write it to the system SMF file, where it can be formatted by a new report program. The collected information includes information pertaining to SYSPLEX, CACHE, CPF, security database input/output operations (I/O) and number of security calls processed through SAF/RACROUTE calls.

Rename Resource Class by Facility.

A single source resource class can be renamed into multiple target resource classes. You can replace internal class names with business-related resource class names to help track and report resource accesses and violations.

New Password Features. eTrust CA-Top Secret r9 has been enhanced to include support for passwords greater than 8 characters long. This feature will position eTrust CA-Top Secret to be able to process and administer passwords up to 128 characters long. At this time, the z/OS operating system does not support passwords greater than 8 characters long. This feature will position eTrust CA-Top Secret for when the operating system expands the password capability.

Extract from Profile. You can now extract data from the first profile in the users profile list. This allows you to define role profiles enabling groups of users to have the same extract information to perform job functions.

RDT Update by Command. eTrust CA-Top Secret Support can issue a PML for a new resource class with a check value. You can now create resource classes specified by support without having to generate a new TSSRTAB. This ensures that you have the same Resclasses and Rescodes.

Audit by Access Level. This feature will allow for the auditing of resources by the access level requested. For example, when auditing for write access is required only those accesses would be recorded and all others such as read accesses would be ignored.

Post Processing Exit Points. The installation exit has been expanded to include new post processing exit points for most resource checking. This will allow for additional processing of resource checks and return codes.

64-Bit Support. eTrust CA-Top Secret r9 is fully 64-bit compatible. Enhancements were engineered to the ENF/USS component, the HSF Security component, and to the USS callable services component. Some of the newer USS callable services are required to be 64-bit compatible.

For more information,
call 1-800-875-9659
or visit ca.com

