

***eTrust*[™] CA-ACF2[®] Security for z/OS**

Release Summary

r8



Computer Associates®
H00065-1E

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2004 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.



Contents

Chapter 1: New Enhancements

ACFRPTLL Report Generator	1-2
ACFXREF Cross-Reference Cleanup Utility	1-2
Automatic UID/GID Assignment Options	1-2
Command Propagation Facility	1-2
DB2 Enhancements	1-3
Enhancement Password Controls	1-3
Enterprise Identity Mapping Support	1-4
eTrust CA-ACF2 Event Filter Control for eTrust Audit (ETAUDIT)	1-4
Install Tape	1-4
JES3	1-4
LDAP Directory Services	1-5
Multilevel Security	1-6
Multiple Node Support for Linux	1-6
Product Guides	1-7
PDF Bookshelf	1-8
SYSPLEX Environment Advancements	1-8

New Enhancements

The Release Summary for eTrust CA-ACF2 Security for z/OS documents new enhancements and changes to existing features for r8. This chapter describes new features added to the product.

The following is a list of the new enhancements and changes to r8:

- ACFRPTLL Report Generator
- ACFXREF Cross-Reference Cleanup Utility
- Automatic UID/GID Assignment Options
- Command Propagation Facility
- DB2 Enhancements
- Enhanced Password Controls
- Enterprise Identity Mapping Support
- eTrust CA-ACF2 Event Filter Control for eTrust Audit (ETAUDIT)
- Install Tape
- JES3
- LDAP Recovery
- Multiple Node Support for Linux
- Multilevel Security (MLS)
- LDAP Directory Services
- Product Guides
- SYSPLEX Environment

ACFRPTLL Report Generator

The ACFRPTLL report generator uses the SMF records issued for eTrust CA-ACF2 recovery purposes to provide an updated activity report for the Logonid database. R8 includes an enhancement to the ACFRPTLL utility; by introducing two new report parameters, LIDFLDS and CHANGER. For more information, see the *Reports and Utilities Guide*.

ACFXREF Cross-Reference Cleanup Utility

The ACFXREF utility identifies invalid INCLUDE or EXCLUDE values associated with cross-reference records. The ACFXREF utility can be used to identify invalid logonids, access rules and resource rules. The ACFXREF utility was designed as a tool for eTrust CA-ACF2 DB2 users implementing secondary authids with regard to X-SGP processing. For more information on the ACFXREF utility, see the *Reports and Utilities Guide*.

Automatic UID/GID Assignment Options

To increase efficiency of defining UID and GID numbers for users within z/OS UNIX and mainframe Linux, support has been added to automatically assign unique numbers and to show which numbers are already assigned. The AUTOIDLX record defines options for the automatic assignment of UID and GID values for PROFILE(USER), DIV(LINUX), PROFILE(GROUP), and DIV(LINUX) records. For more information on the AUTOIDLX record, see the “Maintaining Global System Options Records” chapter in the *Administrator Guide*.

Command Propagation Facility

Additional functionality has been added for CPF to propagate the login ID information and send user and password status changes between eTrust CA-ACF2 and eTrust™ CA-Top Secret® Security.

DB2 Enhancements

The DB2 SHOW command has been enhanced to display the mode setting of DB2 resources that are available for the release of the DB2 subsystem running. See the *Administrator Guide* for an example of the DB2 SHOW command.

Enhancement Password Controls

The already strong eTrust CA-ACF2 password controls have been further enhanced, allowing you to improve the selection of secure passwords. The following enhancements are now provided with eTrust CA-ACF2 r8:

- Password History – You can now optionally decide how many previous passwords are to be stored in history (up to 64 iterations). However, you may not reuse any previous passwords that have been stored. For more information on password history, see the “Maintaining Global System Options Records” chapter in the *Administrator Guide*.
- Global Password Controls – New fields have been added to hold values for global MAXDAYS and MINDAYS for password control. For more information on global password controls, see the “Maintaining Global System Options Records” chapter in the *Administrator Guide*.
- Mixed Case Support – The eTrust CA-ACF2 password controls have been enhanced to support z/OS UNIX and mainframe Linux uses of mixed-case passwords. Before setting the mixed case password controls on, read the section in the *Administrator Guide* titled “Considerations for Mixed-Case Passwords” *very carefully*.
- Bypass Aging of Temporary Passwords – An option to bypass the aging of temporary passwords has been added to eTrust CA-ACF2. A temporary password is a password that is set by a security administrator or account manager on behalf of another user and will expire at the next system entry. For more information on bypass aging of temporary passwords, see the *Administrator Guide*.
- Password Similarity Checking – A new field, PSWDSIM, has been added to the GSO PSWD record to add the ability to compare a new password to the current password to determine if they are too similar. PSWDSIM specifies whether password similarity checking is to be performed. For more information, see the “Maintaining Global System Options Records” chapter in the *Administrator Guide*.

Enterprise Identity Mapping Support

eTrust CA-ACF2 supports Enterprise Identity Mapping (EIM), which includes a default profile and new segments in the LDAPBIND and USER profile classes. In addition, it allows this information to be extracted. For more information on EIM, see the “Maintaining Global System Options Records” chapter in the *Administrator Guide*.

eTrust CA-ACF2 Event Filter Control for eTrust Audit (ETAUDIT)

There are 31 security event types that can be communicated to eTrust Audit. When all the events are selected, the volume of security event notifications may be significant and system performance may be impacted. The ETAUDIT record filters the eTrust CA-ACF2 security event notifications so that only the selected security events are communicated to eTrust Audit.

Install Tape

eTrust CA-ACF2 for DB2 1.2 is now available on the eTrust CA-ACF2 install tape. eTrust CA-ACF2 for DB2 provides protection against unauthorized destruction, disclosure, or modification of data. It protects DB2 resources by default and provides for the controlled sharing of resources. It also replaces the GRANT and REVOKE statements of native DB2 security with eTrust CA-ACF2 for DB2 rules that permit or deny access to DB2 resources.

JES3

Before r8, if a logonid was inherited when a JES3 job was submitted, an SVC call was not issued. However, in r8, an SVC call is now issued when a loginid is inherited. As a result, if you have user-installed exits on the system, JES3 processing may be adversely affected.

LDAP Directory Services

eTrust CA-ACF2 provides LDAP Directory Services, which allows security information to be accessible directly through LDAP-compliant, directory-enabled applications.

The following enhancements have been added to eTrust CA-ACF2 LDS functionality:

- LDS Recovery Enhancements – Recovery support has been added to help ensure LDS requests are transmitted to remove LDAP servers if the network link is not active. LDS requests are saved in the recovery file for transmission when the LDAP server is available.
- Control LDS Options Record Enhancements – The Control LDS OPTIONS record defines global system options available to LDS. For more information on the LDS Options Record see the “LDAP Directory Services (LDS)” chapter in the *Administrator Guide*.
- Control LDS LDAP Record Enhancements – The Control LDS LDAP record defines the LDAP servers in the network and information required to appropriately communicate logonid administrative information. For more information on the Control LDS LDAP Record, see the “LDAP Directory Services (LDS)” chapter in the *Administrator Guide*.
- eTrust CA-ACF2 Modify LDS Command Support – The Modify LDS Command Support enhancements include the following new commands:
 - Modify operator
 - LDS DEBUG
 - LDS NODEBUG
 - LDS ACTIVE
 - LDS NOACTIVE LDS
 - LDS REMOVE

For more information on the Modify LDS Command, see the “LDAP Directory Services (LDS)” chapter in the *Administrator Guide*.

- SHOW LDS Support – The SHOW LDS subcommand has been enhanced to display the new LDS status and options, the active LDAP records and the logonid field information mapped to the LDAP server. For more information on SHOW LDS, see the *Administrator Guide*.

- **SSL Support**—eTrust CA-ACF2 supports SSL technology and allows an SSL-enabled LDAP server to authenticate itself to eTrust CA-ACF2 and eTrust CA-ACF2 to authenticate itself to the SSL-enabled LDAP server. Highly sensitive information, such as passwords, is protected if your site chooses to exploit SSL technology. For more information on SSL, see the *Administrator Guide*.

Multilevel Security

Multilevel Security (MLS) is a security policy in eTrust CA-ACF2 that provides discretionary access control (DAC) protection mechanisms and includes mandatory access control (MAC). MLS is an optional layer of protection on top of DAC, which forces security classifications, called security labels, for virtually all users, data and resources in a system. Additionally, it validates all access based on these labels, regardless of permissions and ownership. MLS is less rigid than MAC, offering selective protection of data and resources based on your organization's individual needs. eTrust CA-ACF2 lets you activate MLS and implement security labels for the users, resources, and data that require a higher level of security.

For complete information on how to implement and administer MLS in eTrust CA-ACF2, see the *Administrator Guide* and the *Multilevel Security Planning Guide*.

Multiple Node Support for Linux

eTrust CA-ACF2 r8 supports multiple Linux definitions for users. An administrator can assign a different set of UID, GID, HOME, and PROGRAM values for a given user for each Linux node the user has access to. Additionally, options for the automatic assignment of UID and GID values may be specified on a per-Linux-node basis. For more information on defining Linux user profile records and automatically assigning UID and GID values for Linux users, see the *Administrator Guide* and the *Getting Started* for eTrust PAM Client for Linux for zSeries.

Product Guides

Computer Associates has adopted the use of Document Identification numbers (DID) to identify guides. The new numbering system provides you with an easy way to determine if a more up-to-date edition of the guide is available on SupportConnect. Each guide in the documentation set has a unique DID number. The DID number consists of six characters that identify the guide, followed by a hyphen, followed by two characters that identify its edition and the language in which it is written. For example, Release Summary H00065-1E identifies the first edition of the English version of eTrust CA-ACF2 Release Summary. When the next edition of this guide is published, the DID number is incremented to H00065-2E. The DID number appears on the cover page. The DID number, without the hyphen, also serves as an eight-character file name.

The following table lists each guide in the eTrust CA-ACF2 documentation set along with the DID number.

Guide Name	DID Number
Administrator Guide	H00053-1E
Auditor Guide	H00054-1E
CICS Support Guide	H00055-1E
Distributed Database Support Guide	H00056-1E
General Information Guide	H00057-1E
Getting Started	H00058-1E
Implementation Planning Guide	H00059-1E
IMS Batch Support Guide	H00060-1E
IMS Support Guide	H00061-1E
MAC Administrator Guide	H00062-1E
Messages Guide	H00063-1E
Multilevel Security Planning Guide	H00421-1E
Quick Reference Guide	H00064-1E
Release Summary	H00065-1E
Reports and Utilities Guide	H00066-1E
Reporting with Advantage™ CA-Earl Guide	H00198-1E
Understanding Mandatory Access Control Guide	H00067-1E
System Programmers Guide	H00068-1E

PDF Bookshelf

The PDF Bookshelf file, ACF80_TOC.pdf, lists all the guides included in the product documentation set and maps each guide title to its DID number. Both the guide title and DID number provide a link to the guide PDF file. Click on the link to open the PDF file for the guide. Each guide's PDF file includes a bookmark (called Bookshelf) that returns you to the Bookshelf file.

SYSPLEX Environment Advancements

The SYSPLEX environment for eTrust CA-ACF2 has been enhanced to optimize couple facility capacity and performance.

- **Optimized Performance** – eTrust CA-ACF2 is now geared toward loginids to help you optimize performance. The element size has been reduced, which minimizes the amount of storage each time a loginid is written to the structure. However, it still allows for rules up to 32K to be written to the structure.
- **Threshold Value Specification** – Two options have been added to the GSO SYSPLEX record. You can now specify a full threshold value as well as what action you would like eTrust CA-ACF2 to perform when that threshold is reached.
- **Updated SHOW SYSPLEX Command** – The SHOW SYSPLEX display has been updated to give you more information on the structure. You can use this information to determine if your structure has been sized appropriately for the system usage at your site.