

White Paper



Mainframe Security Entitlement Cleanup

February 2006

Table of Contents

Executive Overview	3
Introduction	3
1. Regulatory/Statutory Remediation	4
2. Responds to the U.S. DHS Advisory	4
3. Counteracts Ongoing Accumulation of Entitlements Due to User Job Changes and Internal Corporate Restructuring or Acquisitions.....	4
4. Reduces System and Administrative Security Overhead	4
5. Assists with Security Recertification	5
6. Addresses Cleanup of Non-Employee Contractors and Consultants	5
7. Addresses Non-Human Process IDs that Often Pose Greatest Threat.....	5
8. Aids Development and Refinement of Role-based Security	5
9. Return on Investment (ROI): Automated Versus Manual Cleanup	5
10. Provides Customers with a Programmatic, Consistent, Manageable, Policy Based Solution	6
Technology Details	6
Component Overview	7
Tracking Database.....	7
Database Examples	7
Database Load Utility.....	9
Maintask	9
Security System Interface	9
Report and Command Generator	9
Conclusion	11

Executive Overview

Mainframe security databases accumulate obsolete user IDs and entitlement definitions which maybe valid but not appropriate for an individuals role. This creates uncertainty, risk and greater potential for security exposure. It also creates an unnecessary burden for administrators and the system. More so, increasing regulatory, statutory, audit and staffing pressures are bringing new concerns and mandates to address the problem of excessive security entitlements.

eTrust® Cleanup is a technology that provides easily automated, virtually unattended and continuous cleanup of mainframe security databases CA-ACF2, CA-Top Secret and IBM's RACF. Operating as a started task, eTrust Cleanup identifies and removes entitlements that are obsolete, unused, or redundant. eTrust Cleanup deploys within a day and is intended for those lacking time and resources to devote to security compliance. eTrust Cleanup offers an immediate and substantial response to increasing the regulatory, statutory, audit, compliance, privacy and staffing pressures.

eTrust® Cleanup:

1. Provides regulatory remediation for the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Each of which mandate or underscore the removal of unwarranted, unjustified and excessive entitlements.
2. Responds to the U.S. Department of Homeland Security (DHS) advisory issued to U.S. financial firms warning of terrorism threat to U.S. mainframe systems citing protective measures include ensuring that individuals do not have entitlements beyond that needed.
3. Counteracts ongoing accumulation of entitlements due to user job changes and internal corporate restructuring or acquisitions.
4. Reduces system and administrative burden.
5. Assists with security recertification that increasingly exceeds human comprehension, capacity and capabilities.
6. Aids security and HR processes that may neglect non-employee contractors and consultants.
7. Addresses non-human process IDs that often pose greatest threat.
8. Aids with the development and refinement of role-based security.
9. Return on investment (ROI): Automated versus manual cleanup efforts and costs.
10. Provides a programmatic, consistent, manageable, policy based solution for the removal of unused user IDs and inappropriate entitlements within the mainframe security databases.

Introduction

Over a period of time, security databases accumulate unused, obsolete user IDs and entitlements as well as valid but inappropriate entitlements. There are three basic reasons for this accumulation. First, users gain unneeded entitlements due to job changes and one-time requests. When new entitlements are added, old entitlements are seldom removed because users transition rather than cutover cleanly to a new position. Second, obsolete entitlements accumulate in two forms over time: entitlements to resources that no longer exist, and redundant or unused entitlements. Third, while user IDs are typically deleted when employees depart, the deletion may not catch every system and every secondary or alternate ID defined within the mainframe environment, nor are the entitlements to the ID removed.

These problems pose an increasingly important issue for mature security environments and can hamper both security administration and the performance of the systems security product. They can also create uncertainty, risk, and greater potential for security exposures. Until now, administrators have simply had no tools to resolve these problems. This is why eTrust Cleanup is needed. Discussed in greater detail, are the issues and benefits of using eTrust Cleanup:

1. Regulatory/Statutory Remediation

Federal regulation, consumer privacy requirements and the need for increased security post September 11, 2001, fuel increasing emphasis on information security.

- The SOX regulation mandates improved accounting oversight and assurance. Public firms are minimally expected to reassess and recertify the entitlements and integrity of systems primary to corporate financial reporting including the removal of entitlements beyond that needed. For more information, see sarbanes-oxley.com/
- GLBA mandates significant information privacy improvements for U.S. financial firms. Title V of GLBA mandates public disclosure and assurance of privacy practices and underscores need to remove unwarranted, unjustified and excessive entitlements. For more information, see ftc.gov/privacy/glbact/

- HIPAA also mandates improved information privacy emphasizing health care and patient information. HIPAA includes penalties and fines, not just for those who commit inappropriate access, but also those inappropriately allowed such exposure. Firms managing such information must remove excessive entitlements. eTrust Cleanup directly addresses these by identifying those entitlements that are not used and marking them for deletion from the security database. Cleanup provides commands to accomplish the removal of the user IDs or entitlements as well as a recovery set of commands to restore the entries if needed. For more information, visit hhs.gov/ocr/hipaa/ and hipaadvisory.com/

2. Responds to the U.S. DHS Advisory

During 2003, DHS privately issued an advisory to U.S. financial firms warning of terrorism threats to main-frame systems. The DHS advisory recommended the implementation of protective actions and cited eight specific protective measures including item five to “ensure individuals do not have access beyond that needed.” eTrust Cleanup directly responds to this cited protective measure by removing entitlements that are unused, obsolete and excessive. The DHS advisory is privately and separately available and it best provides more information. The DHS Information Analysis and Infrastructure Protection watch offices may also be contacted at: 1-202-323-3205, 1-888-585-9078 for private citizens and companies; 1-703-607-4950 for the telecom industry; and 1-888-282-0870 for federal agencies and departments.

3. Counteracts Ongoing Accumulation of Entitlements Due to User Job Changes and Internal Corporate Restructuring or Acquisitions

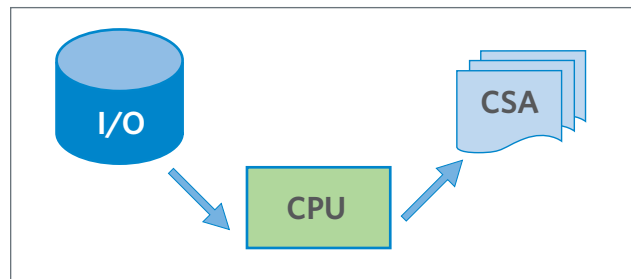
Security databases accumulate unused, obsolete and excessive user IDs and entitlements. There are three primary reasons for this:

- **Users gain unneeded entitlements and access groups.** Job changes and one-time requests ultimately cause users to gain entitlements (such as permissions and rules) and access groups (CA-Top Secret® Security profiles, CA-ACF2® Security rule sets and IBM RACF groups). When new entitlements are added, old entitlements are seldom removed because users transition rather than cut hard to new positions, leaving it unclear at what time old entitlements can be removed. *eTrust Cleanup solves this by monitoring all entitlement grants and reporting when entitlement is no longer used and safe to remove.*

- **Obsolete entitlements accumulates.** Two forms of obsolete entitlements collect over time. There are obsolete entitlements that refer to file names, transactions or other resources that no longer exist. These are obviously obsolete. However, there is often seemingly valid access that is in fact obsolete because it is redundant, simply unused, or never hit due to user entitlements. eTrust Cleanup removes both these forms of obsolete entitlements.
- **Inactive user IDs accumulate.** Typically, user IDs are deleted when employees depart. This deletion may not catch every system and every secondary or alternate ID the user may have had. Beyond this, cleanup is seldom done for IDs used for batch processing, started-tasks, CICS, terminals, consultants and contractors. The main reason for this is that “last use” dates reported for an ID are often unreliable and can cause a cleanup catastrophe if vital production IDs are misjudged as unused and deleted. eTrust Cleanup uses monitoring — not “last use” dates — and can correctly identify and remove all forms of unused IDs.

4. Reduces System and Administrative Security Overhead

Both the system and the security administrator are hampered by unneeded entitlements, access groups and user IDs that accumulate within a security database over time.



The overhead generated by the security system will generally improve linear to cleanup of the security database. When users have twice as many connected entitlements as they actually need, or when an access group has twice as many entitlements as its needs, it means the security system has to perform twice the I/O it needs to retrieve the data, twice the memory to store it and twice the CPU-time to search it. The security system doesn't know that the entitlements it searches will never be used. The system has to read them, store them, and step through them again and again — never using them. Linear savings are stated based on the argument that if you eliminate half the entitlements for a file, the security overhead to access the file will generally be reduced by half.

For the security administrator, savings while performing security cleanup can be calculated. There are also day-to-day savings, though these are not easy to dollar cost. Administrators certainly benefit when they manage less users and less entitlements, and more so, when they know and trust that entitlements seen are valid and actively used — knowing it would otherwise be removed. Auditors similarly benefit, but auditing savings in dollars are also indeterminate.

5. Assists with Security Recertification

Auditing requirements and regulations now require some companies to conduct a regular security recertification or entitlement review. Typically, entitlement lists are distributed for review and adjustments. In practice however, since few can validate what is and is not needed, the security recertification process most often results in little or no change to the entitlements. Further, two trends are making this worse. First, the increasing complexity and interdependencies of applications are making it more difficult to identify the data and programs to be secured for a user or application. Second, globalization is making user recognition and user name interpretation more difficult. The growing global workforce challenges staff certainty and clarity.

eTrust Cleanup monitors security activity and can identify the entitlements used versus unused for any user or application resource defined to the security file without the above hardships. Security recertification can be revolutionized once access lists can be provided that separate, break down and clearly show entitlements used versus unused for a user or application. Security recertification procedures can dramatically shift in their focus from “flag what to remove” to “flag what to keep.” Security recertification procedures could now state that entitlements shown unused will be removed unless claimed, representing a major improvement in the security recertification process.

6. Addresses Cleanup of Non-Employee Contractors and Consultants

While user IDs are typically deleted when company employees depart, removal and cleanup is less certain for consultants and contractors. Typically a batch job is regularly executed to synchronize the human resources and security databases and to identify departing employees. However, since consultants and contractors are not employees, they fall outside the normal employee termination process. As a result, consultant and contractor user IDs and entitlements can miss deletion if security is not notified upon their departure. eTrust Cleanup improves this by identifying and removing all forms of unused user IDs and entitlements. If consultants

and contractors fail to be removed from security upon their departure, eTrust Cleanup will identify and remove these user IDs and entitlements. A further benefit is that eTrust Cleanup does generate contingency commands when it creates deletion commands. Use of the contingency commands simplifies and speeds the recreation of IDs and entitlements for regularly returning consultants and contractors.

7. Addresses Non-Human Process IDs that Often Pose Greatest Threat

Security cleanup is seldom performed for non-human user IDs used for batch jobs, started-tasks, CICS, terminals, FTP and so on. These user IDs pose the greatest threat for mainframe hacking or abuse because they are often:

- Highly-authorized and privileged to bypass security checking
- Password exempt, needing no password
- Industry-known user ID names, for example, IBMUSER, OMVS, JES and HSM

Another reason cleanup seldom occurs for these user IDs is that the “last use” date reported for these IDs is often unreliable and can cause a cleanup catastrophe if vital production or system IDs are misjudged unused and deleted. eTrust Cleanup tracks usage and not “last use” dates to correctly and more accurately identify and remove unused IDs and entitlements. While this area is judged too sensitive and difficult for manual cleanup, non-human process IDs pose no special challenge or handling for eTrust Cleanup. eTrust Cleanup addresses IDs used for batch, started-tasks, CICS, terminal, FTP, operator consoles, NJE, RJE and so forth.

8. Aids Development and Refinement of Role-Based Security

Role-based security is being pursued by many companies, yet few tools exist to help define and refine entitlements within these roles. With eTrust Cleanup, reporting can be done to pinpoint the entitlement used and needed by any user or group of users. This reporting capability can greatly automate accurate development of role-based security entitlements. Subsequent cleanup only further benefits refinement of role-based implementations.

9. Return on Investment (ROI): Automated Versus Manual Cleanup

A cost comparison of automated versus manual security cleanup can be performed as follows: First, quantify the time needed for manual review and cleanup of a security entry (for example, a user ID or entitlement). The time needed for manual review of a security entry should be

the reasonable time needed to answer the following questions:

- Is the entry obsolete or valid?
- Is it redundant?
- Is it used or unused?
- What command removes the entry and what command would restore it?

Assuming five minutes per entry for manual cleanup and assuming \$40 per hour labor cost, a typical cost comparison can be computed as follows:

NOTE: Manual cleanup costs reoccur each time manual cleanup is performed.

Total Security Entries: 100,000
(15,000 user IDs + 5,000 access groups + 60,000 permissions + 20,000 group connections)

Manual Cleanup Cost: \$333,000
(100,000 entries x 5 minutes / 60 = 8313 hours x \$40 per hour)

eTrust® Cleanup: <\$65,000
(Per physical CPU)

10. Provides Customers with a Programmatic, Consistent, Manageable, Policy Based Solution

Here are typical findings that stem from one environment where eTrust Cleanup was used to monitor one small sample subset of 7,007 security entitlements surrounding one specific application for three months.

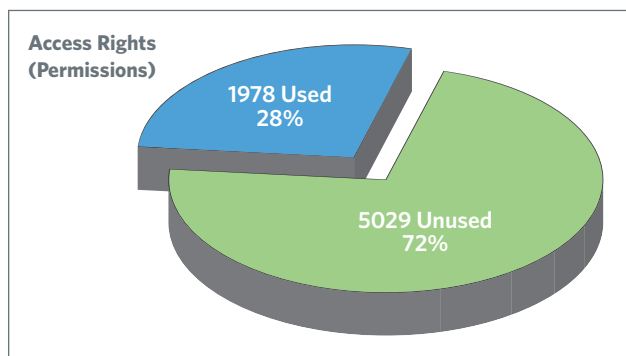


Figure 1. Obsolete permissions.

The above chart shows that 72% of the 7,007 entitlements monitored were found to be unused or excessive. This means that approximately 5,000 of the 7,000 permissions monitored were unused. While longer, prolonged monitoring might reveal usage of some infrequently needed entitlements, it is clear that most of the entitlements are unused, excessive, redundant or obsolete.

During that same period, eTrust Cleanup was also used to monitor the 19,690 group connections with the following results:

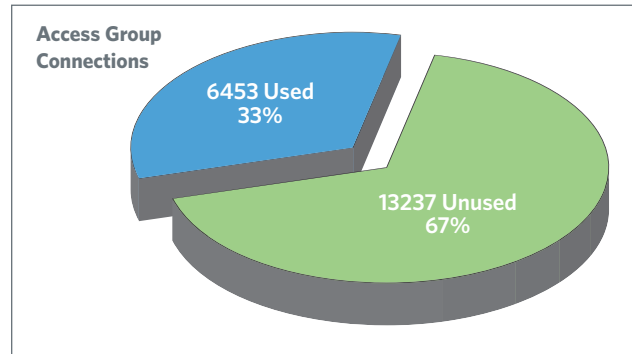


Figure 2. Obsolete group connections.

The above diagram shows that 67% of user access group connections were unused or excessive. It is obvious in this environment that most users could reduce and eliminate many of the access groups connected to their user ID. This would greatly narrow user entitlements and reverse the accumulation of entitlements by long-term users.

Technology Details

eTrust Cleanup from CA is easily automated to provide automatic, ongoing and comprehensive cleanup of mainframe security files for CA-ACF2, CA-Top Secret and IBM's RACF. eTrust Cleanup identifies and removes entitlements and user IDs once unreferenced beyond a specified threshold. In addition, it resolves the ongoing build-up of obsolete and excessive entitlements that accumulate within a security database over time. eTrust Cleanup fully deploys within a day.

Using eTrust Cleanup, you can:

- Identify and remove from individual users, entitlements and access groups no longer used.
- Identify entitlements (such as permissions and rules) actually used and create commands to remove those unused. This includes user-defined resources.
- Identify user IDs actually used and create delete commands for those unused. This is based on actual security usage, not reported "last-use" dates, which are often unreliable.
- Identify the IBM-RACF Groups and Profiles that each ID actually uses and create the RACF Commands to remove those that are unused.
- Produce reports detailing both used and unused entitlements.
- Generate commands to enact or restore security cleanup.

eTrust Cleanup monitors the security system in an independent and passive manner. As security checks complete, eTrust Cleanup tracks the user ID, group, and entitlement used by the security system to actually determine the access. This information is always readily available (although not normally seen unless a security trace is active). eTrust Cleanup takes this information, and using a highly efficient process, marks entries within its own tracking database that can be viewed and reported upon to identify and remove obsolete security information. eTrust Cleanup monitoring imposes no additional I/O to the security system.

NOTE: While eTrust Cleanup generates commands to remove unused security file entries, each site chooses when and how cleanup should occur. Cleanup can be automated or follow manual review processes. In addition, whenever building cleanup commands, eTrust Cleanup also builds contingency commands that can restore the IDs or entitlements.

- When used with CA-ACF2, you can identify active versus inactive logon IDs, rule sets and rules. This includes user-defined resource classes and NEXTKEY source and target rules.
- When used with CA-Top Secret, you can identify active versus inactive ACIDS, permissions and profile connections. This includes user-defined resources and the *ALL* record.
- When used with IBM RACF, you can identify active versus inactive user IDs, profiles, permissions, group connections and IBM RACF resource groups. Permission use is tracked down to each specific access-list entry, whether discrete, generic or conditional.

Component Overview

The following diagram illustrates the components of eTrust Cleanup. Each component is explained in the text following the diagram.

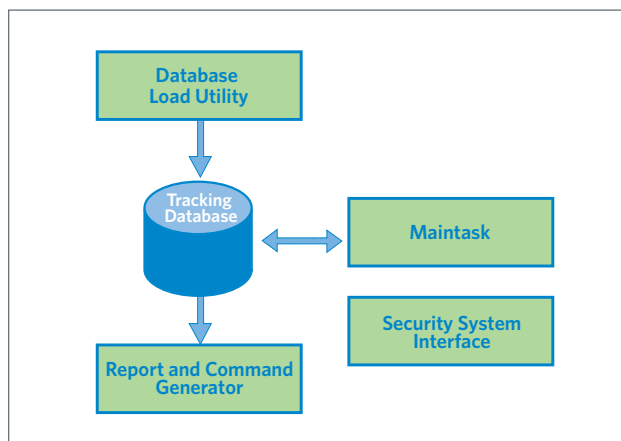


Figure 3. eTrust® Cleanup components.

Tracking Database

A database is used to efficiently manage the security information being monitored and tracked by eTrust Cleanup. The database depicts the security file user IDs and entitlements being tracked. The database is a sequential file with a columnar layout easily viewed using ISPF. Generally, the first column on each line shows the Julian date that the depicted security file entry was last used.

Database Example

The following figure shows an example of a tracking database used with CA-ACF2:

REFDATE	CLASS	KEY	
01.031	DSN	\$KEY(SYS1)	*LOADED=01.018
01.031		PARMLIB UID(systems) R(A) W(A) A(A) E(A)	
01.031		PARMLIB UID(*) R(A)	
		ZZ.OLD.PARMLIB	
01.031	RFAC	\$KEY(BPX.SUPERUSER) TYPE(FAC)	*LOADED=01.018
01.031		UID(*) PREVENT	
01.031	RFAC	\$KEY(BPX) TYPE(FAC)	*LOADED=01.018
		SUPERUSER UID(*) PREVENT	
01.031		- UID(stc) SERVICE(READ) ALLOW	
01.031		- UID(*) PREVENT	
	USER	ASTRO3 SUSAN SMITH	*LOADED=00.246
01.012	USER	CICSID PROD AOR REGION	*LOADED=00.010

The following figure shows an example of a tracking database used with CA-Top Secret:

REFDATE	USERID	CLASS		
05285	CLNUS01	USERID	CLEANUP USER 01	*LOADED=05234
	CLNUS01	PROFILES	CLNPPRO1 05285	
05285	CLNUS01	PROGRAM	TSSAUDIT	
05285	CLNUS01	TSOAUTH	ACCT	
	CLNUS01	TSOPROC	TSOPROC	
	CLNUS01	DATASET	MASTER	
05285	CLNUS01	OTRAN	CEMT	
05235	CLNUS02	USERID	CLEANUP USER 02	*LOADED=05234
05235	CLNUS02	TSOPROC	PROC395	
	CLNUS02	DATASET	SYS1.PARMLIB	
05285	CLNPPRO1	PROFILE	CLEANUP PROFILE 01	*LOADED=05234
	CLNPPRO1	USERLIST	DB2SYNC1	CLNUS01
05285				
05285	CLNPPRO1	DB2PLAN	A3999	
	CLNPPRO1	DB2DBASE	DBASE1	
	CLNPPRO2	PROFILE	CLEANUP PROFILE 02	*LOADED=05234
	CLNPPRO2	USERLIST	DB2SYNC1	CLNUS01
	CLNPPRO2	DB2SYS	MONITOR1	

The following figure shows an example of a tracking database used with IBM RACF:

REFDATE	USERID	CLASS	NAME	
03131	IXGLOGR	USERID	SYSTEM LOGGER TASK	*LOADED=03063
	IXGLOGR	GROUPS	OMVSRP 03131 STCGRP	STGADMG
	IXGLOGR	FACILITY	IXLSTR.LOGREC_P*	
	IXGLOGR	FACILITY	IXLSTR.OPERLOG_P*	
03131	IXGLOGR	DATASET	TSO.SYSPLEX.OPERLOG.*	
	IXGLOGR	DATASET	TSO.SYSPLEX.LOGREC.*	
03130	DPGRACF	GROUP		*LOADED=03063
	DPGRACF	USERLIST	CP25649 CP27735	D80721C E25132B
	DPGRACF	USERLIST	E31104X E31106D 03130	E31109C E31121D
	DPGRACF	USERLIST	E31124B E31125B	E44000A 03130 E44001F
03130	DPGRACF	ACCTNUM	SEC	
	DPGRACF	APPL	A56XTV4S	
	DPGRACF	FACILITY	VRA\$.**	
	DPGRACF	FACILITY	VRAADM\$.VARIABLES	
	DPGRACF	FACILITY	VRAADM\$.VRC.ADMIN	
	DPGRACF	FIELD	USER.TSO.*	
03130	DPGRACF	TSOAUTH	ACCT	
	DPGRACF	DATASET	BET2563.*	
03130	DPGRACF	DATASET	CATALOG.*	
	DPGRACF	DATASET	CATALOG.INTER*	
	DPGRACF	DATASET	CATALOG.TESTDEV*	
03130	DPGRACF	DATASET	CATALOG.TSO.*	
03131	*PROF*	USERID	DEFINED BASE PROFILES	*LOADED=03063
	PROF	ACCTNUM	SAP	
03130	*PROF*	ACCTNUM	SEC	
	PROF	APPL	A56XTV4S	
	PROF	FACILITY	IXLSTR.LOGREC_P*	
	PROF	FACILITY	IXLSTR.OPERLOG_P*	

Database Load Utility

A database load utility is used to identify and load the security information to be tracked by eTrust Cleanup. All or any portion of a security database can be loaded and tracked. The database load utility can be executed anytime against an existing and active tracking file to add, reload or delete items. The eTrust Cleanup tracking database can be shared across systems that share the security file.

Maintask

A maintask is used to perform security monitoring as required by eTrust Cleanup.

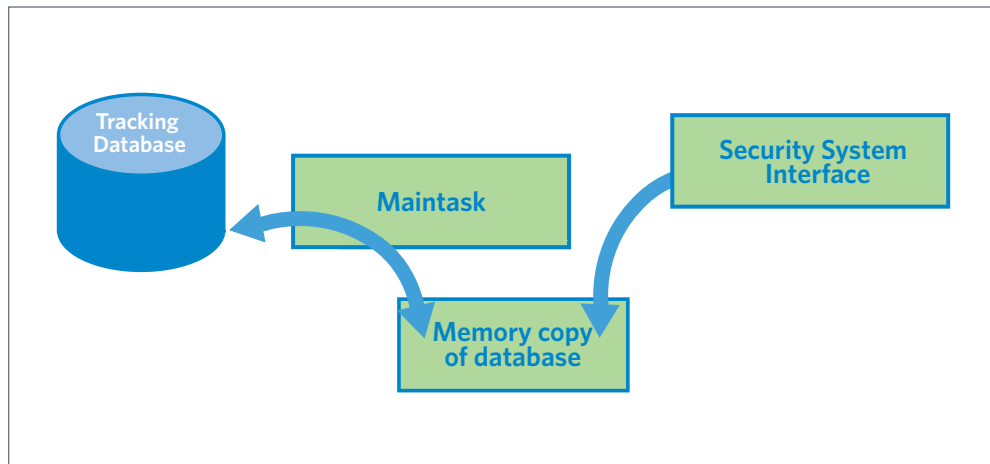


Figure 4. Maintask overview.

The maintask executes continuously as a started-task and provides several functions as follows:

- Upon startup, the maintask loads the tracking database into private memory. For efficiency, an OS/390 Scope=Common Dataspace is utilized.
- Additionally upon startup, the security system interface is loaded into common memory and activated. This activates security monitoring and begins the highly efficient updating of entries within the memory copy of the tracking database.
- Thereafter, and upon regular thirty minute intervals, the memory copy of the tracking database is rewritten to disk. Note, that an operator modify command can also be issued to manually initiate this function at any time.
- At midnight, the memory copy of the database is released, recreated and reloaded. This is done for integrity purposes and to allow recognition of newly loaded items.

- Upon operator requested shutdown, the security system interface is deactivated, the memory copy of the database is written to disk a final time, and the maintask ends.

Security System Interface

A security system interface is loaded and activated upon startup of the eTrust Cleanup maintask. The security system interface:

- Represents a small extension to the normal security check process and executes as each security check completes.
- Is passive and only performs monitoring.
 - Examines the user ID and entitlement involved with each security request and updates, if needed, the corresponding entry within the memory copy of the tracking database.
 - Does not issue I/O, WAIT or SVC requests.
 - Contains ABEND protection that immediately ends monitoring in the event of any problems.
- Is highly efficient and produces no measurable overhead. Additionally, it exploits z/OS branch-relative and dataspace technology, along with binary-search code paths.

Report and Command Generator

Reporting is provided to detail unreferenced and referenced security entries and to generate command files to enact or restore security cleanup. When the report is executed, you can identify whether the report is for referenced or unreferenced security entries. In addition, you can specify a threshold for including or excluding items. For example, "UNREF=30" reports security entries unreferenced thirty days or more. By contrast, "REF=30" reports entries referenced within thirty days. Selective reporting and cleanup of only selected items is also supported.

The generation of command files is optional when running the reports, but when selected, two files are always generated. One contains cleanup commands and the other contingency commands that can be used to restore the cleanup. For example, if the cleanup file contains commands to delete a user ID, the contingency file will contain the commands needed to recreate the user ID.

The following is a sample unreferenced report for CA-ACF2 format:

2001/06/01 (01.152) 15:30			Entries Unreferenced Over 180 Days		
Date Loaded	Date Referenced	Days Unused	Item Class	Item Name	
-----	-----	-----	-----	-----	
			DSN	\$KEY(SYS1)	
00.110	.	408		OEM.PARMLIB UID(SYS) R(A) W(A) A(A)	
00.110	00.336	181		OEM.PROCLIB UID(*) R(A)	
00.110	00.300	218	DSN	\$KEY(SYS9)	
			RFAC	\$KEY(BPX.SUPERUSER) TYPE(FAC)	
00.110	.	408		UID(FTPX) PREVENT	
00.100	00.150	368	USER	ASTRO3	STEVEN SMITH

The following is a sample unreferenced report for CA-Top Secret format:

2002/12/28 (02.362) 11:42			Entries Unreferenced Over 180 Days		
Userid	Date Loaded	Date Referenced	Days Unused	Item Class	Item Name
-----	-----	-----	-----	-----	-----
ALL	02.160	02.178	184	DATASET	TESTDB2
ALL	02.160	.	202	VOLUME	WORK08
ASTRO2	02.160	.	202	PROFILES	STARPROF
ASTRO2	02.160	.	202	PROFILES	SUNPROF
ASTRO2	02.160	.	202	DATASET	STAR.LOG2
MARSPROF	02.160	.	202	USERLIST	ASTRO1
MARSPROF	02.160	.	202	USERLIST	ASTRO3
MARSPROF	02.160	.	202	DATASET	SOLAR.SYSTEM
MARSPROF	02.160	02.167	195	OTRAN	SAPI

The following is a sample unreferenced report for IBM RACF format:

2003/03/31 (03.090) 09:47			Entries Unreferenced Over 100 Days		
Userid	Date Loaded	Date Referenced	Days Unused	Item Class	Item Name
-----	-----	-----	-----	-----	-----
PROF	02.300	02.314	141	DATASET	SYS2.TX.*
P390G	02.300	02.354	101	USERID	SUSAN POPE
TGRP	02.300	02.350	105	GROUP	
U01507	02.300	.	155	GROUPS	IS
U01507	02.300	.	155	GROUPS	SYS2
U01507	02.300	.	155	TSOAUTH	OPER
U01507	02.300	.	155	DATASET	SYS3.**

Conclusion

eTrust Cleanup offers an immediate and substantial response to many of the increasing pressures facing information security today (including regulatory, statutory, audit and staffing issues). Operating virtually unattended, eTrust Cleanup continuously monitors security usage and provides a programmatic approach to cleanup:

- Provides unattended continuous operation
- Allows you to identify entitlements used versus unused
- Generates commands to remove user IDs and entitlements
- Identifies and removes excessive entitlements
- Includes contingency commands to re-establish an ID or entitlement
- Reduces risk/exposures
- Eases administration
- Improves responsiveness
- Enables audit compliance
- Provides greater clarity and conciseness
- Enhances security performance
- Reduces security administration staff workload
- Aids recertification
- Provides regulatory remediation
- Helps you adhere to privacy mandates
- Enables you to develop and/or refine role-based security definitions

For more information on eTrust Cleanup, please visit www3.ca.com/solutions/ProductFamily.aspx?ID=5587

