

Improve XA Security Management Capabilities Ensure Data Security and meet Audit standards

CISTECH’s **Enhanced Security Tool** significantly improves your ability to implement, maintain and audit iSeries and MAPICS XA security compared to base Cross App and IFM Security. The powerful PowerLink interface provides visibility and control of user authority to XA applications and data, as well as to iSeries objects.

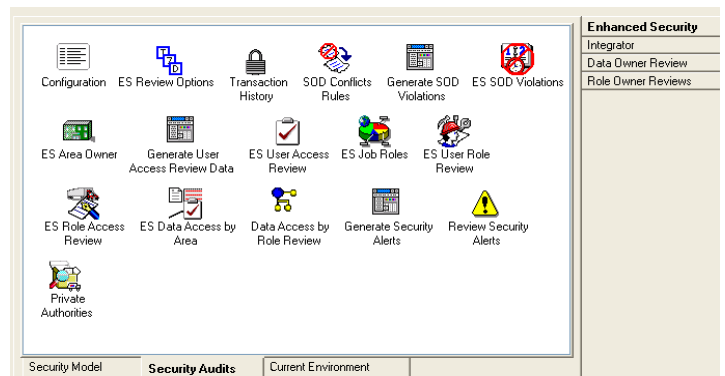
Benefits of Enhanced Security Tool:

- Quickly develop and implement XA Security policies that meet auditor requirements.
- Significantly reduce risk of unauthorized transactions with segregation of duties.
- Easily plan and monitor user rights for XA applications using defined Job Roles.
- Maximize productivity for administrators tasked with managing and reporting security.
- Reduce the disruption to users typically associated with implementing new security policies.
- Provides access to application security information commonly requested by auditors.

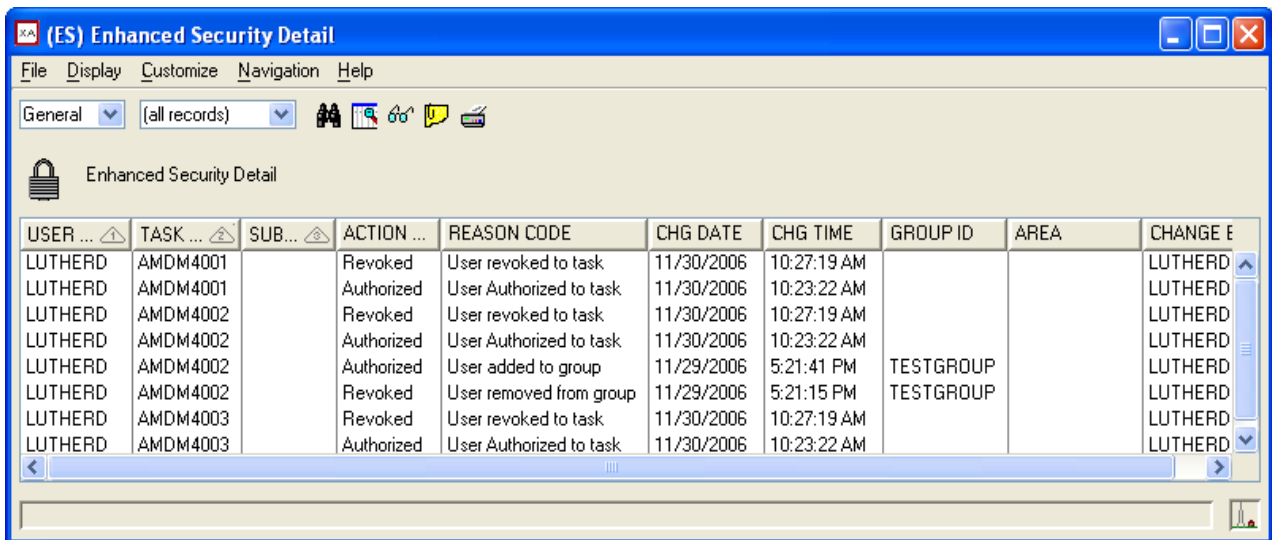
Enhanced Security Tool Features and Functions:

CISTECH’s Enhanced Security Tool, developed with XA Integrator, enables iSeries security administrators to develop and deploy an effective Security Policy for XA applications and data. This tool simplifies the tasks required to successfully implement your new plan, significantly reduces disruption to user productivity, and provides complete visibility to security data.

- Create and implement a security plan incorporating Job Roles with CAS security to easily manage user rights
- Configure SOD conflict rules for areas and/or tasks including manual tasks
- Assign owners to perform routine access reviews to facilitate management and reporting of user rights approvals as required by auditors
- Export and test your new security plan before implementing in the live environment
- Quickly view and navigate user access and how that access was achieved (unlocked or private/group authority), including:
 - User’s current and proposed rights to tasks
 - Rights to CAS tasks that will be granted or revoked to a user by the proposed plan
 - Roles and groups a user is in as well as members of roles and groups
 - Areas that a task is in (so you can secure it)



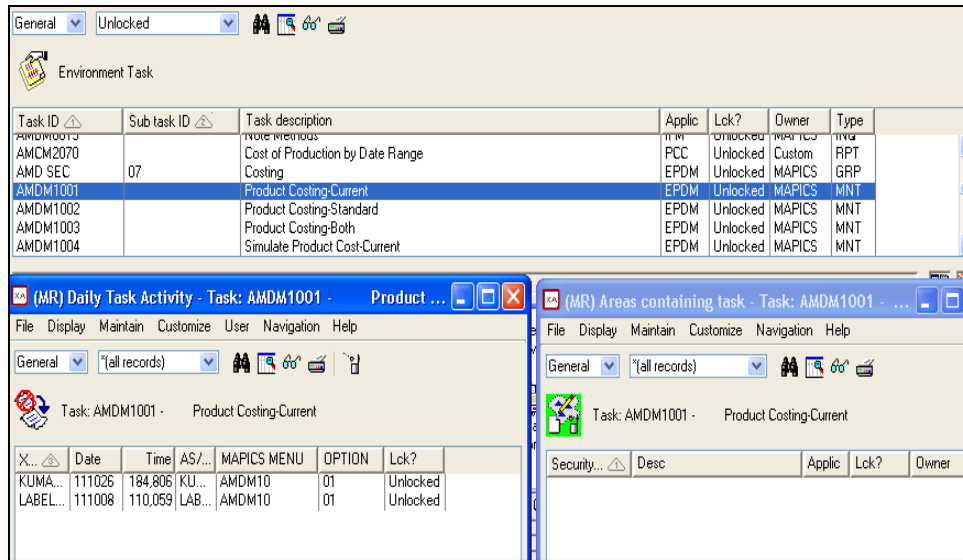
- Capture and view actual user activity for green-screen menu options, Power Link maintenance, and IFM maintenance
- View iSeries profile information including super-users, password rules and logon statistics
- Visibility of IFM Security settings as well as resulting user rights to IFM Tasks
- On-demand inquiry and extract capabilities for common auditing requirements:
 - Review and manage resolution for violations to Segregation-of-Duties rules
 - Configure 'Watched' Tasks to quickly report user access to high-risk functions
 - Routine review and approval of user rights by assigned owners
 - Role owners review users assigned to roles and tasks the roles can perform
 - Data owners review role access to data by functional area and/or task
 - Audit Coordinator tools to prepare and manage routine security review activities
 - Resource assignment and resolution tracking within the tools
 - Audit changes to security to ensure proper procedures are enforced
 - Archival and restore capabilities for audit review data
 - Print security audit results to a PDF file or export information to Excel



The screenshot shows a window titled "(ES) Enhanced Security Detail" with a menu bar (File, Display, Customize, Navigation, Help) and a toolbar. Below the toolbar is a table with the following columns: USER, TASK, SUB, ACTION, REASON CODE, CHG DATE, CHG TIME, GROUP ID, AREA, and CHANGE E. The table contains 10 rows of data for user LUTHERD performing actions on tasks AMDM4001 and AMDM4003.

USER ...	TASK ...	SUB...	ACTION ...	REASON CODE	CHG DATE	CHG TIME	GROUP ID	AREA	CHANGE E
LUTHERD	AMDM4001		Revoked	User revoked to task	11/30/2006	10:27:19 AM			LUTHERD
LUTHERD	AMDM4001		Authorized	User Authorized to task	11/30/2006	10:23:22 AM			LUTHERD
LUTHERD	AMDM4002		Revoked	User revoked to task	11/30/2006	10:27:19 AM			LUTHERD
LUTHERD	AMDM4002		Authorized	User Authorized to task	11/30/2006	10:23:22 AM			LUTHERD
LUTHERD	AMDM4002		Authorized	User added to group	11/29/2006	5:21:41 PM	TESTGROUP		LUTHERD
LUTHERD	AMDM4002		Revoked	User removed from group	11/29/2006	5:21:15 PM	TESTGROUP		LUTHERD
LUTHERD	AMDM4003		Revoked	User revoked to task	11/30/2006	10:27:19 AM			LUTHERD
LUTHERD	AMDM4003		Authorized	User Authorized to task	11/30/2006	10:23:22 AM			LUTHERD

- Regular IT review to ensure long-term integrity of your security configuration:
 - View daily changes to user access including when the change was made, how, and by whom
 - Alerts identifying users that have security not granted by assigned roles
 - Review private authority to ensure users are not circumventing job role access
 - Review unlocked tasks including who uses them and how to access them



Additional Available Services:

- iSeries and XA Security Checkup
- XA Security Policy Planning and Implementation

Pre-requisites: OS/400 V5R3 or higher, MAPICS XA R7, R9, Enterprise Integrator