Enforcive/Security for CICS - MVS

Field-Level Security for the MVS environment

Mainframe Compliance with PCI-DSS, SOX, HIPAA and others

Data protection and masking down to field-level

DB2, IMS and VSAM

Extended security, seamlessly integrated with RACF and TS

Easy authority management for CICS resources at all levels

Monitoring and auditing of user activity and security events

Monitoring of security officer activity

Menu generator

Application-independent

Optional GUI Client and extended auditing

Enforcive/Security for CICS is the answer to auditors' requirements of internal controls for the protection and auditing of your data. It addresses the difficult demands of industry and legal regulatory compliance like PCI, SOX and HIPAA through data protection, privacy and an easy-to-understand audit log.

Field-Level Data Protection and Masking (for DB2, IMS and VSAM)

Data can be protected at the file, record and field level within VSAM files, DB2 tables and IMS records. Authorization at the record and field level is determined by rules you set up, based on field values.

Sensitive fields can be protected from update or even masked from view for unauthorized users, while non-critical data in the same file can be left with full visibility.

For DB2, protection can be implemented at the table level, independent of application or PLAN. Moreover, you can restrict access (or mask) down to the column level, according to column value.

The data protection is application-independent, operating at the system level and applying to all current and future applications.

Extended Security, Seamlessly Integrated with RACF and TS

Enforcive/Security for CICS is a rich set of advanced security components which integrate seamlessly with RACF and other basic security systems. It authenticates passwords against the RACF security system for unity of passwords between the systems.

Easy Authority Management for CICS Resources at All Levels

Alongside field-level authorization, Enforcive/Security for CICS provides easy and user-oriented authorization management of other resources as well. Each user or profile is granted authorization to the resources they require - transaction, terminal, program, file, record (by field value) and individual field.

Authorizations can be multi-level involving different combinations of resources i.e. user permitted to specified files for certain transactions.

With **Enforcive/Security for CICS** the security officer defines CICS authority through clear menus and easy-to-understand, structured screens. Definitions made can be reviewed and changed quickly and simply with no need to remember the format of commands. Changes and additions are made on a full screen while the current authorizations for the user are displayed. Following the changes made, the full updated state of authorizations remains displayed on the screen for confirmation of the updated values.

The handling of authorities is further aided by the way you specify authorized resources for a user. You can choose the specific resources (transaction, file etc.) to which the user is authorized, or decide that the user is authorized to all resources of a certain type, except those specified.

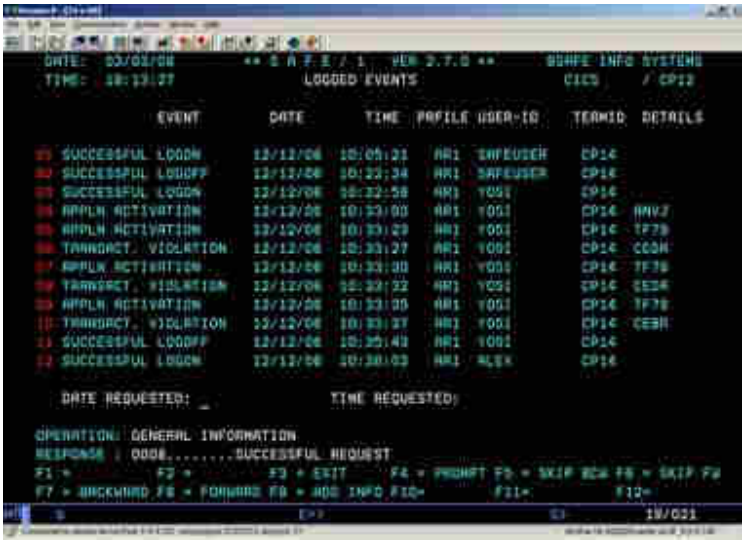
Alongside the product's powerful online update is a mass update facility to make large numbers of authorization definitions in batch. A full set of reports can be produced including details of all authorizations and policies defined in the system and statistical reports like inactive users.

All authorizations defined by Enforcive/Security for CICS are independent of application, operating at the system level and applying to all current and future applications. Authorization definitions are facilitated by group authorities for users and resources, reducing the time required for implementation and maintenance.

This user-oriented approach of Enforcive/Security for CICS means that the security officer can manage security in an easy, natural and logical manner. The result is a reduction in the time and costs required for administrator activity and training in comparison to other solutions.

Monitoring and Auditing of User Activity and Security Events

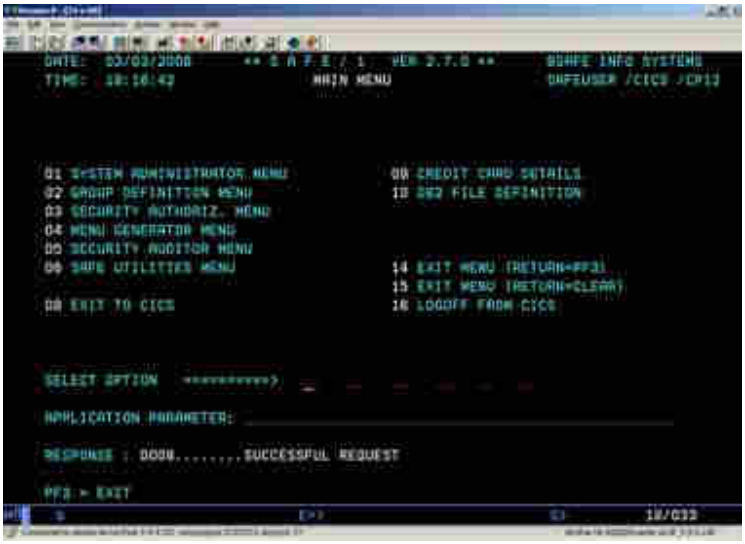
Enforcive/Security for CICS incorporates an audit log of security events. The security officer can view the log in real-time, filtered by various parameters including user, event type, date and time.



The audit log can be viewed on-line and reports can be printed with or without filtering of the events. In addition, the printed reports can be sorted by a variety of criteria.

Menu generator

Enforcive/Security for CICS incorporates a menu generator to create menus for end users. Your users will be able to run clearly-named tasks rather than having to remember transactions and parameters.



This improves user-friendliness, reduces the chances of executing transactions wrongly and prevents users from attempting to run transactions not meant for them.

The security officer can update the user menus on-line, quickly and simply, even while the users continue to work.

Restriction by menu is an additional layer of protection, on top of user authorizations to resources.

Enforcive/Security Server for CICS (Optional)

The Enforcive/Security Server provides the organization's applications with a means of receiving security information from Enforcive/Security for CICS.

User Activity Tracking

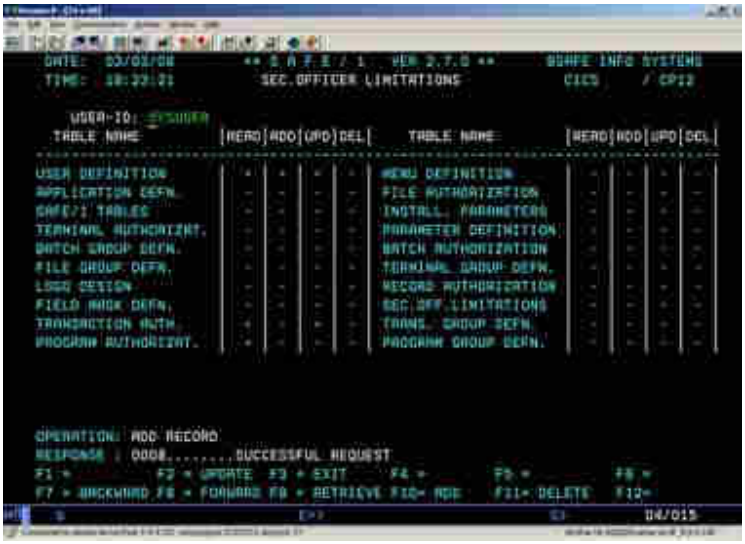
For selected users, monitor usage of specific transactions and programs and access to defined field values. This is done while the user works normally, without being aware of any tracking.

Alerting

The product features a real-time IDS (intrusion detection system) in which alerts can be issued following specific events. For example, users attempting to log on from unauthorized terminals.

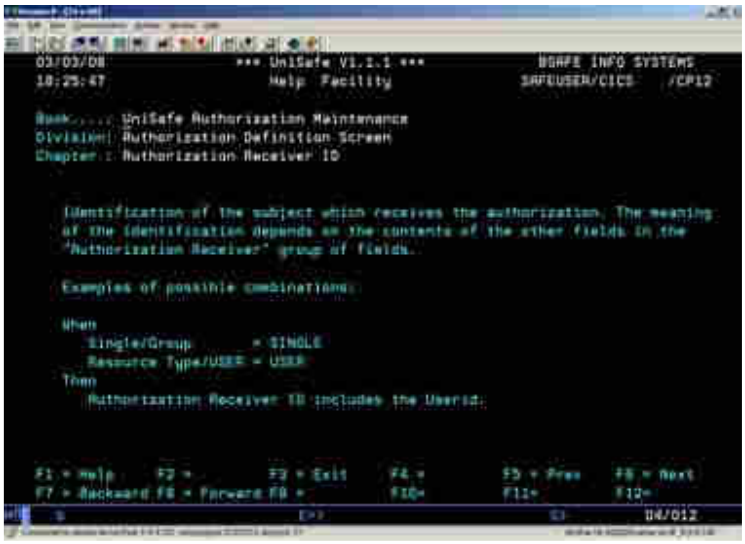
Decentralization of Administration

Enforcive/Security for CICS allows you to distribute administration functions by defining different functions and control for different administrators. For example, you can create a restricted security administrator who can add new users and assign them to existing profiles, but cannot add or change authorizations to access resources.



On-line Help

The product features detailed help screens to assist the administrator in making the required definitions.



Optional Add-ons

1. Windows-based GUI Client

Enforcive/Security for CICS may be managed through a Windows-based GUI called Enforcive/Enterprise Security for System z.

2. Cross-Platform Audit (CPA)

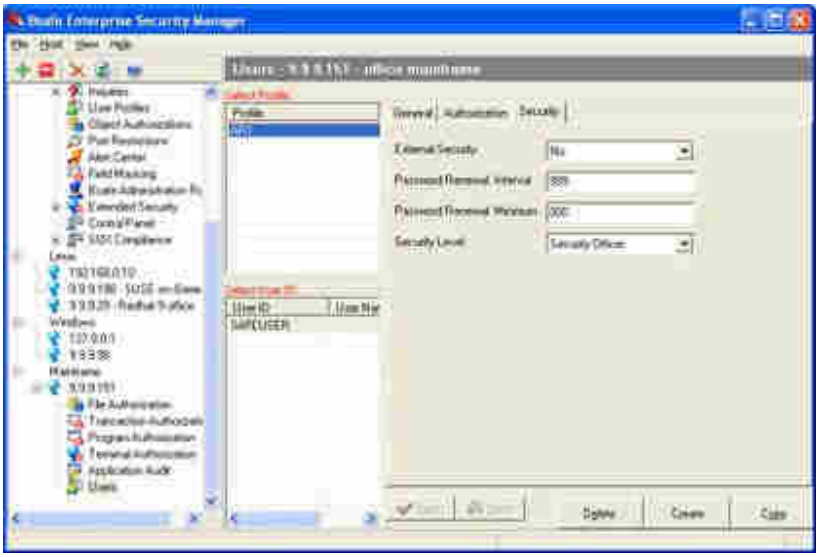
Audit data collected by **Enforcive/Security for CICS** can be downloaded to Enforcive's PC-based database application which consolidates audit data from multiple machines and multiple platforms for mouse-click analysis and reporting. It also serves as a means of freeing up expensive mainframe disk space if you wish to purge the files after transfer to the CPA.

3. CICS Security Implemented by GUI

Download the brochure

Enforcive/Enterprise Security for CICS is a graphical user interface to manage granular security for IBM RACF and CA Top Secret (T/S) implementations in the CICS environment.

The system is an optional add-on for Enforcive/Security for CICS, a granular system of managing authority to CICS resources at the level of user, transaction, terminal, file, record and field.



User-Friendly for Speed and Efficiency

The Windows-based GUI interface makes an already intuitive and easy-to-work-with product the number one CICS security management system both in terms of functionality and simplicity. It makes the experienced administrator's task faster and more pleasant, reducing the chance of errors and allows CICS resource control to be managed by a administrators who do not necessarily possess system programmer skills.

Definitions made can be reviewed and changed quickly and simply with no need to remember the format of commands. The instant online definitions of users, transactions, programs and terminal security reduces the time and costs required for administrator activity and training.