

Bsafe/Security for VSE CICS v2.3

Complete Security for the CICS v2.3 environment

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

- Encrypted passwords
- Passwords set and known only by the user
- Forced periodic password changes
- Automatic user locking following repeated wrong passwords
- Policy management of users and passwords
- Controlled user authority to CICS resources at all levels
- Data protection and masking (file, record and field level)
- Monitoring and auditing of user activity and security events
- Monitoring of security officer activity
- Menu Generator
- Application-Independent

Bsafe/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.



Password Encryption

With **Bsafe/Security for CICS** user passwords are no longer transparent to anyone viewing the password file. Every password stored in the system is encrypted and cannot be viewed even by the security officer. The encryption algorithm is irreversible and encrypted passwords cannot be decrypted.

Passwords Set and Known Only by The User

With the creation of a new user, an initial password is issued by the security officer. On the first logon, the user is forced to set a new password which is known only to that user. Forgotten passwords cannot be restored and a new initial password must be issued.

Forced Periodic Password Changes

The security officer can define for each user the period of time the current password may be used, after which the system will force the user to change the password. The user cannot choose a new password identical or similar to recently-used passwords.

Automatic User Locking Following Repeated Wrong Passwords

Bsafe/Security for CICS allows the security officer to set the number of times a user can attempt to log on with an incorrect password before being locked by the system. Once locked, the user cannot log on from any terminal until unlocked by the security officer.

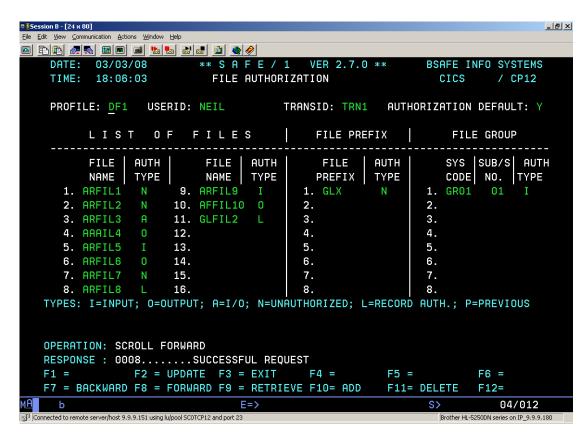
Policy Management of Users And Passwords

The security officer can determine the permitted character structure of the password and other password management features. In addition, he can define the period a user will be authorized to log on to the computer. This is ideal for temporary user IDs which sometimes get forgotten. It also provides a means of restricting the times of day during which each user can log on. Restrictions can be set at the user level.



Controlled User Authority to CICS Resources at All Levels

Bsafe/Security for CICS is a granular system of managing user authority to CICS resources at the level of **terminal**, **transaction**, **program**, **file**, **record** and **field**. Give users authorization only to the resources they require.



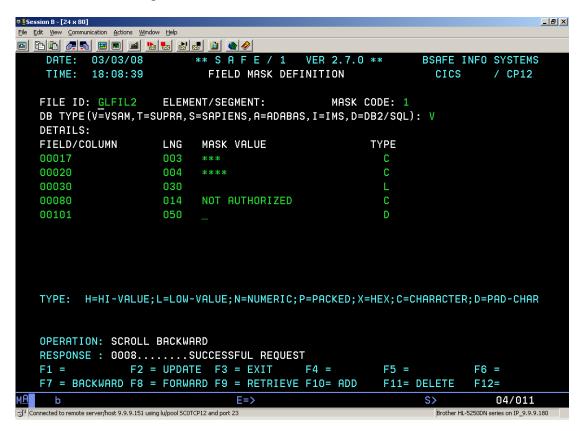
Authorizations can be multi-level involving different combinations of resources i.e. user permitted to specified files for certain transactions. All authorizations defined by **Bsafe/Security for CICS** are independent of application, operating at the system level and applying to all current and future applications.

Authorization definitions are facilitated by group authorities for users and resources, reducing the time required for implementation and maintenance. 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.



Data Protection and Masking (File, Record and Field Level)

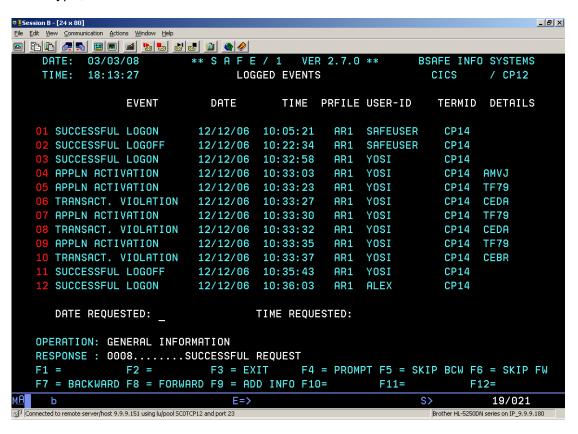
Bsafe/Security for CICS allows you to control data in VSAM files at the file, record and field level. You can define user authorization to specific files (**none**, **read** or **write**). Furthermore you can define which records each user may access according to its field values. Finally, you can mask selected fields from view according to field-value criteria.





Monitoring and Auditing Of User Activity And Security Events

Bsafe/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.

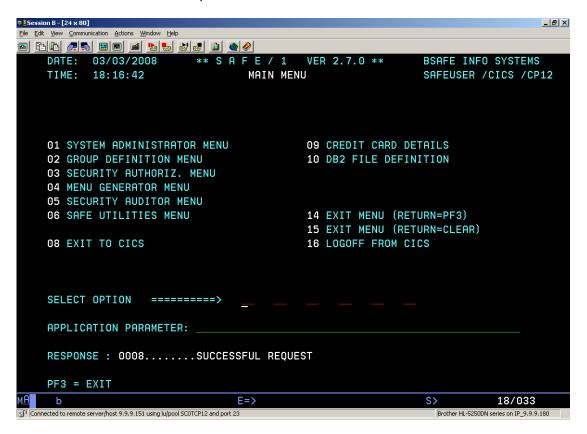


The audit log can be viewed on-line and reports can be printed with or without filtering of the events. In addition, the printed reports can be sorted by a variety of criteria.



Menu Generator

Bsafe/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.



Bsafe/Security Server for CICS (Optional)

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

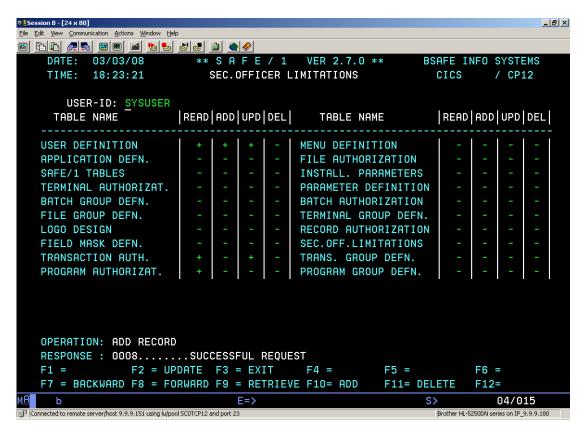
Monitoring of Security Officer Activity

All authorizations and definitions made by the security officers can be logged in a dedicated log file, including details of the authorizations defined and the identification of the administrator who made the definitions.



Decentralization of Administration

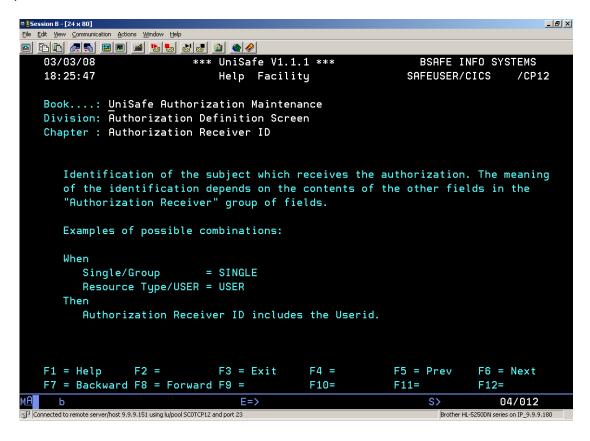
Bsafe/Security for CICS allows you to distribute administration functions by defining different functions and control for different administrators. For example, you can create a restricted security administrator who can add new users and assign them to existing profiles, but cannot add or change authorizations to access resources. Another example is a security help-desk function which could be given authorization only to handle users which have been locked but cannot perform any other security functions.





On-line Help

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



Ease of Use

With **Bsafe/Security for CICS** you implement 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.

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.

Visit our website, www.bsafesolutions.com

Call one of our offices,

USA New Jersey	Tel: 877-237-8024 toll free	salesusa@bsafesolutions.com
Canada	Tel: 905-9434042	info-ca@bsafesolutions.com
Europe & R.O.W.	Tel: +972-9-9610400	info-eu@bsafesolutions.com

Or speak to a local reseller near you. See the list on our website

Maximum Security, Simply!

Bsafe/Security for CICS