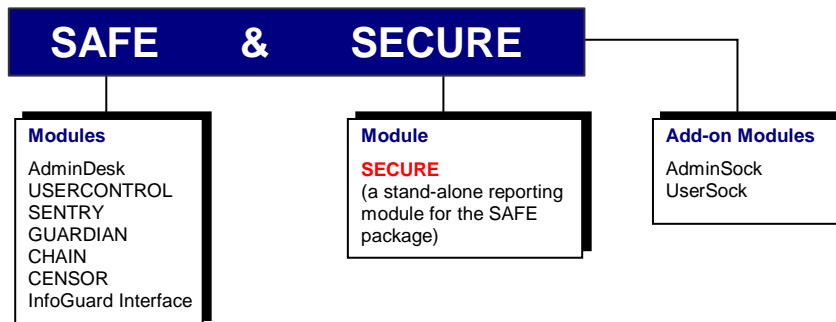


# SECURE

## Feature Sheet

SECURE provides consolidated reports for the SAFE package and is available from Locum Software Services Limited. SECURE provides Security Administrators and auditors with the total security reporting solution. SECURE is a fully integrated module of the SAFE & SECURE software package and may be used as a stand-alone product or in conjunction with other SAFE modules. The following diagram provides an overview of the various modules of the SAFE & SECURE software package.



The need for security information may not be restricted solely to the Security Administrator. In many large organisations, many departments may have a particular requirement to produce security reports. For example:

- Security Officers, Administrators and Managers
- EDP Internal and External Auditors
- State, Federal or Government Examiners

For this reason, SECURE may be used either by any privileged or superuser, or by a specified delegated user.

### Security Reporting

Security reports should inform the user of any activity or condition that could pose a security threat. The SUMLOG file is used by the MCP to log all system activity and is the logical source of information for security reporting. Unfortunately, the reporting facilities contained within standard software are not tailored to address the specific requirements of the security auditor; the reports are not restricted to security issues; the volume of extraneous information makes it difficult to isolate relevant details; and the use of such facilities demands specific technical knowledge for both operation and interpretation. SECURE solves the MCP/AS security reporting problem. SECURE accesses both the SUMLOG file and the System Directory files and produces a comprehensive set of security reports that are:

- Relevant - each targets a specific security issue
- Non-technical - technical jargon is avoided
- Readable - layouts are clear and friendly
- Concise - extraneous information is omitted
- Fast-executing - efficient processing

## Key Features

- Three modes of operation - Batch, Interactive and Realtime
- Individual sumlog reporting
- Multiple sumlog reporting
- Multi-user facility
- Output media - print file, screen or port file

## Three Modes of Operation

**Batch Mode** - for the production of standard or regular reports.

**Interactive Mode** - for the production of ad-hoc reports.

**Realtime Mode** - for the monitoring of specified security events and violation. The CHAIN module will allow SECURE to monitor events on ALL or a selection of systems within the network.

## Individual Sumlog Reporting

Reports may be generated from the current SUMLOG or an 'old' SUMLOG. An 'old' SUMLOG is defined to be a SUMLOG file which has been 'released' by the MCP (i.e. subject to a TL (Transfer Log) operator command).

When producing reports based on a single SUMLOG, the user may specify a smaller time frame than that covered by the selected SUMLOG. If no time frame is specified, the entire SUMLOG is analysed.

## Multiple Sumlog Reporting

A major feature of SECURE is time-based reporting; this enables the user to produce reports covering a specific time range without complicated SUMLOG consolidation. The only action that the user has to perform is to designate the time period; SECURE will identify the required SUMLOG files to be analysed (up to a maximum of 30).

## Multiple User Facility

In an installation where there is more than one Security Administrator, or where several auditors wish to generate reports, SECURE may be invoked by multiple users simultaneously.

The user is identified by his or her usercode/accesscode combination. Only one invocation of SECURE is allowed for each valid usercode and accesscode pairing.

## Output Media

In Interactive Mode, SECURE provides a menu-driven interface allowing the user to generate reports from any CANDE or COMS terminal. Interactive reports may be directed to

the terminal in paged format (Browse Mode), to a disk file for archiving of reports or to a print file. In the last case, SECURE provides facilities to control the routing of printed output.

In Realtime Mode, the output options include routing to a port file interface so that events may be passed to a user-written or third-party program, for example, to generate alerts.

The following reports are available:

Diskfile Privileges  
Usercode Activity  
Accesscode Activity  
Security Violations  
Logon Violations  
MCS Initialisations  
Disk File Accesses  
Program Executions  
System Commands  
Unauthorised File Access  
Password Changes  
Session Information  
Program Timestamp Verification  
Window Accesses  
COMS Cfile Changes  
File Status Changes  
One-time Usercode Changes  
CENSOR Commands  
Installation Records  
Overdue Users  
Userdatafile Changes  
SAFE Audit  
CHAIN Audit  
Sumlog Integrity  
Privileged Actions  
Miscellaneous Security Actions  
Security Policy

Most reports may be filtered, allowing the user to 'home-in' to a particular problem.

## Free Trial

If you would like to see how SECURE can help secure your UNISYS MCP/AS system, contact Affinité Europe today to take advantage of our FREE no-risk trial offer.