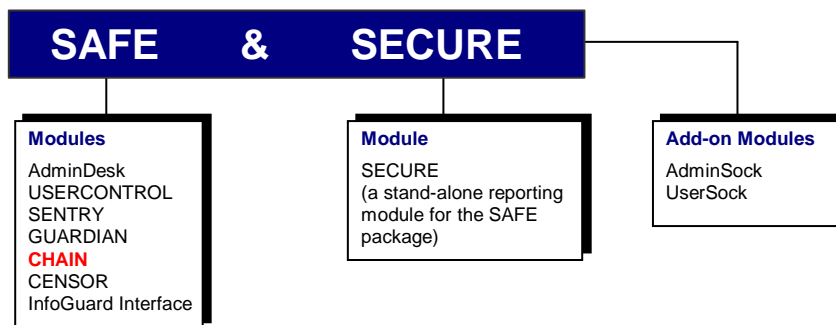


CHAIN

Feature Sheet

CHAIN is a security utility available from Locum Software Services Limited that allows the Security Administrator to determine and establish the level of synchronisation within the network. CHAIN 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 SECURE module provides reporting for the SAFE package and together SAFE & SECURE provides the total security solution.

The Challenges of Security Administration

MCP/AS security is centred on the Userdatafile, the repository of most security-related information. In an MCP/AS network, each system is responsible for its own security, as established and controlled through the Userdatafile. Each system applies its security controls in a discrete environment, with no communication with its neighbours.

From a security viewpoint, it can be seen that the MCP/AS network is a network of individual systems, rather than one complete entity. This approach works well in large networks where the MCP/AS hosts are owned by different companies or organisations. However, most MCP/AS networks are fairly small and belong to a single owner. Therefore, the environment within each system shares a common security policy.

Administration of the Userdatafile in these networks can be difficult, particularly when there is some degree of commonality between systems. At one extreme, it may be required that each Userdatafile to be identical; at the other extreme, the Userdatafile may be required to be completely different. At any point between these two extremes there is a certain degree of commonality.

CHAIN addresses the administration problems where some degree of commonality is required. At the simplest level, consider the situation where a particular usercode is defined on three separate systems. When the user changes his or her password on one of the hosts, he or she must change the password on each of the other hosts in order for the password to remain in synchronisation. Otherwise, the user has to remember three passwords for the three different hosts. Where

password aging is in force, this can become a common, reoccurring problem. On a password aging system which employs automated password generation, the problem of synchronisation would be difficult to solve through standard software packages.

Key Features

- Synchronisation across networks
- Realtime monitoring across networks
- CHAIN components
- Supports BNA and TCP/IP methods of communication
- Function delegation

Synchronisation Across Networks

CHAIN allows the Security Administrator to determine and establish the level of synchronisation within the network. Flexibility is achieved in two ways:

- By providing, via SAFE, a mechanism for designating a host list that determines which hosts within the network are to be subject to synchronisation.
- By providing, via SAFE, a set of CHAIN options which can be tailored to satisfy an installation's own security requirements. These options control which Userdatafile changes should be propagated to the other hosts within the designated host list.

CHAIN options are implemented to propagate the following:

- Usercode password changes performed by the user or by the Security Administrator
- Accesscode password changes performed by the user or by the Security Administrator
- Reactivations of users (both usercodes and accesscodes)
- Deactivations of usercodes or accesscodes by the Security Administrator
- Changes to SAFE's options
- Changes to SENTRY's options
- Changes to CHAIN's list of hostnames
- Changes to CHAIN's options

The CHAIN options need not be set in an identical fashion on all hosts. This allows 'one-way' propagation to be established for any or all changes.

In addition to the CHAIN options described above, CHAIN offers the Security Administrator the capability of performing most SAFE functions on any host whilst remaining within SAFE on the local host.

Realtime Monitoring Across Networks

The CHAIN module enables the realtime monitoring function of the SECURE module to report on all security events on ALL systems (or a selection of systems) within the network to a single terminal or remote printer.

CHAIN Components

CHAIN is structured as a module within the total SAFE & SECURE software package. Functionally, CHAIN is split into two parts: CHAIN administration

and CHAIN operation. The administration of CHAIN is embedded within SAFE, and is available only to the Security Administrator; by this means, the Security Administrator may establish 'propagation rules'. The operation of CHAIN is performed by a separate library. This library communicates with the corresponding CHAIN libraries on the other hosts via a portfile interface. In the event of one or more hosts becoming disconnected from the network, CHAIN will queue up messages from the disconnected hosts, and when reconnection is established, will ensure that the messages are sent in the correct chronological sequence. A full audit may be taken of all activity performed by CHAIN within the network. SAFE provides the mechanisms to release and print the audit files. The CHAIN module is fully compatible with other modules of SAFE. Userdatafile changes performed via AdminDesk, USERCONTROL and SENTRY may be passed to CHAIN and propagated across the network.

BNA and TCP/IP Communication

The way in which the CHAIN libraries communicate depends upon the method of service used within an organisation. CHAIN may use the BNANATIVESERVICE or TCPIPNATIVESERVICE as its portfile protocol.

Function Delegation

In many installations, security personnel are available only during certain hours of the day. For contingency, the Security Administrator may delegate CHAIN functions, for example modification of the CHAIN options or the current host list, to other specified usercodes or accesscodes. Such users require no special privileges; the scope of activity that may be performed is strictly controlled by the Security Administrator.

Free Trial

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