

SAFE & SECURE

Developed by Locum Software Services UK

An Overview

Introduction

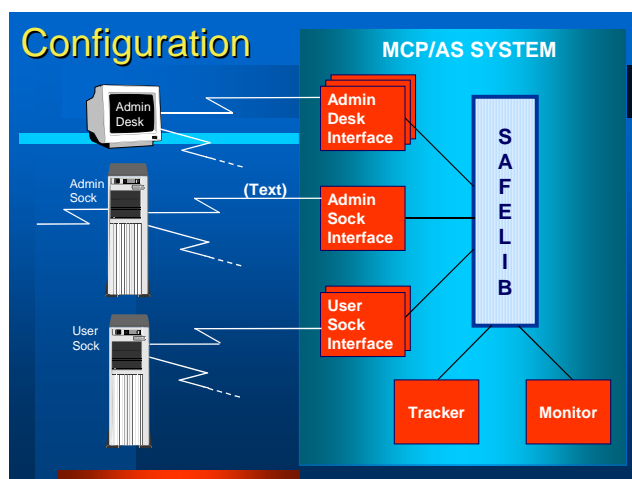
In MCP/AS environments, one of the biggest concerns for system administrators is security. SAFE & SECURE is a comprehensive security package which consolidates and simplifies security mechanisms for security administrators.

SAFE & SECURE provides the following functionality:

- **AdminDesk** - provides a Windows-based PC interface for SAFE & SECURE.
- **Central Administration** - with easy-to-use Userdatafile and COMS Cfile administration and interrogation capabilities.
- **Access Control** through password ageing, log-on, station control and session control.
- **System Command Control** - delegation and authorisation of the use of system commands for end-users.
- **Multi-Host Operations** - simplifies administration of the Userdatafiles in multiple processor environments.
- **Reporting** - a stand-alone, efficient and easy -to-use product, providing administrators and auditors with a total security reporting solution.

In addition to the modules listed above, the following add-on modules are available:

- **AdminSock** - provides a TCP/IP socket interface to enterprise administration software and operates via a batch file interface.
- **UserSock** - provides a TCP/IP socket interface to client-server applications in which end-users bypass the traditional MARC sign-on procedure.
- **SafeSurvey** – provides a mechanism for highlighting security weaknesses on MCP systems.



AdminDesk

AdminDesk is the Graphical User Interface for the SAFE & SECURE software product. AdminDesk provides the Security Administrator or a Regime Administrator with the ability to perform SAFE & SECURE administrative functions via a WINDOWS-based PC.

AdminDesk simplifies security administration with the following features:

- Explorer-style view of hosts and users
- Control of multiple hosts
- System options and user attributes grouped into property pages
- Extensive use of drop-down menus

The AdminDesk Interface

AdminDesk has been designed with the look and feel of the familiar Explorer-type window environment and utilises the 'tree and list' structure, thereby allowing the use of the point-and-click method of selection. Usercode attributes and system options are grouped together into logical combinations and displayed in property pages. Property pages and their contents may be customised to suit an installation's own requirements.

The AdminDesk interface offers greater flexibility, additional functionality and easier maintenance than the terminal emulation interface of SAFE & SECURE.

Key Features

AdminDesk provides the majority of key features offered by the USERCONTROL and SENTRY modules, and in addition offers the following new features:

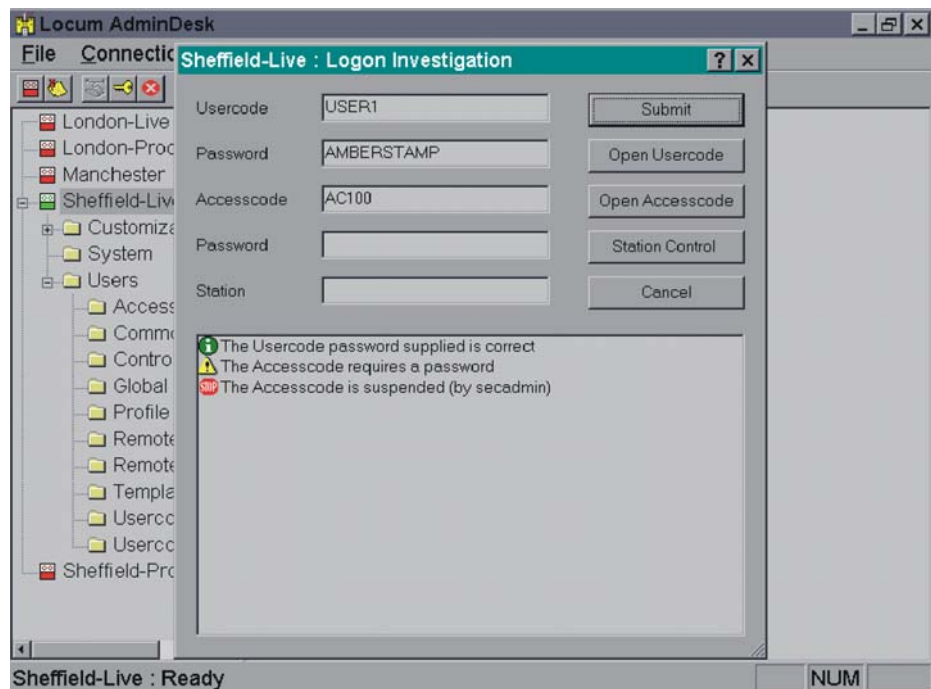
- Single point of administration for multiple hosts
- Logon investigation
- Multiple user update
- Search & update
- Session control
- Regime handling
- HTML on-line help

Single Point of Administration

The AdminDesk main window is divided into two panes; the left-hand pane lists the MCP/AS systems within the network, and the right-hand pane contains information relating to the selected MCP/AS system. AdminDesk allows the Security Administrator to connect to, and administer security on, all the MCP/AS systems within the network via a single window. Switching between systems is simple; a single mouse-click will cause further administration activity to be performed on the selected system.

Logon Investigation

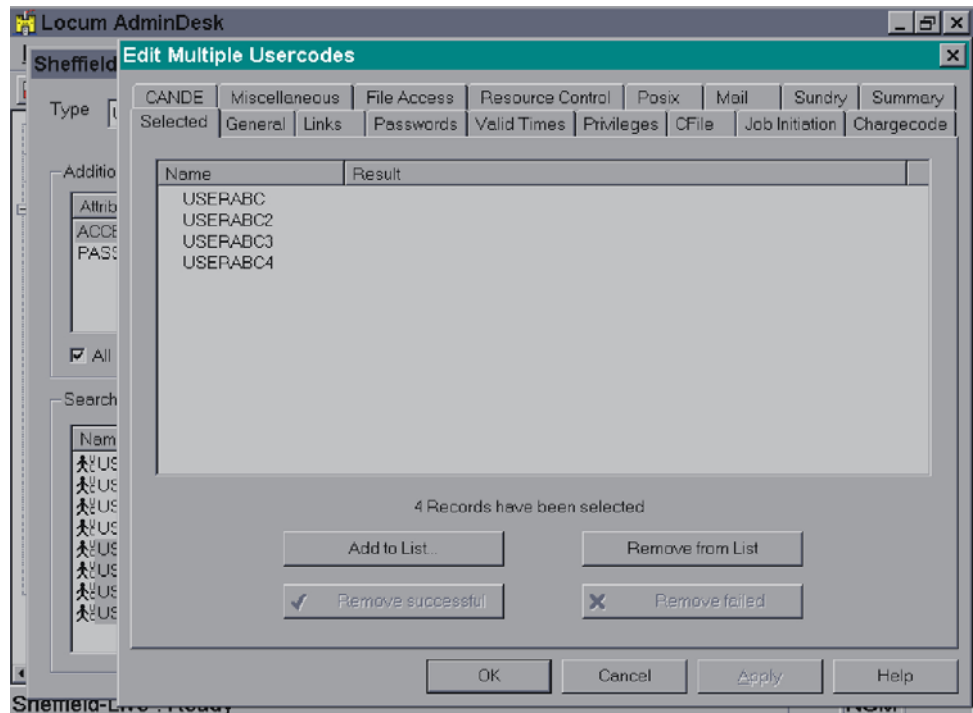
When an attempted logon has been rejected by the system, AdminDesk's Logon Investigation allows the Security Administrator to analyse one or more of the logon elements (i.e. usercode, usercode password, accesscode, accesscode password and station). The more elements supplied the greater the analysis. For example, if a usercode name is supplied and the usercode has a password assignment, the analysis will return information about the usercode requiring a password. If the usercode and usercode password are both supplied, then both elements are analysed and information about the usercode and the usercode password is returned. Information is displayed in the lower half of the dialog box for the Security Administrator to determine the possible reason(s) for the rejection.



Multiple User Update

AdminDesk allows multiple user records to be updated at the same time. The usercode records are listed alphabetically in the right-hand pane of the AdminDesk main window. Multiple user records may be selected for modification and a set of blank property pages will be displayed for you to select and set the required attribute(s).

An example is shown below.



Search & Update

AdminDesk allows the Security Administrator to perform selective searches of the Userdatafile and/or COMS Cfile for all records of a certain entrytype (e.g. usercode, accesscode, profile, template, remoteuser etc.), which conform to specified selection criteria. If a selection criterion is not specified, a list of all entries of the selected entrytype that exist within the Userdatafile is returned. From the resulting list the Security Administrator may modify or delete one or more records and/or save the list results as a report file which may be printed or viewed at a later time.

Session Control

The Security Administrator is able to display all active sessions for all usercodes or all active sessions for all accesscodes via a single mouse-click. From the list displayed, the Security Administrator may view details of the active session(s) for the selected usercode (or accesscode) and terminate one or all of the user's sessions.

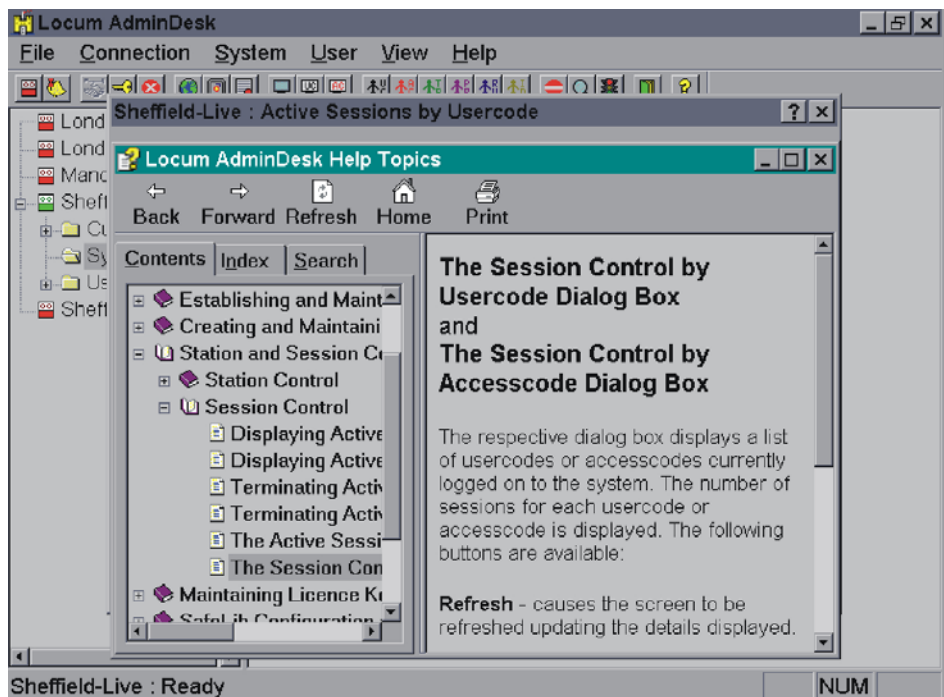
Regime Handling

AdminDesk supports regime administration and also offers additional regime administration facilities. The Security Administrator may take advantage of AdminDesk's 'Group users by regime' option. This option causes records to be grouped by regime and appear in separate folders in the AdminDesk main window, thereby allowing users to be sub-divided into more manageable groups. Even if there is no requirement for regime administration, the Security Administrator may still take advantage of the 'Group users by regime' option.

HTML On-line Help

AdminDesk provides context-sensitive on-line Help using HTML. The Help includes an extensive Contents, Index, and Search capabilities.

An example is shown below.



Central Administration

An important aspect of any security administration is the maintenance of the USERDATAFILE. The USERCONTROL module of SAFE offers many new features and provides a modern, user-friendly interface for Userdatafile maintenance, significantly easing daily operations.

Another important aspect of any security administration is the interrogation of the COMS Cfile. The Security Administrator should be particularly aware of the usercode, program and station definitions that exist within the COMS Cfile. USERCONTROL provides comprehensive Cfile interrogation facilities and simplifies the creation, modification and deletion of usercode definitions.

USERCONTROL provides administrators with a modern, user-friendly interface to the Userdatafile and COMS Cfile. Features include:

- The creation, deletion, modification and interrogation of usercodes and accesscodes.
- Searching the Userdatafile and COMS Cfile, and displaying entries subject to filter conditions.
- Usercode Profile Maintenance
- Profiles contain predefined or required usercode attributes.
- Template Maintenance - templates contain fixed usercode attributes. When these attributes are changed, the changes are applied to all usercodes linked to the specified template.
- Remoteuser Maintenance
- Userdatafile Control Functions
- COMS Cfile Maintenance
Comprehensive interrogation facilities enabling the administrator to interrogate the various Cfile entries. Includes usercode creation, modification and deletion; Cfile housekeeping functions; and optional synchronization between Userdatafile and COMS Cfile.

Key Features

- Simplified usercode maintenance
- Unique accesscode maintenance
- Comprehensive Usercode/Accesscode searches
- Password allocation
- Remoteuser maintenance
- Simplified USERDATAFILE control functions
- COMS Cfile maintenance
- Userdatafile/COMS Cfile synchronisation

- Regime administration
- Function delegation

Usercode Maintenance

USERCONTROL offers interactive usercode maintenance screens which allow the Security Administrator to create, modify, interrogate and delete usercodes with the minimum of effort.

USERCONTROL offers three methods of usercode creation:

1. From scratch - the usercode attributes are presented on screen. Due to the sheer volume of available attributes in the Userdatafile, the number of pages required to display them all may be considered unacceptable for ease-of-use. This can be simplified via the Customize Visible Usercode Attributes function which allows the Security Administrator to select the usercode attributes to be presented on screen. Displaying only those attributes relative to your requirements can significantly reduce the number of screens displayed during maintenance.
2. Via cloning - the attributes of an existing usercode may be cloned to a new usercode. Any attribute settings requiring modification can then be changed via the Modify function. It should be noted that certain attribute values specific to an individual usercode are not cloned (e.g. usercode PASSWORD).
3. Via Profile/Template - the Usercode Profile function allows the Security Administrator to establish a set of fixed or required usercode attributes for a particular 'type' of user significantly reducing the input requirements during usercode creation. Fixed attributes will be set automatically when a usercode is created; required attribute fields will be displayed for input at creation.

Templates are similar to profiles in that they contain a number of fixed attributes that may be applied to a usercode. The difference between a template and a profile is that when the attributes of a template are modified, these changes may be applied dynamically to all usercodes associated with the specified template. An option is provided that allows the Security Administrator to determine whether or not existing attributes are to be overwritten when the current value of the usercode attribute differs from the original value of the template attribute. Templates may be associated directly to a usercode or included in a Profile.

A run-time option called UDF/CFILE LINKING has been provided, which, when set to true, will cause the usercode creation and usercode deletion functions to be synchronised between the Userdatafile and COMS Cfile. This facility is, however, subject to the normal rules of delegation and authorisation (see *Function Delegation*).

The USERCONTROL modify screens are subject to the Customize Visible Usercode Attributes function which can significantly reduce the number of screens displayed during maintenance to a more manageable level.

The interrogation function displays the attributes of a particular usercode in paged format; the deletion function simply requires input of the usercode.

Accesscode Maintenance

USERCONTROL provides facilities to create, modify, interrogate and delete accesscodes associated with one or more usercodes. Accesscode passwords may be applied to all occurrences of the accesscode in a single operation.

USERCONTROL offers two methods of creating accesscodes:

1. From scratch - using a single screen it is possible to add an accesscode to a list of usercodes. A second screen allows the accesscode attributes IDENTITY and USERCLASS to be assigned. Providing the SENTRY module is licensed, the accesscode may be password aged and password aging attributes may also be assigned.
2. Via cloning - a new accesscode may be 'cloned' from an existing accesscode. The new accesscode will be added to the ACCESSCODELISTs declared under each usercode associated with the existing accesscode. Any accesscode attributes assigned to the existing accesscode are transferred to the new accesscode. Attribute settings requiring modification may be changed via the modify function.

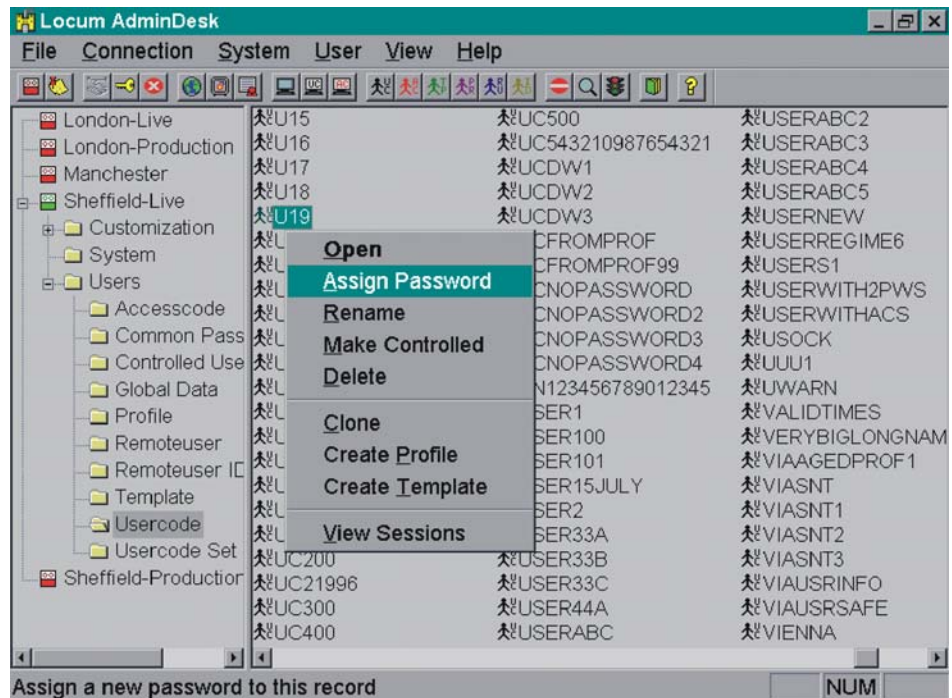
The delete function displays a list of usercodes under which the accesscode has been declared. A field is provided to mark the usercode(s) from which the accesscode is to be deleted.

Usercode/Accesscode Searches

USERCONTROL provides comprehensive searches for both usercodes and accesscodes. The Userdatafile and/or COMS Cfile may be searched to obtain complete reports on all entries or the search may be limited to entries meeting certain selection criteria. Selection may be made by wildcard string on the usercode name, or on the values of chosen attributes or on a combination of these. All usercodes or accesscodes selected through this search are listed in alphabetical order together with the values of attributes used in the selection. The resulting lists may be used to select individual entries for a full display of all attributes.

Password Allocation

When allocating new passwords, USERCONTROL recognises and works with options used by other SAFE modules. The settings of these options will cause USERCONTROL to apply changes to attributes as necessary. For example, the Datestamp attribute of a usercode, which is password aged by SENTRY, will be automatically adjusted to conform to the requirements of password ageing.



Remoteuser Maintenance

For installations using multiple mainframes and BNA, USERCONTROL provides easy-to-use maintenance facilities for remoteuser entries. Remoteuser entries may be created or deleted or reported on using a search facility to select entries by name, hostname, or local alias.

Userdatafile Control Functions

USERCONTROL provides the following USERDATAFILE control functions:

- Copying the USERDATAFILE to a disk file (COPY DISK)
- Copying the USERDATAFILE to printer (COPY PRINTER)
- Recalling an old USERDATAFILE (RECALL)
- Creating a new USERDATAFILE (CREATE NEW)
- Performing a 'garbage collection' (COPY NEW)

- Producing a USERDATAFILE statistics report
- Making a backup copy of the USERDATAFILE
- Enabling/Disabling the MAKEUSERCODE (MU) system command
- Converting the USERDATAFILE

Cfile Maintenance

Within this function, the Security Administrator may adopt a 'top-down' approach to interrogation of the Cfile.

First Level	A Cfile Statistics Report is available, giving high-level statistics regarding the structure of the Cfile; that is, the population of all the activity types (e.g. number of usercodes, windows, stations, etc.).
Second level	Interrogation is concerned with a single activity type. For example, a report may be generated to list on screen all the defined trancodes or window lists.
Third level	Interrogation displays individual definitions, for example an inquiry on window CANDE. In the case of usercodes, the Security Administrator may move simply from interrogation to modification mode.

All reports that are displayed on screen have full forward and backward browse capabilities. The three interrogation levels have 'drop-through' and return capability by using the SPCFY key on any displayed item.

A Cfile Usercode Maintenance sub-function provides creation, interrogation, modification and deletion of usercodes within the Cfile. This closely mirrors the functionality provided for usercodes in the Userdatafile.

The Window Access report offers a quick and easy answer to one of the auditor's favourite questions: Which usercodes have access to this window? The two-stage process via window lists is performed transparently to the Security Administrator.

A set of three housekeeping functions allows the Security Administrator to keep both the Userdatafile and Cfile in a tidy state. Firstly, the Usercode Summary Report combines information from both sources, and produces an easy to read printed report of all usercodes defined on the system, together with all their security relevant attributes. This would typically include attributes such as privileges and identity from the Userdatafile and default window and window list from the Cfile.

Secondly, the Userdatafile/Cfile Compatibility Check function provides details of all usercodes defined in both files, which usercodes are common to both files, and which usercodes are found in only one of the files. At this point, the Security Administrator is offered the opportunity of deleting superfluous usercodes from one or both files.

Thirdly, the Security Healthcare Check function provides details of Cfile definitions which, when combined with Userdatafile definitions, may present a security hazard.

For installations which run two copies of SYSTEM/COMS concurrently, USERCONTROL provides the facility of Cfile Selection, which allows the Security Administrator to switch the interface between 'live COMS' and 'test COMS'.

Regime Administration

USERCONTROL provides the mechanisms for regime administration. The Security Administrator may establish usercodes and accesscodes within a regime and designate a usercode within that regime as the Regime Administrator. A Regime Administrator may maintain usercodes and accesscodes within his regime but is denied access to usercodes and accesscodes outside his regime.

Function Delegation

In many installations, security personnel are available only during certain hours of the day. For contingency, the Security Administrator may delegate USERCONTROL functions, for example creating usercodes or allocating passwords, 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.

Access Control

The Access Control Challenge

Controlling access to systems is one of the major requirements of any installation's security policy. Without proper controls, the opportunity for someone to gain unauthorised access to a system is made much easier. SENTRY overcomes these problems by providing password change, logon and station control facilities that are easy to establish and which present a difficult challenge to a potential hacker.

Key Features

- Password ageing for both usercodes and accesscodes
- Password change control
- Password allocation
- Logon controls
- User logon history
- User and station interrogation
- Function delegation

Password Ageing

Passwords are less likely to be compromised if they are changed on a regular basis. SENTRY enforces such changes by the provision of standard password aging mechanisms for both usercodes and accesscodes. Many of the password aging values and options are maintained as global information, thus simplifying the administration of establishing password aging for users. For specific users, these global values may be changed to suit individual requirements.

Password Change Control

With SENTRY, the Security Administrator can implement password aging using the following attributes and options – see the table on the following page.

Option	Description
DAYSACTIVE	Maximum life of a password.
DAYSWARNING	Period when users are warned of impending password expiry.
MINPWLIFE	Period immediately after a change of password during which the password may not be changed again.
OLDPWLIST	List of previously used passwords that may not be re-used.
MINPWLEN	Minimum number of characters that may be used for a password.
MAXPWLEN	Maximum number of characters that may be used for a password.
PASSWORDGENERATION	Allow self selected or system generated passwords.
FIRSTIMECHANGE	Enforce user change of an allocated password.
DISALLOWNUMERIC	Disallow the use of numeric characters.
CHECKEXCEPTDICT	Debar the use of specified passwords.

Additionally, SENTRY will also disallow the following:

- Use of repeated character strings
- Use of character sequences
- Passwords that are the same as the usercode or accesscode name
- A new password that is similar to the previous password

SENTRY provides the mechanisms to maintain password dictionary items for use with system-generated passwords and also to establish the list of password exceptions to be checked against self-selected passwords.

Users are allowed to change their password at any time, unless within the minimum password life period. During the warning period, users are automatically presented with the password change screen, which they may optionally use to change their password. After the password expiry date, users are forced to change their password. Failure to do so at this time will result in the usercode or accesscode being suspended.

Note
All password change screens and end-user messages are displayed in English, French, German, Dutch, Spanish, Finnish or Portuguese; the Security Administrator may determine the preferred end-user language, which may be allocated on an individual user basis.

Password Allocation

The Security Administrator may allocate a password at any time via the Password Allocation function. Passwords may also be allocated when establishing password aging or when reactivating suspended users. SENTRY provides an option which, when set, will force users to change an allocated password at next logon. There are no restrictions on the format of passwords allocated by the Security Administrator.

Logon Controls

SENTRY provides several logon control mechanisms, namely:

- The Security Administrator may deactivate or reactivate any usercode or accesscode at any time.
- The Security Administrator may select the number of consecutive invalid logon attempts that will be tolerated. In addition, a timeframe may be optionally specified. After the count has been reached, SENTRY will logically deactivate the station and ignore any further input. A deactivated station may be reactivated only via SENTRY. When the VIOLATIONLIMIT attribute has been assigned a value, SENTRY will maintain a logon violation count for the usercode or accesscode. When exceeded, the usercode or accesscode will be suspended.
- To complement the standard COMONLYLOGON facility, SENTRY introduces the NOLOGON attribute which, when set, will disallow any logon for the specified usercode. This attribute is useful to prevent any attempted logon using a production usercode.
- SENTRY also introduces the concept of the Controlled user. A Controlled user is a usercode, often with special privileges, which is used periodically for emergency purposes, for example, troubleshooting. A Controlled user may be established as a one-time or multi-session user and the Security Administrator may also define a time-out period. Before such a user is allowed access to the system, the usercode has to be enabled either by the Security Administrator, or optionally by another delegated user or operator. If the one-time option has been specified, after logging on with a Controlled usercode, the usercode may not be used again.

User Logon History

When logging on to the system, SENTRY provides options to display details of the last logon for the usercode and/or accesscode and the current count of invalid consecutive logons, if any. This feature provides a useful check for users logging onto the system to ensure that no fraudulent logon has been attempted.

User and Station Interrogation

For user interrogation, the Security Administrator may interrogate the status of an individual user or multiple users. In the latter case, the information displayed may be filtered for usercodes or accesscodes whose passwords are within the minimum password life period, in warning mode, overdue or expired. A list of all non-password aged users may also be displayed.

For station interrogation, the current list of offending or deactivated stations will be displayed.

Function Delegation

In many installations, security personnel are available only during certain hours of the day. For contingency, the Security Administrator may delegate SENTRY functions, for example allocating passwords or reactivating suspended users, 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.

System Commands

CENSOR allows the administrator to authorise the use of specified lists of system commands by designated users who would not otherwise have the necessary privileges to do so (i.e. users who do not have systemuser or privileged status). The administrator may also require the user to confirm this authorisation by re-entering the password (for the session usercode) before some, or all, of these commands are actioned.

CENSOR is designed to allow administrators to reduce the requirements for privileged or systemuser usercodes on a system and to allow delegation of ODT functionality while maintaining security restrictions and accountability.

Key Features

- Delegation of system commands
- Delegation by usercode or accesscode
- User verification at time of input
- Logging of command, usercode, accesscode and station name
- Audit available via the reporting module, SECURE
- User interface
- Function delegation

Delegation of System Commands

The delegation of system commands via CENSOR removes the need to give privileges to a user in order for that user to use a certain system command. Consequently, users who do not need privileges, will not have them, leading to a net reduction of privileges (and risk) on the system.

CENSOR administrative functions are integrated into the simple-to-use, established screens of SAFE, and additions and updates to command authorisations are performed dynamically with immediate effect.

System commands which may be used for both interrogation and update purposes may be delegated to users as 'interrogation only', thus restricting update functionality.

Delegation by Usercode or Accesscode

The delegation of system commands is accomplished through a hierarchy. For example, some inquiry commands may be open to all users, whilst more powerful commands may be made available on an individual basis. The hierarchical levels are defined as follows:

- Level 1 - All MARC users
- Level 2 - All users defined to CENSOR
- Level 3 - Individual usercode
- Level 4 - Individual accesscode

Each command list may contain a maximum of 30 commands. A normal usercode user can therefore be authorised to use up to 90 commands, whilst an accesscode user can be authorised for up to 120 commands. A maximum of 147 user definitions may be established.

Below is an example of the use of Censor to restrict the commands allowed for user01_02.

```
Version 03.00.0797 * SECURITY ADMINISTRATION FACILITY * 11:55 16-01-2001
--- C E N S O R : Command Delegation ---
ALLOCATE COMMANDS
USERCODE: USER01_02
Command PwV Command PwV
▶PER MT ▶RY MT
▶PER PK ▶PG MT 44
▶PER NP ▶CL NP
Note: You may use '?' as a wildcard token
COMMAND ... P = Parent H = Home
B = Base Q = Quit
```

Verification of Identity

The Security Administrator may optionally enforce the confirmation of the user's identity when privileged commands are input. This alleviates potential security problems, in the event that a workstation is left unattended by a user who is permitted to use sensitive or 'dangerous' system commands. CENSOR verifies the user's identity by requiring the re-entry of the user's password before the command is accepted.

Audit and Reporting

The user's identity is logged to the system log together with the command used and the station name. Successful and failed confirmations are also logged for those commands requiring verification of the user's identity.

The CENSOR commands report is available through the SECURE module, which supports all security software products developed by Locum Software Services Limited.

User Interface

CENSOR allows the Security Administrator to establish a two-character code for the CENSOR directive. The user interface to CENSOR is via input on MARC's action line of the two-character code established for the directive. By prefixing the system or COMS command by the two-character code, a user is able to use the commands for which he or she is authorised. Entry of the two-character code with no further input will display the CENSOR HELP screen. Entry of the two-character code followed by WHICH displays the commands delegated to the user. All user responses are in the familiar MARC format.

Function Delegation

In many installations, security personnel are available only during certain hours of the day. For contingency, the Security Administrator may delegate CENSOR functions, for example allocating commands, to 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.

Multi-Host Operations

CHAIN is a utility that allows the Security Administrator to determine and establish the level of synchronisation within the network. CHAIN synchronises Userdatafiles on a network of MCP/AS hosts. In particular, password propagation frees both the user and the administrator from the headaches of password management across multiple systems.

CHAIN allows you to establish a “security hub” for your system. With CHAIN, the entire security system is tied together for greater efficiency and increased security.

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 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, remote printer or installation-written program.

CHAIN Components

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 TCPIP NATIVESERVICE 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.

Reporting - SECURE

SECURE provides reporting for the SAFE package.

Having a security system for your MCP/AS environment is less effective if you do not have the ability to monitor and audit security events.

SECURE is an efficient and easy-to-use product, providing administrators and auditors with a total security reporting solution with three different modes of operation; Batch, Interactive, and Realtime reporting.

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 either to the terminal in paged format (Browse Mode) or to a print file. In the latter case, SECURE provides facilities to control the routing of printed output.

Time-based reporting enables the user to produce reports covering a specific time range without complicated log consolidation. The only action the user performs is designating the time period; SECURE identifies the required sumlog files to be analysed.

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

The majority of these reports may be selected as Alert events for Realtime reporting.

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 disk

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.

Below is an example of a SECURE report on screen – the Window Accesses Report.

```
Version 03.00.0485 * SECURITY ADMINISTRATION FACILITY * 12:19 16-01-2001
--- S E C U R E : Security Reporting ---
WINDOW ACCESSES on SERIAL 1111 BROWSE
(Full log) (lines 18-28 of 28)
15/01/01 15:41:03 39810 MARC/1 (Direct) UC=* STA=ODT
15/01/01 16:00:51 39811 MARC/1 (Direct) UC=DUNK STA=IP192_168_1_212/TLX0501
15/01/01 16:00:54 39811 CANDE/1 (MCS) UC=DUNK STA=IP192_168_1_212/TLX0501
15/01/01 16:07:46 39811 CANDE/1 (MCS) UC=DUNK STA=IP192_168_1_212/TLX0501
16/01/01 11:45:30 39815 MARC/1 (Direct) UC=DUNK STA=IP192_168_1_212/TLX0501
16/01/01 11:45:42 39815 SAFE/1 (Remote) UC=DUNK Prog=SAFE
          STA=IP192_168_1_212/TLX0501
16/01/01 11:49:44 39816 MARC/1 (Direct) UC=DUNK STA=IP192_168_1_212/SAFELS01
16/01/01 11:49:48 39816 SAFE/1 (Remote) UC=DUNK Prog=SAFE
          STA=IP192_168_1_212/SAFELS01
-- End of report --

Entries found: 25
COMMANDS: Add Exit First Last Next Prev Save + -
```

Report	Batch	Interactive	Realtime
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	●	●	
Run-time Usercode Changes	●	●	
CENSOR Commands	●	●	
Installation Records	●	●	
Overdue Users	●	●	
Userdatafile Changes	●	●	●
SAFE Audit	●	●	●
CHAIN Audit	●	●	●
Sumlog Integrity	●		
Privileged Actions			●
Miscellaneous Security Actions			●
Security Policy			●

The above table shows all the available reports from Secure.

AdminSock

Many modern organisations operate a number of different hardware platforms and disparate operating systems. In this environment an organisation may wish to adopt a single, enterprise wide security software solution with a single sign on principle.

AdminSock is the agent required to interface the enterprise-wide security solution with the MCP A/S system. It can be run stand alone, or in conjunction with the full Safe & Secure product.

Key Features

- MCP A/S agent for an enterprise-wide security server.
- Two modes of operation – Interactive & Silent.
- Userdatafile and COMS Cfile maintenance.
- Reconciliation function
- Validation function.
- English-text commands.

UserSock

Provides a TCP/IP socket interface to client-server applications in which end-users bypass the traditional MARC sign-on procedure.

UserSock allows an installation to implement access controls for such users.

Key Features

- Simple method of introducing access controls.
- Four functions available – User validation, Password ageing information, Password generation and Password change.
- Sample code provided to ease the integration process between UserSock and the client server application.

SAFESurvey

SafeSurvey is a security utility that helps MCP/AS Security Administrators to maintain a secure system by highlighting any areas where the system's security may be at risk. For example, SAFESurvey analyses and reports on the definitions declared in the Userdatafile and COMS Cfile. Any definitions that pose a threat to the security of the system are identified and the Security Administrator is then able to take the necessary action.

Running SAFESurvey on a regular basis keeps the Security Administrator informed about the status of the system's security, highlighting specific areas where the security of the system may be at risk.

Key Features

- System penetration test and report
- System configuration analysis
- Userdatafile and COMS Cfile compatibility test
- File security analysis
- User-friendly reports

System Penetration Test and Report

In order to ascertain the vulnerability of the system, SAFESurvey analyses the user definitions declared in the Userdatafile and performs a series of tests to determine the ease by which a user may gain access to the system. Passwords are tested for popular words, repetitive characters, sequences and reverse sequences. Passwords may also be checked against an installation's own dictionary file.

The Password Report lists 13 password profiles (or 21 if an installation's own dictionary has been supplied). Each profile poses a threat to the security of the system. For example:

Usercodes with **NO** password

Usercodes with an **EASY-TO-GUESS** password

Usercodes with a password **IDENTICAL** to the usercode name

Totals are printed against each profile and the names of the user definitions matching a profile are listed.

System Configuration Analysis

SAFESurvey analyses the system's configuration and reports the following information:

MCP runtime options

TCP/IP security rules

InfoGuard/SECOPT configuration

Remotes authorisations

Dangerous disk files
Dangerous codefiles and public files

Userdatafile and COMS Cfile Compatibility Test

SAFESurvey analyses the Userdatafile and COMS Cfile and supplies the Security Administrator with the following data:

Userdatafile statistics
COMS Cfile statistics
Userdatafile/COMS Cfile compatibility
Usercode privileges
Remoteusers
Station and Program loopholes

File Security Analysis

SAFESurvey analyses the files on the system and provides the Security Administrator with the following information:

- All files that have a security type of PUBLIC
- Code files with special privileges, including:
 - Privileged programs
 - Privileged transparent programs
 - Compilers
 - Secadmin programs
 - Secadmin transparent programs
 - Tasking programs
 - Tasking transparent programs
- Codefiles with special operational privileges:
 - Control programs
 - Suppressed programs
 - Resident programs
 - Restricted files
 - (Locked files and programs)

User-Friendly Reports

SAFESurvey produces a number of reports in a clear, concise and non-technical format. The Security Administrator has the option of printing ALL the reports or a selection of reports. The reports may be sent to a diskfile or to a printer. If the reports are sent to a diskfile, they will be in text format so that they can be easily transferred to a PC and incorporated into a spreadsheet application.

Some example reports are shown on the following pages.

HEALTHCARE CHECK

Definition	Default user	Privilege
Program COMSPROGRAM	LGH78	None
Program CPRPPROGRAM	BIGCLONE	Secadmin
Program DIR121	S89USER	Systemuser
Program ECHO	LGH78	None
Program OLDDIR	KHJKN5	Not in UDF
Program SURE	CVG1	None
Program TESTPROGRW	DBASE1	Not in UDF
Station AP9208	TGB	Cont Logon
Station DCCLP_TDSTA00		Super User
Station DCCLP_TDSTA04		Cont Logon
Station DCCLP_TDSTA09		Super User
Station IP10_0_0_65/B7895	LGH78	None
Station IP10_0_0_65/B7896B	ICXFER	Cont Logon
Station IP10_0_0_65/TCPB_1	ICXFER	Cont Logon
Station NEXUS0		Super User
Station NEXUS1	STUBBORN	Super User
Station ODT/1		Super User
Station ODT/2		Super User
Station PSEUDO00000	STUBBORN	Not in UDF
Station UUASTA10	B7GHJ	Super User

HEALTHCARE CHECK

Default User attributes

DEFAULT_WINDOW = MARC
 WINDOW_LIST = WL_ADMIN
 DEFAULT_TRANCODE = NONE
 STATION_LIST = ALL
 SECURITY_CATEGORY_LIST = ALL
 STATION_SECURITY_OVERRIDE = N
 CONTROL = N
 INSTALLATION_DATA = ID_DEFAULTUSER
 CLOSE_ACTION = 2 (Previous Window)
 CLOSE_WINDOW = NONE

HEALTHCARE CHECK

Default Station attributes

HOSTNAME = MOA4A
 DEFAULT_WINDOW = MARC
 DEVICE_TYPE = DEFAULTDEVICE
 DEFAULT_TRANCODE = NONE
 MAP_LIST = NONE
 DEFAULT_USERCODE = NONE
 DEFAULT_ACCESSCODE = "."
 DEFAULT_CHARGECODE = "."
 SECURITY_CATEGORY_LIST = ALL
 TRANCODE_POSITION = 1
 TIMEOUT_INTERVAL = 0:0
 CONTROL = N
 SYSTEM_USER = Y
 SUPER_USER = N
 TRANCODE_OVERRIDE_ALLOWED = N
 PRIVILEGED_USER = Y
 CONTINUOUS_LOGON = N
 INSTALLATION_DATA = NONE
 CLOSE_ACTION = 1 (Close Window)
 CLOSE_WINDOW = MARC

No of superuser stations 11

No of continuous logon stations	4
No of stations with default usercode	7
No of stations with default invalid usercode	2
No of stations with default Secadmin usercode	1
No of stations with default Privileged usercode	2
No of programs with default usercode in Cfile	7
No of programs with default invalid usercode	2
No of programs with default Secadmin usercode	1
No of programs with default Systemuser usercode	1

MCS STATUS REPORT

MCS No.	Mixno	Status	Stations	Mcs Name
1	51877	Active	65	SYSTEM/CANDE
2	51881	Active	33	SYSTEM/COMS
3	0	Inactive	22	SYSTEM/RJE
4	0	Inactive	3	SYSTEM/X25
5	0	Inactive	23	SYSTEM/DIAGNOSTICMCS
6	0	Inactive	10	SYSTEM/RJEBSC
7	0	Inactive	7	SYSTEM/BNAMCS
8	0	Inactive	4	SYSTEM/COMS/ENTRY
9	52071	Active	2	SYSTEM/STATION/TRANSFER
10	0	Inactive	1	SYSTEM/COMS/KERNEL
11	52328	Active	1	COMS/ODT/DRIVER
12	0	Inactive	1	GEMCOS/MCS
13	0	Inactive	1	SYSTEM/ASSISTANT
14	0	Inactive	1	SYSTEM/MHS/MSL
15	51910	Active	2	SYSTEM/TELNET
16	0	Inactive	1	SYSTEM/APL

USERDATAFILE STATISTICS

Userdatafile: *SYSTEM/USERDATAFILE ON WORK. Version 1 file.

Total no. of Usercodes	1251	(389 Suspended)
No. of Security Administrators .	33	(9 Suspended)
No. of Privileged Usercodes	66	(22 Suspended)
No. of Accesscode entries	385	(103 Suspended)
No. of Remoteuser records	56	
No. of RemoteuserID records	16	
No. of Profile entries	95	
No. of Template entries	30	
No. of Common Password Groups ..	24	
No. of User Sets	23	
MU command (MU model)	Disabled	

This page is intentionally blank.