Safe & Secure

Access Control

Safe & Secure’s Access Control mechanisms provide Security Administrators with password change and logon control facilities on ClearPath MCP hosts.

Key Features

- Password aging for both usercodes and accesscodes
- Password change controls
- Logon controls
- Station controls
- Violation limits
- Controlled users
- Sessions 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. Safe & Secure 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.

Password Aging

Passwords are less likely to be compromised if they are changed on a regular basis. Safe & Secure 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 Controls

The Security Administrator can implement password aging using a variety of attributes and options. Mechanisms are provided to maintain password dictionary items for use with system-generated passwords and 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 use to change their password.

After the password expiry date, users are forced to change their password. Failure to do so at this time may result in the usercode or accesscode being suspended. All password change screens and end-user messages are displayed in English, French, German, Dutch, Spanish or Finnish; the Security Administrator may determine the preferred end-user language, which may be allocated on an individual user basis.

The Security Administrator may allocate a password at any time. Passwords may also be allocated when creating usercodes/accesscodes, establishing password aging or reactivating suspended users. Safe & Secure 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.

The Security Administrator can control the structure of new passwords input by users by choosing to set any of the Password Structure parameters; enforce a Minimum Password Length or a Maximum Password Length, ensure passwords contain at least one Uppercase Character, Lowercase Character, Numeric Character or Special Character (i.e., non-alphanumeric), or enforce a Minimum Number of Character Types.
Logon Controls

Safe & Secure provides several logon control mechanisms, namely:

- The Security Administrator may detect the number of consecutive invalid logon attempts that will be tolerated. After the count has been reached, Safe & Secure will deactivate the station and/or user and ignore any further input. A deactivated station may be reactivated only via Safe & Secure.
- When logging on to the system, Safe & Secure 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 on to the system to identify any attempted fraudulent logon.
- Safe & Secure 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.

Station Control

For station control, the current list of offending or deactivated stations will be displayed. From the list displayed, the Security Administrator may reactivate all or individual stations.

Violation Limits

When the VIOLATIONLIMIT attribute has been assigned a value, Safe & Secure will maintain a violations count for the usercode or accesscode. When exceeded, the usercode or accesscode will be suspended until reactivated by the Security Administrator.

Controlled Users

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 to access 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.

Session Control

For session control, a list of usercodes or accesscodes currently logged on the system is displayed. From the list displayed, the Security Administrator may terminate all or individual sessions for a particular user.
Safe & Secure is a component of Locum 360, a comprehensive and integrated security solution. For more information on Locum 360, Locum’s ‘full package’, please visit www.unisys.com.