Safe & Secure

Feature Sheet

Safe & Secure is Locum Software’s highly-regarded and well-established security software for Unisys ClearPath MCP hosts and is a component of Locum 360, a comprehensive and integrated security solution. Safe & Secure centralizes and simplifies security administration while offering, through AdminDesk, a wide range of powerful tools and inquiry facilities. Safe & Secure’s set of Security Policy Options are designed to be tailored to comply with the customer’s own policy requirements.

AUTHENTICATION

Password aging is implemented by Safe & Secure’s own SAFEAGING mechanism, which can be applied both to usercodes and accesscodes. Accesscode aging allows full synchronization of the password across all owning usercodes. Global values for aging parameters such as Daysactive and Dayswarning make SAFEAGING easy to implement and manage.

A range of Password Control and Password Validation options allows you to define exactly how aging will work on your system, and also allows you to control the strength of passwords that your end-users select. In addition, you can establish a list of passwords that will be disallowed as password selections.

Often the administrator or help-desk worker needs to verify the identity of a caller, particularly in the case of a password reset request. Safe & Secure’s User Verification feature is a shared secret mechanism, whereby a security question and answer is stored in the user definition. The end-users can be asked to input their own question and answer.
AUTHORIZATION

Safe & Secure provides easy access to all Unisys user attributes to provide individual user authorizations. Moreover, Safe & Secure implements the ability to delegate Administrator Rights, using objects and permissions to create sub-administrator status. For example, Help Desk personnel definitions can be created to allow only the resetting of passwords and reactivation of users.

In addition, Safe & Secure introduces the concept of Regimes, by which the user population may be partitioned to allow a Regime Administrator to control only their own users.

For computer personnel, System Command Authorization allows the Administrator to give a unique and specific command list to individual users, instead of handing out blanket privilege.
ACCESS CONTROL

Station Lockout and/or User Lockout can be enforced when an end-user reaches the set Maximum Logon Attempts. Both variations can be configured to auto-reactivate after a specified time period. The responsibility for manually reactivating stations rests with the Security Administrator.

The implementation of Session Limits as a user attribute allows extra control over active sessions. The administrator can view all active sessions on the system, and if required, terminate unwanted ones. Usercodes can also be designated as NOLOGON, so that for example, production usercodes are barred from initiating active sessions.

Occasionally, emergency access is required, usually for troubleshooting purposes. Safe & Secure’s Controlled Usercode feature allows emergency usercodes to be configured in case of such an eventuality. Control over these usercodes can be delegated to specific individuals.

ADMINISTRATION

Security Administration has never been easier than through AdminDesk, the GUI for Safe & Secure. The implementation of Profiles allows simple creation of new user accounts and modification of existing ones; the Template implementation allows the grouping of users by roles, so that when a user changes jobs within your organization, their authorizations and privileges will be automatically removed or changed; the Zonal Update feature provides simultaneous update capability across all your ClearPath MCP servers, subject to the necessary security clearances. For other powerful administrative features, refer to the AdminDesk Feature Sheet.
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.