

CSP PassPort®

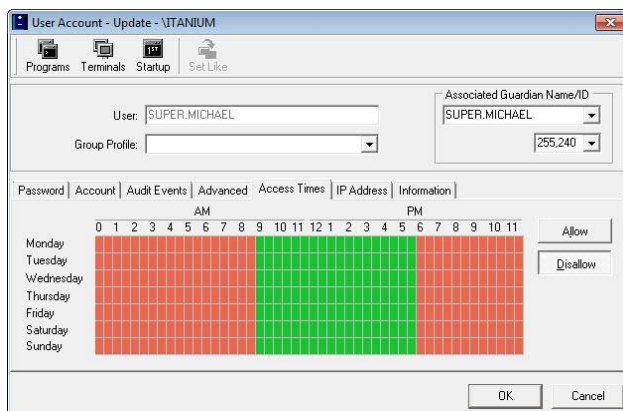
CSP PassPort® is a comprehensive security product for controlling and auditing user access to HP NonStop Servers. It offers superior user authentication, session control, accountability and auditing capabilities not available with Guardian or Safeguard security.

CSP PassPort provides comprehensive user and command control, password quality enforcement and auditing. It controls and filters user access to systems, programs and commands according to customized user profiles.

All user terminal input/output operations (including OSS) can be monitored via an easy-to-use GUI interface, while an audit process records all user activities.

Configurable User Aliases and Groups

CSP PassPort® users are aliases to Guardian IDs. Controls can be imposed on those aliases that are unavailable with other software solutions, including applying different function and access restrictions on each CSP PassPort user, even if they are aliased to the same underlying Guardian ID.



Key Features

- Restrict users, including those with powerful IDs, to authorized operations
- Restrict users to assigned work stations, functions and specified hours and days
- OBEY / EXEC file validation
- Merged Audit provides centralized auditing of events from multiple systems
- User Authentication SEEP prevents users from logging on outside CSP PassPort
- Pass-phrases up to 64 characters in length for users authenticated via CSP PassPort
- Time restrictions by command & program
- Eliminate the need to disclose sensitive SUPERID passwords to users so they can execute powerful commands
- Scrutinize the use of utility commands such as SCF, SQLCI and FUP
- Keystroke level auditing
- Advanced password quality standards
- Uses the same audit trail format as Safeguard for integrated reports
- Controls client connection by IP address
- Use system-based authentication methods or authentication by third party products such as RSA SecurID® Authentication server
- Supports Safeguard or non-Safeguard aliases

User Authentication Options

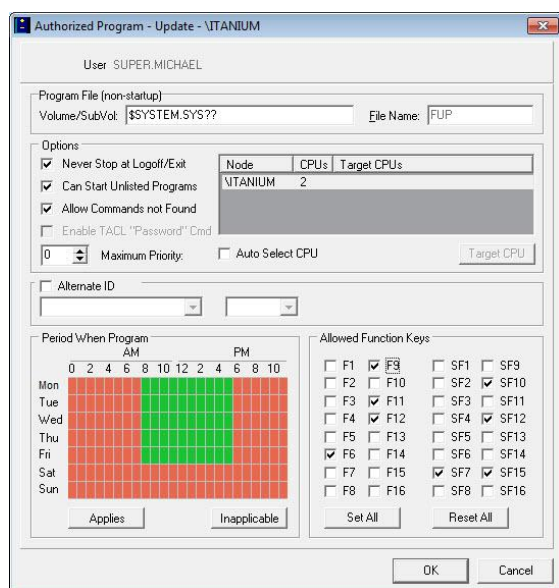
An Authentication SEEP (Security Event Exit Process) prevents users from logging on outside of CSP PassPort. Use system-based authentication methods or authentication by third party products like RSA SecurID® Authentication Server.

CSP PassPort enforces strict control over user password quality, including minimum password length, duration, history and common word avoidance.

[continued overleaf]

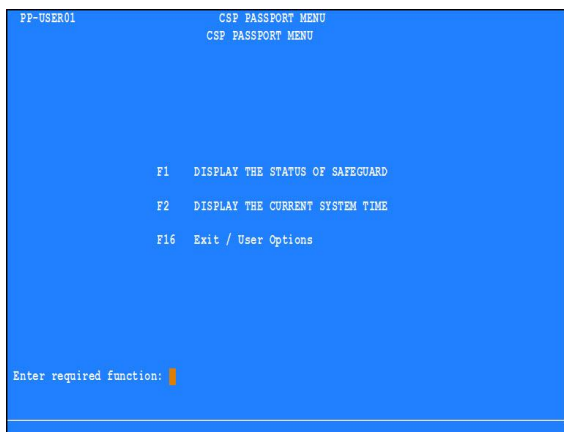
Complete Session Control

CSP PassPort® restricts functions at the program level, and can even control access to individual commands within a program. Programs and commands can also be defined to run under a different Guardian ID, transparent to the user.



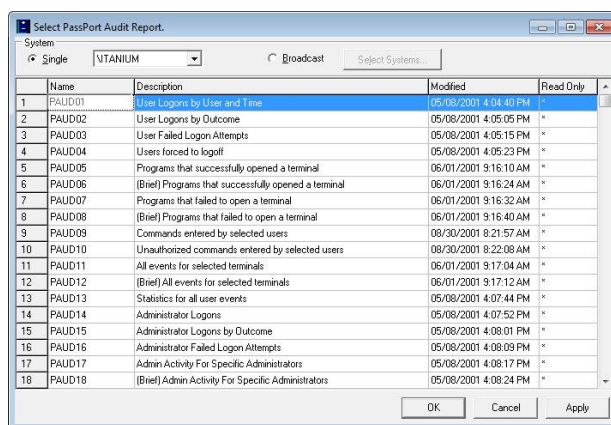
Restrictive Menu of Commands

Using PPMenu, CSP PassPort® users can be assigned a predefined menu of commands invoked at logon. The menu allows execution of configured commands and programs, while preventing further system access. This feature is ideal for operations using powerful IDs and sensitive commands.



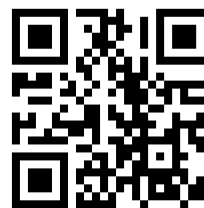
Extensive Standard Reporting

CSP PassPort® provides multiple sets of standard reports. And since it uses the same audit trail format as Safeguard, CSP PassPort® reports can be easily integrated with those from Safeguard using CSP's Auditview® product.



Powerful Custom Reporting

CSP PassPort® standard reports are easily customizable using filters which allow specific data to be extracted on a regular or ad-hoc basis.



Contact Computer Security Products for more information

Tel: 1-800-565-0415 or 1-905-568-8900

Email us at: Sales-csp@cspsecurity.com

Visit us at: www.cspsecurity.com