CSP NetPass

Network Password Quality Control

CSP NetPass

A key security measure is the enforcement of strong passwords.

CSP NetPass provides a unique solution for both enforcing password quality and for managing passwords across multiple HP NonStop systems.

Central Management

Using the CSP Windows client, administrators can:

1. Develop and apply password quality rules
2. Change passwords for users across multiple NonStop systems at once

NetPass servers running on each NonStop system are used to propagate the password based on a common username.

Each new password is “tested” on each server to ensure compliance with NetPass and local system password rules.

Communications between the NetPass servers and the Windows client are fully encrypted for security.

Group managers and their aliases can change the passwords for any user or alias in their group. Super.super and its aliases can change passwords for any user or alias.

Password Quality Rules

Password quality rules can be specified to include:

- Minimum password length
- Minimum alphabetic characters
- Minimum numeric characters
- Maximum same characters
- Maximum consecutive characters
- Passwords cannot be the same as the logon name
- Passwords cannot be the same as part of the logon name
- Check passwords against a dictionary
- Check parts of password against the dictionary

Users can change their own passwords

In addition to the administrator changing passwords, users can also use NetPass to change their passwords across multiple systems using the Windows client or a simple TACL utility.

Password Quality SEEP

NetPass can also run as a SEEP. In this mode, the password quality rules are applied on Safeguard protected systems – and across multiple nodes - regardless of who initiates the password change.

Hewlett Packard Enterprise Silver Partner Technology Partner

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