



XYGATE PASSWORD QUALITY FOR HPE NONSTOP

Improve password security and compliance for HPE NonStop systems



Key benefits

- Easy to use
- Automatic enforcement of password rules
- Warning messages to facilitate compliance
- Resist password attacks and prevent expensive security breaches

Passwords are foundational to supporting the security structure of a system, multiple servers, data center, or even an enterprise. Passwords are also the most common method of system compromise. Detection of fraudulent use is difficult because a compromised password continues to be used by its authorized user. When fraud is discovered, the authorized user rightly, or wrongly is held responsible.

Keeping passwords up-to-date across multiple nodes is a cumbersome task, even when users have only one user ID. Many users have multiple user IDs, along with one or more aliases. Users tend to choose easy-to-remember passwords and re-use them repeatedly. Hackers exploit this simplification, basing password assaults on personal information about users. Another frequent type of attack compares encrypted passwords to a list of words that have been encrypted with the same algorithm as the passwords. Passwords composed of commonly used words will be cracked easily by such dictionary attacks. [HPE NonStop servers](#) are the systems of record in many Fortune 100 enterprises of this world and are classified under the [mission-critical servers](#) category—securing and protecting the access to these [fault-tolerant servers](#) is of paramount importance.

This is where the value of XYGATE Password Quality (XPQ) for [HPE NonStop systems](#) becomes obvious. XPQ installs easily onto the HPE NonStop environments and runs in conjunction with Safeguard or independently. For Guardian user IDs and Safeguard Aliases, XPQ protects passwords in two different ways. First, it reduces password vulnerability by comparing a password being defined to a list of rules specified for governing quality. Alternatively, a random password can be generated that meets pre-specified rules for a strong password. In both cases, it is much harder for hackers using a dictionary attack or personal knowledge about the users to compromise a password that contains different types of characters, such as numbers or special characters.

Key features

- Single-site administration
- Conditional processing exceptions
- User-defined, system-generated, or split password capabilities
- Password updates across your HPE NonStop network

FLEXIBLE AND ENFORCEABLE RULES

XPQ checks changed passwords through its PASSWORD program, or the Safeguard ADD or ALTER commands. Rules can be specified for any combination of nine different quality characteristics, which include:

- Minimum number of rules
- Minimum number of characters and control characters
- Minimum number of upper- and lower-case alphabets
- Minimum number of numbers
- Minimum number of special characters such as \$, %, or #
- Maximum number of repeating consecutive characters
- Maximum number of repeating characters, not necessarily consecutively
- No characters from a list

NETWORK PASSWORD UPDATE

Frequent changes make passwords more resistant to attack. With XPQ, updating the passwords for Guardian user IDs and Safeguard Aliases can be initiated from any node where the user has access. XPQ encrypts the transmission of the new password to all the HPE NonStop nodes where the corresponding user ID or alias is valid. Owner “designation” and “resets” define owners of the password change operation for any user ID or alias, even to the point of excluding the user ID or alias owner from changing the password themselves. If an emergency occurs and case-sensitive user IDs such as SUPER must be used, you can prevent the user ID from changing its password.

USER DEFINED OR SYSTEM GENERATED

In addition to checking user-defined passwords against the management-specified quality rules, XPQ can generate passwords that conform to the specified rules. System-generated passwords can be made mandatory, or users can choose to have their passwords generated via the PASSWORD program.

AUTOMATIC EXPIRATION

New users can be encouraged to change their password at the initial login. This automatic expiration helps ensure that before a new user interacts with the system, only that user knows the password for their user ID.

PASSWORD SPLITTING

To restrict access to powerful user IDs, XPQ enables the password for such case-sensitive user IDs to exist in pre-defined parts or components. Each component is assigned to a different custodian user and all components must be entered to make the user ID accessible.

CUSTOM APPLICATION PASSWORDS

Through a custom-written user exit, XPQ can also synchronize password changes with a custom application that has a separate password database.



Data sheet

A mechanism for **quality control** and standardization to **strengthen passwords** for HPE NonStop user IDs and Safeguard Aliases.



Top 10 most common passwords

123456	qwerty
password	123456789
12345	1234567
12345678	princess
football	1234

WARNING MODE

Like Safeguard, XPQ can run in warning mode. When a password does not conform to the specified rules, it is flagged with a warning message in the audit log and the user receives a warning indicating, which rule or rules the password failed.

You can use warning mode initially to accustom users to the new rules. XPQ can also be placed in warning mode for specified groups of users who share the same password quality rules.

HELP DESK

Enable the help desk to change passwords, even for pre-selected groups of users. A Windows-based GUI allows password resets without logging onto TACL.

ORDERING INFORMATION

XYGATE Password Quality for HPE NonStop can be ordered using the PIDs listed in the following table:

Product	Product Id (L-Series)	Product Id (J-Series)
HPE NonStop XYGATE Password Quality	BE248AC	QXPQ

LEARN MORE AT

hpe.com/info/nonstop

xypro.com

Make the right purchase decision.
Contact our presales specialists.



Chat



Email



Call



Get updates

**Hewlett Packard
Enterprise**

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

a50004729ENW, August 2021