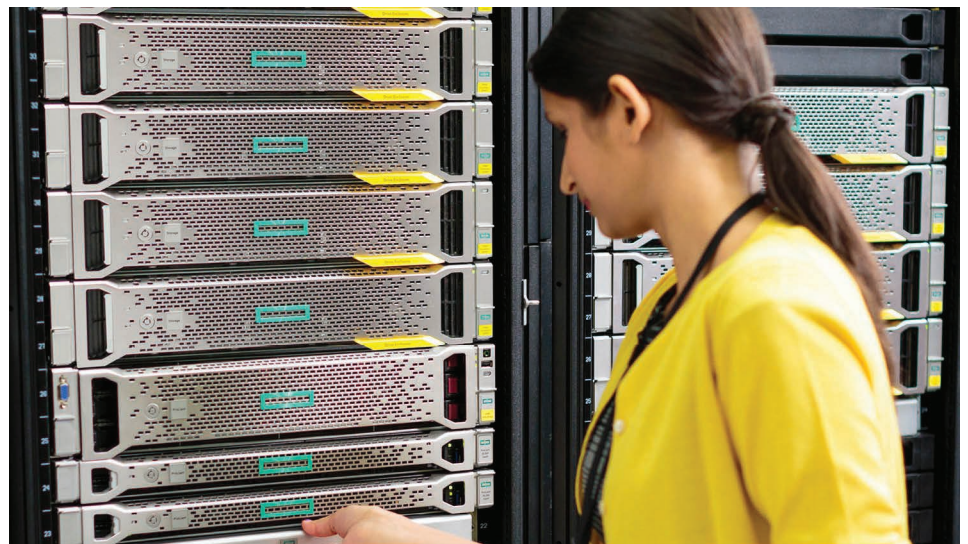




XYGATE User Authentication

Multi-Factor Authentication (MFA) and Single Sign-On (SSO) on HPE NonStop Servers



MFA and SSO for NonStop

XYGATE User Authentication enables the integration of your corporate single sign-on solution with the HPE NonStop server by supporting direct authentication with OpenLDAP, Microsoft® Active Directory, RADIUS, or RSA SecurID tokens.

Security—a key cornerstone

Security is paramount in any mission-critical environment, whether it is government, military, or private. Unless the appropriate security infrastructure is in place, the entire organization is at risk. To defend against ever-increasing attacks, most organizations must adopt a process of hardening their environments to protect sensitive information adequately. Strong user authentication and encryption technologies are adopted to restrict access to the server and to protect information from unauthorized access. In many cases, users are issued multiple IDs and passwords in order to access different applications or servers. This proliferation becomes a significant challenge for both security managers and individual users. Often there is a trade-off between security and manageability; and without the appropriate underlying security, the whole business is at risk.



Single sign-on (SSO)—simplifying integration

Maintaining a secure server requires continued administration on the part of the IT manager. Provisioning users is an essential aspect of security and can become burdensome. Many large organizations use single sign-on (SSO) solutions to manage their user base. This makes it easier for users to avoid potential confusion over multiple passwords and user IDs for different systems and applications. In addition, SSO solutions help reduce the administrative overhead associated with adding, reclassifying, and deleting users as well as resetting passwords when users forget them.

MFA for HPE NonStop servers

Stealing user credentials are the most common way to compromise a system. For too long, a single user name and password combination were relied on to protect the most critical assets. Multi-factor authentication was introduced as a practical way to add a second layer of security to traditional user name/password authentication. MFA requires a user name/password plus either something you have (token) or something you are (biometrics). Security frameworks are also making MFA a requirement. For example, PCI-DSS requirement 3.2 now requires any non-console administrator access to authenticate via MFA. On the NonStop, this can be accomplished using XUA. XUA can integrate seamlessly with your RSA SecurID environment and enable MFA functionality for your NonStop users, making you more secure and compliant.

SSO for HPE NonStop servers

HPE NonStop systems deliver mission-critical infrastructure and are used by financial institutions, mobile operators, global manufacturing companies, hospitals, and other public sector organizations for their most critical business processes. For such enterprises, there can be no downtime, especially in a world of increasingly complex computing environments, ever-tightened compliance regulations, and soaring costs of security breaches. It is therefore essential for organizations to implement effective system and data security measures. Confirming the identity of users accessing your system is crucial to protect your systems and data. The native NonStop operating system and its Safeguard security infrastructure provide unique identification for users through Guardian user IDs and aliases, both with 64-character—strong password and passphrase support.



XYGATE User Authentication

XYGATE User Authentication (XUA), now included with all new HPE NonStop commercial systems, allows NonStop servers to integrate into an enterprise's SSO environment, thereby simplifying provisioning and management of NonStop users. Users can now access all of their authorized systems, including NonStop servers, using a single user ID and password. The user benefits from the simplicity of authentication while the administrator benefits from a reduced user ID and password maintenance burden. Overall, security is improved and costs are reduced for the enterprise with XUA.

XUA supports OpenLDAP, Microsoft Active Directory, RADIUS, and RSA SecurID multifactor authentication. It also extends NonStop server's authentication capabilities to support log-on controls based on attributes such as time, location, or requestor, and generates authentication audit.

All authentication activity is captured in the XUA audit log. XUA can capture audit data in up to nine different locations and formats. The audit data is also collected by the XYGATE Merged Audit software and can be reported, alerted, and transmitted to your Security Information and Event Management (SIEM) solution. XUA uses the Security Event Exit Process (SEEP) interface supplied by Safeguard to participate in the log-on process on the NonStop server. It requires that Safeguard be installed and running on the system. XUA empowers security administrators with the necessary tools to meet strict compliance requirements (such as PCI-DSS, SOX, and HIPAA).

XUA features and benefits

XUA enables enterprises to increase business efficiency, productivity, and authorized collaboration among employees, partners, customers, and suppliers. It strengthens user authentication and supports enforcement of corporate password policies while reducing the costs of user provisioning and management. Its features include:

- Enterprise SSO participation through LDAP and Microsoft Active Directory client interfaces
- Support for RSA SecurID tokens and RADIUS authentication
- Log-on controls based on ancestor program, requester program, port or IP address, time of day or day of week, or current logged-on user
- User impersonation support to reduce the need for sharing sensitive user passwords, for example—ability to log on as SUPER.SUPER but provide the individual user's password
- Authentication controls customized at the user or group level
- Enhanced log-on event audit collection and reporting capabilities
- Integration with SIEM solutions through XYGATE Merged Audit



Simplifying user authentication and management

In today's complex world of network access, it is essential to define a security policy and apply it to your system in order to protect your business-critical data and comply with government and commercial regulations. HPE continues to collaborate with partner companies such as XYPRO to offer single sign-on as well as superior security and encryption solutions for your HPE NonStop server platform. You can now gain peace of mind with XUA and meet authentication and compliance regulations for your NonStop environment.

Ordering Information




Product name	Product ID (L-Series)	Product ID (J-Series)	Product ID (H-Series)
XYGATE User Authentication	See Note 1	See Note 2	HXUA

Note 1: On the L-Series systems, XUA is included in the commercial NonStop OS bundle BE338AC. For systems using Telco NonStop OS (BE071AM), XUA is included in the security bundle (SKU BE014AC) which can be purchased separately.

Note 2: On the J-Series systems, XUA is orderable in the following ways:

- i) QSN52—the OS security bundle which includes XUA and 3 other products
- ii) QSN52U—on systems having the PID QSN51
- iii) QXUA—on all other systems

Learn more at
hpe.com/info/nonstop

 Make the right purchase decision. Click here to chat with our presales specialists.



Sign up for updates

© Copyright 2011–2012, 2015, 2017 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.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All other third-party trademark(s) is/are property of their respective owner(s).

4AA3-5035ENW, December 2017, Rev. 4

