Data sheet

HP NonStop Platform Security

Safeguard, Open System Services, and the HP NonStop Operating System Security Update Bundle

To help reduce insider data theft or data misuse, security experts recommend that only the minimum required access be granted to authenticated users. For the HP NonStop platform, Safeguard security software provides flexible authentication, authorization, and audit services based on a subject/object access control model that allows you to appropriately restrict authenticated users' access to Guardian system resources. Optional products that extend Safeguard's capabilities are available from HP as well as from NonStop security partners, including plug-in modules that allow consultation in authentication, password quality, and authorization decisions.

Security in the Open System Services (OSS) environment shares Safeguard's user management capabilities while providing a UNIX®-based authorization model. It also leverages Safeguard's audit management infrastructure to provide granular control over OSS auditing.

In today's networked world, modern operating systems must cooperate with other systems to protect sensitive data in transit—both user credentials such as user names and passwords and the data itself. HP now bundles support for two of the most popular methods of encrypting data in transit, Secure Shell (SSH) and Secure Socket Layer (SSL), with new NonStop system purchases. Most companies must also monitor security activities through security event reports and alerts. To meet this need, HP also includes XYGATE Merged Audit (XMA) on new systems. XMA greatly enhances Safeguard audit reporting capabilities with a GUI-based interface and a series of standard reports oriented toward demonstrating compliance with security regulations such as the Payment Card Industry Data Security Standard (PCI DSS). XMA also can aggregate audits from multiple sources, issue configurable alerts based on reported security events, and export audit information to many types of security incident event management (SIEM) systems, including ArcSight, now available from HP.

These three products are available for the NonStop server as part of the HP NonStop Operating System Security Update Bundle, which is delivered as part of the base system with new system purchases. The NonStop OS Security Update Bundle also can, for a moderate fee, be added to HP Integrity NonStop J-series and H-series systems purchased before September 2010. These products are provided by HP through a business relationship with NonStop security partners. NonStop SSH and NonStop SSL are developed by comForte 21, and XMA is developed by XYPRO Technology Corporation.

Guardian standard security infrastructure

The NonStop OS has a built-in security model for Guardian authentication and authorization. Each user is assigned to an administrative group, with the group manager having some degree of authority over its group members. One distinguished group, the SUPER group, has extra operational privileges. The manager of that group, whose user name is SUPER.SUPER, by default has total access to resources within the local system.

You can configure minimum and maximum password lengths, with support for up to 64-character passwords and pass phrases. You also can establish password quality requirements, such as a minimum number of uppercase, lowercase, alpha, numeric, or special characters. User passwords are stored in encrypted form, with support for the HMAC SHA256 algorithm.

The owner of an object such as a Guardian file authorizes access to it by configuring its read, write, execute, and purge access settings. These controls are similar, but not identical, to UNIX file permissions. Additional attributes may be configured, including running a program under the user ID of its owner and a "clear contents on purge" option for Guardian disk files to help protect your sensitive data.

A user who exists on multiple NonStop systems connected by an Expand network can create matching "remote passwords" between pairs of systems, which allow transparent remote access to system resources subject to the usual security checks.

Safeguard

The Safeguard product builds on Guardian standard security, adding more flexible user naming, extensive user management, much more granular access control to objects, and auditing. Safeguard is a standard product for Integrity NonStop J-series and H-series systems, and is available as an optional product for the G-series. Safeguard must be explicitly started and configured in order to take advantage of its capabilities.

Authentication

Safeguard supports both traditional Guardian user names and, for additional flexibility and usability, user name aliases. Safeguard gives you the ability to configure the management of user accounts, including:

- Password history depth
- Required password change intervals
- Automatic user account suspension after excessive log-on failures
- Temporary access suspension and restoration
- Account expiration
- Assignment of users to administrative or file-sharing groups, including security administration groups
- Audit generation controls for authentication, user account management, and authorization

You can reduce your help desk calls by configuring Safeguard to issue a warning to users when their password expiration date approaches, and by extending a postexpiration grace period to users. The authentication service lets users conveniently change passwords during log-on.

User authentication record contents track the times of the user's last successful and unsuccessful log-ons, and include a text description field that you can use to hold customer-specific data about each user such as contact information.

Some applications have a legitimate requirement to authenticate themselves as different users at different times so that they can perform tasks on behalf of each user. To meet this need, Safeguard provides an authorized Privileged Logon feature that allows designated applications to authenticate themselves as any user in the system without either password checks or delays in the case of authentication failures, but with the appropriate audit generated.

Authorization

Authenticated Safeguard users can define appropriate access controls for objects that they own such as disk files, volumes, and subvolumes; for devices such as printers, tape drives, PCs, and communications lines; and for named and unnamed processes and subprocesses.

You establish protection for an object by creating an access control list (ACL) for it. ACLs also are referred to as protection records. An ACL contains subjects or groups of subjects (users) and the access rights that they are granted for the object. Access categories include read, write, execute, create, purge, and ownership. ACLs also can explicitly deny access to designated individuals and groups, including the super ID. Safeguard allows different authorization privileges for an object to be assigned to the same user, depending on whether the user is connected locally or remotely. Safeguard allows definition at the individual user level of both a default Guardian security vector and a default protection record that is applied automatically whenever that user creates a new file.

Diskfile ACLs

You can protect a disk file in multiple ways: with a diskfile ACL specific to that file, a subvolume or volume ACL, or a more flexible disk file pattern or saved disk file pattern that includes wildcard support. Where multiple ACLs apply to the same file, Safeguard gives you control over the evaluation rules. For example, a volume ACL may override the ACL associated with an individual file on that volume, or vice versa.

Safeguard provides a persistence option for diskfile ACLs. This feature allows you to create an ACL for a file before the file exists and to retain the ACL even after the file is purged, which is useful in situations in which files are deleted and recreated with the same name during each run of an application.

Testing new ACLs

You can configure ACL warnings at the individual protection record level to test security settings for new applications or files without affecting security for applications and objects already in production on the same system. Guardian security settings control access to any object that has the Warning Mode attribute enabled in an ACL. Safeguard software then unconditionally audits the new access decision even if the ACL would deny the access. This allows the security administrator to easily and safely tune new ACLs.

Auditing

Safeguard audits log-on attempts, access to objects, and changes to the security settings for those objects. Audit controls allow your security administrators to:

- Detect unauthorized system access
- Detect unauthorized security setting changes
- Discourage users from abusing their authorized power
- Verify that policies are being followed

Your security administrators can specify the objects and the types of access to be audited. The security administrator decides which categories of system activity need to be recorded for later review.

Safeguard is used to configure audit controls for both the Guardian environment and the OSS environment. You can configure Safeguard to log each attempt to access an object, as well as the establishment of communication between client or server application processes. Each audit record includes such information as the object name, date, and time of the access attempt, and whether the attempt was authorized or denied. Safeguard can also be configured to log information about the user accounts and user ID activity such as when a user logs on or off.

Safeguard also logs changes made to user authentication records, an object's ACLs, and (unconditionally) its own configuration attributes. This record can be reviewed by management and auditors to verify that security administrator activity conforms to established management policies.

Safeguard offers a number of audit log management options, including audit rollover.

Safeguard configuration

You can configure Safeguard using the SAFECOM command-line interface. Safeguard has a rich set of documented application program interfaces (APIs), so you also can write your own programs to customize the software according to your needs and improve administrative productivity by simplifying complex and repetitive tasks.

By default, the SUPER.SUPER user has access to all system resources. Safeguard can be configured to restrict SUPER.SUPER access in various ways and improve the separation of duties.

Safeguard extensions

You can configure Safeguard to consult with a security event exit process (SEEP) when making decisions on user authentication, password quality, or access control. Multiple security partners offer SEEP-based products, and you can write your own SEEP if desired.

Open System Services

If you are used to working with UNIX or Linux security, you will find that OSS has a familiar security model. There is a superuser similar to root user, namely the SUPER.SUPER user and its Safeguard aliases. Every file has a user (owner) and a group associated with it. These can be changed through the *chown* or *chgrp* utilities or via the *chown()* API. OSS, like some UNIX systems, restricts the use of *chown()* to privileged users—only the superuser can change file ownerships, and the user can change the group membership of files to one of the supplementary groups only.

File permissions correspond to UNIX file permissions, with a few NonStop-specific extensions to enable features such as enhanced data integrity.

To allow more flexible control over file access, OSS supports ACLs. OSS ACLs are implemented as a part of the OSS environment rather than as Safeguard ACLs. OSS also supports a fileset-level Restricted Access attribute, which allows users to explicitly deny SUPER.SUPER (root) access to resources within the fileset that are protected by OSS ACLs.

OSS supports very granular controls over audit generation, including user and operation type. These controls are configured through Safeguard.

As in all other UNIX systems, OSS resources can be accessed through NFS. NonStop OSS filesets support the NFS permission-mapping feature, which allows requests from NFS to be either restrictive or permissive.

The NonStop OS Security Update Bundle

The NonStop OS Security Update Bundle enhances NonStop system security for both data in use and data in motion. It includes three components:

- **XMA** can be configured to collect security audit records from multiple sources, generate reports, export selected audit data to external SIEMs, and issue alerts.
- **NonStop SSH** uses the SSH v2 protocol to protect data in transit. It includes support for Secure File Transfer Protocol (SFTP).
- **NonStop SSL** encrypts data sent or received by programs on NonStop servers over TCP/IP. It adds Transport Layer Security (TLS) to TCP/IP protocols that do not have built-in support of SSL or TLS on NonStop, such as TELNET, FTP, or ODBC.

The NonStop OS Security Update Bundle is a standard part of the NonStop OS for newly purchased Integrity NonStop J-series and H-series systems. You can purchase it for existing J-series and H-series systems, and also can purchase either XMA or NonStop SSH for Integrity NonStop G-series systems.

XYGATE Merged Audit

XMA key features include:

- A single, SQL-based repository for audit data, for consolidation and ease of reporting
- Integration of audit records from additional sources such as Event Management System logs and Measure
- Consolidation of audits across multiple NonStop systems
- A customizable, GUI-based reporting tool, including predefined reports for compliance with regulations such as PCI DSS
- A sophisticated filtering mechanism to extract selected data
- Near-real-time GUI-based event monitoring based on user-defined, customized filters
- User-definable alerts
- Audit delivery to industry-leading SIEM devices, including HP ArcSight SIEM, RSA, LogLogic, and Splunk

Optional HP plug-in products that add support for ACI BASE24 and HP OpenCall Home Location Register also are available.

See the **XYGATE Merged Audit data sheet** or visit the **Integrating HP NonStop with the HP ArcSight SIEM platform brochure** for additional details.

NonStop SSH

NonStop SSH key features include:

Full compliance with the SSH v2 protocol

- Strong public key authentication, with key sizes of up to 2,048 bits and ciphers such as Advanced Encryption Standard (AES) and algorithms for message authentication code
- SFTP clients for both OSS and NonStop OS SFTP, as well as for an SFTP server, with support for navigating the Guardian file system, specifying files using the OSS or Guardian file name syntax, and specifying file attributes
- Support of full-screen terminal access for administrators and developers with the ability to run applications such as TEdit, vi, or emacs
- Built-in user base support, allowing remote users to log on with virtual user names instead of a Guardian user ID to avoid exposure of system credentials to file transfer clients
- A key and password store with central access control, enabling easy and secure implementation of batch processing without requiring the inclusion of passwords in batch files
- Preconfigured services or windows for particular terminal-based users to restrict their system access; this feature is also available for non-6530 pseudo terminals
- Restriction of individual user capabilities, such as allowing file transfers only to a specific subvolume
- Restriction of individual user connections, such as allowing connections only from specific IP addresses
- TCP and FTP port forwarding, allowing secure tunneling both locally and remotely
- Advanced auditing capabilities, including audit of all operations initiated from remote clients
- Load balancing using SSH command attributes to select the range of CPUs where SSH will start new processes for a particular user

An optional HP plug-in that adds support for an SFTP API interface for NonStop applications also is available.

See the **HP NonStop SSH data sheet** for additional details.

NonStop SSL

NonStop SSL key features include:

- Secure connections with SSL 3.0 and TLS 1.0, with strong ciphers such as 168-bit triple Data Encryption Standards and 256-bit AES
- Support of the FTP-TLS standard (RFC 4217), providing compatibility with a wide range of SSL-enabled FTP solutions for the PC and other platforms
- Enforcement of both client and server authentication using Public Key Infrastructure with X.509 certificates and RSA key sizes of up to 8,192 bits
- Basic firewall functionality, including disabling unencrypted protocol access and support for white lists and black lists
- Optional auditing of network traffic for protocols such as ODBC or TELNET when a complete byte-by-byte dump is desired

See the **HP NonStop SSL data sheet** for additional details.

HP security products

HP offers a number of products that work in conjunction with Safeguard to help meet your security requirements, including:

- **XYGATE Compliance PRO** for GUI-based security configuration management and compliance-oriented reporting for standards such as PCI DSS
- **XYGATE User Authentication** for additional log-on controls and integration into Lightweight Directory Access Protocol environments
- **XYGATE Access Control** for command-level access control and audit

See the individual product data sheets for more details.

Technical specifications

HP product name	HP NonStop server	Ordering information
HP Safeguard	HP Integrity NonStop BladeSystem servers running J-series HP Integrity NonStop systems running H-series HP NonStop servers running G-series	Safeguard is included with the OS at no additional charge on these systems Safeguard is included with the OS at no additional charge on these systems 9750
HP NonStop Operating System Security Update Bundle	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QSN51 HSN51 Not offered on G-series
HP NonStop Secure Shell	NonStop servers running G-series	SSH01V1 (full SSH server) SSH02V1 (SFTP only)
HP NonStop SSH—Plug-in for SFTP API	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QSFTPAPI HSFTPAPI SFTPAPI
XYGATE Merged Audit	NonStop servers running G-series	XMA
XYGATE Merged Audit—Plug-in for ACI BASE24	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QXMABASE24 HXMABASE24 XMABASE24
XYGATE Merged Audit—Plug-in for HP OpenCall Home Location Register	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QXMAHLR HXMAHLR XMAHLR
XYGATE Compliance PRO	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QXSW HXSW XSW
XYGATE Access Control	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QXAC HXAC XAC
XYGATE User Authentication	Integrity NonStop BladeSystem servers running J-series Integrity NonStop systems running H-series NonStop servers running G-series	QXUA HXUA XUA

Security partners

There are many HP partner products available that interact with Safeguard to extend system security capabilities. HP works closely with its partners and regularly adds Safeguard features based on their requirements.

HP Financial Services

HP Financial Services provides innovative financing and financial asset management programs to help you acquire, manage, and ultimately retire your HP solutions. Learn more at **hp.com/go/hpfinancialservices**.

Improve the control and security of your systems' user access. For more information on HP NonStop security products, visit **hp.com/go/nonstop/security**.

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts
delivered directly to your desktop

4AA2-0313ENN, Created November 2011; Updated May 2012, Rev. 2