





















## Requirement 3: Protect stored cardholder data

PCI DSS Requirement 3	GlobalSCAPE HS Module
<p>3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy...</p>	<p>GlobalSCAPE HS Module provides scheduled automatic clean-up. Files are securely deleted or purged by writing over the initial data with encrypted and/or pseudorandom data.</p>
<p>3.2-3.2.3 Do not store sensitive authentication data subsequent to authorization...</p>	<p>Authentication data is only persisted in memory for the duration of the session.</p>
<p>3.3 Mask PAN when displayed...</p>	<p>PAN data and other sensitive cardholder data cannot be rendered or displayed in any way.</p>
<p>3.4 Render PAN, at minimum, unreadable anywhere it is stored...</p>	<p>GlobalSCAPE HS Module provides OpenPGP encryption for data at rest.</p>
<p>3.4.1 If disk encryption is used, logical access must be managed independently of native operating system access control mechanisms.</p>	<p>Any use of Microsoft EFS is detected and a warning is given.</p>
<p>3.5-3.5.2 Protect cryptographic keys...</p>	<p>Only sub-administrators who have been specifically granted access can create, access, or manage PGP key pairs, SSL certificates, and SSH public keys.</p>
<p>3.6-3.6.8 Fully document and implement all key management processes and procedures...</p>	<p>Requires measures external to GlobalSCAPE HS Module. (Exception 3.6.1 below)</p>
<p>3.6.1 Generation of strong keys.</p>	<p>GlobalSCAPE HS Module disallows 512 or lesser certificate/key bit lengths. Default bit-length is set to 2048 bits for new keys. When importing SSL or SFTP keys, a warning appears if a weak key is imported.</p>

## Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirement 4	GlobalSCAPE HS Module
<p>4.1 Use strong cryptography and security protocols...</p>	<p>Secure protocols such as SSL, TLS, and SFTP (SSH2) are provided for data transmission. For PCI-compliant sites, SSL is restricted to versions v3 or higher, and ciphers to a minimum of 128 bits. Secure data transmission is enforced by automatically redirecting incoming HTTP traffic to HTTPS.</p>
<p>4.1.1 Ensure wireless networks transmitting cardholder data...</p>	<p>Requires measures external to GlobalSCAPE HS Module.</p>
<p>4.2 Never send unencrypted PANs by email...</p>	<p>Requires measures external to GlobalSCAPE HS Module.</p>

## Requirement 5: Use and regularly update anti-virus software

PCI DSS Requirement 5	GlobalSCAPE HS Module
<p>5.1-5.1.1</p> <p>Deploy anti-virus software on all systems commonly affected by viruses.</p>	<p>Requires measures external to GlobalSCAPE HS Module. However the upload or download of certain file types can be blocked based on their extensions.</p>
<p>5.2</p> <p>Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>Requires measures external to GlobalSCAPE HS Module.</p>

## Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirement 6	GlobalSCAPE HS Module
<p>6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release...</p>	<p>The latest version of GlobalSCAPE HS Module software is always made available online.</p>
<p>6.2 Establish a process to identify newly discovered security vulnerabilities...</p>	<p>Customers are notified via e-mail if a security vulnerability or exploit patch is available for download.</p>
<p>6.3 – 6.3.7 Develop software applications in accordance with PCI DSS...</p>	<p>GlobalSCAPE HS Module was designed to comply with relevant PCI DSS and FIPS 140-2 requirements.</p>
<p>6.4 – 6.4.3 Follow change control procedures for all system and software configuration changes.</p>	<p>Requires measures external to GlobalSCAPE HS Module.</p>
<p>6.4 .4 Back-out procedures</p>	<p>EFT Server's Backup and Restore utility aids in disaster recovery and server migration.</p>
<p>6.5 – 6.5.9 Develop all web applications based on secure coding guidelines....</p>	<p>GlobalSCAPE HS Module is constantly evaluated and tested for security vulnerabilities and exploits. Any problems found are immediately remediated and communicated to our customers.</p>
<p>6.6 For public-facing <i>web applications</i>, address new threats and vulnerabilities on an ongoing basis.</p>	<p>Requires measures external to GlobalSCAPE HS Module.</p>

## Requirement 7: Restrict access to cardholder data by business need-to-know

PCI DSS Requirement 7	GlobalSCAPE HS Module
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	The administrator is given complete control over managing which resources can be accessed by users or sub-administrators.
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know.	Segregation and control of user access is achieved using permission groups, virtual folders, and settings templates. Delegated administrators or help-desk personnel can be granted varying levels of control over server settings and resources.

## Requirement 8: Assign a unique ID to each person with computer access

PCI DSS Requirement 8	GlobalSCAPE HS Module
<p>8.1 Assign all users a unique ID.</p>	<p>Unique usernames are enforced across user accounts when using the High Security Module.</p>
<p>8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate users: password, two factor authentication.</p>	<p>Standard passwords, one-time-passwords (OTPs), certificate, and public-key authentication mechanisms are all supported.</p>
<p>8.3 Incorporate two-factor authentication for remote access...</p>	<p>Two-factor authentication with SSL-based logins for administrator sessions are supported.</p>
<p>8.4 Render all passwords unreadable during transmission and storage.</p>	<p>All user authentication passwords are stored as a one-way, non-reversible hash.</p>
<p>8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components.</p>	<p>See sub-requirements for specific implementation.</p>
<p>8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.</p>	<p>Only privileged sub-administrators are permitted to add and remove users and set user permissions.</p>
<p>8.5.2 Verify user identity before performing password resets</p>	<p>User authentication is required prior to a user-initiated password reset.</p>

<p>8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use...</p>	<p>Users are forced to change their first-time passwords upon initial login.</p>
<p>8.5.4 Immediately revoke access for any terminated users</p>	<p>When an account is disabled, expired, or removed, the user can no longer access server resources.</p>
<p>8.5.5 Remove/disable inactive user accounts at least every 90 days</p>	<p>Inactive users can be disabled or removed after a specified period of time (set to 90 days by default).</p>
<p>8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.</p>	<p>Account can be configured to automatically expire on any specified date.</p>
<p>8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.</p>	<p>User's credentials can be automatically emailed to a specified email address. The default text of the message can be customized to include your organization's password policies and procedures.</p>
<p>8.5.8 Do not use group, shared, or generic accounts and passwords</p>	<p>The "Anonymous" password type is disallowed when running in PCI DSS mode.</p>
<p>8.5.9 Change user passwords at least every 90 days</p>	<p>Automatic expiration of passwords can be enabled for administrators and users.</p>
<p>8.5.10 Require a minimum password length of at least seven characters.</p>	<p>Complex passwords can be enforced using multiple criteria, including minimum length, definition of alphanumeric sub-options, disallowing words contained in a dictionary file, disallowing the username as the password, disallowing cyclical passwords and others.</p>
<p>8.5.11 Use passwords containing both numeric and alphabetic characters.</p>	
<p>8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords used.</p>	<p>Password history is recorded and the reuse of historical passwords is disallowed for administrators and users.</p>

<p>8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts</p>	<p>Repeated access attempts can be limited by locking out a user or an administrator. The settings for lockout—the number of failed attempts and the elapsed time between failed attempts—are fully customizable. The lockout duration can be set to 30, 60 or 90 minutes.</p>
<p>8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.</p>	
<p>8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal</p>	<p>An idle timeout setting is applied across all connection protocols supported, for both users and administrators.</p>
<p>8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.</p>	<p>Multiple authentication options are provided for accessing data resources, including AD/NTLM, LDAP, ODBC based, and EFT Server's proprietary authentication manager.</p>

## Requirement 9: Restrict physical access to cardholder data

This requirement mainly relates to restricting physical access to the computer room or data center, and destroying transportable media, which are a function of organizational security, not GlobalSCAPE HS Module.

PCI DSS Requirement 9	GlobalSCAPE HS Module
9.1-9.9 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Requires measures external to GlobalSCAPE HS Module.
9.10-9.10.1 Destroy <i>media</i> containing cardholder data when it is no longer needed for business or legal reasons.	Requires measures external to GlobalSCAPE HS Module.
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Data wiping is provided by GlobalSCAPE HS Module for sanitizing deleted data on disk.

## Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirement 10	GlobalSCAPE HS Module
10.1 Establish a process for linking all access to system components to each individual user (audit trails).	Preconfigured reports of all activity within GlobalSCAPE HS Module can be generated on-demand.
10.2 – 10.2.7 Implement automated audit trails for all system components...	GlobalSCAPE HS Module will audit all user access to data (10.2.1), and all administrator changes to configuration settings (10.2.2). Access to audit trails, invalid logical access, authentication mechanisms, object creation, and initialization of audit logs (10.2.3-2.7) is managed at the database server.
10.3 Record at least the following audit trail entries for all system components...	GlobalSCAPE HS Module audits user identity (10.3.1), type of transaction (10.3.2), date and time of transaction (10.3.3), transaction result (10.3.4), remote and local IP (10.3.5), and objects affected (10.3.6).
10.4 Synchronize all critical system clocks and times	Requires measures external to GlobalSCAPE HS Module.
10.5-10.5.5 Secure audit trails so that they cannot be altered.	Audited data integrity depends on the chosen database solution and authentication architecture. EFT Server supports auditing to a central SQL or Oracle server.
10.6 Review logs for all system components at least daily....	A daily PCI DSS compliance report can be generated and sent via email to the appropriate recipient(s). This report details the PCI DSS compliance status of each security element monitored by the HSM. The report includes the recorded reason (compensating control) for any non-compliant setting.
10.7 Retain audit history for at least one year.	Requires measures external to GlobalSCAPE HS Module.

## Requirement 11: Regularly test security systems and processes

System, process, and software testing are measures external to GlobalSCAPE HS Module. The daily HS-PCI Compliance Report can be a helpful guide during your testing. GlobalSCAPE's online help also includes guidelines for Best Practices for Configuration and Validation to assist you with periodic testing.

PCI DSS Requirement 11	GlobalSCAPE HS Module
11.1-11.5 Requirements relating to regular testing of security systems and processes.	Requires measures external to GlobalSCAPE HS Module defined by your organizational policy.

# Requires measures external to GlobalSCAPE HS Module defined by your organizational policy.

The development of a security policy is a measure that is external to the GlobalSCAPE HS Module. However the ability to automatically generate and email daily reports will help you monitor daily operations and enforce the security policies you have in place.

PCI DSS Requirement 12	GlobalSCAPE HS Module
12.1-12.9 Requirements relating to the maintaining of a policy that addresses information security	Requires measures external to GlobalSCAPE HS Module defined by your organizational policy.

The logo for GlobalSCAPE, featuring the word "GlobalSCAPE" in a bold, sans-serif font. The letter "i" in "Global" is lowercase and has a dot, while "Global" is lowercase and "SCAPE" is uppercase. A registered trademark symbol (®) is located to the upper right of the "E".

**g**i**ObalsCAPE®**

GlobalSCAPE  
4500 Lockhill-Selma Suite 150  
San Antonio, TX 78249  
800-290-5054  
210-308-8267  
[www.globalscape.com](http://www.globalscape.com)