GO ANYWHERE®
Managed File Transfer

PCI DSS

Meeting PCI DSS Regulations with GoAnywhere MFT

PCI DSS is a regulation that applies to every organization around the world that processes credit or debit card information. Failing a PCI DSS audit can result in fines, but IT's responsibilities extend beyond avoiding these penalties. Meeting PCI's standards contributes to the security of your business by helping to avoid data breaches and all of their related costs: litigation, customer notification and compensation, damage to the company's reputation, and diminished share value.

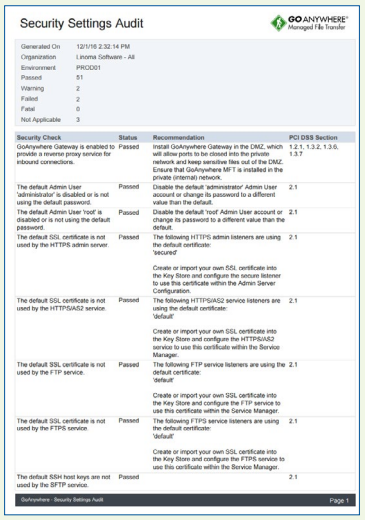
GoAnywhere is a cross-platform managed file transfer solution that is designed to help you meet PCI DSS compliance standards while saving you time and money. It can also eliminate the custom programming and scripting normally required to transfer data, while improving the security and quality of those transfers.

A Strategic Tool for Compliance and Beyond

GoAnywhere Managed File Transfer helps organizations meet the requirements of PCI DSS by providing a managed, centralized, and auditable solution. The benefits of GoAnywhere for security and compliance include:

- Centralized control and management of file transfers
- Role-based administration and permissions
- Secure connections for the transmission of sensitive data
- Encryption of data at rest
- Strong encryption key management with separation of duties
- Keeping PCI-related data out of the DMZ
- Closed inbound ports into the private network to prevent intrusion
- Detailed audit logs for reporting

PCI compliance requirements will continue to evolve, but by implementing robust solutions, forward-thinking IT shops can meet current requirements while laying a strong foundation for future security enhancements.


Security Settings Audit

GO ANYWHERE® Managed File Transfer

Generated On	12/1/16 2:32:14 PM
Organization	Linoma Software - All
Environment	PROD01
Passed	51
Warning	2
Failed	2
Fatal	0
Not Applicable	3

Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Passed	Install GoAnywhere Gateway in the DMZ, which will allow ports to be closed into the private network and keep sensitive files out of the DMZ. Ensure that GoAnywhere MFT is installed in the private (internal) network.	1.2.1, 1.3.2, 1.3.6, 1.3.7
The default Admin User 'administrator' is disabled or is not using the default password.	Passed	Disable the default 'administrator' Admin User account or change its password to a different value than the default.	2.1
The default Admin User 'root' is disabled or is not using the default password.	Passed	Disable the default 'root' Admin User account or change its password to a different value than the default.	2.1
The default SSL certificate is not used by the HTTPS admin server.	Passed	The following HTTPS admin listeners are using the default certificate: 'secured' Create or import your own SSL certificate into the Key Store and configure the secure listener to use this certificate within the Admin Server Configuration.	2.1
The default SSL certificate is not used by the HTTPS/AS2 service.	Passed	The following HTTPS/AS2 service listeners are using the default certificate: 'default' Create or import your own SSL certificate into the Key Store and configure the HTTPS/AS2 service to use this certificate within the Service Manager.	2.1
The default SSL certificate is not used by the FTP service.	Passed	The following FTP service listeners are using the default certificate: 'default' Create or import your own SSL certificate into the Key Store and configure the FTP service to use this certificate within the Service Manager.	2.1
The default SSL certificate is not used by the FTPS service.	Passed	The following FTPS service listeners are using the default certificate: 'default' Create or import your own SSL certificate into the Key Store and configure the FTPS service to use this certificate within the Service Manager.	2.1
The default SSH host keys are not used by the SFTP service.	Passed		2.1

GoAnywhere - Security Settings Audit — Page 1

SECURITY SETTINGS AUDIT REPORT

GoAnywhere MFT can analyze more than 60 different security settings to determine compliance with applicable sections of the Payment Card Industry Data Security Standards (PCI DSS).

If a security setting does not meet the standard, the report will indicate the corresponding PCI section and the recommendation on how to correct the security setting.

GO ANYWHERE® Managed File Transfer

GoAnywhere Helps You Meet PCI DSS Data Transfer Security Requirements

GoAnywhere directly addresses several of the twelve PCI DSS requirements through features including encryption, role-based security, and audit logs.

	PCI DSS	Corresponding GoAnywhere Feature
Required Standards	**Requirement: 1.1.6, 1.2.1, 1.3** Install and maintain a firewall configuration to protect cardholder data.	IP addresses and ports are customizable in GoAnywhere, allowing flexibility with firewalls. Description fields make it easy to document why connections are used. Combined with GoAnywhere Gateway, full separation of internal data, DMZ, and public networks is simplified.
	Requirement: 2.1, 2.2, 2.3 Do not use vendor-supplied defaults for system passwords and other security parameters.	The GoAnywhere Security Settings Audit report provides a detailed list of all GoAnywhere security defaults, enabled services, and configured security features. Using HTTPS will ensure that all administrative access is encrypted.
	Requirement 3.1, 3.4, 3.5, 3.6 Protect stored cardholder data.	With GoAnywhere, your files are protected at rest using strong encryption methods like AES and OpenPGP. It also provides cryptographic key management. Data retention can also be automated.
	Requirement 4.1 Encrypt transmission of cardholder data across open public networks.	GoAnywhere protects transmissions over public and private networks using secure protocols including SFTP, FTPS, AS2, and HTTPS. TLS 1.1 and 1.2 are fully supported.
	Requirement 5.1, 5.3 Use and regularly update anti-virus software or programs	GoAnywhere can run on systems with 3rd party anti-virus solutions. It also supports ICAP integration for external scanning and data loss prevention.
	Requirement 6.2, 6.4, 6.5.7, 6.5.10, 6.6 Develop and maintain secure systems and applications.	GoAnywhere supports change control by working in conjunction with test, QA, or development systems, allowing easy promotion of projects from test to production while maintaining separation of duties. Project revisions are recorded, allowing easy rollback of changes.
	Requirement 7.1 Restrict access to cardholder data by business need-to-know.	GoAnywhere provides role-based security so each user only has access to the information they need.
	Requirement 8.1.4, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.5 Assign a unique ID to each person with computer access.	GoAnywhere has full individual account management features. It can also integrate with LDAP and external RSA 2-factor authentication to satisfy all account requirements in PCI DSS.
	Requirement 9.5 Restrict physical access to cardholder data.	GoAnywhere's multi-platform and virtual environment flexibility will allow you to run software and store data in your secure location.
	Requirement 10.2, 10.3, 10.5 Track and monitor all access to network resources and cardholder data.	With detailed audit logs, GoAnywhere makes it easy to monitor all activity on the system. Integration with external logging solutions is built in.