



DATASHEET (GOANYWHERE)

Meeting PCI DSS Requirements with GoAnywhere MFT

PCI DSS 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 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.

Fortra's GoAnywhere is a cross-platform managed file transfer (MFT) solution that is designed to help you meet PCI DSS compliance requirements while saving you time and money. It can also eliminate the custom programming and scriptwriting 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 and in motion
- 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 REPORT

GoAnywhere MFT can analyze more than 100 different security settings to determine compliance with applicable sections of the Payment Card Industry Data Security Standard (PCI DSS).

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

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.

Required Standards	PCI DSS	Corresponding GoAnywhere Feature
	Requirement 1: Install and Maintain Network Security Controls Applicable Requirements: 1.3.1, 1.3.2, 1.4.1, 1.4.2, 1.4.4, 1.4.5	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: Apply Secure Configurations to All System Components Applicable Requirements: 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.7	The GoAnywhere Security Settings Audit report provides a detailed list of GoAnywhere security defaults, enabled services, and configured security features. Using HTTPS will ensure that all administrative access is encrypted.
	Requirement 3: Protect Stored Account Data Applicable Requirements: 3.2, 3.5.1, 3.6.1.3, 3.7.5	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: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks Applicable Requirements: 4.2.1	GoAnywhere protects transmissions over public and private networks using secure protocols including SFTP, FTPS, AS2, and HTTPS. TLS 1.2 and 1.3 are fully supported.
	Requirement 5: Maintain a Vulnerability Management Program	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: Develop and Maintain Secure Systems and Software Applicable Requirements: 6.2.4, 6.3.3, 6.4.1, 6.4.2	GoAnywhere provides various security configurations to support the secure implementation of the environment.
	Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know Applicable Requirement: 7.2.2	GoAnywhere provides role-based security so each user only has access to the information they need.
	Requirement 8: Identify Users and Authenticate Access to System Components Applicable Requirements: 8.2.2, 8.2.6, 8.2.8, 8.3.1, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.5.1, 8.6.3	GoAnywhere has full individual account management features. It can also integrate with LDAP and external 2-factor authentication to satisfy all account requirements in PCI DSS.
	Requirement 9: 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: Log and Monitor All Access to System Components and Cardholder Data Applicable Requirement: 10.5.1	With detailed audit logs, GoAnywhere makes it easy to monitor all activity on the system. Integration with external logging solutions is built in.

Get started with PCI compliance today.

Download your free 30-day GoAnywhere trial by visiting www.goanywhere.com/trial.

You can also contact us by emailing goanywhere.sales@fortra.com.

FORTRA[®]

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.