Remote Control

Optimizing Security and Efficiency
PCI compliance Review

Are you interested in learning more about how CrossTec Remote Control fits into your PCI Compliance Strategy?

PCI Security Requirements	How CrossTec Remote Control Address Them
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	CrossTec Remote Control can encrypt all data using the Advanced Encryption Standard with key length of 256-bits. (this is classed as strong Encryption in the PCI DSS Glossary)
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: • The Internet • Wireless technologies, • Global System for Mobile communications (GSM) • General Packet Radio Service (GPRS).	This applies to transmitting card holder data over a public network. Card holder data should only be transmitted from the card holder to the system and from the system to a payment processor. PCI Compliance requires that if the Card Holder data is stored then it should be unreadable anywhere it is stored. Although CrossTec Remote Control would rarely, if ever, be involved in actual card holder data transmission and never in the storage of it, it does provided encryption of all transmitted data as outlined in 2.3 above.

500 NE Spanish River Blvd Suite 201, Boca Raton, FL 33431
Toll Free 800-675-0729 | www.CrossTecSoftware.com

CrossTec Corporation

PCI Security Requirements	How CrossTec Remote Control Address Them
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations.	CrossTec Provides a notification to registered customers on any software update. By doing this instead of automatically updating software, any updates are managed by the customer. Thus there are no unplanned interruptions to service or untested changes being applied automatically.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities 7.1.2 Assignment of privileges is based on individual personnel's job classification and function 7.1.3 Requirement for a documented approval by authorized parties specifying required privileges. 7.1.4 Implementation of an automated access control system	Access to all remote control functions can be profiled with by using the CrossTec local configuration or by using the Active directory policy templates available for the product. Profile selection can be based on the privileged user ID or that User ID's security group membership.
8.1 Are all users assigned a unique ID before allowing them to access system components or cardholder data? 8.2 In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? 8.3 Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties? 8.4. Are all passwords rendered unreadable during transmission and storage on all system components using strong cryptography?	Multiple Authentication Methods Users connections can be authenticated by one and combination of the following authentication methods: CrossTec configured authentication. Local windows Security Active directory Security SmartCard authentication Multifactor Authentication: In addition to the connection authentication above, connections can also be restricted base on a security key or the software license; on the source address of the connection. Smartcard pass-through authentication is also supported for authentication during a remote session.
10.2 Are automated audit trails implemented for all system components to reconstruct the following events: 10.5 Are audit trails secured so they cannot be altered, as follows:	Using Client logging and recording of remote sessions to replay files. Full logging is available for any forensic team. The CrossTec Client can be configured to write Log files and Replay files to a secure location.

500 NE Spanish River Blvd Suite 201, Boca Raton, FL 33431
Toll Free 800-675-0729 | www.CrossTecSoftware.com

CrossTec Corporation