

Confidentiality	Payment Card Industry Data Security Standard	How WS_FTP Server and WS_FTP Professional Support Compliance
<b>Authentication</b>	<p><i>Requirement 8:</i> Assign a unique ID to each person with computer access. 8.4 Encrypt all passwords during transmission and storage, on all system components. 8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components.</p>	<ul style="list-style-type: none"> <li>- Unique user IDs</li> <li>- Integrates with existing user databases such as Active Directory, LDAP, NT and ODBC databases</li> <li>- Active Directory support for Distinguished Name, Group and Organizational Unit</li> <li>- All passwords encrypted during client-server authentication when using WS_FTP Professional and WS_FTP Server</li> <li>- All passwords stored in WS_FTP Server database are encrypted</li> <li>- Ability to enforce strong password creation</li> <li>- Auto-expiring passwords with options to allow client reset</li> <li>- Rules on using previously used passwords</li> <li>- Two-factor authentication using username/passwords pairs, with SSL Certificates for mutual authentication, or with SSH public keys</li> </ul>
<b>Access Control</b>	<p><i>Requirement 7:</i> Restrict access to data by business need-to-know. <i>Requirement 8:</i> Assign a unique ID to each person with computer access</p>	<ul style="list-style-type: none"> <li>- Administrative SoD (Separation of Duties) with multiple levels of access control and administrator permissions</li> <li>- Permissions can be set on shared folders and applied to individual users or entire user groups</li> <li>- Administrators can set disk space, maximum file storage, and maximum bandwidth for entire groups or users</li> <li>- Block file uploads, downloads, deletions, renaming, and directory creation on a per user basis and per IP address</li> <li>- Set read, write, delete, list, and rename permissions on shared folders</li> <li>- Lock users to their home folder, hide other folders from view</li> <li>- Administrative options to hide the existence of other users' folders</li> <li>- Control server access by IP address and port ranges</li> <li>- Block IP addresses manually, or automatically, using set criteria (such as number of failed connections),</li> <li>- Block IP addresses by subnet</li> <li>- Support for IP address "whitelist" (safe from automatic blocking)</li> <li>- Virtual folders are supported for accessing Universal Naming Convention (UNC) and mapped drives</li> <li>- Create SSL certificates and a trusted authorities database on a per host basis</li> <li>- Force mutual authentication for client and server to both exchange SSL certificates</li> <li>- Clear Command Channel (CCC) enables Firewall/Network Address Translations (NAT) support for SSL connections</li> <li>- Configure IP address and ports when using PASV command (with or without SSL) for better performance with firewalls, NAT devices</li> <li>- User IDs and passwords always encrypted</li> </ul>
<b>Privacy</b>	<p><i>Requirement 2:</i> Do not use vendor-supplied defaults for system passwords and other security parameters. 2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. <i>Requirement 3:</i> Protect stored data. Use strong cryptography on stored data. <i>Requirement 4:</i> Encrypt transmission of cardholder data and sensitive information across public networks. 4.1 Use strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC).</p>	<ul style="list-style-type: none"> <li>- Encrypts client connections over SSH, SSL (Version 3—Implicit, Explicit and TLS) and SCP2 protocols</li> <li>- Session encryption using 256-bit AES encryption and 3DES</li> <li>- FIPS 140-2 validated encryption using 256-bit AES, 3DES, and SHA 1, SHA 2</li> <li>- Force SSH, SSL/FTPS or TLS 1.0 or higher on all client connections to WS_FTP Server 128 bit SSL on folder access</li> <li>- Encrypts stored files with fully-integrated OpenPGP mode</li> <li>- Configurable SSL/TLS encryption down to the folder level</li> <li>- Policy based cryptographic strength enforcement</li> <li>- Import, export and create SSL x.509v3 certificates</li> <li>- Support for full chain and peer-level SSL certificate chains</li> <li>- Import, export and create SSH keys, including OpenSSH keys, for Windows, Unix, and Linux</li> <li>- Support for suppressing SSH protocol name in version in login banner, preventing malicious actions</li> <li>- Create, Edit, Import, Export, Delete OpenPGP keys with support for PGP, OpenPGP and GPG</li> <li>- Select and prioritize ciphers to use in OpenPGP key creation</li> <li>- Support for RSA and Diffie-Hellman key types with settable expiration date</li> <li>- OpenPGP asymmetric key length of 1024 – 4096 bits</li> </ul>