

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, NT and ODBC databases</li> <li>- Active Directory support for Distinguished Name, Group and Organization 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> </ul>
<b>Access Control</b>	<p><i>Requirement 7:</i> Restrict access to data by business need-to-know.</p> <p><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 privileges</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</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>- 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 and NAT devices</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.</p> <p><i>Requirement 3:</i> Protect stored data. Use strong cryptography on stored data.</p> <p><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>- User IDs and passwords always encrypted</li> <li>- Encrypts client connections over SSH and SSL (Implicit, Explicit and TLS) protocols</li> <li>- Session encryption using 256-bit AES encryption and 3DES</li> <li>- Force SSH, SSL/FTPS or TLS 1.0 or higher on all client connections to WS_FTP Server</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>- Import, export and create SSH keys</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>

Integrity	Payment Card Industry Data Security Standard	How WS_FTP Server and WS_FTP Professional Support Compliance
	<p><i>Requirement 11:</i> Regularly test security systems and processes. 11.5 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated).</p>	<ul style="list-style-type: none"> <li>- Built-in file integrity checking of up to SHA-512 secure hashing algorithms</li> <li>- Encrypts stored files with fully-integrated OpenPGP mode</li> <li>- Encrypts client connections over SSH and SSL (Implicit, Explicit and TLS) protocols</li> <li>- Session encryption using 256-bit AES encryption and 3DES</li> <li>- File and folder size comparing to ensure accuracy and completeness</li> <li>- Syslog integration into centralized network or security management logging systems</li> <li>- Automate the mirroring of two locations with built-in schedule, synchronization and backup utilities</li> <li>- File lock during upload prevents users from downloading a file before it is fully uploaded to the server</li> </ul>
Availability	<p><i>Requirement 12:</i> Maintain a policy that addresses information security for employees and contractors. 12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.</p>	<ul style="list-style-type: none"> <li>- Server architecture enables load balancing to distribute workload among multiple servers for improved performance</li> <li>- Clustering groups servers for redundancy and to overcome scheduled/unscheduled server downtime</li> <li>- Session manager delivers real-time performance statistics on WS_FTP Server connections and file transfer events</li> <li>- Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files</li> <li>- Administration Logging: Keep an auditable record of server administrator actions</li> <li>- Syslog Support: Integrate WS_FTP logs with a company database or central data repository</li> <li>- Logging server and notification server both require administrator login</li> <li>- Ability to install logging server and notification server on a different server to optimize availability</li> <li>- Automatic restart of interrupted file transfers so users never lose valuable data because of an interrupted connections</li> <li>- Multipart mode splits large files into smaller segments and downloads all segments via different, yet concurrent, connections</li> <li>- File compression enables faster file transfers by reducing the size of files</li> <li>- Scheduler lets you program one-time or recurring transfers with auto-login, navigation and transfer</li> <li>- Backup wizard automates file backup to any device, drive or FTP server</li> <li>- Synchronize files and file directories between any two locations</li> <li>- Automated notifications triggers communication and workflows. Generate email, SMS and pager alerts and launch external programs based on server events such as uploading a file or creating a directory</li> <li>- Configure to execute an application and include command line variables</li> <li>- Firewall scripting engine lets you create and edit firewall scripts and Firewall Wizard walks you through creation of multiple firewall types including HTTP Proxy</li> </ul>
Audit	<p><i>Requirement 10:</i> Track and monitor all access to network resources and cardholder data. 10.1 Establish process for linking access (especially those done with administrative privileges) to system components to an individual user. 10.2 Implement automated audit trails to reconstruct the following events: 10.2.1-7 User access to cardholder data; All actions with root or admin privileges; Audit trail access; Access attempts, Identification and authentication mechanisms; Initialization of the audit logs; Creation and deletion of system-level objects. 10.3 Record at least the following audit trail entries for each event, for all system components: 10.3.1-6 User identification; Type of event; Timestamp; Success or failure; Event origination; Identity or name of affected data or system. 10.5 Secure audit trails so they cannot be altered, 10.5.5 Use file integrity monitoring/change detection software on logs.</p>	<ul style="list-style-type: none"> <li>- Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files</li> <li>- Administration Logging: Keep an auditable record of server administrator actions</li> <li>- Syslog Support: Integrate WS_FTP logs with a company database or central data repository</li> <li>- Log viewer provides four levels of reporting including verbose for all client-server activity, administration activity and errors</li> <li>- Nested filtering provides custom views of file transfer or other server events</li> <li>- Logs are exportable in XML format</li> <li>- Automated notifications triggers communication and workflows. Generate email, SMS and pager alerts and launch external programs based on server events such as uploading a file or creating a directory</li> <li>- Log the details of encrypted connections to verify encryption strength and type negotiated for a given session</li> <li>- Session manager delivers real-time performance statistics on WS_FTP Server connections and file transfer events</li> <li>- Connection log shows all commands sent from WS_FTP Professional to a server and shows the replies from the server</li> </ul>