How does 3P® CONNECT SOFTWARE ensure compliance with the Highest International Standards?

Benefits	Requirements	3P® CONNECT SOFTWARE Features
Authentication & Authorization	Automatic logoff	The software automatically logs off users based on a configurable period of inactivity.
	Authorization	User Management feature that allows customers to manage access to the software. User access to the software is performed only through the web application.
	Person Authentication	The service providing authentication to the software can be configured according to : - Security policy - Active Directory - Associated with a Windows centralized authentication provider The web login interface of 3P CONNECT SOFTWARE may be integrated on your authentication service.
	Configuration of Security Features	Authentication services can be configured according to the customer's security policy, and associated with a Lightweight Directory Access Protocol (LDAP) centralized authentication provider. The web login interface of 3P® CONNECT SOFTWARE may be integrated onto the customer's authentication services.
	Node Authentication	Authentication between the system's nodes (e.g. LIMS or LDAP) uses certificates.
Availability	Network Controls	The software leverages Windows Firewall configuration for restricting traffic only to specific ports and services.
	Malware Detection/ Protection	Anti-Virus of your choice can be installed and your custom security policies can be applied.
Data	Classification(s) of Data Stored	The software doesn't store or processes any sensitive data.
	Data Integrity and Authenticity	Includes integrity monitoring features that alerts on potential failures that could affect data integrity.
	Data Backup and Disaster Recovery	Enables users to download backups manually, as well as configuring data backups in an encrypted format, and store it on a local network or server.
		Software can be restored to default customer delivery configuration if necessary, and can be restored with customer backups with the assistance of bioMérieux support.
	Transmission Confidentiality	Data is encrypted using AES 256 prior to transmission. TLS 1.2 is supported.
	Transmission Integrity	The software is able to detect and recover from communication failures for critical messaging.
Audit	Audit Controls	Audit Trail records cannot be deleted, are stamped and can be exported. Supports customers to be compliant with the current GMP, by following the ALCOA principle.
	Regulatory Compliance	The software is designed to support 21 CFR11 compliance.
Maintenance	System and Application Hardening	Cybersecurity risk assessments, penetration testing, static application security testing, vulnerability monitoring, and manual code review are performed as part of the Software Development Lifecycle (SDLC) of 3P® CONNECT Software, ensuring appropriate hardening.
	Cybersecurity product updates	3P® CONNECT SOFTWARE will receive periodic updates as needed to remediate discovered vulnerabilities. These updates can be deployed through VILINK®.
	Third-party Components in Product Lifecycle Roadmaps	Software Composition Analysis are performed to facilitate Software Bill of Materials (SBOM) generation and to ensure that all libraries and third-party components stay up to date.
Other	Security Guides	A detailed Product Security Technical Whitepaper is available for 3P® CONNECT Software.
	Note	This features have been assessed for the 3P® CONNECT v3.X, in case of future releases differences may apply.

bioMérieux S.A. • 69280 Marcy l'Etoile • France • Tel.: + 33 (0)4 78 87 20 00 • Fax: +33 (0)4 78 87 20 90
www.biomerieux.com

3P® CONNECT SOFTWARE

CYBERSECURITY BY DESIGN

Your Ally in Advancing Quality

biomerieux.com

PIONEERING DIAGNOSTICS

CYBERSECURITY BY DESIGN

Cybersecurity is integrated in the design of our products. Supported by our partners and bioMérieux experts in cybersecurity and data privacy, bioMérieux has implemented a Secure Development Lifecycle that ensures Security by Design and follow the highest cybersecurity standards.

PROACTIVITY

- Development and maintenance of 3P® CONNECT SOFTWARE is performed following a secure development lifecycle integrating mandatory security activities and in compliance with standards and guidelines such as 21CRF11, and TIR57.
- A cybersecurity risk assessment is performed prior to each 3P® CONNECT SOFTWARE release to ensure safety & security.
- Continuous updates and upgrades are released and made available via VILINK® for 3P® CONNECT SOFTWARE with the latest features and cybersecurity improvements.

SURVEILLANCE

- 3P® CONNECT SOFTWARE is scanned for cybersecurity threats using an external reference tool. All scanned vulnerabilities are assessed for impact and criticality, and are corrected in a patch if relevant.
- A cybersecurity bulletin is issued internally for 3P® CONNECT SOFTWARE.

EXPERTISE

- bioMérieux enforces data protection by implementing security features in compliance with current standards, such as cryptographic measures, role-based access control, malware protection, or a strong backup and restore process.
- Using encrypted transmission protocols, security of confidential data processed by 3P® CONNECT SOFTWARE is ensured during its entire lifecycle.
- For every new 3P® CONNECT SOFTWARE release, penetration tests are performed by external companies to detect new vulnerabilities and threats. All found vulnerabilities are assessed (impact/criticality) and corrected in a patch if required.