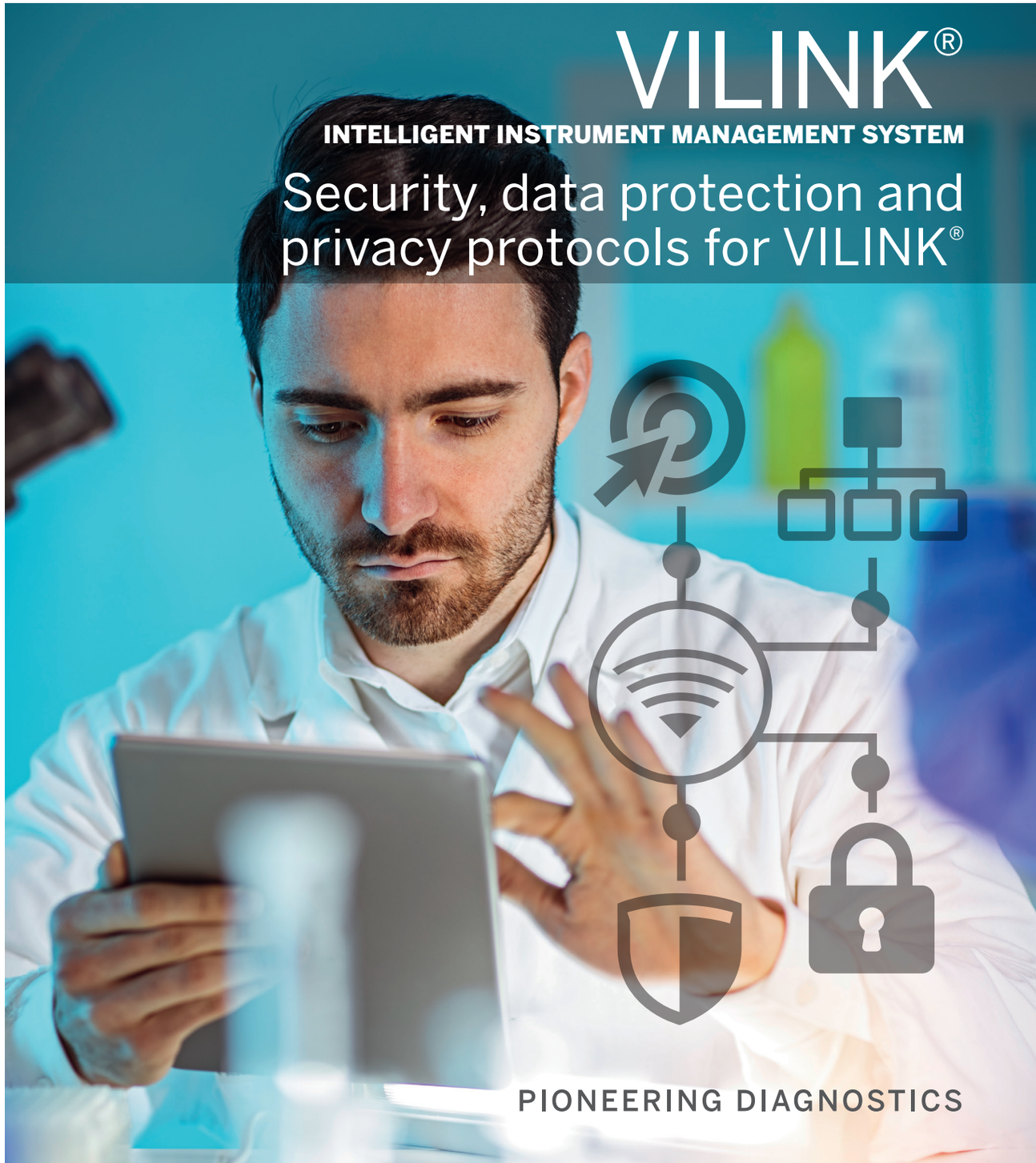
bioMérieux S.A. • 69280 Marcy l'Étoile • France • Tel.: + 33 (0)4 78 87 20 00 • Fax: +33 (0)4 78 87 20 90
www.biomerieux.com • www.biomerieux-diagnostics.com



Safe & Sound

VILINK® is a highly secured modular solution that is firewall-configurable and compatible with your organization's security systems. VILINK® provides a direct connection between bioMérieux's technical support representative and your systems, offering traceability, logging and data security via user-approved access and SSL-based encrypted communication.

VILINK® enables our service support teams to offer real-time troubleshooting and operator training at your request, reducing down time and improving efficiency in your laboratory by providing:

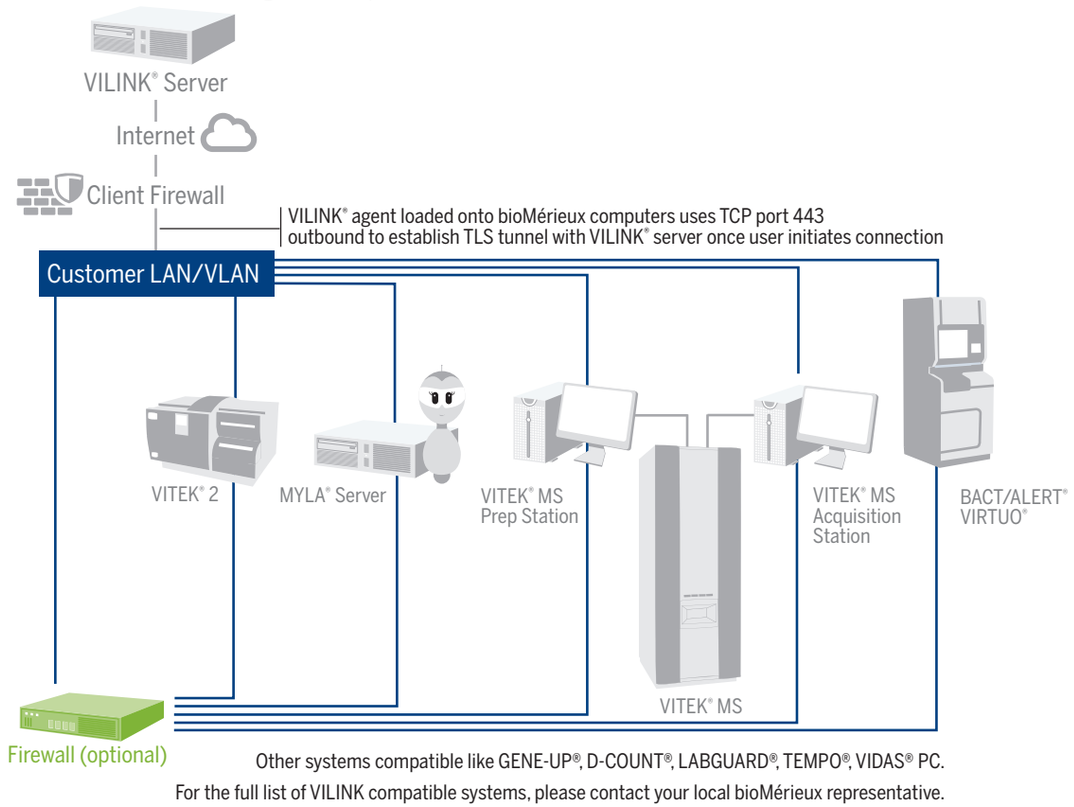
- Remote technical support
- Remote software/firmware updates
- Flexible installation options for connecting instrument computers in your laboratory local area network.

bioMérieux's security principles:

- We protect the integrity of your patient data
- We trace activities and all accesses
- We provide flexibility and control to enforce your business policies

System Architecture

VILINK® software is powered by PTC (Axeda Solution), which provides an advanced cloud-based service and software for managing connected products and machines. PTC has gained industry leadership by incorporating rigorous security principles and standards to the design and operation of services such as VILINK®.



Other systems compatible like GENE-UP®, D-COUNT®, LABGUARD®, TEMPO®, VIDAS® PC.
For the full list of VILINK compatible systems, please contact your local bioMérieux representative.

Outbound information

The combination of VILINK® functionality and our remote technical support capabilities creates a full service support offering.

VILINK® is installed locally on systems computers and only sends device-relevant service data, so you will never have to accept incoming connections, and IP addresses will never be revealed outside the network. VILINK® Agents can also be configured with FIPS mode enabled, which imposes the strictest security standards (often required in government settings).

Firewall-friendly

VILINK®'s patented Firewall-friendly™ technology provides two-way communication based on Web Service standards, including Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML). All outbound communications are initiated using the HTTPS protocol exclusively on port TCP 443.

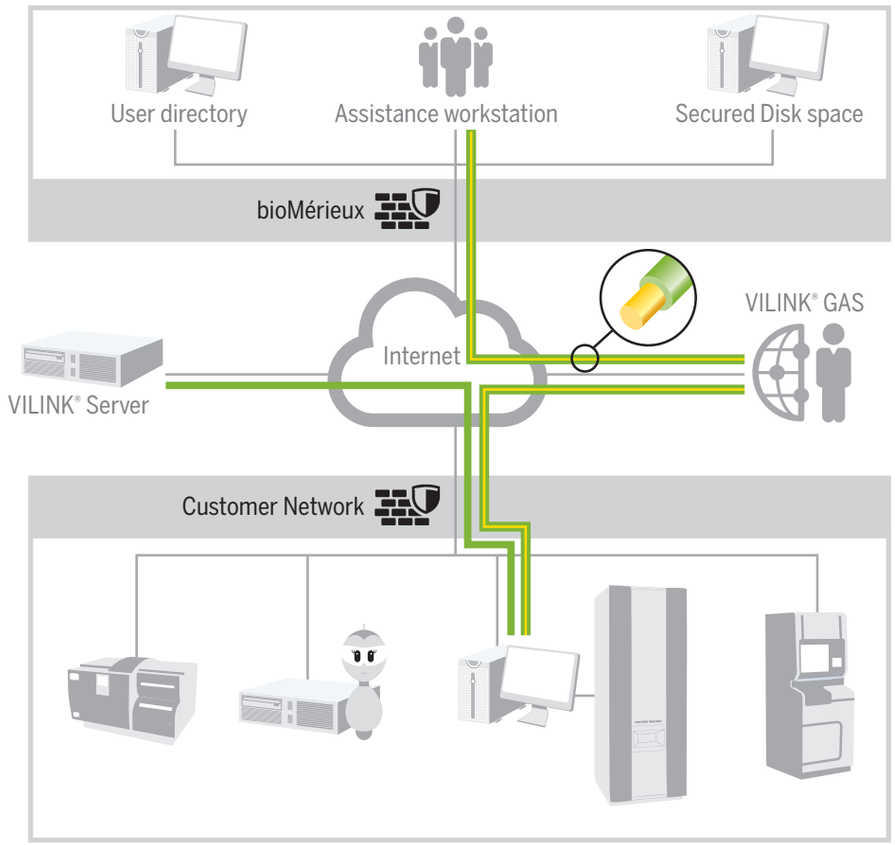
Remote access

When remote access is required, the VILINK® support user connects to the VILINK® Server with his credentials and selects the system he wants to access, creating a secure tunnel (based on HTTPS) between the help desk and your bioMérieux commercial system.

The remote user uses validated tools (UVNC, Teamviewer, SSH, RDP) to request remote access, which you can choose to accept or reject. All communication and transferred data goes through the VILINK® secure tunnel.

To optimize the remote support experience, we use the Global Access Server (GAS) on TCP port 443. The VILINK® server uses the commercial system's nearest GAS server, and if that doesn't work will use the next nearest server.

Your Firewall and Proxy must enable access to the GAS servers on the HTTPS (TCP/443) port: a list of GAS servers is available at https://vilink.biomerieux.com/install.



GAS: Global Access Server

Teamviewer® Remote Access

Teamviewer® software can be used in order to improve the speed of the remote access without any compromise on the security.

You can use

Teamviewer® interface within a VILINK® TLS tunnel so using the AES 256 bits encryption

OR

Teamviewer® Direct Mode using the Teamviewer® infrastructure. To enable this method you will have to allow the traffic on the tcp port 443 or tcp port 5938 to the domain *.teamviewer.com or on a specific list of IP addresses to be provided on demand

In this Teamviewer Direct Mode configuration, the security features are using the following:
- Whitelist to protect access to commercial systems only to bioMérieux accounts and trusted devices
- RSA Public / Private Keys exchange and AES 256 bits session encryption
- Specific login and password for establishing the Teamviewer session
- Usage of Teamviewer is limited to valid VILINK sessions
- By default, the Teamviewer account is inactive and activated only during a VILINK valid session

Teamviewer is certified SOC2, ISO9001 and help you to be HIPAA compliant

Automatic monitoring

Depending which bioMérieux commercial system VILINK® has been installed on, it is possible to automatically monitor the system's computer and devices (instrument, network or signalization device). Monitoring focuses on technical information such as RAM size, disk-filling ratios, log files and instrument sensor values, allowing bioMérieux to detect or anticipate variations that may have an impact on the bioMérieux commercial system or its behavior. Only technical information that enables system support is uploaded to the VILINK® Server (never information related to patients, or to biological results), with access restricted to bioMérieux.

Options

You can choose to:
- Have the remote intervention report on remote accesses on your systems mailed to you
- Authorize our service support teams to perform file transfers, or not
- Enable automatic monitoring of your bioMérieux commercial systems, or not
- Retain full access control with the Axeda Policy Server option (see next).

The Axeda Policy Server (option that establishes and enforces device security and data privacy policies):

The Axeda® Policy Server enables your IT administrators to establish and enforce the privacy policy for all of your devices in a single place.

The software application resides on your network, providing a comprehensive and granular set of permission settings that continuously govern behavior, and applies to every kind of Axeda activity, including handling remote diagnostics, sending software upgrades, retrieving log files, running sessions, and executing commands and scripts.

Control can either be automatic, based on the set policy, or configured to notify you that an action request is pending. Policies can also be scoped to time windows and to particular remote users.

Easily Managed User Authentication and Access Control

User access control is addressed through activity-based access control and device-based access control, combined in a wide variety of ways to allow users to do their jobs effectively while protecting access to sensitive information:

1. Activity-based access control enables the system administrator to assign and classify users in Axeda, and define the activities that can be performed. Each user group is given controlled access at the Axeda application, page, and function levels.
2. Device-based access control provides a method for defining the specific devices visible to each user group. This method of control limits the view of device information to only those devices for which a user is responsible.

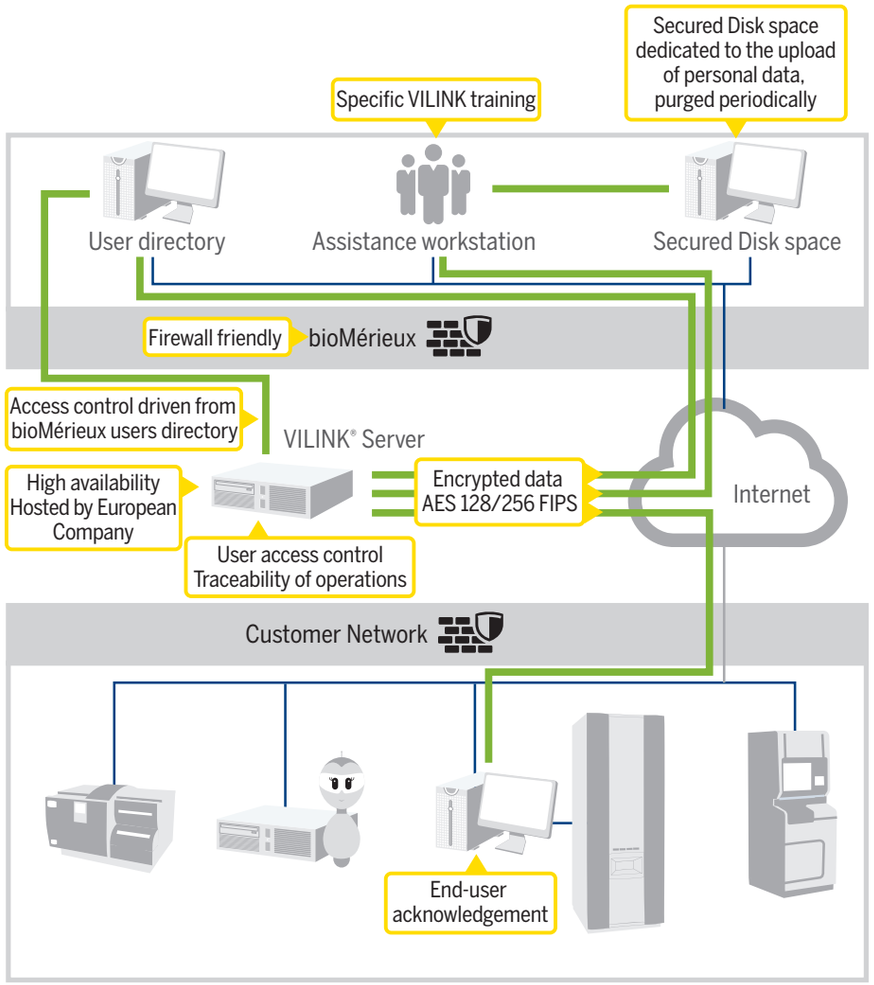
User and Application Security

The Axeda Policy Server supports its own internal user store, or it can connect to any Microsoft® Active Directory® (AD) server. This allows end-user IT departments to have centralized control via their normal operating procedures in order to control who manages policies and administers the Axeda Policy Server.

Automatic group synchronization sets roles within the Policy Server based on the AD group membership.

Highly Secure

bioMérieux VILINK® is a highly secured solution using a communication encrypted in AES 256 bits. An acknowledgment on the customer side is required to approve the remote access. Only trained users can use the VILINK solution.



About the VILINK® Server

- The VILINK® Server is hosted in a highly controlled protected area, and continuously controlled and policed in order to meet both our own high security standards and the requirements of the most rigorous regulations.
- All Server accounts for bioMérieux users are managed by a robust security policy, with encrypted communications established through HTTPS using a 2048 bit RSA certificate. The only protocol allowed through HTTPS at this level is TLS.
- Audit logs record all VILINK® user activity (remote sessions, files transfers etc.) and are maintained on the VILINK® Server.
- The VILINK® Server is maintained at a continuously high security and availability level, using the most appropriate and up-to-date security tools (e.g. security scanners) to follow best practice in monitoring and penetration testing.

Connections to the VILINK® Server

All Commercial Systems connected to bioMérieux VILINK® communicate with the VILINK® Server through a TLS tunnel (AES 128/256 bits encryption). Every remote session and file transfer goes through this TLS tunnel, protecting any exchange against unauthorised accesses.

Security configuration

bioMérieux strongly recommends the customer to install anti-virus software (supporting Microsoft Windows) on all bioMérieux Commercial Systems, and to apply regular Operating System security updates. Please see the documentation provided with your bioMérieux Commercial System relating to the use of anti-virus and operating systems security updates.

Data Privacy & Organizational Security

bioMérieux has implemented a rigorous data privacy and security program to ensure compliance with all relevant privacy laws during the operation of our software. This program includes, but is not limited to:

1. Assessing and implementing the regulations and standards applicable to the healthcare domain.

2. Gaining your formal agreement before implementing remote access to your network and instrumentation.

3. Implementing a procedure to guard against any data breach in the event of systems being refurbished or swapped over by systematically removing hard drives containing patient data.

4. Limiting users' access to information and information systems in line with their role in the organization, as part of a comprehensive security management system.

5. Screening (when authorised by local regulation) of the personnel accessing patient information.

6. Training all personnel who have access to patient data on internal policies and procedures, to help them understand their responsibility to maintain the confidentiality of such information and to comply with regulations in force.

7. Implementing physical security measures to ensure that unauthorised users can not enter bioMérieux premises. These measures include restricting physical access to data servers and data-hosting environments.

8. Complying with password security standards to ensure that authentication can not easily be compromised.

9. Encrypting access to patient data on laptops used by bioMérieux personnel.

10. Protecting connected systems on bioMérieux network from external security vulnerabilities through a combination of hardware firewalls, antivirus software, intrusion prevention systems and regular Microsoft security updates.

11. Monitoring events at the remote service in order to provide sound and other recordings for use in case of investigation.

To follow these security principles, bioMérieux – acting with the support of security experts – regularly performs penetration tests, security assessments and regulatory audits (e.g. HIPAA, GDPR).

Local data privacy and security regulations

The protection of personal data and respect of privacy are fundamental rights derived from the Universal Declaration of Human rights of 1948. bioMérieux is committed to protecting the confidentiality of the personal data of his employees and partners.

Many countries have tightened regulations restricting the use and disclosure of personal data (e.g.**US HIPAA Federal law, EU GDPR**). These laws require companies to take steps to ensure the confidentiality, integrity and availability of this kind of data. In 2018, bioMérieux has deployed a compliance program regarding regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which has entered into force in May 25, 2018 (GDPR) as well as national French laws.

bioMérieux has officially designated a Data Protection Officer (DPO) to the French Data Protection Authority (CNIL) to control and ensure compliance of the Company with this regulation.

GDPR HIPAA COMPLIANT