Operating Manual

Secure Operating Manual Veya

Title:	Secure Operating Manual Veya	**Part number:**	n.a.
ID:	403037, en, V1.2	**Translated from:**	n.a.

Version:	**Revision:**	**Issue:**	**Document History:**
1	0	2024-10-22	First edition
1	1	2025-06-12	Added: 5.2 Anti-malware Software Updated: 7 Security Controls
1	2	2025-11-25	Updated: 3.1 Description of External Interfaces, 4 User Access and Authentication and 7 Security Controls

Table of Contents

1 About This Manual

1.1 Scope of This Manual

This manual provides cybersecurity information to customers for the Veya software system according to IEC-81001-5-1.

1.2 Definitions, Acronyms and Abbreviations

Abbreviations / Terms	Description
ASM	Application Software Manual
FAS	Field Application Scientist
FSE	Field Service Engineer
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
IAM	Identity Access Management
IoT	Internet of Things
LTSC	Long-Term Servicing Channel (Microsoft)
Maintained Software	Maintained software are software components for which Tecan will notify customers regarding known risks related to security and provide updates.
MFA	Multi-Factor Authentication
MQTT	Message Queuing Telemetry Transport
OS	Operating System
Supported Software	Supported software are software components from 3rd parties for which Tecan will notify customers regarding known risks related to security and the availability of compatible updates.
UMS	User Management System

2 General Information

Description	Information
Product Name	Veya (all models)
Software System Name	Software Image Veya (30252493)
Software Application Name	vControl
Reference to SBOM	Provided by Tecan upon request

2.1 Supported Software

Tecan will monitor the availability of security updates for supported SW. Tecan will provide information about compatible updates on its website.
https://www.tecan.com/knowledge-portal.
Customers are responsible for checking the platform regularly for updates.
Customers are responsible for downloading updates provided by 3rd party and applying them to their systems.
In case available security updates are not compatible with the system, Tecan informs customers about other mitigations that can be used instead of applying the updates.
The following list contains all software items categorized as supported software.

- Inheco ODTC Script Editor
- Inheco ODTC Device Manager
- Inheco Incubator Control
- SAP Crystal Reports
- Microsoft .NET Framework/Runtime
- Microsoft Visual C++
- Microsoft Windows 10 LTSC
- Microsoft SQL Server
- Microsoft Edge WebView2 Runtime

2.2 Maintained Software

Tecan will monitor the availability of security updates for maintained SW. Tecan will provide information about compatible updates on its website
https://www.tecan.com/knowledge-portal.
Customers are responsible for checking the platform regularly for updates.
Updates will either be provided for download on the website or installed by Tecan personnel.

Tecan will provide regular Windows security updates to customers with Tecan embedded PC. The updates are cumulative which means that customers can always install the most recent update which contains all previous updates.

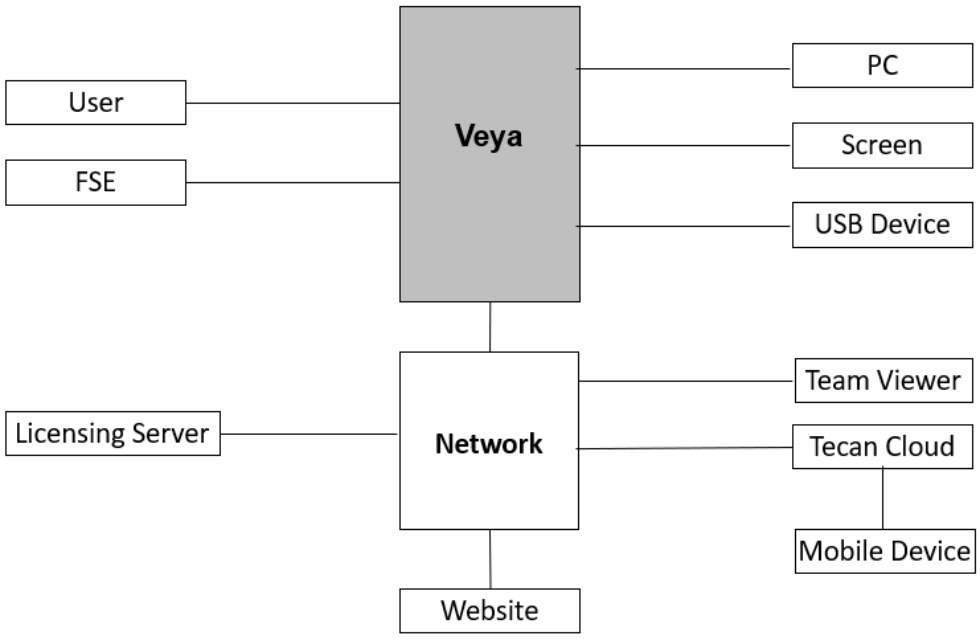
The following list contains all software items categorized as maintained software.

- Tecan MAPLinx Setup software

- Tecan vControl
- Tecan Licensing Client
- Tecan IoT Client
- Tecan G (OLEG)
- Tecan Sample Tracking
- Tecan UMS
- Tecan Magellan
- Tecan Hydroflex Driver
- Tecan 3D Simulator
- Tecan OneView
- Tecan Worktable Editor
- Microsoft Windows (only Windows installed by Tecan on Tecan embedded PC)

3 System Overview

In this chapter and in the system diagram, all external systems or applications that are connected to the system are described to provide an overview of the integration and dependencies that the system requires.



3.1 Description of External Interfaces

Name	Protocol	Purpose
IoT Client (Tecan Cloud)	HTTPS, MQTT	Sending data from the instrument to the Tecan cloud (MQTT). Remote update of IoT Client and instrument registration (HTTPS). All communication to the Tecan cloud service is encrypted using TLS connections with high security ciphers. Please refer to document 403014 IT Considerations for Introspect Software.
vControl API	COM	Option to control vControl from external applications.
Generic USB Device	USB	Communication with external storage and modules like keyboard and mouse.
Tecan Licensing Server	HTTPS	The device gets license from Tecan server via the internet.

Name	Protocol	Purpose
Team Viewer	HTTPS	The device establishes communication with the Team Viewer server for remote support via the internet. Requires download of Team Viewer exe via link provided by Local Helpdesk. Team Viewer exe is not part of the delivered SW system. Please refer to document 401994 Tecan Remote User Guide for security information related to this process.
User	-	PC login with Windows admin or user password. vControl login with admin or user password.
FSE	-	PC login with Windows admin password (provided by customer). MAPlinx Setup login using FSE authenticator.
Customer PC	USB Ethernet	The external customer PC is connected via a USB cable to the USB- port on the outlet panel to control the device variant without an internal PC. The external PC is connected via an Ethernet cable to the RJ45 port on the outlet panel to stream the Deckcheck camera signal.
Customer screen	DP	The external screen is connected via a display cable to the display port on the outlet panel. This applies to the device variant with internal PC (optional).
Network	Ethernet	The PC (internal or external) of the device is connected to the network of the customer for local data exchange and through the internet. For device variants with internal PC the connection is established via Ethernet cable using the RJ45 port at the outlet panel.
Mobile device	HTTPS	Tecan Cloud data can be displayed on the smart phone of the user or other mobile device. This is currently based on a web browser, in the future possibly via an app.

Name	Protocol	Purpose
Websites	HTTPS	The user/FSE can access websites to download or upload data via internet: - Team Viewer software can be downloaded for remote support from the Team Viewer website*. - Manuals can be downloaded from the Tecan website*. - Snapshot files can be uploaded to the Tecan storage location using a link from the Local Helpdesk. - Software updates can be downloaded from the Tecan website*.

***Websites for Download:**

https://get.teamviewer.com/tecanqs

https://www.tecan.com/knowledge-portal

4 User Access and Authentication

This chapter describes what user types and roles are existing and what needs to be considered during operation.

Physical access control shall be in place as defined by local laboratory and facility regulations or GLP / GMP.

Tecan pre-configures the system to isolate it from a network perspective, except for the required external interfaces.

Tecan pre-configures the system with admin accounts for Windows and vControl application software.

The administrator of the operating system of the customer (OS admin) receives full Windows admin rights. The customer assumes full responsibility once the installation of the instrument has been completed. From this point on, Tecan personnel no longer has access. In the event of a service call, the customer must provide Tecan personnel with admin access.

The customer OS admin shall create personalized user accounts for all operators of the device. vControl admin (key operator) shall create personalized accounts for vControl operators.

Tecan will activate Bitlocker hard-disk encryption and handover the recovery key to customer. The customer is responsible for the safe storage of this recovery key.

It is imperative that operators and key operators are not granted Windows administrator rights for safe and secure operation.
Tecan FSE and FAS only require Windows administrator rights when installing, uninstalling or upgrading the software. Windows administrator rights should only be granted temporarily. Alternatively, these tasks can be performed by your Windows administrator with guidance from Tecan FSA/FAS.

Summary of different roles and privileges are shown in the table below:

No.	User Group	User Sub-Group	Windows Account and Privileges	vControl Account and Privileges	Setup / Service SW Access
1	End user (customer)	Operator	“User” Read & execute	“User” Execution of defined processes (no rights to modify processes)	No
2	End user (customer)	Key operator	“User” Read & execute	“Admin” Setup, modification, validation and execution of processes	No

No.	User Group	User Sub-Group	Windows Account and Privileges	vControl Account and Privileges	Setup / Service SW Access
3	End user (customer)	OS admin	“Admin” Full admin rights	Optional	No
4	Tecan personnel	FSE, FAS	Admin rights to be provided by customer OS admin to Tecan personnel	Admin rights to be provided by customer vControl admin to Tecan personnel	MAPlinx Setup (certificate/FSE authenticator) Xflex Service SW (on FSE laptop) XInfiniTe-F50 Service SW (on FSE laptop)

5 System Setup and Configuration

5.1 Network Configuration

To allow additional Tecan services, the following configurations are required:

- IoT Client: For more information please refer to **https://www.tecan.com/knowledge-portal/digital-solutions**
- Team Viewer: Outbound connections on TCP port 443 need to be enabled to accommodate https requests.
- License server: Outbound connections on TCP port 443 need to be enabled to accommodate https requests.
- Tecan and Team Viewer websites need to be reachable (https).

For instruments with internal PC the required settings have been pre-configured by Tecan. However, it is the customer's responsibility to integrate the system into the local network and to adapt the required configurations.

5.2 Anti-malware Software

Tecan recommends refraining from actively scanning hard drives or memory while a run is in progress in vControl. If a virus scan must be executed during a run, exclude (whitelist) the following directories and their subdirectories from the scan:

```
C:\Program Files (x86)\Tecan
C:\Program Files (x86)\Common Files\Tecan
C:\Program Files\Tecan
C:\ProgramData\Tecan
```

5.3 Decommissioning of the System

It is in the responsibility of the system user to properly decommission the system. Tecan recommends the following actions in case the complete product is decommissioned:

- Revert network configuration described in “5.1” [13] for additional Tecan services.
- Deactivation of the user accounts.
- Inform Tecan to deactivate the cloud services linked to the decommissioned system.
- Inform Tecan to deactivate licences linked to the decommissioned system.
- Wiping of the system hard drive.
- Destroy the relevant BitLocker Recovery Key.

Tecan recommends following in case only the system’s PC is decommissioned:

- Wiping of the system hard drive.
- Destroy the relevant BitLocker Recovery Key.

6 System Operation and Maintenance

Please refer to the following checklist during system operation and maintenance:

- Customers shall regularly check the availability of software security updates on the Tecan web portal **https://www.tecan.com/knowledge-portal/**.
- Customers shall perform regular backups of their system (please refer to Document 402665, vControl Application Software Manual, Chapter 13 Data Handling).
- Users shall always shut down the system and the running software properly.
- Disconnecting the power cord while the system is powered or closing the application software by shutting down the operating system, may result in the system ending in an undefined state.
- Tecan recommends shutting down and restarting the system periodically to avoid performance problems.

7 Security Controls

The following security controls shall be implemented by the customer to mitigate the risk for cyberattacks:

Risk	Mitigation
Access of unauthorized persons to the system can facilitate cyberattacks.	The system is operated by trained personnel in a professional laboratory with physical access restrictions as defined by local laboratory and facility regulations or GLP / GMP.
In case of a successful cyberattack (no system can be made 100 % secure), confidential information could be accessed and or manipulated.	Never store confidential information (i.e. patient or personal information) on the system (e.g. by use of anonymized data).
When integrating the system into a local network, data transfer from/to the system is enabled from the network and cyberattacks through the network might therefore be possible.	Customers must protect their network by effective means such as a firewall.
Weak passwords can easily be cracked by an attacker and render the system vulnerable to cyberattacks.	Secure passwords shall be used for all Windows and Tecan software accounts. Recommendations are: min. 12 characters, including special, upper & lower and numeric & alphanumeric characters; max.duration of 365 days. The minimum requirements preconfigured by Tecan are: min. 12 characters and max. duration of 365 days.
An attacker could steal usernames and passwords, if you use Command-Line Interface (CLI) arguments for starting and logging into vControl.	When you log into vControl, avoid using the CLI arguments.
User accounts with too many privileges render the system vulnerable to cyberattacks (e.g. malware can be executed or important files deleted/modified).	Provide minimum privileges to User accounts (e.g. use Windows user account type with strongly reduced privileges for instrument operators).
The use of insecure communication protocols (e.g. http) render the communication between the system and the network vulnerable for cyberattacks.	Use secure default communication protocols as preconfigured by Tecan for communication with network.
Account and password sharing strongly increase the risk of cyberattacks and make traceability of actions difficult.	Generate personalized User accounts for all device operators and prohibit account and password sharing.

Risk	Mitigation
An attacker could gain unauthorized access to the Veya software system by using stolen, previously leaked or compromised credentials (e.g., from data breaches).	• Implement a password policy that includes using strong passwords, complexity rules, and update rules. • Do not share passwords between different systems. • Use UMS or IAM with a third-party identity provider (e.g., Windows Active Directory), to enable Multi-Factor Authentication (MFA).