TECAN.

Operating Manual

Secure Operating Manual EVOlution

Title:	Secure Operating Manual EVOlution			Part number:	n.a.
ID:	403467, en, V1.0			Translated from:	n.a.
Version:	Revision:	Issue:	Document History:		
1	0	2026-07-28	First edition		

© 2026, Tecan Trading AG, Switzerland, all rights reserved.

Information contained in this document is subject to change without notice.

Table of Contents

1 About This Manual

1.1 Scope of This Manual

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

1.2 Definitions, Acronyms and Abbreviations

Abbreviations / Terms	Description
ASTM	American Society for Testing and Materials (now ASTM International): a standards-developing organization. In lab/instrument contexts, it refers to the ASTM E1381/ E1394 protocols for transmitting data between laboratory instruments and information systems (LIS/LIMS).
FAS	Field Application Scientist
FSE	Field Service Engineer
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
LIMS	Laboratory Information Management System: software for managing samples, workflows, and data in research, industrial, and analytical labs.
LIS	Laboratory Information System: software for managing clinical/medical lab workflows.
Maintained Software	Maintained software are software components for which Tecan notifies customers regarding known risks related to security and provides updates.
OS	Operating System
Supported Software	Supported software are software components from 3rd parties for which Tecan notifies customers regarding known risks related to security and the availability of compatible updates.
UMS	User Management System

2 General Information

Description	Information
Product Name	EVOlution for Freedom EVOlyzer (all models)
Software System Name	Freedom EVOlution
Software Application Name	EVOlution

2.1 Supported Software

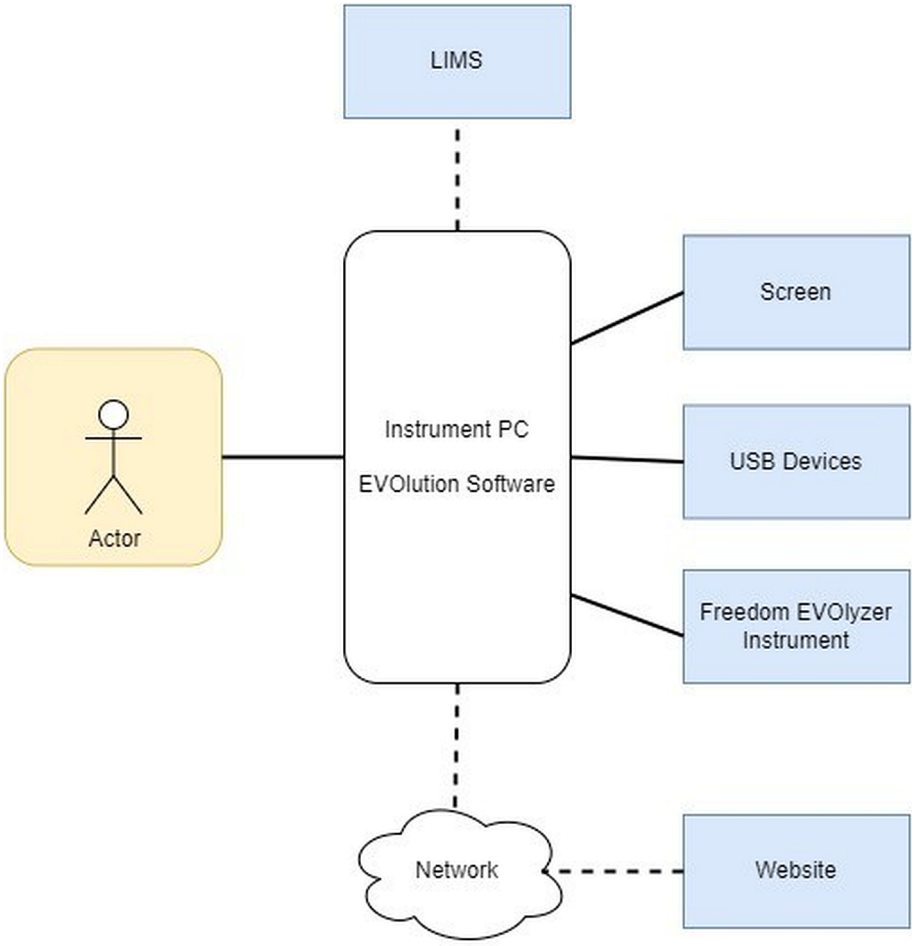
Tecan monitors the availability of security updates for supported software. Tecan provides information about compatible updates on its website.
https://www.tecan.com/knowledge-portal.
Customers are responsible for checking and applying Microsoft security updates and patches through Windows Update or manually.

2.2 Maintained Software

Tecan monitors the availability of security updates for maintained software. Tecan provides information about compatible updates on its website.
https://www.tecan.com/knowledge-portal.
Customers are responsible for checking the platform regularly for updates to EVOlution. Updates are either provided for download on the website or installed by Tecan personnel.

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
LIMS Interface	ASTM E 1394	Serial interface to connect to a LIS/LIMS.
USB Device	USB	Communication with external storage and modules like keyboard and mouse.
Actor	-	Different user roles interacting with EVOlution.
Instrument PC	USB	The instrument PC is connected via a USB cable to the USB-port on the EVOlyzer instrument.

Name	Protocol	Purpose
Customer screen	DP/HDMI/ VGA/DVI	The external screen is connected to the EVOlution instrument PC.
Network	-	The customer PC is connected to the network of the customer for local data exchange and optionally to the internet through a properly configured firewall for recommended OS security updates.
Websites	HTTPS	The user/FSE can access websites to download or upload data via internet: • Manuals can be downloaded from the Tecan website*. • Collect&Zip files can be uploaded to the Tecan storage location using a link from the local Helpdesk.

***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 exist and what needs to be considered during operation.

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

During the initial installation and configuration, an OS administrator account is required on the instrument control PC. The customer assumes full responsibility once the installation of the instrument has been completed, including the application of security updates (refer to chapter “Supported Software” [5]). From this point on, Tecan personnel no longer has access. In the event of a service call, the customer must provide Tecan personnel with OS administrator access.

The customer OS administrator must create personalized unprivileged user accounts for all users of the instrument according to their policies. **EVOlution should never be run with a privileged (Administrator) OS user account.**

The EVOlution administrator must create personalized accounts for EVOlution users and assign them to the specific EVOlution user groups (refer to Freedom EVOlution SW Runtime Controller Manual).

EVOlution User Group	EVOlution Access Rights
Lab operator	Start Run, Maintenance
Application specialist	Start Run, Maintenance, Application Settings
Administrator	Start Run, Maintenance, Application Settings, User Management

Tecan Support, FSE and FAS needs to be provided with an OS administrator account and an EVOlution administrator account when requested.

5 System Setup and Configuration

5.1 Network Configuration

It is the customer's responsibility to integrate the system into the local network and to adapt the required configurations.
It is recommended to set up firewall rules to block all incoming traffic and only allow services that are necessary on the PC.

It is recommended to isolate the EVOlyzer instrument PC running EVOlution from the rest of the network (e.g., by putting it in an isolated VLAN).

5.2 Anti Malware/Virus Software

Tecan recommends refraining from actively scanning hard drives or memory while a run is in progress in EVOlution. 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:\ProgramData\Tecan
```

5.3 Folders of Interest

Logs are readable for regular OS user accounts. If the content is deemed sensitive by the individual use case, it is advised to move the files periodically to a more secure location if desired.

Tecan provides the "Collect and Zip" as part of the EVOlution installation to collect EVOlution logs and configuration. UMS is not included in the output.

Below are the directories in the default installation containing configuration and logs recommended to be backed up periodically to restore the installation in case files are deleted or modified outside of EVOlution.

Product	Description	Path
EVOlution	Logs and Configuration	`C:\ProgramData\Tecan\`
EVOlution	TPL Files	`C:\Transfer`
HydroFlex	Logs	`C:\Users\Public\Documents\Tecan\LogFiles\Freedom EVOlution\`
HydroFlex	Pdfx Files	`C:\Users\Public\Documents\Tecan\Pdfx\ *.pdfx`
LIS	ASTM com settings	`C:\Program Files (x86)\Common Files\Tecan\Communication\2.3.0\Config\*Lis.channel.config`
Columbus	Logs	`C:\Users\Public\Documents\Tecan\LogFiles\Washer\`

Product	Description	Path
Magellan	Logs	`C:\Users\Public\Documents\Tecan\LogFiles`
Sunrise	Logs	`C:\Users\Admin\AppData\Local\Temp\*rdrole*.log*`
Sunrise	Archived Files	`C:\Users\Admin\AppData\Local\Temp\*rdrole*.zip*`

UMS logs and configuration are recommended to be backed up periodically to restore the installation in case files are deleted or modified outside of UMS. The encrypted UMS database is protected and requires elevated OS privileges to be read or backed up.

Product	Description	Path
UMS	Database	`C:\ProgramData\Tecan\Tecan User Management\v1.1\UserManagement.xml`
UMS	Logs	`C:\ProgramData\Tecan\Tecan User Management\v1.1\Log\`
UMS	Audit Trail	`C:\ProgramData\Tecan\Tecan User Management\v1.1\Audit\`

5.4 Decommissioning of the System

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

- Wipe the system hard drive.
- Destroy any relevant BitLocker Recovery Key.

The instrument itself does not store any data.

6 System Operation and Maintenance

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

- Customers must regularly check the availability of software security updates on the Tecan web portal https://www.tecan.com/knowledge-portal/.
- Customers must perform regular backups of their system (Freedom EVOlution SW Application Software Manual, 394802, en, V2.3, Chapter 16.5.7 Backing Up Files).
- Users must 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.
- Customers are responsible for applying Windows security updates.

7 Security Controls

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

Risk	Mitigation
Tecan FSE has Admin Access to EVOlution Software system and can change user access.	Change the UMS admin password to a strong password at system handover part of IQ/OQ.
An attacker could try one password after another to gain access to system.	• Implement a password policy that includes password strength, complexity rules, and update rules, and not to share passwords between different systems. • Enable email to Admin when the account locks because of too many incorrect password entries. • Periodically audit UMS logs for suspicious entries.
If a user uses the same password across multiple accounts, a compromise of just one of the accounts will enable an attacker to access all of them.	• Implement a password policy that includes password strength, complexity rules, and update rules. • Implement a password policy that forbids sharing of passwords between different systems.
An attacker could gain unauthorized access to the EVOlution Software system by using stolen, previously leaked or compromised credentials (e.g., from data breaches).	• Implement a password policy that includes password strength, complexity rules, and update rules. • Implement a password policy that forbids sharing of passwords between different systems.
Attack through open Internet connection.	Implement a firewall and end point protection to allow only connections needed by the EVOlution PC.
The email account login credentials for the UMS Email notification service could be exposed and used maliciously. These credentials are stored unencrypted in the configuration.	When using the UMS Notify via e-mail option for UMS account, it is recommended to use a dedicated email account with restrictive sending policies applied for this function.
Accidental or malicious deletion of configuration files for EVOlution and other Tecan Software components, on which EVOlution depends, might temporarily make the system unusable. These files are in a user writable directory.	It is recommended to keep periodic backups of all configuration files and folders listed in chapter “Folders of Interest” [9] for quick system recovery in case files are lost or corrupted. The backup should be stored on a different PC and be read-only for regular users.

Risk	Mitigation
Unencrypted communication when using a web browser to interact with Tecan support.	It is recommended to setup the system web browser, via Windows Group Policies or Plugins, in a way that only HTTPS connections are allowed and any HTTP connection gets changed to HTTPS by default.
A specially prepared (malicious) log entry can cause the LogViewer to automatically execute arbitrary code in the context of the user viewing the logs with the LogViewer.	Harden the Windows default settings so that all active content is disabled by updating the registry keys listed in the chapter “System Hardening” [14]. Verify the settings remain in place after any Windows or Internet Explorer update. Test these changes before roll-out, since disabling active content may affect other components that rely on the same engine.

8 System Hardening

```
; ===========================================================
; GLOBAL IE/MSHTML HARDENING - STATIC HTML & IMAGES ONLY
; Zones:
; 0 = Local Machine (Your computer / file://)
; 1 = Local Intranet
; 2 = Trusted Sites
; 3 = Internet
; 4 = Restricted Sites
; ===========================================================

; ------------------------------
; Helper: apply to all zones HKLM
; ------------------------------

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\0]
"1400"=dword:00000003 ; Active scripting (JS/VBScript) = Dis-
able
"1402"=dword:00000003 ; Scripting of Java applets = Disable
"1405"=dword:00000003 ; Script ActiveX controls marked safe
for scripting = Disable
"1200"=dword:00000003 ; Run ActiveX controls and plug-ins =
Disable
"1201"=dword:00000003 ; Download signed ActiveX controls =
Disable
"1208"=dword:00000003 ; Allow previously unused ActiveX con-
trols to run without prompt = Disable

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\1]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\2]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\3]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
```

```
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\4]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

; ------------------------
; Same for HKCU (per-user)
; ------------------------

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\0]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\1]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\2]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\3]
"1400"=dword:00000003
"1402"=dword:00000003
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Internet Settings\Zones\4]
"1400"=dword:00000003
"1402"=dword:00000003
```

```
"1405"=dword:00000003
"1200"=dword:00000003
"1201"=dword:00000003
"1208"=dword:00000003

; =============================================================
; Disable legacy JScript engine for IE
; (affects IE and WebBrowser control using iexplore.exe host)
; =============================================================

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Ex-
plorer\Main\FeatureControl\FEATURE_DISABLE_LEGACY_JSCRIPT]
"iexplore.exe"=dword:00000001
```