

Recommendations for data security policy on ZEISS Microscopy Systems

About this document

This document is intended for ZEISS field service engineers to address customer questions concerning security measures when connecting ZEISS PC's to a network. It's covering the complete MIC portfolio including light-, electron-, X-ray- and helium ion microscope system software.

General rules

When the PC of the microscopy system is connected to a network, activation of Windows Update functionality and installation of security software is recommended.

Changes on the Operating System

The following modifications have, in our experience, no effects on the functionality of the PC system:

- Network integration possible
- Logon as Domain Users in an Active Directory environment (possibly with local administrator privileges if user needs to install software)
- Installation of standard software (e.g. Microsoft Office)
- Installation of printers
- Windows automatic updates and third-party software updates (Windows Service Packs are to be considered different)

Recommended settings

- *Windows 7*
Allow option "Check for updates but let me choose whether to download and install them".
- *Windows 10*
Choose what updates are installed "Current Branch for Business".

Effects of following modifications can't be estimated:

- Modifications in the Windows operating system
- Implementation of group policies and scripts
- Installation of third-party software with hardware support
- Installation of third-party software for generating large data rates (such as backup software) due to possible performance problems of the simultaneous operation of system operation software
- Storage of data on network drives by redirecting folder structures (e.g., there can occur performance problems in case of Fast Acquisition systems or limitation of the available data storage capacity (disk quota))

Configure security software and operating system settings for ZEN blue edition, ZEN black edition and ZEN core

Configure security software

The following section explains how to configure your security software for installation and optimum operation of ZEN properly.

i INFO

The term security software combines all programs which protect your computer from viruses, unwanted interventions, etc. This includes virus scanners, firewalls and intrusion detection systems. If you don't adapt the security settings there can be problems while installing or running ZEN. The following topics will show you how to avoid problems with the security software and adapt the settings correctly.

Remark

ZEISS is using McAfee security software on all systems connected to the company network, no corresponding issues were reported during software development and testing of microscopy systems.

Before installation

To ensure correct installation, we recommend to perform the following settings:

- *Restore point*
Set a restore point for the possibility to roll back the system in the case problems occur. It also is possible to ask the local ZEISS support team to create an image of the main drive of the PC before the security software is installed and setup by the customers IT department.
- *Lower security rules*
Set the security rules from "high" to "low". How you set the security rules, refer to the respective operating instructions of your security software.
- *Disable security software*
In rare cases, you may need to disable the security software completely. Make sure that you enable the security software after installation. How to disable or enable the security software, refer to the respective operating instructions of your security software.

After installation

To ensure the optimal operation on Windows, we recommend you to perform the following settings after the installation:

- *Exclude ZEN program files from virus scanning*
Exclude the following files from virus scanning:

- ZEN.exe
- ZENService.exe
- MTBconfig.exe
- Configuration tool.exe
- AimApplication.exe
- CZCanCheck.exe
- CZCansrv.exe
- System_Maintenance_Tool.exe
- ZISProtocolServer.exe
- ZISProtocolServerx64.exe
- MTBService.exe
- MTBMonitor.exe

Remark

How to exclude files from virus scanning, refer to the respective operating instructions of your security software.

- *Exclude ZEN specific file extensions from virus scanning*
Exclude files with the file extensions

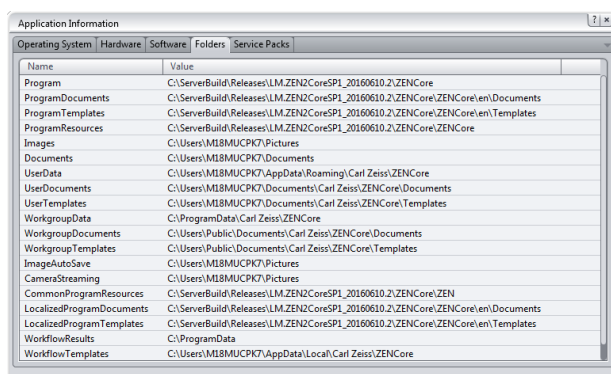
- *.dzi
- *.zvi
- *.zishm
- *.lsm
- *.zmbi
- *.fcs
- *.raw

Remark

How to exclude file extensions from virus scanning, refer to the respective operating instructions of your security software.

- *Exclude ZEN specific folders from virus scanning*

Under Help | About ZEN ... | Show ZEN Information | Folders you can see the program specific folders. How to exclude folders from virus scanning, refer to the respective operating instructions of customers security software.



Default folders

In the following table you can see the folders in which the captured images will be stored in ZEN per default.

Operating system	Folder / path
Windows 7 (en)	My Pictures and %USERPROFILE%\My Pictures and C:\Users\{user name}\My Pictures
Windows 10 (en)	Pictures and %USERPROFILE%\Pictures and C:\Users\{user name}\Pictures

- [Change default ZEN image folder](#)
Under File | Export/Import | Export or under File | Save as change the folder you want to store your images into.
- [Change default folder for automatic image storage and continuous image acquisition](#)
Under Tools | Options | Saving | Auto Save Path set your desired path/folder.
- [Change default folder for images on your operating system](#)
In Windows 7 in the context menu of My pictures.

Temporary files

Operating system	Folder / path
Windows 7 & 10 (en)	%TEMP% or %LOCALAPPDATA%\temp or C:\Users\{user name}\AppData\Local\Temp

- Change default folder for temp files
 - First, define an appropriate path for the TEMP environment variable (user context).
 - Then define the environment variable SWAP indicating a corresponding path.

For Windows 7 & 10 this has the following paths or folders that you must exclude from virus scanning:

Operating system	Folder / path
Windows 7 (en)	C:\Users\{user name}\My Pictures
Windows 10 (en)	C:\Users\{user name}\Pictures
Windows 7 & 10 (en)	C:\Users\{user name}\AppData\Local\Temp
Windows 7 & 10 (en)	%TEMP%
Windows 7 & 10 (en)	%SWAP%

System specific folders

If you are using a ZEISS PC system, the location of your images is predefined. The table below shows the system specific folders for the following ZEISS Microscopy High-End and Mid-Range workstations:

- Microscopy Workstation High-End GPGPU - 410203-9910-000
- Microscopy Workstation HighEnd - 410203-9909-000
- Microscopy High-End Workstation - 410203-9908-000
- Microscopy Workstation Mid-Range - 410202-9902-000
- Microscopy Mid-Range Workstation - 410202-9901-000
- Microscopy Workstation Compact - 410201-99010-000
- User PC Compact Smartpool - 410211-9002-000

Operating system	Folder / path
Windows 7 (en)	D:\Users\{user name}\\Pictures Notice: C:\Users was moved to D:\Users by changing the registry keys: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\ProfileList\ProfilesDirectory Default: %SystemDrive%\Users Modified: D:\Users

Summary

To ensure correct operation of ZEN it is necessary to ensure that the security software on your computer is not blocking the program. For full functionality you should have made the following settings:

- You have disabled the security software during installation or reduced the security settings.
- You have excluded the entire application, the defined paths or relevant files from virus scanning.

Configuration of security software and operating system settings for SmartSEM

In general, operation of SmartSEM and the respective software is supported only on the delivered All-in-One PC with Windows 10 as the operating system.

Installation of the SmartSEM software on third-party computers is not supported. Windows 7 is now only supported for legacy systems. SmartSEM and its supporting software require Windows Updates to be installed.

Recommended Settings for Anti-Virus Software

- *Exclusion of program files*
Exclude the files SmartSEM.exe, EMServer.exe and ASAPEngine.exe from the anti-virus scan.
- *Exclusion of file types*
Exclude these file types from the anti-virus scan: Image files: *.czi, *.tif
- *Exclusion of program specific folders*
Exclude the following program specific folders including all subfolders from the anti-virus scan:
 - Folder for application settings:
%programdata%\Carl Zeiss\SmartSEM or C:\ProgramData\Carl Zeiss\SmartSEM
 - SmartSEM application folder (default): C:\Program Files\Carl Zeiss\SmartSEM
 - Carl Zeiss Remote Service folder (default): C:\Program Files\Axeda
- *Exclusion of the USB3 interface from the behavior-based surveillance and analysis*
If your security software contains a host based intrusion prevention, turn it off for the USB3 interface to the SmartSEM Microscope.

Instructions how to exclude specific folders and files from the antivirus scan can be found in the security software instruction manual.

Configuration of security software and operating system settings for ORION NanoFab

Antivirus and Spyware Compatibility

The user-interface that runs on the NanoFab's control computer is certified to be compatible with the Microsoft Windows Defender and the McAfee Total Protection software. It has not been tested for compatibility with other software products of this type. Virus and spyware scanning can be expected to degrade system response time, and therefore should be scheduled to occur during off-hours. The ORION NanoFab system requires that the following endpoints remain open at all times:

- Access to and from the 192.168.0.1 to all addresses on the 192.168.0.nnn sub-domain.
- On the local-host the following ports must remain open at all times: 1234, 1235, 1236, 3306.

Configuration of security software for Xradia systems

All customer PCs are shipped with the ESET Nod32 antivirus software and automatic update function of this antivirus software should be activated. ZEISS is using McAfee security software on all systems connected to the company network, no corresponding issues were reported during software development and testing of microscopy systems also in the context of Xradia systems. It has not been tested for compatibility with other software products of this type. Virus and spyware scanning can be expected to degrade system response time, and therefore should be scheduled to occur during off-hours.

Configuration of security software for Zeiss Predictive Service

If your system is connected to ZEISS Predictive Service please exclude the Zeiss Predictive Service Agent executable from anti-virus scanning. The default location for this folder is: C:\Program Files (x86)\Carl Zeiss\Predictive Service Agent\Zeiss Predictive Service Agent.exe.