WinGuard System Requirements

Updated March 2023

The hardware requirements depend on the expansion stage of the system and the linked devices. The following system requirements apply for the standard expansion stages:

Server:

Basic

- Intel Xeon E-2374G 3,7 GHz 8 MB, Quad-Core CPU *(or comparable)*
- 8 GB ECC DDR4-3200 RAM
- 250 GB NVMe SSD*
- 1 Gbit NIC
- Windows Server 2022, Windows Server 2019, Windows Server 2016

Professional

- Intel Xeon E-2386G 3,5 GHz 12 MB, Hexa-Core CPU *(or comparable)*
- 16 GB ECC DDR4-3200 RAM
- 500 GB NVMe SSD*
- 1 Gbit NIC
- Windows Server 2022, Windows Server 2019, Windows Server 2016

Enterprise

- Intel Xeon E-2388G 3,2 GHz 16 MB, Octa-Core CPU *(or comparable)*
- 32 GB ECC DDR4-3200 RAM
- 1 TB NVMe SSD*
- 1 Gbit NIC
- Windows Server 2022, Windows Server 2019, Windows Server 2016

Workstation:

Express / Client

- Intel i5-11600K 3,9 GHz, Hexa-Core CPU *(or comparable)*
- 16 GB DDR4-3200 RAM
- 2 GB PCIe Graphics Card
- 100 GB NVMe SSD*
- 1 Gbit NIC
- Windows 11, Windows 10 Pro (64-Bit)

) The required storage space depends on the system usage and the system settings. For operation of a WinGuard Server, at least 100 GB available local disk space is required. A WinGuard workstation requires at least 50GB available **local disk space. The usage of redundant local disks (e.g. RAID-technology) is recommended for safeguarding against failure.*

Interface Server:

The interface server specification is depending on the connected systems. For remote connection of a single system, it is possible in most cases to use a fanless Embedded PC (e.g. Intel Celeron N5105 2,0 GHz CPU, 8 GB DDR4 RAM *or comparable*).

Notes

Compatibility

A binding statement about the compatibility of the used operating system in combination with the installed software components of other manufacturers (e.g. required SDKs or APIs) cannot be given by Advancis Software & Services GmbH but only by the respective manufacturers.

Time synchronization

For the operation of WinGuard, the time synchronization between the network participants must be ensured, e.g. via a domain server, an NTP server or a WinGuard function. However, the latter requires starting of WinGuard with administrator rights.

User account control

In order to use WinGuard, especially the “Watch-Dog”-function, write/read permissions of the program directory are required. This may go along with the configuration of the user account control of Windows 8.1 (or more recent) and Windows Server 2012 (or more recent).

Anti-Virus software

Using Anti-Virus software can cause interferences between the access from WinGuard and access from Anti-Virus software to critical system files. Therefore, access can be blocked or delayed. We suggest taking precautionary measures (e.g. adding the WinGuard files/folders to the exclusion list of the Anti-Virus software).

Operating system patches/updates

Windows operating system patches/updates always need to be up-to-date. It is required that patches/updates recommended by Microsoft are installed.

Software Security and Hardening

Please note the information on system hardening in the WinGuard manual, chapter "Software security". Regarding the use of the WinGuard web server, please note the information in the manual in the "Web server and web client" chapter.

Virtual Machines

WinGuard has been designed to run on dedicated hardware under a Windows operating system. A virtualization of the hardware by hardware emulation/hardware virtualization or para-virtualization is possible subject to the following restrictions:

System restrictions

As WinGuard is, depending on the project, using numerous interface modules to connect the hard- and software of third party manufacturers, it must be ensured that all components linked to the total system are functional in a (partly) virtualized environment.
For serial connections it must be ensured that the connection must be similar to real hardware, e.g. with regard to the timing behaviour for sending/receiving of telegrams.

Advancis Software & Services GmbH cannot give any binding information about the virtualization characteristics of any connected third-party system. Problems might occur especially upon switching the Virtual Machine for load balancing or high availability purposes. To ensure high operation reliability it is recommended to use the proprietary Hot-Standby system of WinGuard instead.

License restrictions

If WinGuard software licenses are applied, please note that the hardware specifications of the used virtual machine must be invariable as otherwise a new activation of the software license will be necessary. The linkage to the system hardware is established based on the Serial number of the system drive and the MAC address of the primary network adapter.

As it depends on the applied virtualization system which actions lead to a system hardware change of the host system, it is not possible to provide further information about the general possibility to copy/switch the host system between different hosts without a new activation.

If the system hardware of the host system is changed regularly, a hardware dongle should be used to avoid required reactivation efforts.