## CARTO® 3 System OS Hardening

The Operating System of the CARTO® 3 System has been hardened **based on NIST recommendations** in the **USGCB** for specific Windows 7-based systems, with respect to their relevance for the specific needs of CARTO® 3 System.

During the preparation of the CARTO® 3 System PC® image, the OS hardening is installed by execution of dedicated scripts which:

* Disable network discovery by disabling SSDP Discovery Service (SSDPSRV)
* Define **Windows Log Size** and **Windows Log Retention** policy for all Windows logs:
  + Application
  + Security
  + System
* Restrict **Windows Guest** user access to said Windows logs
* Define **Windows Local Policies** settings for:
  + Audit Policy
  + User Right Assignments
  + Security Options
* Operate directly on **Windows Registry** keys by:
  + Modifying their default values
  + Creating them with specific values
  + Deleting them

The OS hardening scripts are updated before each new CARTO® 3 System release and before the validation phase of the product with sufficient time to detect any potential negative impacts on the system function.

CARTO® 3 System Antivirus

|  |  |  |
| --- | --- | --- |
| DxNoteCaution.png | ***CAUTION*** | Do not disable or reconfigure the antivirus application or settings. It can expose the CARTO®3 System to security risks. |

### Antivirus Scan Timing

The system will not start scheduled antivirus scans while a study is in progress in order to prevent a negative impact on performance.

* If a study is started while an antivirus scan is in progress, the scan will automatically stop.

When an antivirus scan is due, the user will be prompted to select the “Scan & Shut Down” exit option upon exit from the CARTO® 3 System application. This exploits the pre-shutdown time for virus scan and avoids disturbance of studies.

Connected USB storage devices are scanned only when accessing files.

* If the scan detects a file with a virus that cannot be removed, the user is notified that the file cannot be accessed.
  + The antivirus then blocks access to the infected file to protect the operating system.
* Unaffected files from the same USB storage device will remain accessible.

### Antivirus Actions Taken upon Virus Detection

If the antivirus application detects a virus during a scan, it automatically attempts to remove the virus and repair the infected file with no need for user action

* If the antivirus application cannot remove a virus, the CARTO® 3 System opening screen displays a message recommending not to use the system until Biosense Webster Service and Support Department resolves the issue.
  + Refer to the CARTO® 3 System IFU supplied with this system for further details.
* To continue using the system without resolving the issue, the user must explicitly select a check box to confirm that they are aware of the risks taken when using the system under such conditions.

## Proprietary Software

CARTO® 3 System Workstation Software includes in-house designed, implemented, and validated software, using standard tools and according to the Biosense Webster SOPs. The main programming languages are C++ and C#. The development environment is within the secured Johnson & Johnson network.

Software Development Tools and Methods are implemented according to the Quality requirements of Biosense Webster Software Development Procedures and Guidelines.