RI.HIP NAVIGATION on CORI◊ Surgical System

OPERATING SYSTEM & SECURITY SOFTWARE UPDATES

General Information

To ensure your Smith+Nephew RI.HIP NAVIGATION on CORI Surgical System continues to operate as intended, Smith+Nephew recommends following these guidelines on Windows and antivirus software updates. These guidelines will be updated on an ongoing basis through this website. Please ensure that you consult with your organization's IT security team in relation to use of RI.HIP NAVIGATION and these guidelines.

Windows Updates

RI.HIP NAVIGATION is configured via local "Group Policy" settings by default. If your organization uses Windows "Group Policy" settings on any servers where RI.HIP NAVIGATION software is installed, do not change the configuration.

Only install Microsoft security updates; both **Monthly Rollups** and **Security-only updates** are allowed. Do not install service packs and optional updates. Medical device regulations require service packs to be tested and released by the medical device manufacturer. If RI.HIP NAVIGATION is added to the hospital domain, the guidance in this document is recommended.

Although **Microsoft security updates** may be installed immediately after release from Microsoft, Smith+Nephew recommends postponing the installation by five working days. This document will be updated within the five days, if needed, after Smith+Nephew evaluation of the security updates.

Below is the information concerning following computer-based policy settings:

For Windows 10 and later:

- Disable "**Turn on recommended updates**" via Automatic Updates.
- Disable "**Allow Automatic Updates immediate installation**."
- Enable "**No auto-restart with logged on users**" for scheduled automatic updates installations.
- Set "**Configure Automatic Updates**" to "**Disabled**".

Do not install updates during patient treatment.

The following Security updates cannot be installed:

- **KB2823324**: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege (2829996): MS13-036
- **KB2984615**: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege (2984615) MS14-045
- **KB4577051**: 2020-09 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based systems

Driver Updates

Do not update drivers on RI.HIP NAVIGATION.

Do not use either manual setup or Windows updates to update drivers on RI.HIP NAVIGATION. This policy is ensured by the “Group Policy” settings, which should not be changed.

For Windows 10:

- Set “**Specify search order for device driver source locations**” to “**Enabled**” and check the “**Do not search Windows Update**” checkbox.
- In the Local Group Policy Editor, set “**Do not include drivers with Windows Updates**” to “**Enabled**”.

Applicable Group Policy Settings
If your organization uses Windows “Group Policy” settings on any servers where Smith+Nephew software is installed, do not change the configuration of the following policies:

- Computer ConfigurationPoliciesAdministrative TemplatesWindows ComponentsRemote Desktop Services*
- Computer ConfigurationPoliciesAdministrative TemplatesWindows ComponentsWindows PowerShell*
- Computer ConfigurationPoliciesWindows SettingsSecurity SettingsSoftware Restriction Policies*
- User ConfigurationPoliciesAdministrative TemplatesWindows ComponentsRemote Desktop Services*
- User ConfigurationPoliciesAdministrative TemplatesWindows ComponentsWindows PowerShell*
- User ConfigurationPoliciesWindows SettingsSecurity SettingsSoftware Restriction Policies*

Antivirus Software
Smith+Nephew recommends protecting the system with state-of-the-art antivirus software. System performance must be verified by a Smith+Nephew representative after the first antivirus software installation. Be aware that some malware protection software (e.g. virus scanner) settings can negatively affect system performance. For example, if real-time scans are performed and each file access is monitored, then access to patient data may be restricted. For best results:

- Disable any extra antivirus software features (e.g. browser or email-scanners, additional firewall).
- Disable antivirus software pop-up messages.

Configure antivirus software (e.g. by adding to folder exceptions) so that it does not scan or modify the following:

- C:\Brainlab, D:\Brainlab and F:\Brainlab, etc.
- C:\PatientData, D:\PatientData and F:\PatientData, etc.

Third-Party Software
With the exception of antivirus and Microsoft security updates, do not install any third-party software without approval from Smith+Nephew. If third party software is installed, the medical device’s safety and effectiveness can no longer be ensured, and any warranties may be void.

Best Practices

For best results, Smith+Nephew recommends the following:

- Conduct security scans of storage devices and media (e.g., CD-ROM, DVD-ROM, USB HDD and USB flash memory drives) for detection and removal of any malware prior to device or media usage.
- Enable "**System Restore**" for drive **C:** in order that the system can be restored to a previous state, if required.
- Schedule download and installation of Windows and anti-virus updates at system shutdown. Pay special attention to servers and virtual machines and ensure that the systems are fully rebooted afterwards.
- If an on-access/real-time scan is not activated, schedule an on-demand/scheduled scan at system shutdown.

More Information

This policy supersedes all past and present product documentation. For further information or assistance, contact Smith+Nephew customer support.

- +1 833 766 2846 (Telephone)
- ri.support@smith-nephew.com