RALS™
CONNECTIVITY FOR POCT

Abbott

RALS™ System Anti-Virus/Endpoint Security Software Exclusions and Back-up Recommendations

General Anti-Virus and Endpoint Security Software Recommendations:

- Install your organization's preferred anti-virus package immediately following connection to the network (or prior to connection if possible).
  - If using Sophos® Anti-Virus, avoid Sophos® Endpoint Security and Control for Windows (Web Intelligence component), which has been found to interfere with proper RALS™ System operation. Contact RALS for additional information.
- Ensure virus definitions are current and updated automatically.
- Configure the anti-virus application based on the recommendations in this document to ensure that performance of the RALS System is not impacted. The recommendations take into consideration the following:
  - Avoid scanning of non-executable type files, where altering or deleting an "infected" file (potentially a false positive detection) may cause significant harm to the system.
  - Avoid "real-time" scanning of non-executable type files that are frequently accessed/written as part of normal system operations to avoid the potentially significant performance impact to the system.
- If active/real-time scanning is enabled, set to scan files when modified only.
- Perform a manual full-scan after installation and configuration of the AV system to verify system is "clean."

System	File/Process Exclusions	Explanation
RCS (RALS Core System)	**Application files:** • *.log files from D:\MAS and all sub-directories • .exe files from D:\MAS and all sub-directories. • *.txt files from D:\MAS\RALSIntf and all sub-directories • D:\Temp\LISEventLog.txt	The files should be excluded from scanning to prevent interference with the RALS application Optionally, exclude D:\MAS*.*
	Database files: The following file types are typically located in the RALS install directory: • *.mdf • *.ldf • *.ndf The default location is D:\MAS\RALSPlus\DB\Backup.	Reference: http://support.microsoft.com/kb/309422 Optionally, exclude D:\MAS\RALSPlus\DB*.*

	Windows OS related: %windir%\SoftwareDistribution\Datastore*.edb • %windir%\SoftwareDistribution\Datastore\Logs*.log • %systemroot%\System32\Spool*.*	Reference: http://support.microsoft.com/kb/822158
	IIS related: • %systemroot%\IIS Temporary Compressed Files • %systemroot%\system32\inetsrv • *.log [in IIS logging directory location(s)]	Reference: http://support.microsoft.com/kb/817442
	File Share: • After the RALS 8.0.0 and higher versions, customers will need to back up device files and reports on a nightly basis from the File Share directory. • The default File Share location is D:\RALSFileShare. • If an alternate local location or a remote location is used for the file share, the device files and reports will need to be backed up. • Previously, these files and reports were included in the database and covered by database backups.	
RALS V-Host (Hyper-V host)	**Hyper-V related:** • D:\VSystems and all sub-directories • C:\ProgramData\Microsoft\Windows\Hyper-V and all sub-directories	Reference: https://support.microsoft.com/en-us/help/3105657/recommended-antivirus-exclusions-for-hyper-v-hosts
Customer Self-Hosted Virtual System	Please consult your specific hypervisor manufacturer for recommended AV exclusion guidance.	
i-STAT/DE System	**Application files:** • C:\istat32*.*	The following files are excluded from scanning to prevent lockup of executables and DLLs by AV solution: • Core DE Application files • DE database files • i-STAT analyzer software files • eVAS files are excluded
	Database files: • C:\Program Files (x86)\SQL Anywhere 17*.*	The following files are excluded from scanning to prevent lockup of executables and DLLs by AV solution: • SQL Anywhere application files

	Internet Information Services: • C:\inetpub\wwwroot\ActiveX*.* • C:\inetpub\wwwroot\IstatDeSystem*.* • C:\inetpub\wwwroot\iSTATDMI*.* • C:\Windows\system32\inetsrv\w3wp.exe • C:\Windows\SysWOW64\inetsrv\w3wp.exe	The following files are excluded from scanning to prevent lockup of executables and DLLs by AV solution: • DE web application files • IIS Worldwide web publishing service

Note: Abbott does not recommend a specific vendor or product for antivirus protection. If you require additional assistance configuring your antivirus application, please contact your software vendor.

General Backup Recommendations:

- ARDx Informatics, Inc. does not provide an off-server backup method. If a system failure should occur, we depend on the IT backup from the night before to restore the data lost.
- On the RALS Server, the RALS SQL Database will back up every night at 3AM (Note: 3AM is the default but may be changed by customer) into the location: (D:\MAS\RALSPlus\DB\Backup).
  - The hospital IT staff will need to back up the files in the Backup folder at the time the automatic nightly backup has completed, using their backup software to a secure location, on a nightly basis.
- On the RALS-DE Server, the C:\AUTODEBACKUP directory will need to be backed up on a nightly basis.

Doing live VM based “snapshots” with the RALS™ Systems when the SQL database is installed locally is not recommended, and is not a supported approach for doing a system recovery.