Antivirus Configuration

Last Modified on 03/02/2023 1:57 pm AEST

With today's online digitally connected world, it is now more important than ever to have up-to-date, current and reputable anti-virus and firewall software installed on your environment to protect your operations from security vulnerabilities, malicious hackers as well as adware / spyware to name but a few areas.

It is also important to consider the impact / overhead anti-virus applications have on your IT infrastructure at a resource level, for example CPU / RAM, as well as ensuring that any anti-virus application you use is tuned and optimised for your operating environment.

As part of this, many applications have specific requirements and recommendations around whitelisting and exclusions so as to avoid conflicts and compatibility issues between them. This helps mitigate impacts that can occur such as performance degradation, restricted access to critical application components that results in undesired operations, and false/positive antivirus detections.

Because of the transactional nature of StrataMax, and its underlying database engine – in this case Microsoft SQL Server / MySQL, there are a number of specific requirements to configure in order for each application component to function as desired.

Antivirus Exclusions

From an initial StrataMax perspective, this encompasses the following:

- Anti-virus software must be configured on all workstations that run StrataMax, as well as on the server, to ignore the StrataMax application network share while the software is in active use. This means that anti-virus software should not be scanning or checking these folders while users are using the product, or when nightly automated tasks such as building uploads or banking downloads are running. Uploads are normally scheduled to run overnight during weekdays and banking downloads usually run each morning.

- It is recommended that anti-virus scans do take place, but not during times when StrataMax is in operation. If you are concerned about finding a suitable regular slot for running your antivirus scanning, please liaise with StrataMax Support to confirm the StrataMax upload & download run times to avoid.

- The network folders listed below should be excluded from scanning by anti-virus software while StrataMax is in use during office hours. Exclusions must be defined on all servers and workstations that access these folders:

\\<SERVER>\<SHARE>\BCM (network folder)

\\<SERVER>\<SHARE>\GLMax (network folder)

C:\BCMax (if an Approval List of programs is not used as exclusion)

C:\Program Files\StrataMax\ (StrataMax Scheduler and Communications server/s)

C:\ProgramData\StrataMax\ (Scheduler batch tasks)

Firewall Configuration

Database ports for MSSQL / MySQL. Please consult with StrataMax support on this as depending on your configuration, this may utilise non-standard ports. Generally, however, for MSSQL this will be port “1433” and for MySQL, port “3306”.

It is not StrataMax policy to specifically recommend the use of a particular antivirus software product. All products are equally acceptable so long as they allow the software to function via the use of application and file/folder exceptions, and whitelisting StrataMax domains for file upload/download if the A/V software has that capability.

Database Server A/V Best Practices

Depending on the database engine you are using, there are various recommendations from these vendors to configure your anti-virus application to minimise performance impact, further information can be found here:

- Microsoft SQL Server: https://support.microsoft.com/en-us/topic/how-to-choose-antivirus-software-to-run-on-computers-that-are-running-sql-server-feda079b-3e24-186b-945a-3051f6f3a95b
- MySQL: https://dev.mysql.com/doc/refman/8.0/en/windows-installation.html

If you have any further queries, or would like to discuss further if you have any specific requirements, please contact the StrataMax Support team.