Practices in maintaining GuardPointPro Software

Any Access control system requires a level of maintenance to insure a system is running smoothly and consistently. The server PC and software can often be overlooked but this can be equally or if not more important than the access control boards.
The amount of care involved is really determined by how important the software is to the site in particular.

A very small site for example: 1 door with 10 cardholders where users are rarely added. The software in this case may not be required to run at all. Let's not forget that the controllers themselves will operate without the software running.
Even if the software was lost, it may be considered ok to simply setup the software again on a new PC.
A very large site with many doors and cardholders being added frequently would have a completely different perspective. At a site like this it may require the software running all the time to add delete cardholders and manage alarm events.
The typical tasks to consider for the smooth running of the system would be:

1.   Database Size in relation to PC performance. Can old events be archived?
2.   When using a SQL Database pls see our article:
       https://sensoraccess.zendesk.com/hc/en-us/articles/360001054111-GuardPoint-P
       This will cover things like:
       DB Backup - remote location + so important! To have a procedure in place of how to restore
       Rebuild indexes
       Update statistics
       Shrink DB
       Removing old events
       If you're not familiar with SQL administration it is worth finding someone who is
3.   Software updates we would always recommend checking for software updates on a yearly basis.
       https://sensoraccess.zendesk.com/hc/en-us/sections/360000238632-NEWS
4.   Check size of installation against recommended PC specifications.
       As a system grows so does the demand on the PC hardware
       https://sensoraccess.zendesk.com/hc/en-us/articles/360001055631-GuardPoint-Pro-Server-Specifications-PC-Requirements
5.   Check the AME log for Errors/DB errors. GuardPointPro has a running log which can be reviewed to see the running of the system. Any failures in the software will be shown in here.

6. GPP has a diagnostic window which will show communication status and pending events on the controller and also the controller firmware – this is the first place to check when reviewing the GuardPointPro system. (offline controllers do effect the overall performance of the software)
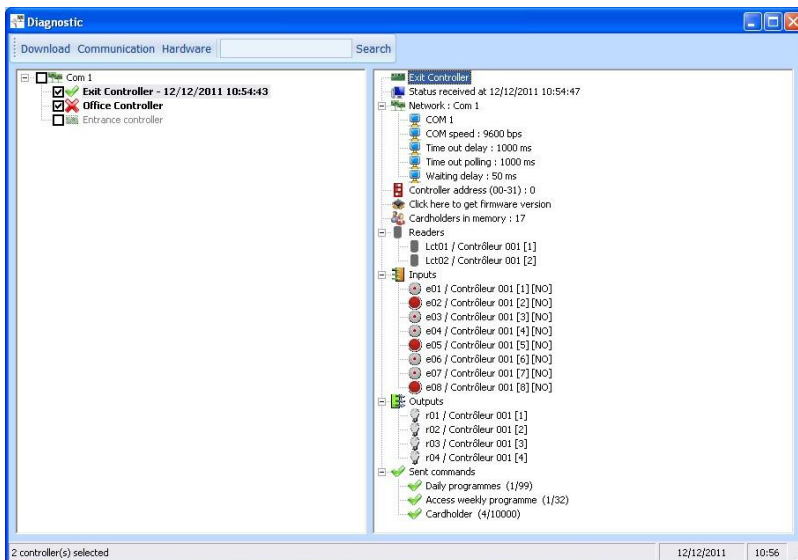
7. Check for controller firmware updates (newer firmware maybe have improvements which will also improve the way the software interacts with them)
   https://sensoraccess.zendesk.com/hc/en-us/articles/360001031112-IC-Controller-Firmware
8. Your standard PC hardware checks:
   -Check Disk Usage
   -Check Memory Usage
   -Check for hardware Errors - Windows event log
9. Check to see if Deleted cardholders and unused badges can be removed from the system
10. Check the windows event log for GPP application errors and potential PC Crashes
11. Windows updates
12. Make sure Windows Time synchronisation is working correctly
13. Backup! It is so important to back up the database and have a recovery plan in place
14. Test you disaster recovery plan and make sure people know what to do in a failure

Practices in maintaining GuardPointPro Software

Disaster recovery:

It is very important to have a disaster recovery process in place.
An assessment typically needs to be arranged between the company maintaining the system and the customer.
Questions need to be asked such as:

- What risks do you face if the GuardPointPro application where to fail for a day, a week, or longer?
- If the GuardPointPro Software is not running/working how quickly does it need to be back up and running?
- Who are the decision makers and who needs to be involved in the recovery process?
- What functions will be lost in the event of the software not running and are these critical?
- Is the expertise available to restore a system ie a failure on the weekend

Once the importance of software is determined a procedure can be decided upon and put into place and things like backup frequency and location and redundant servers can then be considered.
Also one must consider whether a non-production server should be used first for any windows/software updates to mitigate any unforeseen problems.