

Increasing Stability

Protection against reloading of GN server

End-users may try to run more copies of the protected application in the network than permitted. After running a maximally permitted number of copies, they may force reloading of Guardant Net server and get an opportunity to run just as many application copies again. It is quite easy to protect against this.

The protected network application should periodically verify the dongle's presence. Use timer-based dongle verification option during the automatic protection of the application and/or periodically poll the dongle with the API functions from different locations of the application.

The thing is that after being reloaded Guardant Net server will not process queries of those applications started before reloading. Thus, the first polling of the dongle carried out by an 'old' application copy after the server has been reloaded will return an error.

Optimizing Performance of Guardant Net Server

1. It is not recommended that you call the dongle too often. The point is that the minimum response time of Guardant Net is about 150-200 milliseconds. Thus, the server can exchange with Guardant Net no more than 5 to 6 times per second. Moreover, during the execution of Transform operation the time of exchange may even increase several times (Transform operation is quite slow). Therefore, for example, five applications, each calling the dongle once in a second, can easily overload Guardant Net server, because in this case little will depend on its speed. The server will start 'freezing' for a long time and lose network packets. Therefore, you should remember that the optimal interval between the polls should be random and range between 5 and 30 minutes. It is not recommended that you carry out many tests at one time, because in this case the possibility of peak overloads increases dramatically. If you follow these recommendations, the server will be able to poll up to 100 protected applications, which are running simultaneously. This number seems big enough, however it should be kept in mind that there has to be only one server in the network and that several dongles can be registered on it (each with its own network license limit). Network administrators should be warned against the risk of overloading the server.
2. It is not recommended that you enable the automatic start function for the protected network application, because in this case the risk of overloading is also very strong. For example, imagine how a new day begins in a big bank, where hundred of terminals are turned on at once, and all of them start to send their queries to the dongle almost simultaneously.
3. To avoid overloading it is not recommended that complicated checks on the dongle be carried out when loading the protected application. A simple check of the dongle's presence would be enough, while more complicated tests should be better postponed until a later stage, making them incidental and timed to certain events.
4. Do not assign too high values to configurable parameters in ini file of Guardant Net server. This will not lead to the effect you expect. Instead, the server will start to consume system resources (RAM and CPU usage) excessively. The default values of parameters appear to be optimal for the networks with little and medium number of workstations; there is sense in increasing them only when serious matters arise (for example, when the server has to work in large-scale networks with many dongles). If there is a shortage of resources specified by the configurable parameters, the server will inform of this by displaying a corresponding message on the screen.

Sharing dongle resource over network

1. When polling the dongle try not only binding it to its Private codes, but also do carry out a deeper check, involving general-purpose fields (serial number, version, etc.). This will guarantee that the protected application will only use the network licenses of the dongle to which it is bound. It is of importance when several dongles with your Private codes are registered on one server.
2. When hardware algorithms are used which depend on the decrementing value of their executions counter, there is a risk of this protected application copy receiving wrong responses from such algorithm, because only one counter is used in it for all copies of the protected application.