Recommended settings for best performance in GFI LanGuard

GFI LanGuard's remote communication needs and intensive resource access pattern make it a possible victim of third party software like anti-virus/anti-spyware solutions, intrusion prevention systems, or firewalls. Such problems can be avoided by following a few configuration guidelines as described below:

Real-time protection engines can severely diminish GFI LanGuard's scanning speed

- Disable the real-time anti-virus engine from scanning the following GFI LanGuard paths:

- GFI LanGuard 2011, 2012, or 2014:

Windows XP, Windows 2003:
<..\Program Files\GFI\.>
<..\Documents and settings\all users\application data\GFI>
Windows Vista, Windows Server 2008, Windows 7, Windows 2008 R2:
<..\Program Files\GFI\>
<..\ProgramData\GFI>
64 bit machines need to also include <..\Program Files (x86)\GFI>

- These same exclusions should be made on any machine that has an agent installed on it as well for the same reason, also to prevent the Anti-Virus from interfering with the httpd communication of the Apache process.

The firewall might slow down GFI LanGuard scanning or even block outbound connections to scanned computers

- Configure the firewall so that it allows the following GFI LanGuard components to freely open outbound connections:
  - <..\Program Files\GFI\LanGuard 11>\languard.exe
  - <..\Program Files\GFI\LanGuard 11 Agent>\Httpd\bin\httpd.exe
  - <..\Program Files\GFI\LanGuard 11 Agent>\lnsscomm.exe
  - <..\Program Files\GFI\LanGuard 11 Agent>\lnssatt.exe
  - <..\Program Files\GFI\LanGuard 11 Agent>\lnsscorollary.exe
  - <..\Program Files\GFI\LanGuard 11 Agent>\update.exe

- For best communication between agents and server open the following ports in the firewall (both TCP and UDP as well as inbound and outbound)
  - GFI LanGuard communication server (httpd.exe) port as configured in Agent Settings: (1070 by default)
  - SMB/RPC ports: 445,135,139, 9292

By default some firewall applications (like the Microsoft Windows inbuilt firewall) disable various ports and services. This can make the target computers totally un-discoverable, or negatively affect the scanning accuracy

- Make the following changes on the target computers firewall:
  1. Enable File and Printer Sharing
  2. Enable port 135 for message sending

3. Enable Windows Management Instrumentation (WMI) traffic
    - It should only be needed to enable the above types of traffic with the GFI LanGuard computer's IP address (most current firewall products allow for such granularity)
- See: What are the required settings to scan a machine and successfully install missing patches using GFI Languard
- http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx

The port scanning section of a GFI LanGuard scan is considerably slower when the scanned computer is firewalled. Also, UDP port scanning may not be reliable with some firewall solutions. GFI LanGuard will determine such cases and will report accordingly

- Only enable port scanning when needed and be prepared for doubled scan duration.
    - You can disable / enable port scanning from a Scanning Profile using the GFI LanGuard configuration. Further information can be found in the GFI LanGuard Manual (Section: Scanning Profiles > 'Configuring TCP port scanning options')

Some Systems might see the intensive port querying done by GFI LanGuard as a possible attack and may totally block communication with the GFI LanGuard computer's IP address for a period of time

- Disable the intrusion prevention engine on targets while scanning them with GFI LanGuard or disable port scanning in GFI LanGuard.
    - You can disable / enable port scanning from a Scanning Profile using the GFI LanGuard configuration. Further information can be found in the GFI LanGuard Manual (Section: Scanning Profiles > 'Configuring TCP port scanning options')

GFI LanGuard program updates will not work if the GFI LanGuard computer cannot access the GFI web servers

- Configure GFI LanGuard to download program updates from an alternative location.
    - Related: How to update GFI LanGuard if in a secure network

During security scanning, GFI LanGuard will check if the supported virus scanners or anti-spyware software definition files are up to date. This check will fail when the GFI LanGuard computer has no Internet access. Also, downloading Microsoft updates requires Internet access

- Temporarily allow Internet access if possible
    - Related: How to manually download a patch in GFI LanGuard

The GFI LanGuard database backend is growing to maximum capacity in a short period of time

- Use the Microsoft SQL database backend option in GFI LanGuard to store scan results (vs. the default Access option)
    - Access Databases have a limit of 2GB in size
    - If Microsoft SQL Server option is used, Microsoft SQL Server Express Editions may be used
        - SQL Server Express 2005 has a max database size of 4GB, where SQL Server Express 2008, R2 has a max database size of 10GB

Related Articles:

- For more information on communications used when scanning and deploying

with GFI LanGuard, refer to:Which settings are required to be able to scan a machine and successfully update missing patches using GFI LanGuard?