How to set up GFI LanGuard server

Best practices

GFI Software™

System requirements

Database backend

- You have an existing SQL Server that you want to use for LanGuard's database.

  - Before installing LanGuard you need to install the SQL Server Native client as a prerequisite so LanGuard can connect to the SQL Server and create the database.

- You have a SQL Server license and you will install it on the same server as LanGuard.

  - Install it before installing LanGuard. If you are using Windows Authentication, make sure that the account used for the installation is added as an administrator in SQL Server. As an alternative the SA account can be enabled.

- You don't have any database or anyone with SQL Server knowledge.

  - You can use SQL Server 2019 Express Edition, there is no license needed. It should be installed on the same server as LanGuard and the **Basic installation type** has all the needed requirements.

> **Reference knowledgebase article:** 🔗 GFI LanGuard System Requirements

Network and security permissions

- Communication between the LanGuard server and the target machines should be available. The following tests can be performed to make sure the requirements are in place:

  - Ping to the IP, HOSTNAME and FQDN (Fully qualified domain name).

  - Nslookup to the IP, HOSTNAME and FQDN.

- Antivirus and real time protection engines should be disabled before installing LanGuard. Afterward, the LanGuard paths on the server as well as agent machines, should be excluded from antivirus scanning.

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

- Make sure that the account being used for scanning and remediation is a local administrator on the remote computer. If no alternative credentials are used.

Reference knowledgebase articles:

🔗 Recommended Settings for Best Performance in GFI LanGuard

🔗 Verifying Required Network Connectivity and Security Permissions for GFI LanGuard Operations

🔗 Best Practices for Setting up Account Permissions with Alternative Credentials in LanGuard

Scanning

- After completing the installation of LanGuard, it will automatically start a scan on the local host. It is important that this scan finishes correctly as it will download the latest patch management database for the first time. Because of this, it is normal behavior if it takes +2 hours for the first scan.

- Network discovery method can be used to add machines to LanGuard or add them manually as needed.

- Full scan can be a heavy operation if done over the network. Recommended profiles to start testing during business hours are: missing patches, security patches, high security vulnerabilities, custom profile for Linux machines.

- Use agent scans over interactive scans whenever possible, to take advantage of the target machine's resources.

Reference knowledgebase articles:

🔗 Recommendations for Performing Scans over a Slow Network Connection

🔗 Creating a New Scanning Profile for Linux Machines To Avoid Being Stuck and Getting Timeouts / Irrelevant Errors During a Scan

Remediation

- Note that patch deployment is made directly from the LanGuard console to the target machines. The agent is not involved in this operation, therefore, the LanGuard server resources are consumed for this.

- In case agent deployment or patch management doesn't work, run an interactive scan as it can find some prerequisites that might be missing.

- Special requirements to pay attention for remediation operations and patch deployment:

    - Ping and nslookup to the HOSTNAME and FQDN should resolve to the correct IP.

- Ping and nslookup to the HOSTNAME and FQDN should resolve to the correct IP.

- The account used in the LanGuard services or the alternative credentials used, should have local administrator privileges on the machines that are being patched.

- There should be no restrictive GPOs that prevent installing patches on the target machines.

Reference knowledgebase articles:

🔗 Explaining LanGuard Patch Deployment Process

🔗 What are the Services Prerequisites, Settings, and Administrator Privileges Requirements to Scan a Machine, Deploy Agent and Install Missing Patches using GFI LanGuard

GFI Software™