Administrator's Guide

GFI LanGuard WAN Agent feature

GFI Software™

Table of contents

LanGuard WAN Agent

The WAN agent is a new feature that helps address the need of customers to scan remote users without the need to use a VPN. The WAN agent empowers customers to identify and address vulnerabilities across distributed infrastructures from a centralized interface. With its lightweight design and minimal footprint, the WAN Agent ensures minimal resource consumption, granting you the freedom to optimize your vulnerability assessment and patch management strategy.

How does it work?

The WAN agent is installed in each remote computer that needs to be remotely scanned and patched using the LanGuard console.

The WAN agent and the LanGuard console will communicate securely using AWS to send/receive the commands for scanning and patching.

Enabling the WAN Agent feature

Prerequisites

All the needed installers and prerequisite files (referenced in the next sections) are present in this GDrive folder.

Besides that, you would also need the below information to *use* the WAN Agent for your installation - it would be provided to you by GFI.

a. Provisioning claim certificate
b. Private key for certificate
c. Certificate ID
d. Tenant ID
e. LanGuard server WAN name
f. LanGuard server certificate
g. LanGuard server private key

Steps to enable WAN feature

Firstly, Install or Upgrade GFI LanGuard to the version supporting the WAN feature.

1. Open the LanGuard console, and go to **Configuration > Agents management > WAN Agents settings**.
2. In the dialog's 6 input fields, you specify the data and files provided by the GFI Admin.
3. You can limit the bandwidth the WAN agents will take when downloading patches by checking "Enable download bandwidth limit" and setting the MB/sec you want.
4. Once filled in all the details, click on **"Generate WAN Agent Installer"** to generate the WAN Agent installer MSI file. **Note down the location of the generated files.**
    a. It takes a couple of seconds to generate the installer file.
5. Finally, click Apply.

Install the Agent on remote machine

1. Download **VC_redist.x86.exe** and install it. Cancel the installation if the installer notifies you the machine has already had the distribution.
2. Download **tls12.ps1** and unblock it. Run it in a Powershell editor in administrator mode. Reboot the system before proceeding.
    a. If you get an error message stating that the script cannot be loaded because script execution is disabled, run the following command:
    Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
3. Run "**MsiExec.exe /X{160301DE-306A-4ADE-8A47-BC5790AF0486}**" to uninstall any past installations.
4. Download **LanGuardWANAgent.msi** generated via step 4 of server installation, right-click it, and run it as an administrator on the remote machine:
    a. If you install it without Admin rights, start the agent manually after installation (you just need to do it once). You can check it by running "services.msc" in the command prompt and searching for the service "GFI LanGuard 12 Attendant Service".
5. Once the installation finishes, a new node for this agent will show up under "Remote Devices" in the computer tree of the LanGuard server dashboard, with the machine's name of the target.

Important: When the installer finishes, please verify under Services if the GFI Attendant service is running.

Run a scan

Once the agent is installed it will appear automatically in the LanGuard console under "Remote devices". To start a scan select the newly added machine and follow the next steps:

1. Right click on the machine and go to Scan > Custom Scan. Alternatively you can choose a group of computers that have the agent deployed.
2. Choose the scanning profile that will be used to collect information.
3. Click on “Scan”
4. The scan will be initiated but no input will be received on the console as the scan is running directly on the target machine.

Monitor the scan operation

To monitor the scan operation you can go to the Activity Monitor > Security Scans.