Administrator's Guide

GFI LanGuard WAN Agent feature

GFI Software™

Table of contents

LanGuard WAN Agent **3**

How does it work? 3

Enabling the WAN Agent feature 3

Prerequisites 3

Tenant information 4

Server installation / Upgrade 4

Enabling WAN Agent Capability on the server 4

Agent installation 5

Run a scan 6

Monitor the scan operation 6

Appendix **7**

WAN Agent communication protocols 7

Wan Agent scan timeout FAQs 8

Last modification date: 12/26/2024

LanGuard WAN Agent

The WAN agent is a new feature that helps customers scan remote users without using a VPN. It 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, allowing you 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. The ports used by the WAN Agent are 443, 8443, and 8883

Enabling the WAN Agent feature

Prerequisites

You need the information below to *use* the WAN Agent. If you already have an existing LanGuard deployment, please contact Customer Care to receive the needed information.

Tenant information

a. **Provisioning claim certificate** (file): companyname_cert.pem
b. **Private key for the certificate** (file): compan_private_key.pem
c. **Certificate ID** (string): 1aaf76we24ff9933g5509q34q347d2h4sg528249dd3e5745f0d13b6513b4115d
d. **Tenant ID** (string): companyname
e. **LanGuard server WAN name** (string): companyname-8182e550-7186-4cf7-8156-1a5a7f09f123
f. **LanGuard server certificate** (file): companyname-8182e550-7186-4cf7-8156-1a5a7f09f123_cert.pem
g. **LanGuard server private key** (file): companyname-8182e550-7186-4cf7-8156-1a5a7f09f123_private_key.pem

***Note**: The above are just sample values. They are not meant to be used for configuring the WAN agent feature.*

- Outbound communication should be allowed from ports 443, 8443, and 8883 on the target machines where the WAN Agent is installed.
- Download the installers referenced in this document from the prerequisite files folder.

Server installation / Upgrade

1. Download and install the Microsoft Visual C++ Redistributable on the server where LanGuard is or will be installed. If the installer informs you that the required version is already installed on the machine, you can skip this step.
2. Install or Upgrade GFI LanGuard to the version supporting the WAN feature.
3. Unblock tls12.ps1 and run it in Powershell in administrator mode Note: 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**
4. Reboot the system

Enabling WAN Agent Capability on the server

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 tenant information and files provided by GFI.
3. You can configure the WAN agent offline timeout (in hours), which defines how long the LanGuard console will wait for a WAN agent to be offline before it is considered inactive and removes itself from the target computer. "Offline" means there has been no communication between the WAN agent and the LanGuard console, which could occur if the target computer lacks internet access or has been decommissioned.
4. You can also limit the bandwidth the WAN agents will take when downloading patches by checking "Enable download bandwidth limit" and setting the MB/sec you want.
5. 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. (**It takes a couple of seconds to generate the installer file)
6. Finally, click **Apply**.

Agent installation

Follow these steps to install the agent in the target machines that will be scanned and patched remotely by LanGuard:

1. Download and install the Microsoft Visual C++ Redistributable. If the installer informs you that the required version is already installed on the machine, you can skip this step.

2. Unblock tls12.ps1 and run it in Powershell in administrator mode Note: 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. Reboot the system
4. If you have had previous LanGuard agents running, you can run the command "**MsiExec.exe /X{160301DE-306A-4ADE-8A47-BC5790AF0486}**" to uninstall any prior installations.
5. Download **LanGuardWANAgent.msi** generated on step 5 of Enabling WAN Agent capability, right-click it, and run it as an administrator on the remote machine:
    a. If you install it without admin rights, you will need to manually start the agent after the installation (this only needs to be done once). You can verify this by running "services.msc" in the command prompt and looking for the service named "GFI LanGuard 12 Attendant Service."
6. Once the installation finishes and the connection is established successfully, 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.

Appendix

WAN Agent communication protocols

For the WAN Agent feature, messages are exchanged between the WAN Agents and the GFI LanGuard console. These messages are classified into several distinct categories:

- **1XX (Agent to Server)**: These are specific, targeted messages initiated by the agent to communicate its status, perform actions like changing network modes (WAN/LAN), initiate scans, or send updates. Examples include:
    - **AgentInstalled** (100): Notifies the server that an agent has been installed.
    - **AgentSwitchToWAN** (101): Informs the server that the agent is switching to WAN mode.
    - **AgentScanStart** (110): The agent informs the server that it has started a scan.
- **2XX (Broadcast by Agent):** Broadcast messages initiated by agents.
- **3XX (Agent Acknowledgements)**: These are acknowledgement (ACK) messages sent by agents to confirm receipt or successful execution of requests initiated by the server. For example:
    - **AgentScanRequest_ACK** (300): Acknowledges the server's scan request.

    - **AgentUpdateRequest_ACK** (303): Acknowledges the server's request to update the agent.
- **4XX (Agent Error Messages)**: These messages indicate errors that occurred during actions initiated by the agent. Examples include:
    - **AgentDeployPatchAgentRequest_ERR** (401): Indicates an error occurred while the agent was trying to deploy a patch.
    - **AgentUpdateRequest_ERR** (403): Signals an issue with the agent update process.
- **5XX (Server to Agent Requests)**: These are direct messages from the server to the agent, requesting specific actions. For example:
    - **ServerRequestScan** (500): Requests that the agent start a scan.
    - **ServerRequestDeployPatchAgent** (501): Requests the agent to deploy a patch.
- **6XX (Broadcast by Server)**: These would be broadcast messages initiated by the server.
- **7XX (Server Acknowledgements)**: These are acknowledgement messages sent by the server in response to agent actions. For example:
    - **ServerAgentInstalled_ACK** (700): Confirms that the server acknowledges the agent installation.
    - **ServerScanStart_ACK** (710): Acknowledges the agent's notification of scan start.
- **8XX (Server Error Messages)**: These messages indicate errors that occurred during server-initiated actions or in response to agent actions. For instance:
    - **ServerAgentInstalled_ERR** (800): Indicates an issue with the server's handling of an agent installation.
    - **ServerScanFinished_ERR** (812): Indicates an error occurred when the scan finished.

In summary, the system facilitates a structured communication protocol where the WAN agents report status, perform actions, and respond to GFI LanGuard server requests. The

GFI LanGuard servers can issue commands to agents, which are acknowledged or may trigger error responses based on success or failure.

Wan Agent scan timeout FAQs

- How does the counter for the WAN agent offline timeout function?

The WAN agent scan timeout setting controls how long remote network scans can run before timing out. This setting is managed centrally on the LanGuard server and ensures that WAN agent scans don't run indefinitely by enforcing a maximum duration limit.

- After the timeout, does the absence of connection continue?

Once the timeout expires, the LanGuard server cancels its tracking of the scan job. However, the WAN agent continues scanning independently. If the scan completes, the WAN agent will send the results back to the server, which will process and update them despite having canceled the job.

- After a timeout, when and how is the agent restarted?

The scan timeout only affects job tracking on the server side, not the WAN agent. The WAN agent continues running normally and will not restart due to this timeout.

- Who is counting the time? The Agent, Relay, or Server?

The LanGuard server tracks and enforces the timeout, maintaining the timer for how long each WAN agent scan runs.

- Who decides when the time is fulfilled? The Server, Agent, or Relay?

The LanGuard server decides and controls the timeout period for each WAN agent scan job.