

## INLEIDING

Welkom bij GFI LANguard: Uw alles-in-een oplossing voor patchmanagement, kwetsbaarheid scannen en netwerkcontroles. GFI LANguard (of "LANguard") scant uw netwerk en poorten om beveiligingslekken te detecteren, onderzoeken en verhelpen met minimale administratieve handelingen.

**Deze handleiding is ontworpen om u een overzicht te geven van wat LANguard is, wat het doet, hoe u snel en effectief de krachtige functies van LANguard kunt gebruiken, en assisteert bij het succesvol in gebruik nemen.**

Deze handleiding biedt u:

1. Een **overzicht** van wat LANguard voor uw bedrijf kan betekenen
2. **Zes (6) belangrijke onderwerpen** om rekening mee te houden voordat u LANguard gaat gebruiken
3. **Hoe u computers veilig en bijgewerkt kunt houden** om het beste uit LANguard te halen

Voor meer gedetailleerde documentatie kunt u verder nog het volgende lezen:

1. GFI LANguard veel gestelde vragen (FAQ) – <http://kbase.gfi.com/showarticle.asp?id=KBID001966>
2. GFI's Knowledge Base – <http://kbase.gfi.com>
3. GFI LANguard documentatie – <http://www.gfi.nl/lannetscan/manual>

Als u na het lezen van deze SmartGuide nog vragen hebt, zijn we beschikbaar om u te helpen. Neem daarvoor **hier** contact met ons op.

## Overzicht GFI LANguard

Allereerst een korte uitleg over wat GFI LANguard doet. Simpel gezegd, met de resultaten van de drie (3) steunpilaren voor kwetsbaarheidbeheer: **patchmanagement**, **kwetsbaarheidcontroles** en **netwerkcontroles**, kan LANguard uw netwerk **scannen, analyseren en herstellen**.

LANguard **scant** uw netwerk hetzij handmatig of op basis van een tijdschema naar beveiligingsgerelateerde zaken en verzamelt relevante gegevens over de beveiliging. Bijvoorbeeld het verzamelen van informatie over beveiligingskwetsbaarheden, ontbrekende patches, open poorten, open bestandsdeling, gebruikers en groepen, geïnstalleerde applicaties, hardwareoverzicht, enzovoorts.

Met de resultaten van de scans kunt u vervolgens de status van uw netwerk **analyseren**. GFI LANguard biedt tools om door de scanresultaten te bladeren en deze te onderzoeken. Aan iedere gescande computer wordt een kwetsbaarheidscijfer toegekend op basis van de problemen die tijdens de controle zijn gevonden, en daarbij worden tevens rapporten en resultaatvergelijkingen geleverd. Voorbeelden van deze scans en rapporten zijn te vinden in **voorbeeld A**.

Met deze scan en analyse helpt GFI LANguard u bij het **herstellen** van de beveiligingsproblemen en waar mogelijk bij het automatiseren van het proces.

Nadat er een eerste basisscan is gemaakt, kunt u de verschillen of wijzigingen in de beveiliging en de computerconfiguraties van alle computers in een netwerk bepalen. Vervolgens kunt u beslissen welke acties te ondernemen zoals het installeren van ontbrekende Microsoft beveiligingspatches en service packs, Microsoft updates terugdraaien, maatwerk software en scripts installeren, ongeautoriseerde programma's verwijderen, extern bureaublad-verbindingen maken met gescande computers, enzovoort. Al deze acties zorgen ervoor dat uw systemen zijn bijgewerkt en dat de nieuwste beveiligingspatches zijn geïnstalleerd.

Onze ervaring leert dat klanten een licentie van GFI LANguard nemen om het volgende te bereiken:

### **PATCHMANAGEMENT**

- Ontbrekende patches detecteren en installeren

### **KWETSBAARHEID SCANNEN**

- Scannen van Windows besturingssysteem of programma's
- Identificeren en sluiten van openstaande bestandsdelingen, poorten, enzovoorts.

### **NETWERKCONTROLE**

- Monitoren netwerkgezondheid
- Netwerkcontrole
- Identificeren welke pc's welke software hebben
- Wijzigingsbeheer – wanneer er wijzigingen zijn
- Apparaten identificeren op een netwerk

## **ZES BELANGRIJKE ONDERWERPEN TER OVERWEGING VOORDAT U GFI LANGUARD GAAT INSTALLEREN**

Er zijn zes (6) zaken waar u rekening mee dient te houden voordat u GFI LANguard gaat installeren. Het is belangrijk dat u ze allemaal begrijpt, dus als u na het lezen van onderstaand gedeelte nog vragen heeft, of ze met ons wilt bespreken, neem dan **contact** met ons op.

1. **Licentie**
2. **Systeeminstallatievereisten**
3. **Profielen scannen – wat dient u te weten**
4. **De juiste database kiezen**
5. **Tips over scannen en prestaties**
6. **GFI LANguard filters en/of rapportage**

### **1. LICENTIE**

De licentie van GFI LANguard is gebaseerd op het aantal actieve\* ("Actieve") IP-adressen dat u scant. Bijvoorbeeld:

1. Wanneer u een IP-reeks hebt van 192.160.1.1 tot en met 192.160.1.254.
2. En u hebt 20 actieve IP-adressen in dit bereik die u wilt scannen, hoeft u alleen een licentie te hebben voor deze 20 actieve IP-adressen.
3. Het is echter belangrijk te weten dat wanneer er meer dan 20 actieve IP-adressen in het bereik zitten, EN u hebt een licentie voor maar 20 IP-adressen in GFI LANguard, dan zullen alleen de eerste 20 actieve IP-adressen worden gescand (daarom zullen actieve IP-adressen na de eerste 20 niet worden gescand).

\* Een "actieve" IP is gedefinieerd als een IP-adres dat te benaderen en beschikbaar is middels een verbindingsverzoek verzonden in de vorm van NETBIOS-queries, SNMP-queries en/of ICMP pingverzoeken.

### **2. SYSTEEMINSTALLATIEVEREISTEN**

#### **Systeemvereisten: Hardware**

Hardwarevereisten zijn afhankelijk van de grootte van het netwerk. Raadpleeg onderstaande tabel voor de aanbevolen minimale specificaties voor uw netwerk grootte.

	1 tot 10 scandoelen	10 tot 500 scandoelen	500 tot 1500 scandoelen
Processor	1 GB	2 GHz	2 x 3 GHz Quad Core
Fysieke opslag	1 GB	2 GB	10 GB
Geheugen	1 GB	2 GB	4 GB
Gebruik netwerkbandbreedte	256 Kbps	256 Kbps tot 550 Kbps	256 Kbps tot 550 Kbps

### **Systeemvereisten: Software**

#### **Ondersteunde besturingssystemen (x86 of x64)**

- Microsoft Windows Server 2008 Standard/Enterprise
- Microsoft Windows Server 2003 Standard/Enterprise
- Microsoft Windows 2000 Professional/Server/Advanced Server (SP4 of hoger)
- Microsoft Windows 7 Ultimate
- Microsoft Windows Vista Business/Enterprise/Ultimate
- Microsoft Windows XP Professional (SP2 of hoger)
- Microsoft Small Business Server 2008 Standard
- Microsoft Small Business Server 2003 (SP1)
- Microsoft Small Business Server 2000 (SP2)

#### **Ondersteunde databases**

- Microsoft Access
- Microsoft SQL Server 2000 of recenter
- MSDE/SQL Server Express Edition

#### **Overige serveronderdelen**

De volgende onderdelen dienen op de server te zijn geïnstalleerd waar ook GFI LANguard is geïnstalleerd:

- Microsoft .NET Framework 2.0

#### **Onderdelen op doelcomputer**

De volgende onderdelen dienen op een doelcomputer te zijn geïnstalleerd zodat GFI LANguard ze kan scannen:

- Windows Management Instrumentation (WMI) – nodig om op Windows-gebaseerde scandoelen te kunnen scannen. Meegeleverd met alle besturingssystemen vanaf Windows 2000 en recenter (kenmerkend voor Windows omgevingen).
- Secure Shell (SSH) – nodig voor op UNIX gebaseerde scandoelen. Gewoonlijk meegeleverd bij alle grote Unix/Linux distributies.
- SAMBA (SMB) server – nodig voor op UNIX gebaseerde scandoelen. Gewoonlijk meegeleverd bij alle grote Unix/Linux distributies.

### **3. SCANPROFIELEN – WAT DIENT U TE WETEN**

LANguard wordt standaard geleverd met een uitgebreide lijst scanprofielen\*. Een lijst met beschikbare scanprofielen is beschikbaar op: <http://support.gfi.com/manuals/en/lanscan9/lanscan9manual.1.43.html>

Op het hoogste niveau, zijn er 3 standaard profielen:

1. Volledige/combinatie scans
2. Kwetsbaarheidbeoordelingscans
3. Netwerk- en softwarecontrole scans

\*Scanprofiel: een scanprofiel bestaat uit een set met criteria die wordt gebruikt om de scan te definiëren. LANguard heeft meerdere vooraf gedefinieerde profielen die u kunt aanpassen en u kunt ook uw eigen scanprofielen creëren/aanpassen.

#### 4. DE JUISTE DATABASE KIEZEN


Telkens wanneer een scan is uitgevoerd, worden de resultaten opgeslagen in een database. Er zijn drie (3) Microsoft databases die u kunt gebruiken. De keuze voor een database hangt af van de grootte van het gescande netwerk, de frequentie waarmee wordt gescand en het soort scans (bijvoorbeeld volledig, gedeeltelijk, enzovoorts) dat u uitvoert:

- Microsoft Access (LANguard wordt geleverd met Microsoft Access database maar het is niet nodig dat u hiervoor Access hebt geïnstalleerd)
- Microsoft SQL Express
- Microsoft SQL Server

Wanneer u Microsoft SQL server overweegt als voorkeursdatabase maar u weet niet zeker wat de licentie-eisen zijn, raadpleeg dan onderstaande links naar informatiepagina's over Microsoft SQL-licenties.

[SQL 2008](#), [SQL 2005](#), [SQL Express 2008](#)

 **Het is altijd raadzaam uw Microsoft partner te raadplegen voor advies.**

 De standaard Microsoft Access database voor scanresultaten die met GFI LANguard wordt meegeleverd, is niet toereikend voor grote netwerken. Het wordt sterk aangeraden om over te schakelen naar een Microsoft SQL server database voor netwerken met meer dan 250 actieve IP-adressen wanneer het IP-adres een computer is. (Een computerscan biedt meer informatie, dan alleen aangeven dat het een printer is).

\* **OPMERKING:** GFI levert geen Microsoft-licentie en is ook geen vertegenwoordiger van enig product daarvan. We weten ook niet alles over uw interne systemen, applicaties en data. De inhoud van deze SmartGuide is bedoeld om u enige suggesties te geven over zaken die u ter overweging kunt nemen bij het kiezen van een database en hardwarevereisten bij het implementeren van GFI LANguard. Ze worden uitdrukkelijk alleen als leidraad vermeld.

#### 5. TIPS OVER SCANNEN EN PRESTATIES

Hier volgen enige suggesties die zorgen voor betere scans.

- Mocht u bezorgd zijn over de belasting van uw netwerkbandbreedte, zoals een trager netwerk, kunt u wellicht het profiel Complete/combinatie scans (volledige scan (trage netwerken)) raadplegen in hoofdstuk 7 LANguard scanprofielen die u [hier](#) kunt vinden.
- Wanneer u er voor kiest om een volledige netwerkscan uit te voeren: hoe groter en complexer uw netwerk, des te langer zal de scan duren. De standaardinstelling van LANguard is dat u drie (3) IP-adressen tegelijkertijd kunt scannen. Om de benodigde tijd voor het scannen van uw netwerk te verminderen, kunt u de standaardinstelling wijzigen naar 10 (tien) IP-adressen tegelijkertijd. **BEDENK** echter dat u met de gewonnen tijd ook meer netwerkbronnen zult gebruiken.

Raadpleeg [Aanbevelingen voor het scannen van grote netwerken met GFI LANguard](#) voor meer details.

- Een volledige scan kan tijdrovend zijn. Dus voordat u er een gaat uitvoeren raden we aan een representatief gedeelte van uw netwerk op te zoeken en een testscan uit te voeren om er zeker van te zijn dat uw omgeving correct is geconfigureerd. Bijvoorbeeld een kleine testscan zal snel fouten laten zien die u eerst wilt herstellen voordat u alle actieve IP-adressen in uw netwerk gaat scannen. Bijvoorbeeld geen verbinding kunnen maken met WMI of het externe register.
- Wanneer u het netwerk scant, kunnen er problemen voordoen met uw beveiligingssoftware (zoals anti-virus). Dergelijke problemen zijn te voorkomen door een aantal configuratierichtlijnen aan te houden. Raadpleeg hiervoor <http://kbase.gfi.com/showarticle.asp?id=KBID002344>
- Standaard zullen sommige firewallprogramma's (zoals de ingebouwde firewall van Windows XP Service Pack 2) verscheidene poorten en services uitschakelen. Hierdoor kunnen doelcomputers in zijn geheel niet getraceerd worden, of de scanprecisie negatief beïnvloeden.

Breng de volgende wijzigingen aan in de firewall van de doelcomputers. Wanneer u dit doet hoeft u alleen het IP-adres van de computer waarop LANguard is geïnstalleerd op te geven

- Bestands- en printerdeling inschakelen
- Poort 135 inschakelen om het versturen van berichten mogelijk te maken
- Windows Management Instrumentation (WMI) inschakelen

- 💡 Het wordt aanbevolen niet meer dan 2000 IP-adressen in een enkele scan uit te voeren. Dit is geen beperking van GFI LANguard, maar wordt aanbevolen om de scantijd beperkt te houden.
- 💡 Zorg ervoor dat u een scanprofiel gebruikt dat alleen de handelingen uitvoert die u nodig hebt (bijvoorbeeld niet het profiel "Volledige scan" gebruiken om alleen te zoeken naar open bestandsdelingen; poort scannen is zeer tijdrovend dus overweeg dit als een aparte scan uit te voeren).
- 💡 Wanneer u IP-reeksen scant, kunt u het beste een controle uitvoeren op bepaalde apparaten zoals printers, IP-telefoons, enzovoorts en deze verwijderen uit de te scannen lijst.

Heeft u verder vragen over het scannen of prestatieproblemen, neem dan [hier](#) contact op. Voor extra technische artikelen, klik [hier](#).

## 6. GFI LANGUARD FILTERS EN/OF RAPPORTAGE

GFI LANguard is een krachtige tool waarmee u uw netwerk kunt scannen, analyseren en herstellen. De informatie geboden door LANguard stelt u in staat om effectief patchmanagement, kwetsbaarheidscans en netwerkcontroles uit te voeren. Het verkrijgen van gegevens is slechts de helft van het resultaat dat u krijgt met LANguard. Er zijn twee (2) verschillende methodes om de resultaten van uw scans samen te vatten: Resultaten filteren en het GFI LANguard ReportPack.

- **Resultaten filteren:** met de LANguard interface kunt u uw eigen filter creëren (bijv. direct, snel, eenvoudig rapport). Scanresultaten bieden gewoonlijk veel informatie en het filteren van resultaten wordt gebruikt wanneer u specifieke informatie wilt voor een bepaald doel, zoals identificeren welke patches er ontbreken in uw systeem. Het filteren van resultaten is mogelijk met een recente scan of een die u uit de database hebt geladen.

Om een nieuw filter met resultaten te creëren, volg dan de stappen zoals [hier](#) beschreven.

- **GFI LANguard ReportPack:** is onderdeel van het product (als aparte download [hier](#) te verkrijgen), en is een eenvoudig te gebruiken rapportageprogramma [GFI LANguard ReportPack](#). De rapporten die in ReportPack beschikbaar zijn, zijn zo ontworpen dat ze voldoen aan de behoeftes van de organisatie: zowel grafische weergaven op hoog niveau voor management (bijv. trendrapporten) tot gedetailleerde rapporten en scans (zoals dagelijkse doorklikrapporten) nodig om te voldoen aan de behoeftes van de technische staf. Voor management is een afbeelding vaak sterker dan 1000 woorden.

Soort rapporten die met LANguard ReportPack zijn te maken:

- **Rapporten voor beheerder:** overzicht- en trendanalyses in de vorm van grafische rapporten. Voorbeelden van rapporten voor de beheerder: [samenvatting van kwetsbaarheden op het netwerk](#) en [trends in kwetsbaarheden op het netwerk](#).
- **Statistische rapporten:** informatie over besturingssysteem en de distributie van kwetsbaarheden over het gehele netwerk. Voorbeelden van statistische rapporten: [service pack-distributie per besturingssysteem](#), [distributie van kwetsbaarheden per host](#) en [distributie van kwetsbaarheden per besturingssysteem](#).
- **Technische rapporten:** technische informatie over kwetsbaarheden, ontbrekende patches en trojans. Voorbeelden van technische rapporten: [Geïnstalleerde patches per Host](#), [Ontbrekende patches per besturingssysteem](#), [Open trojanpoorten per host](#) en [Kwetsbaarheden per host](#).
- Top 20-rapporten: de top 20 van meeste kwetsbare hosts op basis van open poorten, ontbrekende patches of trojans. Voorbeelden van top 20-rapporten: [Open trojanpoorten](#), [Kwetsbare hosts op basis van ontbrekende patches](#) en [Kwetsbare hosts op basis van open poorten](#).

## **BELANGRIJK: Voer de volgende procedure uit om GFI ReportPack te installeren**

1. Installeer GFI LANguard
2. De standaarddatabase is Microsoft Access (vooraf geconfigureerd). Kiest u voor Microsoft SQL als database, dan dient u SQL te hebben geïnstalleerd en uw database-instelling te wijzigen om Microsoft SQL te gebruiken
3. Installeer tenslotte ReportPack. (OPMERKING: wanneer u ReportPack installeert, is er een onderdeel genaamd "GFI ReportCenter" dat eerst wordt geïnstalleerd en daarna wordt het GFI LANguard ReportPack geïnstalleerd. Het GFI ReportCenter is een regulier onderdeel dat door alle GFI ReportPacks wordt gebruikt).

De volledige documentatie over het GFI LANguard ReportPack vindt u [hier](#).

## **Uw computer veilig en bijgewerkt houden**

U hebt LANguard geïnstalleerd, de database geconfigureerd en het ReportPack geïnstalleerd. Daarna hebt u enige scans uitgevoerd en wellicht enige beveiligingsproblemen gevonden. Het doel van dit hoofdstuk is om richtlijnen te geven over hoe u kunt omgaan met sommige algemene beveiligingsproblemen. De drie (3) hoofdonderwerpen die we zullen beschrijven zijn: LANguard bijgewerkt houden, het identificeren en herstellen van Microsoft patches/service packs en het identificeren van overige netwerkkwetsbaarheden.

### **1. LANguard bijgewerkt houden**

- Zorg ervoor dat de machine waarop LANguard is geïnstalleerd toegang heeft tot het Internet.\* LANguard controleert dagelijks op nieuwe informatie over kwetsbaarheden en patches. Beveiligingskwetsbaarheden worden dagelijks ontdekt, we raden daarom aan om uw netwerk regelmatig te scannen.
- Als er een proxy server wordt gebruikt, kan deze worden ingesteld in GFI LANguard interface > hoofdmenu > configuratie > proxy-instellingen [EN: user interface > main menu > Configure > Proxy Settings].

**\*Als er geen Internettoegang beschikbaar is op de machine waarop GFI LANguard is geïnstalleerd, kunt u het programma configureren om updates te ontvangen via een alternatieve locatie. Meer informatie hierover vindt u [hier](#).**

### **2. Microsoft patches/service packs identificeren en herstellen**

Veel beveiligingskwetsbaarheden kunnen worden opgelost door ervoor te zorgen dat alle beveiligingspatches en service packs op iedere machine zijn bijgewerkt. Het eerste dat u daarom dient te doen is uw netwerk scannen naar ontbrekende patches (raadpleeg [hier](#) het scanprofiel "Ontbrekende patches" in hoofdstuk 7 van de GFI LANguard handleiding). Nadat u het netwerk hebt gescand naar ontbrekende patches/service packs met GFI LANguard, kunt u vervolgens deze ontbrekende patches/service packs op de doelmachines installeren.

-  **Het is raadzaam eerst de service packs te installeren**
-  **Nadat de service packs zijn geïnstalleerd raden we aan het netwerk opnieuw te scannen (waardoor u een bijgewerkt overzicht krijgt van de status van ontbrekende patches van uw netwerk)**
-  **Als er geen service packs beschikbaar zijn nadat u opnieuw hebt gescand, kunt u de ontbrekende patches installeren**
-  **Als Internetbandbreedte of schijfruimte een probleem is**
  - GFI LANguard kan gebruikmaken van de opslagruimte van een WSUS-server in het netwerk. Hiermee maakt u gebruik van de patches en service packs die al door WSUS zijn gedownload en bespaart daarmee ruimte en bandbreedte. Meer details vindt u [hier](#).
  - Als er geen WSUS-server beschikbaar is, kunt u het downloaden van patches/service packs door LANguard plannen tijdens daluren.
-  **LANguard kan ook automatisch patches/service packs herstellen indien ze vooraf door de administrator zijn goedgekeurd.**

### 3. Identificeren en herstellen van overige netwerkkwetsbaarheden

Zodra de computers zijn bijgewerkt (patched), raden we aan om een scan uit te voeren voor overige kwetsbaarheden of mogelijke beveiligingsproblemen.

- De resultaten uit de scan bieden de mogelijkheid gedetailleerde informatie te krijgen over bepaalde kwetsbaarheden.
- LANGuard wordt geleverd met tools waarmee u kwetsbaarheden kunt aanpakken door op afstand (ongeautoriseerde) software te verwijderen, of maatwerk software en script te installeren, of extern bureaublad-verbindingen te maken met computers, enzovoorts.