GFI LanGuard™

ADMINISTRATOR GUIDE

Find out how to configure GFI LanGuard in different environments and how to set up advanced features.

Document Version: 12.3

Last updated (month/day/year): 01/30/2018

Contents

1 Introduction

GFI LanGuard is a patch management and network auditing solution that enables you to easily manage and maintain end-point protection across devices within your LAN. It acts as a virtual security consultant that offers Patch Management, Vulnerability Assessment and Network Auditing support for Windows® Linux and MAC computers as well as mobile devices. GFI LanGuard achieves LAN protection through:

» Identification of system and network weaknesses via a comprehensive vulnerability checks database. This includes tests based on OVAL, CVE and SANS Top 20 vulnerability assessment guidelines

» Auditing of all hardware and software assets on your network, enabling you to create a detailed inventory of assets. This goes as far as enumerating installed applications as well as devices connected on your network

» Automatic download and remote installation of service packs and patches for Microsoft® Windows, Linux and MAC operating systems as well as third party products

» Automatic uninstallation of unauthorized software.

1.1 How GFI LanGuard works

Use GFI LanGuard to scan, analyze and remediate the health of your network devices. Install GFI LanGuard on a server within your network to:

SCAN
Scan network devices to detect vulnerabilities, missing patches, open ports, running services and more.

ANALYZE
View the network security status and analyze network security trends in the graphical dashboard and by generating reports.

REMEDIATE
Install missing updates, uninstall unauthorized applications, execute scripts, open remote desktop connections and run other tasks to maintain the health of your network and devices connected to it.

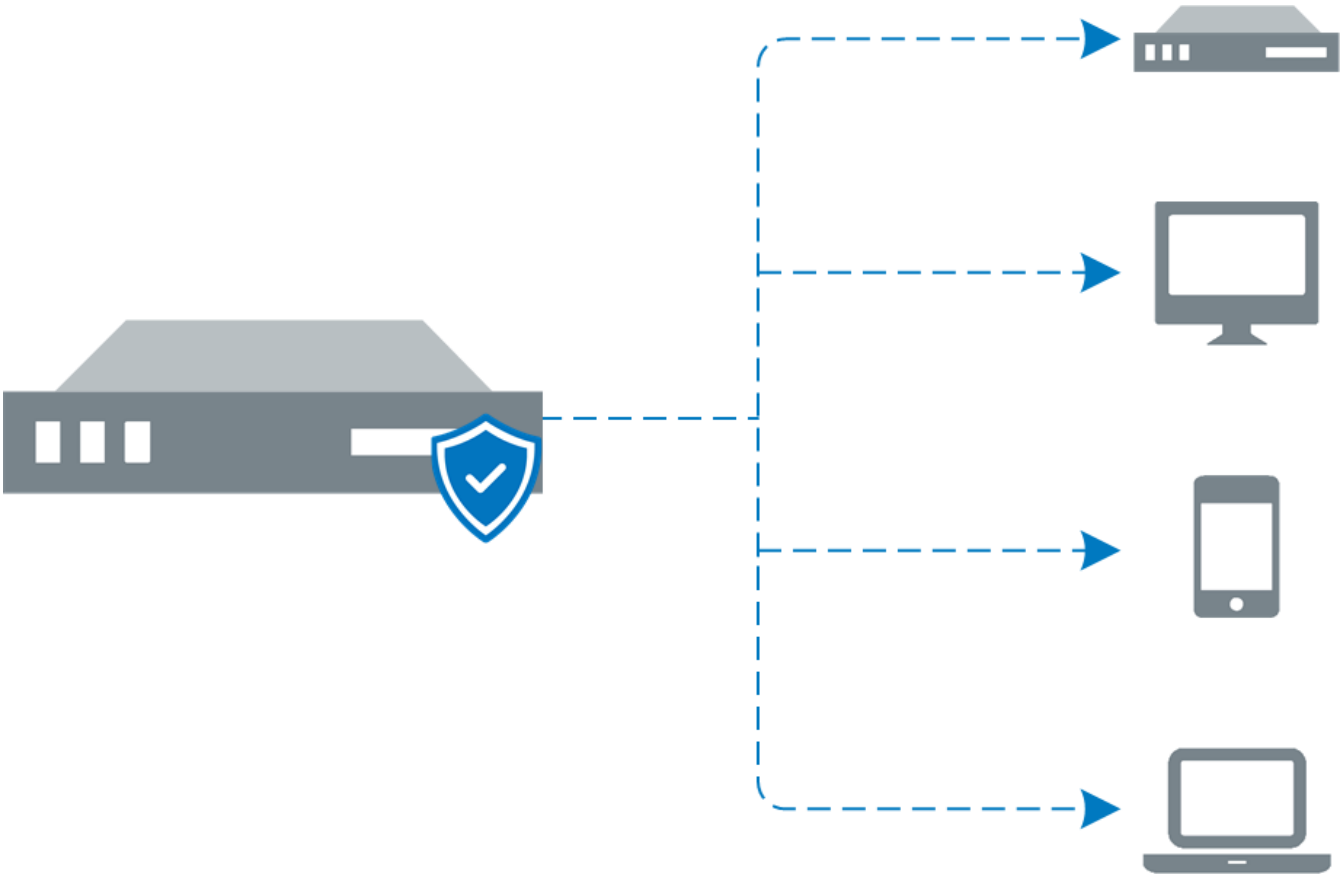
On installation, GFI LanGuard identifies reachable machines within your network. It collects information sets from the network machines as part of its Network Discovery operations and performs a deep scan to enumerate all the information related to target computers.

GFI LanGuard can be deployed in a number of ways, depending on the number and type of computers and devices you want to monitor, network bandwidth usage during normal operation times and the network topology.

Use the information below to help you understand the different deployment options. For more information, refer to Deployment scenarios (page 15).

1.1.1 Basic scanning and auditing of network devices

Install GFI LanGuard on a server that meets the system requirements to run scans and audits of computers and devices. No additional software installations are required. GFI LanGuard creates a remote session with the specified scan targets and audits them over the network. On completion, the results are imported into the results database and the remote session ends. You can audit single computers, a range of specific computers and an entire domain/workgroup. For more information, refer to Manual scans (page 96).



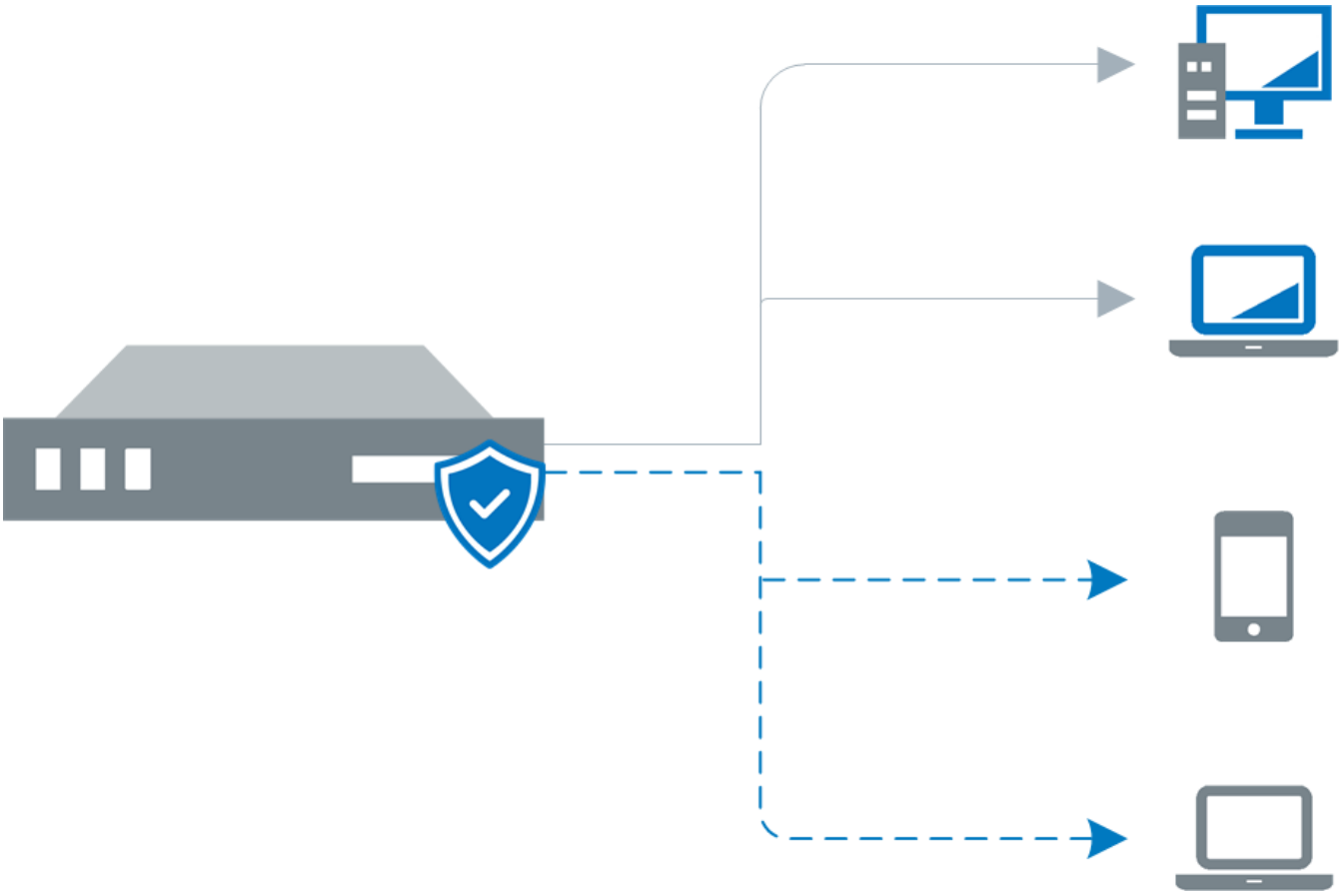
Screenshot 1: GFI LanGuard scanning devices over the network.

Note that scans run in this mode use the resources of the machine where GFI LanGuard is installed and utilize more network bandwidth since all auditing is done remotely. When you have a large network of scan targets, this mode can drastically decrease GFI LanGuard's performance and can affect network speed. Refer to the sections below if you have a large network.

1.1.2 GFI LanGuard Agents

GFI LanGuard can be configured to automatically deploy agents on computers. Agents minimize network bandwidth utilization because audits are done using the scan target's resources and only a result XML file is transferred over the network. Devices that have a GFI LanGuard agent installed will be scanned even if the device is not connected to the company network and are more accurate that agent-less scans because agents can access more information on the local host. For more information refer to Managing Agents,

Typically, networks contain a mixture of agent-based devices and other devices scanned over the network.



Screenshot 2: Devices that have an agent installed and devices scanned by GFI LanGuard over the network.

Agents send scan data to GFI LanGuard through TCP port 1072. This port is opened by default when installing GFI LanGuard. Agents do not consume resources on the scan target unless the agent is performing a scan or a remediation operation.

Note that agents can only be deployed on computers running a Microsoft Windows operating system and they require approximately 25 MB of memory and 350 MB of hard disk space.

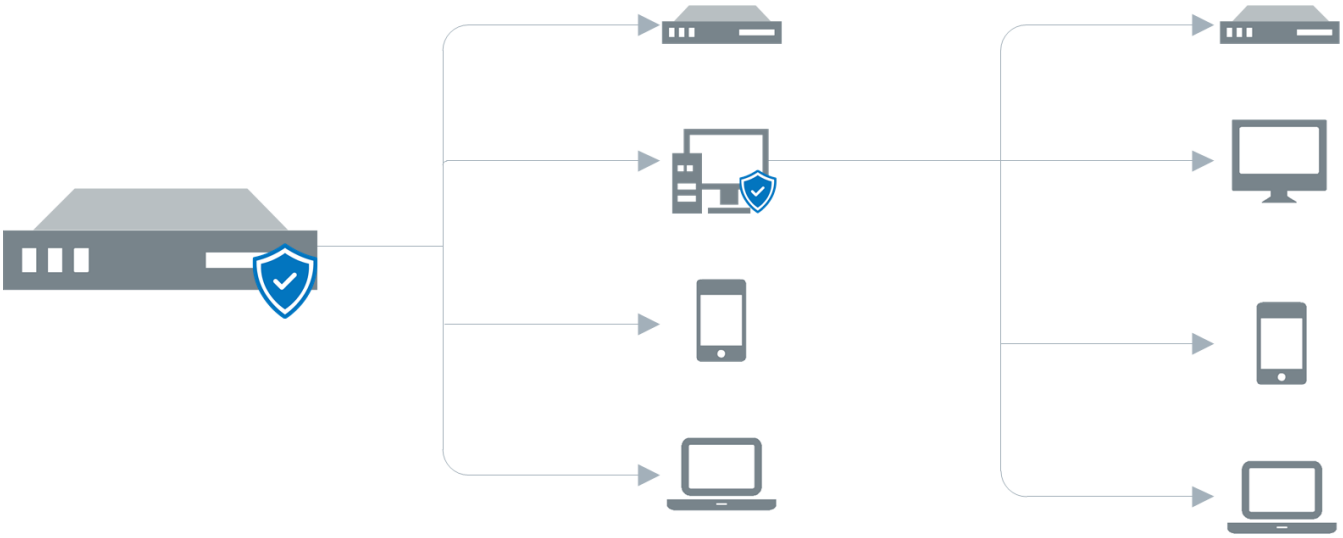
1.1.3 Relay Agents

Relay agents reduce the load from the server where GFI LanGuard is installed to increase server performance and to apply bandwidth load balancing techniques. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers. The main advantages of using relay agents are:

» Reduced bandwidth consumption in local or geographically distributed networks. If a Relay Agent is configured on each site, a patch is only downloaded once and distributed to client computers

» Reduced hardware load from the GFI LanGuard server component and distributed amongst relay agents

» Using multiple Relay Agents increases the number of devices that can be protected simultaneously.



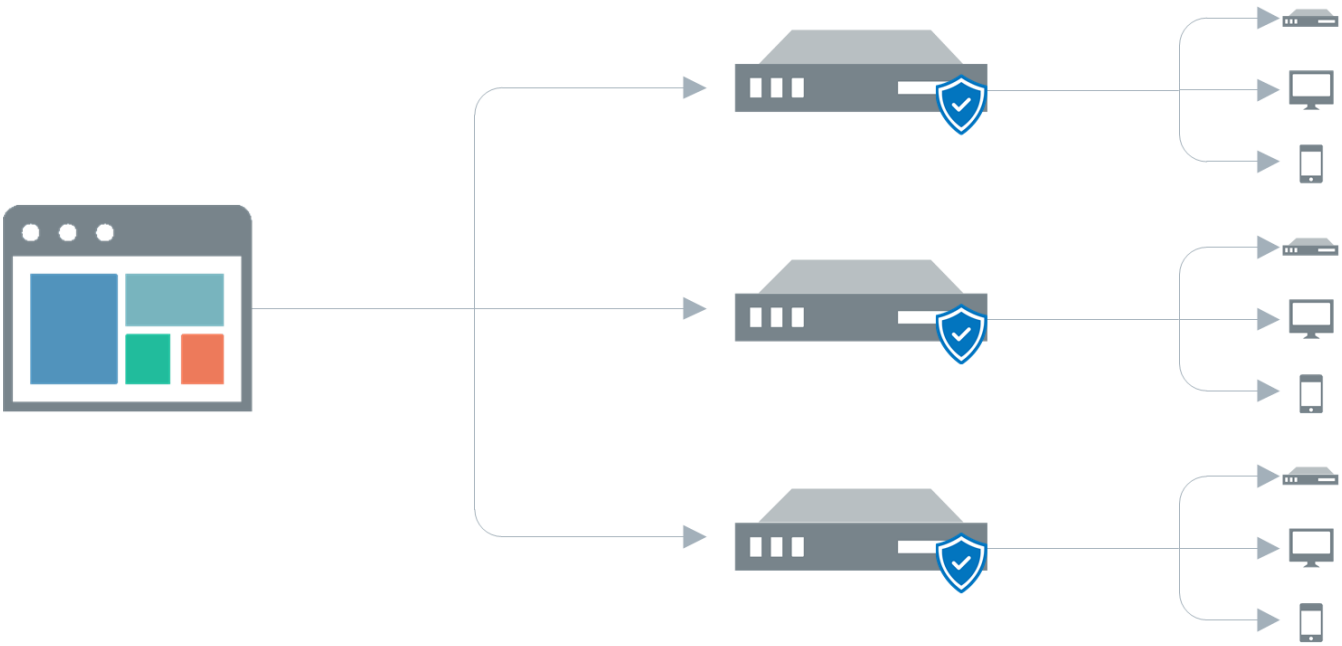
Screenshot 3: Devices relaying data through a GFI LanGuard Relay Agent.

Note that you can have cascading relay agents where a relay agent relays data through another relay agent. It is recommended to keep the number of computers and agents directly connected to the GFI LanGuard server or to one Relay Agent below 100.

Only devices that have the GFI LanGuard Agent installed can be promoted to Relay Agents. Promoting an agent to a Relay Agent is done from within GFI LanGuard. For more information, refer to Configuring Relay Agents (page 83).

1.2 The GFI LanGuard Central Management Server

GFI LanGuard Central Management Server is aimed at very large networks that want to monitor the operation of multiple GFI LanGuard instances in one central console. It offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances. For more information refer to GFI LanGuard Central Management Server.



Screenshot 4: Multiple GFI LanGuard instances monitored by the GFI LanGuard Central Management Server

The GFI LanGuard Central Management Server is used for reporting only. Scans and remediation take place within each individual GFI LanGuard instance. Information is centralized to the GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard, depending on network size and amount of data being transferred.

1.3 GFI LanGuard Components

This section provides you with information about GFI LanGuard components. The installation files enable you to install both GFI LanGuard from where you can perform patch management and remediation tasks from the dashboard and also GFI LanGuard Central Management Server - a web console that unifies multiple GFI LanGuard installations into one centralized console. All the other components are deployed through GFI LanGuard once installation is complete. Available components are described in the table below:

Component	Description
GFI LanGuard Central Management Server	Also known as Central Management Server, this component provides integration between several GFI LanGuard instances, even in remote locations. GFI LanGuard Central Management Server enables reporting but does not allow scans or remediation tasks. For more information, refer to GFI LanGuard Central Management Server (page 40).
GFI LanGuard	Enables you to manage agents, perform scans, analyze results, remediate vulnerability issues and generate reports. For more information, refer to Introduction (page 6).
GFI LanGuard Agents	Enable data processing and auditing on target machines; once an audit is finished, result is sent to GFI LanGuard. For more information, refer to Deploying Agents (page 73).
GFI LanGuard Update System	Enables you to configure GFI LanGuard to auto–download updates released by GFI to improve functionality. These updates also include checking GFI web site for newer builds. For more information, refer to Configuring Program Updates (page 240).
GFI LanGuard Attendant Service	The background service that manages all scheduled operations, including scheduled network security scans, patch deployment and remediation operations. For more information, refer to Scanning Your Network (page 94).
GFI LanGuard Scanning Profiles Editor	This editor enables you to create new and modify existing scanning profiles. For more information, refer to Scanning Profile Editor (page 247).
GFI LanGuard Command Line Tools	Enables you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up GFI LanGuard. For more information, refer to Command Line Tools (page 281).

1.4 Supported features per operating system, application and device

GFI LanGuard provides a detailed analysis of the state of your network and a complete picture of installed applications, hardware on your network, mobile devices that connect to the Exchange servers, the state of security applications (antivirus, anti-spam, firewalls, etc.), open ports and any existing shares and services running on your machines.

GFI LanGuard features, such as Device Identification and Port Scanning (DI/PS), Vulnerability Assessment (VA), Patch Management (PM), Software Audit (SA) and Hardware Audit (HA) are supported by a wide range of devices, operating systems and applications listed in the table below:

Windows® Server Operating System	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Server 2016	✓	✓	✓	✓	✓

Windows® Server Operating System	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Server 2012 (including R2)	✓	✓	✓	✓	✓
Server 2008 (including R2) Standard/Enterprise	✓	✓	✓	✓	✓
Server 2003 Standard/Enterprise	✓	✓	✓	✓	✓
Small Business Server 2011	✓	✓	✓	✓	✓
Small Business Server 2008 Standard	✓	✓	✓	✓	✓
Small Business Server 2003 (SP1)	✓	✓	✓	✓	✓

Windows® Client Operating System	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Windows 10 Professional/Enterprise	✓	✓	✓	✓	✓
Windows 8/8.1 Professional/Enterprise	✓	✓	✓	✓	✓
Windows 7 Professional/Enterprise/Ultimate	✓	✓	✓	✓	✓
Windows Vista Business/Enterprise/Ultimate	✓	✓	✓	✓	✓
Windows XP Professional (SP2 or higher)	✓	✓	✓	✓	✓

Windows® Third Party Applications	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Microsoft Office	✗	✓	✓	✗	✗
Microsoft Exchange	✗	✓	✓	✗	✗
Microsoft SQL Server	✗	✓	✓	✗	✗
Microsoft Visual Studio	✗	✓	✓	✗	✗
Other Microsoft applications	✗	✓	✓	✗	✗
Java Runtime Environment	✗	✓	✓	✗	✗
Adobe Flash Player	✗	✓	✓	✗	✗
Adobe Reader	✗	✓	✓	✗	✗
Adobe AIR	✗	✓	✓	✗	✗
Adobe Shockwave Player	✗	✓	✓	✗	✗

Windows® Third Party Applications	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Mozilla Firefox	✗	✓	✓	✗	✗
Apple Safari	✗	✓	✓	✗	✗
Apple QuickTime	✗	✓	✓	✗	✗
Apple iTunes	✗	✓	✓	✗	✗
Opera Browser	✗	✓	✓	✗	✗

Linux Distributions	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Mac OS X (versions supported by OS vendor)	✓	✓	✓	✓	✓
Red Hat Enterprise Linux (versions supported by OS vendor)	✓	✓	✓	✓	✓
CentOS (versions supported by OS vendor)	✓	✓	✓	✓	✓
Ubuntu (versions supported by OS vendor)	✓	✓	✓	✓	✓
Debian (versions supported by OS vendor)	✓	✓	✓	✓	✓
SUSE Linux Enterprise (versions supported by OS vendor)	✓	✓	✓	✓	✓
openSUSE (versions supported by OS vendor)	✓	✓	✓	✓	✓
Other distributions	✓	✓	✗	✓	✓

Virtual Machines (with supported guest operating systems)	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
VMware	✓	✓	✓	✓	✓
Microsoft® Hyper-V	✓	✓	✓	✓	✓
Oracle Virtual Box	✓	✓	✓	✓	✓
Citrix Xen	✓	✓	✓	✓	✓
Parallels	✓	✓	✓	✓	✓

Network Devices	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Cisco	✓	✓	✗	✗	✗
HP	✓	✓	✗	✗	✗
Linksys	✓	✓	✗	✗	✗
D-Link	✓	✓	✗	✗	✗
Netgear	✓	✗	✗	✗	✗
SonicWall	✓	✗	✗	✗	✗
Alcatel Lucent	✓	✗	✗	✗	✗
3Com	✓	✗	✗	✗	✗
Nortel	✓	✗	✗	✗	✗
Juniper Networks	✓	✗	✗	✗	✗
IBM	✓	✗	✗	✗	✗
Dell	✓	✗	✗	✗	✗
H3C	✓	✗	✗	✗	✗
Nortel Networks	✓	✗	✗	✗	✗

Mobile Devices	DI/PS Device Identification and Port Scanning	VA Vulnerability Assessment	PM Patch Management	SA Software Audit	HA Hardware Audit
Google Android	✓	✓	✗	✗	✗
Apple iOS	✓	✓	✗	✗	✗
Windows phone	✓	✓	✗	✗	✗

Acronyms used in table above:

- **DI/PS**: Device Identification and Port Scanning
- **VA**: Vulnerability Assessment
- **PM**: Patch Management
- **SA**: Software Audit
- **HA**: Hardware Audit

For a detailed list of every supported model of each application see http://go.gfi.com/?pageid=LAN_WindowsThirdPartyApplications

For a detailed list of every supported model of each device see http://go.gfi.com/?pageid=LAN_SupportedDevices

1.5 About this guide

The aim of this Administrator Guide is to help System Administrators install, configure and run GFI LanGuard with minimum effort.

1.5.1 Terms and conventions used in this manual

Term	Description
Note	Additional information and references essential for the operation of GFI LanGuard.
Important	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and file names.
`Code`	Indicates text values to key in, such as commands and addresses.

2 Installing GFI LanGuard

The following topics provide information on how to successfully deploy a fully functional instance of GFI LanGuard and how to upgrade existing installations.

Topics in this section:

2.1 Deployment scenarios

GFI LanGuard deployments depend on the number of computers and devices you want to monitor and traffic load on your network during normal operation time. Refer to the following deployment scenarios to determine whether you want to:

» Deploy a GFI LanGuard instance - Install a GFI LanGuard instance to scan, detect and remediate network vulnerabilities.

» Deploy GFI LanGuard Central Management Server - connect multiple GFI LanGuard instances in one centralized UI for reporting purposes.

» Deploy GFI LanGuard in Agent-less mode - in this mode, GFI LanGuard creates a remote session with scan targets and audits them over the network.

» Deploy GFI LanGuard Agents - deploy Agents on newly discovered computers to minimize network bandwidth utilization.

» Deploy GFI LanGuard Relay Agents - Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers to reduce the load from the GFI LanGuard server.

» Deploy GFI LanGuard in mixed mode - in this mode GFI LanGuard is configured to work in Agent and Agent-less mode on the network.

Deploy a GFI LanGuard instance

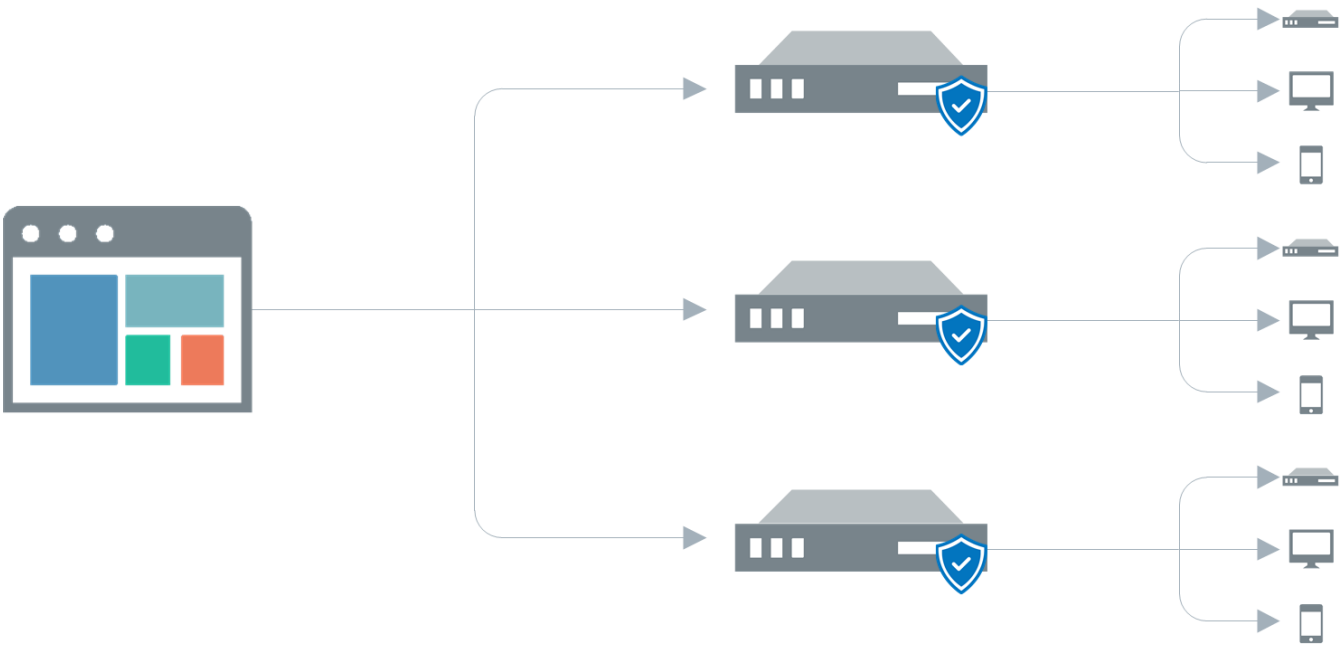
Any GFI LanGuard deployment starts with installing the product in your environment. After a GFI LanGuard instance is successfully installed, it will:

» Determine reachable machines on your network and collect information from target machines as part of its Network Discovery operations, using a subset of SMB, NETBIOS, and ICMP protocols. Supported targets include the localhost, IP, computer name, computers list, IP range, whole domain/workgroup and/or organizational unit.

» Once targets are identified, GFI LanGuard performs a scan to enumerate all the information related to the target computer. GFI LanGuard uses a variety of techniques to gain access to this information ranging from file and folder property checks, registry checks, WMI commands, SMB commands as well as port scan checks (TCP/UDP) and more.

Deploy the GFI LanGuard Central Management Server to connect multiple GFI LanGuard instances

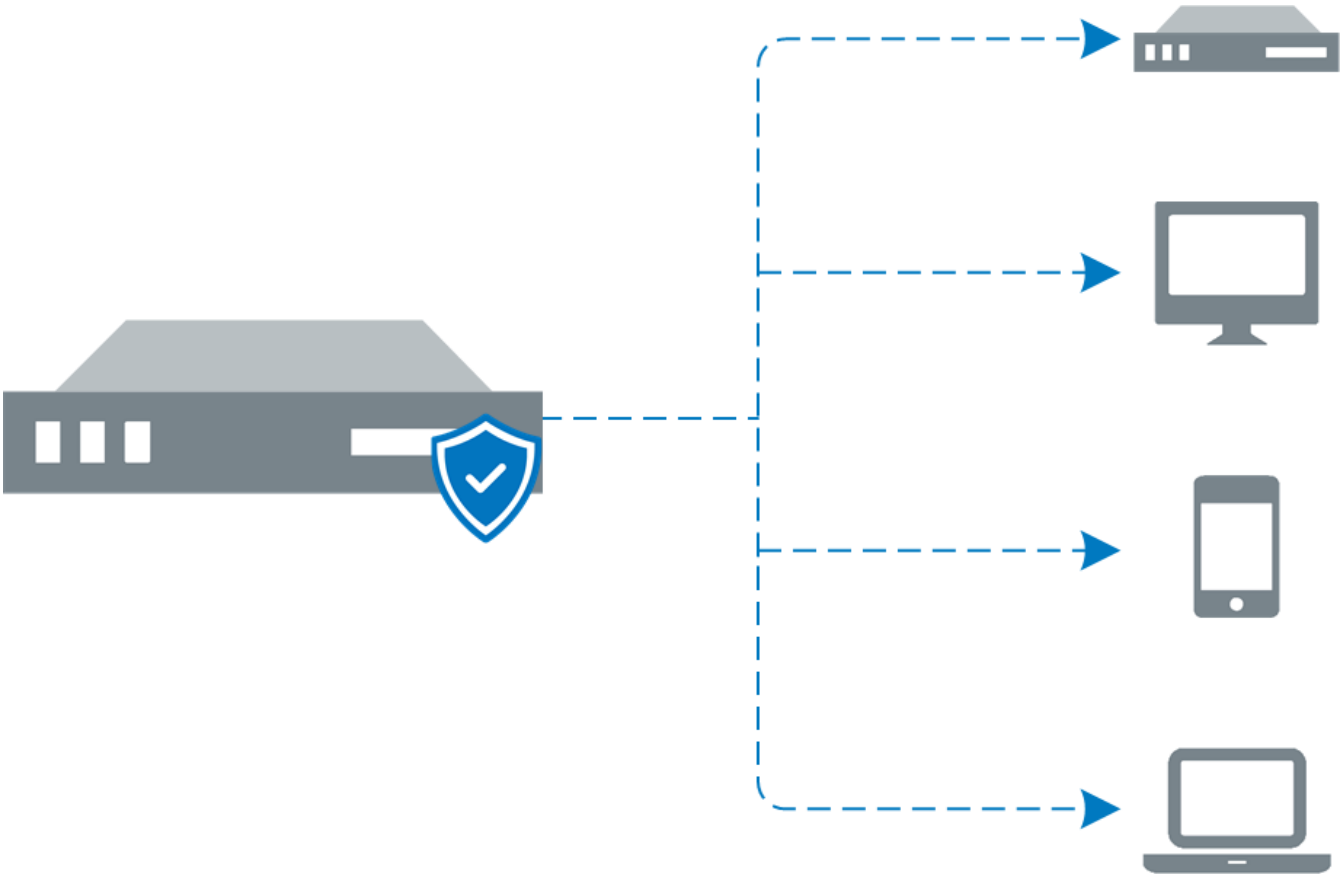
With GFI LanGuard Central Management Server, multiple GFI LanGuard instances can be brought together through a common console, even when installed in separate locations. The GFI LanGuard Central Management Server console offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances. It also offers centralized reporting and visibility by capturing data from the various deployments of GFI LanGuard. For more information, refer to GFI LanGuard Central Management Server (page 40).



GFI LanGuard Central Management Server is used only for reporting. Scans and remediation take place only in GFI LanGuard and then information is centralized to GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard. Synchronization usually takes a few minutes. Delay depends on network size and amount of data being transferred.

Deploy GFI LanGuard in Agent-less mode

Agent-less auditing is started from GFI LanGuard. GFI LanGuard creates a remote session with the specified scan targets and audits them over the network. On completion, the results are imported into the results database and the remote session ends. You can audit single computers, a range of specific computers and an entire domain/workgroup. For more information, refer to Manual scans (page 96).



NOTE

Scans in Agent-less mode use the resources of the machine where GFI LanGuard is installed and utilize more network bandwidth since auditing is done remotely. When you have a large network of scan targets, this mode can drastically decrease GFI LanGuard's performance and affects network speed. In larger networks, deploy Agents/Relay Agents to balance the load appropriately.

Deploy GFI LanGuard Agents

GFI LanGuard can be configured to automatically deploy agents on newly discovered computers. Agents minimize network bandwidth utilization. This is because in Agent-less mode, the GFI LanGuard server component performs audits over the network; while in Agent mode, audits are done using the scan target's resources and only a result XML file is transferred over the network.

Agents send scan data to GFI LanGuard through TCP port 1072. This port is opened by default when installing GFI LanGuard. Agents do not consume resources of the scan target's machine unless it is performing a scan or remediation operations. If an Agent becomes unresponsive for 60 days, it is automatically uninstalled from the target machine. For more information, refer to Managing Agents (page 73).

NOTE

GFI LanGuard Agents can be deployed only on machines running Microsoft Windows operating systems that meet a minimum set of system requirements. For more information, refer to GFI LanGuard system requirements (page 20).

Deploy GFI LanGuard Relay Agents

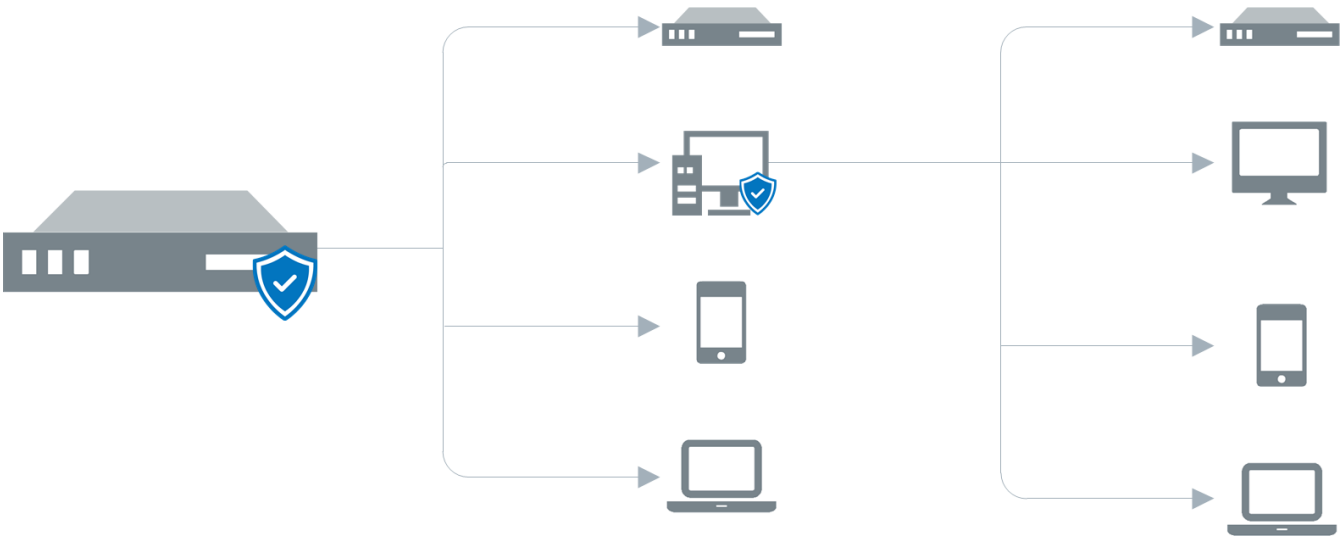
Relay agents are used to reduce the load from the GFI LanGuard server. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers. The main advantages of using relay agents are:

» Save Network Bandwidth in local or geographically distributed networks. If a relay agent is configured on each site, a patch is only downloaded once and distributed to clients

» Load is removed from the GFI LanGuard server component and distributed amongst relay agents

» Since computers are managed from multiple relay agents, it increases the number of devices that can be protected simultaneously.

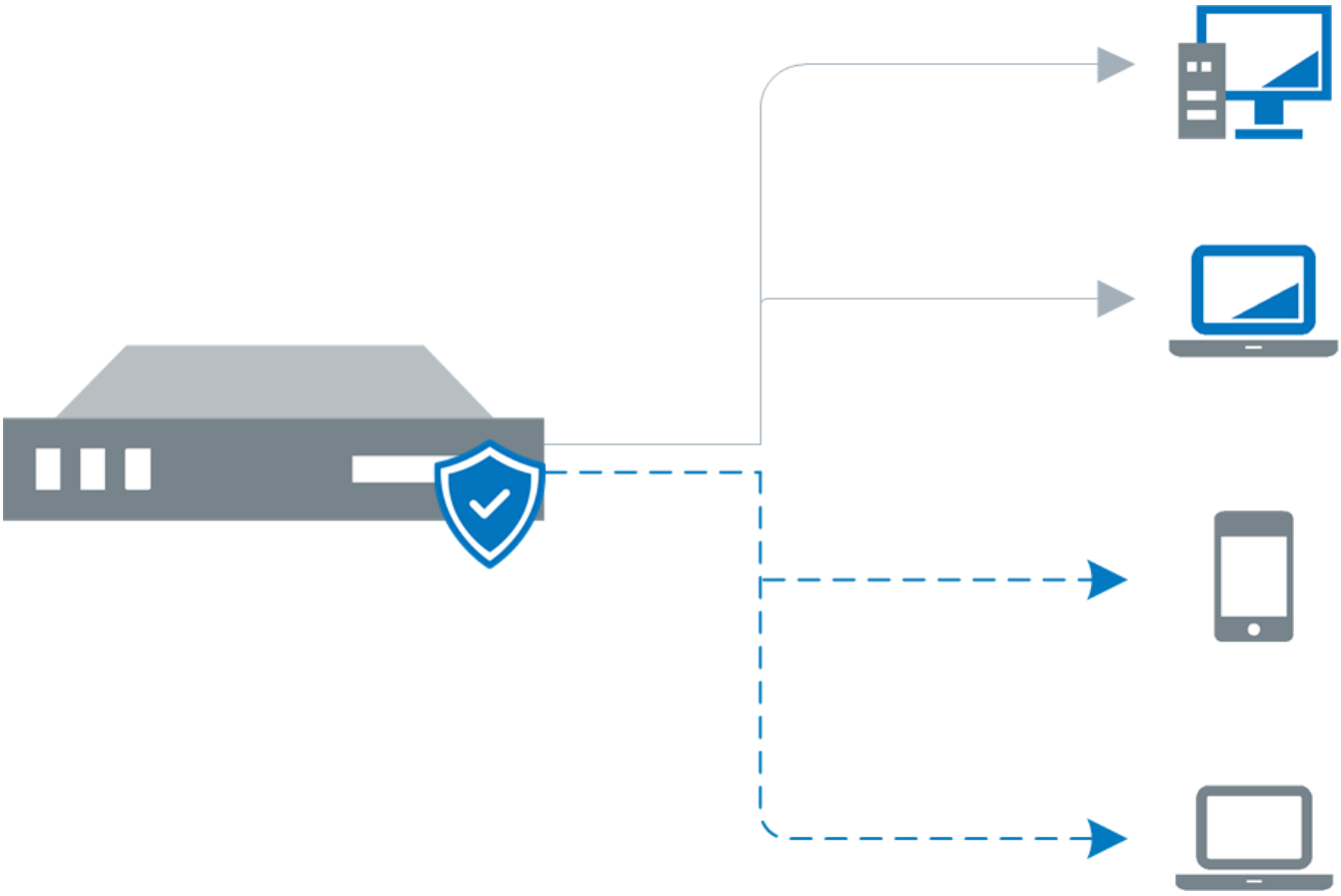
In a network, computers can be grouped and each group can be assigned to a relay agent. For more information, refer to Configuring Relay Agents (page 83).



Deploy GFI LanGuard in mixed mode

In mixed mode, GFI LanGuard is configured to work in Agent mode on some computers and in Agent-less mode on other computers or devices.

The following screenshot shows how GFI LanGuard can be deployed in mixed mode on a Local Area Network (LAN):



2.2 System Requirements

The following topics provide information about the system requirements for all GFI LanGuard components.

2.2.1 GFI LanGuard system requirements

Computers running GFI LanGuard must meet the system requirements described below for performance reasons.

Refer to the following sections for information about:

- Hardware requirements
- Software requirements
- Firewall ports and protocols
- Gateway permissions
- Antivirus & Backup exclusions

Hardware requirements

Computers hosting GFI LanGuard must meet the following hardware requirements:

Component	1 to 100 Computers	100 to 500 Computers	500 to 3,000 Computers
Processor	2 GHz Dual Core	2.8 GHz Dual Core	3 GHz Quad Core
Physical Storage	5 GB	10 GB	20 GB
RAM	2 GB	4 GB	8 GB
Network bandwidth	1544 kbps	1544 kbps	1544 kbps

Software requirements

GFI LanGuard components can be installed on any computer that meets the software requirements listed in this section. For more information, refer to:

- Supported operating systems
- Supported databases
- GFI LanGuard and TLS 1.1 or higher
- Target computer components

Supported operating systems (32-bit/64-bit)

The following table lists operating systems and versions where GFI LanGuard can be installed. Ensure that you are running the Full (with GUI) version of these operating systems, and running the latest Service Pack as provided by Microsoft.

Operating System
Windows® Server 2016
Windows® Server 2012 (including R2)
Windows® Server 2008 (including R2) Standard/Enterprise
Windows® 10 Professional/Enterprise
Windows® 8/8.1 Professional/Enterprise

Operating System
Windows® 7 Professional/Enterprise/Ultimate
Windows® Vista Business/Enterprise/Ultimate
Windows® Small Business Server 2011

Supported databases

GFI LanGuard uses a database to store information from network security audits and remediation operations. The database backend can be any of the following:

Database server	Recommended Use
SQL Server® Express® 2008 or later	This database server has a 10GB limit and is therefore recommended for networks containing up to 500 computers. If a database server is not available, the GFI LanGuard installer can automatically download and run the Microsoft SQL Express installer.
SQL Server® 2008 or later	Recommended for larger networks containing 500 computers or more.

For improved performance, it is highly recommended to use an SSD drive for the database server. Compared to traditional Hard Disk Drives, SSDs deliver superior performance with lower access time and lower latency.

GFI LanGuard and TLS 1.1 or higher

If you plan to deploy GFI LanGuard in an environment where TLS 1.1 and above is running, you need to enable FIPS-Compliant algorithms on the computer where the GFI LanGuard is installed.

To enable FIPS-Compliant algorithms:

1. Go to **Start > Run** and type `gpedit.msc`
2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**.
3. Double-click **Security Options**.
4. In the details pane, double-click **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**.
5. Check **Enabled** and click **OK**
6. Reboot the computer or open a command prompt and type `gpupdate /force`.

Target computer components

The following table provides you with information about components that are required to be installed or enabled on computers to be scanned remotely (agent-less) by GFI LanGuard:

Component	Description
Secure Shell (SSH)	Required for UNIX/Linux/Mac OS based scan targets. SSH server must be installed and enabled.
File and Printer Sharing	Required for machines running Microsoft operating systems to enumerate and collect information about scan targets.
Remote Registry	Ensure that this service is running on machines using Microsoft operating systems. This is required to collect information about scan targets, such as Operating System details, user and computer data.

Firewall Ports and Protocols

This section provides you with information about the required firewall ports and protocols settings for:

- GFI LanGuard and Relay Agents
- GFI LanGuard Agent and Agent-less computers

GFI LanGuard and Relay Agents

Configure your firewall to allow **inbound** connections on TCP port **1072**, on computers running:

- GFI LanGuard
- Relay Agents

This port is automatically used when GFI LanGuard is installed, and handles all inbound communication between the server component and the monitored computers. If GFI LanGuard detects that port 1072 is already in use by another application, it automatically searches for an available port in the range of **1072-1170**.

To manually configure the communication port:

1. Launch GFI LanGuard.
2. Go to **Configuration > Manage Agents**.
3. From the right pane, click **Agents Settings**.
4. From the **Agents Settings** dialog, specify the communication port in the **TCP port** text box.
5. Click **OK**

GFI LanGuard Agent and Agent-less computers

Communications between GFI LanGuard and managed computers (Agents and Agent-less), are done using the ports and protocols below. The firewall on managed computers needs to be configured to allow **inbound** requests on the following ports:

TCP Ports	Protocol	Description
22	SSH	Auditing Linux systems.
135	DCOM	Dynamically assigned port.
137	NetBIOS	Computer discovery and resource sharing.
138	NetBIOS	Computer discovery and resource sharing.
139	NetBIOS	Computer discovery and resource sharing.
161	SNMP	Used for computer discovery. GFI LanGuard supports SNMPv1 and SNMPv2c. SNMPv3 and SNMP over TLS / DTLS are not supported.
445	SMB	Used while: » Auditing computers » Agent management » Patch deployment.

Gateway permissions

To download definition and security updates, GFI LanGuard connects to GFI, Microsoft, and Third-Party update servers via HTTP. Ensure that the firewall settings of the machine where GFI LanGuard is installed allows connections to:

- gfi-downloader-137146314.us-east-1.elb.amazonaws.com
- *software.gfi.com/lnsupdate/
- *.download.microsoft.com
- *.windowsupdate.com
- *.update.microsoft.com
- All update servers of Third-Party Vendors supported by GFI LanGuard.

For more information, refer to:

- Supported Third-Party applications: http://go.gfi.com/?pageid=LAN_PatchMng
- Supported application bulletins: http://go.gfi.com/?pageid=3p_fullreport
- Supported Microsoft applications: http://go.gfi.com/?pageid=ms_app_fullreport
- Supported Microsoft bulletin: http://go.gfi.com/?pageid=ms_fullreport

Antivirus & Backup exclusions

Antivirus & backup software can cause GFI LanGuard to malfunction if it is denied access to some of its files.

Add exclusions that prevent antivirus & backup software from scanning or backing up the following folder on the GFI LanGuard server, Agents, Relay Agents and the GFI LanGuard Central Management Server: <system drive>\ProgramData\GFI\

2.2.2 GFI LanGuard Agent and Relay Agent system requirements

Computers running GFI LanGuard Agent and GFI LanGuard Relay Agent must meet the system requirements described below for performance reasons.

Refer to the following sections for information about:

- Hardware requirements
- Software requirements
- Firewall ports and protocols
- Antivirus & Backup exclusions

Hardware requirements

GFI LanGuard Agent

Computers running a GFI LanGuard Agent must meet the following hardware requirements:

Component	Requirement
Processor	1 GHz
Physical Storage	800MB are required for the installation & an additional 2GB are required during a scan to extract update archives.
RAM	25 MB dedicated to GFI LanGuard
Network band-width	1544 kbps

GFI LanGuard Relay Agent

A computer is eligible to be configured as a Relay Agent when:

- The computer is online and has good uptime (an offline Relay Agent incapacitates its clients)
- Has fast network access to computers connected to it
- Has the required disk space to allow caching.

Computers configured as Relay Agents must meet the following hardware requirements:

Component	1 to 100 Clients	100 to 500 Clients	500 to 1,000 Clients
Processor	2 GHz Dual Core	2 GHz Dual Core	2.8 GHz Dual Core
Physical Storage	5 GB	10 GB	10 GB
RAM	2 GB	2 GB	4 GB
Network bandwidth	100 Mbps	100 Mbps	1 Gbps

Software requirements

GFI LanGuard components can be installed on any computer that meets the software requirements listed in this section. For more information, refer to:

Supported operating systems (32-bit/64-bit)

The following table lists operating systems that GFI LanGuard Agent and GFI LanGuard Relay Agent can be installed on:

Windows® Operating System	GFI LanGuard Agent	GFI LanGuard Relay Agent
Windows Server 2016	✓	✓
Windows Server 2012 (including R2)	✓	✓
Windows Server 2008 R2 Standard/Enterprise (latest SP)	✓	✓
Windows Server 2008 Standard/Enterprise (latest SP)	✓	✓
Windows Server 2003 Standard/Enterprise	✓	✗
Windows 10 Professional/Enterprise	✓	✓
Windows 8/8.1 Professional/Enterprise	✓	✓
Windows 7 Professional/Enterprise/Ultimate (latest SP)	✓	✓
Windows Vista Business/Enterprise/Ultimate	✓	✓
Windows XP Professional (latest SP)	✓	✗
Small Business Server 2011	✓	✓
Small Business Server 2008 Standard	✓	✗
Small Business Server 2003 (latest SP)	✓	✗

Firewall Ports and Protocols

This section provides you with information about the required firewall ports and protocols settings for:

- GFI LanGuard and Relay Agents
- GFI LanGuard Agent and Agent-less computers

GFI LanGuard and Relay Agents

Configure your firewall to allow **inbound** connections on TCP port **1072**, on computers running:

- GFI LanGuard
- Relay Agents

To manually configure the communication port:

1. Launch GFI LanGuard.
2. Click **Configuration** tab > **Manage Agents**.
3. From the right pane, click **Agents Settings**.
4. From the **Agents Settings** dialog, specify the communication port in the **TCP port** text box.
5. Click **OK**

GFI LanGuard Agent and Agent-less computers

Communications between GFI LanGuard and managed computers (Agents and Agent-less), are done using the ports and protocols below. The firewall on managed computers needs to be configured to allow **inbound** requests on the following ports:

TCP Ports	Protocol	Description
22	SSH	Auditing Linux systems.
135	DCOM	Dynamically assigned port.
137	NetBIOS	Computer discovery and resource sharing.
138	NetBIOS	Computer discovery and resource sharing.
139	NetBIOS	Computer discovery and resource sharing.
161	SNMP	Used for computer discovery. GFI LanGuard supports SNMPv1 and SNMPv2c. SNMPv3 and SNMP over TLS / DTLS are not supported.
445	SMB	Used while: » Auditing computers » Agent management » Patch deployment.

Antivirus & Backup exclusions

Antivirus & backup software can cause GFI LanGuard to malfunction if it is denied access to some of its files.

Add exclusions that prevent antivirus & backup software from scanning or backing up the following folder on the GFI LanGuard server, Agents, Relay Agents and the GFI LanGuard Central Management Server: <system drive>\ProgramData\GFI\

2.2.3 Central Management Server system requirements

Computers running GFI LanGuard Central Management Server must meet the system requirements described below.

Hardware requirements

Computers hosting GFI LanGuard Central Management Server must meet the following minimum hardware requirements:

Component	Requirement
Processor	2.8 GHz quad-core
Physical Storage	10 GB HDD free space
RAM	8 GB RAM

Supported operating systems (32-bit/64-bit)

The following table lists operating systems and versions where the GFI LanGuard Central Management Server can be installed. Ensure that these operating systems are running the latest Service Pack as provided by Microsoft.

Operating System
Windows® Server 2016
Windows® Server 2012 (including R2)
Windows® Server 2008 (including R2) Standard/Enterprise
Windows® 10 Professional/Enterprise
Windows® 8/8.1 Professional/Enterprise
Windows® 7 Professional/Enterprise/Ultimate
Windows® Vista Business/Enterprise/Ultimate
Windows® Small Business Server 2011

Supported databases

GFI LanGuard Central Management Server uses a database to store information retrieved from multiple GFI LanGuard installations. The database backend can be any of the following:

Database server	Recommended Use
SQL Server Express® 2008 or later	This database server has a 10GB limit and is therefore recommended for networks containing up to 500 computers. If a database server is not available, the GFI LanGuard installer can automatically download and run the Microsoft SQL Express installer.
SQL Server® 2008 or later	Recommended for larger networks containing 500 computers or more.

For improved performance, it is highly recommended to use an SSD drive for the database server. Compared to traditional Hard Disk Drives, SSDs deliver superior performance with lower access time and lower latency.

Firewall Ports and Protocols

GFI LanGuard instances communicate with the GFI LanGuard Central Management Server via port **1077**. Configure your firewall to allow **inbound** connections on TCP port **1077**, on computers running GFI LanGuard and the GFI LanGuard Central Management Server.

If port 1077 is already in use by another application, the GFI LanGuard Central Management Server automatically searches for an available port in the range of **1077-1277**.

Antivirus & Backup exclusions

Antivirus & backup software can cause GFI LanGuard to malfunction if it is denied access to some of its files.

Add exclusions that prevent antivirus & backup software from scanning or backing up the following folder on the GFI LanGuard server, Agents, Relay Agents and the GFI LanGuard Central Management Server: <system drive>\ProgramData\GFI\

2.3 Importing and exporting GFI LanGuard settings

The Import and Export Configurations Wizard is a GFI LanGuard feature that enables you to import and export settings, including:

- Scanning Profiles
- Vulnerability Assessment
- Ports (TCP/UDP)
- Results Filtering Reports
- Auto–Remediate Settings (Auto–Uninstall and Patch settings)
- Options (Database Backend, Alerting, Schedule scan and Internal Settings).

This feature is useful when you want to retain configuration settings from an older version of GFI LanGuard and reuse them in a new version. The following sections contain information about:

- Exporting configurations to a file
- Importing configurations from a file
- Importing configurations from another instance of GFI LanGuard

Exporting configurations to a file

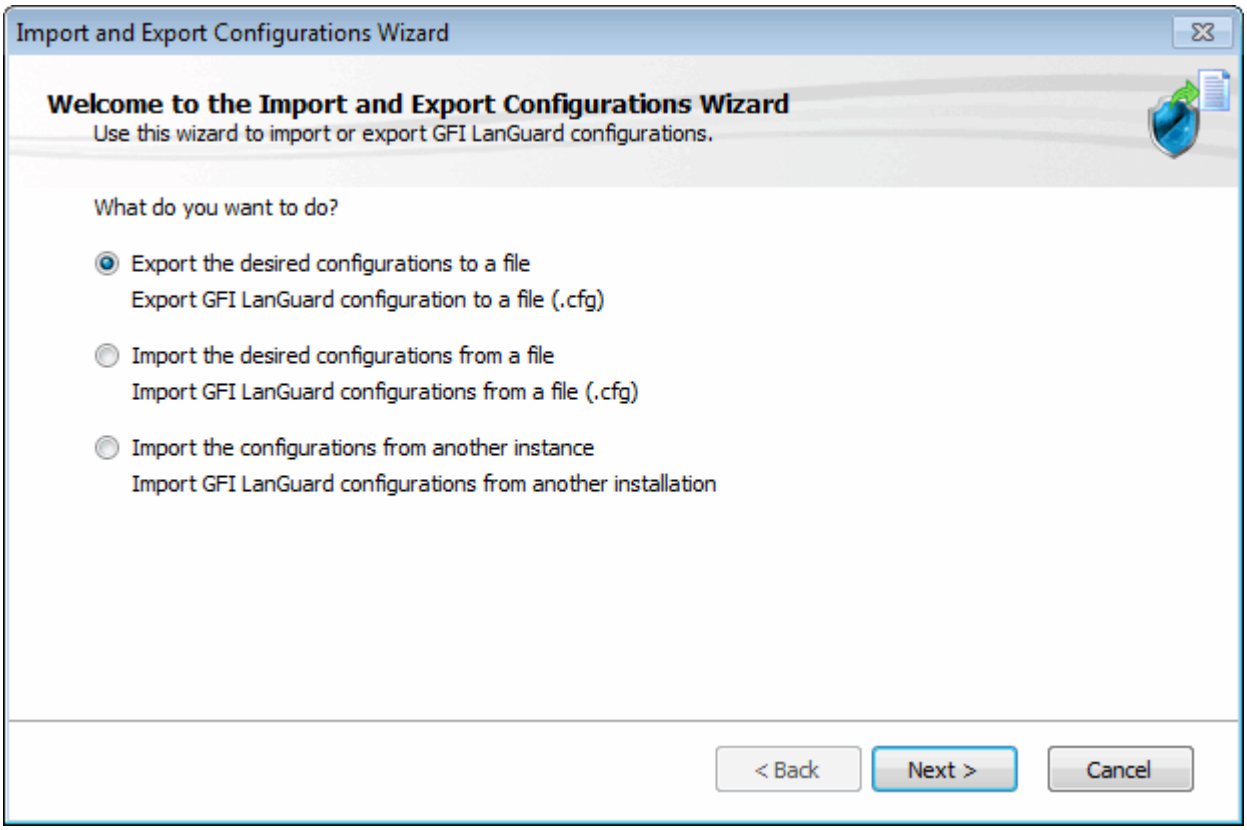
To export the configurations:

1. Launch GFI LanGuard.

2. From the top navigation click **File > Import and Export Configurations**.

3. Select **Export the desired configuration to a file** and click **Next**.

4. Specify the path were to save the exported configuration, and click **Next**.



Screenshot 5: Export configurations to file

5. Wait for the configuration tree to load and select the configurations to export. Click **Next** to start export.

6. A notify dialog will confirm that exporting is completed.

7. Click **OK** to finish.

Importing configurations from a file

To import saved configurations:

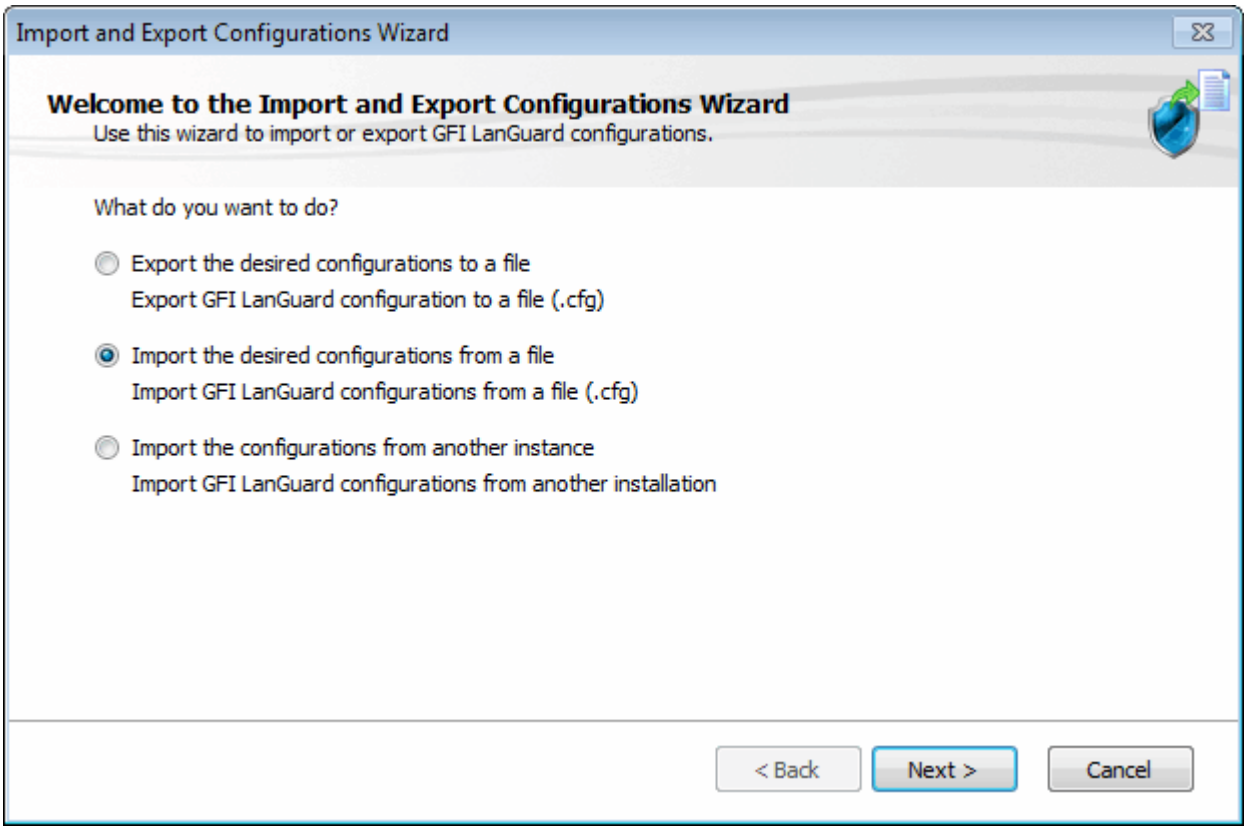
1. Launch GFI LanGuard.

2. From the top navigation click **File > Import and Export Configurations**.

3. Select **Import the desired configuration from a file** and click **Next**.

4. Specify the path from where to load configuration, and click **Next**.

5. Wait for the configuration tree to load and select the configurations to import. Click **Next** to start import.



Screenshot 6: Import configurations from a file

6. Confirm the override dialog box by clicking **Yes** or **No** as required.

7. A notify dialog will confirm that exporting is completed.

8. Click **OK** to finish.

Importing configurations from another instance of GFI LanGuard

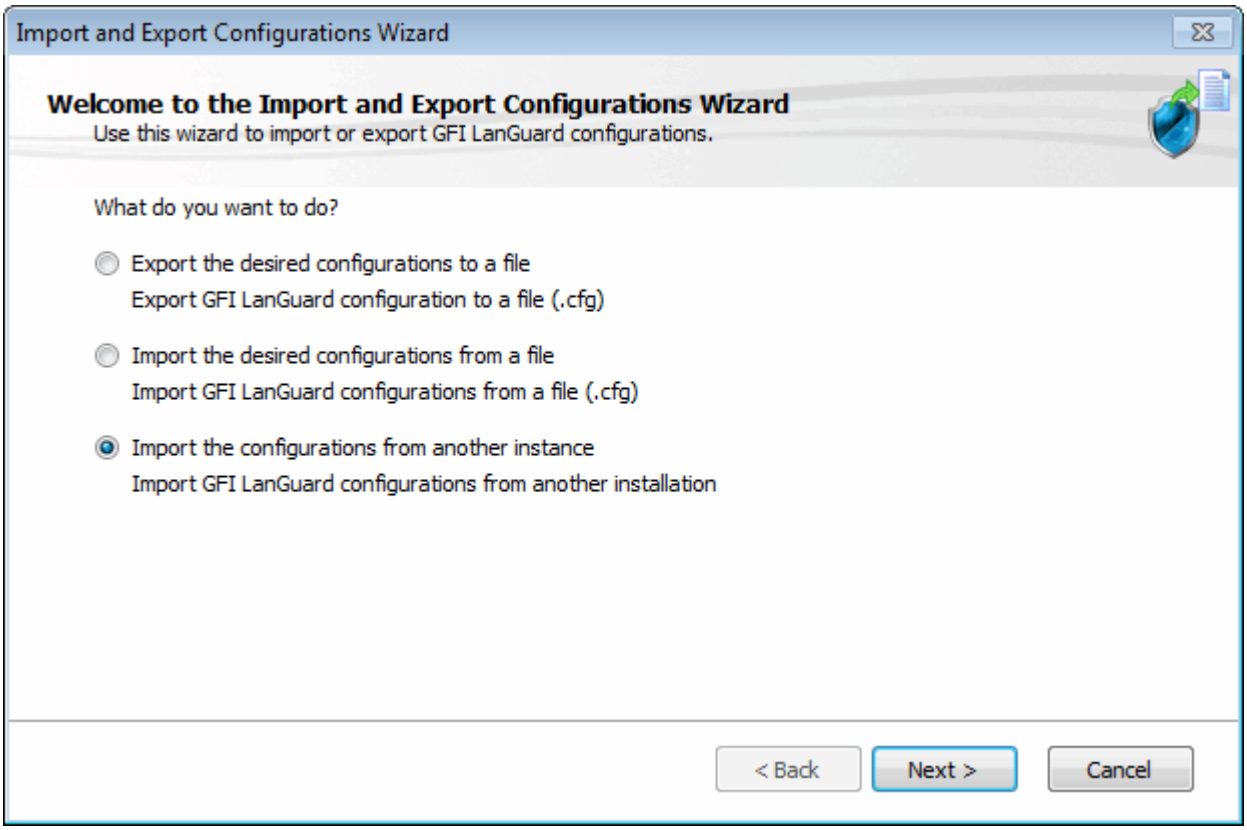
1. Launch GFI LanGuard.

2. From the top navigation click **File > Import and Export Configurations**.

3. Select **Import the configuration from another instance** and click **Next**.

4. Click **Browse** to select the GFI LanGuard installation folder on the machine from where you want to import the configurations. The default location is:

Operating Systems	Path
Windows® XP Professional (SP2 or higher)	<Local Disk>\Documents and Settings\All Users\Application Data\GFI\LanGuard <Version>
Windows® Server 2003 Standard/Enterprise	<Local Disk>\Documents and Settings\All Users\Application Data\GFI\LanGuard <Version>
Windows® Vista Business/Enterprise/Ultimate and later	<Local Disk>\Program Files\GFI\LanGuard <Version>
Windows® Server 2008 (including R2) Standard/Enterprise and later	<Local Disk>\Program Files\GFI\LanGuard <Version>



Screenshot 7: Import setting

5. Select which settings you want to import and click **Next**.

6. While importing, GFI LanGuard will ask you whether you want to override or keep your settings. Select one of the following options:

Option	Description
Yes	Override the current setting with the imported setting.
No	Keep the current setting and ignore the imported setting.
Auto Rename	Rename the imported settings and keep the current settings.

7. Click **OK** when the import is ready.

2.4 Installing GFI LanGuard

2.4.1 Important notes

Before running the installation wizard:

» If you are currently using a previous version of GFI LanGuard, you can upgrade your current installation while at the same time retaining all your existing configuration settings. Upgrade is not reversible; you cannot downgrade to the previous version that you had installed. For more information, refer to Upgrading GFI LanGuard (page 35).

» You must have a GFI Account or a license key to install GFI LanGuard. For more information, refer to Obtaining a GFI LanGuard subscription (page 34).

» Ensure that the machine where GFI LanGuard is going to be installed meets the system requirements. For more information, refer to GFI LanGuard system requirements (page 20).

» Configure your firewall to allow GFI LanGuard to connect to GFI servers and to the remote machines to be monitored. For more information, refer to Firewall Ports and Protocols (page 22).

» Disable third-party antivirus during the installation process.

» Save any pending work and close all open applications on the machine.

2.4.2 Installation procedure

1. Log in using administrator credentials on the machine where you want to install GFI LanGuard.

2. Right-click the GFI LanGuard installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the GFI LanGuard installer.

4. Select the language for your installation and click **OK**

NOTES

» The GFI LanGuard Central Management Server and all GFI LanGuard instances joined to it need to be installed in the same language.

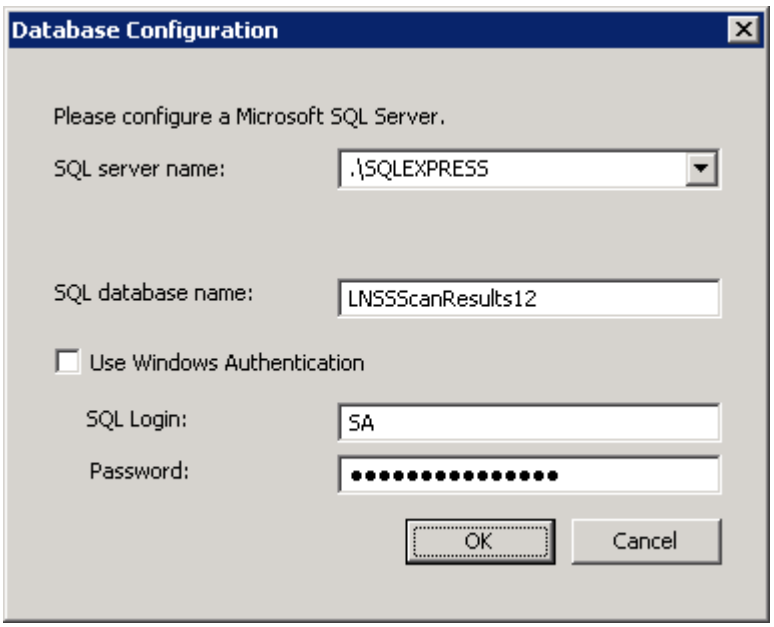
» The graphical user interface of the GFI LanGuard Central Management Server is available only in English, including in instances when GFI LanGuard is installed in another language.

Screenshot 8: Select components to be installed

5. From the list of components, select **GFI LanGuard** and click **Next**. The installation wizard will automatically download and install any missing components.

NOTE
An Internet connection is required to download missing components.

6. In the **Username** and **Password** fields, enter your GFI Accounts area credentials or the account used when signing up to download GFI LanGuard. Click **Sync** to retrieve the license keys registered to your account. Choose a key from the **Available keys** drop-down. If you do not have a GFI account or if you do not have a license key, click **Sign up here** and fill in the registration form. You may also manually specify a license key in the **Enter license key** field. Click **OK** when a valid license is specified. For more information, refer to Obtaining a GFI LanGuard subscription (page 34).



Screenshot 9: Configure the database server

7. In the database server configuration window provide the following details:

OPTION	DESCRIPTION
Database server name	The name of the Microsoft SQL server where the GFI LanGuard database is hosted.
SQL database name	Displays the database name. GFI LanGuard keeps the default name of the database. During an upgrade, you may decide to specify a different database name so that you can use a clean database while maintaining the old database from a previous version.
Use Windows Authentication	Select this option if you want the GFI LanGuard to use the Microsoft Windows credentials of the currently logged in user when connecting to the Microsoft SQL database.
Username / Password	If GFI LanGuard is not using Windows Authentication when connecting to the Microsoft SQL database, provide the username and password to be able to connect to the database.

8. In the GFI LanGuard welcome screen, click **Next**.

Screenshot 10: End-user license agreement

9. Read the licensing agreement carefully. To proceed with the installation, select **I accept the terms in the License Agreement** and click **Next**.

Screenshot 11: Attendant service credentials

10. Key in the administrator credentials and password. The credentials are used for the service account under which scheduled operations run. Click **Next**.

NOTE
It is highly recommended to provide a valid username and password and not to skip this option. Scan and remediation processes will fail if the credentials do not have permission on the remote machines.

11. Click **Install** to install GFI LanGuard in the default location or **Browse** to change the path.

12. Click **Finish** to finalize the installation.

When launched for the first time, GFI LanGuard automatically enables auditing on the local computer and scans the local computer for vulnerabilities. On completion, the GFI LanGuard **Home** page displays the vulnerability result.

NOTES
Test your installation after the product is installed. For more information, refer to Testing the installation (page 38).

2.4.3 Obtaining a GFI LanGuard subscription

During the GFI LanGuard installation, you are requested to key in your GFI account credentials or a license key.

Choose the procedure that best describes your scenario for information on how to obtain a subscription:

Evaluating GFI LanGuard for 30 days

For a free GFI LanGuard trial for 30 days:

1. Fill in the registration form at https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-lan-guard/download

2. Check your mail box and open the email from sales@gfi.com.

3. Click the link provided to confirm your account details and to create a password for your GFI Account.

4. After confirming your account details, the installer is automatically downloaded.

5. During the installation process, provide your GFI account credentials.

I have a GFI Account and want to install GFI LanGuard for the first time

During installation, key in the username and password associated with your account and verify that the account is valid.

Your license status can also be verified from the GFI Accounts Portal. Login to https://accounts.gfi.com and click **My products**. Select GFI LanGuard to check the status of your license.

Upgrading to a newer build or Service Release of the same version

When upgrading GFI LanGuard to a build of the same version, such as when installing a Service Release, you have two options to enter a license:

Enter your GFI account credentials or select a license key from the **Available keys** list.

If you don't have access to your previous license key, but you have a GFI account, you can retrieve the license key from the GFI Accounts portal. Login to https://accounts.gfi.com and click **My products**. Select GFI LanGuard to get your license key.

Upgrading to a newer version of GFI LanGuard

When upgrading your current installation to a newer major version, there are two scenarios:

» If using GFI Accounts, enter your credentials.

» If using a license key, upgrade your key:

Log in to the GFI Customer Area on https://customers.gfi.com/.

- If you have a valid GFI LanGuard maintenance agreement, click the blue key icon on the right and select **Upgrade License Key** to upgrade your license key. Then, key in your upgraded license key.
- If you do not have a valid GFI LanGuard maintenance agreement, click on the blue key icon on the right and select **Renewal**. Then, renew your maintenance agreement. On completion a new license key is available.

2.5 Upgrading GFI LanGuard

Choose your current GFI LanGuard version for notes and instructions on how to upgrade to the latest version while retaining all settings:

» GFI LanGuard 12.1

» GFI LanGuard 12

» GFI LanGuard 2015 and earlier

To determine your current version number open the GFI LanGuard console click  and navigate to **Help > About**.

2.5.1 Upgrading from GFI LanGuard 12.1 or later

This topic describes how to upgrade a GFI LanGuard version 12.1 or later installation to the latest version while retaining all settings.

Important notes before upgrading

» GFI LanGuard 12.2 supports TLS 1.1. If you plan to deploy GFI LanGuard in an environment where TLS 1.1 and above is running, you need to enable FIPS-Compliant algorithms on the local policy. For more information, refer to GFI LanGuard and TLS 1.1 or higher (page 21).

» Ensure your server meets the system requirements.

» Backup your current GFI LanGuard database and the GFI LanGuard Data directory which is typically available from: `C:\ProgramData\GFI\LanGuard <version>\`

» Export the GFI LanGuard settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to Importing and exporting GFI LanGuard settings (page 27).

» Log on to your current GFI LanGuard server as an Administrator or use an account with administrative privileges.

» Save any pending work and close all open applications on the machine before starting the upgrade.

» Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

Upgrade procedure

1. Download the latest build of GFI LanGuard on the server where GFI LanGuard is currently installed. Go to http://go.gfi.com/?pageid=lan_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the installer.

4. In the components screen, select **GFI LanGuard** to install a local server instance. You may optionally select **GFI LanGuard Central Management Server** to install a central server instance. Install only one instance of the Central Management Server within your organization.

5. Follow the wizard steps to install the new version.

6. On update completion, test your installation by running a scan to ensure GFI LanGuard installed successfully.

2.5.2 Upgrading from GFI LanGuard 12

This topic describes how to upgrade a GFI LanGuard version 12 installation to the latest version while retaining all settings.

Important notes before upgrading

» GFI LanGuard 12.1 introduces the Central Management Server for GFI LanGuard instances installed in another language. GFI LanGuard Central Management Server brings together the management of multiple GFI LanGuard instances through a common console, enabling you to manage many more devices. You can install this component on the local server while running the upgrade process. Install only one instance of the Central Management Server within your organization. Note that this component can be installed on any machine within the organization and has different system requirements than the product.

» GFI LanGuard 12.2 supports TLS 1.1. If you plan to deploy GFI LanGuard in an environment where TLS 1.1 and above is running, you need to enable FIPS-Compliant algorithms on the local policy. For more information refer to Support for TLS 1.1

» Ensure your server meets the system requirements.

» Backup your current GFI LanGuard database and the GFI LanGuard Data directory which is typically available from: `C:\ProgramData\GFI\LanGuard <version>\`

» Export the GFI LanGuard settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to Importing and exporting GFI LanGuard settings (page 27).

» Log on to your current GFI LanGuard server as an Administrator or use an account with administrative privileges.

» Save any pending work and close all open applications on the machine before starting the upgrade.

» Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

Upgrade procedure

1. Download the latest build of GFI LanGuard on the server where GFI LanGuard is currently installed. Go to http://go.gfi.com/?pageid=lan_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the installer.

4. In the components screen, select **GFI LanGuard** to install a local server instance. You may optionally select **GFI LanGuard Central Management Server** to install a central server instance. Install only one instance of the Central Management Server within your organization.

5. Follow the wizard steps to install the new version.

6. On update completion, test your installation by running a scan to ensure GFI LanGuard installed successfully.

2.5.3 Upgrading from GFI LanGuard 2015 or earlier

This topic describes how to upgrade a GFI LanGuard version 2015 or earlier installation to the latest version while retaining all settings.

The upgrade can be performed for the following versions:

» GFI LanGuard 2015

» GFI LanGuard 2014

» GFI LanGuard 2012

Important notes before upgrading

» Log in to the GFI Customer Area to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.

» GFI LanGuard 12 introduces the Central Management Server. GFI LanGuard Central Management Server brings together the management of multiple GFI LanGuard instances through a common console, enabling you to manage many more devices. You can install this component on the local server while running the upgrade process. Install only one instance of the Central Management Server within your organization. Note that this component can be installed on any machine within the organization and has different system requirements than the product.

» Installation on Windows Server 2003, Windows Small Business Server 2003 or Windows XP are no longer supported. Install the latest version of GFI LanGuard on a supported OS and then import the settings from your current installation to the new instance. For more information, refer to Importing and exporting GFI LanGuard settings (page 27).

» GFI LanGuard 12 does not support Microsoft SQL Server 2005 or earlier versions. If using an unsupported version it is recommended to install a supported version and move your current GFI LanGuard database to the new SQL server. Configure your current GFI LanGuard instance to use the new database and proceed to upgrade GFI LanGuard.

» GFI LanGuard 12 does not support Microsoft Access database. If using a Microsoft Access database, on running the upgrade, GFI LanGuard can be configured to use an existing SQL Server or SQL Express. Alternatively the wizard can install Microsoft SQL 2012 Express for free on the local server.

» Ensure your server meets the system requirements.

» Backup your current GFI LanGuard database and the GFI LanGuard Data directory which is typically available from: `C:\ProgramData\GFI\LanGuard <version>\`

» Export the GFI LanGuard settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to Importing and exporting GFI LanGuard settings (page 27).

» Log on to your current GFI LanGuard server as an Administrator or use an account with administrative privileges.

» Save any pending work and close all open applications on the machine before starting the upgrade.

» Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

Upgrade procedure

1. Download the latest build of GFI LanGuard on the server where GFI LanGuard is currently installed. Go to http://go.gfi.com/?pageid=lan_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the installer.

4. In the components screen, select **GFI LanGuard** to install a local server instance. You may optionally select **GFI LanGuard Central Management Server** to install a central server instance. Install only one instance of the Central Management Server within your organization.

5. After specifying your account's license key, the wizard prompts you to choose an existing Microsoft SQL Server or SQL Express. Alternatively click the option to install Microsoft SQL Express (free) on the local server. Follow the Microsoft SQL Express 2012 wizard.

6. Follow the wizard steps to install the new version side-by-side to your old version.

7. On launching GFI LanGuard the first time, you will be asked to import the configuration from the old instance. Choose the settings to import and click **Next**.

8. On import completion, test your installation by running a scan to ensure GFI LanGuard installed successfully. When the operation of the new version is confirmed, you may proceed to uninstall the old version from Windows Programs and Features.

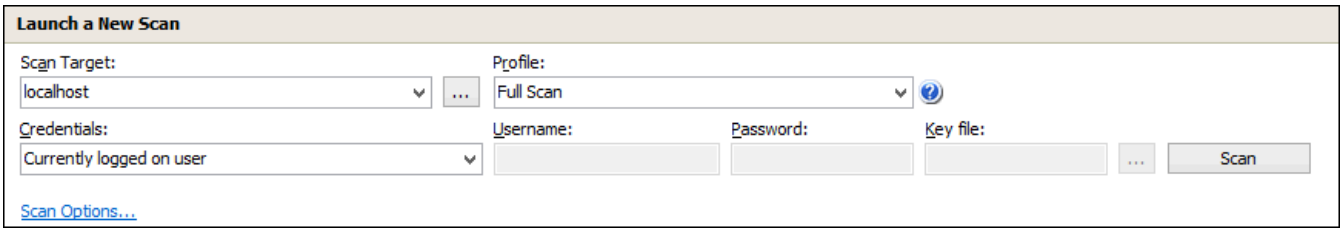
2.6 Testing the installation

Once GFI LanGuard is installed, test your installation by running a local scan to ensure it installed successfully.

1. Launch GFI LanGuard.

Screenshot 12: Launch a scan

2. From GFI LanGuard home page, click **Launch a Scan**.



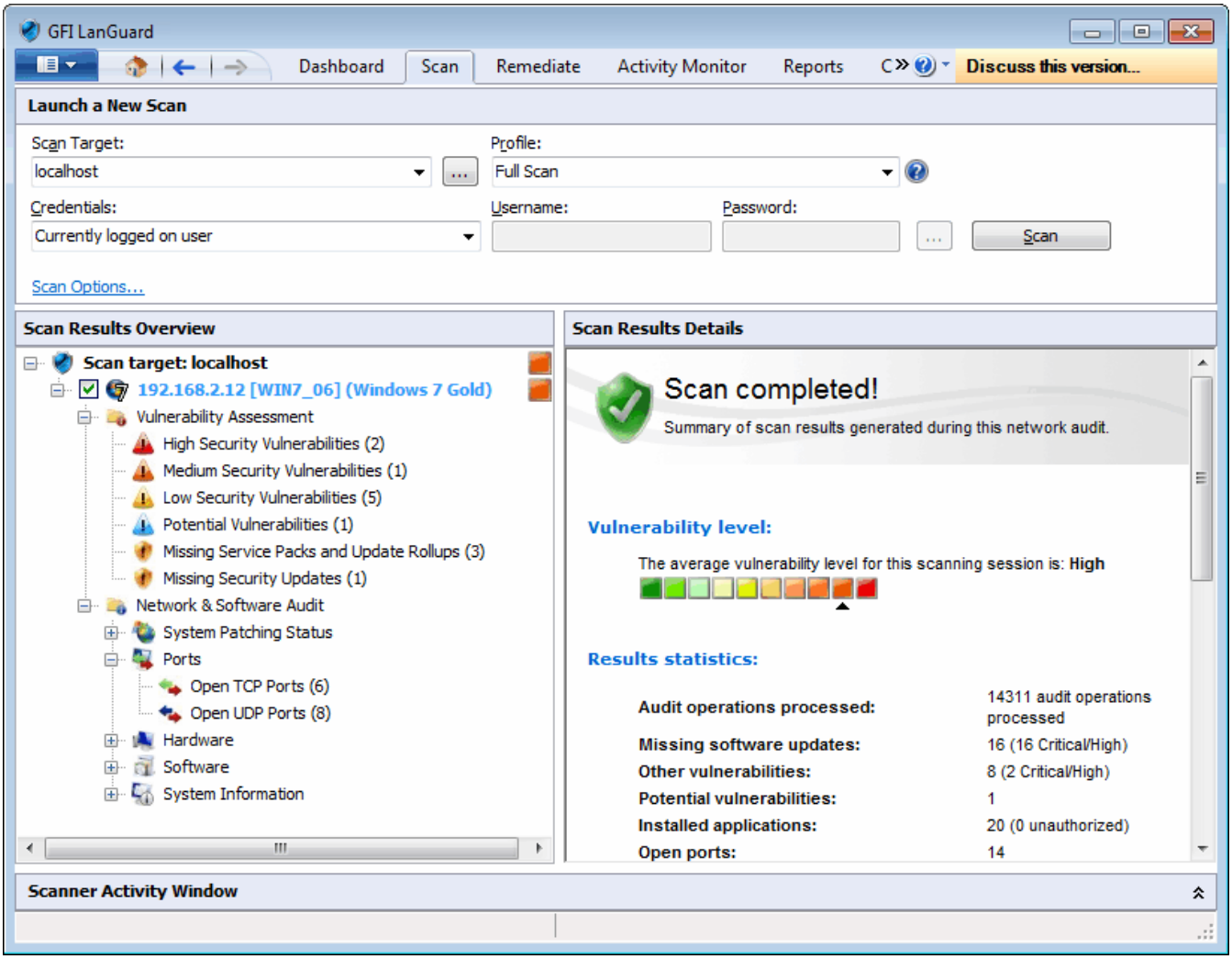
Screenshot 13: Launch a scan properties

3. From **Scan Target** drop–down menu, select **localhost**.

4. From **Profile** drop–down menu, select **Full Scan**.

5. Click **Scan** to start the scan on the local computer.

6. The scan progress is displayed in the **Scan** tab.



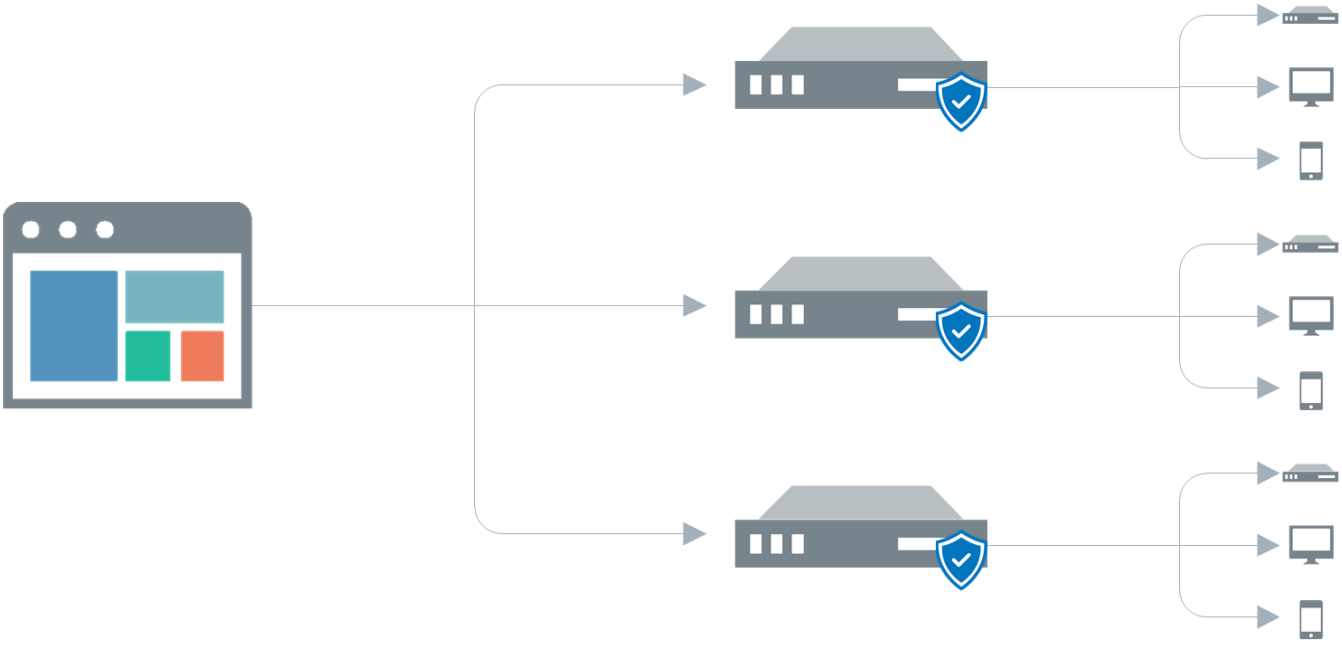
Screenshot 14: Scan results summary

7. On completion, the **Progress** section will display an overview of the scan result.

8. Use the **Scan Results Details** and **Scan Results Overview** to analyze the scan result. For more information, refer to Interpreting scan results (page 151).

3 GFI LanGuard Central Management Server

With GFI LanGuard Central Management Server, multiple GFI LanGuard instances installed in separate locations can be brought together through a common console. The GFI LanGuard Central Management Server console offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances. It also offers centralized reporting and visibility by capturing data from the various deployments of GFI LanGuard.



GFI LanGuard Central Management Server is used only for reporting. Scans and remediation take place only in GFI LanGuard and then information is centralized to GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard. Synchronization usually takes a few minutes. Delay depends on network size and amount of data being transferred.

NOTES

» The GFI LanGuard Central Management Server and all GFI LanGuard instances joined to it need to be installed in the same language.

» The graphical user interface of the GFI LanGuard Central Management Server is available only in English, including in instances when GFI LanGuard is installed in another language.

3.1 Installing GFI LanGuard Central Management Server

GFI LanGuard Central Management Server uses the same installation file of GFI LanGuard. Before starting the installation ensure that the system requirements are met. For more information, refer to Central Management Server system requirements (page 41).

3.1.1 Central Management Server system requirements

Computers running GFI LanGuard Central Management Server must meet the system requirements described below.

Hardware requirements

Computers hosting GFI LanGuard Central Management Server must meet the following minimum hardware requirements:

Component	Requirement
Processor	2.8 GHz quad-core
Physical Storage	10 GB HDD free space
RAM	8 GB RAM

Supported operating systems (32-bit/64-bit)

The following table lists operating systems and versions where the GFI LanGuard Central Management Server can be installed. Ensure that these operating systems are running the latest Service Pack as provided by Microsoft.

Operating System
Windows® Server 2016
Windows® Server 2012 (including R2)
Windows® Server 2008 (including R2) Standard/Enterprise
Windows® 10 Professional/Enterprise
Windows® 8/8.1 Professional/Enterprise
Windows® 7 Professional/Enterprise/Ultimate
Windows® Vista Business/Enterprise/Ultimate
Windows® Small Business Server 2011

Supported databases

GFI LanGuard Central Management Server uses a database to store information retrieved from multiple GFI LanGuard installations. The database backend can be any of the following:

Database server	Recommended Use
SQL Server Express® 2008 or later	This database server has a 10GB limit and is therefore recommended for networks containing up to 500 computers. If a database server is not available, the GFI LanGuard installer can automatically download and run the Microsoft SQL Express installer.
SQL Server® 2008 or later	Recommended for larger networks containing 500 computers or more.

For improved performance, it is highly recommended to use an SSD drive for the database server. Compared to traditional Hard Disk Drives, SSDs deliver superior performance with lower access time and lower latency.

Firewall Ports and Protocols

GFI LanGuard instances communicate with the GFI LanGuard Central Management Server via port **1077**. Configure your

firewall to allow **inbound** connections on TCP port **1077**, on computers running GFI LanGuard and the GFI LanGuard Central Management Server.

If port 1077 is already in use by another application, the GFI LanGuard Central Management Server automatically searches for an available port in the range of **1077-1277**.

Antivirus & Backup exclusions

Antivirus & backup software can cause GFI LanGuard to malfunction if it is denied access to some of its files.

Add exclusions that prevent antivirus & backup software from scanning or backing up the following folder on the GFI LanGuard server, Agents, Relay Agents and the GFI LanGuard Central Management Server: <system drive>\ProgramData\GFI\

3.1.2 Installing Central Management Server

To install GFI LanGuard Central Management Server:

1. Logon using administrator credentials on the machine where to install GFI LanGuard Central Management Server.

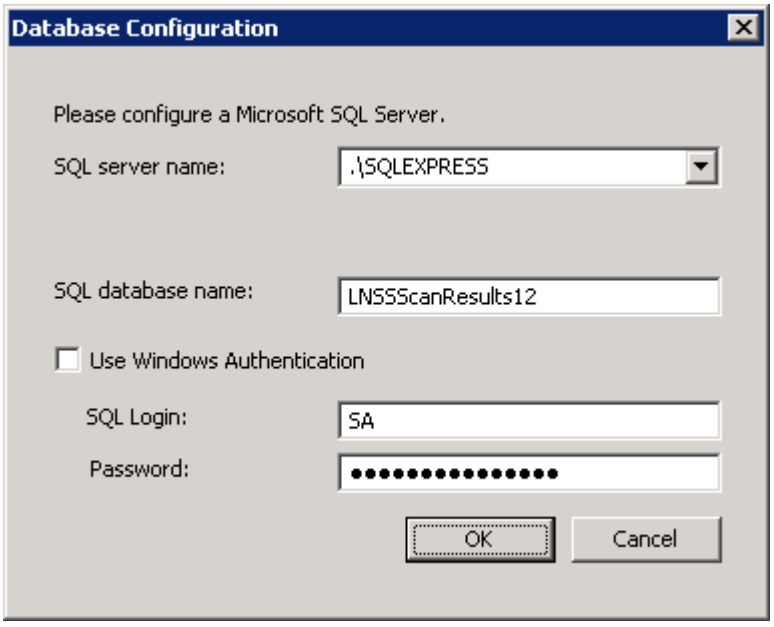
> **NOTE**
> If you are installing both GFI LanGuard and GFI LanGuard Central Management Server on the same machine, the installation wizard will first guide you to install GFI LanGuard. For more information, refer to Installing GFI LanGuard (page 30).

2. Launch the setup and select the installation language.

> **NOTES**
>
> » The GFI LanGuard Central Management Server and all GFI LanGuard instances joined to it need to be installed in the same language.
>
> » The graphical user interface of the GFI LanGuard Central Management Server is available only in English, including in instances when GFI LanGuard is installed in another language.

Screenshot 15: Select components to be installed

3. Ensure GFI LanGuard Central Management Server is selected in the components list and click **Next**.



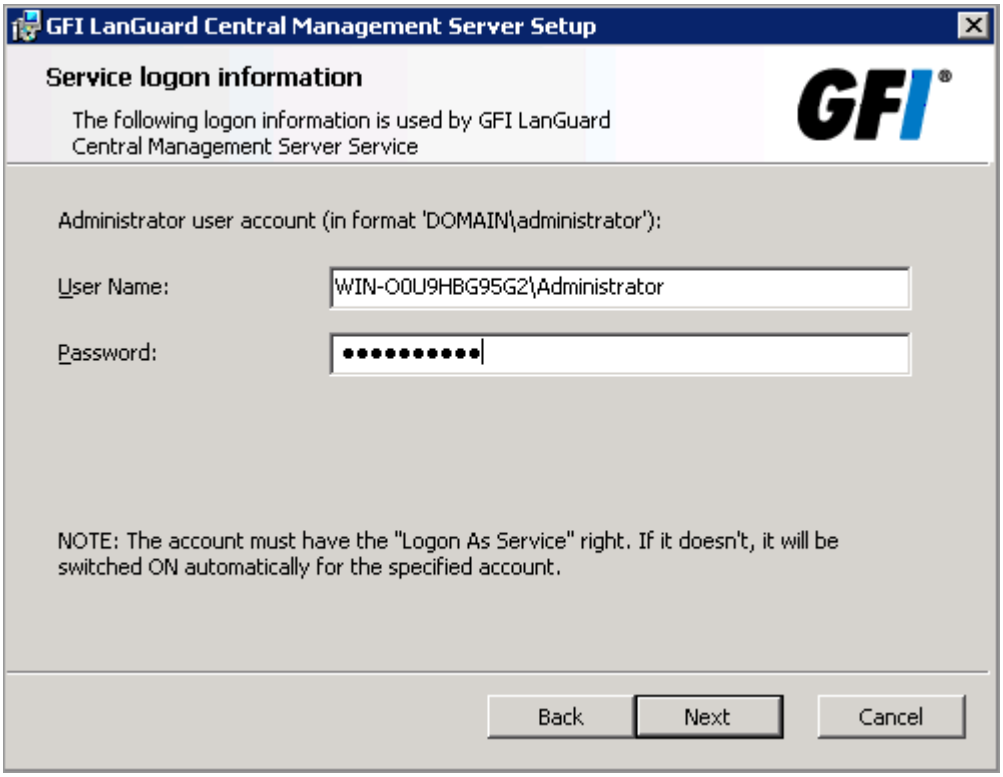
Screenshot 16: Configure the database server

4. In the database server configuration window provide the following details:

OPTION	DESCRIPTION
Database server name	The name of the Microsoft SQL server where the GFI LanGuard Central Management Server database is hosted.

OPTION	DESCRIPTION
Use Windows Authentication	Select this option if you want the GFI LanGuard Central Management Server to use the Microsoft Windows credentials of the currently logged in user when connecting to the Microsoft SQL database.
Username / Password	If GFI LanGuard Central Management Server is not using Windows Authentication when connecting to the Microsoft SQL database, provide the username and password to be able to connect to the database.

5. Read the licensing agreement carefully. To proceed with the installation, select **I accept the terms in the License Agreement** and click **Next**.



Screenshot 17: Key in credentials for the Windows service

6. In the Service logon information screen, key in the administrator credentials and password for the Windows service under which scheduled operations run. Click **Next** to continue setup.

7. Click **Install** to install GFI LanGuard Central Management Server in the default location or **Browse** to change path.

8. Click **Finish** to finalize installation.

3.1.3 Uninstalling Central Management Server

To uninstall GFI LanGuard Central Management Server

1. Click **Start > Control Panel > Programs > Programs and Features**.

2. Select GFI LanGuard Central Management Server from the list, and click **Uninstall**.

3. When **Are you sure you want to uninstall** GFI LanGuard Central Management Server**?** appears, click **Yes**.

4. On completion, click **Finish**.

3.2 Joining GFI LanGuard to Central Management Server

The GFI LanGuard Central Management Server provides centralized reporting for multiple GFI LanGuard instances. However, each and every GFI LanGuard instance needs to be manually configured to point to a GFI LanGuard Central Management Server to avail yourself of this feature.

NOTES

» The GFI LanGuard Central Management Server and all GFI LanGuard instances joined to it need to be installed in the same language.

» The graphical user interface of the GFI LanGuard Central Management Server is available only in English, including in instances when GFI LanGuard is installed in another language.

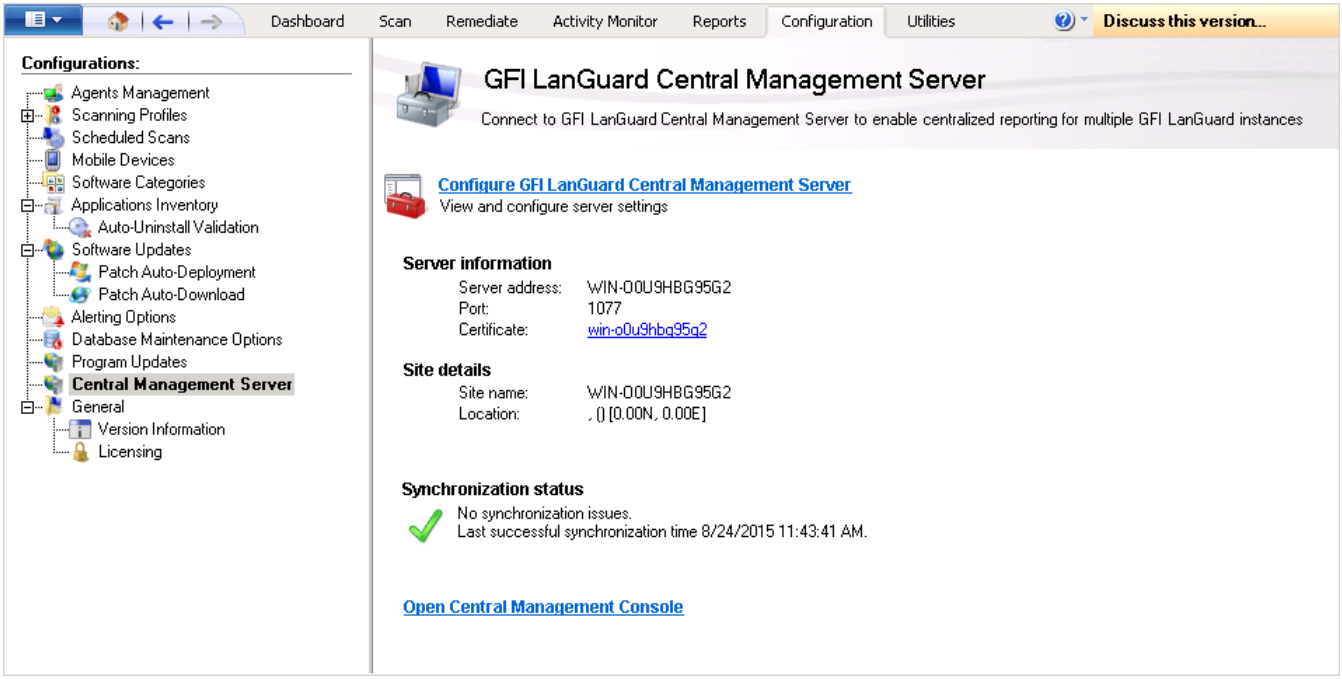
GFI LanGuard Central Management Server is used only for reporting. Scans and remediation take place only in GFI LanGuard and then information is centralized to GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard. Synchronization usually takes a few minutes. Delay depends on network size and amount of data being transferred.

NOTE

GFI LanGuard Central Management Server requires a Microsoft SQL or SQL Express database. If this is not configured, click the provided link or navigate to **Database Maintenance Options > Database backend settings** to set up an SQL Database. For more information, refer to Configuring Database Maintenance Options (page 236).

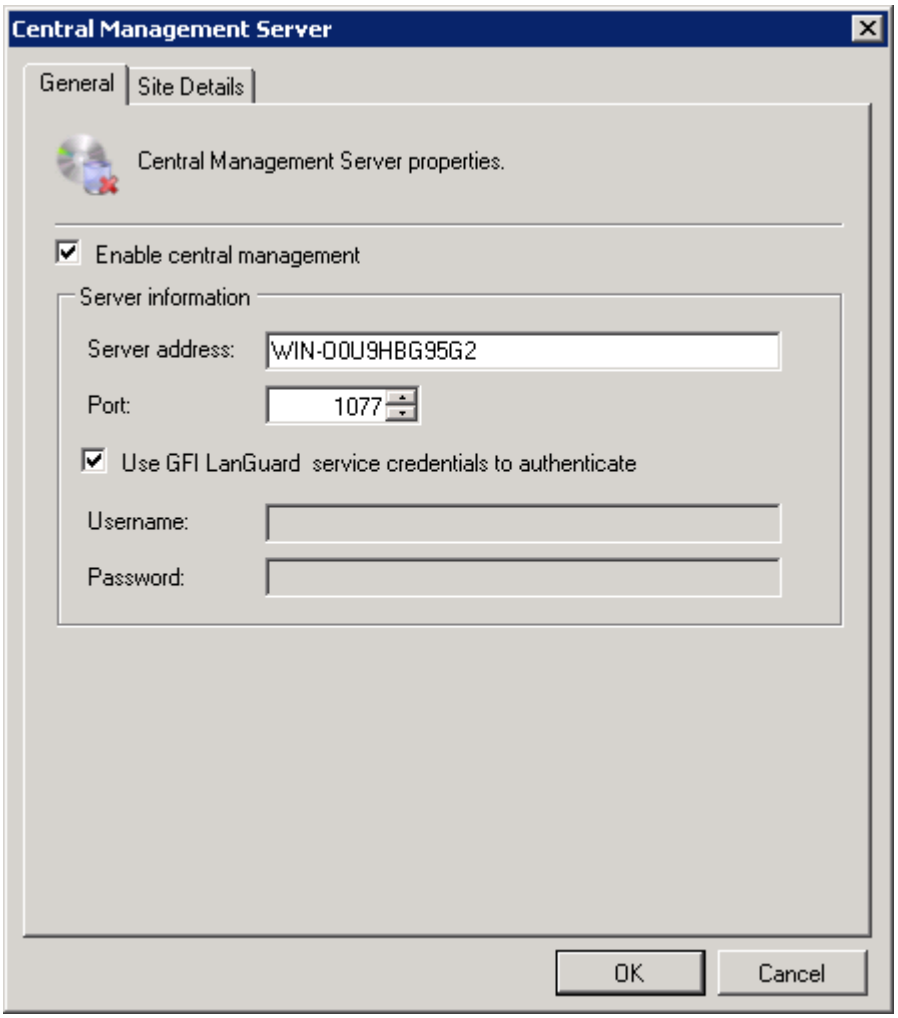
To configure Central Management Server options:

1. Click **Configuration** tab **> Central Management Server**.



Screenshot 18: The GFI LanGuard Central Management Server page

2. Click **Configure** GFI LanGuard Central Management Server.

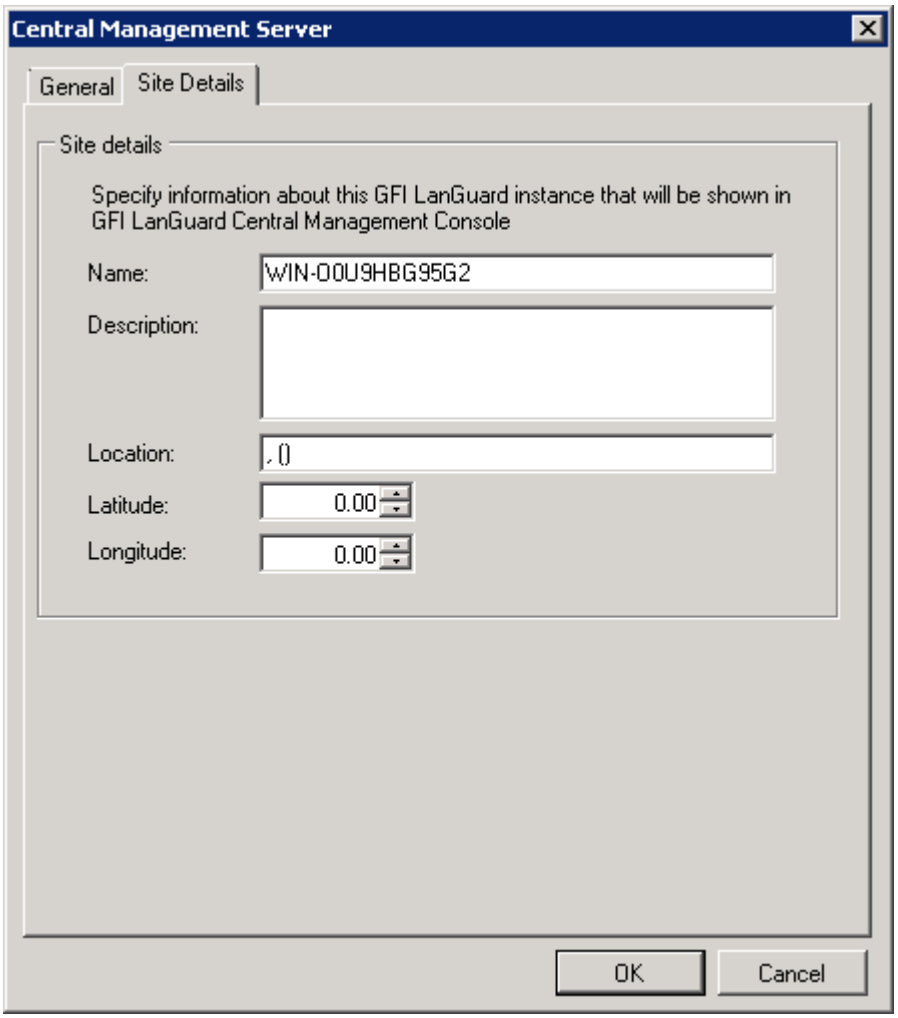


Screenshot 19: Central Management Server dialog - General tab

3. From the **General** tab, configure the following options:

Option	Description
Enable central management	Click to enable GFI LanGuard Central Management Server. Also enables you to provide the server IP address and port on which this instance of GFI LanGuard will communicate with GFI LanGuard Central Management Server.
Use GFI LanGuard service credentials to authenticate	Enables you to use the GFI LanGuard service credentials provided during setup to authenticate with GFI LanGuard Central Management Server. This is enabled by default. If disabled, you will need to provide a username and a password to be used with GFI LanGuard Central Management Server.

4. Click **Site Details** to continue setup



Screenshot 20: Central Management Server dialog - Site Details tab

5. In the **Site Details** tab, provide the site details that will be shown in GFI LanGuard Central Management Server. These include the name of this GFI LanGuard instance, a description, the location name and the latitude and longitude values.

3.3 Configuring GFI LanGuard Central Management Server

The following topics help you configure GFI LanGuard Central Management Server:

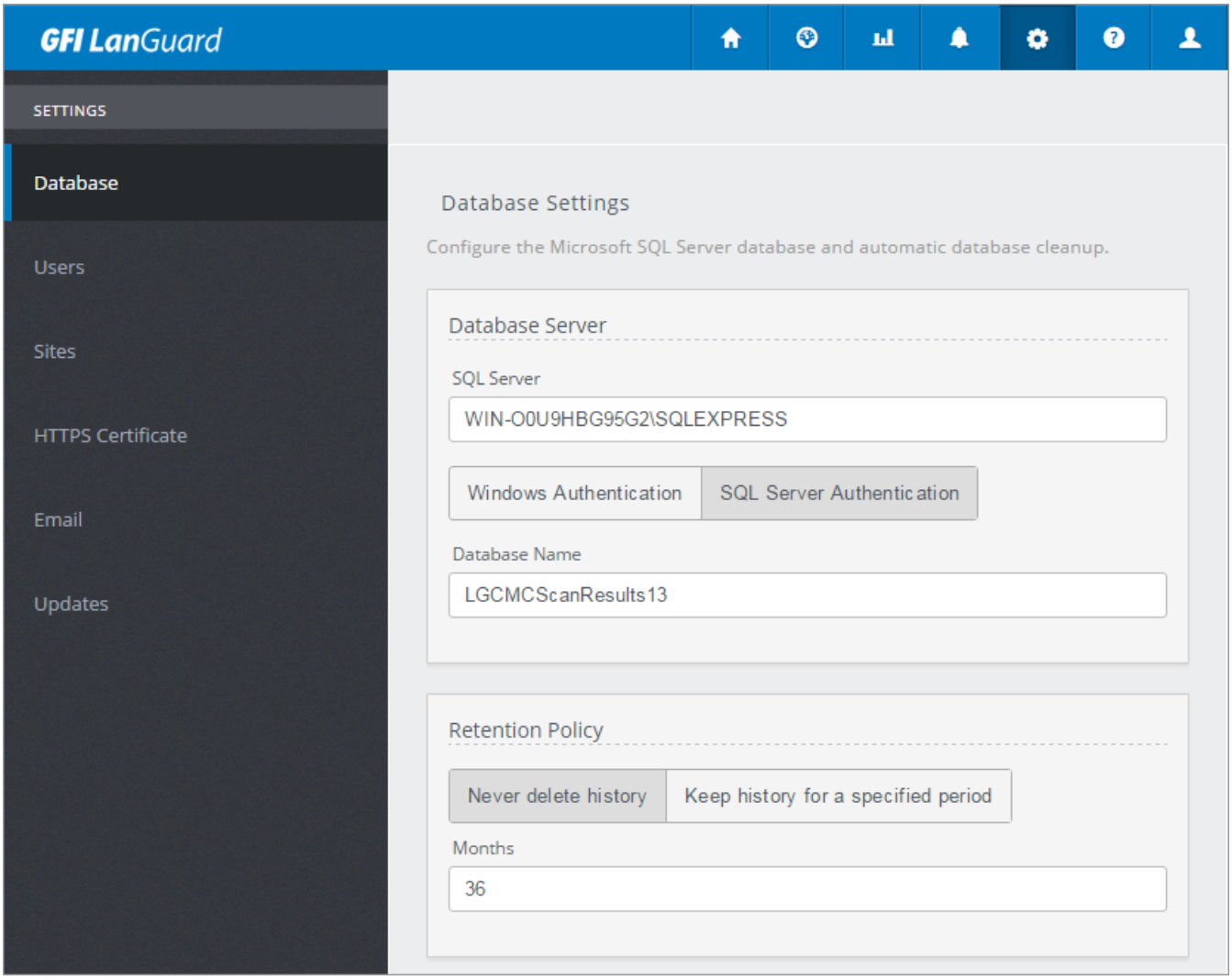
3.3.1 Configuring GFI LanGuard Central Management Server database settings

GFI LanGuard Central Management Server supports Microsoft SQL Server and SQL Server Express databases (2005 and later editions) that can be configured to store collected monitoring data. This data is used by GFI LanGuard Central Management Server to populate the dashboards and for reporting purposes.

The currently configured database can be viewed from **Settings > Database**. Here you can also specify data retention settings.

To change the current database configuration or create a new database:

1. In GFI LanGuard Central Management Server, go to **Settings > Database**.



Screenshot 21: Configuring Database settings for GFI LanGuard Central Management Server

2. Under the **Database Server** area, modify the following options:

OPTION	DESCRIPTION
SQL Server	The name of the SQL Server instance. Key in the name of the server where the database is installed.
Windows Authentication	Select this option to use Windows credentials when connecting to your SQL Server.

OPTION	DESCRIPTION
SQL Server Authentication	If your SQL Server has been installed in SQL Server Authentication Mode, select this option and provide **Username** and **Password**.
Database Name	If you want to create a new database, use this field to type the name of the database you want to create in SQL Server. **IMPORTANT** Ensure that the database name entered is unique, otherwise you will overwrite the existing database.

3.3.2 Specifying data retention settings

Retention policy settings define whether to keep all historical data stored in the configured database or whether to delete this data after a specified amount of time. By default, GFI LanGuard Central Management Server is set to keep historical data for a period of 36 months.

To change data retention settings:

1. In GFI LanGuard Central Management Server, go to **Settings > Database**.

2. Under the **Retention Policy** area, modify the following options:

Select from the following options:

OPTION	DESCRIPTION
Never delete history	Select to keep all data gathered by GFI LanGuard Central Management Server indefinitely. **NOTE** If selecting this option ensure adequate disk space on the server.
Keep history for a specified period	Select this option to delete collected data after a defined amount of time. Use the Months field to specify an amount in months. Default is 36.

3.3.3 Configuring Central Management Server user privileges

Use this area to configure user access rights to the GFI LanGuard Central Management Server Console. Configured users will be able to access the console from any location using an internet browser. GFI LanGuard Central Management Server uses Active Directory to authenticate users.

GFI LanGuard Central Management Server offers the following roles:

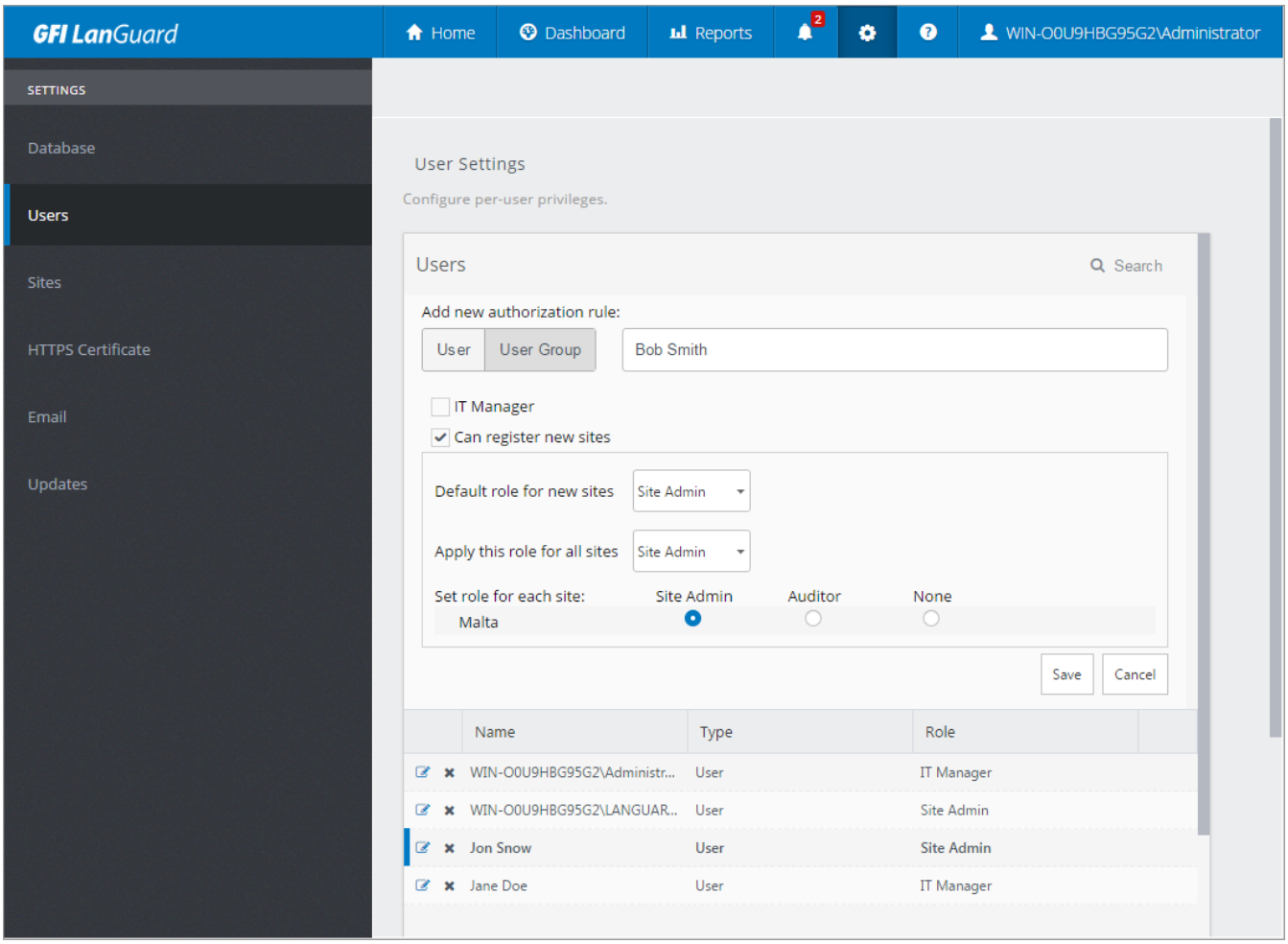
OPTION	DESCRIPTION
IT Manager	This role is made up of both the Site Admin and the Auditor roles and allows users full access to the GFI LanGuard Central Management Server.
Site Admin	Users with Site Admin rights are able to configure and manage the console.
Auditor	The auditor role permits users to access the reporting tools of GFI LanGuard Central Management Server Console and the Dashboards.

To add a new user:

1. In the top navigation bar, click the settings icon.

2. Select **Users**.

3. Click **Add User** icon.



Screenshot 22: Configuring user access rights to the GFI LanGuard Central Management Server Console

4. Select from the following options:

OPTION	DESCRIPTION
Search	Click the Search icon to expand a search field where you can key in a user or group name to search for.
User / User Group	Key in the name of an existing Active Directory User or Group of users. A list of existing users or groups is automatically displayed as you type. Select the desired name from the list.
IT Manager	Check the checkbox to assign the role of IT Manager to the user. This role gives users both Site Admin and Auditor rights.
Can register new sites	Select this option if you want the user to be able to register new sites with GFI LanGuard Central Management Server.
Default role for new sites	Set the default role for this user for new sites that are added to GFI LanGuard Central Management Server.
Apply this role for all sites	Select the role for the new user to apply to existing sites.
Set role for each site	Use the provided buttons if you want to manually set different roles for different sites. Use the drop down list to select one of the following options: **None**, **Auditor**, **Site Admin**.

5. Click **Save**.

3.3.4 Managing GFI LanGuard sites in Central Management Server

The Sites window lists all the GFI LanGuard instances that have been connected to the GFI LanGuard Central Management Server. The following details are listed:

OPTION	DESCRIPTION
Name	The name of the machine where the GFI LanGuard instance is installed.
Location	The location where the GFI LanGuard machine is located.
Last sync	The date when the GFI LanGuard instance last synced with the GFI LanGuard Central Management Server.
License usage	An amount showing the percentage used.
License expiry	The date when the current GFI LanGuard Central Management Server expires.
Status	Shows the current license status, for example whether it has been registered or expired.

IMPORTANT

New sites cannot be added through the GFI LanGuard Central Management Server console. The configuration needs to be carried out in GFI LanGuard as the GFI LanGuard Central Management Server cannot automatically detect GFI LanGuard instances. For more information refer to: http://go.gfi.com/?pageid=LGCMSSites

Editing site details

You can edit details of sites that have been connected to GFI LanGuard Central Management Server. To do this:

1. In the list of sites, click the edit icon next to the site to edit.

2. Select the **Identity and Sync Information** tab to edit the following details:

OPTION	DESCRIPTION
Name	The name of the site where a GFI LanGuard instance is located. You can replace this by a friendly name. This name will appear as alt text when hovering over markers in the home page.
Location	The name of the country where a GFI LanGuard instance is located.
Latitude / Longitude	Use the down and up arrows to manually set the latitude and longitude of the GFI LanGuard instance location.
Description	A description of the site, for example, Main Office.
Last Sync	This field contains the date and time of the last synchronization between the GFI LanGuard instance and GFI LanGuard Central Management Server which cannot be edited.

3. Select the **Authorized users** tab to edit the following details:

OPTION	DESCRIPTION
Site admins	Site admins are granted access to the configuration area of GFI LanGuard Central Management Server. Click the Add icon to add new users or groups.
Auditors	Auditors have access to reports and dashboard areas of the GFI LanGuard Central Management Server Console. Click the Add icon to add new users or groups.

NOTE

Users or groups configured in the Users area will be automatically added to these lists. For more information, refer to Configuring Central Management Server user privileges (page 49).

4. Select the **License information** tab to view additional information related to license usage and license expiry date.

5. Click **Save**.

3.3.5 Configuring HTTPS Certificate in Central Management Server

GFI LanGuard Central Management Server Console is accessed securely through HTTPS. This requires digital certificates for server authentication and communication encryption purposes. By default, GFI LanGuard Central Management Server Console uses a certificate issued during installation by a special-purpose Certificate Authority (CA) called **GFI LanGuard Central Management Console CA**. The web clients of GFI LanGuard Central Management Server Console are subsequently presented a certificate chain consisting of:

- A self-signed CA certificate issued by **GFI LanGuard Central Management Console CA**
- A certificate issued to the computer where the product is installed, having as subject the name of the computer

For any web browser or a GFI LanGuard instance to seamlessly connect to GFI LanGuard Central Management Server Console, the **GFI LanGuard Central Management Console CA** certificate needs to be trusted. Trust the CA certificate by adding it to the list of Trusted Certificate Authorities on client computers.

The **GFI LanGuard Central Management Console CA** creates a single certificate during installation. This certificate is then permanently disabled and the CA cannot issue more certificates. This makes it safe to add this CA to the list of Trusted Certificate Authorities on client computers.

Alternatively, if you already have a trusted certificate, you can use it instead of the default certificate generated by GFI LanGuard.

The following topics provide more information on how to implement Trusted Root Certificates:

Adding the CA Certificate as Trusted Certificate Authority

This topic describes how to download the CA certificate from within GFI LanGuard Central Management Server and how to install it as a Trusted Certificate Authority.

For Microsoft Internet Explorer, Google Chrome and Opera on Microsoft Windows

1. Open GFI LanGuard Central Management Server Console in your browser.

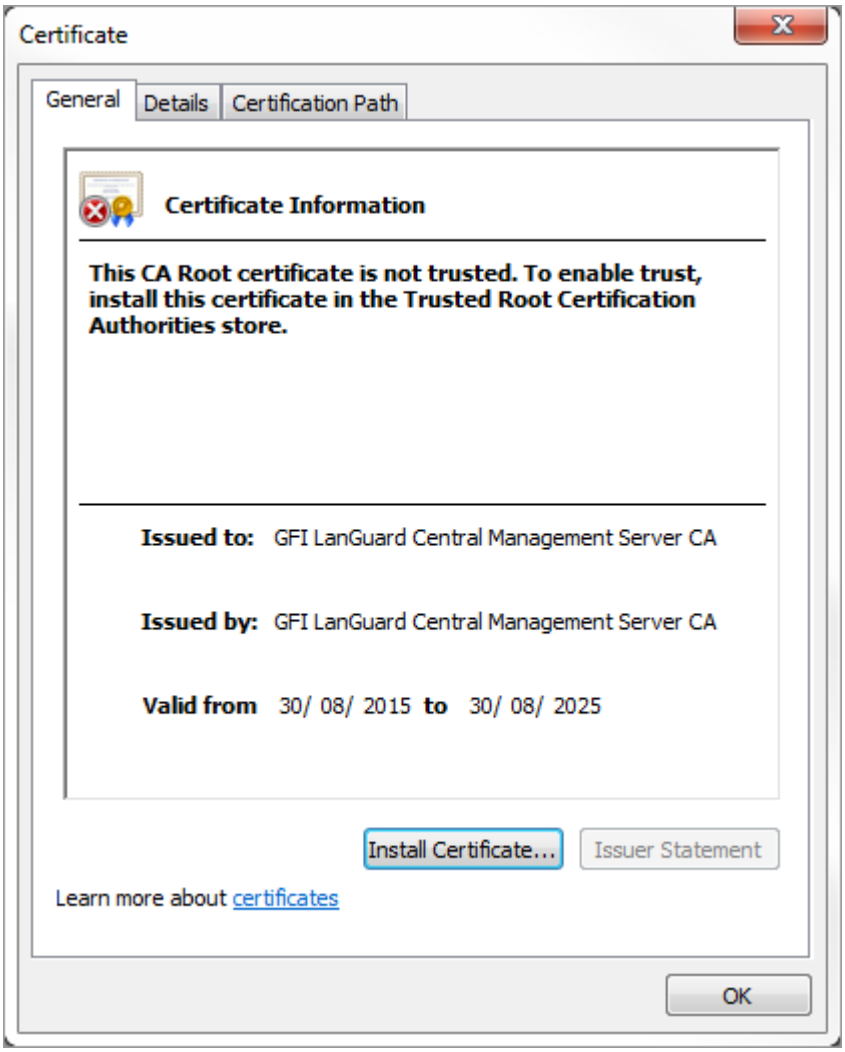
2. When you receive the certificate error in the browser, select **Continue to this website (not recommended)**.

3. Key in the authentication credentials.

4. From the top navigation menu click the **Settings** icon.

5. Select **HTTPS Certificate** and click **Download certificate**. The following file will be downloaded to your computer: `root.cer`.

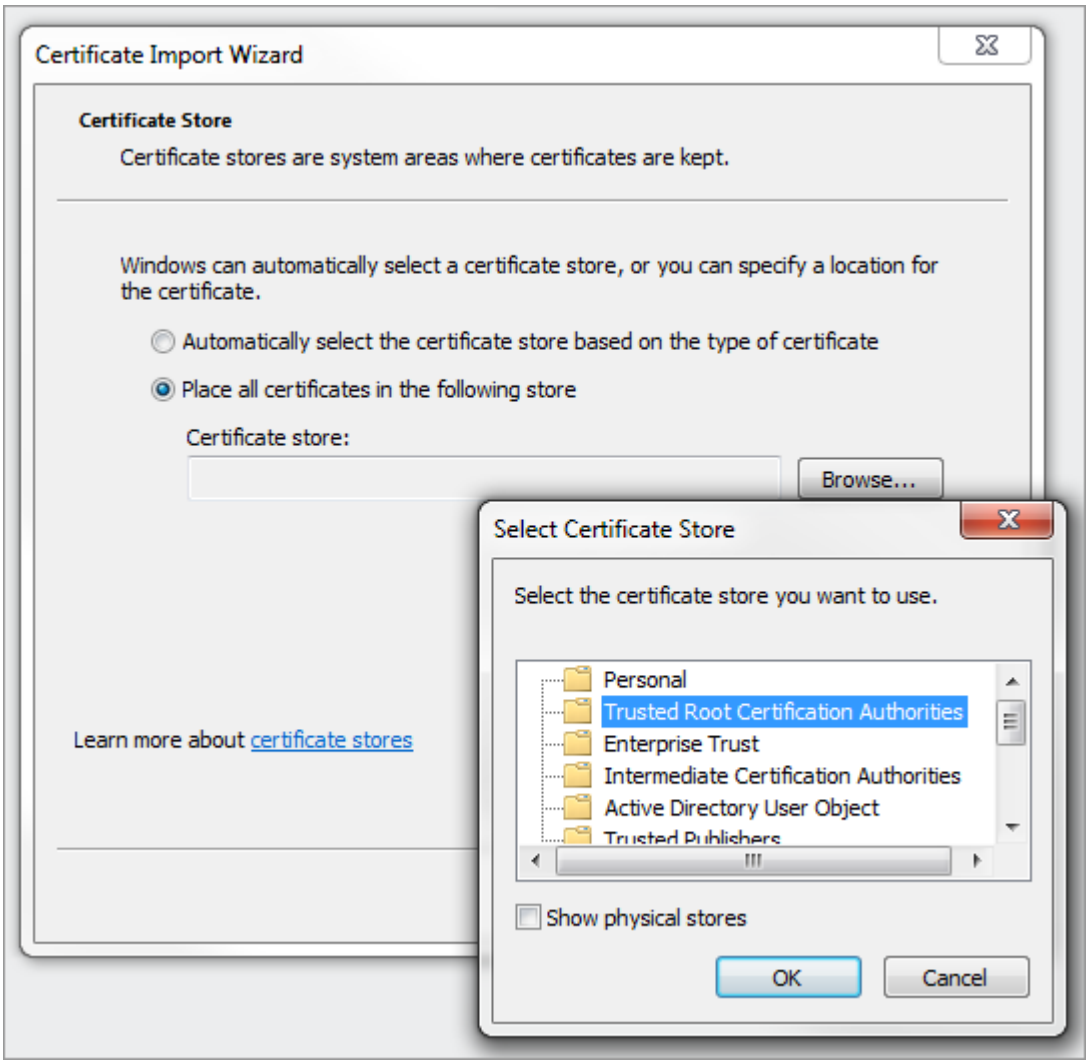
6. Locate the file and double-click to open.



Screenshot 23: Installing the CA Certificate

7. Click **Install Certificate…**.

8. In the Certificate Import Wizard, click **Next**.



Screenshot 24: Select location for imported certificate

9. Select **Place all certificates in the following store**, then click **Browse…** and select **Trusted Root Certification Authorities**. Click **OK**

10. Click **Next**.

11. Click **Finish**.

12. Click **OK** The CA Certificate is now trusted.

For Mozilla Firefox on any operating system

1. Open GFI LanGuard Central Management Server Console in your browser.

2. When you receive the certificate error in the browser, select **I Understand the Risks** then click **Add Exception…**.

3. In the **Add Security Exception** window, click **Confirm Security Exception**. This allows you to continue to the application.

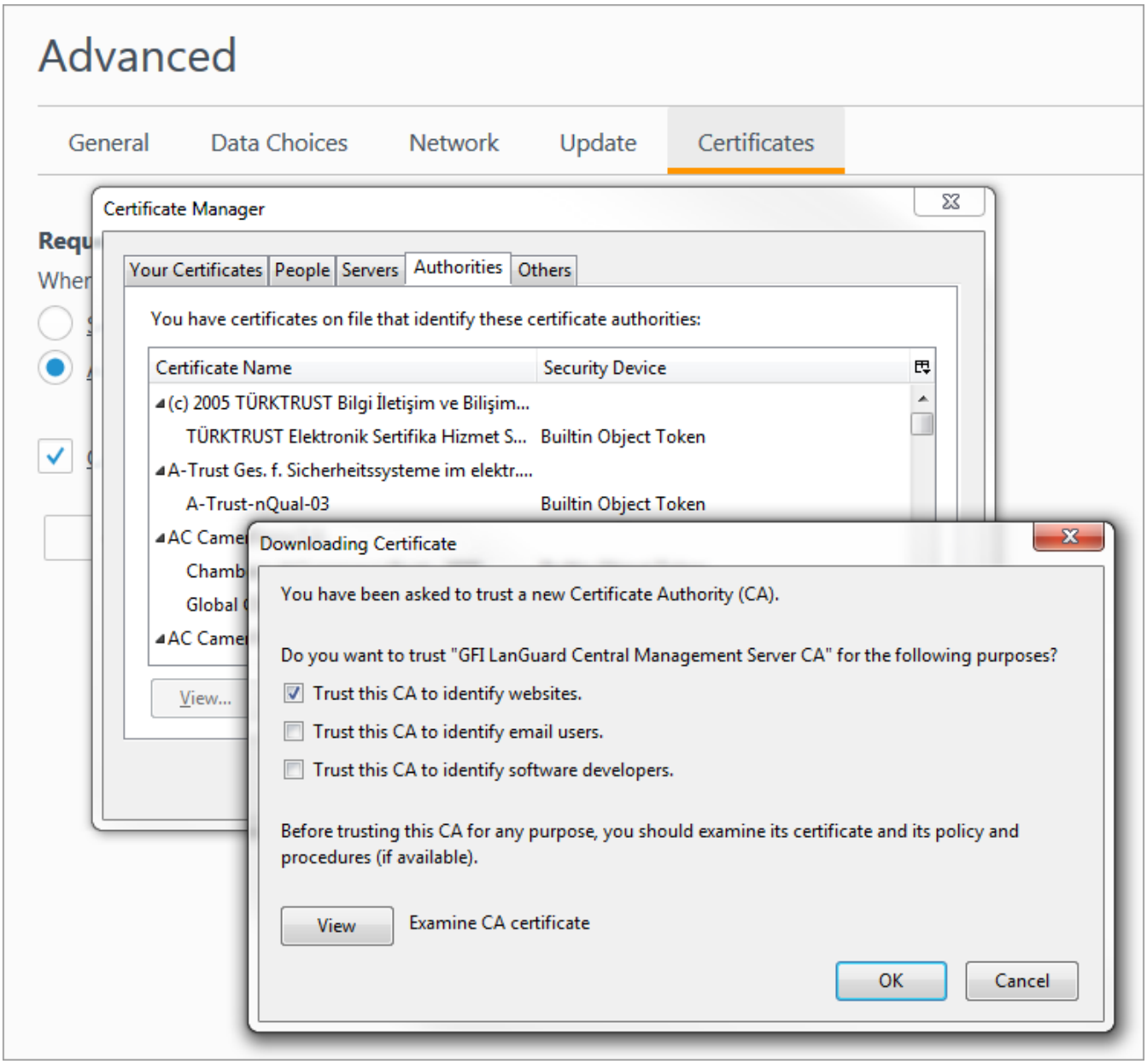
4. Key in the authentication credentials.

5. From the top navigation menu click the **Settings** icon.

6. Select **HTTPS Certificate** and click **Download certificate**. The following file will be downloaded to your computer: `root.pem`.

7. In Mozilla Firefox, go to **Settings > Options > Advanced > Certificates > View Certificates > Authorities tab** and click **Import…**.

8. Select the previously downloaded file `root.pem`.



Screenshot 25: Importing a trusted CA Certificate in Firefox

9. Select **Trust this CA to identify websites** and click **OK** to complete the import.

For Safari, Google Chrome and Opera on Apple OS X

1. Open GFI LanGuard Central Management Server Console in your browser.

2. When you receive the certificate error in the browser, select **Continue**. This allows you to continue to the application.

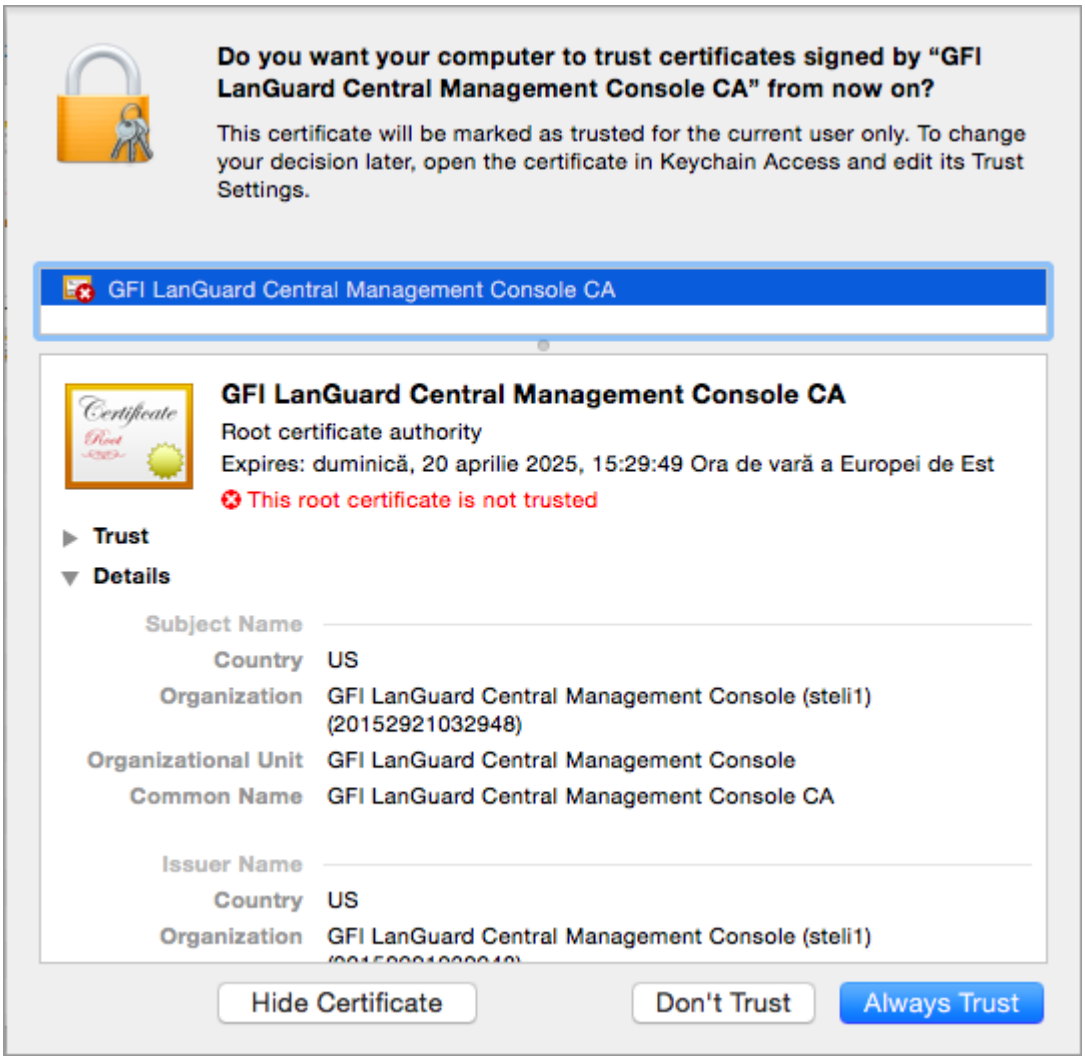
3. Key in the authentication credentials.

4. From the top navigation menu click the **Settings** icon.

5. Select **HTTPS Certificate** and click **Download certificate**. The following file will be downloaded to your computer: `root.p12`.

6. Open the downloaded file `root.p12` with Keychain Access.

7. Leave the Password field empty and select **OK**



Screenshot 26: Configuring a CA Certificate in Safari, Google Chrome and Opera on Apple OS X

8. Select **Always Trust**.

Using an existing SSL certificate in Central Management Server

GFI LanGuard Central Management Server can be configured to use existing SSL certificates. This allows you to leverage your existing trust infrastructure. Follow the steps below after installing GFI LanGuard Central Management Server:

1. Open Internet Information Services Manager (IIS Manager).

2. From the **Connections tree**, select your server.

3. In the right pane, open **Server Certificates**.

4. From the **Actions** menu, click **Import…**.

5. In the **Import Certificate** dialog, click **...** to browse and locate the PFX file which contains your existing SSL certificate.

6. If the certificate is password protected, key in the password and click **OK**

7. In the **Connections tree**, expand **Sites** and select **GFI LanGuard Central Management Server Website**.

8. From the **Actions** menu, click **Bindings…**

9. In the **Site Bindings** dialog, select **https** from the list and click **Edit…**.

10. In the SSL certificate field select your SSL certificate and click **OK**.

> **NOTE**
> Ensure your existing SSL certificate is trusted on all machines where GFI LanGuard is installed since GFI LanGuard requires the certification chain to be trusted by the operating system.

3.3.6 Email settings in Central Management Server

The Email settings page lets you configure alerting options. These are required when GFI LanGuard Central Management Server needs to send important administrative notifications. To configure sender and recipient details:

1. Click **Settings > Email**.

2. In the **SMTP Server Details** area, key in the parameters described below:

Option	Description
From email address	The sender email address. GFI LanGuard Central Management Server will use this email account to send the required emails.
SMTP Server	Key in the IP address of the server through which emails are routed.
Port	Define the port number through which emails are routed. Default value is 25
Authentication	Enable if SMTP server requires a username and password to authenticate when sending administrative notifications. Enter a username and password in the appropriate fields.
Use SSL	Select this option if you have an SSL (Secure Sockets Layer Protocol) encrypted connection to send the required emails.
Send notifications by email	Enable to send important administrative notifications via email.

3. In the **Email Recipients** area, key in the following:

Email Address	Emails sent by GFI LanGuard Central Management Server are received by the email addresses configured in this area. Key in the email address in the appropriate field and press the add icon. Add as many email addresses as required.
Verify Email Settings	Click **Verify Email Settings** to verify that email settings are configured correctly.

4. Click **Save**.

3.3.7 Configuring Central Management Server Updates

The Product Updates area displays information about version and build number of the currently installed GFI LanGuard Central Management Server instance as well as the history of installed updates. Product updates enable you to keep your GFI LanGuard Central Management Server installation up to date with the latest updates. When enabled, GFI LanGuard Central Management Server checks for new updates at specified intervals, downloads the updates, and installs them.

> **NOTE**
> During product updates the GFI LanGuard Central Management Server services need to be stopped and restarted. This action causes disruption with remote GFI LanGuard instances. Operations can resume once the services are restarted.

To configure system updates:

1. Go to **Settings > Updates**.

2. Configure the following:

OPTION	DESCRIPTION
Install updates automatically	When enabled, GFI LanGuard Central Management Server automatically checks for new updates, downloads newly found packages and installs them. Click **Customize** to specify a schedule for the updates.
Update Now	Click to make GFI LanGuard Central Management Server check for updates.
Download from alternative version	Enable this option if you want GFI LanGuard Central Management Server to check in a particular location when looking for new product updates. Specify the URL location where to look for in the available field.
Proxy Server	Enable if GFI LanGuard Central Management Server needs to connect to a specific Proxy Server to download updates. Provide the following details: **Proxy Address** - specify the IP address of the server from where GFI LanGuard Central Management Server will download the new updates. **Port** - Specify the port number used by GFI LanGuard Central Management Server to connect to the Proxy Server. Default is 8080. **Authentication** - if authentication is required, enable this option and provide the credentials of the target server.

3. Click **Save**.

3.4 Using the GFI LanGuard Central Management Server Console

The GFI LanGuard Central Management Server Console can be accessed by authorised users through any supported internet browser by using the following address:

`https://<server name/IP address>:1077/Home/Home`.

Different user access rights can be granted from the settings area. For more information, refer to Configuring Central Management Server user privileges (page 49).

The following topics provide information on how to use GFI LanGuard Central Management Server Console:

3.4.1 Central Management Server Home Page

The home page of the GFI LanGuard Central Management Server console offers two graphical overviews of relevant information collected from deployed GFI LanGuard instances at remote locations. To display the home page click **Home** in the top navigation.

Screenshot 27: The GFI LanGuard Central Management Server Home page

Toggle between the following views:

OPTION	DESCRIPTION
Sites Overview	A map displays GFI LanGuard instances that have been connected to the GFI LanGuard Central Management Server. High, Medium and Low markers define the vulnerability status of the sites at a glance, while an additional filter can be toggled to display the following: » Vulnerability Status » Auditing Status » Patch Management Status » License Usage

OPTION	DESCRIPTION
Top Sites	The Top Sites view offers an in-depth look at the status of top sites. The interactive info-graphic offers the following 4 nodes: » **Vulnerability Status** - View the number of vulnerabilities found on a site, grouped by severity. This area enables you to determine a site's vulnerability rating with high, medium and low percentages. You can also filter data by: • number of high vulnerability nodes • percentage of high vulnerability nodes • number of nodes » **Patch Management Status** - View sites that are missing updates. Filter by: • number of nodes having missing updates • percentage of nodes having missing updates • number of nodes » **Auditing Status** - identify how many audits have been performed in top sites grouped by time. Filter data by the following: • number of nodes not scanned last week • percentage of nodes not scanned last week • number of nodes not scanned last 24 hours • percentage of nodes not scanned last 24 hours • number of nodes » **License Usage** - Explore top sites by their license status. Available filters are: • license usage • license limit • number of nodes • expiry date

NOTE

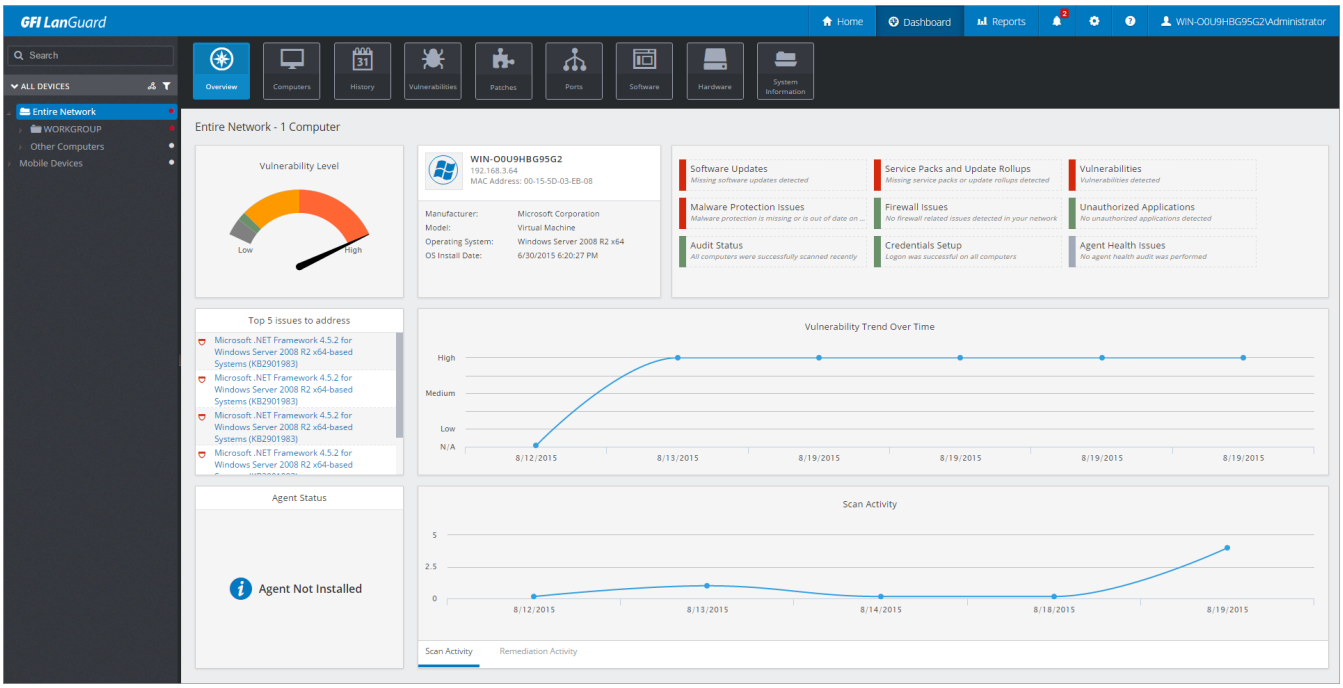
The sites displayed by the GFI LanGuard Central Management Server represent GFI LanGuard instances that have been set up within each GFI LanGuard deployment. The GFI LanGuard Central Management Server is unable to detect any sites automatically. To view or edit details of connected sites refer to: Managing Sites.

The bottom part of the home page contains three widgets with additional information, listed in the following table:

Option	Description
Notifications	A list of events describing actions carried out or problems that have been identified by GFI LanGuard Central Management Server, for example when a service is not running.
Security Sensors	Displaying information related to security issues such as missing updates or malware protection issues. Click any item in the list to drill down further details.
Missing Updates / Operating Systems / Software	Toggle between **Missing Updates**, **Operating Systems** and **Software** view to obtain quick information about what operating systems are running within your network or which important patches need to be deployed. Click Show all to be redirected to the dashboards.

3.4.2 Central Management Server Dashboards

The dashboards in GFI LanGuard Central Management Server Console provide information related to issues, missing patches or updates, vulnerabilities and other important information that provide insight into the security status of your entire network. Click **Dashboard** in the top navigation to access the overview page.



Screenshot 28: The overview dashboard

The **Overview** page is a dashboard that provides instant access to important information obtained from various GFI LanGuard installations. Information such as the vulnerability level of computers, domains or entire networks, missing updates alerts, vulnerability trends, top issues that need to be addressed and other data is displayed in one location for ease of access. Several additional dashboards that focus on specific features can be accessed by clicking the appropriate tabs in the upper part of the Console. These dashboards are described in the following table:

OPTION	DESCRIPTION
Computers	Select this dashboard to view information related to computers audited by GFI LanGuard. The Computers dashboard provides the discovered machine names, IP address, Domain name, installed Operating System and other relevant data.
History	The History view shows the changes done to target computers between audits. The report includes changes related to vulnerability level, user accounts, groups, ports, shares and registry entries. Audit results can be filtered by date, grouped by computer, information category or date and exported in several formats.
Vulnerabilities	A list of missing updates and types of vulnerabilities affecting your network. Select items from the list to display additional details.
Patches	Displays a list of missing or installed patches and service packs found during a network audit. When a patch or service pack is selected from the list, the **Details** section provides more information on the selected item.
Ports	Displays details on open TCP or UDP ports found during a network audit. When a port is selected from the **Port** List, the **Details** section provides more information on the selected port.
Software	A list of installed applications found during a network audit. When an application is selected from the **Application** List, the **Details** section provides more information on the selected application.
Hardware	Displays more information on the hardware found during a network audit. Select hardware from the list to display more details.
System Information	The **System Information** tab displays information associated with the operating system of a scan targets, such as users and groups, ongoing processes and services currently running.

NOTE

When a computer or domain is selected, the results related to the selected computer/domain are automatically updated in the dashboard.

3.4.3 Central Management Server Computer Tree

GFI LanGuard Central Management Server Console includes filtering and grouping options that enable you to quickly find a site, computer or domain and immediately display results. These options can be managed from the **Computer Tree** within the Dashboard and Reports areas.

When a computer or group is selected from the computer tree, results in the dashboard are automatically updated. Press **CRTL** and select multiple computers to display results for specific computers.

Saved filters can also be used to generate targeted reports. For more information, refer to Using GFI LanGuard Central Management Server Reports (page 66).

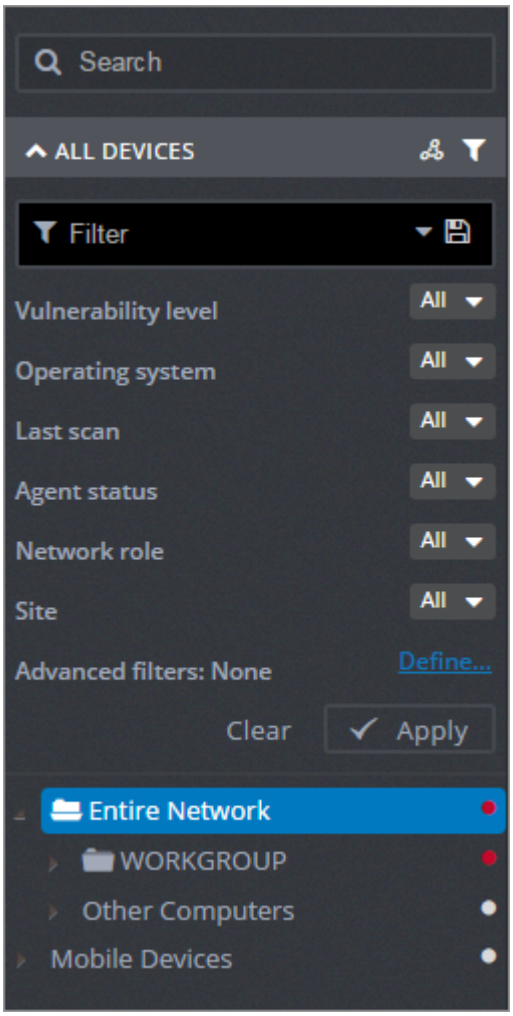
The following are functions supported by the computer tree:

- Simple filtering
- Advanced filtering
- Grouping
- Saved Filters

Simple filtering

To filter for a specific computer or group:

1. From the left pane, click the **Filter** icon.



Screenshot 29: Using a simple filter

2. Next to each filter item, configure the filtering criteria.

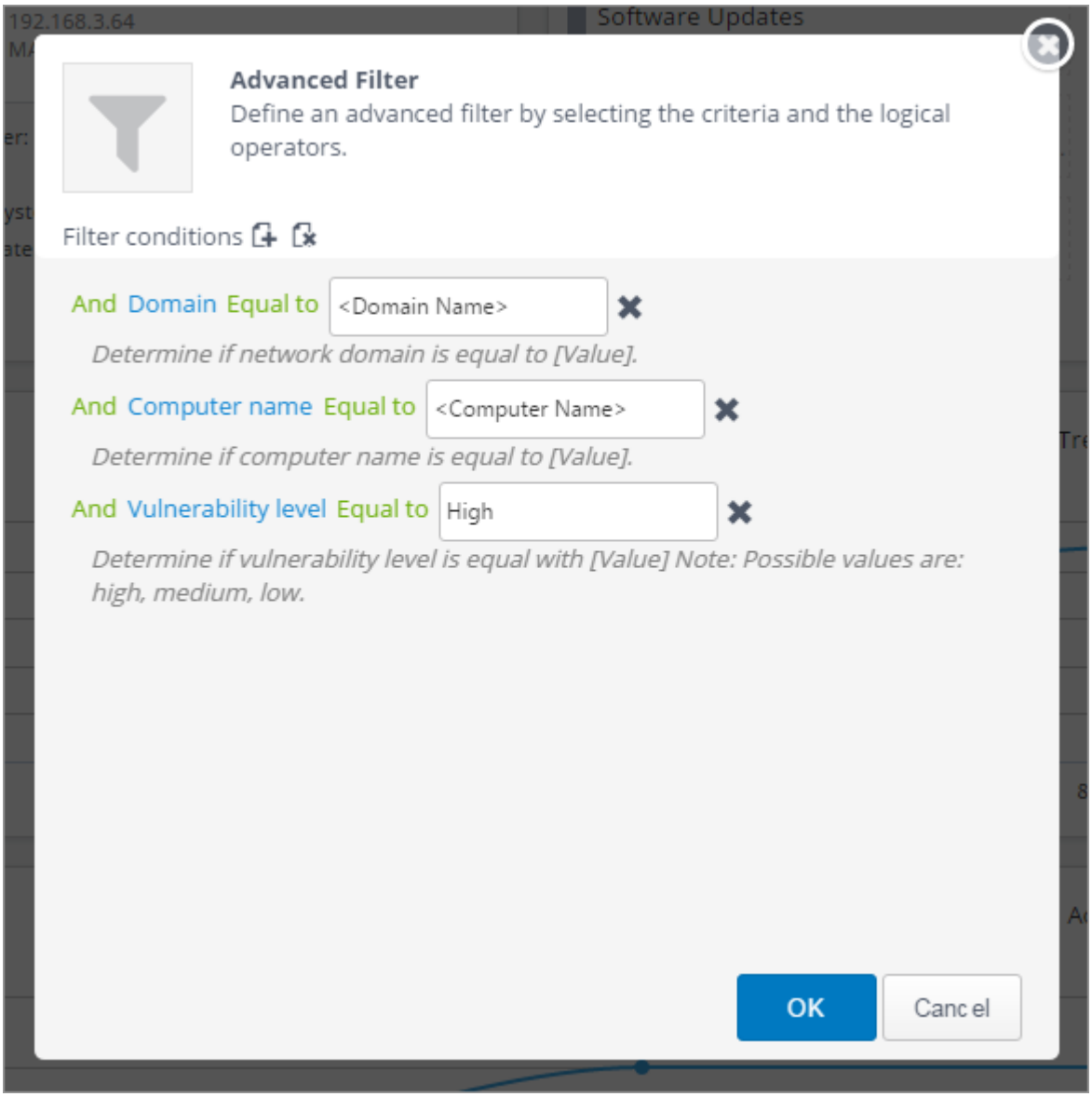
3. Click **Apply**.

Advanced filtering

To filter for a specific computer or group using advanced filtering:

1. From the left pane, click the **Filter** icon.

2. Next to **Advanced filters** click **Define**.



Screenshot 30: Using advanced filtering

3. From the **Advanced Filtering** dialog, click the **Add** icon.

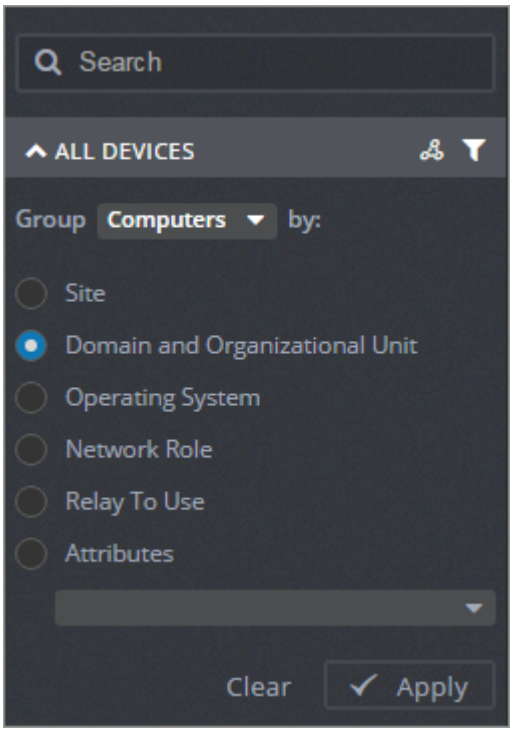
4. Select filtering conditions and key in the condition value. You can add as many as required.

5. Click **OK**

Grouping

To group machines by specific attributes:

1. From the left panel, click **Grouping** icon.



Screenshot 31: Group machines by specific attributes

2. Click on one of the following tabs and select a specific attribute:

Tabs	Attributes
Computers	» Site » Domain and Organizational Unit » Operating System » Network Role » Relays Distribution » Attributes
Mobile Devices	» Site » User Account » Operating System » Device Model » Attributes

NOTE

If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to Using Attributes in Central Management Server (page 66).

3. Click **Apply**.

Saved Filters

Saved Filters enable you to customize views and save them to quickly find frequently accessed information. Saved filters are also used in report scheduling. For more information, refer to Scheduling a report in GFI LanGuard Central Management Server (page 71).

To use a saved filter, click the **Filters** icon and select a saved filter from the drop down list.

To save a new filter:

1. From the **Computers tree**, click the **Filters** icon.

2. Click inside the Filter field and key in a name for the filter.

3. Configure the filtering options. Use the available drop down lists next to each filter option or click **Advanced Filters** for more options.

4. Click the **Save** icon.

Using Attributes in Central Management Server

Attributes enable you to group and configure single or multiple computers at one go. Attributes also enable you to remediate vulnerabilities or deploy software on specific computers based on the assigned attribute.

Attributes are configured in separate GFI LanGuard sites. When the remote sites synchronize with GFI LanGuard Central Management Server, they appear in the attributes list. For more information, refer to Using Attributes (page 130).

3.4.4 Using GFI LanGuard Central Management Server Reports

This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard Central Management Server. New reports can be added by customizing existing reports and saving them with a new name. For more information, refer to Customizing GFI LanGuard Central Management Server Reports (page 72).

There are two main types of reports:

» General reports - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity

» Legal compliance reports - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

For information on how to generate or schedule a report, refer to the following sections:

» Generating reports

» Scheduling reports

General reports

To view **General** reports:

1. Click **Reports** tab.

2. Click **View**, and from the list of reports, click **General Reports**, then select any of the following reports:

Report Title	Description
Network Security Overview	An executive summary report showing: » Network vulnerability level » Most vulnerable computers » Agent status » Audit status » Vulnerability trends over time » Information on operating systems » Servers and workstations.

Report Title	Description
Computer Security Overview	An executive summary report showing: » Computer vulnerability level » Agent status » Audit status » Vulnerability trends over time » Computer summary and details.
Vulnerability Status	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by: » Computer name » Vulnerability severity » Timestamp » Category.
Patching Status	Shows statistical information related to missing and installed updates detected on your scan targets. Updates can be grouped by name, severity, timestamp, vendor and category. Use this report to get: » Missing vs. Installed updates comparison » Charts and tables displaying missing updates distribution for each item from the first and second grouping criteria » Charts and tables displaying installed updates distribution for each item from the first and second grouping criteria » Patching details for missing and installed patches.
Full Audit	A technical report showing information retrieved during an audit. Amongst others, the report contains information on: » Vulnerabilities » Open ports » Hardware and software.
Software Audit	Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on: » Antivirus » Antispyware » Applications inventory.
Scan History	An overview of the network security audits performed over time. Amongst others, the report includes information on: » Most scanned computers » Least scanned computers » Auditing status » History listing.
Remediation History	Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on: » Remediation actions per day » Remediation distribution by category » Remediation list grouped by computers.
Network Security History	Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to: » The vulnerability level » User accounts » Groups » Ports » Shares » Registry entries.

Report Title	Description
Baseline Comparison	Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on: » Registry » Installed Service Packs and Update Rollups » Missing Security/Non-Security Updates » Vulnerability level.
Mobile Devices Audit	Shows information related to detected mobile devices found during an audit. Amongst others, the report includes information on: » Vulnerability distribution by severity » Vulnerability distribution by computer » Vulnerability listing by computer.
Sites Overview	Shows a high level overview of managed GFI LanGuard sites, displaying for each site
Sites Summary	List of GFI LanGuard sites. For each site the report shows: » Number of nodes » License usage » Vulnerability level » Patching and auditing status » User rights assignments.
USB Devices	Lists all USB devices found in an audit, grouped by computer.
Missing Microsoft® Security Updates	Shows statistical information related to missing Microsoft® security updates, detected on your scan targets. Select items to include in your report: » General missing updates distribution chart » Distribution table » Vulnerability list.
Missing Non-Microsoft® Security Updates	Shows statistical information related to missing non-Microsoft® security updates, detected on your scan targets. Select items to include in your report: » General missing updates distribution chart » Distribution table » Vulnerability list.
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.
Computer Summary	A summary of scan target information, including: » Operating system information » Agent status » Vulnerabilities severity.
Hardware Audit	Illustrates information related to the hardware found during an audit.
Computer Details	Provides a detailed list of computer properties, including: » MAC Address » Time to Live » Network Role » Domain » Lan Manager » Is relay agent » Uses relay agent » Attributes » Operating system » IP address.
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.

Report Title	Description
Open Ports	Lists all the open ports found during an audit. The results are grouped by port type (TCP and UDP).
Services	Lists all services found during an audit. Results are grouped by computer name.
Groups and Users	Lists all Groups and Users found during an audit. The result is grouped by computer name.
Mobile Device Policies	Lists all mobile device policies found during an audit. The result is grouped by computer name.
Unauthorized Applications	Lists all unauthorized applications installed scan targets, including: » Top Computers with Unauthorized Applications » Top Unauthorized Applications » Applications Inventory » Computers without Antivirus Installed
Antivirus Applications	Shows information related to the antivirus installed on scan targets.
New Devices	Lists all new devices found during last week audits.

Legal Compliance reports

To view **Legal Compliance** reports:

1. Click **Reports** tab.

2. Click **View** and from the list of reports, expand any of the following compliance reports suites:

Report Suite Title	Description
PCI DSS Compliance Reports	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. GFI LanGuard Central Management Server provides you with a number of reports that cater for PCI DSS compliance, including: » PCI DSS Requirement 1.4 - Installed Firewall Applications » PCI DSS Requirement 2.2.3 - Disk Encryption Applications » PCI DSS Requirement 5.2 - Antivirus Applications » PCI DSS Requirement 6.1 - Remediation History by Date » PCI DSS Requirement 12.12 - Open Trojan Ports by Host.
HIPAA Compliance Reports	The Health Insurance Portability and Accountability Act (HIPAA) is a requirement of all healthcare providers that regulates the exchange of private patient data. This helps prevent unlawful disclosure or release of medical information. To help you follow HIPAA regulations, GFI LanGuard Central Management Server provides you with a suite of HIPAA compliance reports, including: » HIPAA 164.308(a)(1)(ii)(A) - Missing Security Updates by Host » HIPAA 164.308(a)(1)(ii)(A) - Vulnerability Distribution by Host » HIPAA 164.308(a)(4)(ii)(A) - Open Ports » HIPAA 164.308(a)(5)(ii)(D) - Audit Policy » HIPAA 164.308(a)(8) - Baseline Changes Comparison.
SOX Compliance Reports	The Sarbanes-Oxley Act (SOX) is regulation created in response to high-profile financial scandals as well as to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. GFI LanGuard Central Management Server provides a list of SOX compliance reports, including: » SOX 302.a - Network Vulnerability Summary » SOX 302.a - Remediation History by Host » SOX 302.a - Security Scans History » SOX 404 - Vulnerability Listing by Category » SOX 404 - Missing Security Updates by Host.

Report Suite Title	Description
GLBA Compliance Reports	The Gramm–Leach–Bliley Act (GLBA) is an act that allows consolidation between Banks and Insurance companies. Part of the act focuses on IT network compliance for such companies. GFI LanGuard Central Management Server offers a list of GLBA Compliance reports, including: » GLBA 501.b - Baseline Changes Comparison » GLBA 501.b - Network Patching Status » GLBA 501.b - Open Trojan Ports by Host » GLBA 501.b - Vulnerable Hosts Based on Open Ports » GLBA 501.b - Vulnerable Hosts by Vulnerability Level.
PSN CoCo Compliance Reports	The Public Service Network - Code of Connection (PSN CoCo) is simply a list of conditions that should be met before connecting an accredited network to another accredited network. GFI LanGuard Central Management Server helps you monitor the status of such connections through the list of PSN CoCo Compliance reports, which include: » PSNCoCo RIS. 1 - Baseline Changes Comparison » PSNCoCo MAL. 1 - Disk Encryption Applications » PSNCoCo MAL. 1 - Installed Firewall Applications » PSNCoCo PAT. 1 - Installed Security Updates by Host » PSNCoCo PAT. 1 - Installed Security Updates by Severity.
CIPA	The Children's Internet Protection Act (CIPA) addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. GFI LanGuard Central Management Server provides a list of CIA Compliance reports including: » Req. 47 USC § 254(l)(1)(A)(iv) - Network Vulnerability Summary » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Distribution by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Category » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Severity » Req. 47 USC § 254(l)(1)(A)(iv) - Open Trojan Ports by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Network Patching Status » Req. 47 USC § 254(l)(1)(A)(iv) - Missing Security Updates by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts Based on Open Ports » Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Baseline Changes Comparison
FERPA Compliance Reports	The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. GFI LanGuard Central Management Server provides a list of FERPA Compliance reports, including: » FERPA 20 USC 1232g (b) - Network Patching Status » FERPA 20 USC 1232g (b) - Network Security Log by Host » FERPA 20 USC 1232g (b) - Remediation History by Date » FERPA 20 USC 1232g (b) - Vulnerability Distribution by Host » FERPA 20 USC 1232g (b) - Vulnerable Hosts Based on Open Ports.
ISO/IEC 27001 & 27002 Compliance Reports	The Information technology – Security techniques – Information security management systems (ISO/IEC) standard formally specifies a management system that is intended to bring information security under explicit management control. GFI LanGuard Central Management Server offers an extensive list of ISO/IEC Compliance reports, including: » ISO/IEC 27001 A. 10.4 - Antivirus Applications » ISO/IEC 27001 A. 10.7.2 - Disk Encryption Applications » ISO/IEC 27001 A. 10.6.2 - Open Shares » ISO/IEC 27001 A. 10.6.2 - Services » ISO/IEC 27001 A. 10.6.2 - System Information.

Report Suite Title	Description
FISMA Compliance Reports	The Federal Information Security Management Act (FISMA) assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. GFI LanGuard Central Management Server helps you be compliant to FISMA standards through the provided reports, which include: » FISMA NIST SP 800-53 AC-2 - Groups and Users » FISMA NIST SP 800-53 PM-5 - Computer Details » FISMA NIST SP 800-53 PM-5 - Computer Summary » FISMA NIST SP 800-53 SI-5 - Missing Security Updates by Host » FISMA NIST SP 800-53 SI-7 - Antivirus Applications.
CAG Compliance Reports	The Consensus Audit Guidelines (CAG) is a publication of best practice guidelines for computer security. The project was initiated as a response to extreme data losses experienced by organizations in the US defense industrial base. GFI LanGuard Central Management Server offers a list of CAG Compliance reports, including: » CAG CC1 - Hardware Audit » CAG CC1 - Scan History » CAG CC3 - Audit Policy » CAG CC3 - Low Security Vulnerabilities » CAG CC11 - Open Ports.
NERC CIP Compliance Reports	The North American Electric Reliability Corporation (NERC) develops standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. GFI LanGuard Central Management Server provides a list of NERC CIP Compliance reports, including: » NERC CIP-005 R2 - Installed Firewall Applications » NERC CIP-005 R2 - Open Ports » NERC CIP-007 R2 - Open Shares » NERC CIP-007 R2 - Services » NERC CIP-007 R2 - System Information.

Generating a report in GFI LanGuard Central Management Server

To use one of the reports:

1. From the top navigation, click **Reports**.
2. Select a report category from the View menu.
3. Hover over one of the report names and click **Generate** to run the report.

Scheduling a report in GFI LanGuard Central Management Server

Reports can be run on a schedule. To schedule a report:

1. From the top navigation, click **Reports**.
2. Use the **View** filter on the left to select the category of reports you need.
3. Hover over a report and click **Schedule**.
4. In the **General** tab, define the following:

OPTION	DESCRIPTION
Enable Schedule	Click to enable a schedule for the selected report.
One time only on	Select this option and specify date and time if you want the report to run only once.

OPTION	DESCRIPTION
Recurrence pattern	Select this option if you want the report to be generated a number of times. Specify **Daily**, **Weekly**, **Monthly** intervals and the time of day at which to generate the report. For each of the selected options, define additional recurrence details.

5. In the **Customize** tab, define the following:

OPTION	DESCRIPTION
Choose a filter that applies to the target	Filters enable you to generate more targeted reports. For example, you can generate reports for high vulnerability issues only. Select one of the saved filters from the drop down list that apply to the currently selected report. If you have not saved any filters, this option will be grayed out. For information on how to create new filters refer to: Using the Computer Tree.
Export to file	Select this option to export the generated report. This can be saved to file or sent by email as an attachment. Use the **Report Format** drop down field to specify the format of the exported report. Available formats are *.pdf, *.rtf, *.xls, *.xlsx, *.html, *.mht and *.png
Send by email	Select this option if you want the generated report to be automatically sent as an attachment by email. GFI LanGuard Central Management Server uses configured email settings when sending reports. To view currently configured settings click **Email Setup**. For more information, refer to Email settings in Central Management Server (page 57).
Override general alerting options and send email to:	Select this option if you want GFI LanGuard Central Management Server to ignore currently configured email settings and send the generated report to a specific email addresses. Enter the email address in the available field. Separate multiple email addresses with a semi-colon.

6. Click **Save**.

Customizing GFI LanGuard Central Management Server Reports

Existing reports can be modified and saved as new reports. For a full list of default reports, refer to: Available reports.

To customize a report:

1. From the top navigation, click **Reports**.
2. Hover over one of the report names and click **Customize**.
3. Modify the following options:

OPTION	DESCRIPTION
Report name	Every report name must be unique. Click on the report name to change.
Report Items	Each report is preconfigured with a list of specific items to include in the report. For example, the Software Audit report includes Antivirus Status, Applications Inventory and Computers without Antivirus amongst others. Select the items to be included in the report from the available list. The criteria change according to the selected report.
Filters	Filtering helps create more targeted reports. Filters are different for each report. Click the **Filters** tab and configure the criteria to use.
Grouping & Sorting	Configure the items and report criteria by which the report will be grouped and sorted.

4. Click **Generate** to run the report or **Save as Custom** to store the customized report as a new report.

4 Using GFI LanGuard

GFI LanGuard helps you strengthen your network's security and integrity with positive patch management, vulnerability management and legal compliance results, while ensuring that your network is protected using the most up-to-date vulnerability detection methods and techniques.

4.1 Managing Agents

GFI LanGuard can be configured to deploy agents automatically on newly discovered machines or manually, on selected computers. Agents enable faster audits and drastically reduce network bandwidth utilization. When using Agents, audits are performed using the scan target's resource power. Once an audit is finished, the results are transferred to GFI LanGuard in an XML file.

> **NOTE**
> GFI LanGuard Agents can be deployed only on machines running Microsoft Windows operating systems that meet a minimum set of system requirements. For more information, refer to GFI LanGuard system requirements (page 20).

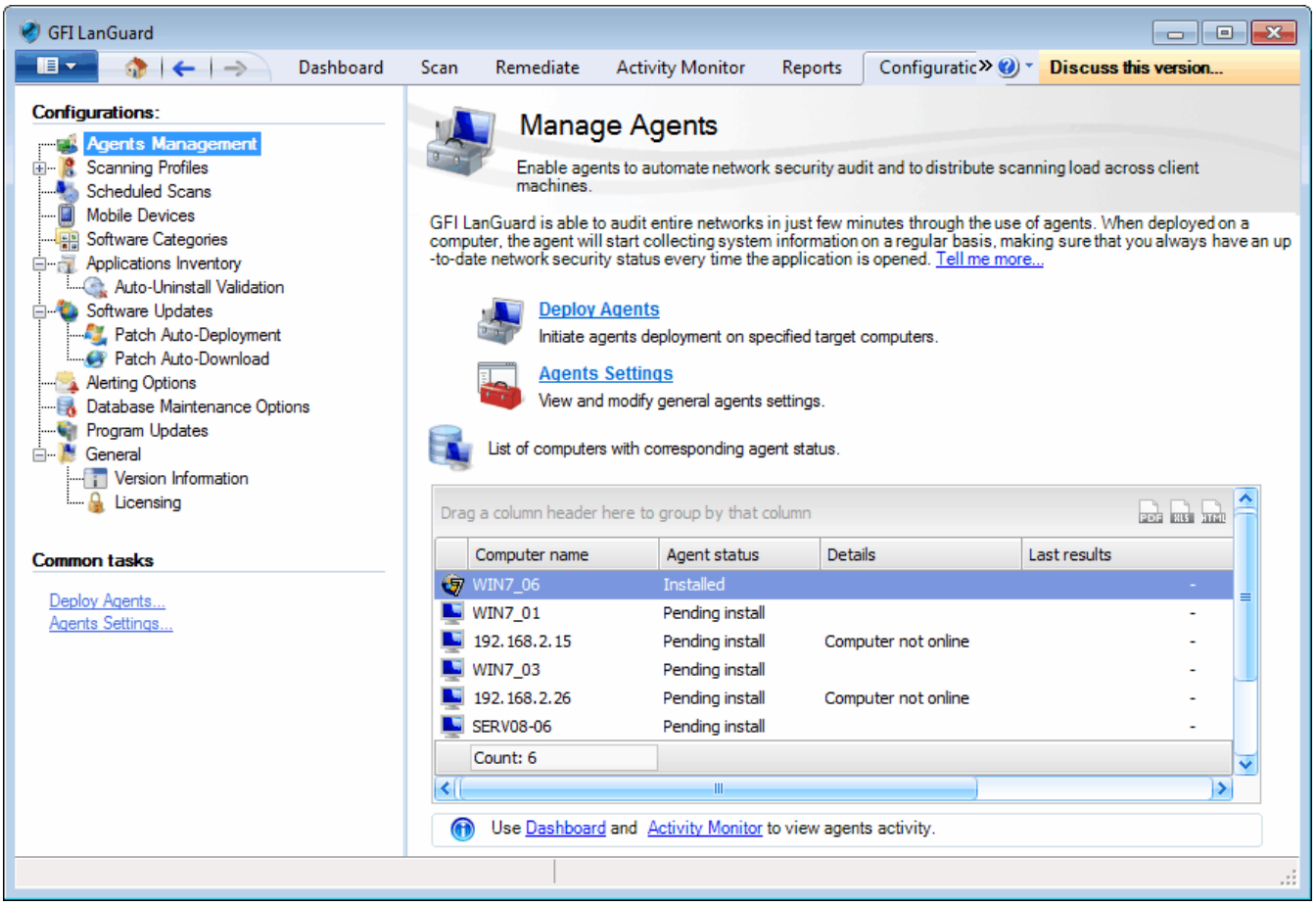
Topics in this section:

4.1.1 Deploying Agents

To deploy GFI LanGuard Agents on network computers:

1. Launch GFI LanGuard.

2. From the **Home** menu, select **Manage Agents**. Alternatively, click **Configuration tab > Agents Management**.



Screenshot 32: Manage agents

3. From **Common Tasks**, click **Deploy Agents** to select the target scan computers and click **Next**. Select one of the options described below:

Option	Description
Local Domain	Deploy agents on all reachable computers within the same workgroup / domain where GFI LanGuard is installed. No further configuration is required in **Define target** step.
Custom	Deploy agents on specific computers or group of computers. Add new rules to search or specify target scan computers.

4. If **Custom** option is selected, click **Add new rule** and select the **Rule type** described below:

Rule type	Description
Computer name is	Manually enter a computer name or import the names from a saved text (.txt) file. Click **Select** and manually select computers from the list, or click **Import** and specify the text file location.
Domain name is	Select domains from the list of reachable domains.
Organization unit is	Select computers from one or more reachable organization units. Use the following options: » **Retrieve** – Specify the user name and password to retrieve the list » **Refresh** – Refresh the list of domains and Organization Units » **Add** – Manually add an Organization Unit.

Repeat step 4 for each rule. Once completed, click **OK**

5. From **Deploy Agents** dialog, click **Next**.

6. (Optional) Select **Authenticate** using checkbox to specify alternate credentials.

7. (Optional) Click **Advanced Settings**, and configure the settings in the following tabs:

Tab	Description
General	Configure the schedule for when GFI LanGuard automatically scans for new machines in the network perimeter where agents are enabled.
Audit Schedule	Configure how often the agent audits the host computer (where the agent is installed). Select the recurrence pattern, the time the audit will start and the scan profile to use.
Auto remediation	Configure GFI LanGuard to automatically download and install missing patches and service packs. Uninstall unauthorized applications on the scanned computers. For more information, refer to Automatic Remediation (page 162).

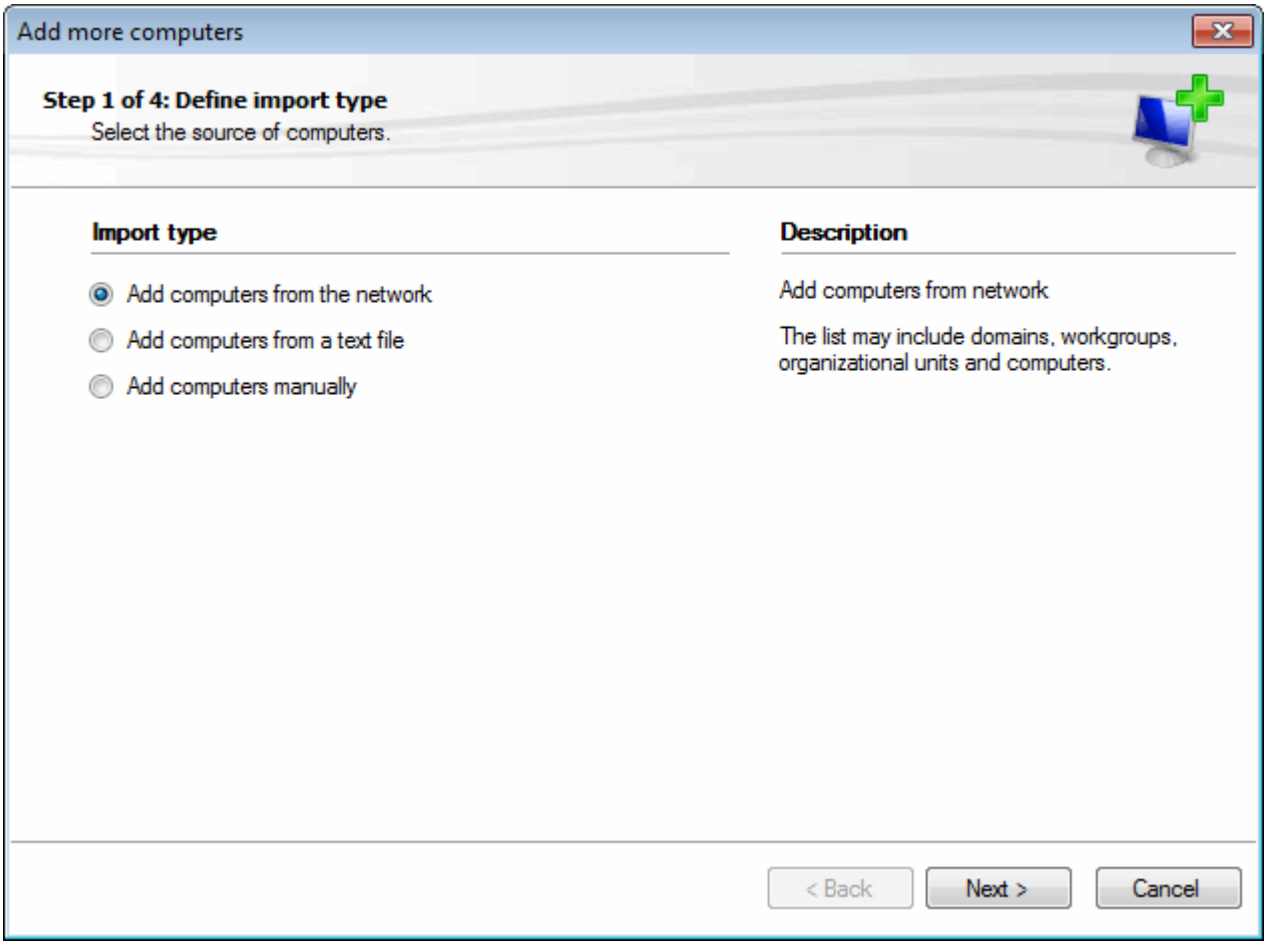
8. Click **Next** and **Finish** to complete agent deployment.

4.1.2 Deploy Agents manually

To deploy agents manually:

1. Launch GFI LanGuard and select **Dashboard**.

2. From **Common Tasks**, select **Add more computers**.

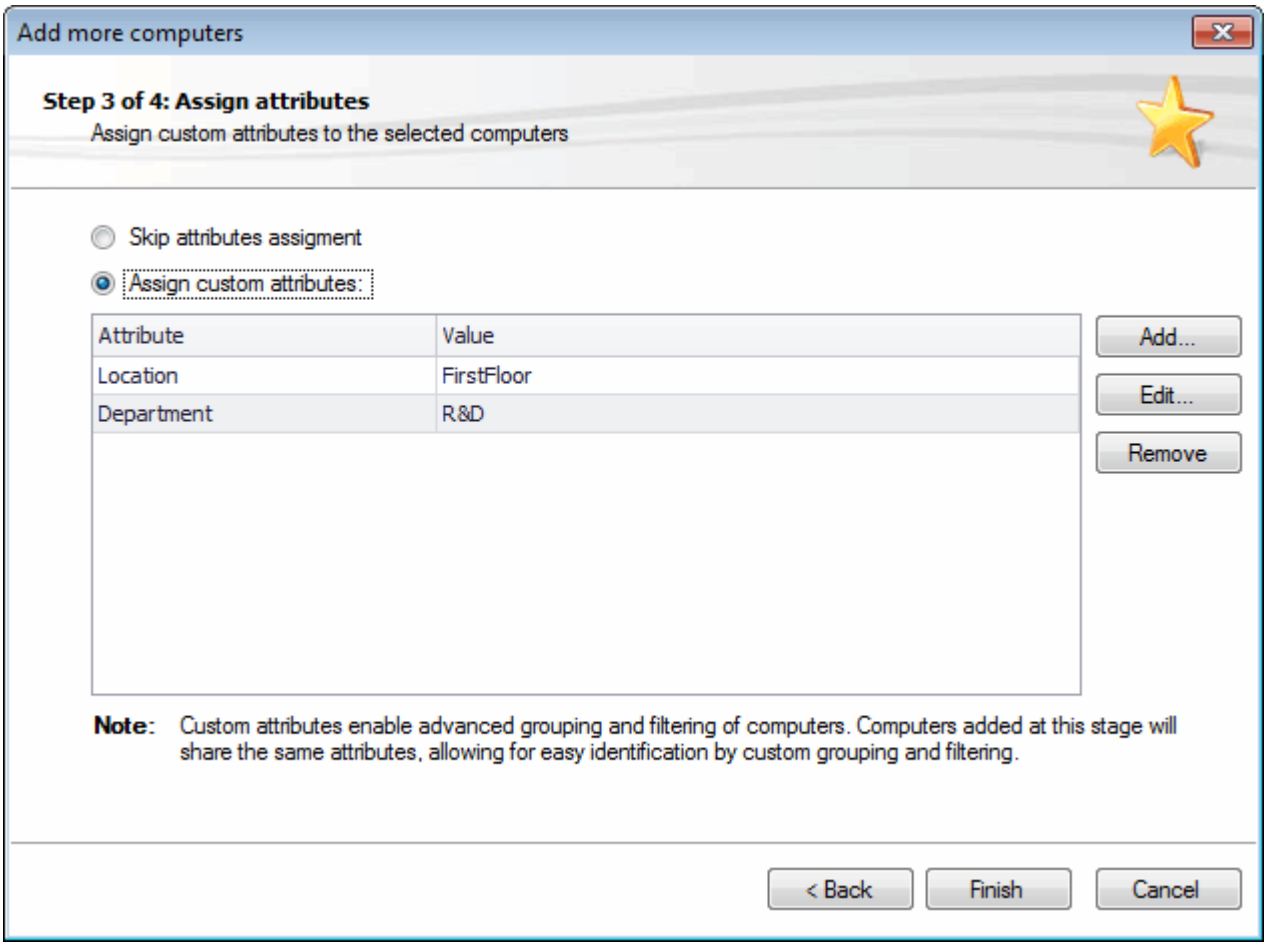


Screenshot 33: Add more computers - Select import type

3. From the Add more computers wizard, select one of the following options:

Option	Description
Add computers from the network	Select domains, organizational units and computers from the list. Use the **Add domain** to add a new domain to the list of computers.
Add computers from a text file	Import computer list from text file. Click **Browse** and locate the text file containing the list of computers.
Add computers manually	Manually create a list of computers. Use the **Add** and **Remove** buttons to add and remove computers from the list. Use the **Import** and **Export** buttons to import and export the list from\to a text file.

Click **Next**.



Screenshot 34: Add more computers - Assign attributes to new computers

4. Custom attributes can be assigned to specific computers to ease grouping and filtering. From the **Assign attributes** wizard, configure the following:

Option	Description
Skip attributes assignment	No attributes are added to the computers list.
Assign custom attributes	Assign attributes to the list of computers. Click the **Add** button and specify the new attribute name and value. **NOTE** When importing a list of computers from a text file, GFI LanGuard automatically assigns the file name as an attribute (File) to the imported list.

5. Click **Finish**.

NOTE

If the selected computers have different login credentials from the GFI LanGuard machine, GFI LanGuard launches a dialog that enables you to specify valid credentials.

6. Once the computers are added to the list, click **Close**.

7. From the computer tree, right-click the newly added computers and select the computer where to deploy the agent and from the **Agent Status** click **Deploy Agent**.

8. Configure the Agent properties. For more information, refer to Agent properties (page 77).

4.1.3 Agent properties

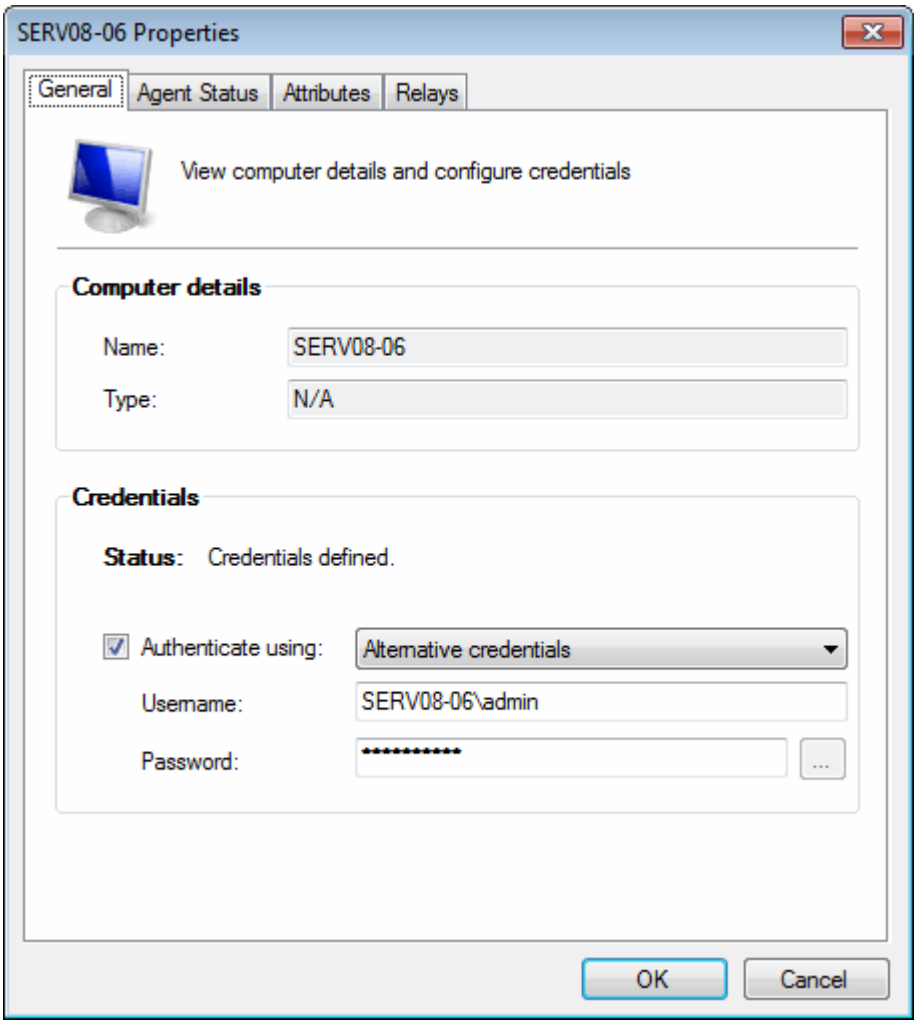
To modify agent properties:

1. Click **Configuration** tab > **Agents Management**.

2. From the right pane, right–click an agent and select **Properties**.

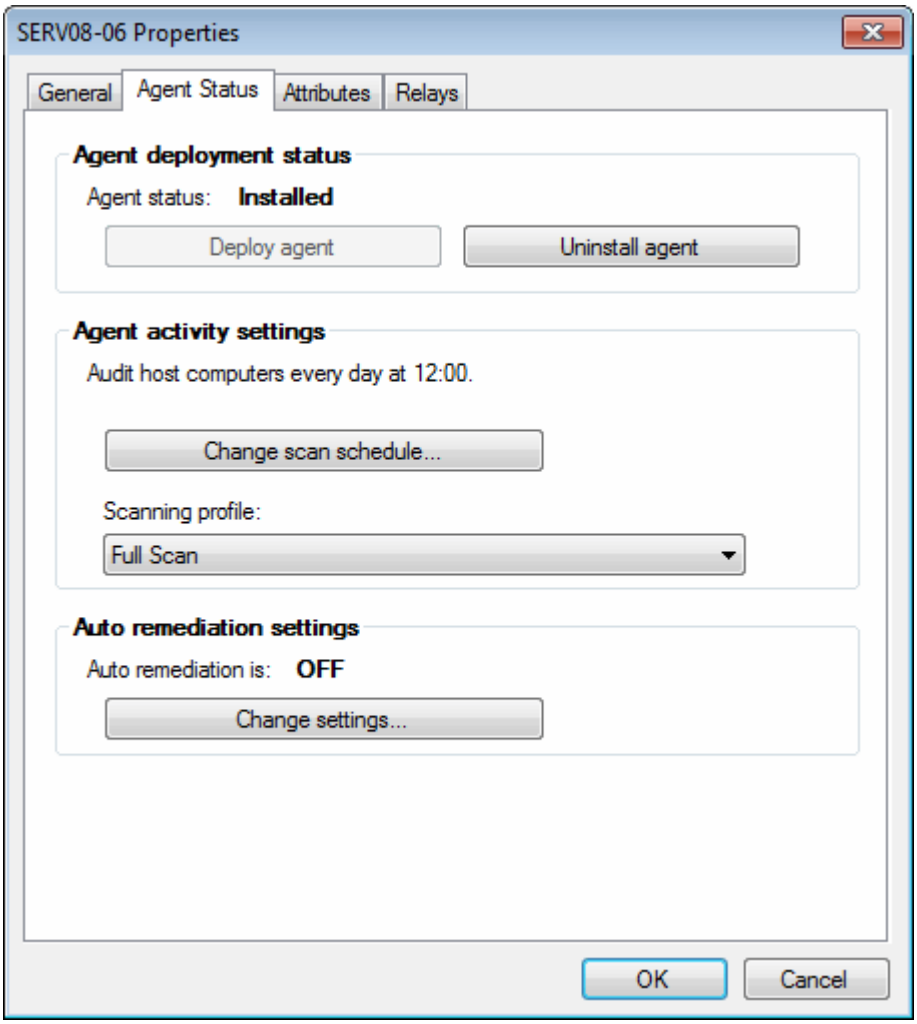
NOTE

The **Properties** dialog can also be accessed from the computer tree within the **Dashboard**. Right-click a computer or a group and select **Properties**.



Screenshot 35: Agent Properties - General tab

3.(Optional) From **General** tab, specify the name, type and authentication method for the selected agent.



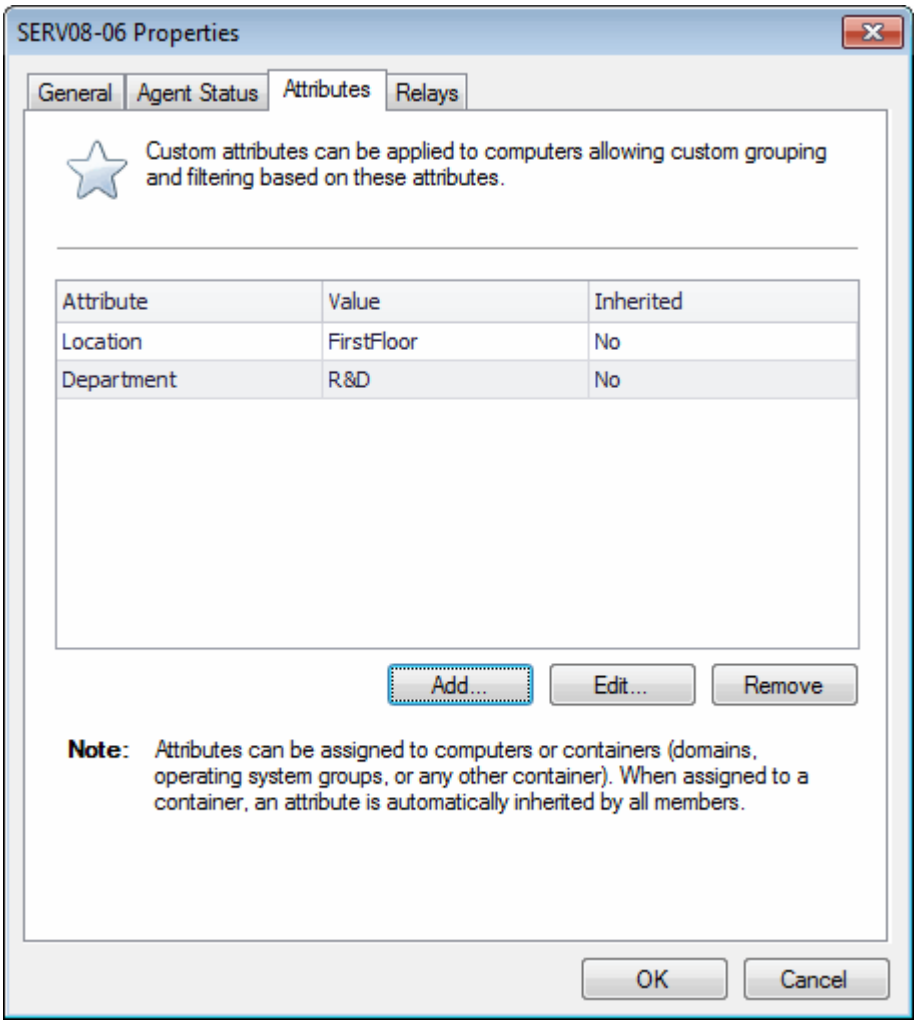
Screenshot 36: Agent Properties - Agent Status tab

4. From **Agent Status** tab, enable/disable agent deployment by clicking **Deploy agent** or **Disallow agent installation**.

5. Click **Change scan schedule…** to configure the selected agent's scan schedule.

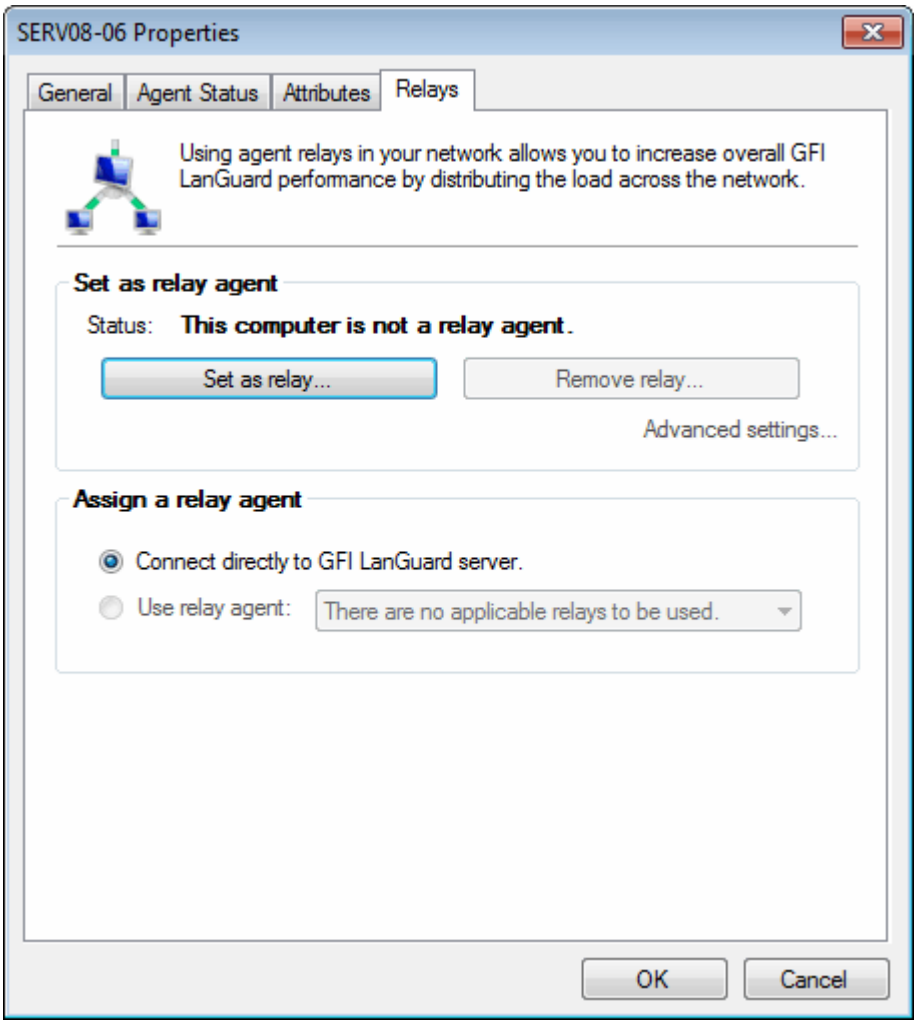
6. From **Scanning profile** drop-down menu, select the active scan profile.

7. From **Auto remediation settings**, click **Change settings…** to enable/disable agent auto–remediation. For more information, refer to Configuring auto-remediation options (page 173).



Screenshot 37: Agent Properties - Attributes tab

8. Click **Attributes** tab to manage the attributes assigned to the selected computer. Use the **Add**, **Edit** and **Remove** buttons to manage attributes.



Screenshot 38: Agent Properties - Relays tab

9. Click **Relays** tab to configure agent relays. Relays enable computers other than the one hosting GFI LanGuard to act as GFI LanGuard server. This helps you load-balance traffic directed to that machine and optimize network scanning performance.

10. Configure the options described below:

Option	Description
Set as relay	Set the selected computer as a relay agent. The selected computer will send product updates and patches to other agents to reduce the load from the GFI LanGuard machine. Click **Set as relay...** and follow the configuration wizard.
Remove relay	Remove the relay agent role from the selected computer. Click **Remove relay...** and follow the configuration wizard.
Connect directly to GFI LanGuard server	The selected computer will download product updates and patches from the GFI LanGuard server.
Use relay agent	The selected computer will use a relay agent to download product updates and patches. Select the relay agent to use from the drop down list.

11. (Optional) Click **Advanced Settings** and configure the following options:

Option	Description
Caching directory	All patches and updates are stored in this location before installation on the client computer.
Port where to serve	The port used by the relay agent to serve requests.
Address where to server	The address used by client computers to connect to the relay agent (By default the DNS host name is used).

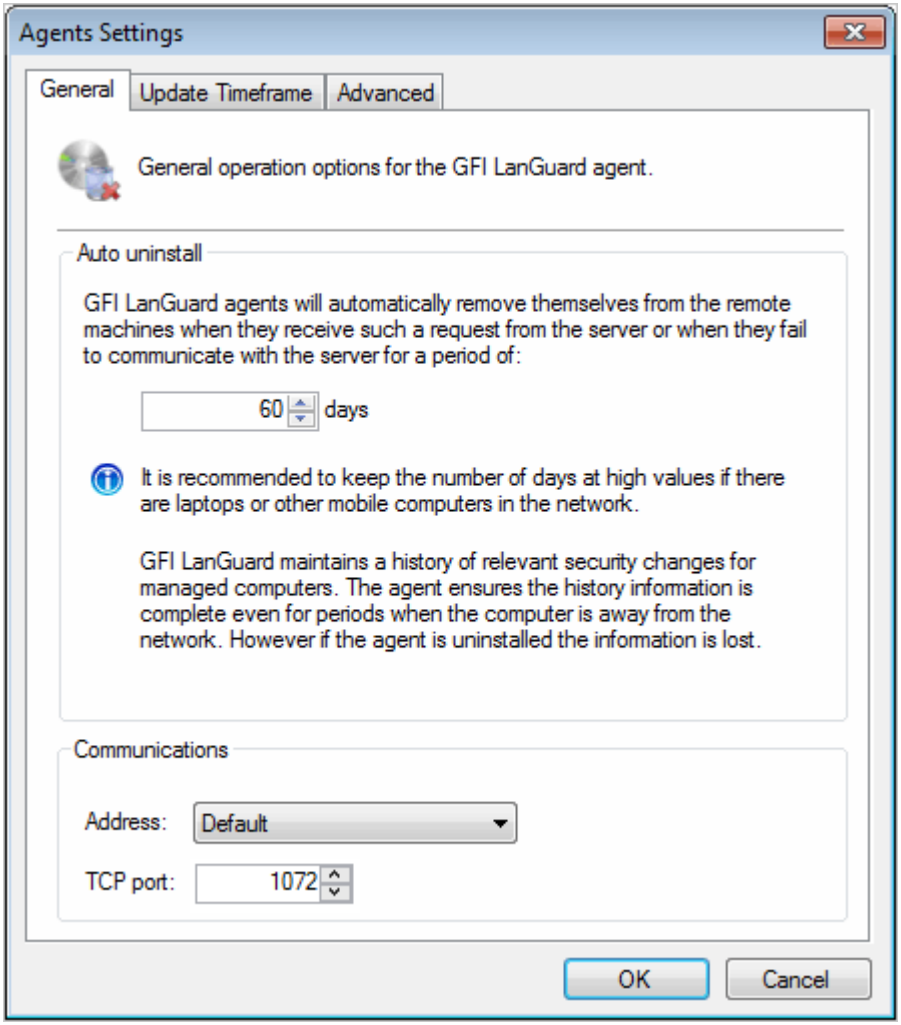
12. Click **OK** twice.

4.1.4 Agents settings

To configure additional agents' settings:

1. From **Configuration** tab, select **Agents Management**.

2. Click **Agents Settings**.

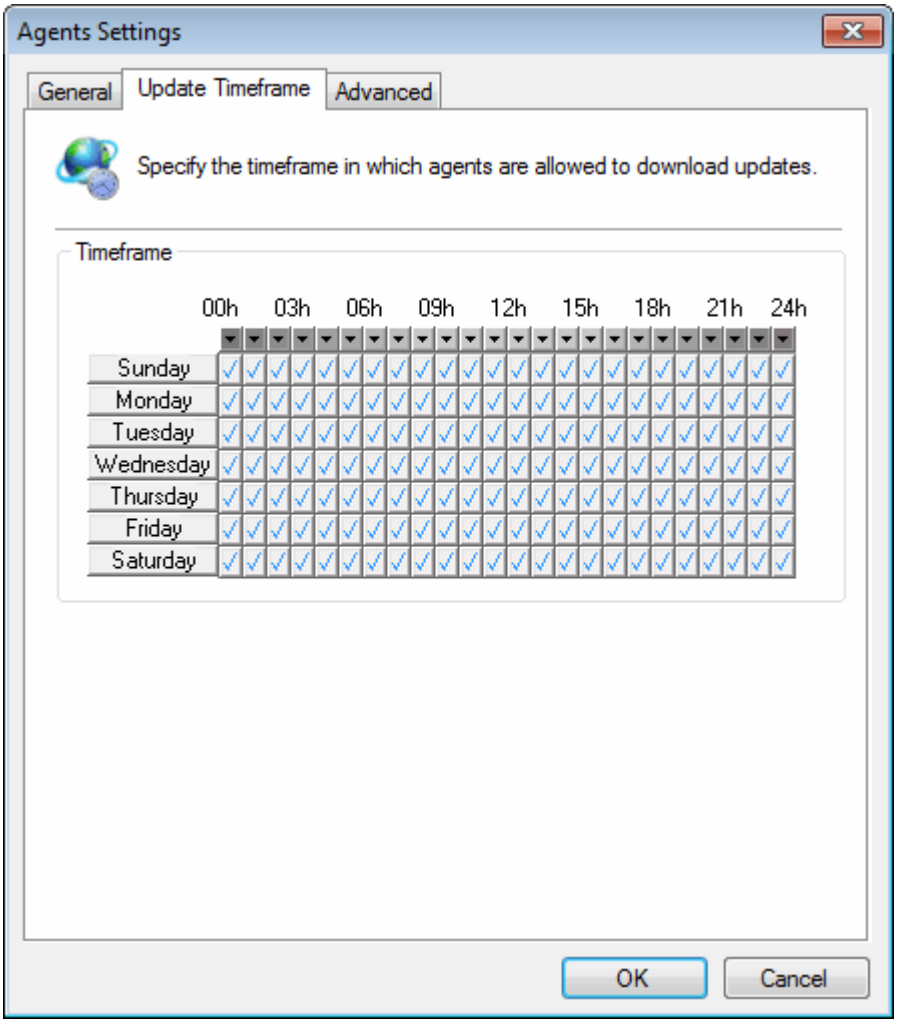


Screenshot 39: Agent Settings - General tab

3. Configure the options described below:

Option	Description
Auto uninstall	Set the number of days after which GFI LanGuard Agents automatically uninstall themselves if the host computer is unresponsive for the set period of days.

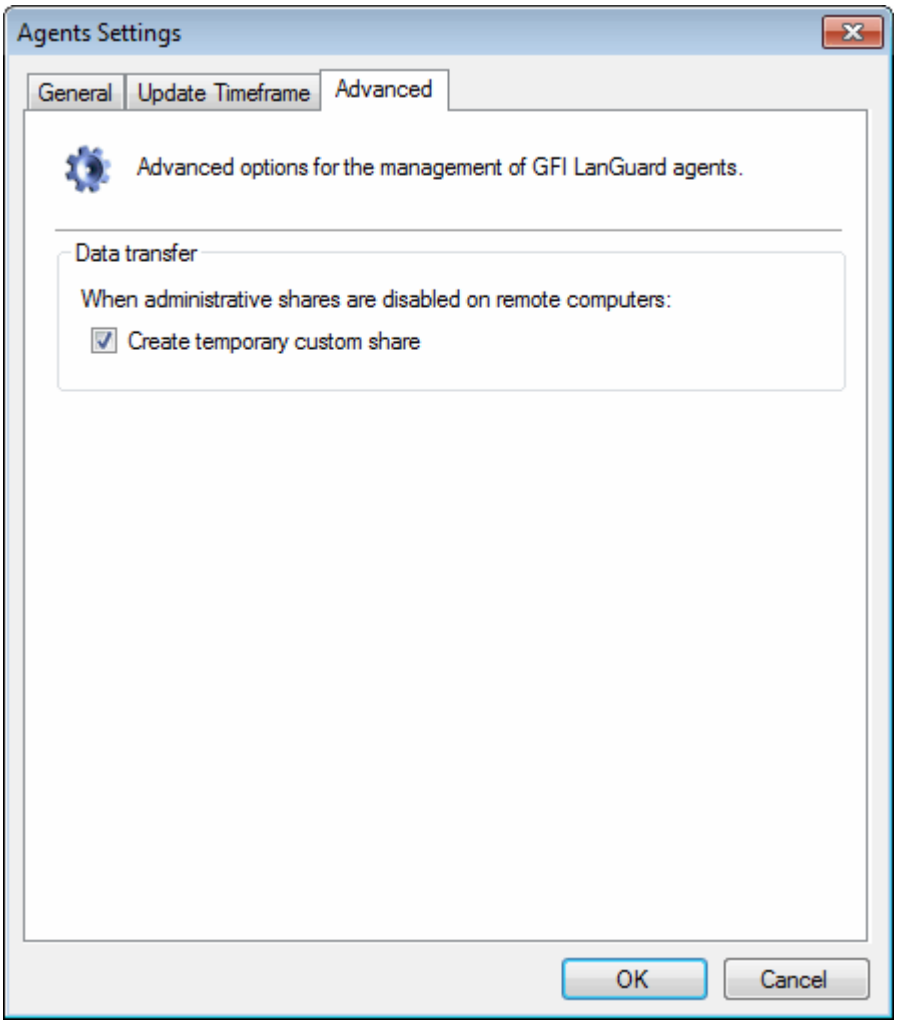
Option	Description
Agents report using	Configure the port and IP address used by agents to communicate and report status to GFI LanGuard. When GFI LanGuard machine has multiple IP addresses and Default setting is selected, GFI LanGuard automatically selects the IP address to use.



Screenshot 40: Agent Settings - Update Timeframe tab

4. Specify the timeframe in which agents are allowed to download updates.

5. Click **OK** to save and close dialog.



Screenshot 41: Agent Settings - Advanced tab

6. (Optional) Click **Advanced** tab and select **Create temporary custom share**. When this option is enabled and administrative shares are disabled on agent machines, GFI LanGuard creates a temporary shared folder for transferring information.

7. Click **OK** to save and close dialog.

> **WARNING**
>
> Communication on TCP port **1072** must be enabled in Windows firewall for GFI LanGuard Agents to send data to GFI LanGuard.

4.1.5 Configuring Relay Agents

In larger networks you may experience increased network bandwidth use due to the amount of data transferred from the GFI LanGuard server to managed computers. The data consists of definition updates delivered to Agent computers and of patches being deployed to target computers.

To help avoid performance issues and to apply load balancing techniques, GFI LanGuard enables you to configure Agents as a relay of the server. Agents that are configured as Relay Agents act as caching points. These download patches and definitions directly from GFI LanGuard server or from an upstream Relay Agent and forward them to client computers (which can be Agent-based and Agent-less computers). The main advantages of using Relay Agents are:

» Reduced bandwidth consumption in local or geographically distributed networks. If a Relay Agent is configured on each site, a patch is only downloaded once and distributed to client computers

» Reduced hardware load from the GFI LanGuard server component and distributed amongst relay agents

» Using multiple Relay Agents increases the number of devices that can be protected simultaneously.

Follow the below recommendations to take full advantage of Relay Agents:

1. Keep the number of computers/agents directly connected to the GFI LanGuard server or to one Relay Agent below 100.

2. In geographically distributed networks, designate at least one Relay Agent for each remote site. This ensures that each file is only transmitted once from the GFI LanGuard server site to the remote site.

3. Fine-tune network use by configuring cascading Relay Agents

Refer to the following sections for information about:

» Configuring an Agent as a Relay

» Configuring Relay Agent advanced options

» Connecting computers to a Relay Agent

Configuring an Agent as a Relay

To configure an Agent to act as a Relay Agent:

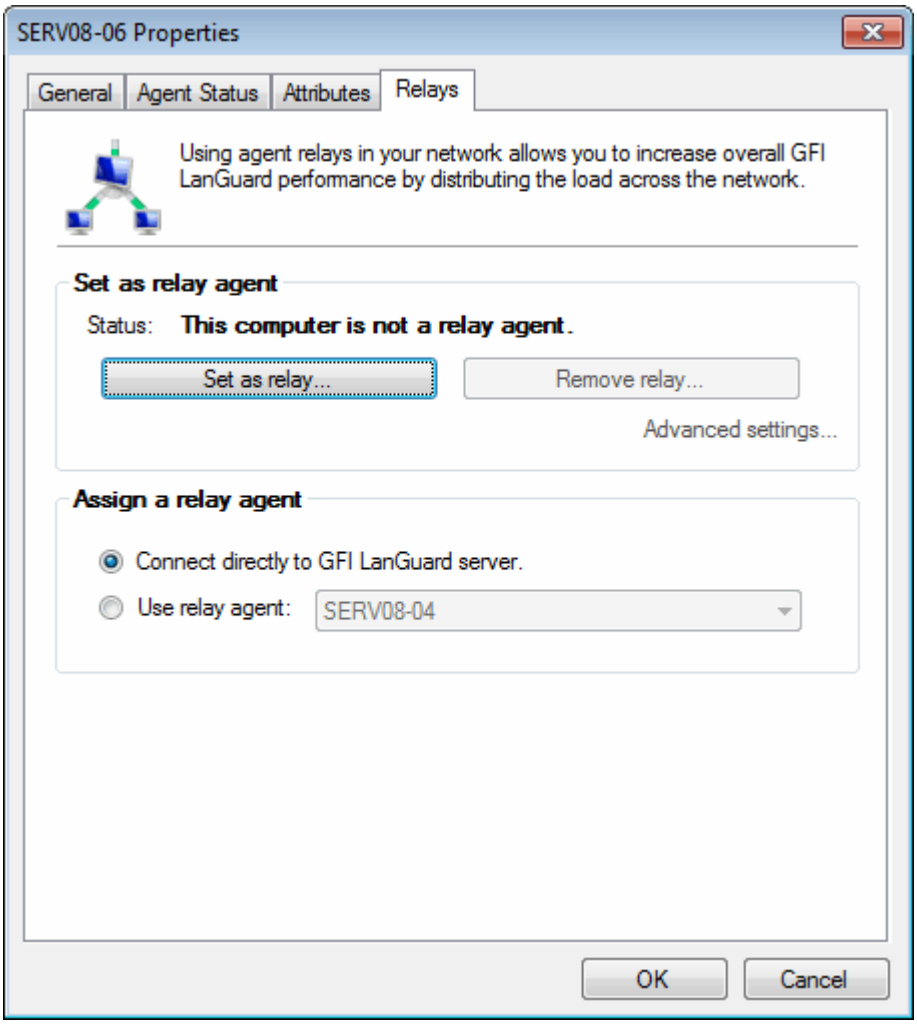
> **NOTE**
> The machine where GFI LanGuard is installed cannot be configured as a Relay Agent. The **Relays** tab from the Agent's **Properties** dialog is missing for the GFI LanGuard host.

1. Open GFI LanGuard.

2. Click **Configuration** tab **> Agents Management**.

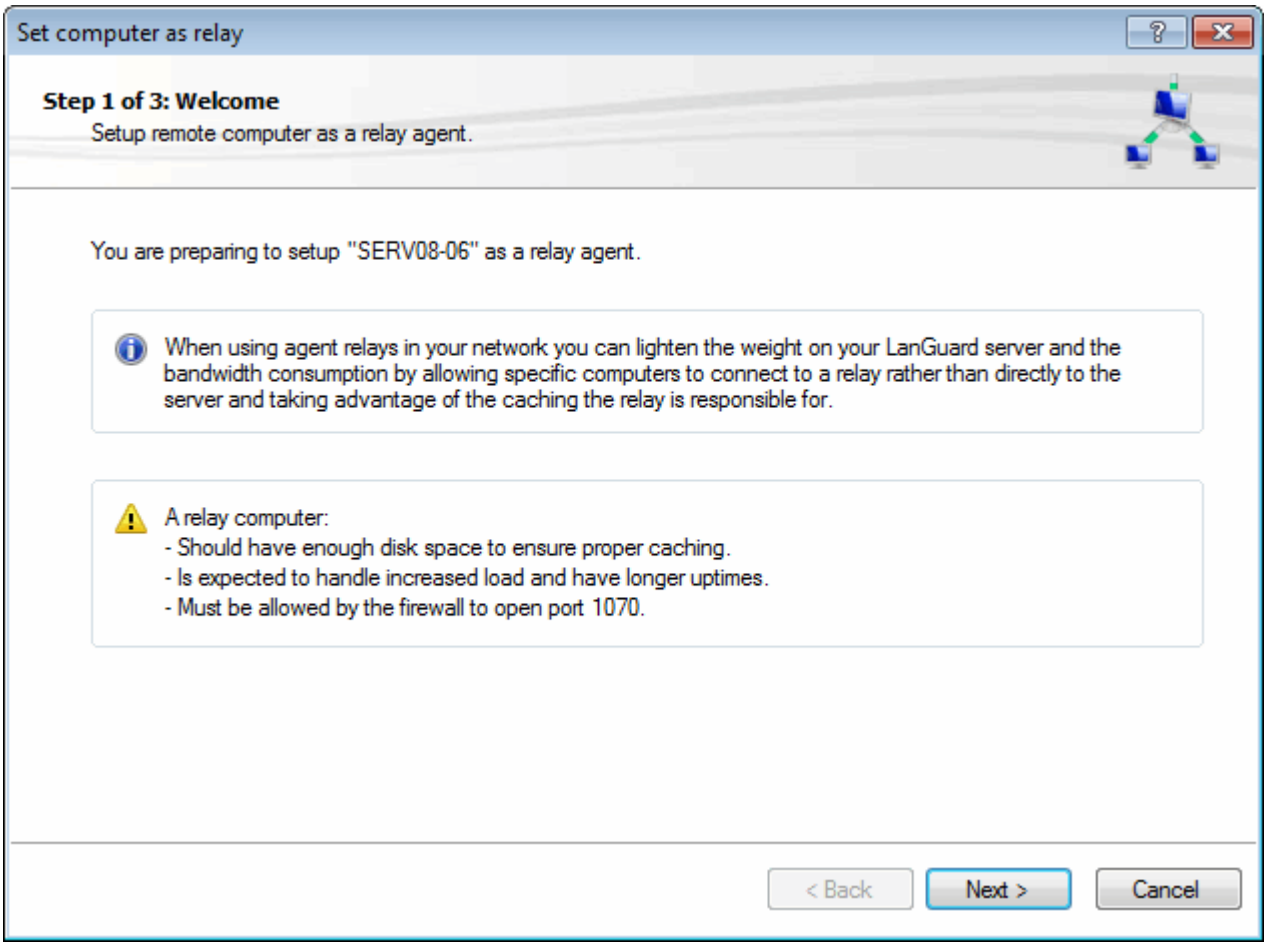
3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

> **NOTE**
> Alternatively, right-click on an computer/group from the computer tree and select **Properties**.



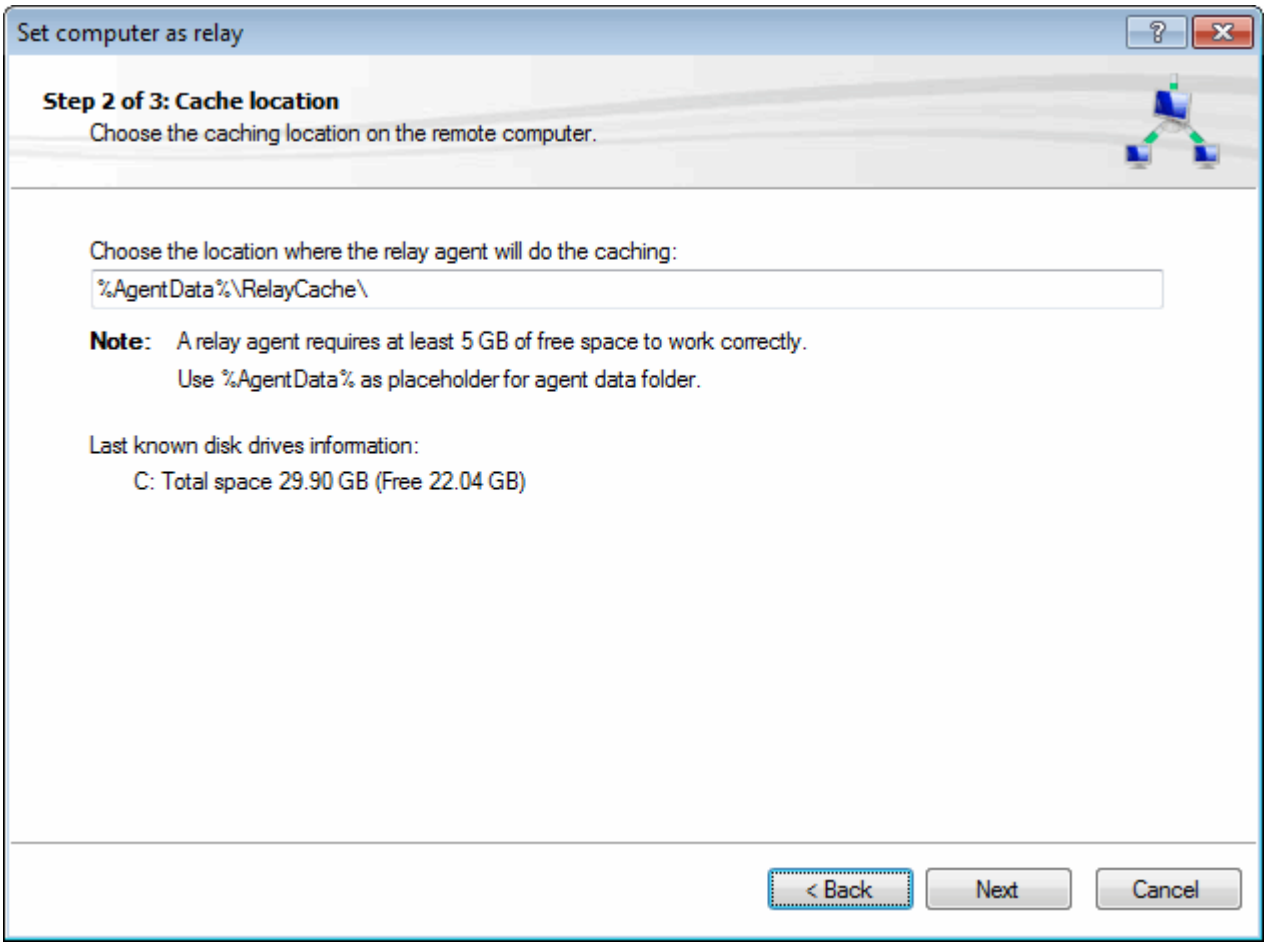
Screenshot 42: Agent Properties dialog

4. From the **Relays** tab, click **Set as relay...**



Screenshot 43: Set computer as relay wizard

5. Carefully ready the warning about resource requirements for the computer running a Relay Agent. Click **Next**.

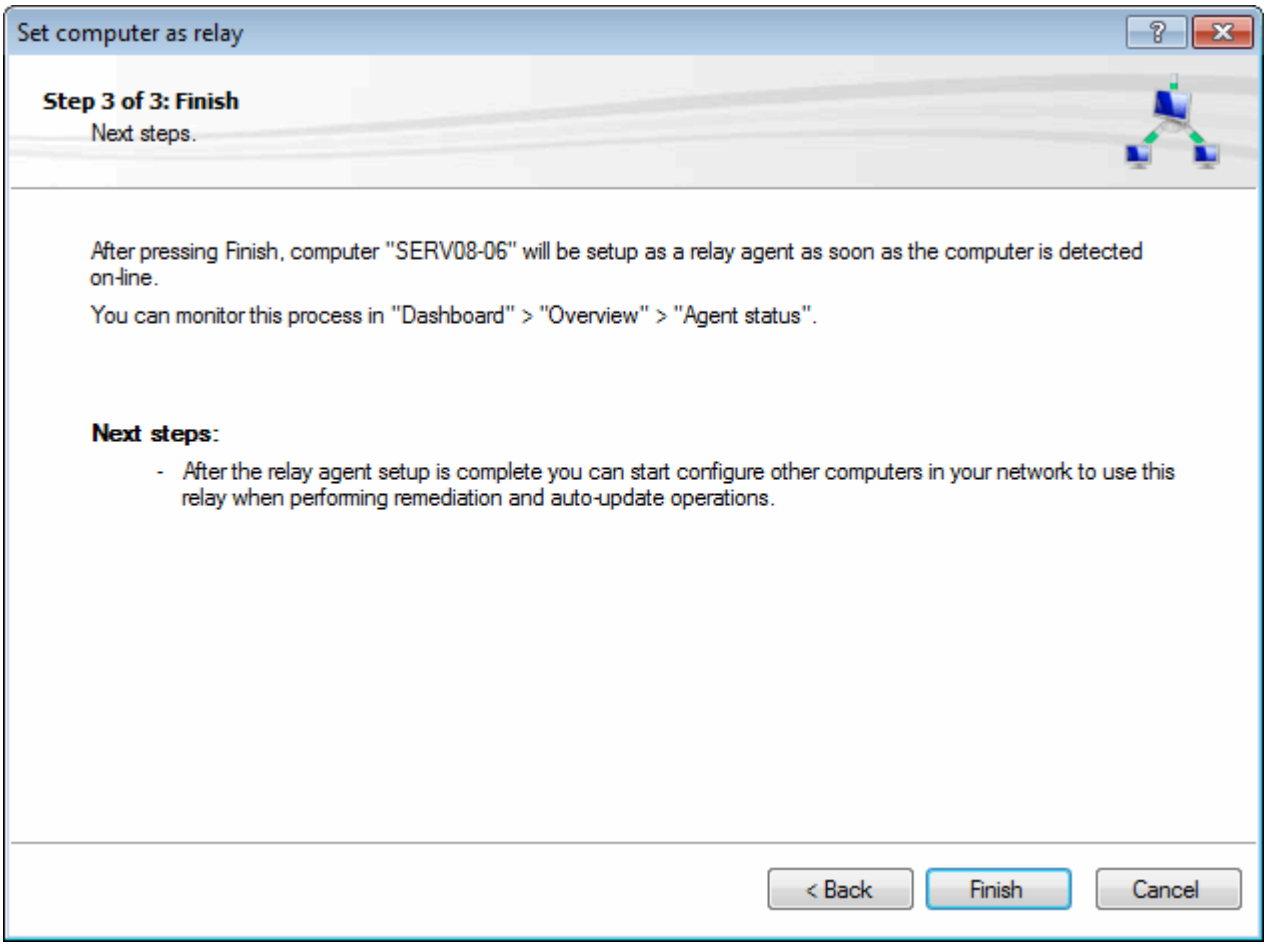


Screenshot 44: Choose caching directory for the new Relay Agent

6. Choose the caching location for the Relay Agent. The caching directory is used by the relay to store audit and remediation information when auditing remote computers. By default, the **RelayCache** folder is created in `C:\ProgramData\GFI\LanGuard 12\RelayCache`. Click **Next**.

NOTE

Use the **%AgentData%** placeholder to quickly refer to the Agent's data folder.



Screenshot 45: Settings summary step

7. Click **Finish**.

> **NOTE**
> After you click **Finish**, the selected Agent is configured as a Relay Agent. You can monitor this process from **Dashboard > Overview > Agent status**.

Configuring Relay Agent advanced options

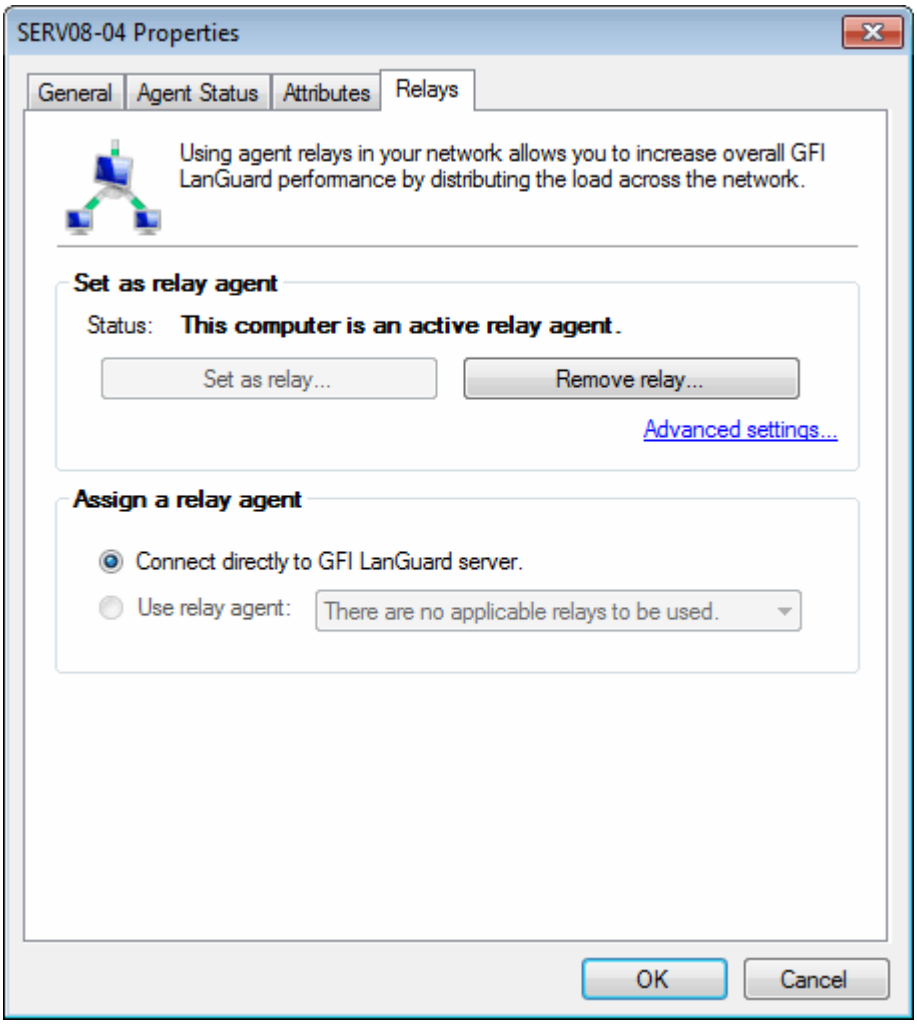
To configure Relay Agent advanced options:

1. Open GFI LanGuard.

2. Click **Configuration** tab **> Agents Management**.

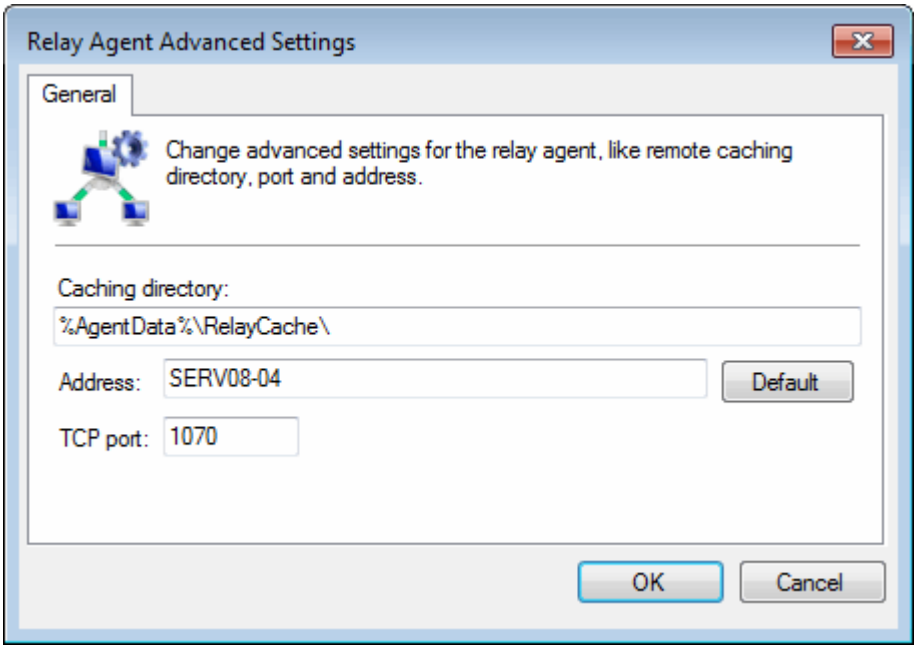
3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

> **NOTE**
> Alternatively, right-click on an computer/group from the computer tree and select **Properties**.



Screenshot 46: Relay Agent properties - Advanced settings

4. Click **Relays** tab > **Advanced settings...**



Screenshot 47: Relay Agent advances settings dialog

5. From the **Relay Agent Advanced Settings** dialog, configure the options described below:

Option	Description
Caching directory	Location where the relay agent caches information when auditing remote computers.
Address	Displays the computer name that is running the relay agent. Click **Default** to restore the field to its original value.
TCP port	Communication port used by the relay agent to communicate with GFI LanGuard server. Port 1072 is assigned by default and is automatically changed if GFI LanGuard detects that port 1072 is being used by another application.

6. Click **OK**

Connecting computers to a Relay

To connect a computer to a Relay:

1. Open GFI LanGuard.

2. Click **Configuration** tab > **Agents Management**.

3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

> **NOTE**
> Alternatively, right-click on an computer/group from the computer tree and select **Properties**.

4. Click **Relays** tab.

5. From the **Assign a relay agent** area, select **Use relay agent** and choose the relay from the drop-down menu.

6. Click **OK**

4.1.6 Managing Agent groups

The computer tree enables you to configure agent properties of groups of computers. To configure computer group properties:

1. From the computer tree, right-click a group of computers and click **Properties**.

2.(Optional) From **General** tab, specify name, type and authentication method for the selected group.

3. Select **Agent Status** tab, and configure the following options:

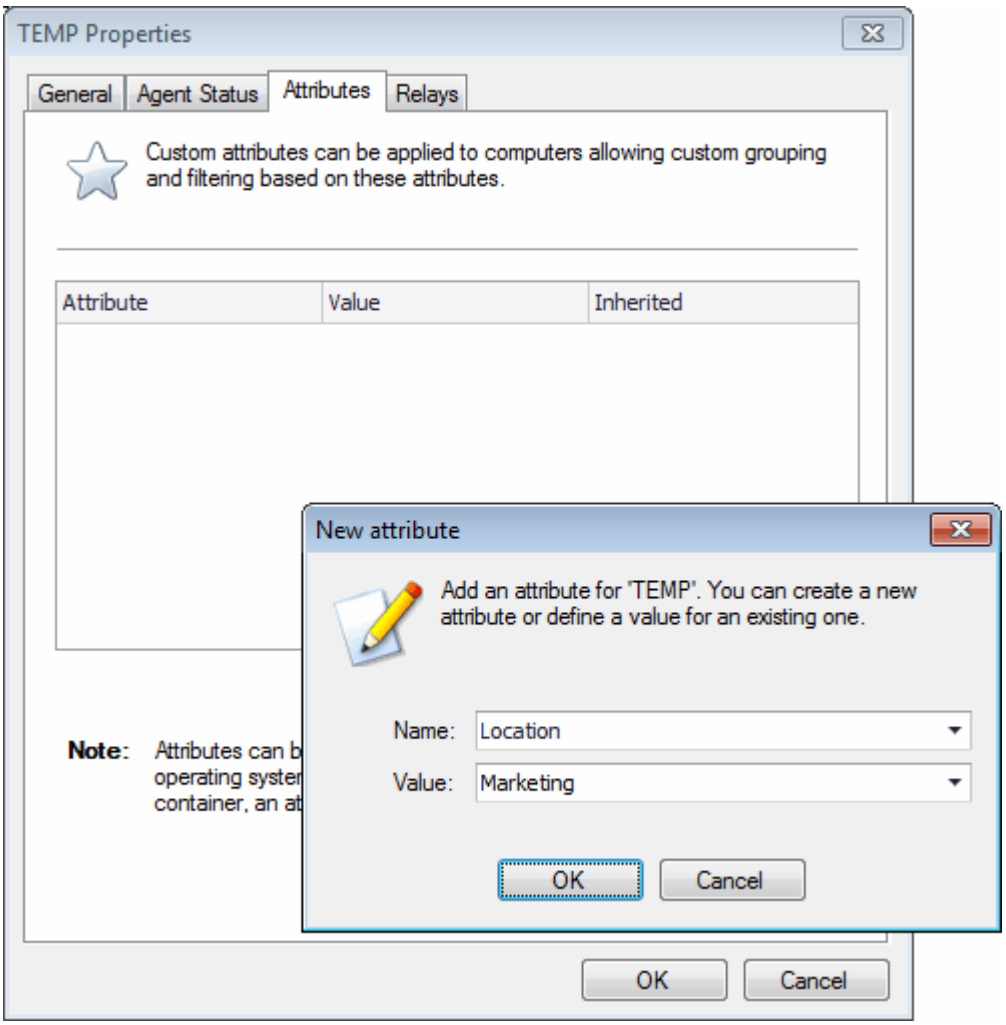
Option	Description
Enable automatic agents deployment	Automatically deploy agents on newly discovered computers.
Remove all agents	Remove all installed agents from this group.
Change scan schedule	Configure the schedule, when GFI LanGuard searches for new computers.
Scanning profile	Configure the audit schedule; when target computers are scanned.
Auto remediation settings	Configure the auto remediation actions to perform on all computers in this group. For more information, refer to Configuring Agent auto-remediation (page 183).

4. Select **Network Discovery** and configure the following options:

Option	Description
Check automatically for new machines in this group	GFI LanGuard will search for new machines automatically.

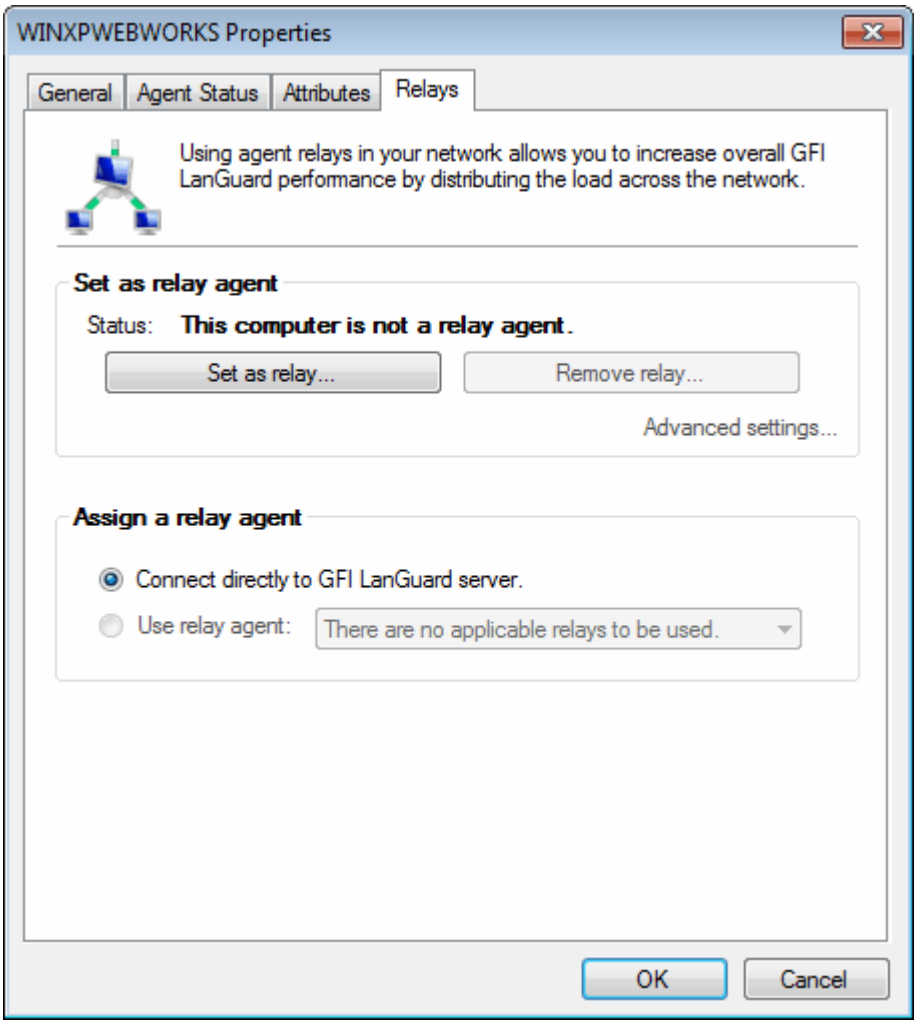
Option	Description
Change schedule	Change the schedule when GFI LanGuard searches for new computers.
Run now	Run network discovery.
Scan OU recursively	Recursively, loop through all organization units and enroll computers.

5. Select **Attributes** tab to manage the attributes assigned to the computer selected. Use the **Add**, **Edit** and **Remove** buttons to manage attributes.



Screenshot 48: Agent Attributes

6. Click **Relays** tab to configure agent relays. Relays enable computers other than the one hosting GFI LanGuard to act as GFI LanGuard server. This helps you load-balance traffic directed to that machine and optimize network scanning performance.



Screenshot 49: Agent Relays

7. Configure the options described below:

Option	Description
Connect directly to GFI LanGuard server	The selected computer will download product updates and patches from the GFI LanGuard server.
Use relay agent	The selected computer will use a relay agent to download product updates and patches. Select the relay agent to use from the drop down list.

> **Note**
> Some options are disabled because they are applicable only for single computers.

8. Click **OK**

4.1.7 Updating Agents

GFI LanGuard Agents manage updates for three primary components:

» **Product updates** - updates to the agent itself. Ensures that agents are running with the latest updates as released by GFI

» **Threat definition updates** - vulnerability definitions that enable agents to detect the latest threats as soon as they are detected and fixed by software vendors

» **Security updates** - missing third-party and system, patches and service packs detected on a target computer

GFI LanGuard merges **Product** and **Threat Definition** updates and are handled as a single entity; separately from **Security** updates.

Threat definition updates

GFI LanGuard definition updates are important to run at regular intervals to ensure that any updates, as released by vendors, are detected and reported back by GFI to your solution. The **UpdateAgent** Method exposes an out parameter in which the results XML are built. It is synchronous and the update process will not return a value, until it ends.

GFI recommends triggering a GFI LanGuard Agent update session, immediately after the installation. This ensures that agents:

» Acquire the latest patch definition files from GFI. This ensures that scans always detect the latest missing patches

» Acquire the latest vulnerability definitions as soon as they become available from GFI

» Acquires product updates to fix bugs which surfaced after GFI LanGuard SDK was released.

With the increasing number of sophisticated cyber threats occurrences, GFI recommends you to check for updates once every 24 hours on every end-point or designated concentrator.

A lesson learned by GFI is to trigger agents to check for updates at random time intervals. Configuring agents to check for and download updates simultaneously, causes undesired network bandwidth problems if a significant number of downloads occur at the same time. Randomizing the update times is enough to smoothen out the update operation, effectively making the process unnoticeable.

IMPORTANT

» GFI LanGuard Agents connect to ***.software.gfi.com/lnsupdate/** to retrieve threat definition updates. Ensure that this URL is not blocked by your firewall and/or web gateway.

» GFI LanGuard definition updates do not include patches and service packs as release by Microsoft and other vendors over time. These patch updates are treated separately to all of the above.

Security updates

Security updates refer to the missing patches and service packs detected on target computers by patch management scans. These updates fix bugs or performance issues of the operating system and third-party software installed on a computer. Patch updates are downloaded directly from the vendors servers. Microsoft updates are downloaded from Microsoft and third parties such as Adobe and Firefox are downloaded from third party servers respectively. GFI does not tamper or provide customized installations of patch and service pack updates. We distribute patches as provided and signed off by the vendor.

Supported software vendors

The following table provides you with links to supported Microsoft and Third-Party application patches:

Supported Patches	Link
Supported Microsoft applications	https://www.gfi.com/lannetscan/msappfullreport.htm
Supported Microsoft applications (Detailed)	https://www.gfi.com/lannetscan/msfullreport.htm

Supported Patches	Link
Supported MAC OS X applications	https://www.gfi.com/lannetscan/macfullreport.htm
Supported Third-Part applications (Detailed)	https://www.gfi.com/lannetscan/3pfullreport.htm
Supported security applications	https://www.gfi.com/lannetscan/securityappfullreport.htm
Supported OVAL and CVE checks	https://www.gfi.com/lannetscan/ovalfullreport.htm

IMPORTANT

Ensure that end point firewall settings, web-gateways and caching proxy server allow traffic from the below URLs:

- gfi-downloader-137146314.us-east-1.elb.amazonaws.com
- *software.gfi.com/lnsupdate/
- *.download.microsoft.com
- *.windowsupdate.com
- *.update.microsoft.com

4.2 Scanning Your Network

This topic provides you with information about the different scanning profiles that ship with GFI LanGuard, as well as how to trigger immediate or scheduled manual scans. Select the most suitable scanning profile and scanning mode (such as using Agent-less versus Agent-based scans), depending on the availability and location of your scan targets.

Topics in this section:

4.2.1 About Scanning Profiles

GFI LanGuard enables you to scan your IT infrastructure for particular vulnerabilities using pre–configured sets of checks known as scanning profiles. Scanning profiles enable you to scan your network targets and enumerate only specific information. For example, you may want to use a scanning profile that is set to be used when scanning the computers in your DMZ as opposed to your internal network.

In practice, scanning profiles enable you to focus your vulnerability scanning efforts on to a specific area of your IT infrastructure, such as identifying only missing security updates. The benefit is that you have less scan results data to analyze; tightening up the scope of your investigation and help you quickly locate the information that you require, more easily.

Through multiple scanning profiles, you can perform various network security audits without having to go through a reconfiguration process for every type of security scan required.

4.2.2 Available Scanning Profiles

GFI LanGuard ships with the default scanning profiles described in the sections below. To create your own custom scanning profiles, refer to Creating a new Scanning Profile. Use the information provided in the following sections to understand what each scanning profile detects on your scan targets:

- Complete/Combination Scans profiles
- Vulnerability Assessment profiles
- Network and Software Audit profiles

Complete/Combination Scans

Complete/Combination Scans profiles	
Full Vulnerability Assessment	Use this scanning profile to enumerate particular network vulnerabilities such as open TCP/UDP ports commonly exploited by Trojans as well as missing patches and service packs. The list of vulnerabilities enumerated by this profile can be customized through the Vulnerabilities tab. Installed USB devices and applications are not enumerated by this profile. This profile will scan for all vulnerabilities. This includes vulnerabilities which have an associated Microsoft® patch to them and which are considered missing patches.
Full Scan (Active)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN environments.
Full Scan (Slow Networks)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more… The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with WAN environments.

Vulnerability Assessment

Vulnerability Assessment profiles	
Top SANS 20 Vulnerabilities	Use this scanning profile to enumerate all vulnerabilities reported in the SANS top 20 list.
High Security Vulnerabilities	Use this scanning profile to enumerate open TCP/UDP ports and high security vulnerabilities. The list of TCP/UDP ports and high security vulnerabilities that will be enumerated by this profile can be customized through the TCP/UDP Ports tabs and the Vulnerabilities tab respectively.
Last Year's Vulnerabilities	Use this scanning profile to enumerate network vulnerabilities that emerged during the last 12 months.
Only Web	Use this scanning profile to identify web–server specific vulnerabilities. This includes scanning and enumerating open TCP ports that are most commonly used by web–servers such as port 80. Only TCP ports commonly used by web–servers are scanned by this profile. Network auditing operations as well as enumeration of vulnerabilities and missing patches are not performed using this profile.
Missing Patches	Use this scanning profile to enumerate missing patches. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.
Critical Patches	Use this scanning profile to enumerate only missing patches that are tagged as critical. The list of critical patches that will be enumerated by this profile can be customized through the Patches tab.
Last Month's Patches	Use this scanning profile to enumerate only missing patches that were released last month. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.

Vulnerability Assessment profiles	
Only Service Packs	Use this scanning profile to enumerate missing service packs. The list of service packs that will be enumerated by this profile can be customized through the Patches tab.
Non-Microsoft® Patches	Use this scanning profile to enumerate missing Third-Party patches, such as Adobe products.
Security Patches	Use this scanning profile to enumerate missing Microsoft® and non-Microsoft® Security Patches on your scan targets.

Network & Software Audit

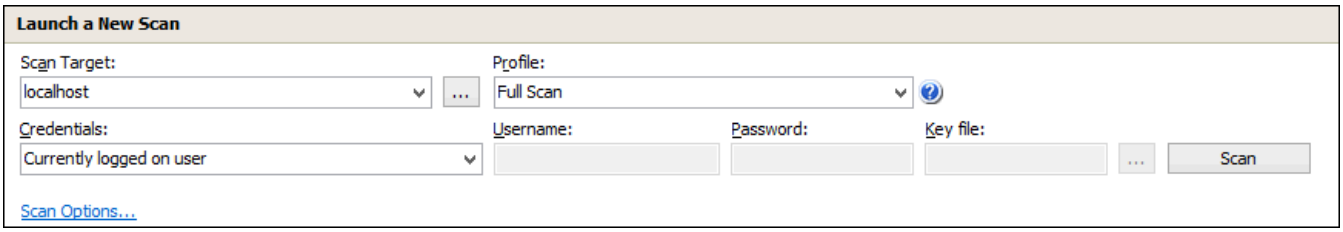
Network & Software Audit profiles	
Trojan Ports	Use this scanning profile to enumerate open TCP/UDP ports that are commonly exploited by known Trojans. The list of TCP/UDP ports to be scanned can be customized through the TCP Ports and UDP Ports tabs respectively. Only the TCP/UDP ports commonly exploited by known Trojans are scanned by this profile. Network auditing operations as well as enumeration of other open TCP/UDP ports and missing patches are not performed by this profile.
Port Scanner	Use this scanning profile to enumerate open TCP/UDP ports including those most commonly exploited by Trojans. The list of ports that will be enumerated by this profile can be customized through the TCP/UDP ports tab.
Software Audit	Use this scanning profile to enumerate all software applications installed on scan targets. This includes security software such as antivirus and antispyware.
Full TCP & UDP Scan	Use this scanning profile to audit your network and enumerate all open TCP and UDP ports.
Only SNMP	Use this scanning profile to perform network discovery and retrieve information regarding hardware devices (routers, switches, printers, etc.) that have SNMP enabled. This enables you to monitor network–attached devices for conditions that require administrative attention.
Ping Them All	Use this scanning profile to audit your network and enumerate all computers that are currently connected and running.
Share Finder	Use this scanning profile to audit your network and enumerate all open shares either hidden or visible. No vulnerability checks are performed by this profile.
Uptimes	Use this scanning profile to audit your network and identify how long each computer has been running since the last reboot.
Disks Space Usage	Use this scanning profile to audit your network and retrieve system information on available storage space.
System Information	Use this scanning profile to retrieve system information such as operating system details, wireless/virtual/physical network devices connected, USB devices connected, installed applications and more.
Hardware Audit	Use this scanning profile to audit your network and enumerate all hardware devices currently connected to your network computers.
Network Discovery	Use this scanning profile to enumerate any IP enabled device connected to your network.

4.2.3 Manual scans

Manual scan is the process of performing audits on target computers without using agents. To perform a manual scan on a specific computer:

1. Launch GFI LanGuard.

2. From the **Home** tab click **Launch a Scan**. Alternatively, click the **Scan** tab.



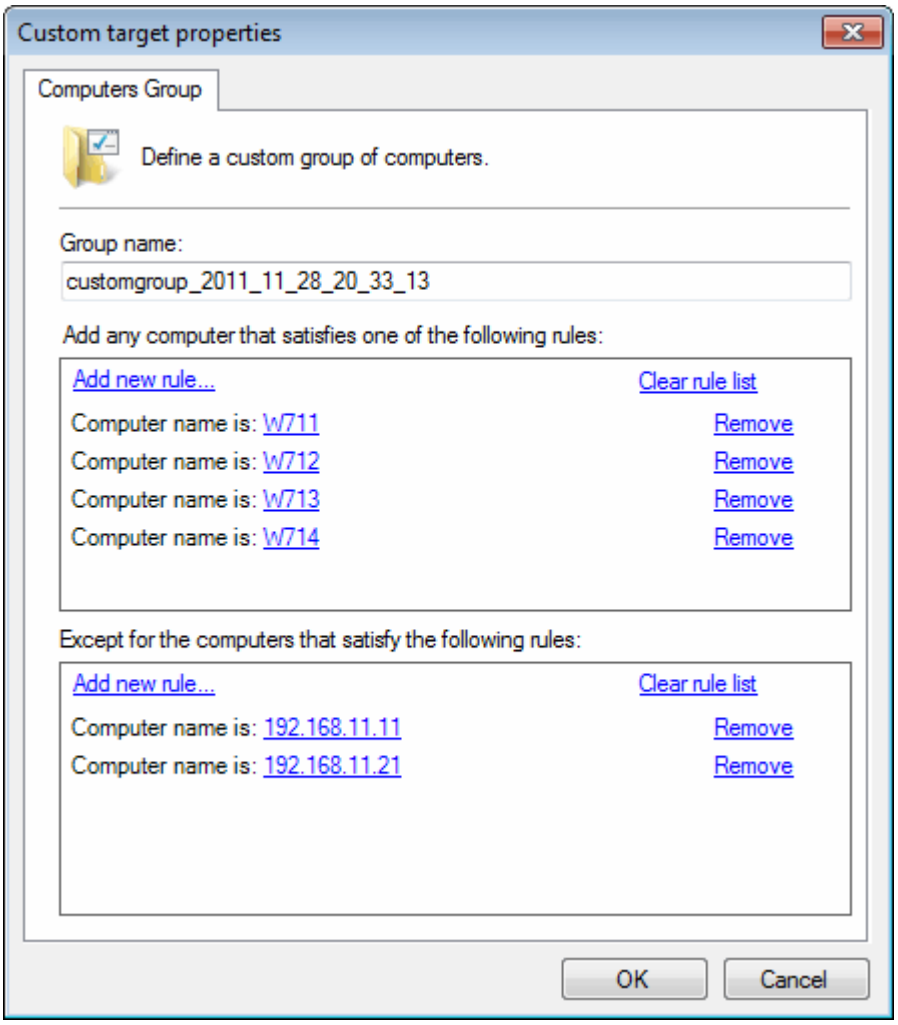
Screenshot 50: Manual scan settings

3. From the **Scan Target** drop–down menu, select the target computer or group of computers to scan using the following options:

Option	Description
Localhost	Audit the local host where GFI LanGuard is installed.
Domain: primary domain	Audit the entire domain / workgroup of the computer / server where GFI LanGuard is installed.

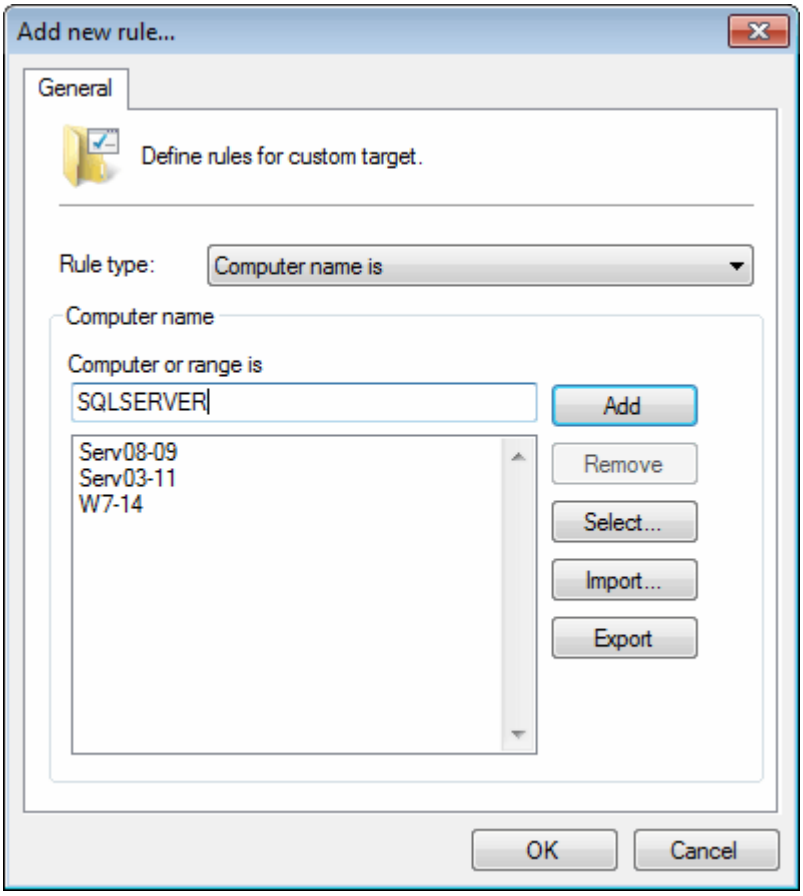
> **NOTE**
> Optionally, from the computer tree, right-click a computer/computer group and select **Scan > Custom Scan**.

4. Click the browse button (**...**) to define custom rules for adding scan targets.



Screenshot 51: Custom target properties

5. From the **Custom target properties** dialog, click **Add new rule** links to create a custom rule for computers you want to scan or exclude from scanning.



Screenshot 52: Add new rule...

6. From the **Add new rule** dialog, select the **Rule type** described below to add computers:

Rule type	Description
Computer name is	Search and add computers by name. Key–in a valid computer name and click **Add** for each computer. Click **OK** to apply changes.
Computers file list is	Search and add computers from a text file. Click the browse button and locate the text file. Click **OK** to apply changes. **NOTE** When submitting a list of target computers from file, ensure that the file contains only one target computer name per line.
Domain name is	Search and add computers that are members of a domain. Select the domains from the list and click **OK**
IP address is	Search and add computers by IP address. Select **This computer** to add the local host or **Scan another computer** to add a remote computer. Key–in the IP address if required and click **OK**

Rule type	Description
IP address range is	Search and add computers within an IP range. Select **Scan an IP address range** and key in the IP range or select CIDR subnet and key–in the range using CIDR notation. **NOTE** The Classless Inter–Domain Routing (CIDR) provides an alternative way of specifying an IP address range. The notation is as follows: `<Base address> / <IP network prefix>`. Example: 192.168.0.0/16
Organization unit is	Search and add computers within an organizational unit. Click **Select** and from the list select the Organizational units. Click **OK**

7. Once the rules are added, click **OK** to close the **Add new rule dialog**. Click **OK** to close the **Custom target properties** dialog and return to the scan settings.

8. From the **Profile** drop–down menu, select the scan profile that you want GFI LanGuard to action during the scan. For more information, refer to Available Scanning Profiles (page 95).

9. From the **Credentials** drop–down menu, select the log–on method used by GFI LanGuard to log onto the scan targets. The table below describes the available options:

Option	Description
Currently logged on user	Use the current logged on user credentials when logging on scan targets.
Alternative credentials	Use custom credentials. Key–in the user name and password to use.
A null session	Log onto scan targets using a null session. The user will log onto the target machine as an anonymous user.
A private key file	Log onto UNIX/LINUX/MAC machines using SSH. Three elements are required for the login: » Username » SUDO password » path to the file that stores the private key

NOTE
The credentials provided need to have administrator privileges in order for GFI LanGuard to log–on to the target computers and carry out the network audit.

10. (Optional) Click **Scan Options** and configure the options described below:

Option	Description
Use per computer credentials when available	Login to the target machines using the credentials specified in the Dashboard
Remember credentials	Use the configured credentials as default when performing an audit.
Wake up offline computers	GFI LanGuard attempts to power on offline computers using Wake-on-LAN. For more information, refer to Configuring Wake-on-LAN on scan targets (page 178).
Shut down computers after scan	Shut down when a scan is complete.

11. Click **Scan** to start auditing the selected targets.

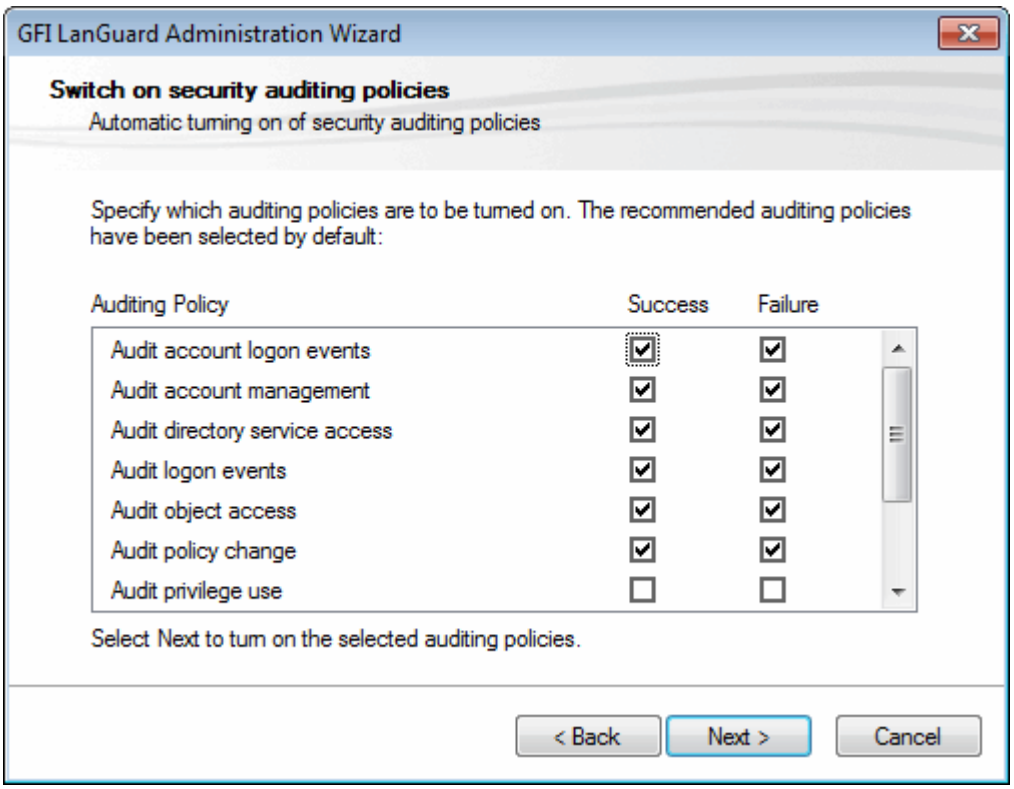
4.2.4 Enabling security audit policies

An important part of any security plan is the ability to monitor and audit events on your network. These event logs are frequently referenced to identify security holes or breaches. Identifying attempts and preventing them from becoming successful breaches of your system security is critical. In Windows, you can use **Group Policies** to set up an audit policy that can track user activities or system events in specific logs.

To keep track of your system auditing policy, GFI LanGuard collects the security audit policy settings from target computers and includes them in the scan result. To access more information on the result click on **Security Audit Policy** sub–node.

Apart from gaining knowledge on the current audit policy settings, you can also use GFI LanGuard to access and modify the audit policy settings of your target computers. To achieve this:

1. After scanning a remote computer, from the **Scan Results Overview** panel, right–click on the respective target computer and select **Enable auditing on** > **This computer/Selected computers/All computers**.



Screenshot 53: The audit policy administration wizard

2. Select/unselect auditing policies accordingly, and click **Next** to deploy the audit policy configuration settings, on the target computer(s).

3. At this stage, a dialog will show whether the deployment of audit policy settings was successful or not. To proceed to the next stage click **Next**. Click **Back** to re–deploy settings on failed computers.

4. Click **Finish** to finalize configuration. Restart a scan to update results.

4.2.5 Scheduled scans

A scheduled scan is a network audit that is scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically. Scheduled scan status is monitored using the **Activity Monitor** tab > **Security Scans**.

GFI recommends scheduled scans:

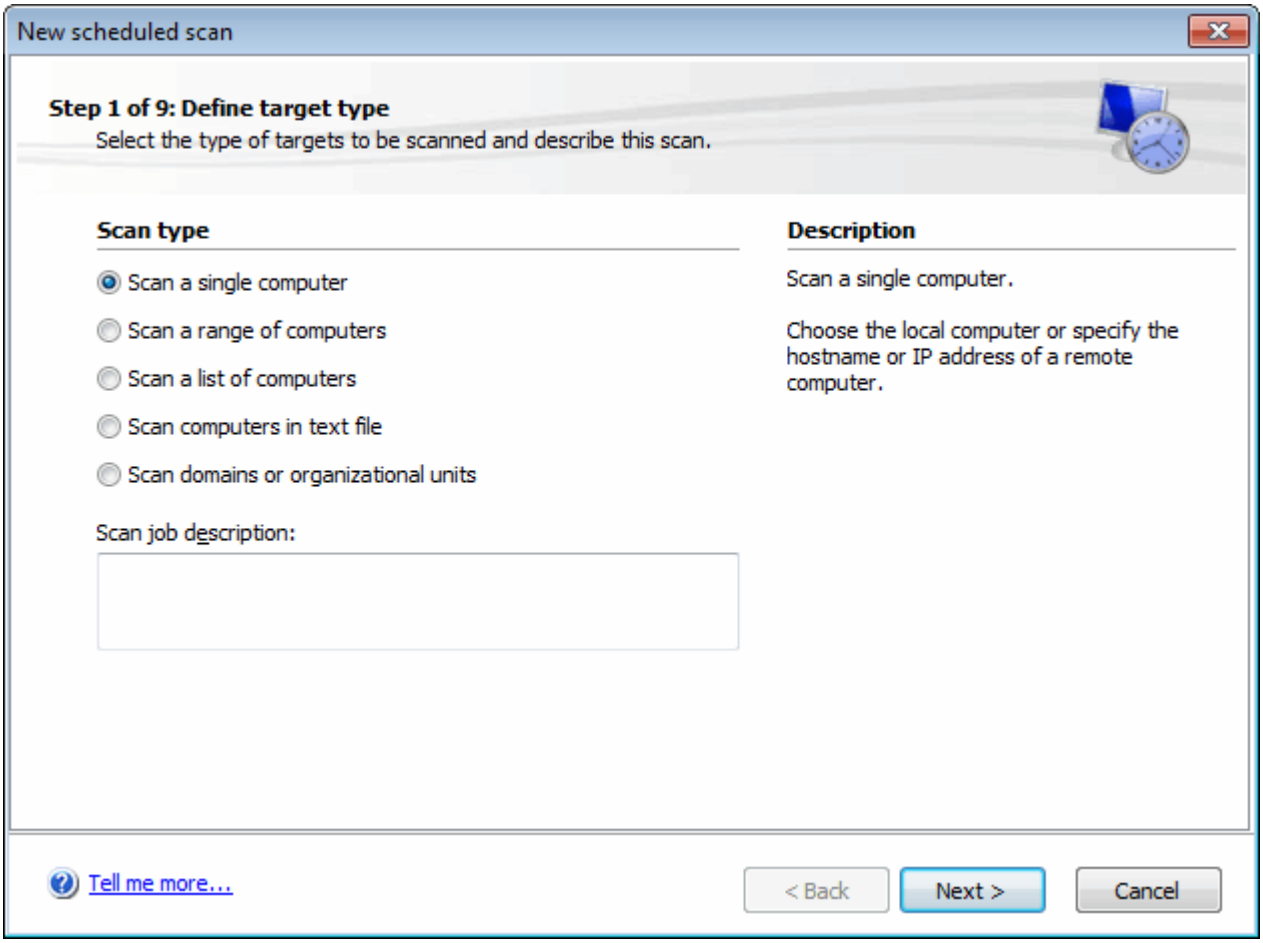
- When GFI LanGuard Agents are not deployed on the target computers
- To automatically perform periodical/regular network vulnerability scans using same scanning profiles and parameters
- To automatically trigger scans after office hours and generate alerts and auto–distribution of scan results via email
- To automatically trigger auto–remediation options, (Example: Auto-download and deploy missing updates).

The following sections contain information to guide you in configuring and executing scheduled scans:

- Creating a scheduled scan
- Editing scheduled scan settings
- Configuring scheduled scan properties

Creating a scheduled scan

1. Launch GFI LanGuard.
2. Click **Configuration** tab **>Scheduled Scans**.
3. From **Common Tasks**, select **New scheduled scan**.



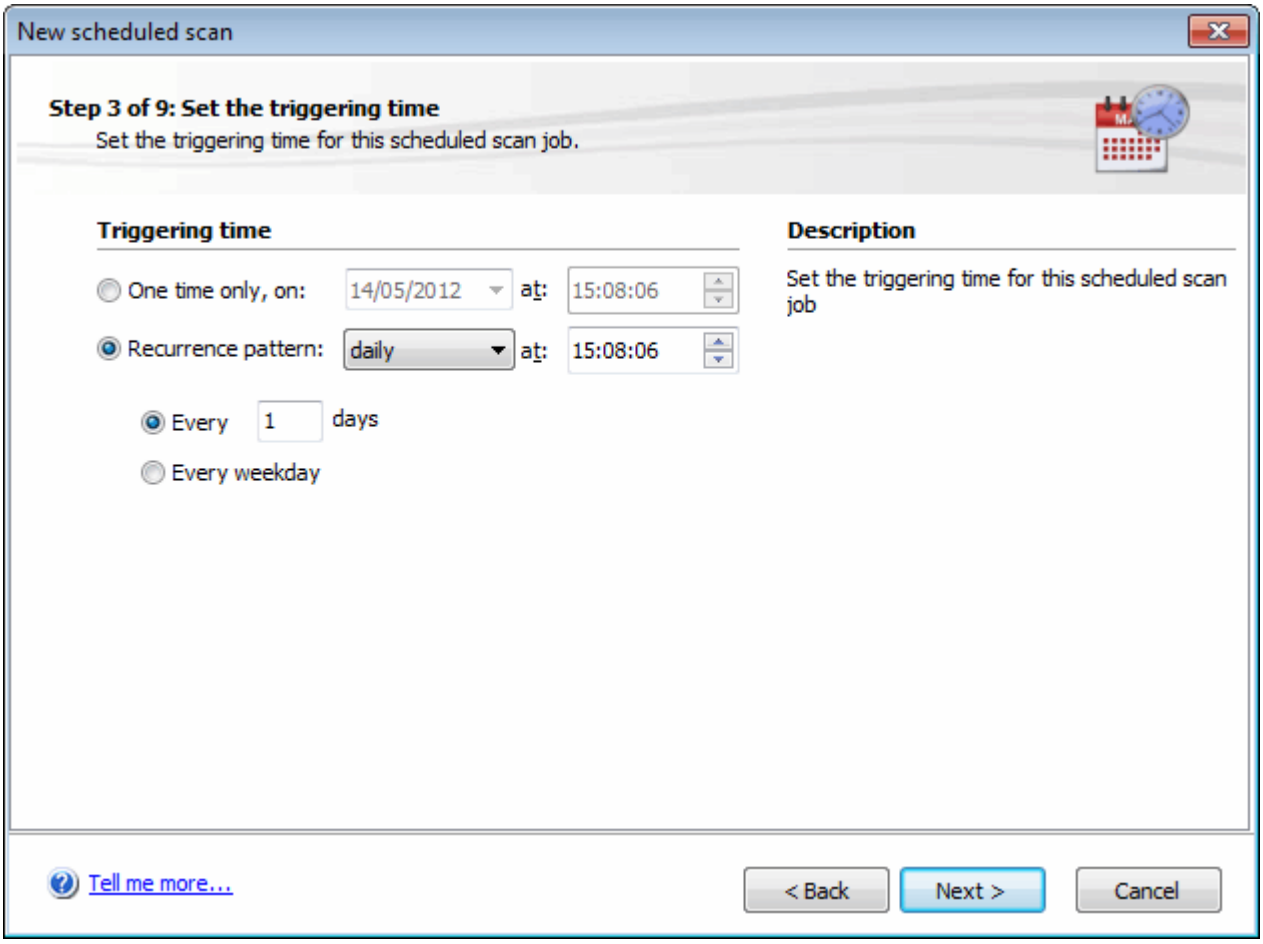
Screenshot 54: New Scheduled Scan dialog

4. Select one of the options described below and click **Next**.

Option	Description
Scan a single computer	Scan local host or one specific computer.

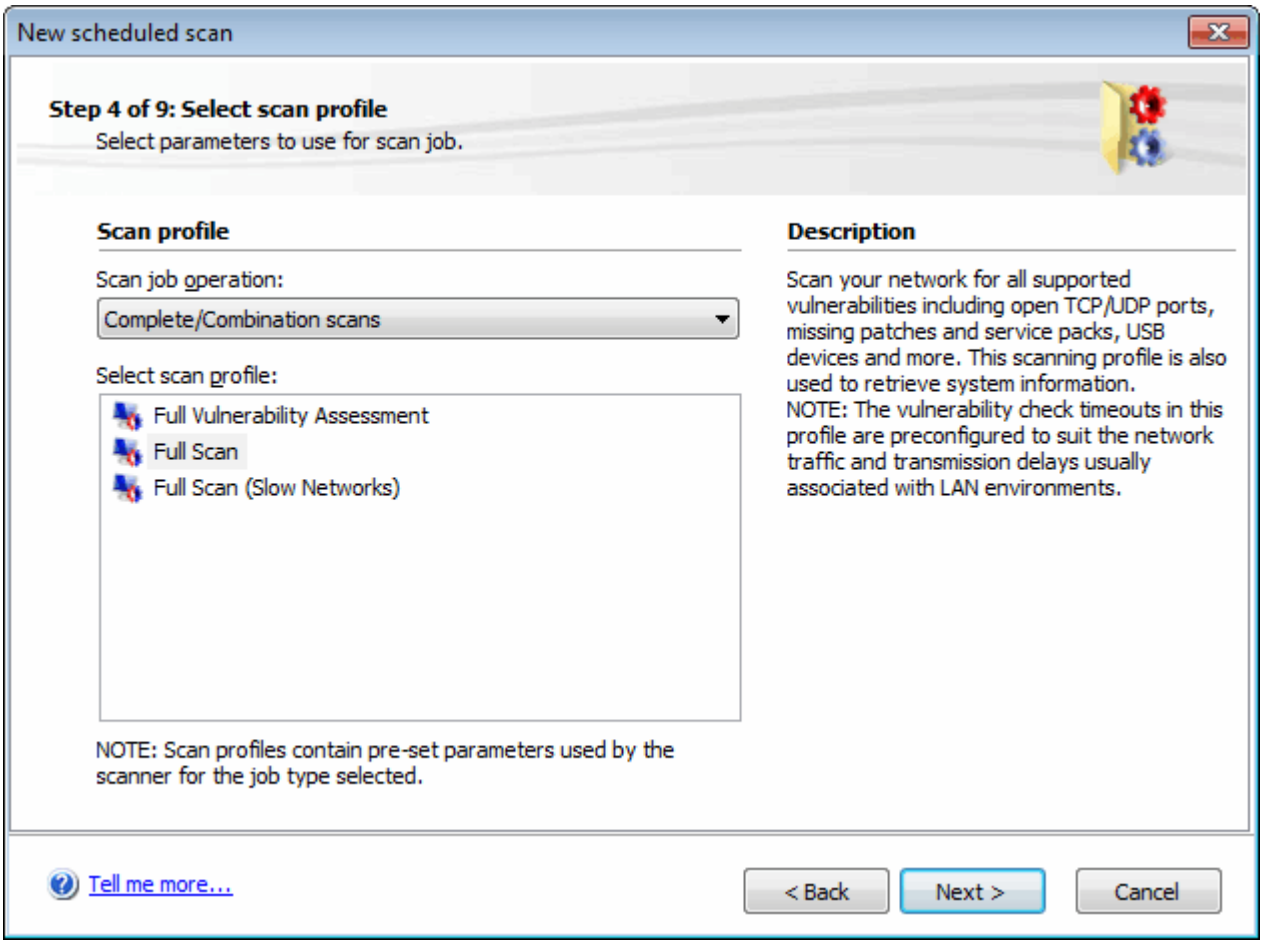
Option	Description
Scan a range of computers	Scan a number of computers defined through an IP range.
Scan a list of computers	Create manually a list of targets, import targets from a file or select targets from the network list.
Scan computers in text file	Scan targets enumerated in a specific text file.
Scan a domains or organizational units	Scan all targets connected to a specified domain/organizational unit.

5. Depending on the option selected in the previous step, specify the respective target computer(s) details and click **Next**.



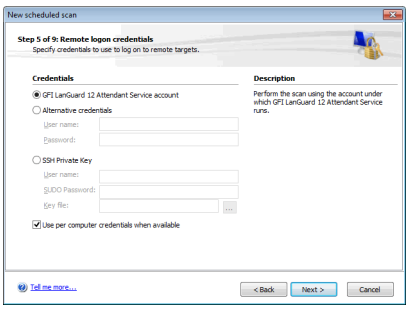
Screenshot 55: Scheduled scan frequency

6. Specify date/time/frequency of the new scheduled scan and click **Next**.



Screenshot 56: Select scanning profile

7. From the **Scan job operation** drop-down menu, select the scanning profile to be used during the scan and click **Next**. For more information, refer to Available Scanning Profiles (page 95).

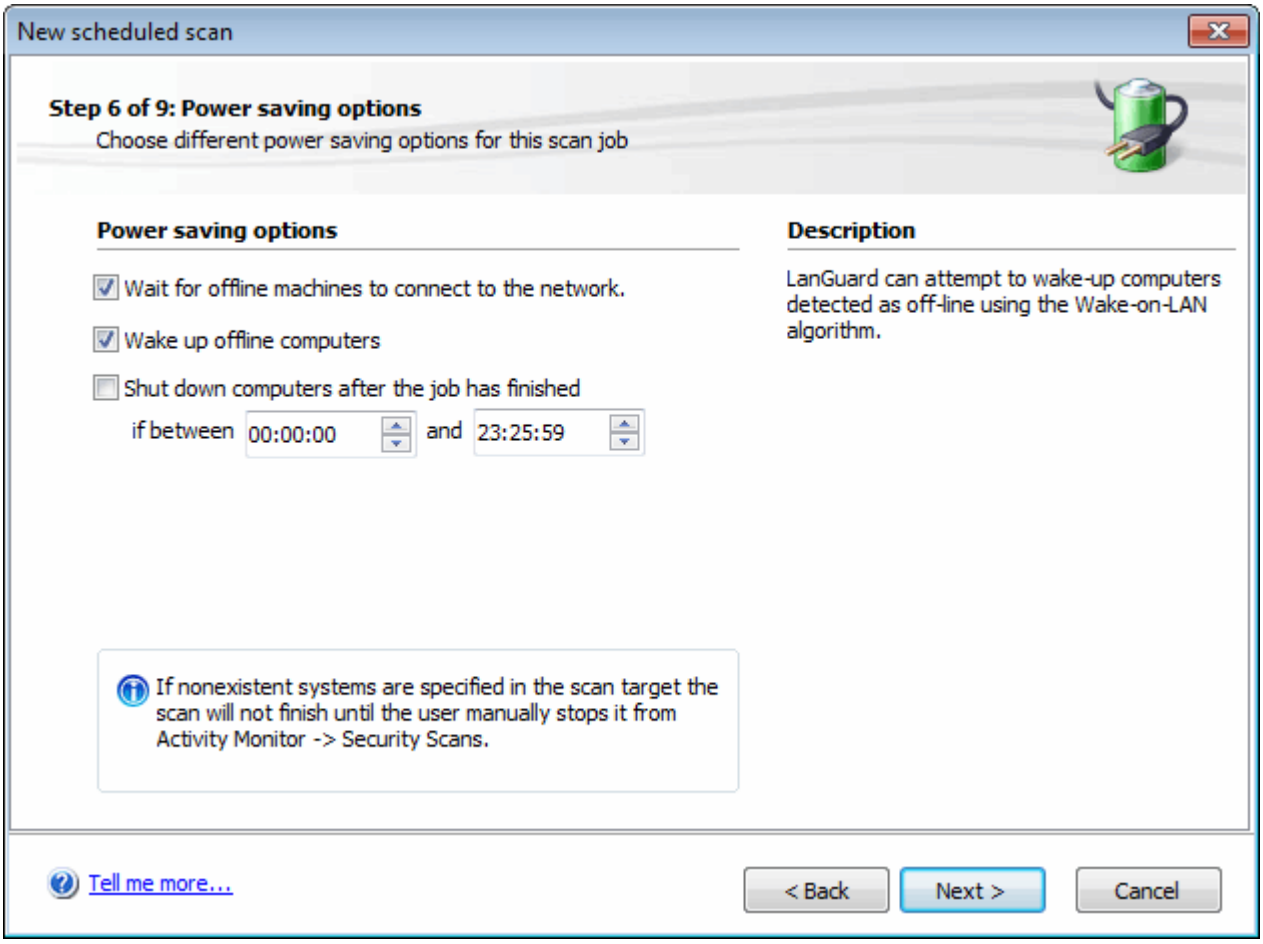


Screenshot 57: Remote logon credentials

8. (Optional) Specify **Remote logon credentials** and click **Next**. Remote logon credentials can be either one of the following:

Option	Description
GFI LanGuard 12 Attendant Service account	Performs the scan using the credentials specified while installing GFI LanGuard.
Alternative credentials	Specify alternate credentials to connect to the scan computers. **NOTE** Ensure the supplied credentials have administrative privileges.

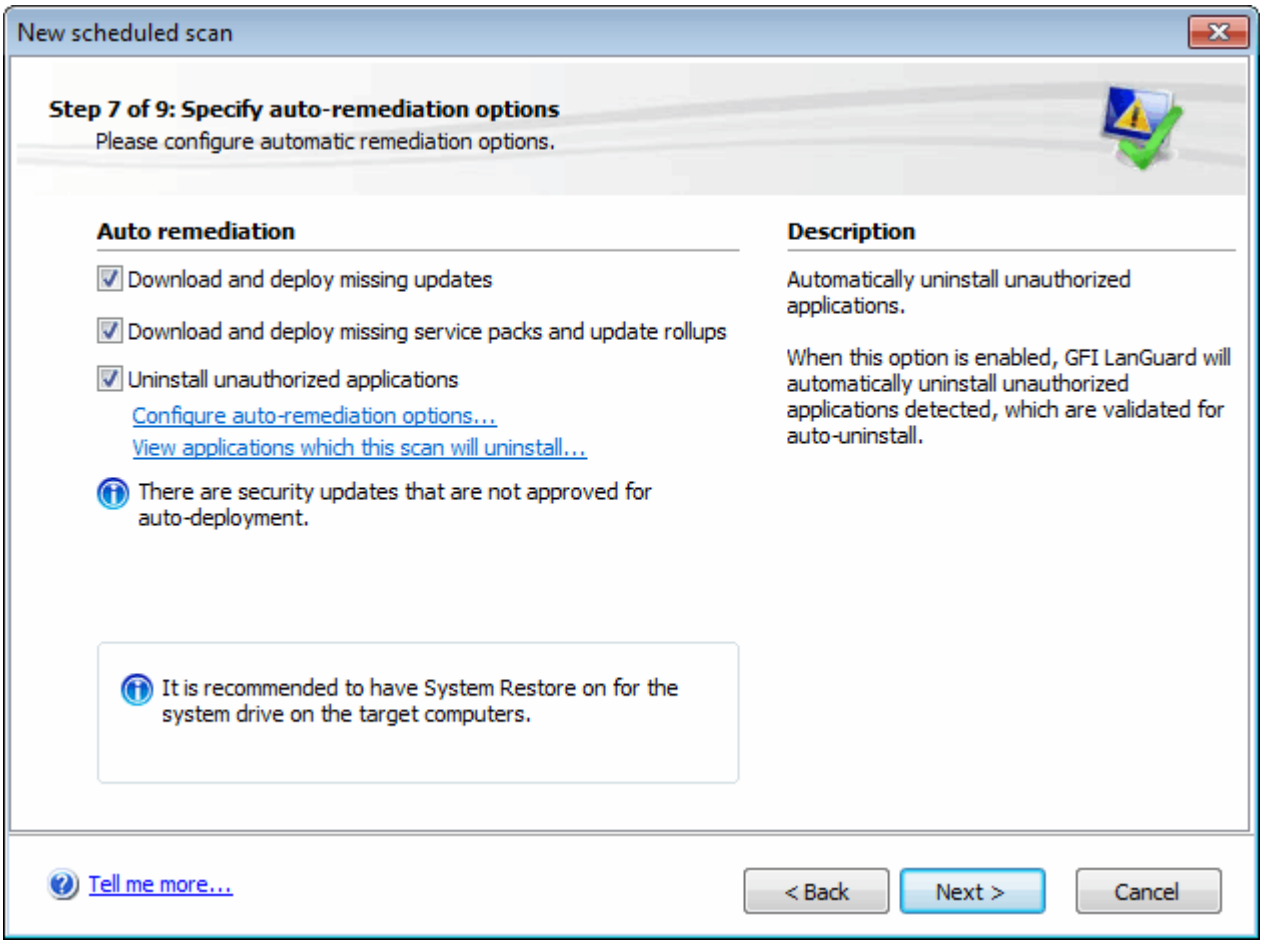
Option	Description
SSH Private Key	Key in a username with respective SUDO password and select the key file used to logon to UNIX/LINUX/MAC based systems.
Use per computer credentials when available	Use predefined credentials for the scan being configured.



Screenshot 58: Scheduled scan reporting options

9. From the **Power saving** options, configure the following options:

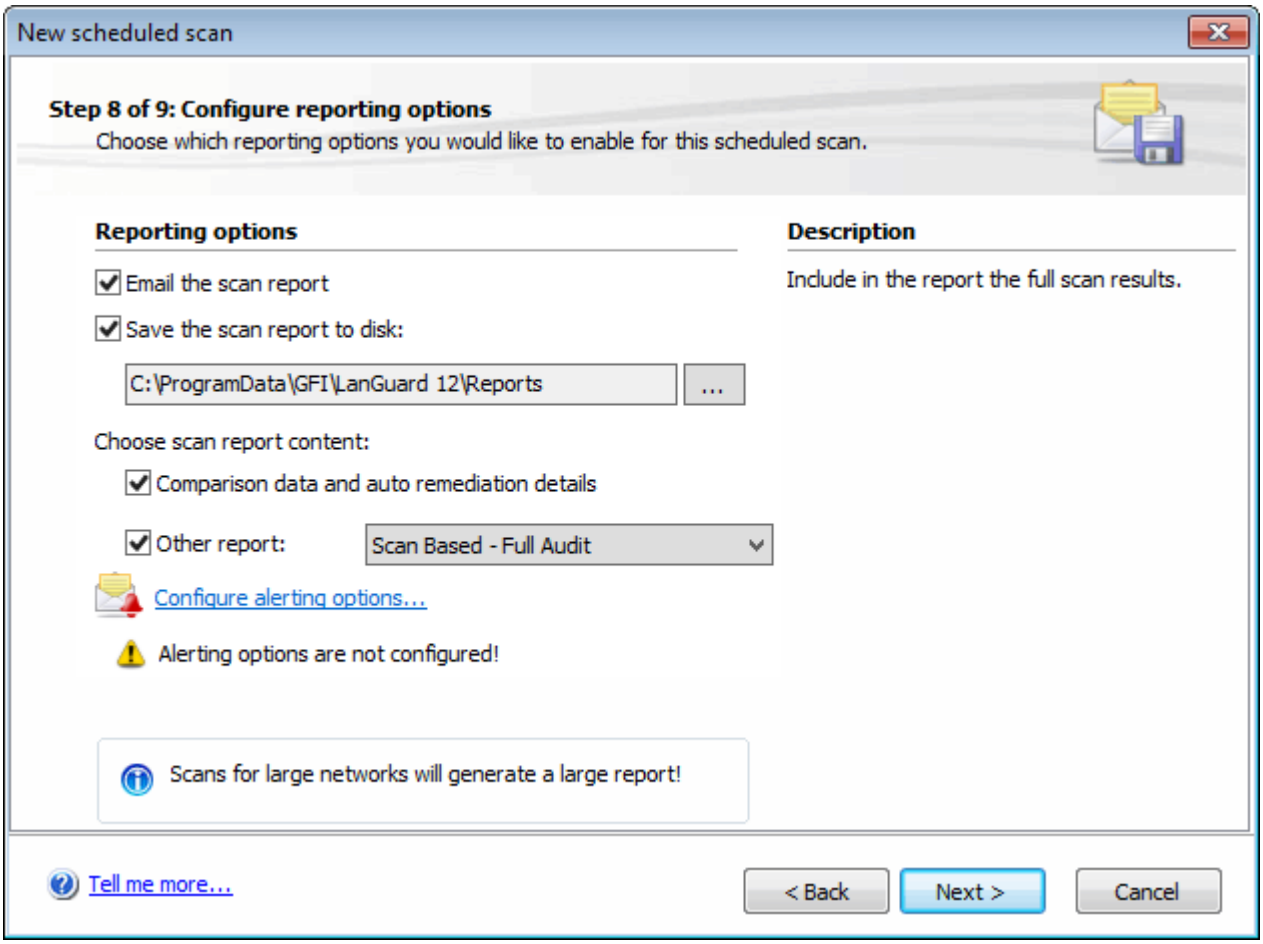
Option	Description
Wait for offline machines to connect to network	If this option is selected, GFI LanGuard attempts to wait for offline machines to connect to the network.
Attempt to wake up offline computers	GFI LanGuard attempts to power on offline machines using Wake-on-LAN. For more information, refer to Configuring Wake-on-LAN on scan targets (page 178).
Shut down computers after the job has finished	After a computer has been scanned or an auto-remediation job has been done, GFI LanGuard attempts to shut down the computer if the time is in the specified timeframe. **NOTE** If shut down options are defined in Auto-remediation options, the power saving options are ignored.



Screenshot 59: Scheduled scan auto–remediation options

10. From the auto–remediation dialog, select the required options and click **Next**. The table below describes the list of available options:

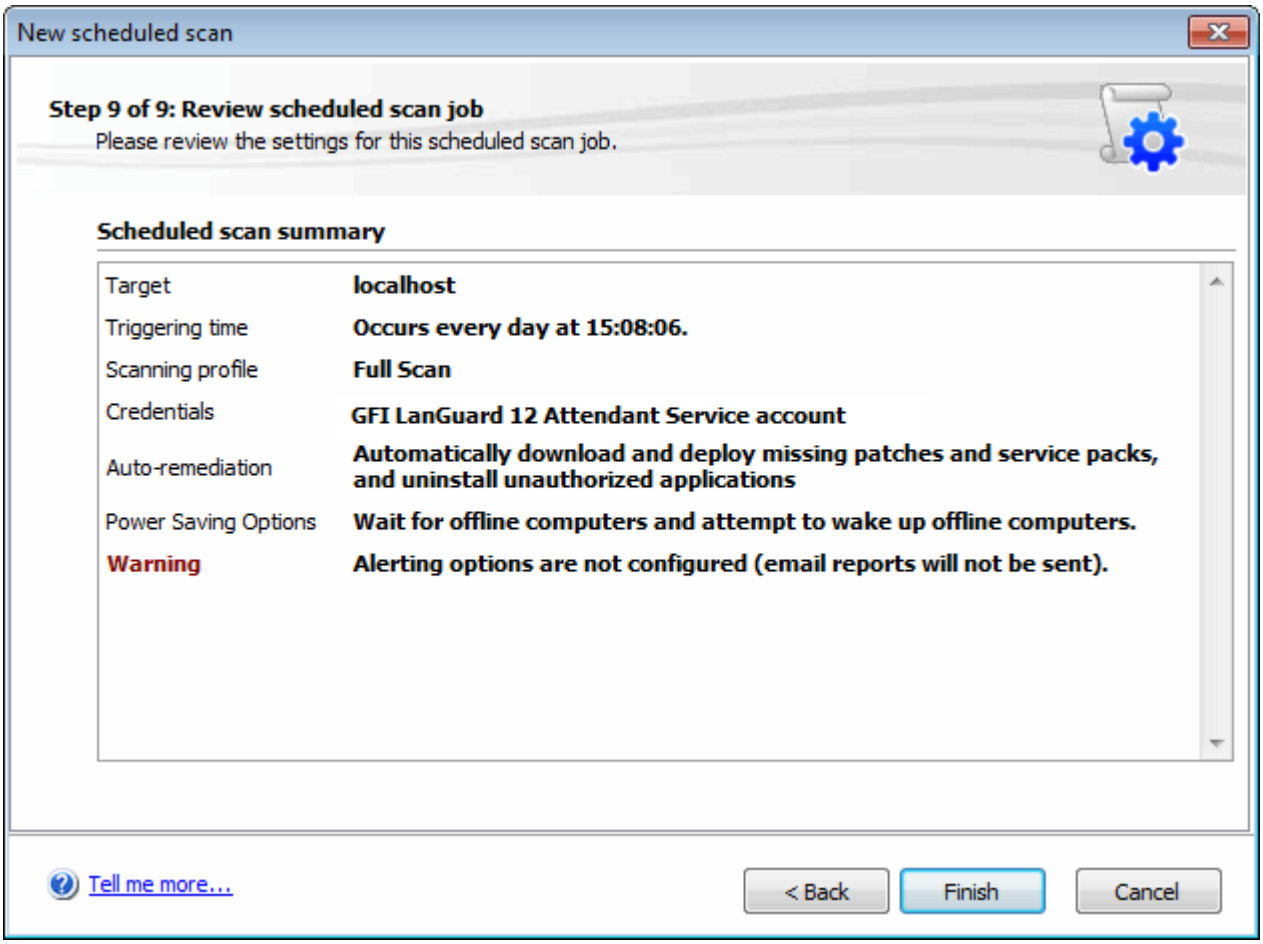
Option	Description
Download and deploy missing updates	Automatically download and deploy missing patches on target machines.
Download and deploy missing service packs and update rollups	Automatically download and deploy missing service packs on target machines.
Uninstall unauthorized applications	If this option is selected all applications validated as unauthorized, will be uninstalled from the scanned computer (unauthorized applications are defined in Application Inventory). For more information, refer to Configuring unauthorized applications auto-uninstall (page 169).
Configure auto–remediation	Automatic-Remediation enables you to automatically download and deploy missing patches as well as uninstall unauthorized applications during scheduled operations, automatically. For more information, refer to Automatic Remediation (page 162).
View applications which this scan will uninstall	Click the link to launch the applications which will be uninstalled dialog. This will list all the applications that will be uninstalled when the scheduled scan is finished.



Screenshot 60: Scheduled scan reporting options

11. (Optional) Configure **Reporting options** as described below:

Option	Description
Email the scan report	Send a report by email at the end of each scheduled scan.
Save the scan report to disk	Save a report to disk at the end of each scheduled scan
Comparison data and auto remediation details	Include details of auto remediation actions performed and result comparison with previous security scans. **NOTE** Comparison is done between scans with same scan target(s) and scanning profile.
Full scan results data	Include full scan result details.
Configure alerting options	(Optional) Click Configure alerting options… to specify sender/recipient details. For more information, refer to Configuring Alerting Options (page 235).
Override general alerting options, and send email to	(Optional) Send a report by email to specific email address. GFI LanGuard alerting options are overridden.



Screenshot 61: Scheduled scan reporting options

12. Review the scan settings summary and click **Finish**.

NOTE

By default, all new scheduled scans are disabled. To enable, select **Configuration** tab **>Scheduled Scans** and click on the button.

NOTE

Confirm that the new scheduled scans are successfully set by clicking on **Activity Monitor** tab **> Security Scans**.

Editing scheduled scan settings

Scan schedules can be reviewed, edited, or deleted from **Configuration** tab **> Scheduled Scans** node. All scans are listed in the review page together with the relevant information. Use the scheduled scan toolbar to perform the actions described below:

Icon	Description
	Add new scan Display the New scheduled scan wizard and create a new scheduled scan.
	Delete Use this button to delete the selected scheduled scan.

Icon	Description
	Properties Review and edit the properties of the selected scan.
	Enable/Disable Toggle the status of the selected scan between enabled and disabled. This enables you to activate/suspend a scanning schedule without deleting the scheduled scan.
	Scan now Trigger the selected scheduled scan. This button overrides the scheduled scan date/time settings and executes an immediate scan.

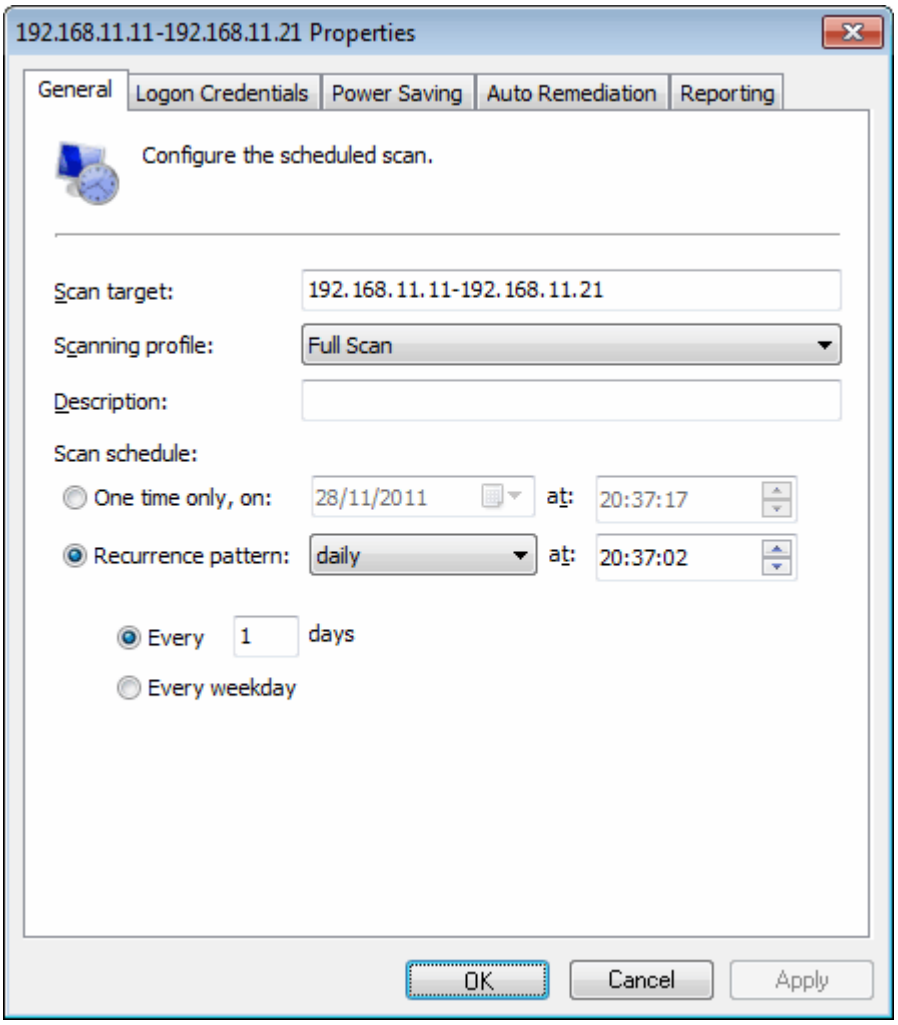
Configuring scheduled scan properties

The scheduled scan properties page enables you to configure all the parameters of the scheduled scans.

To use the scheduled scan properties tab:

1. Go to **Configuration** tab > **Scheduled Scans**.

2. Select the scheduled scan and click the **Scheduled Scan Properties**.



Screenshot 62: Scheduled Scan properties

Tab	Description
General	Make changes to scan target setting, type of scanning profile and scan frequency.

Tab	Description
Logon Credentials	Specify logon credentials used when scanning the specified target.
Power Saving	Configure power saving options. This dialog enables you to configure the scan to wait for offline machines to connect to the network, attempt to wake up offline machines and shut down machines when the scan is completed.
Auto–remediation	Configure the remediation options applicable to the scan being configured. This includes downloading and installing missing patches and service packs and unauthorized software un–installation.
Reporting	Configure reporting options used for the selected scheduled scan.

3. Click **OK**

4.2.6 Agent scheduled scans

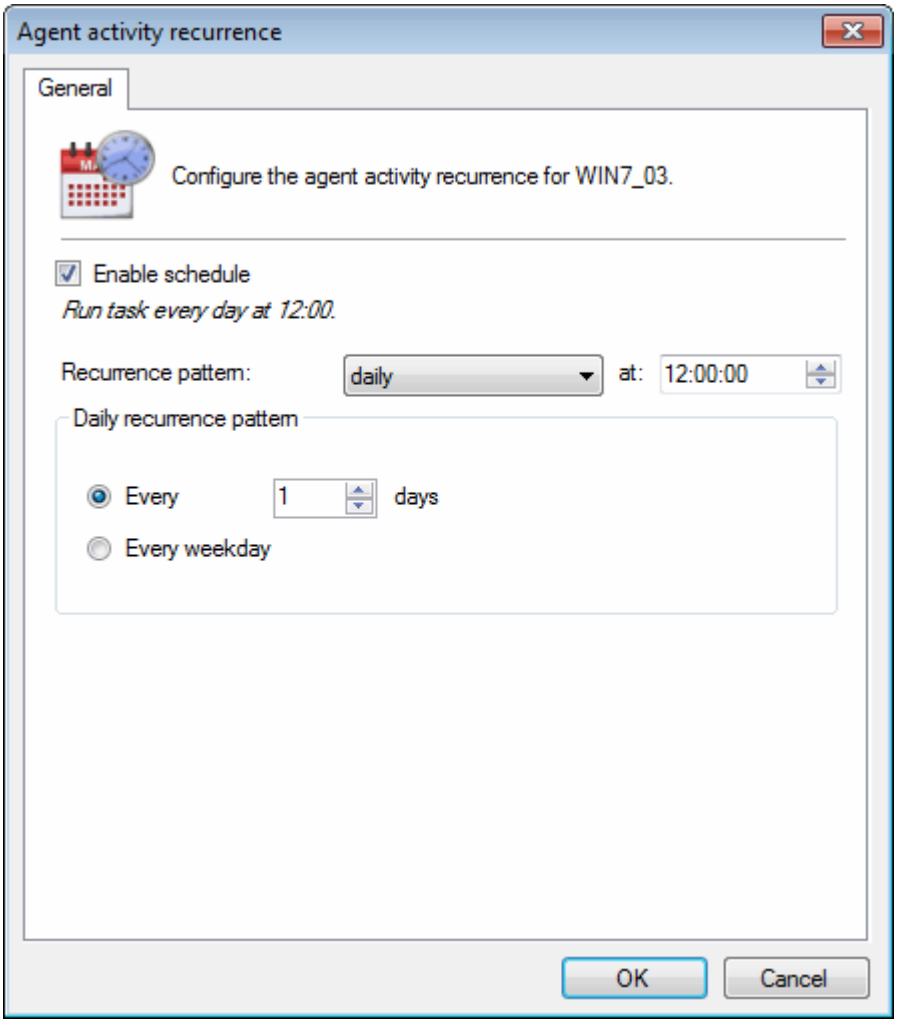
GFI LanGuard enables you to configure scheduled scans on computers running agents. Scheduling can be configured from the Agent properties dialog as follows:

1. Launch GFI LanGuard.

2. From the **Home** screen, select **View Dashboard**.

3. From the computer tree, right-click the computer/computer group you want to configure and select **Properties**.

4. Click **Agent Status tab > Change scan schedule...**.



Screenshot 63: Agent Activity Recurrence

5. Select **Enable Schedule** and configure the recurrence pattern.

6. Click **OK**

> **NOTE**
> Additional properties can be configured from the **Properties** dialog. For more information, refer to Agent properties (page 77).

4.2.7 Starting an Agent scan manually

To start an on demand scan on an agent computer:

1. Launch GFI LanGuard.

2. Click **View Dashboard** and select the computer(s) you want to start scanning.

3. From the **Agent Status** section, click **Scan Now**.

> **Note**
> **Scan Now** is only visible when the **Agent Status** is **Agent Installed**.

4.2.8 Discovering Mobile Devices

GFI LanGuard enables you to discover and manage mobile devices (such as phones or tablets) that connect to your mobile device management source.

This section contains information about:

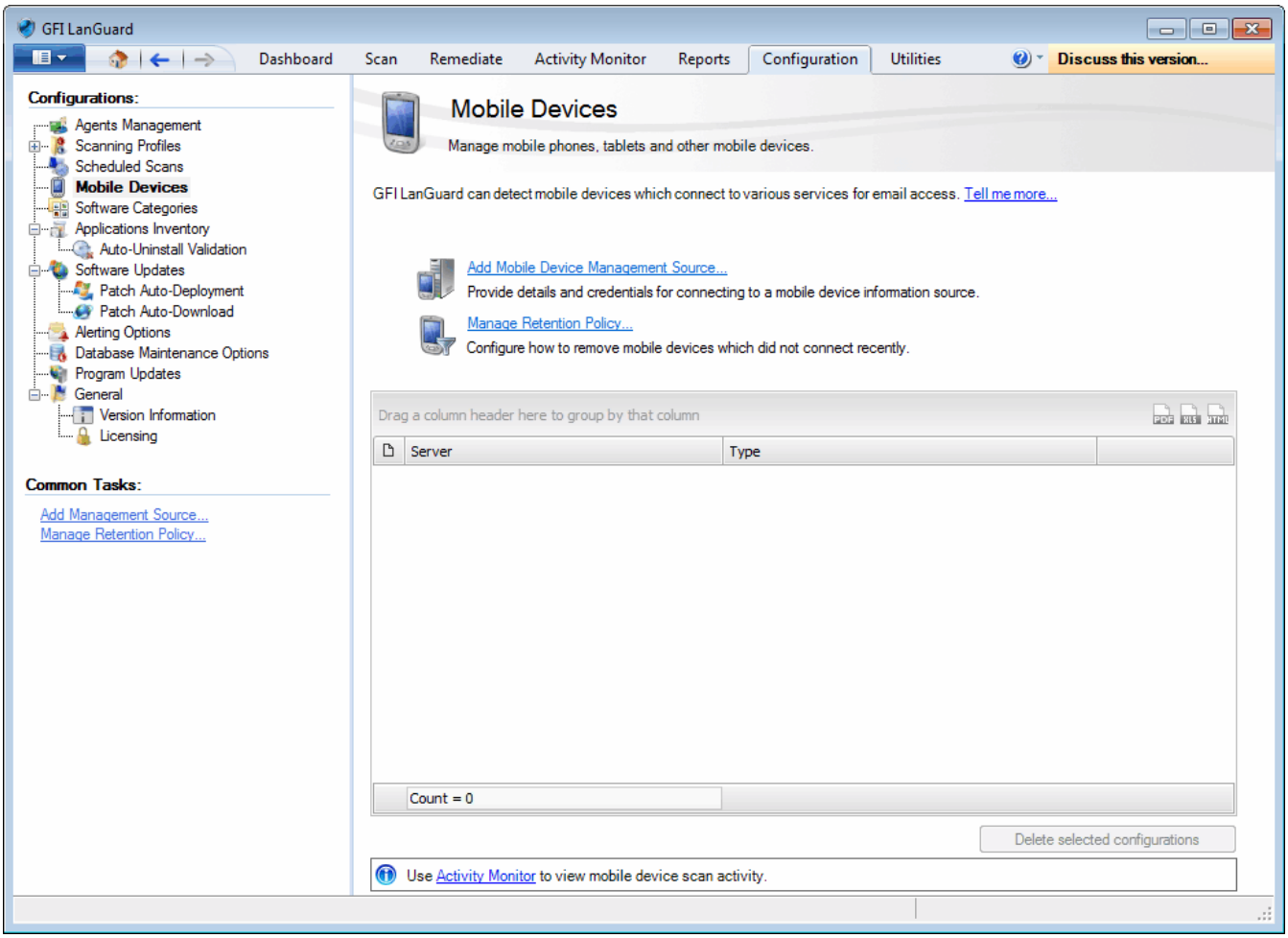
- Configuring a mobile device information source
- Adding mobile device management sources
  - Microsoft Exchange Server
  - Microsoft Office 365
  - Google Apps for Business
  - Apple Profile Manager
- Managing retention policies
- Unmanaged devices

Configuring a mobile device information source

To manually configure mobile devices:

1. Click on **Configuration** tab **> Mobile Devices**.

2. From the right pane, select one of the options.



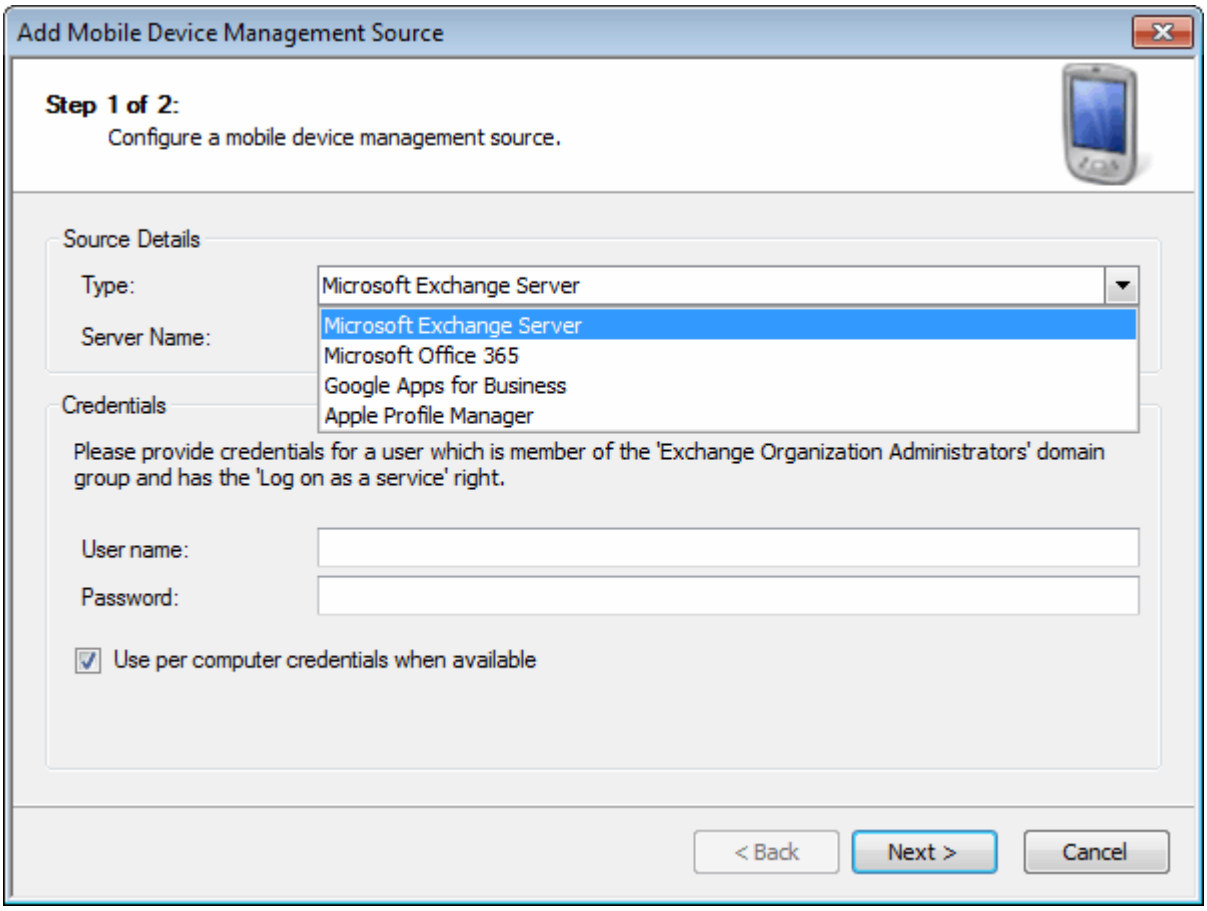
Screenshot 64: Mobile Devices

Adding mobile device management sources

To add a mobile device management source:

1. Click **Add mobile device management source**.

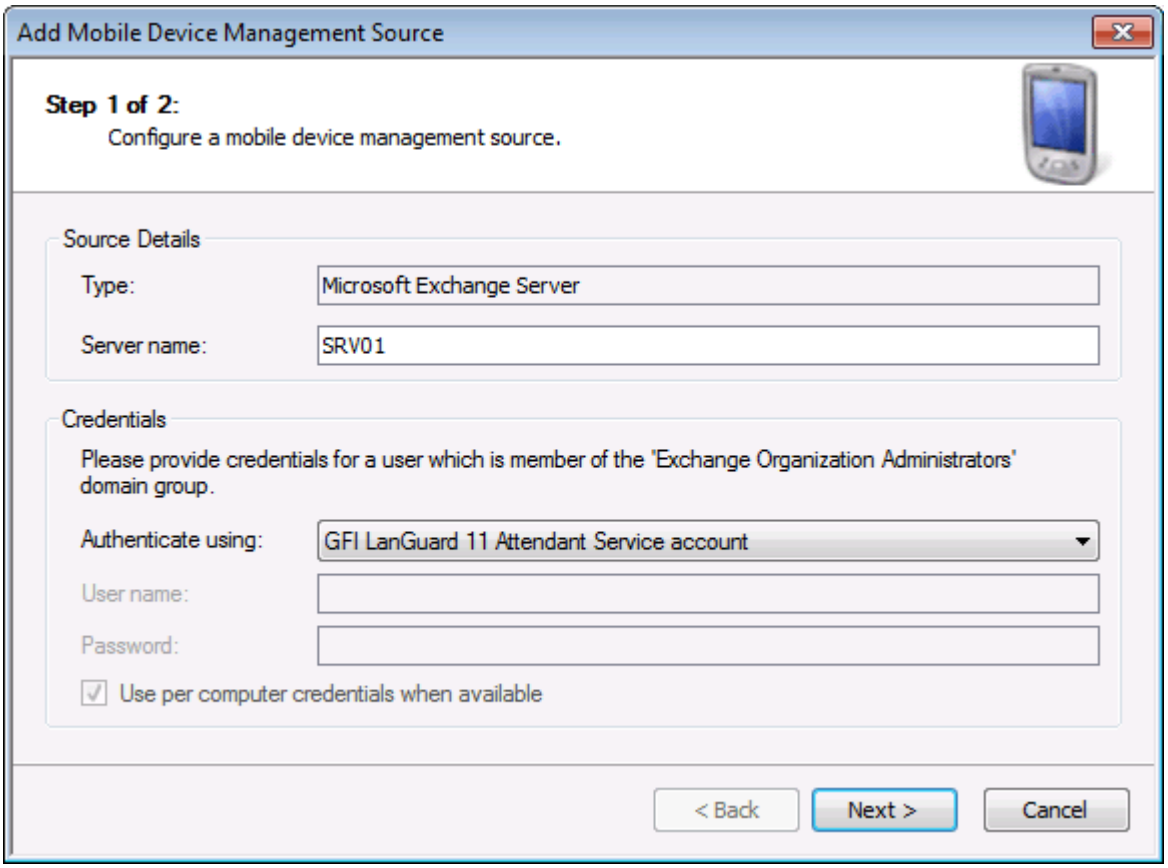
2. Select the type of Mobile Device Management Source.



Screenshot 65: Configuring a mobile device management source: Selecting type of source

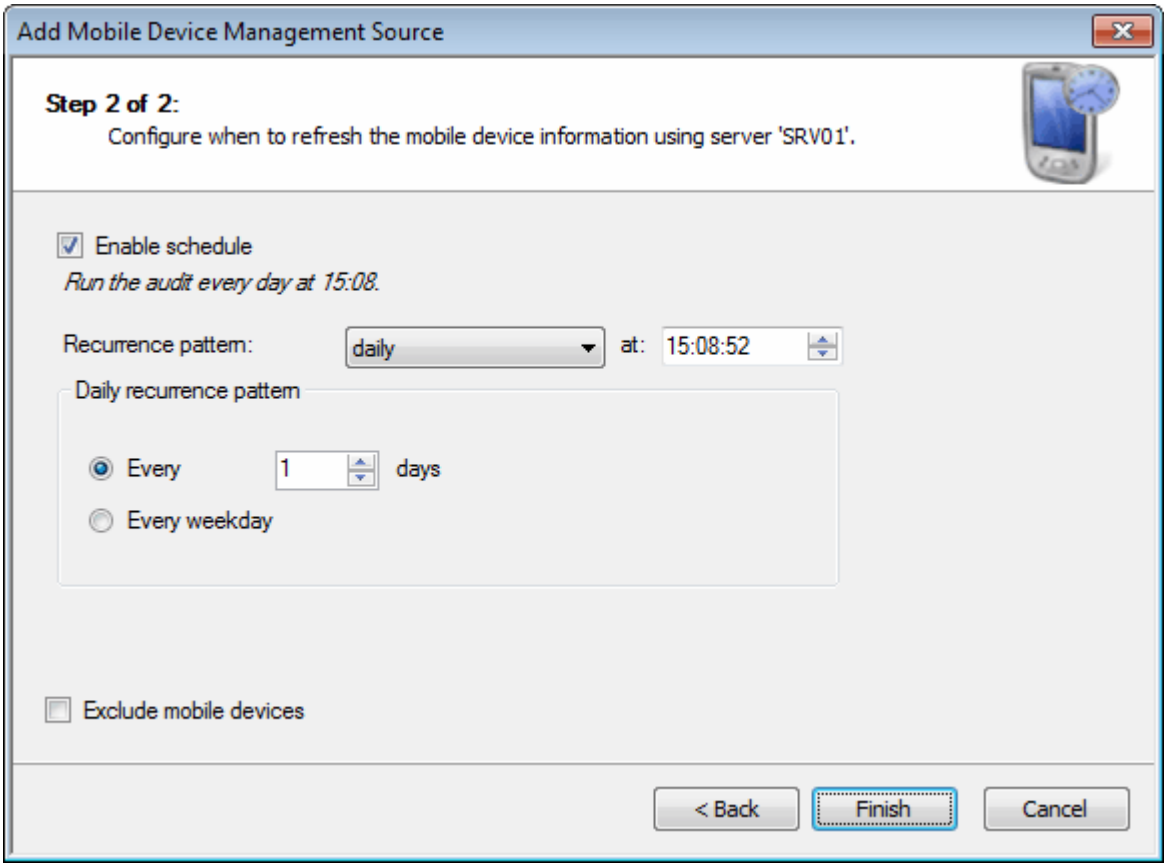
Source: Microsoft Exchange Server

1. Specify the credentials for Microsoft Exchange and click **Next**.



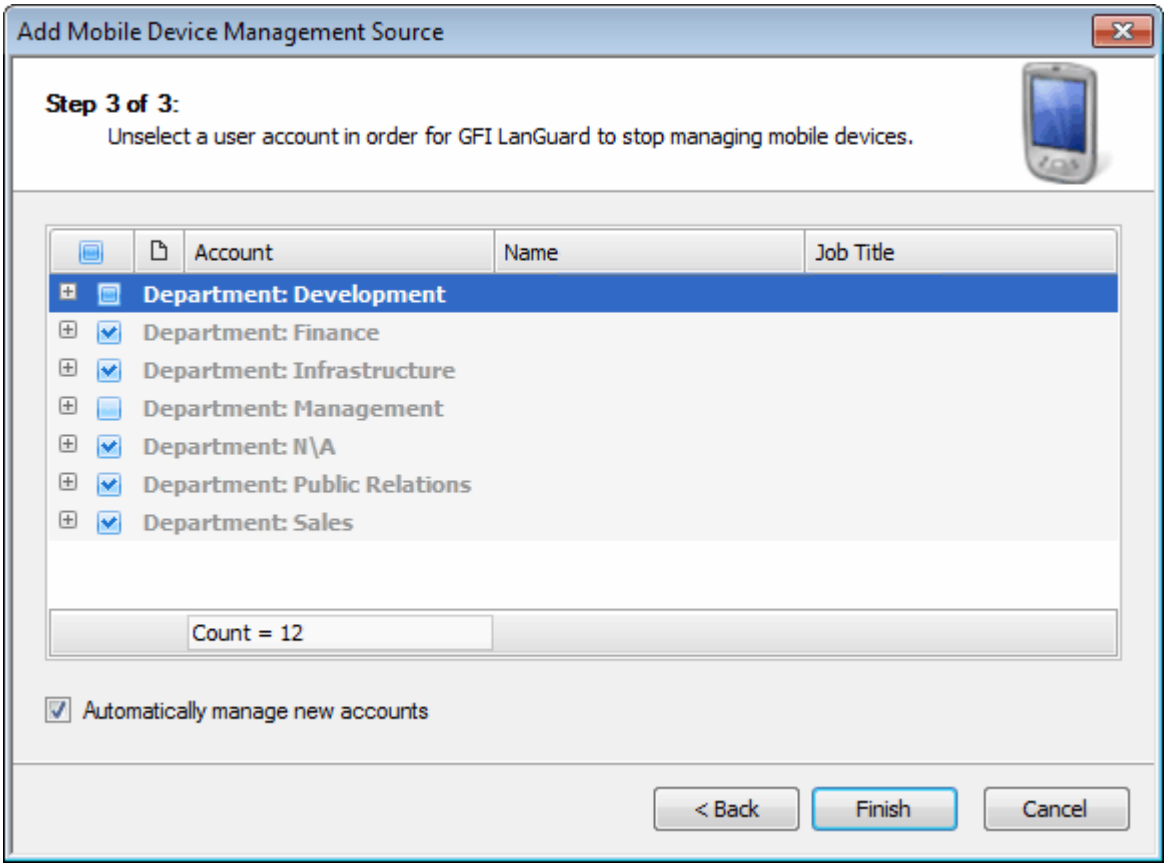
Screenshot 66: Configuring a mobile device management source: Source details

2. Configure when to refresh mobile device information and select (Optional) **Exclude mobile devices** and click **Next**.



Screenshot 67: Configuring a mobile device management source: Scheduling an audit

3. Select or unselect the accounts to manage and click **Finish**.



Screenshot 68: Configuring a mobile device management source: Managing devices

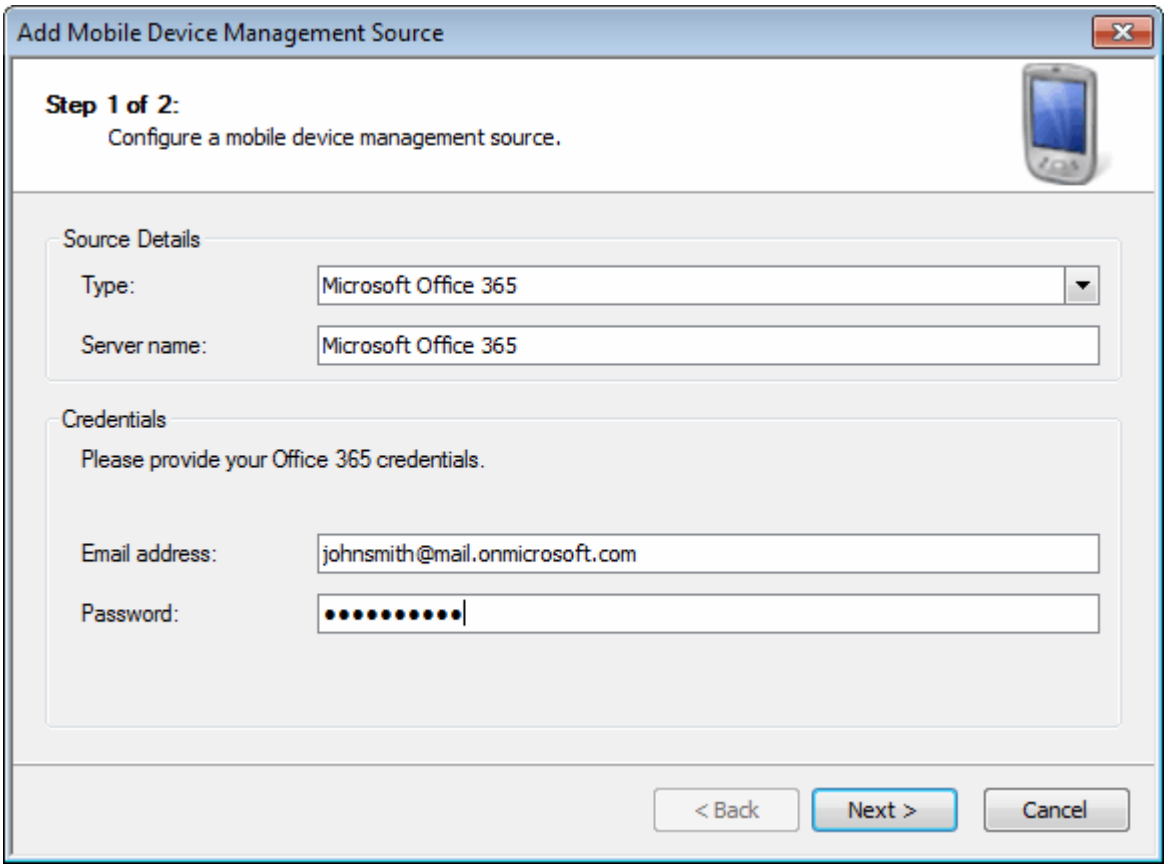
Source: Microsoft Office 365

1. Specify the credentials for Microsoft Office 365 and click **Next**.

NOTE

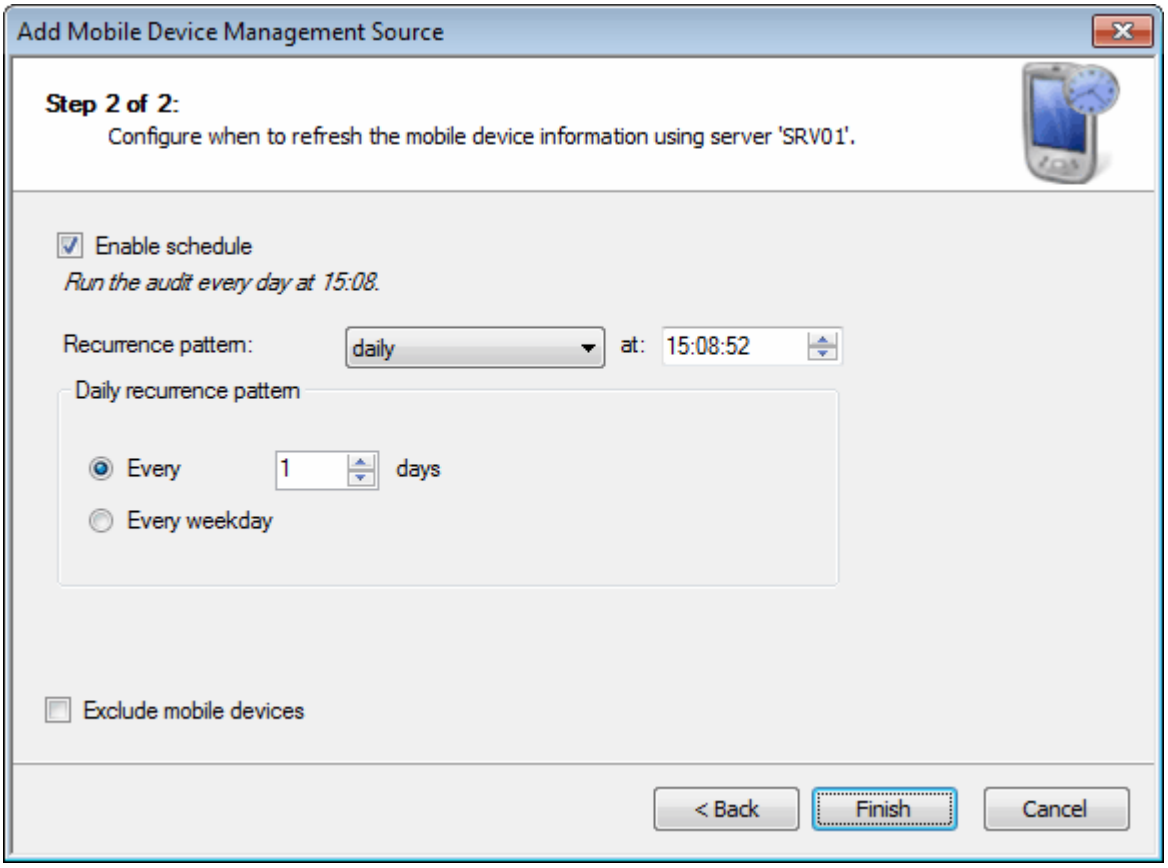
» The specified account needs to be a global administrator.

» Working with **Microsoft Office 365** requires .NET Framework 4.5. GFI LanGuard provides the facility to to install .NET 4.5 automatically whilst configuring a new mobile device management source with **Microsoft Office 365**.



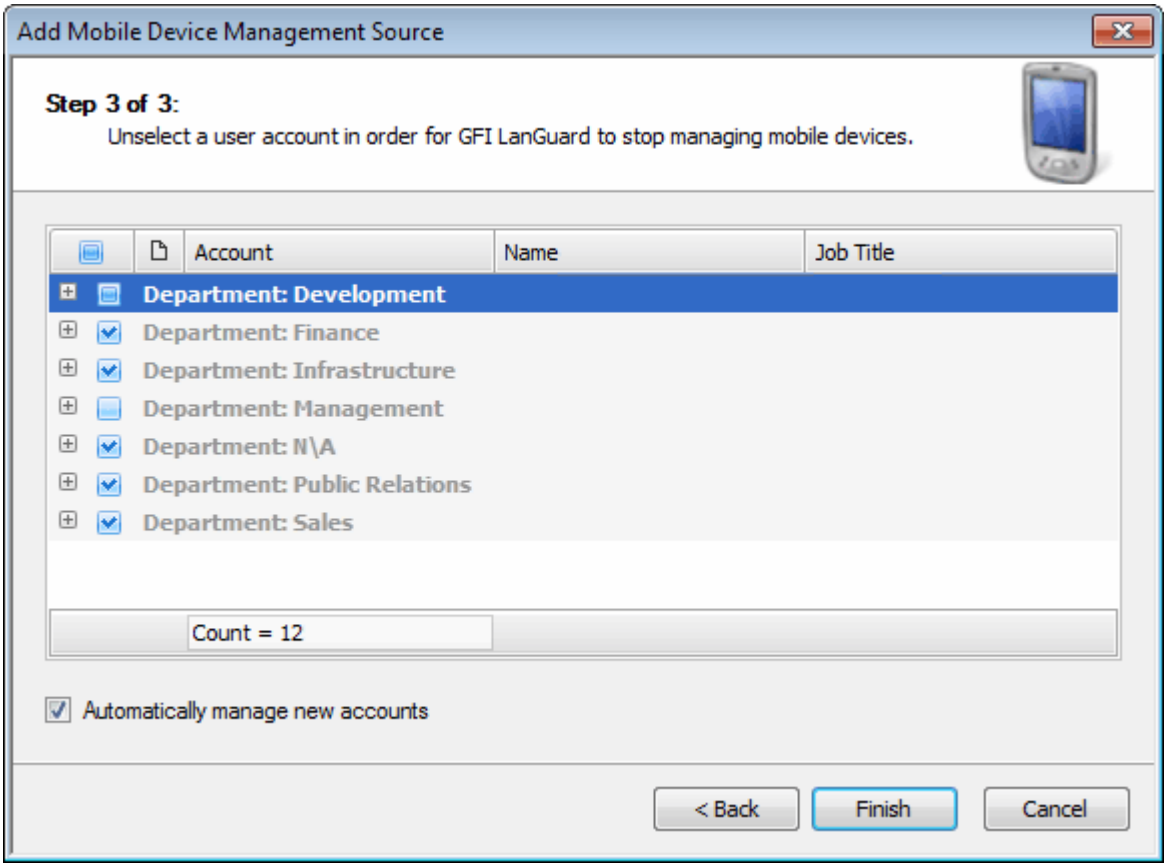
Screenshot 69: Configuring a mobile device management source: Source details

2. Configure when to refresh mobile device information and select (Optional) **Exclude mobile devices** and click **Next**.



Screenshot 70: Configuring a mobile device management source: Scheduling an audit

3. Select or unselect the accounts to manage and click **Finish**.



Screenshot 71: Configuring a mobile device management source: Managing devices

Source: Google Apps for Business

NOTES

» If you use Google Apps for Business , GFI LanGuard can retrieve the list of mobile devices that connect to your Google Apps domain.

» By default, your Google Apps domain is not configured to allow querying by other software such as GFI LanGuard. Below are the required step-by-step changes required for your Google Apps domain configuration to enable mobile device scanning with GFI LanGuard

To configure your Google Apps domain to enable mobile device scanning with GFI LanGuard:

1. Enable API access in your Google Apps Admin console. Log in to your admin account and select **Security**. If **Security** is not listed, select **More controls > Security** from the options shown in the gray box. Select **API reference**, and then select the checkbox to Enable API access. Click **Save** to save your changes.

2. Set up a new project in the Google APIs Console and activate the Admin SDK API for this project.

3. In the **Credentials** section of your project, enable **OAuth** authentication by selecting **Create New Client ID**. Choose the **Service Account** option and save the service account's Client ID, email address and the generated private key file.

4. Grant read-only access to user data to your Service Account:

    a. Open your Google Apps domain control panel, at https://www.google.com/a/cpanel/example.com

    b. Click **Security** icon. This can be found under **More controls**

c. Select **Advanced tools > Manage third party OAuth Client access**

d. In the Client name field enter the service account's **Client ID**

e. In the **One or More API Scopes** field, copy and paste the following list of scopes

- `https://www.googleapis.com/auth/admin.directory.device.mobile.readonly`
- `https://www.googleapis.com/auth/admin.directory.group.readonly`
- `https://www.googleapis.com/auth/admin.directory.user.readonly`

f. Click **Authorize**.

5. Optionally enable **Application auditing** so that GFI LanGuard can report the applications installed on mobile devices:

» Log in to your admin account and select **Device Management/Device management settings**.

» In the **Advanced settings** section. mark the **Enable application auditing** option.

» Click **Save** to save your changes.

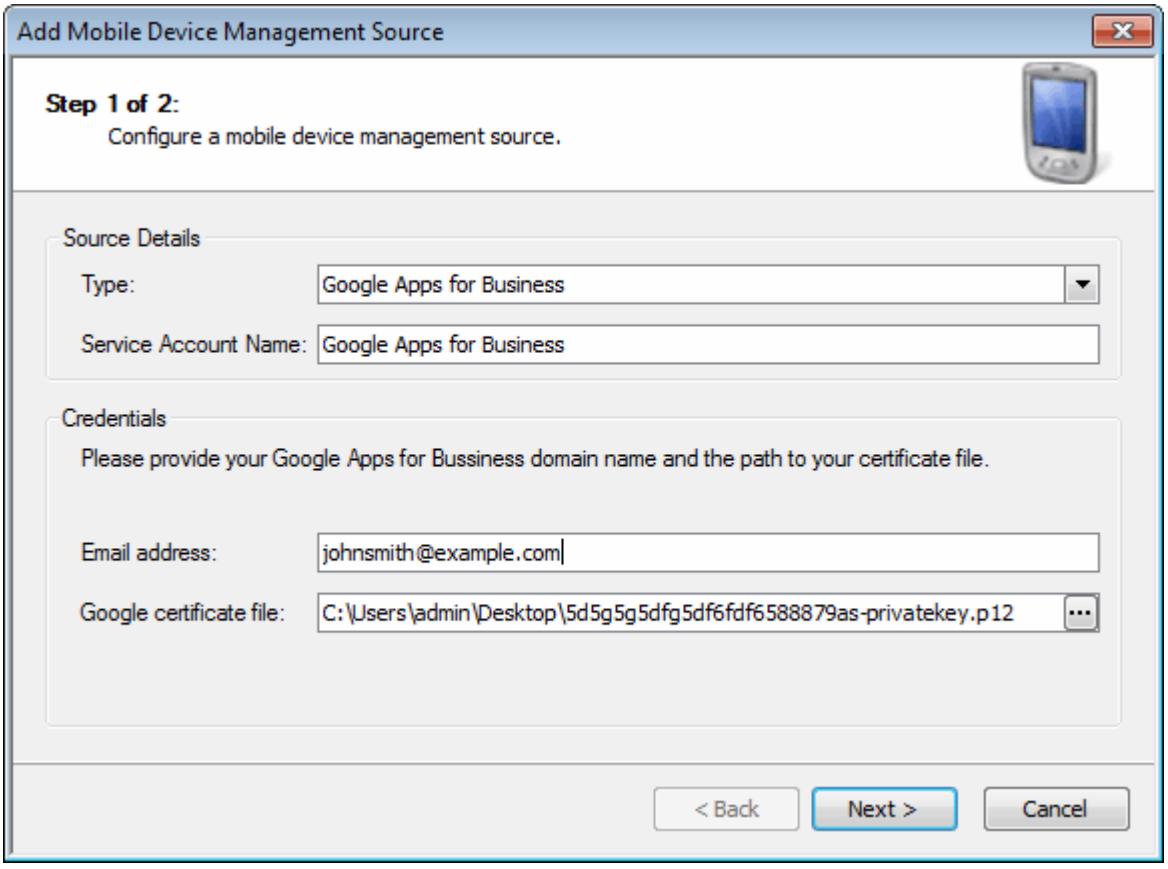
NOTE

For more information on how to set up Google Apps for API access see:

» http://go.gfi.com/?pageid=LAN_GoogleAppsPrerequisites

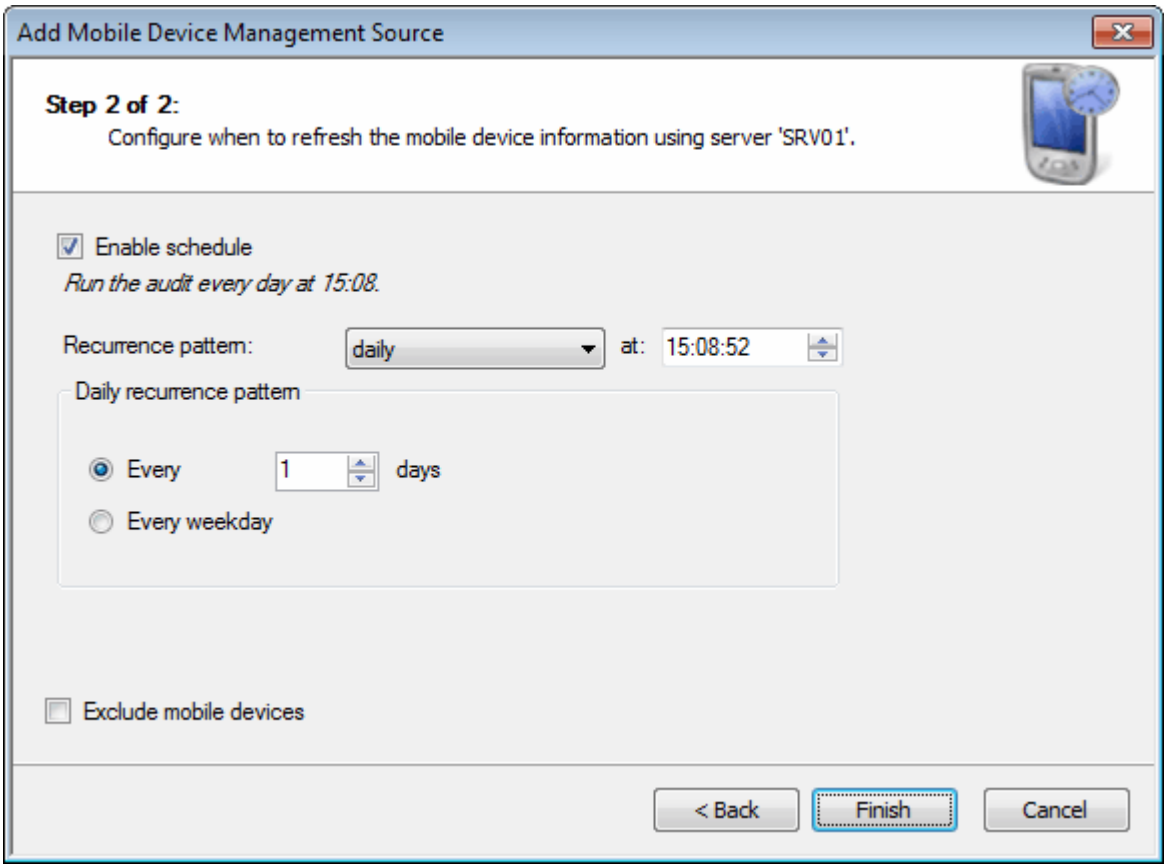
» http://go.gfi.com/?pageid=LAN_GoogleAppsGeneratingOAuth

6. Specify the credentials for Google Apps for Business and click **Next**.



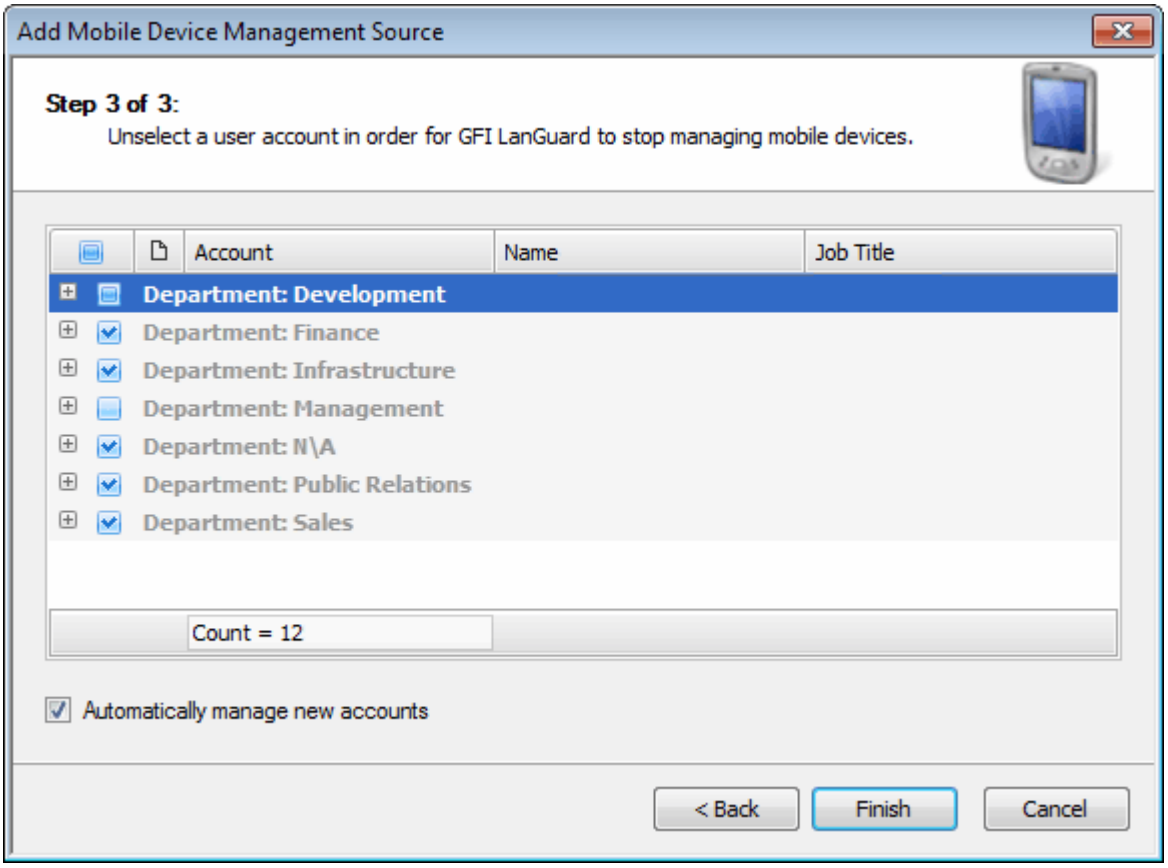
Screenshot 72: Configuring a mobile device management source: Source details

7. Configure when to refresh mobile device information and select (Optional) **Exclude mobile devices** and click **Next**.



Screenshot 73: Configuring a mobile device management source: Scheduling an audit

8. Select or unselect the accounts to manage and click **Finish**.



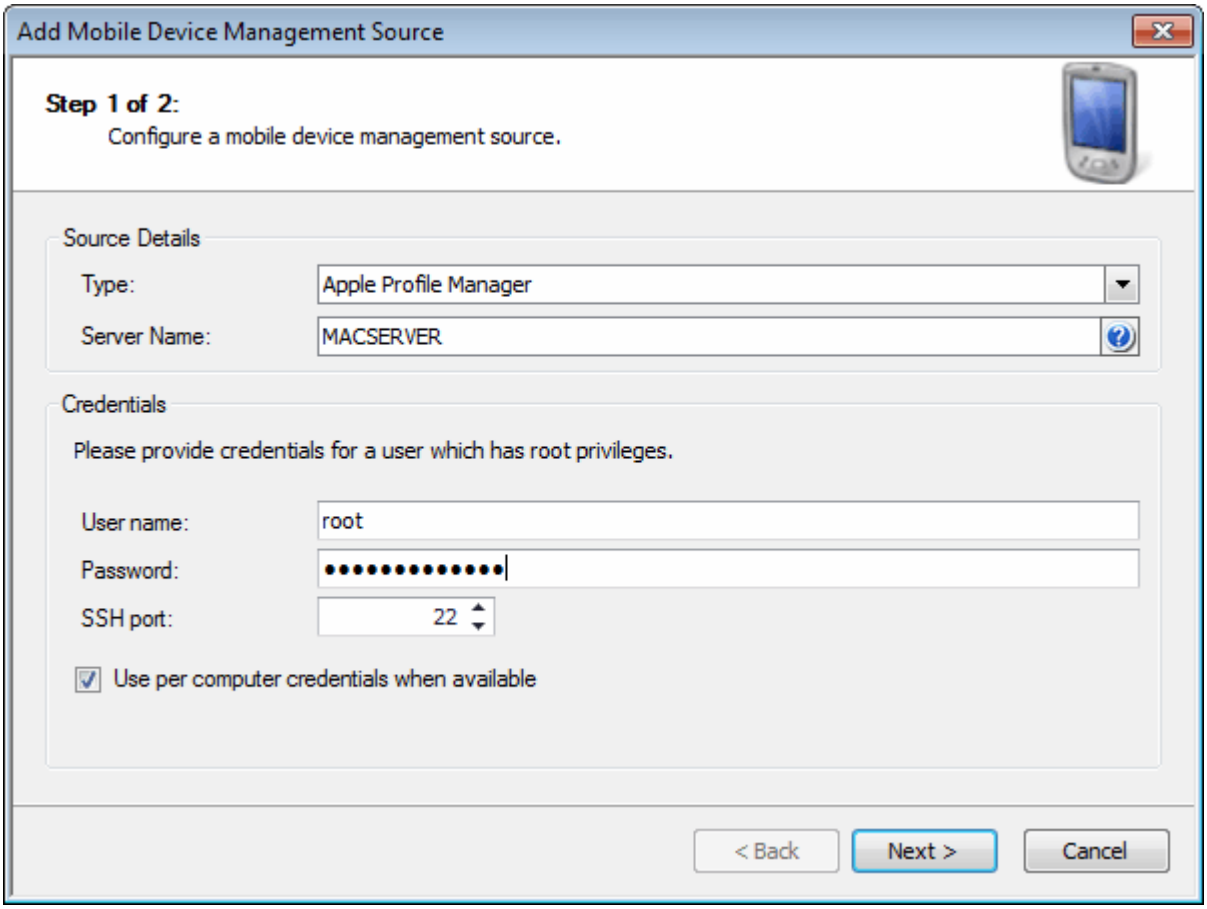
Screenshot 74: Configuring a mobile device management source: Managing devices

Source: Apple Profile Manager

NOTE

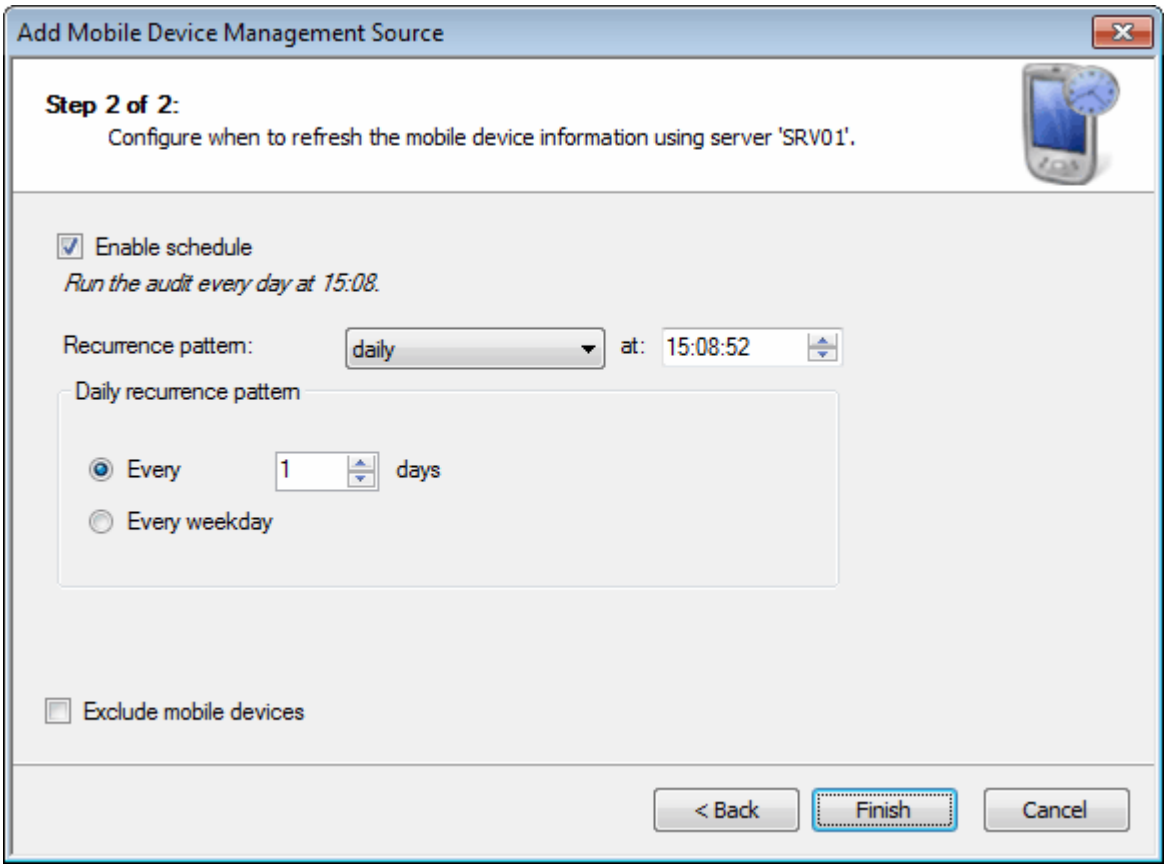
GFI LanGuard can query Apple Profile Manager for the list of managed mobile devices such as mobile phones or tablets running iOS. You need to provide root credentials to the OS X Server hosting Profile Manager.

1. Specify the credentials for Apple Profile Manager and click **Next**.



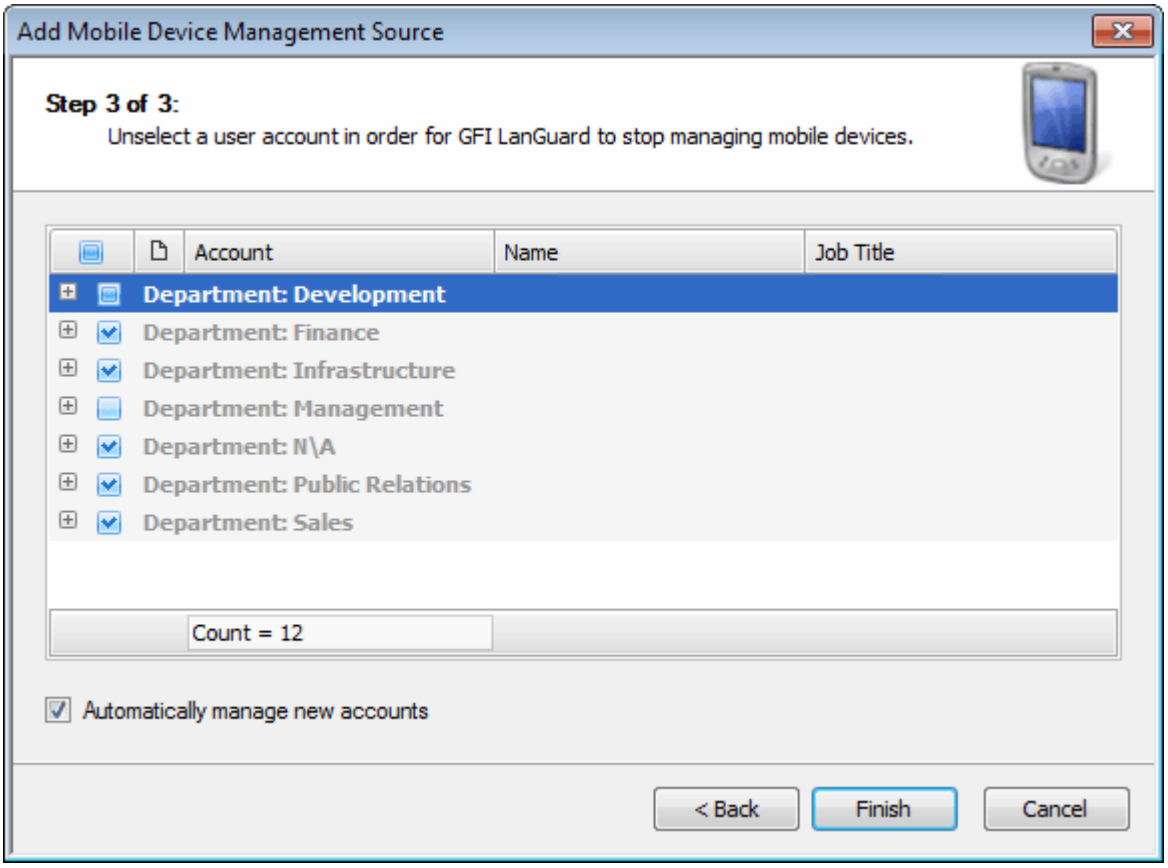
Screenshot 75: Configuring a mobile device management source: Source details

2. Configure when to refresh mobile device information and select (Optional) **Exclude mobile devices** and click **Next**.



Screenshot 76: Configuring a mobile device management source: Scheduling an audit

3. Select or unselect the accounts to manage and click **Finish**.



Screenshot 77: Configuring a mobile device management source: Managing devices

Managing retention policies

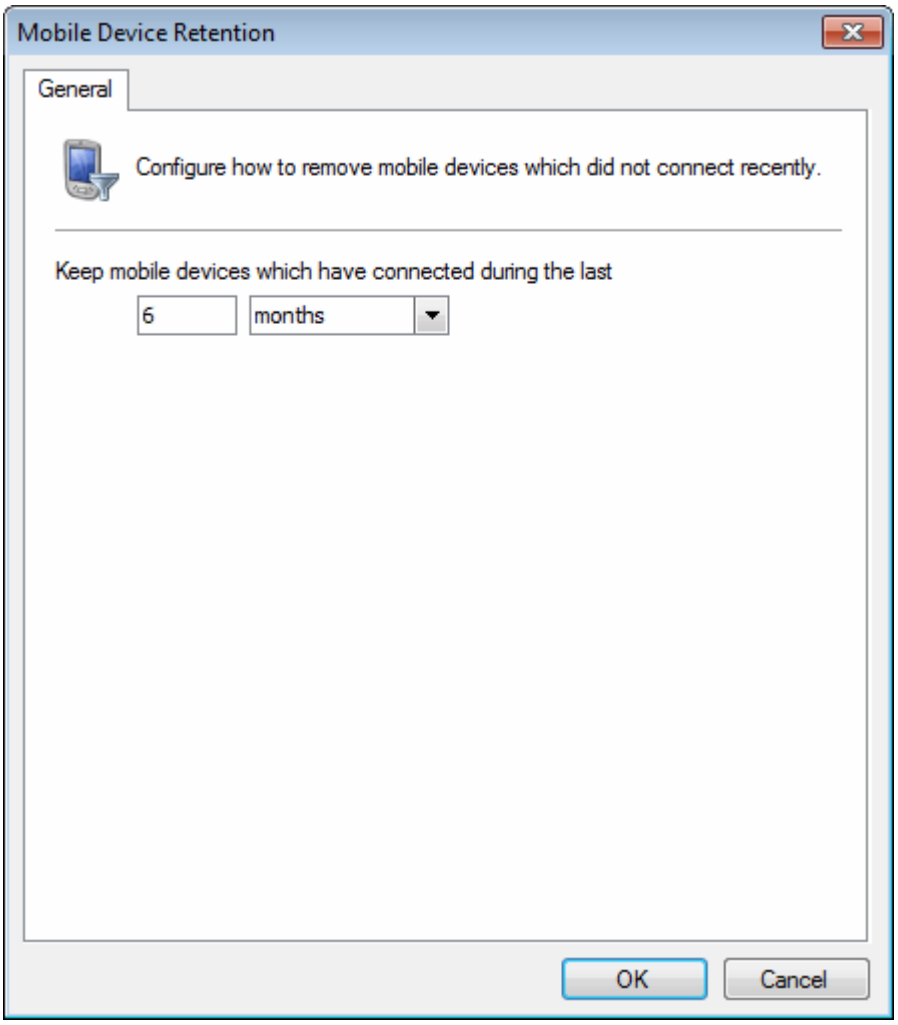
> **NOTE**
> Use **Managing retention policies** to clean up mobile devices that have not recently connected.

To manage retention policies:

1. Click on **Configuration** tab **> Mobile Devices**.

2. From the right pane, select **Manage retention policy**.

3. Specify the time frame to keep non-active devices.



Screenshot 78: Managing retention policies

Unmanaged devices

GFI LanGuard does not perform full audits of mobile devices unless a mobile device management source has been configured and user accounts are approved.

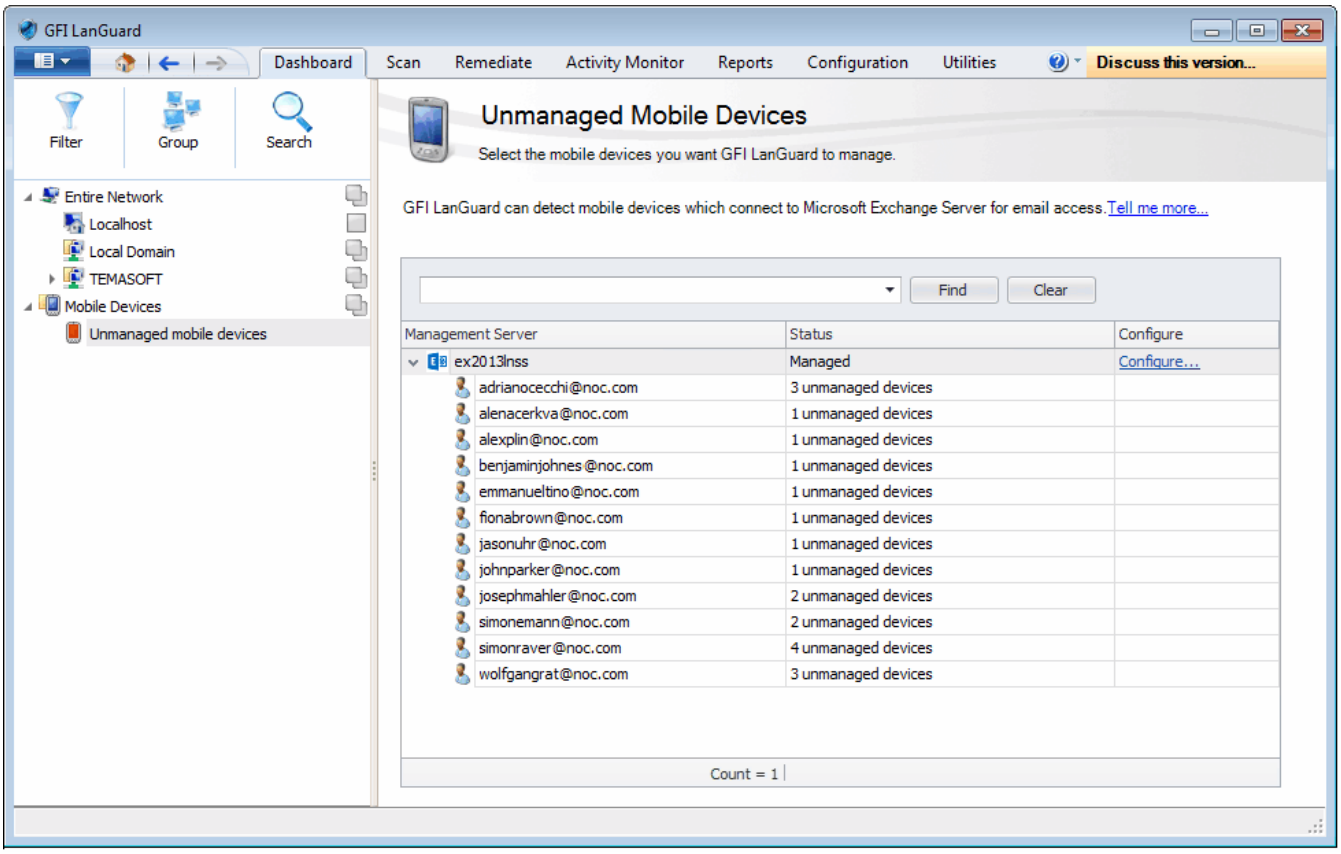
To view unmanaged mobile devices:

1. Click **Dashboard** tab and from the computer tree select **> Unmanaged mobile devices**.

(Optional)To change settings for unmanaged devices:

2. From the right pane, select a server containing unmanaged mobile devices and click **Configure**.

3. Select a user account to start managing the devices connected to the particular account.



Screenshot 79: Unmanaged mobile devices

4.3 Dashboard

The **Dashboard** section provides you with extensive security information based on data acquired during audits. Amongst others, the Dashboard enables you to determine the current network vulnerability level, the top–most vulnerable computers, and the number of computers in the database.

Topics in this section:

4.3.1 Achieving results from the dashboard

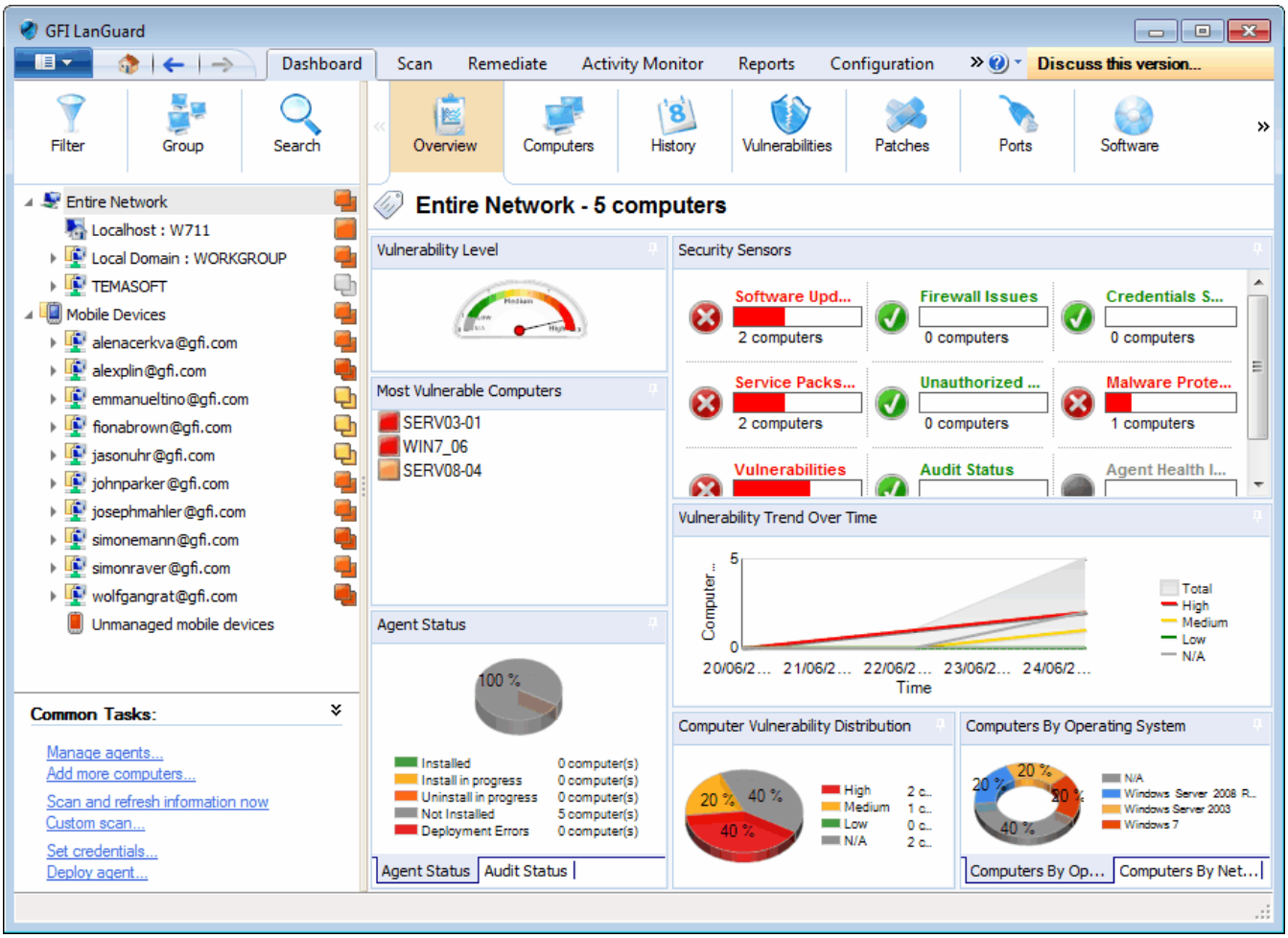
The dashboard is an important feature of GFI LanGuard. As the central point of the application, it enables you to perform all the common tasks supported by GFI LanGuard, including:

- Monitoring all computers managed by GFI LanGuard
- Managing scan targets. Add, edit or remove computers, domains and workgroups
- Deploying agents on scan targets and configure agent settings
- Configuring computer credentials
- Configuring auto–remediation options
- Configuring recurrent network discovery on the managed domains/workgroups/OUs
- Trigger security scans/refresh scan information
- Analyze computers security state and audit details
- Jump to relevant locations by clicking on security sensors and charts.

4.3.2 Using the Dashboard

This section provides the required information on how to use the GFI LanGuard Dashboard. To display the **Dashboard**:

1. Launch GFI LanGuard and click **Dashboard** tab.



Screenshot 80: View Dashboard

2. From the computers list, select a computer or mobile device. The dashboard information updates according to your selection.

4.3.3 Using the Computer Tree

GFI LanGuard includes filtering and grouping options that enable you to quickly find a computer or domain and immediately display results.

When a computer or group is selected from the computer tree, results in the dashboard are automatically updated. Press **CRTL** and select multiple computers to display results for specific computers.

The following are functions supported by the computer tree:

» Simple filtering

» Advanced filtering

» Grouping

» Searching

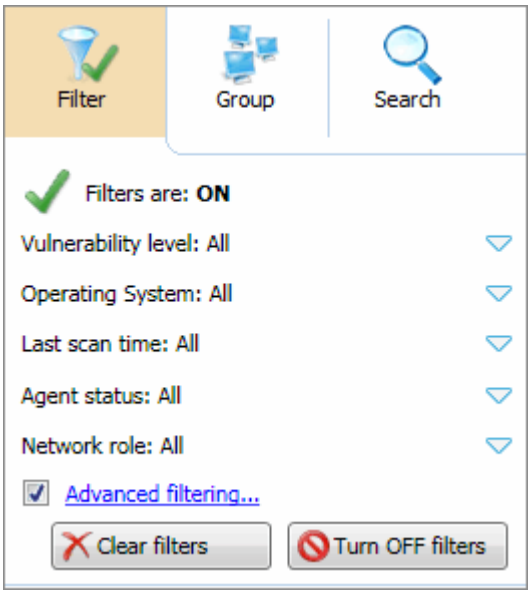
» Sync-up with Active Directory

Simple filtering

To filter for a specific computer or group:

1. From the left pane, click **Filter**.

2. Configure the criteria and click **Turn ON filters**.



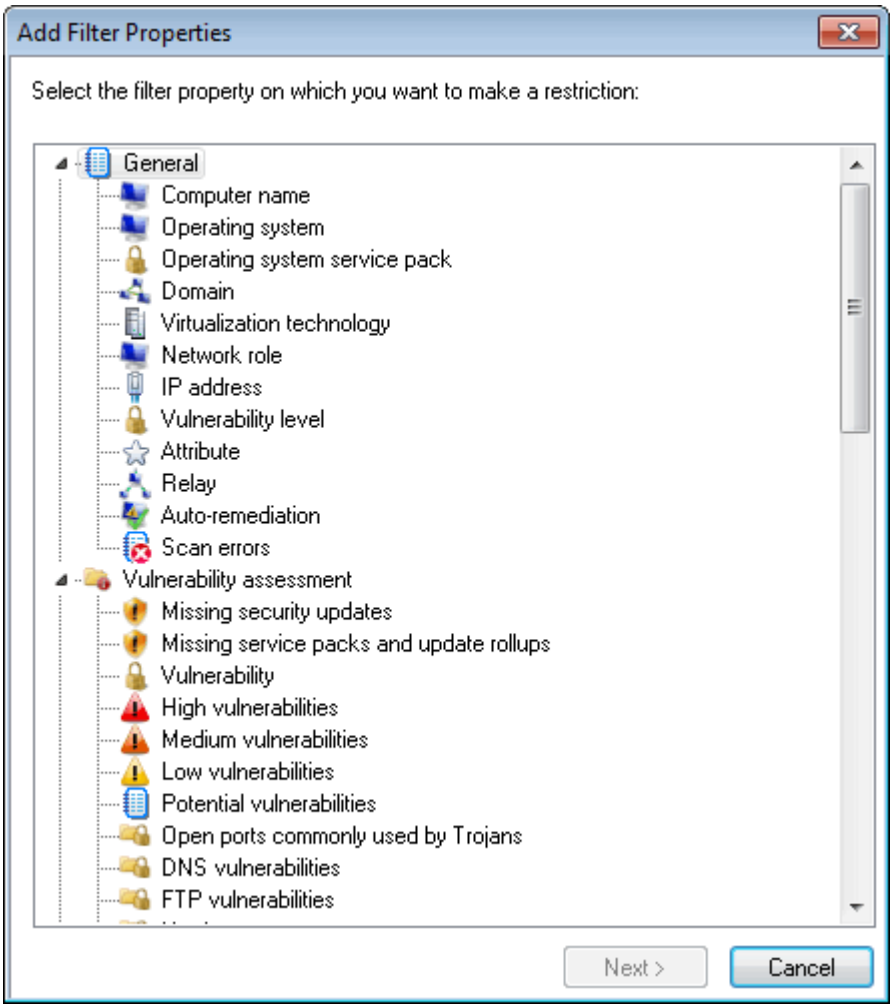
Screenshot 81: Simple filtering

Advanced filtering

To filter for a specific computer or group using advanced filtering:

1. From the left pane, click **Filter** and **Advanced filtering...**

2. From the **Advanced Filtering** dialog, click **Add**.



Screenshot 82: Add Filter Properties

3. Select the filter property to restrict and click **Next**.

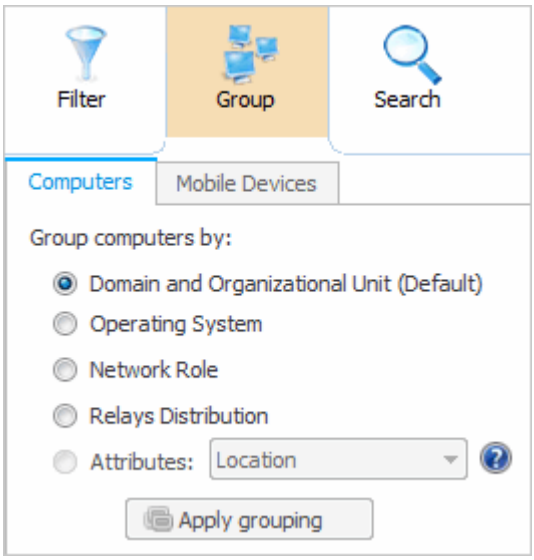
4. Select the condition and key in the condition value. Click **Add**.

5. Repeat steps 2 to 4 for each condition. Click **OK**

Grouping

To group machines by specific attributes:

1. From the left panel, click **Group**.



Screenshot 83: Grouping

2. Click on one of the following tabs and select a specific attribute:

Tabs	Attributes
Computers	» Domain and Organizational Unit » Operating System » Network Role » Relays Distribution » Attributes
Mobile Devices	» User Account » Operating System » Device Model » Attributes

NOTE

If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to Using Attributes (page 130).

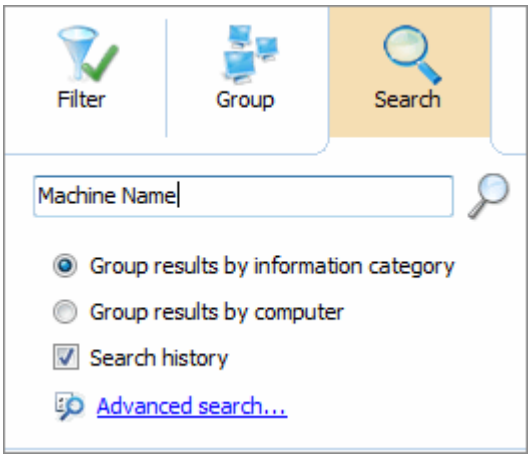
3. If Attributes is selected, select the attribute from the drop-down list.

4. Click **Apply grouping**.

Searching

The Search tab within the **Computers tree** enables you to search and display results for a specific computer or group. To display results for a specific computer:

1. From the **Computers tree**, select **Search**.



Screenshot 84: Search specific computers and groups

2. Key in the search criteria and use the following options:

Option	Description
Group results by information category	Search results are grouped by category. The result contains the latest computer information. Amongst others results are grouped by: » Computer Information » Hardware devices » Logged on Users » Processes » Virtual technology
Group results by computer	Search results are grouped by computer name. The result contains the latest computer information.
Search History	Search results include the information from previous scans.
Advanced search	Configure advanced search options. **NOTE** For more information, refer to Full text searching (page 223).

Sync-up with Active Directory

This feature enables you to perform the following tasks:

» Add computers that are in Active directory but not yet in GFI LanGuard

» Move computers to the correct Organizational Unit (OU) in the GFI LanGuard computer tree

» Remove computers that have been deleted from Active Directory but are still present in GFI LanGuard

1. Right-click the computer tree to synchronize and select **Synchronize with Active Directory**.

2. If displayed, key in the domain credentials require to retrieve the domain's Organizational Units and click **OK**

3. Click **Next** to start the synchronization process.

4. In the list of discovered computers, review the displayed list of changes that this process will do. This list shows where specific computers will be repositioned to which Active Directory Organizational Units. Click **Next**.

5. Review the list of computers that will be added to GFI LanGuard from Active Directory. Click **Next**.

6. Review the list of computers that are no longer present, or have been deleted from Active Directory. Click **Sync**.

7. On process completion, click **Finish**.

4.3.4 Using Attributes

Attributes enable you to group and configure single or multiple computers at one go. Attributes also enable you to remediate vulnerabilities or deploy software on specific computers based on the assigned attribute. The following sections contain information about:

» Assigning attributes to a computer

» Assigning attributes to a group

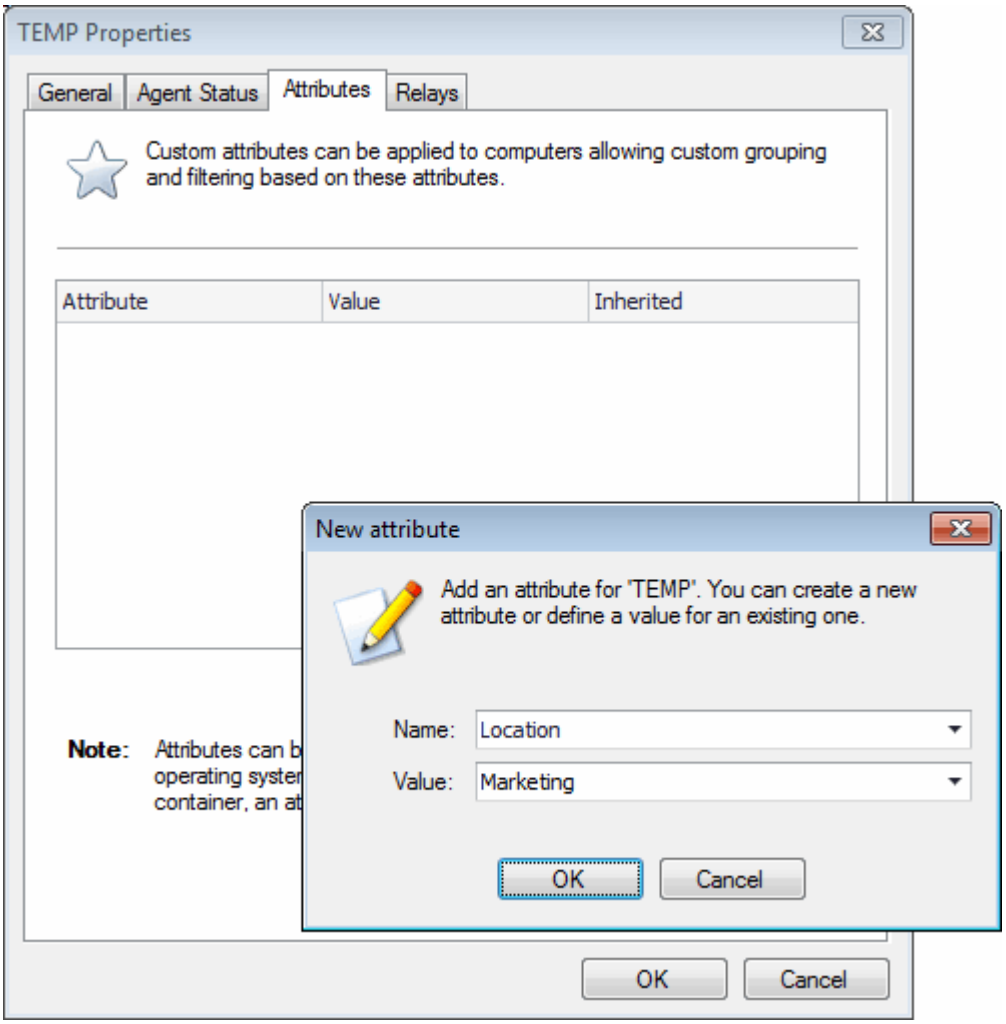
» Configuring attributes

Assigning attributes to a computer

To assign attributes to a single computer:

1. Click **Dashboard** tab.

2. From the computer tree, right-click a computer and select **Assign attributes**.



Screenshot 85: Assigning attributes: Single computer

3. From the **Properties** dialog **>Attributes** tab, click **Add**.

4. Configure new attributes settings and click **OK**

5. Click **OK** to save your settings.

Assigning attributes to a group

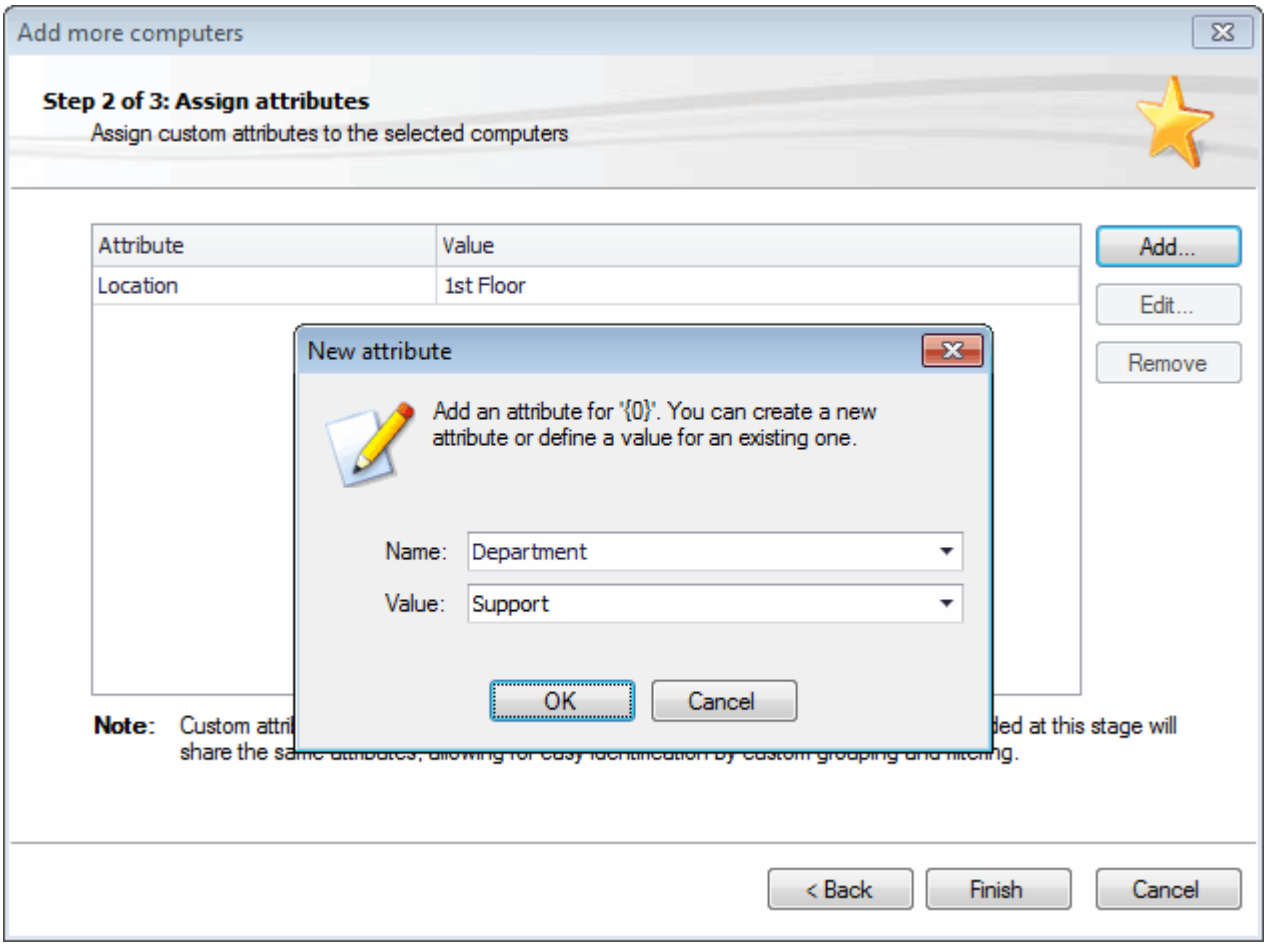
GFI LanGuard enables you to assign attributes to specific groups, domains, organizational units and networks. Once attributes are assigned, each member of the selected group inherits the attributes settings.

To assign attributes to a group:

1. Click **Dashboard** tab.

2. From the computers list, right-click network and select **Assign attributes**.

3. From the **Add more computers** wizard, select network and click **Next**.



Screenshot 86: Assigning attributes: Multiple computers

4. Click **Add** and configure the respective attributes. Use the **Edit** and **Remove** buttons to edit or remove the selected attributes.

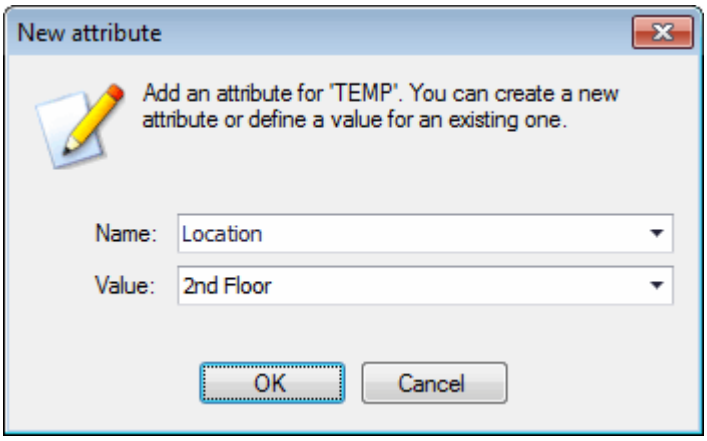
5. Click **Finish** to save your settings.

Configuring attributes

To configure attributes:

1. From the **Properties** dialog, click **Attributes** tab.

2. Click **Add** to launch the **New attribute** dialog.



Screenshot 87: New attribute dialog

3. From the **Name** drop-down menu, select an attribute or key-in a name to create a new one.

4. Specify a value for the attribute in the **Value** field. Click **OK**

5. Repeat steps 2 to 4 until you add all the required attributes.

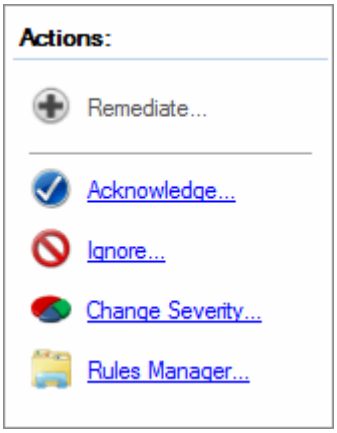
6. Click **OK** to save your settings.

4.3.5 Dashboard actions

The **Actions** section enables you to manage and remediate vulnerabilities and missing patches found in your network. To access the **Actions** section:

1. Select **Dashboard** tab.

2. Click **Vulnerabilities** or **Patches** tab.



Screenshot 88: Actions section in the Dashboard

3. Select one of the following actions:

Action	Description
Remediate	Launch the Remediation Center to deploy and manage missing patches. **NOTE** For more information, refer to Manual Remediation (page 185).
Acknowledge	Launch the Rule-Acknowledge Patch dialog. This enables you to acknowledge issues so that they will not affect the Vulnerability level of your network. Configure for which machine this rule applies.

Action	Description
Ignore	Launch the Rule-Ignore Patch dialog. This enables you to ignore missing patches or vulnerabilities so that they will not be reported as issues in the future, and include reasons why to ignore such vulnerabilities. Configure for which machine this rule applies and the time span that the issue is ignored.
Change Severity	Launch the Rule-Change Severity dialog. This enables you to change the severity level of vulnerability. Configure for which machines this rule applies and the severity level.
Rules Manager	Launch the Rules Manager dialog. This enables you to search and remove configured rules and view the reasons to ignore missing patches and vulnerabilities.

4.3.6 Exporting issue list

GFI LanGuard enables you to export issue lists to Portable Document Format (PDF), Microsoft Office Excel (XLS) or Hyper Text Markup Language (HTML). When a list supports exporting, these icons  are displayed in the top-right corner of the list. Select the respective icon and configure the export settings.

4.3.7 Dashboard views

The GFI LanGuard dashboard is made up of multiple views. These different views enable real-time monitoring of your scan targets and allow you to perform instant remedial and reporting operations. The following sections contain information about:

- Dashboard overview
- Computers view
- History view
- Vulnerabilities view
- Patches view
- Ports view
- Software view
- Hardware view
- System Information view

Overview

Screenshot 89: Dashboard Overview

The **Dashboard Overview** is a graphical representation of the security level/vulnerability level of a single computer, domain or entire network.

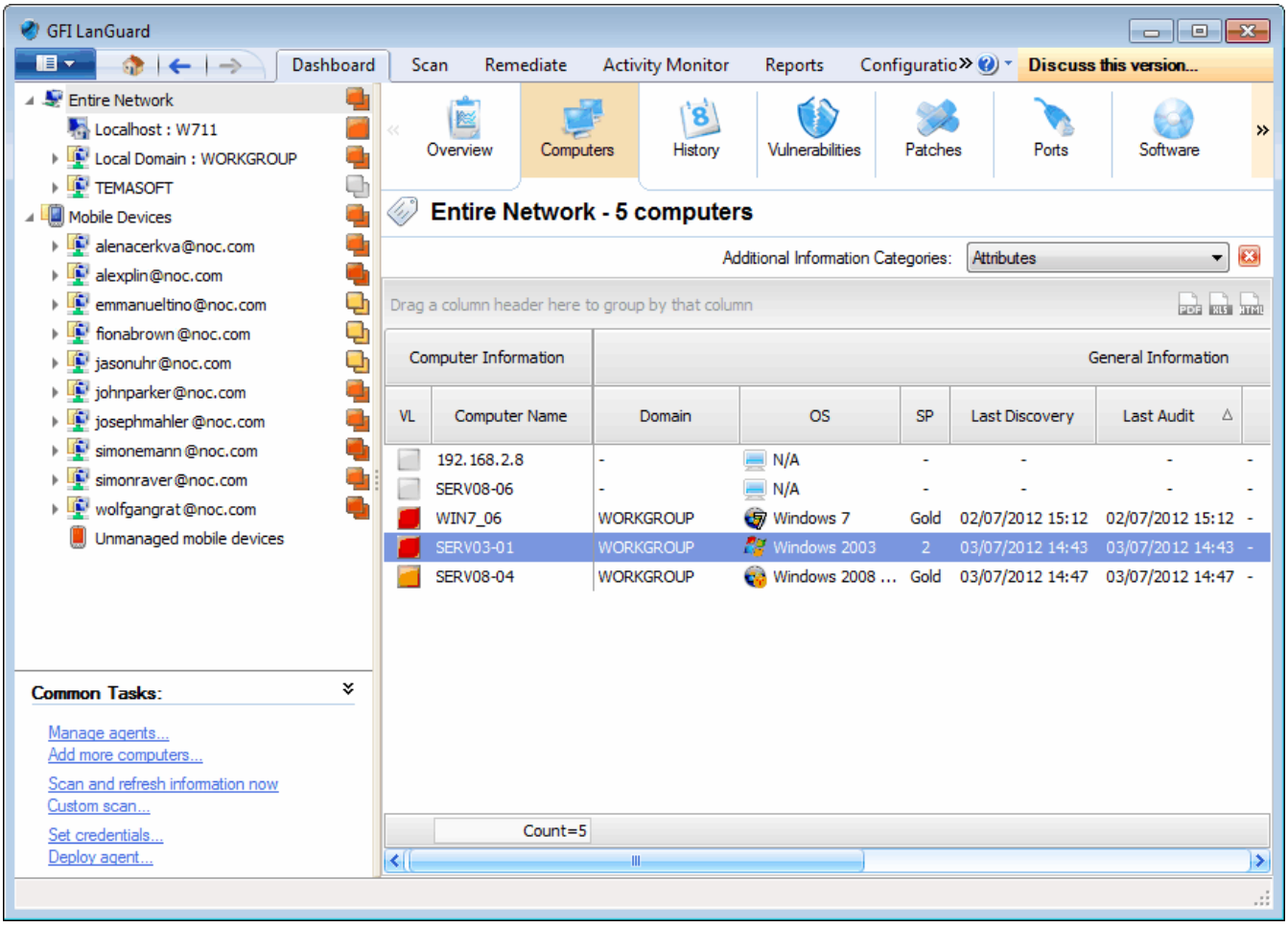
When a computer or domain is selected, the results related to the selected computer/domain are automatically updated in the dashboard. Below is a description of each section found in the dashboard:

Section	Description
Network security level	This rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found. A high vulnerability level is a result of vulnerabilities and/or missing patches which average severity is categorized as high.
Computer vulnerability distribution	This chart is available only when selecting a domain or a workgroup, and displays the distribution of vulnerabilities on your network. This chart enables you to determine how many computers have high, medium and low vulnerability rating.
Most vulnerable computers	This list is available only when selecting a domain or a workgroup, and shows the most vulnerable computers discovered during the scan. The icon color on the left indicates the vulnerability level.

Section	Description
Agent Status	When selecting a domain or workgroup, a chart showing the overall agent status of all computers within the domain/workgroup is displayed. This enables you to determine the number of agents installed or pending installation on the selected domain/workgroup. When selecting a single computer, this section displays an icon representing the agent status. The icons are described below: »  **Not installed** - Agent is not installed on the target machine. »  **Pending installation** - Installation is pending. A status can be pending when the machine is offline or the agent is being installed. »  **Pending uninstall** - Uninstallation is pending. A status can be pending when the machine is offline or the agent is being uninstalled. »  **Installed** - Agent is installed on the target machine. »  **Relay Agent Installed** - The selected computers are relay agents.
Audit status	This chart is available only when selecting a domain or workgroup and enables you to identify how many audits have been performed on your network grouped by time.
Vulnerability trends over time	When a domain or workgroup is selected, this section displays a line graph showing the change of vulnerability level over time grouped by computer count. When a single computer is selected, this section displays a graph showing the change of vulnerability level over time for the selected computer.
Computers by network role	This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by network role. Amongst other roles, this graph identifies the number of servers and workstations per selected domain.
Computers by operating system	This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by the installed operating system.
Computer details	This section is available when selecting a single computer and enables you to view the selected computer details.
Scan activity	This line graph is available only when selecting a single computer and enables you to view the number of scans/audits performed on the selected computer. In addition enables you to verify if scheduled scans are being performed.
Remediation Activity	This line graph is available only when selecting a single computer and enables you to view the number of remediation activities performed on the selected computer. In addition, this graph enables you to verify that auto–remediation is performed.
Top 5 Issues to Address	This section is available only when selecting a single computer, and displays the top five issues to address for the selected computer.
Results statistics	This section is available only when selecting a single computer and displays an overview of the audit result. Amongst others, the result enables you to identify the number of missing patches, number of installed applications, open ports and running services.

Section	Description
Security Sensors	This section enables you to identify issues at a glance. Click a sensor to navigate and display issues and vulnerabilities for a specific computer or group. Sensors enable you to identify: » Missing Software Updates » Missing service packs » Vulnerabilities » Firewall Issues » Unauthorized Applications » Audit Status » Credentials setup » Malware Protection Issues » Agent Health Issues.

Computers view



Screenshot 90: Analyze results by computer

Select this view to group audit results by computer. From the drop-down list, select one of the options described below:

Option	Description
Agent Details	Select this option to view the agent status. This option enables you to identify if an agent is installed on a computer and if yes, displays the type of credentials being used by the agent.
Vulnerabilities	View the number of vulnerabilities found on a computer grouped by severity. Severity of a vulnerability can be: » High » Medium » Low » Potential.
Patching status	View the number of: » Missing Security/non-Security Updates » Missing Service Packs and Update Rollups » Installed Security/non-Security Updates » Installed Service Packs and Updates Rollups.
Open ports	View the number of: » Open TCP ports » Open UDP ports » Backdoors.

Option	Description
Software	View the number of: » Antiphishing engines » Antispyware engines » Antivirus engines » Backup applications » Data loss prevention applications » Device access and desk encryption applications » Firewalls » Installed applications » Instant messengers » Peer to peer applications » Unauthorized applications » Virtual machines » VPN clients » Web browsers.
Hardware	View information on: » Number of disk drives » Free disk space » Memory size » Number of processors » Other hardware.
System information	View information on: » The number of shared folders » Number of groups » Number of users » Logged users » Audit policy status.
Attributes	Adds an **Attributes** column and groups your scan targets by the assigned attribute.

NOTE

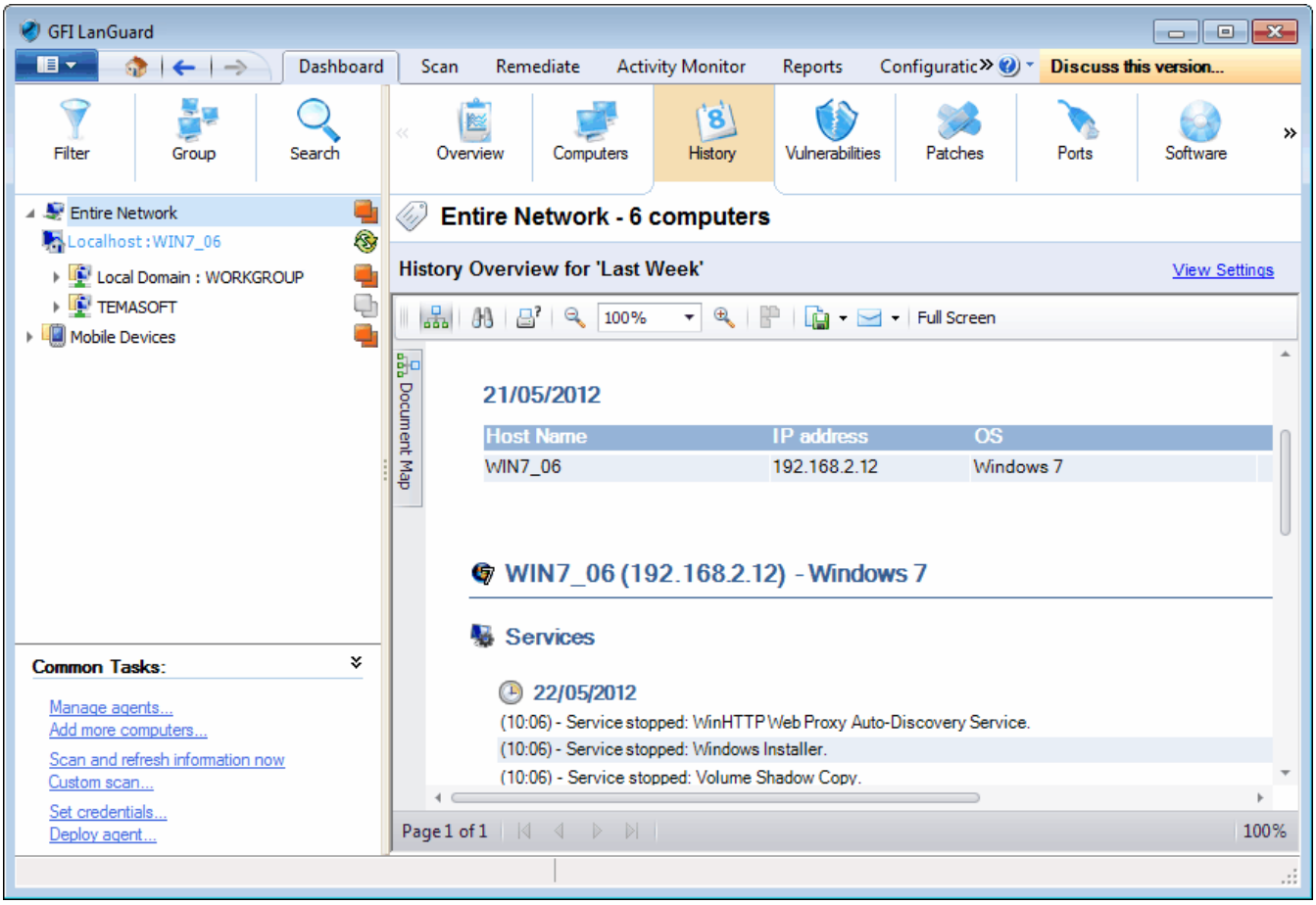
To launch the **Overview** tab and display more details on a specific computer, double click a computer from the list.

NOTE

Drag and drop a column header in the designated area to group data by criteria.

History view

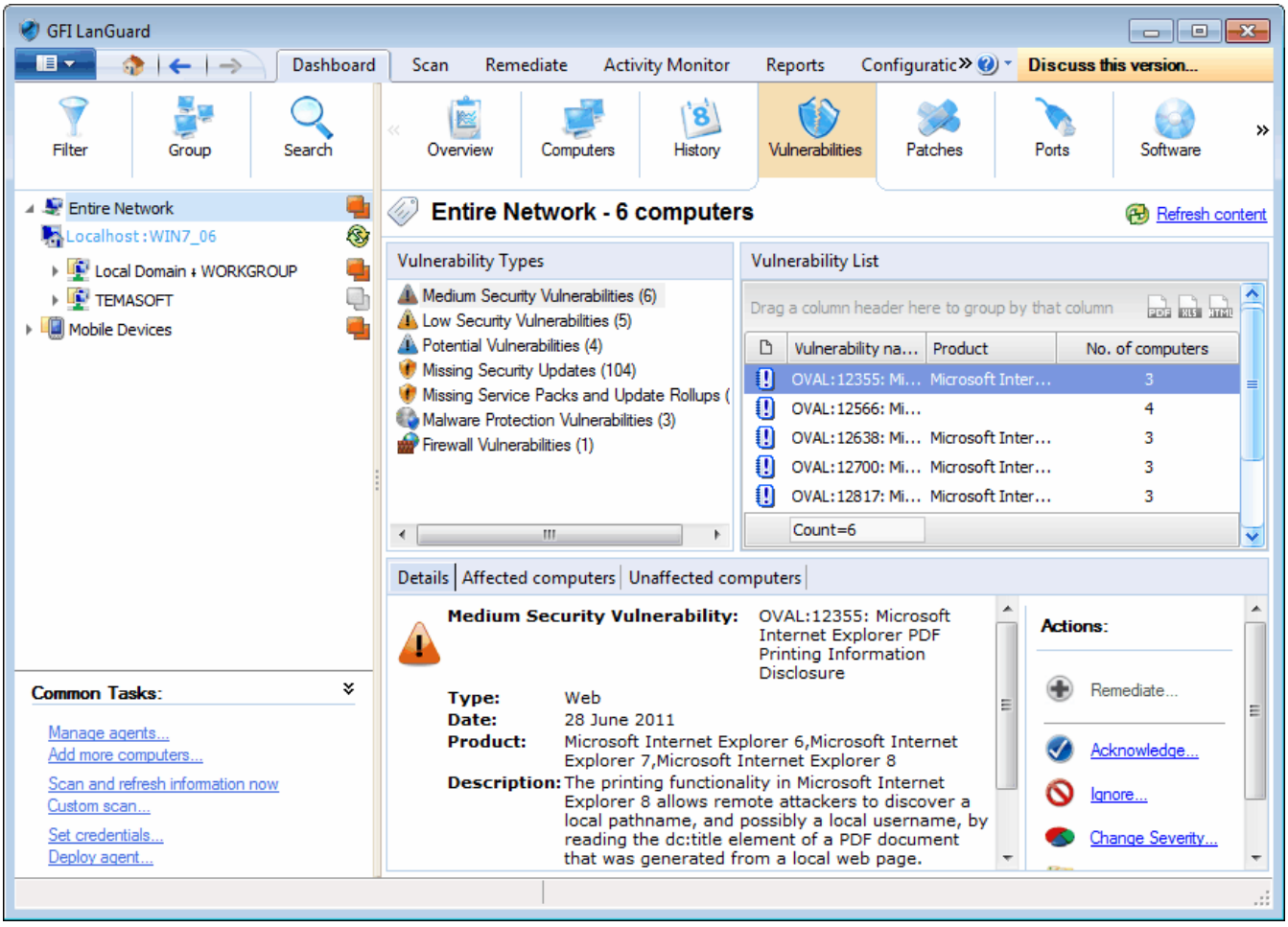
Select this view to group audit results by date for a specific computer. To configure the history starting date or history period click the link provided.



Screenshot 91: History view in the Dashboard

Vulnerabilities View

Display more details on the vulnerabilities found on a network and the number of affected computers. When a vulnerability is selected from the **Vulnerability** List, the **Details** section provides more information on the selected vulnerability. From the **Details** section click **Affected computers** or **Unaffected computers** to display a list of affected and unaffected computers.



Screenshot 92: Vulnerabilities view in the Dashboard

> **NOTE**
> Drag and drop a column header in the designated area to group data by criteria.

Configuring actions

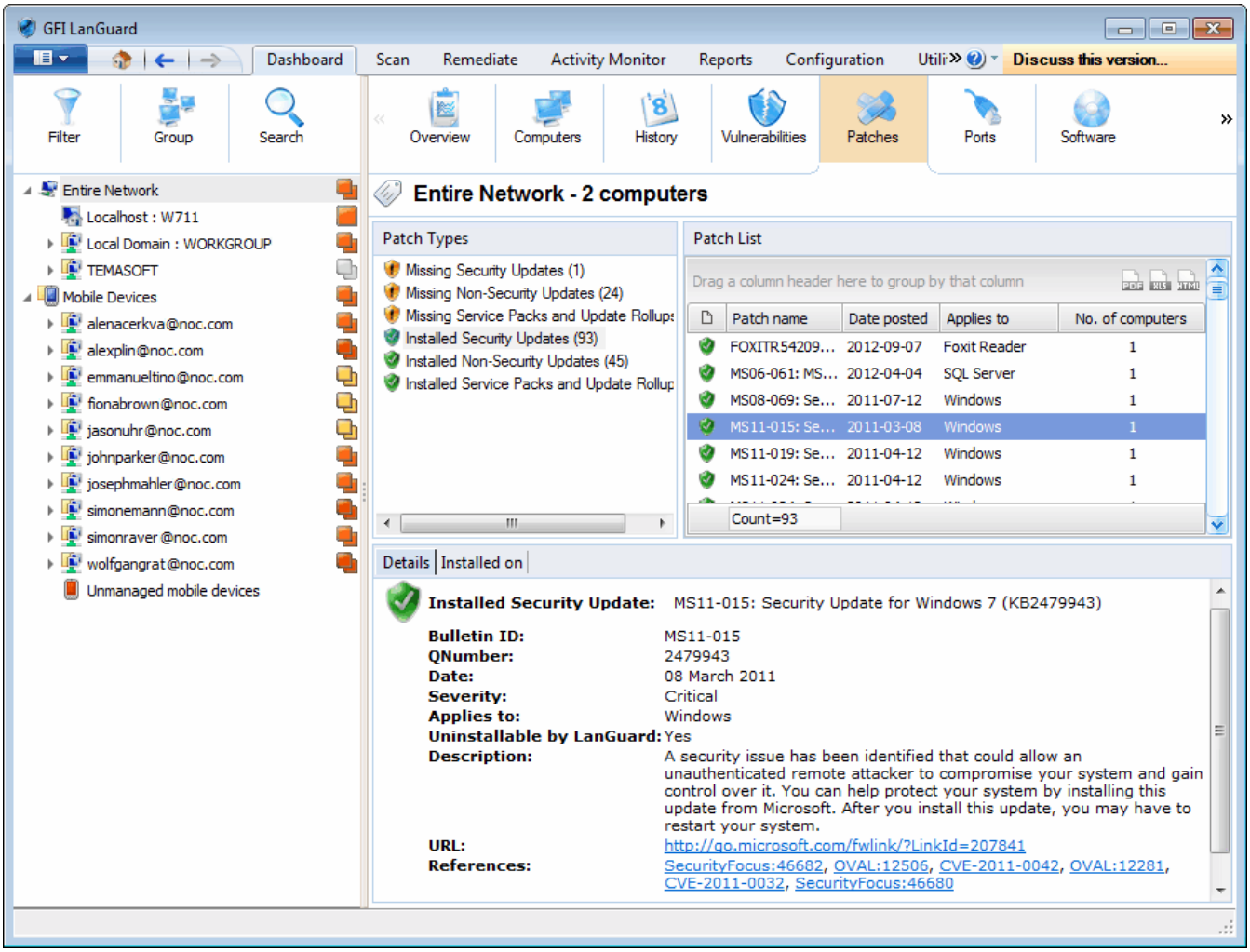
From the actions section select one of the actions described below to manage and remediate vulnerabilities and missing patches found in your network.

Action	Description
Remediate	Launch the Remediation Center to deploy and manage missing patches. **NOTE** For more information, refer to Manual Remediation (page 185).

Action	Description
Acknowledge	Launch the Rule-Acknowledge Patch dialog. This enables you to acknowledge issues so that they will not affect the Vulnerability level of your network. Configure for which machine this rule applies.
Ignore	Launch the Rule-Ignore Patch dialog. This enables you to ignore missing patches or vulnerabilities so that they will not be reported as issues in the future, and include reasons why to ignore such vulnerabilities. Configure for which machine this rule applies and the time span that the issue is ignored.
Change Severity	Launch the Rule-Change Severity dialog. This enables you to change the severity level of vulnerability. Configure for which machines this rule applies and the severity level.
Rules Manager	Launch the Rules Manager dialog. This enables you to search and remove configured rules and view the reasons to ignore missing patches and vulnerabilities.

Patches View

Display more details on the missing/installed patches and service packs found during a network audit. When a patch/service pack is selected from the list, the **Details** section provides more information on the selected patch/service pack. From the **Details** section, click **Missing on** to display a list of computers having the selected patch missing.



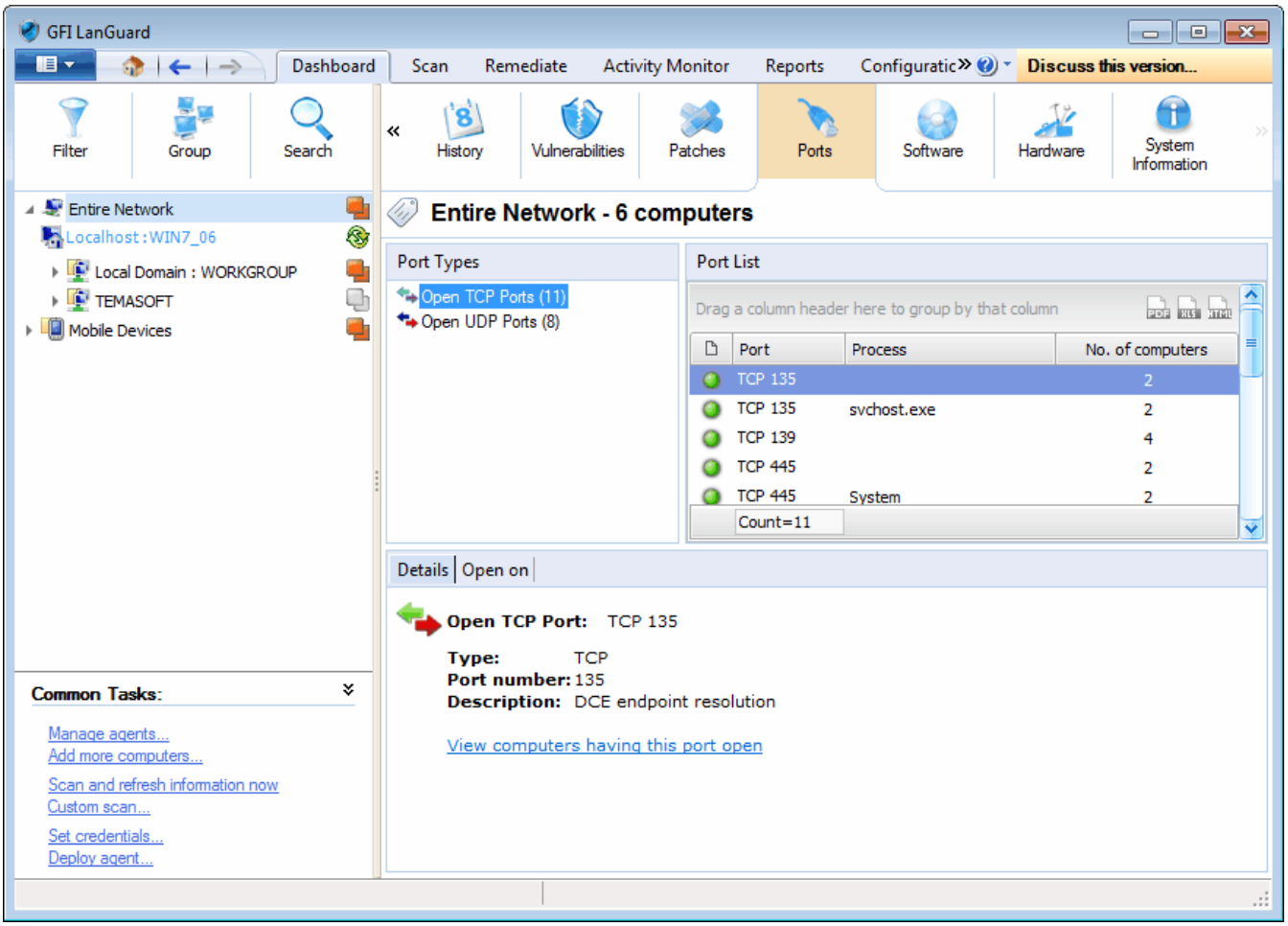
Screenshot 93: Patches view in Dashboard

NOTE

Drag and drop a column header in the designated area to group data by criteria.

Ports View

Display more details on the open ports found during a network audit. When a port is selected from the **Port** List, the **Details** section provides more information on the selected port. From the **Details** section, click **View computers having this port open** to display a list of computers having the selected port open.



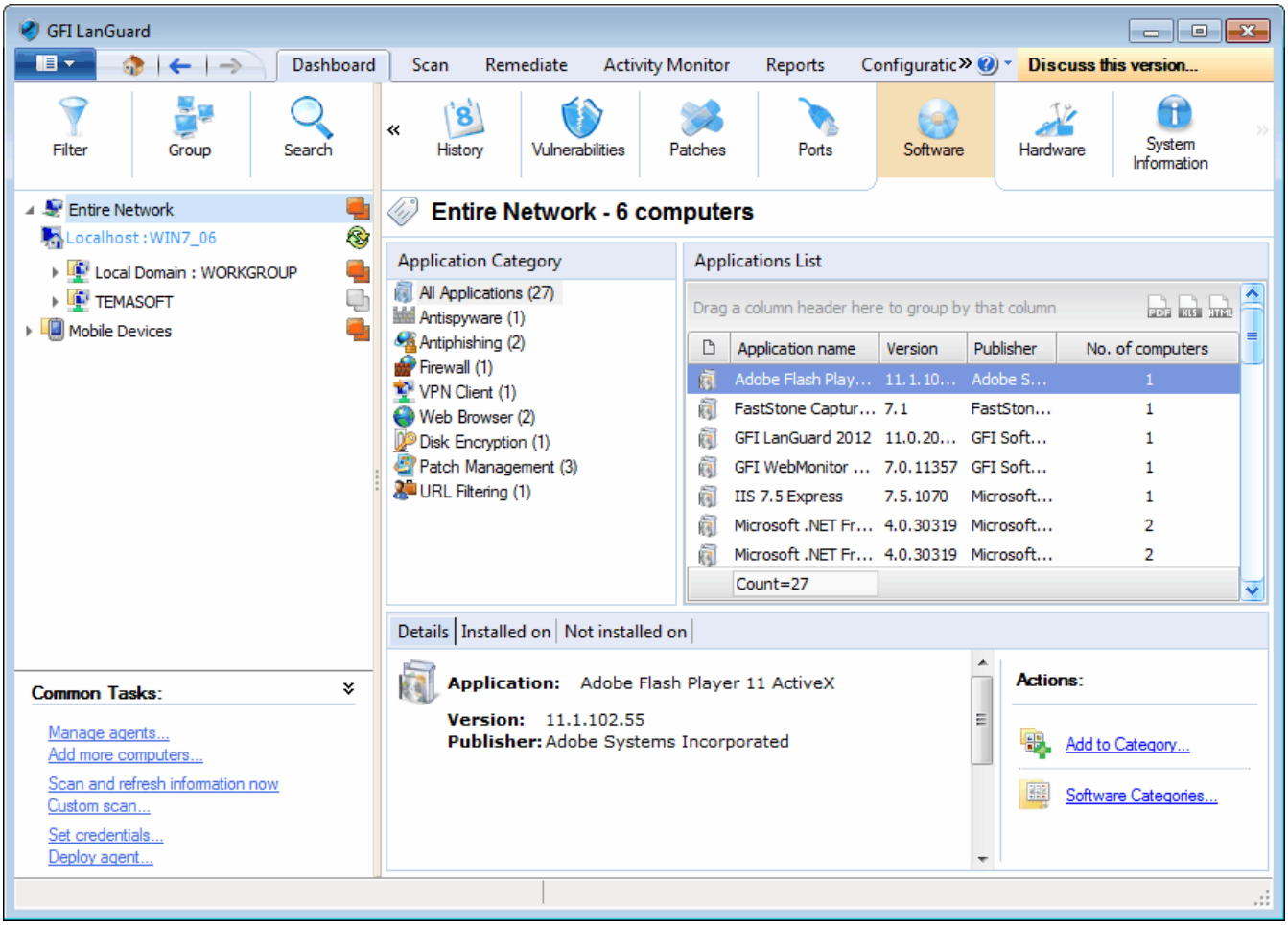
Screenshot 94: Ports view in Dashboard

NOTE

Drag and drop a column header in the designated area to group data by criteria.

Software View

Display more details on the installed applications found during a network audit. When an application is selected from the **Application** List, the **Details** section provides more information on the selected application.



Screenshot 95: Software view in Dashboard

From the actions section select one of the actions described below to manage and categorize software applications.

Option	Description
Add to category	Add applications to a particular category
Software Categories	Configure rules for particular software categories and applications. For more information refer to Configure software categories

NOTE

Drag and drop a column header in the designated area to group data by criteria.

NOTE

Agent-less scans require to temporarily run a service on the remote machine. Select **Enable full security applications audit…** to enable this service on all agent-less scanning profiles.

Configuring software categories

GFI LanGuard comes with a software categories feature that enables you to add and sort software according to different categories. GFI LanGuard also supports editing on software details.

» Adding New Software Categories

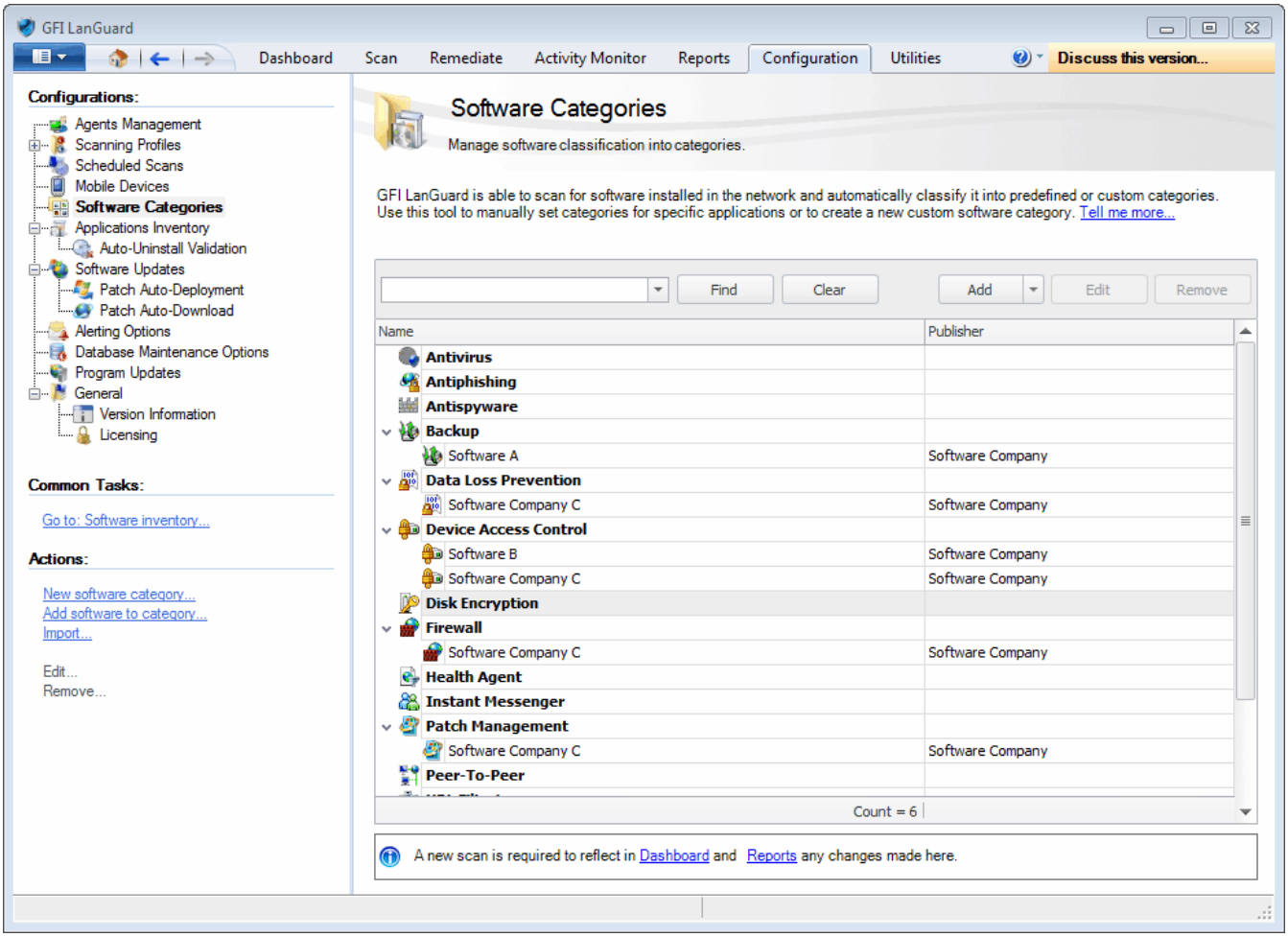
» Adding New Software to a Category

» Importing Software to a Category

» Customizing Software

To configure Software categories:

1. Click on the **Configuration** tab **> Software Categories** to set categories for specific applications or to create a new software categories.

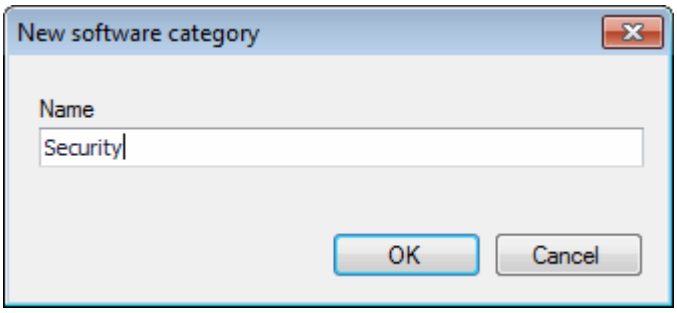


Screenshot 96: Software Categories

Adding New Software Categories

To add new software categories:

1. Click **Configuration** tab **> Software Categories** and from the right panel click on the **Add**drop-down list and select**New software category**.



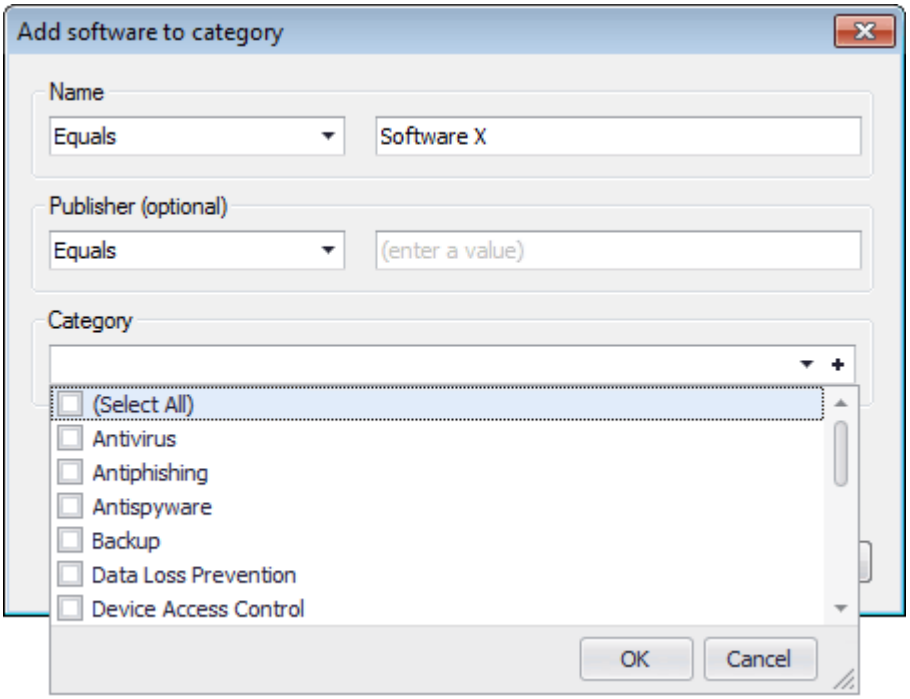
Screenshot 97: Software category name

2.
Key in the name for the new software category.

Adding New Software to a Category

To add new software to a category:

1. Click **Configuration** tab **> Software Categories** and from the right panel click on the **Add**drop-down list and select**Add software to category**.



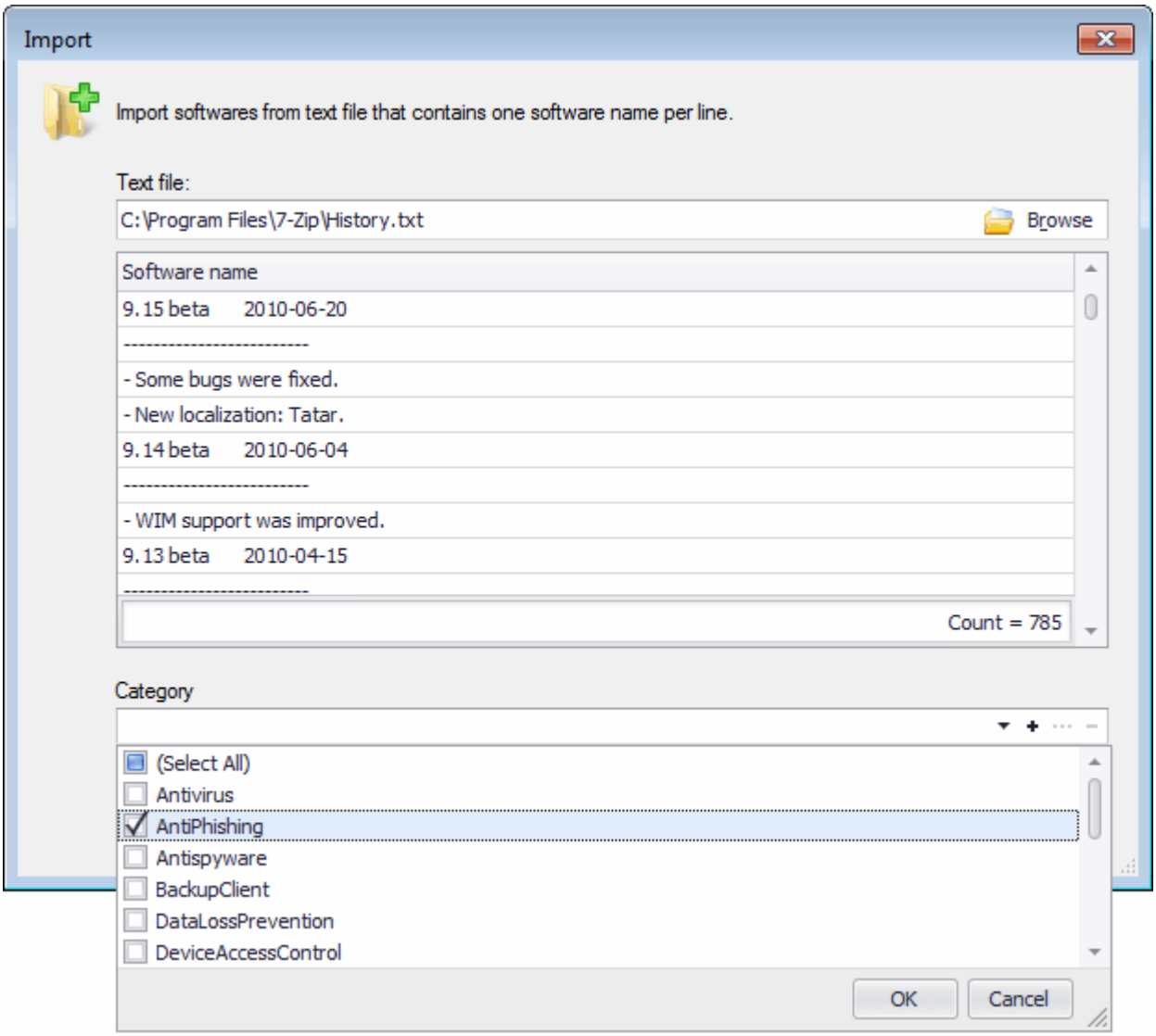
Screenshot 98: Adding a software to a category

2.
Enter the name and publisher of the new software and select the category for the new software.

Importing Software to a Category

To import software to a category:

1. Click **Configuration** tab **> Software Categories** and from the right panel click on the **Add**drop-down list and select**Import**.



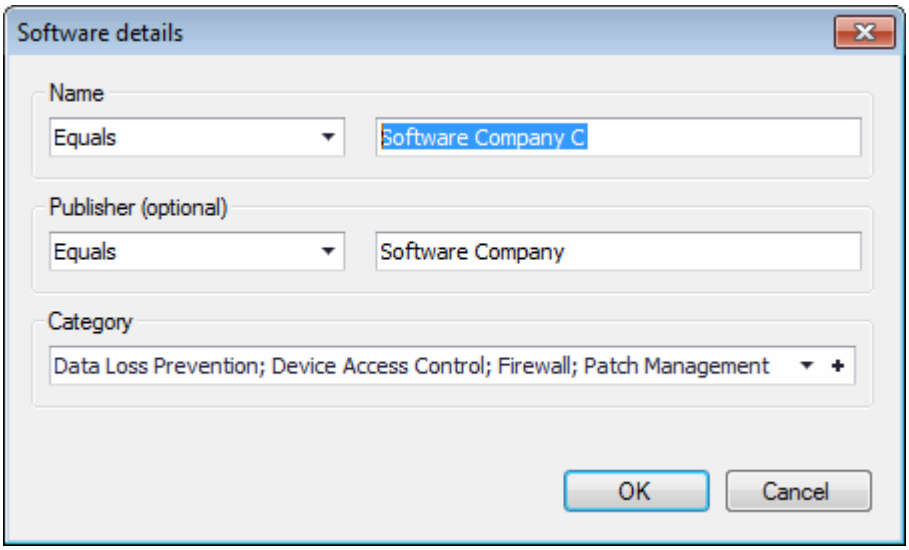
Screenshot 99: Importing a software to a category

2. Select the text file containing the software name and select the category you want the software to be included in.

Customizing Software

To customize software in a category:

1. Click **Configuration** tab **> Software Categories** and from the right panel click **Edit**.

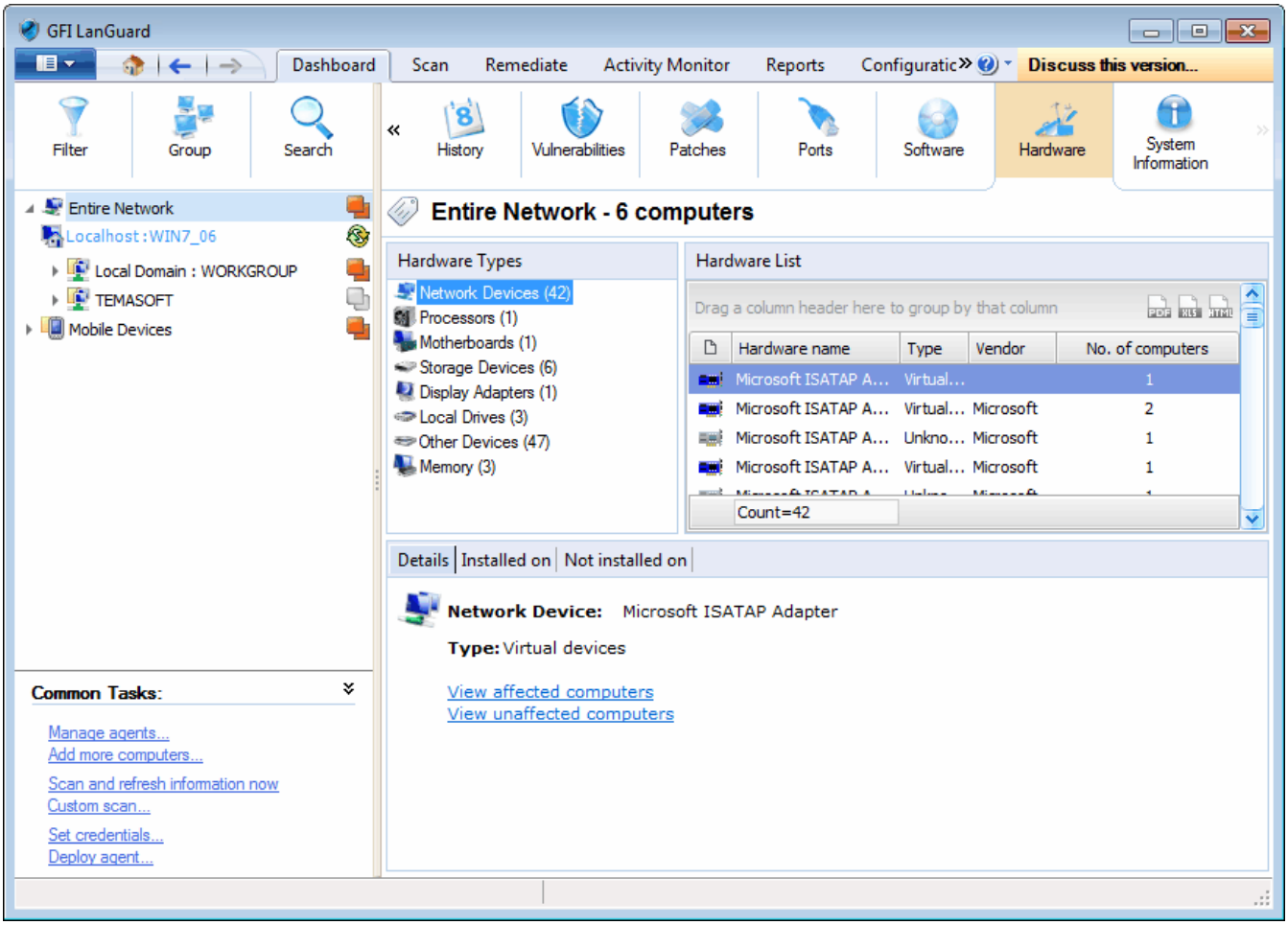


Screenshot 100: Editing software details

2.
Change the necessary details and click **OK** to save the changes.

Hardware View

Display more information on the hardware found during a network audit. Select hardware from the list to display more details.



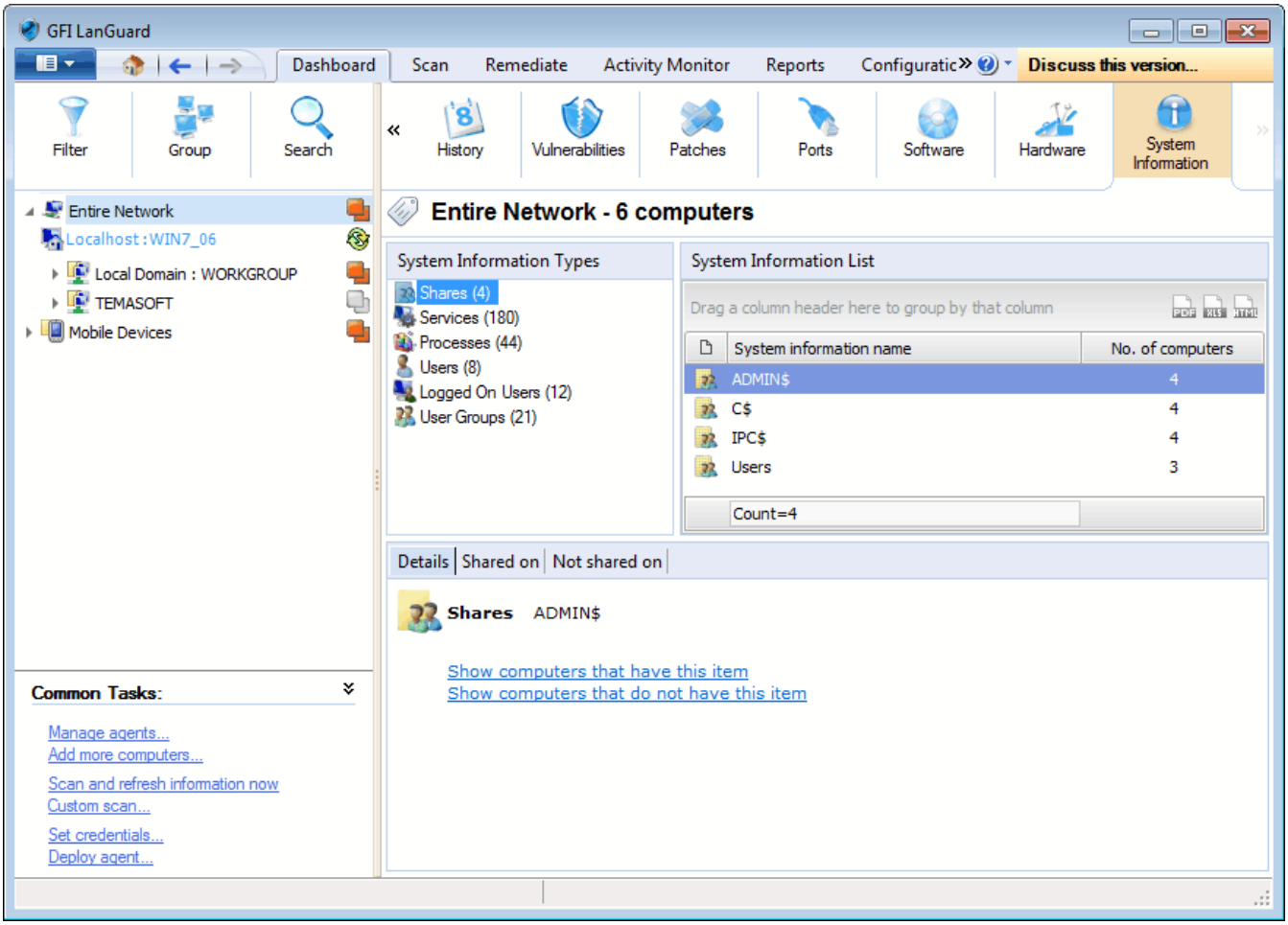
Screenshot 101: Hardware view in Dashboard

NOTE

Drag and drop a column header in the designated area to group data by criteria.

System Information View

The **System Information** tab, displays information associated with the operating system of a scan target(s).



Screenshot 102: System Information view in Dashboard

NOTE

Drag and drop a column header in the designated area to group data by criteria.

4.4 Interpreting Results

On completion of a network security scan, it is important to identify the areas that require immediate attention. Use the information provided in this topic to determine the correct analysis and interpretation approach to get the most out of your scan results and apply the appropriate fixes.

Topics in this section:

4.4.1 Interpreting scan results

The **Scan Results Overview** and **Scan Results Details** sections in the **Scan** tab, are designed to facilitate the result analysis process as much as possible. Use the information in the following sections to learn how scan results are interpreted and to know which areas require your immediate attention:

- Viewing scan results
- Vulnerability level rating
- Vulnerability Assessment
- Network & Software Audit

Viewing scan results

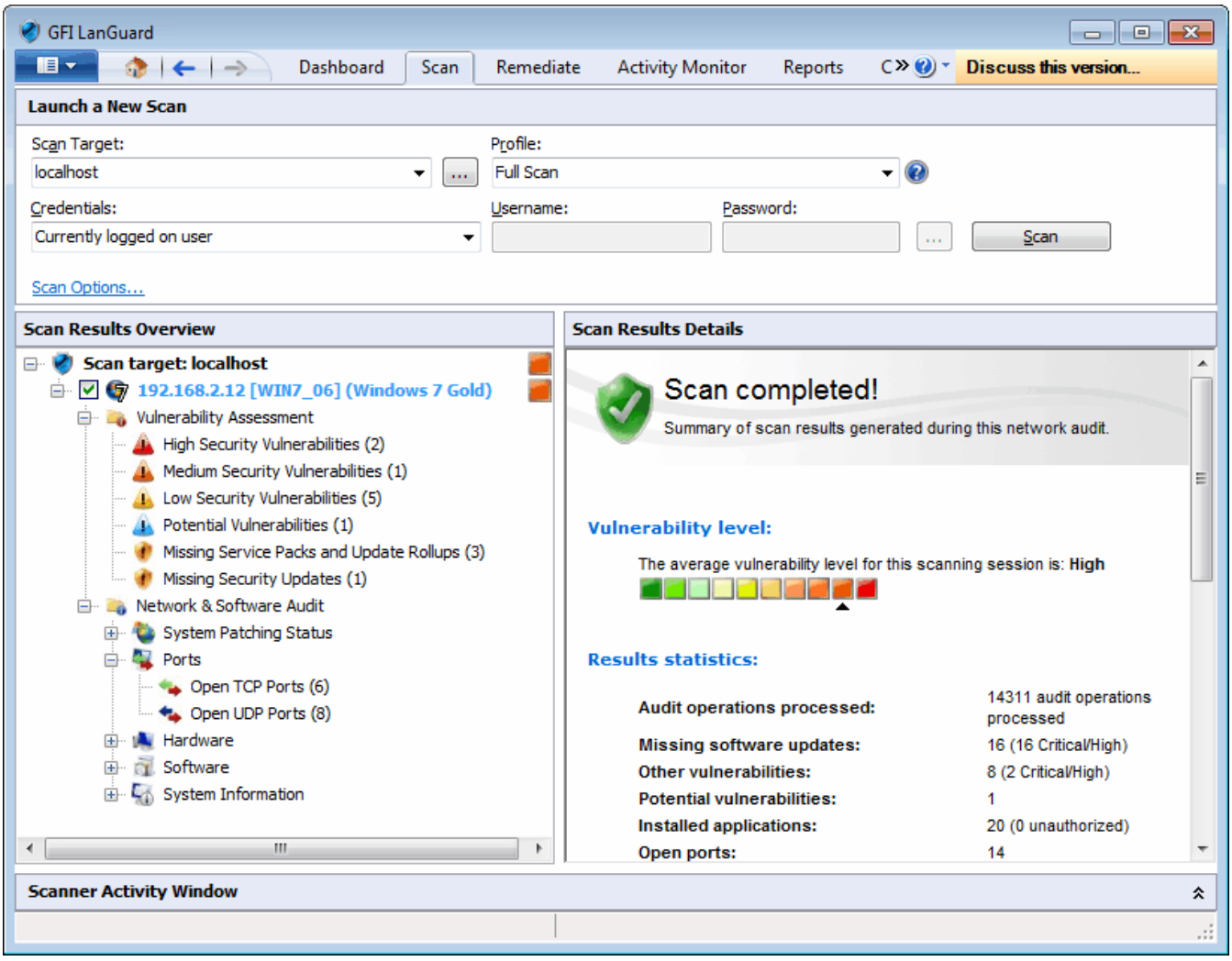
Use this section to interpret results generated by manual scans and results stored in the database backend. For more information, refer to Manual scans (page 96).

To view scan results:

1. Launch GFI LanGuard and click the **Scan** tab.

2. Launch a new scan or load the result from the database/file. For more information, refer to Loading results from the database (page 160).

3. Once completed, the results are displayed in the **Scan Result Overview** and the **Scan Results Details** sections.



Screenshot 103: Results overview

From **Scan Results Overview**, expand a computer node to access results retrieved during the scan. Security scan results are organized in two sub–nodes tagged as:

» Vulnerability Assessment

» Network & Software Audit

While a scan is in progress, each computer node has an icon that categorizes the response time. The table below describes the different icons used by GFI LanGuard to categorize the response time. The first icon indicates that the scan is queued, while the second icon indicates that the scan is in progress.

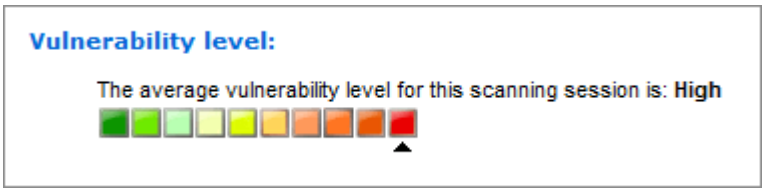
Category	Information	Description
	Fast response	Less than 25ms
	Medium response	Between 25ms and 100ms
	Slow response	More than 100ms

Vulnerability Level Rating

The GFI LanGuard vulnerability level is a rating assigned to each scanned computer. The rating can be viewed from:

» **Scan Results Details** – This section in the Scan tab provides you with a vulnerability level meter assigned the computers/groups that have been scanned

» **Dashboard** – The Dashboard section provides you with information for specific computers or selected groups of computers, from the computer tree. Select the computer/group and view the vulnerability meter from the right pane. Select Entire Network to view the vulnerability level for all your scan targets.



Screenshot 104: Vulnerability level meter

How is the vulnerability level calculated?

The vulnerability level is calculated using a weighting system. After a scan, GFI LanGuard groups the discovered vulnerabilities in categories sorted by severity rating:

» High

» Medium

» Low

For each rating, a weighted score is given. This is based on the total number of vulnerabilities per category.

> **NOTE**
> When the vulnerability level cannot be assessed or vulnerability scanning was not performed, GFI LanGuard gives a rating of **N/A**.

Weight scores

Category	Number of Detected Vulnerabilities	Scores
High Vulnerabilities	1-2 3-5 > 5	8 9 10
Medium Vulnerabilities	1-2 3-5 > 5	5 6 7
Low Vulnerabilities	1-2 3-5 > 5	2 3 4

Score classification

After categorizing detected vulnerabilities and generating a score for each category, the overall vulnerability level is generated. The vulnerability level is the severity rating with the highest score.

Vulnerability level scores:

» A score of >= **8**, results in **High** vulnerability rating

» A score of <= **7** and >= **5**, results in **Medium** vulnerability rating

» A score of <= **4** and >=**1**, results in a **Low** vulnerability rating

Example

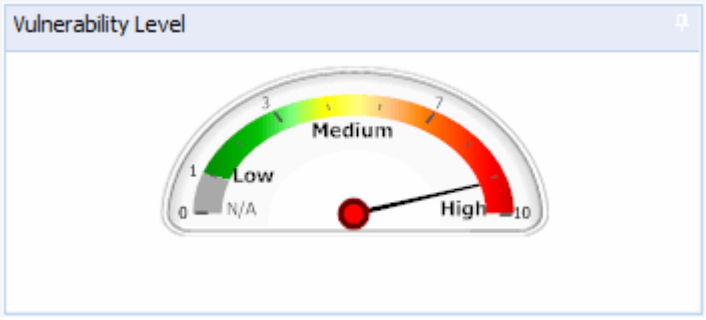
During a scan of Computer A, the following vulnerabilities were discovered:

- 3 high vulnerabilities
- 8 medium vulnerabilities
- 5 low vulnerabilities

The score for each category was calculated with the following results:

- 3 high vulnerabilities = 9
- 8 medium vulnerabilities = 7
- 5 low vulnerabilities = 3

The vulnerability level for Computer A is therefore **HIGH**.

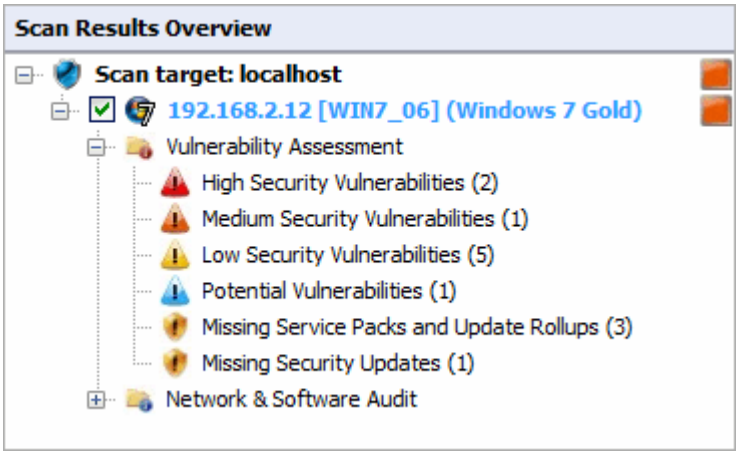


Screenshot 105: Dashboard Vulnerability Meter

The vulnerability level is indicated using color–coded graphical bar:

- Red bar = high vulnerability level
- Green bar = low vulnerability level.

Vulnerability Assessment



Screenshot 106: The Vulnerability Assessment node

Click on any **Vulnerability Assessment** node to view the security vulnerabilities identified on the target computer grouped by type and severity.

High Security Vulnerabilities

Click on the **High Security Vulnerabilities** or **Low Security Vulnerabilities** sub–nodes for a list of weaknesses discovered while auditing a target device. Groups are described in the following table:

Group	Description
Mail, FTP, RPC, DNS and Miscellaneous	Shows vulnerabilities discovered on FTP servers, DNS servers, and SMTP/POP3/IMAP mail servers. Links to Microsoft® Knowledge Base articles or other support documentation are provided.
Web	Lists discovered vulnerabilities on web servers (such as wrong configuration issues). Supported web servers include Apache, Internet Information Services (IIS®) and Netscape.
Services	Lists vulnerabilities discovered in active services as well as the list of unused accounts that are still active and accessible on scanned targets.
Registry	Registry settings of a scanned network device are listed. Links to support documentation and short vulnerability descriptions are provided.
Software	Enumerates software installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.
Rootkit	Enumerates discovered vulnerabilities because of having a rootkit installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.

Potential vulnerabilities

Select **Potential vulnerabilities** sub–node to view scan result items classified as possible network weaknesses. Although not classified as vulnerabilities, these scan result entries still require particular attention since malicious users can exploit them during malicious activity.

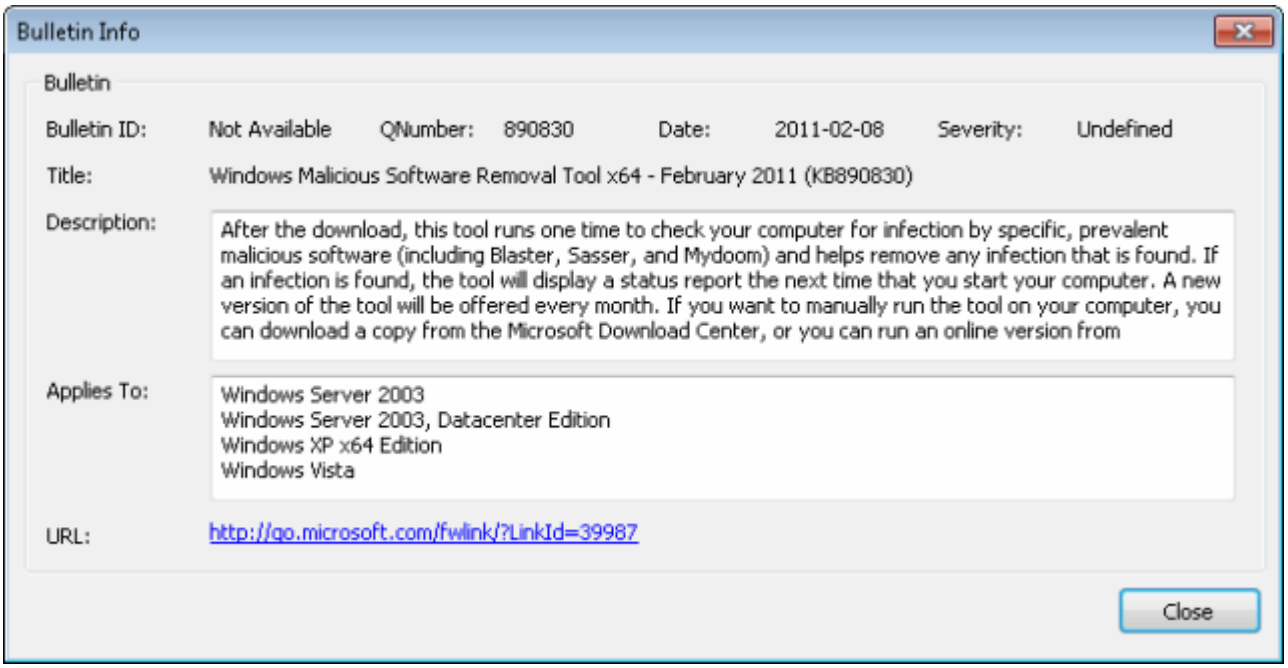
For example, during vulnerability scanning GFI LanGuard enumerates all modems installed and configured on target computers. If unused, modems are no threat to your network. If connected to a telephone line these modems can, however, be used to gain unauthorized and unmonitored access to the Internet. Users can potentially bypass corporate perimeter security including firewalls, antivirus, website rating and web content blocking. This exposes the corporate IT infrastructure to a wide range of threats including hacker attacks. GFI LanGuard considers installed modems as possible threats and enumerates them in the **Potential Vulnerabilities** sub–node.

Missing Service Packs

Click **Missing Service Packs and Update Rollups** or **Missing Security Updates** sub–nodes to check any missing software updates or patches. For a full list of missing service packs and missing patches that can be identified by GFI LanGuard, refer to http://go.gfi.com/?pageid=ms_app_fullreport

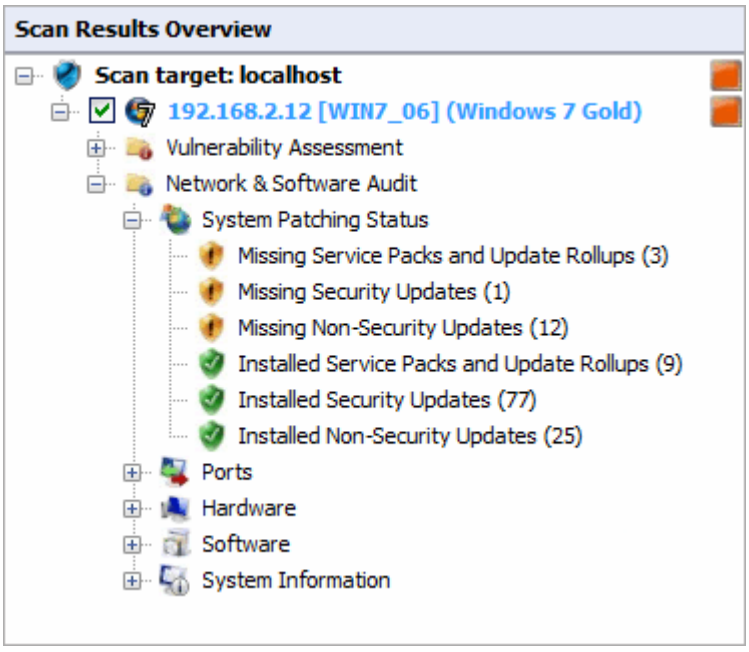
Bulletin information.

To access bulletin information, right–click on the respective service pack and select **More details>Bulletin Info**.



Screenshot 107: Bulletin info dialog

Network & Software Audit



Screenshot 108: The network and software audit node

Click **Network & Software Audit** to view security vulnerabilities identified on scanned targets. In this section, vulnerabilities are grouped by type and severity.

System Patching Status

Click **System Patching Status** to view all missing and installed patches on a target machine. Available links are:

- Missing Service Packs and Update Rollups
- Missing Security Updates

- Missing Non-Security Updates
- Installed Service Packs and Update Rollups
- Installed Security Updates
- Installed Non-Security Updates.

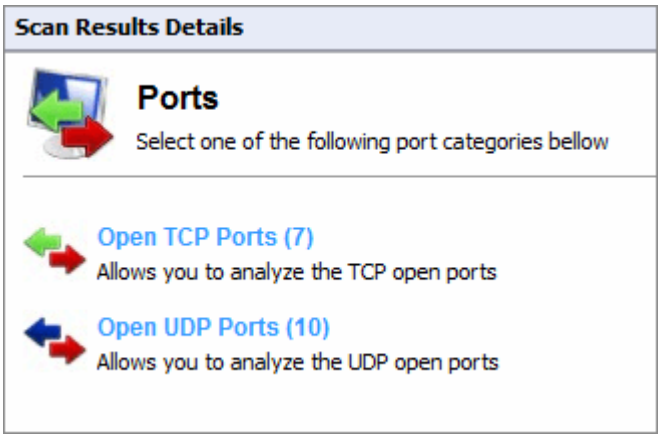
Screenshot 109: System patches status

Open Ports

Click **Ports** to view all open TCP and UDP ports detected during a scan. If a commonly exploited port is discovered to be open, GFI LanGuard marks it in red.

> **NOTE**
> Some software products may use the same ports as known Trojans. For additional security, GFI LanGuard identifies these ports as a threat.

Apart from detecting open ports, GFI LanGuard uses service fingerprint technology to analyze the services that are running behind the detected open ports. With service fingerprint, GFI LanGuard can detect if malicious software is using the detected open port.



Screenshot 110: All UDP and TCP ports, found during a scan

Hardware audit

Click **Hardware** to view all details discovered by the hardware audit. The hardware audit, amongst others, displays information such as MAC addresses, IP addresses, device type; device vendor etc. The table below describes the hardware information groups:

Information	Description
Network Devices	Includes information of all physical, virtual and software–enumerated devices.
Local Drives	Includes information on local drives such as available disk space and file system type.
Processors	Includes information regarding the processor of a target machine, such as vendor name and processor speed.
Motherboard	Includes information regarding the motherboard of a target machine, such as product name, manufacturer, version and serial number.
Memory details	Includes information regarding the memory allocation of a target machine, such as free physical/virtual memory available.
Storage details	Includes information regarding the storage of a target machine, such as floppy disk drive, CD/ROM and hard drives.
Display adapters	Includes information regarding the display and video devices of a target machine, such as the device manufacturer.
Other devices	Includes information of devices that do not fall under the mentioned categories above, such as keyboard, ports, mouse and human interface devices.

Software audit

Click **Software** to view all details involved in the software audit. The software audit amongst others displays information such as:

- Application name
- Publisher
- Version.

The table below describes the hardware information groups:

Icon	Description
General Applications	Enumerates installed software on scan targets.

Icon	Description
Antivirus Applications	Lists installed antivirus engines on scan targets.
Instant Messenger Applications	Lists all detected instances of Instant messenger applications on scan targets.
Patch Management Applications	Lists all the installed patch management applications, detected on your scan targets during a scan.
Web Browser Applications	Contains scanned targets that have Internet browsers installed.
Firewall Applications	Enumerates information on installed Firewall applications on scan targets.
Antiphishing Applications	Lists information of installed antiphishing engines on scan targets.
VPN Client Applications	Includes information on installed Virtual Private Network clients on scan targets.
Peer–To–Peer Applications	Shows installed Peer–To–Peer applications on scan targets.

System Information

Click **System Information** to view all details related to the operating system installed on a target machine. Table below describes the system information groups:

Category	Information	Identify
Shares	» Share name » Share remark (extra details on the share). » Folder which is being shared on the target computer » Share permissions and access rights » NTFS permissions and access rights.	» Users sharing entire hard–drives, shares that have weak or incorrectly configured access permissions. » Start-up folders, and similar system files, that are accessible by unauthorized users, or through user accounts, that do not have administrator privileges, but are allowed to execute code on target computers. » Unnecessary or unused shares.
Password Policy	» Minimum password length » Maximum password length » Minimum password expiry date » Force logoff » Password history.	» Incorrectly configured lockout control » Password strength enforcement policies.
Security Audit Policy	» Audit account logon events » Audit account management » Audit directory service access » Audit logon events » And more…	» Security holes or breaches. **NOTE** To view Security Audit Policy, enable auditing on target computers. For more information, refer to Enabling security audit policies (page 100).
Registry	» Registered owner » Registered organization » Product name » Current build number.	» Hardware and software settings such as which drivers and applications will be automatically launched at system startup.

Category	Information	Identify
NETBIOS Names	» Workstation service » Domain name » Domain controllers » File server service.	» Rogue computers » Wrong configurations.
Groups	» Account operators » Administrators » Backup operations » Guest.	» Wrong configurations » Security flaws due to rogue or obsolete user groups.
Users	» Full name » Privilege » Flags » Login.	» Rogue, obsolete or default user accounts.
Logged On Users	» List of logged on users.	» Authorized and unauthorized users currently logged on computers.
Sessions	» Lists hosts remotely connected to the target computer during scanning.	» Authorized and unauthorized remote connections.
Services	» List of active services.	» Rogue or malicious processes; redundant services.
Processes	» List of active processes.	» Rogue or malicious processes.
Remote TOD (time of day)	» Time of remote workstation, server or laptop.	» Time inconsistencies and regional settings » Wrong configurations.

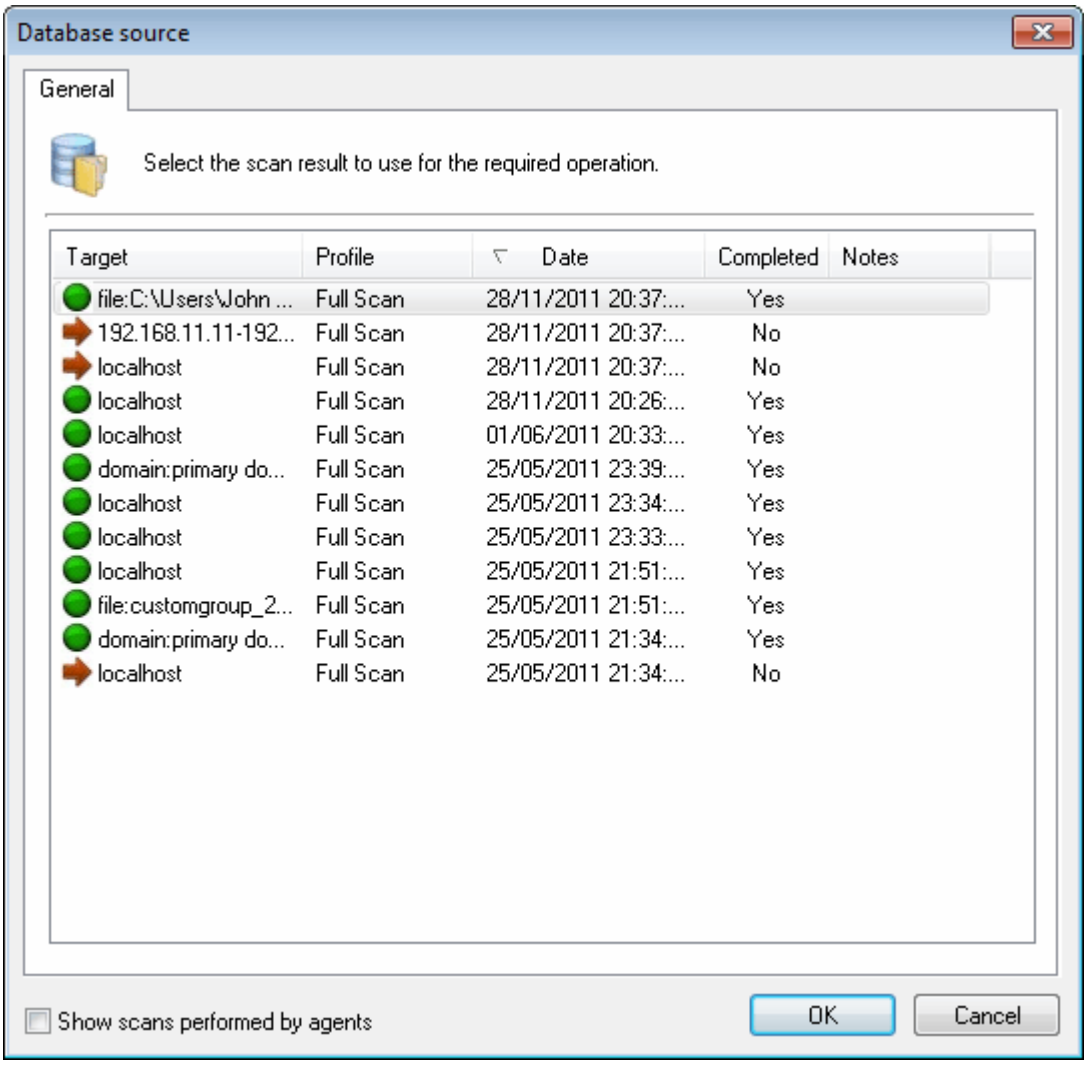
4.4.2 Loading results from the database

By default, saved scan results are stored in a database. GFI LanGuard stores the results data of the last 10 scans performed per scanning profile. You can configure the number of scan results that are stored in a database file. For more information, refer to Configuring Database Maintenance Options (page 236).

To load saved scan results from the database backend or from XML files:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button **> File > Load Scan Results from > Database…**



Screenshot 111: Reloaded scan results

3. Select the saved scan result and click **OK**

4. Analyze loaded results. For more information on how to interpret results. refer to the following sections:

» Vulnerability Assessment

» Network and Software Audit.

4.4.3 Saving and loading XML results

Scan results are an invaluable source of information for systems administrators. GFI LanGuard results are stored in a SQL Server® or a Access™ database. In addition, scan results can also be exported to XML.

To save scan results to XML file:

1. Launch GFI LanGuard.

2. Perform a manual scan. For more information, refer to Manual scans (page 96).

3. Once the scan is completed, click GFI LanGuard button **> File > Save Scan Results**.

4. Locate the destination where you want to save the XML and click **Save**.

To load saved scan results from an XML file:

1. Click the GFI LanGuard button **> File > Load Scan Results from > XML File…**

2. Locate the scan results to load and click **OK**

3. Analyze loaded results.

> **NOTE**
> For more information on how to interpret results, refer to the following sections:
>
> » Vulnerability Assessment
>
> » Network and Software Audit

4.5 Remediate Vulnerabilities

GFI LanGuard enables you to manually or automatically fix vulnerabilities on network computers. Use the information in this topic to learn how to configure and manage remediation operations to maintain a high level of security amongst your scan targets.

Topics in this section:

4.5.1 Automatic Remediation

Automatic-Remediation enables you to automatically download and deploy missing patches as well as uninstall unauthorized applications during scheduled operations, automatically.

> **IMPORTANT**
> Auto–remediation and un–installation of un–authorized applications only work with scanning profiles that detect missing patches and/or installed applications.

Automatic Remediation tasks:

» Review Auto-Remediation Considerations

» Configure Missing Updates Auto-Deployment

» Configure Unauthorized Applications Auto-Uninstall

» Configure Auto-Remediation options

» Configure Wake-on-LAN on client machines

» Configure End-User reboot and shut down options

» Define Auto-Remediation Messages

» Configure Agents Auto-remediation

» Configuring Software Categories

Auto-remediation notes

Before enabling and configuring auto-remediation options, review the following notes about:

Installing software

Always test patches in a test environment before deployment.

By default, Microsoft® updates are not enabled for automatic deployment. Manually approve each patch (as it is tested) or set all Microsoft® updates as approved.

Uninstalling software

To uninstall software, a 3–stage process is required in order to identify whether the selected application supports silent uninstall:

Stage	Description
Stage 1	Select the application to auto–uninstall.
Stage 2	Ensure that application supports silent uninstall. Test this by trying to remotely uninstall the application. This is the validation process.
Stage 3	Setup a scheduled audit that will remove the unauthorized application. This is done automatically (using agents) or manually (agent–less approach).

Auto–remediation and un–installation of un–authorized applications only work with scanning profiles that detect missing patches and/or installed applications.

Configuring missing updates auto-deployment

GFI LanGuard ships with a patch auto–deployment feature that enables you to deploy missing patches and service packs in all languages supported by Microsoft® products. GFI LanGuard also supports patching of third party (Non–Microsoft®) patches. For a complete list of supported third party applications refer to http://go.gfi.com/?pageid=3p_fullreport. Refer to the following section for information about:

» Enabling Patch Auto-Deployment

» Configuring Patch Auto-Deployment advanced options

» Configuring Patch Auto-download settings

Enabling Patch Auto-Deployment

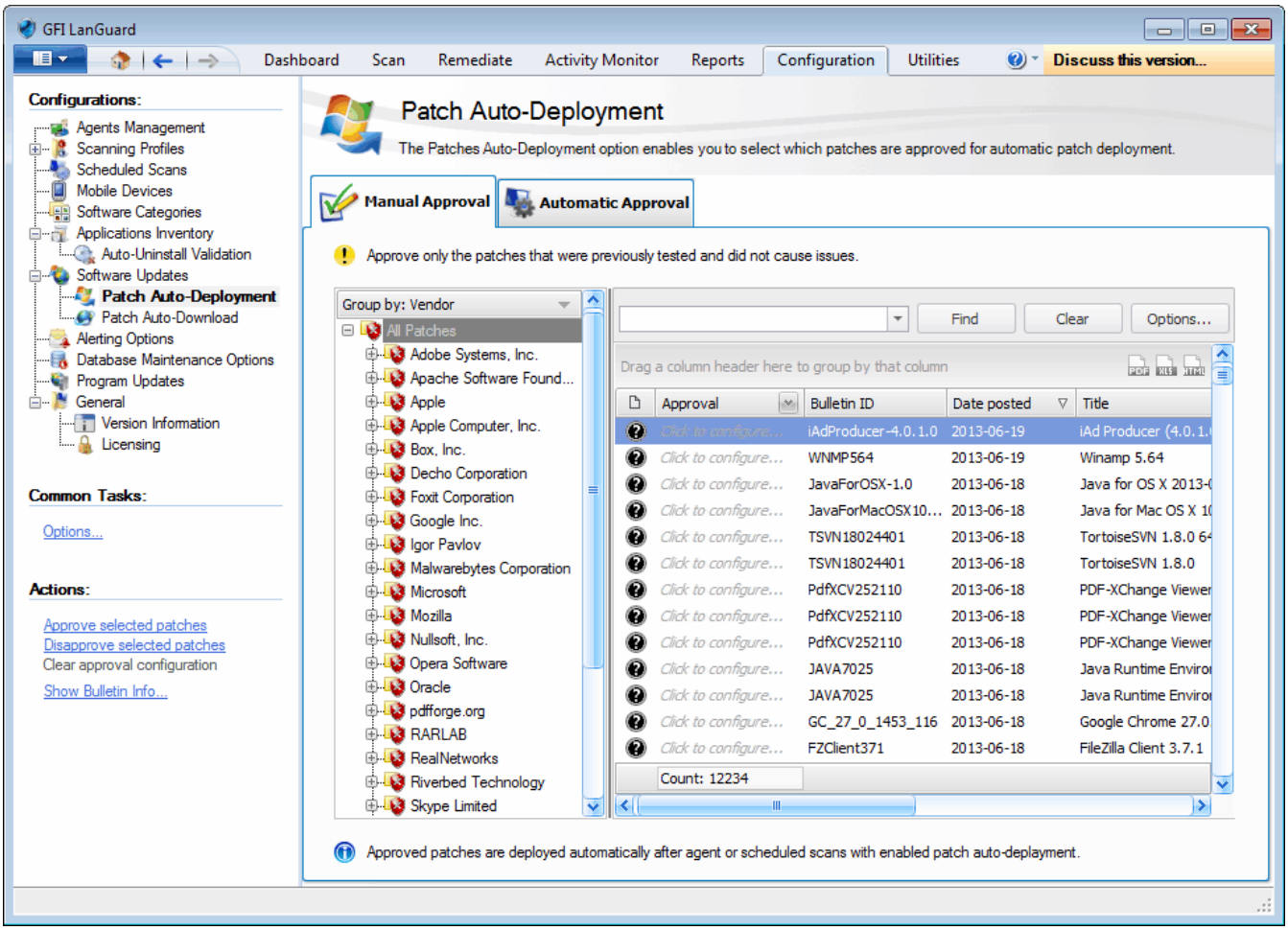
To configure patch auto–deployment:

1. Click on **Configuration** tab **> Software Updates > Patch Auto–Deployment**.

2. In the right pane, select the method for approval.

Manual approval

Use the **Manual approval** tab to approve patches one by one. This is achieved by using the list of unapproved patches grouped by vendor or severity that you want to be approved.

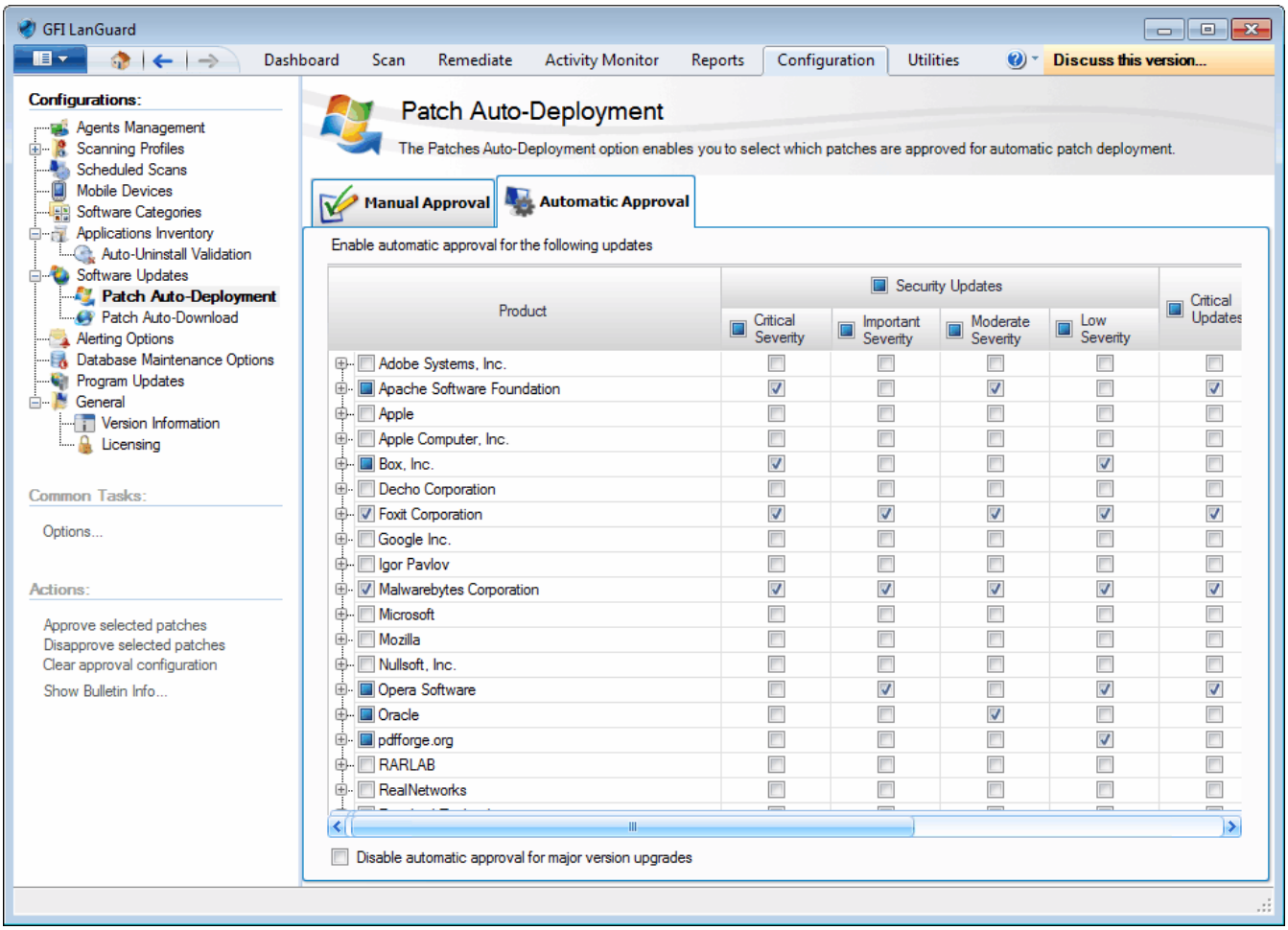


Screenshot 112: Patch auto–deployment: Manual approval

> **NOTE**
>
> Key-in a search criteria and click **Find** to search for a specific application.

Automatic approval

The **Automatic approval** tab enables you to specify which group of patches are automatically approved according to a category for a particular vendor.

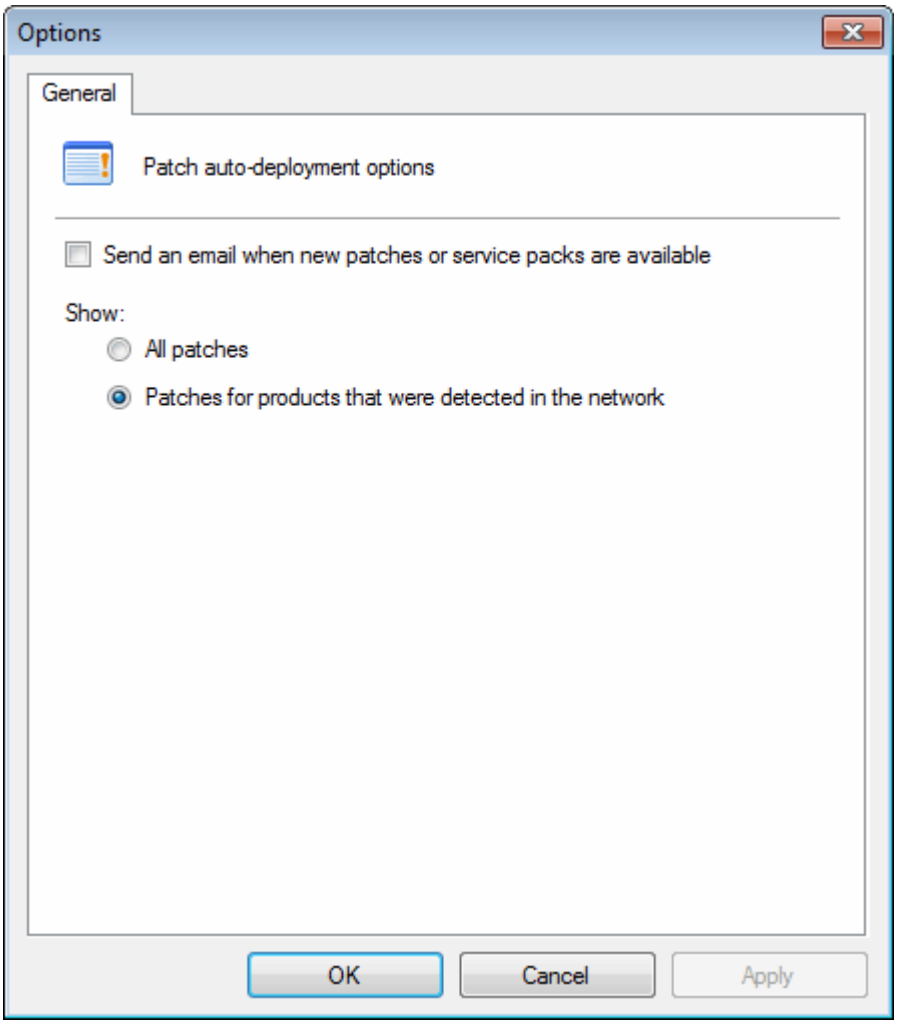


Screenshot 113: Patch auto–deployment: Automatic approval

Configuring Patch Auto-Deployment advanced options

To configure auto–remediation:

1. Click **Configuration** tab **> Software Updates > Patch Auto–Deployment** and from **Common Tasks**, click **Advanced options**.



Screenshot 114: Patch Auto–Deployment Advanced Options

2. Configure the following options:

Option	Description
Send an email when new patches or service packs are available.	Send an email when new patches are identified.
Show all patches:	Displays all the identified patches .
Show patches for products that were detected in the network:	Displays only the patches identified on the selected network.

3. Select the appropriate check boxes and click **OK** to save changes.

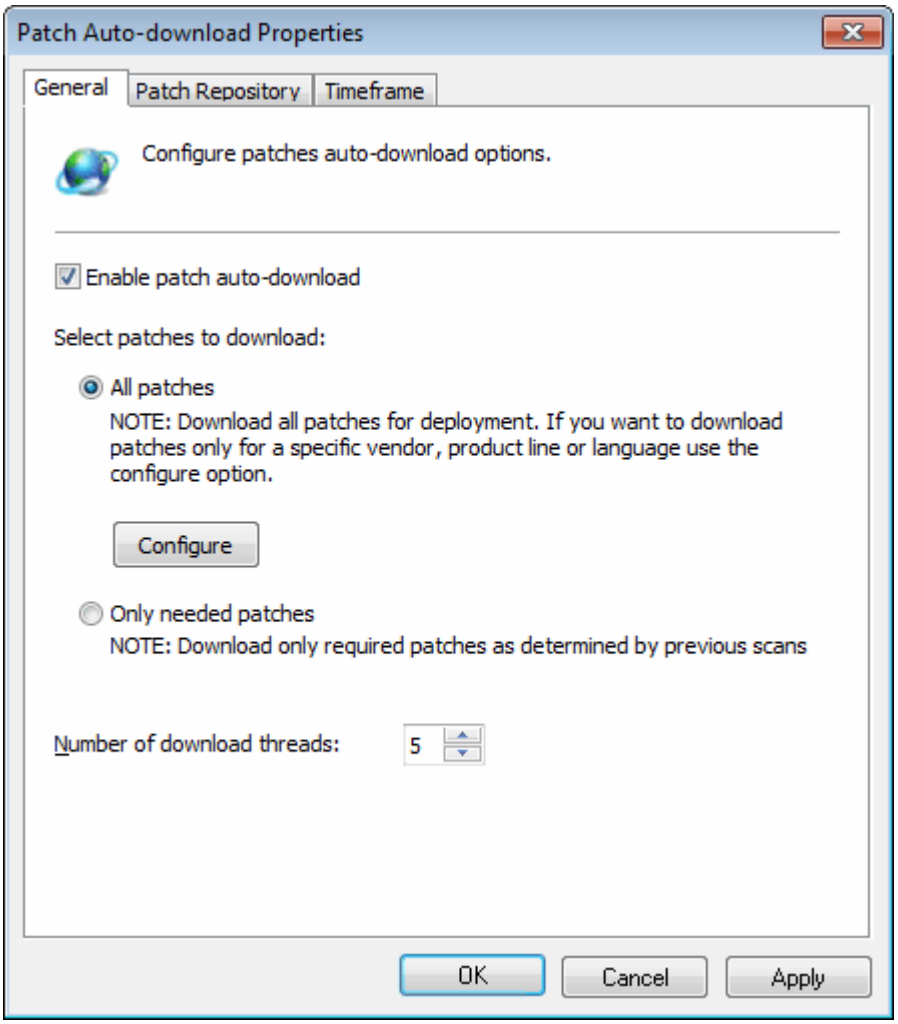
Configuring Patch Auto-download settings

GFI LanGuard ships with a patch auto–download feature that enables the automatic download of missing patches and service packs in all languages supported by Microsoft® products. In addition, you can also schedule patch auto–download by specifying the time-frame within which the download of patches is performed.

To configure patch auto–download:

1. Click **Configuration** tab **> Software Updates > Patch Auto–Download**.

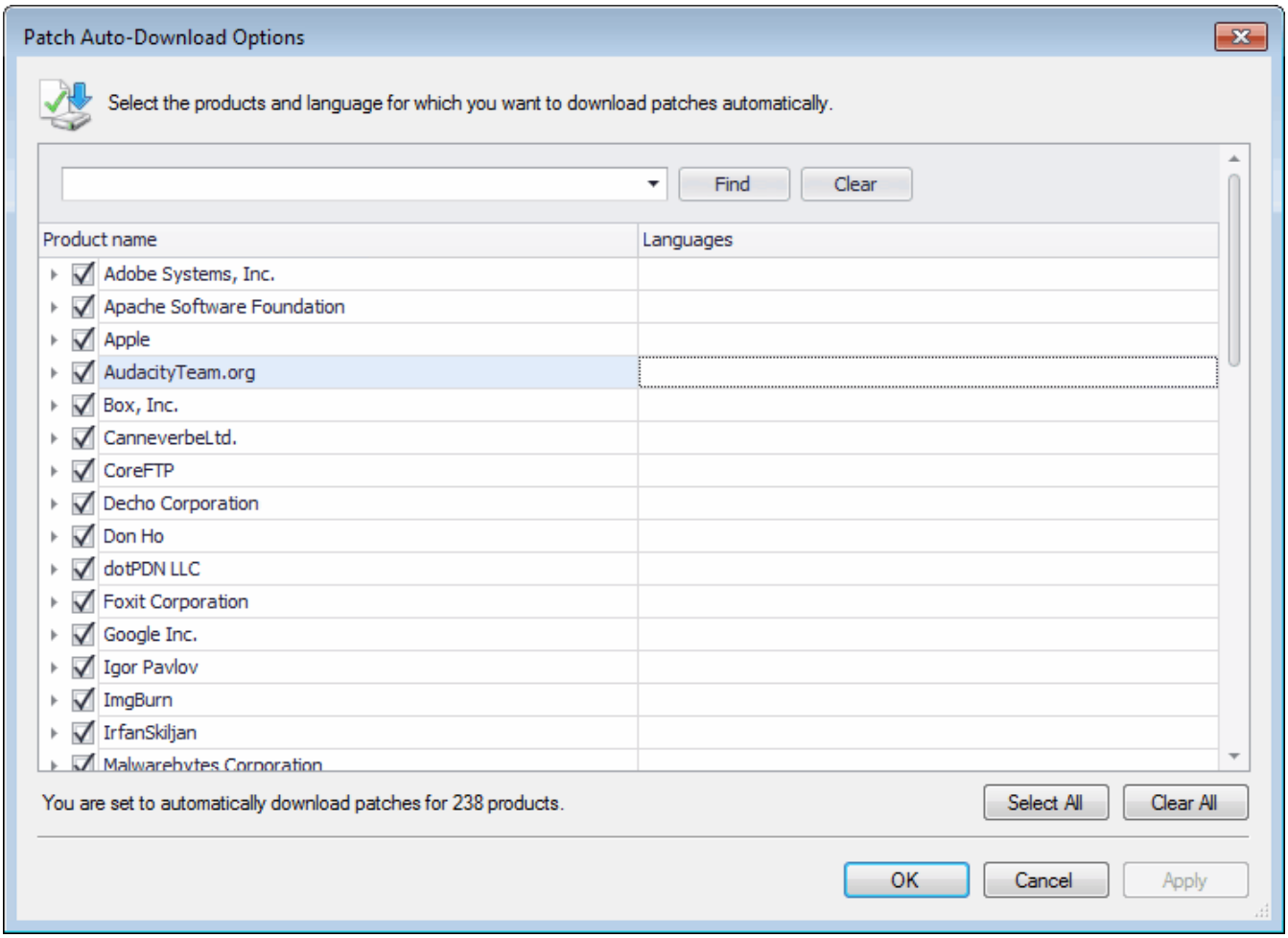
2. From the right pane, click the link.



Screenshot 115: Configuring Patch Auto–download Properties

3. In the **General** tab, select between **All patches** or **Only needed patches**.

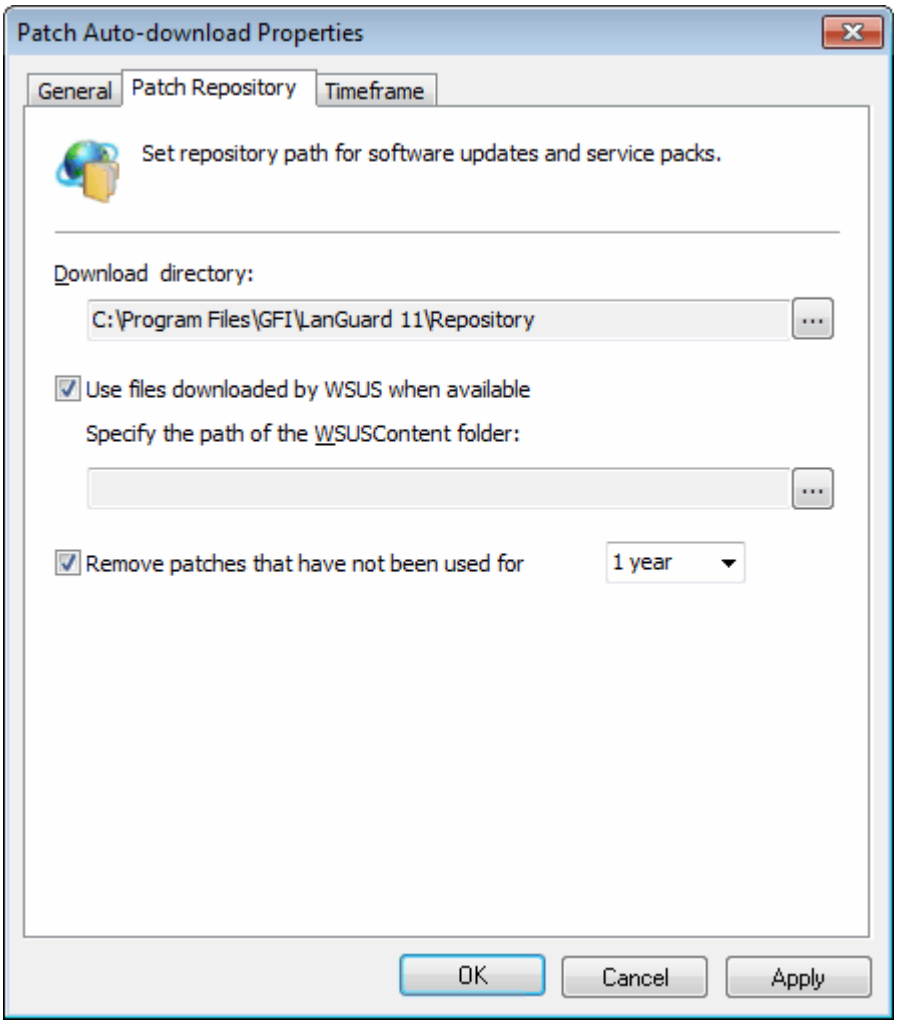
4. In the **All patches** tab click **Configure** to restrict auto-download of patches for configured languages.



Screenshot 116: Configuring Patch Auto–download - All Patches Properties

NOTE

Selecting **All patches > Configure**, enables administrators to manually select the Microsoft® patches to download , regardless of whether these are required for deployment. The **Only needed patches** option downloads only patches required for deployment.



Screenshot 117: Patch Repository settings

4. To change the location where the downloaded patches are stored click the **Patch Repository** tab and specify the required details.

5. Select **Use files downloaded by WSUS when available**, if you are using an existing setup of WSUS.

6. Select **Remove patches that have not been used for** and select the time duration if you want to remove files that have not been used for remediation in the specified time interval.

7. To change the time frame during which patch downloads are performed, click **Timeframe** tab and specify the required details.

8. Click **Apply** and **OK**

Configuring unauthorized applications auto-uninstall

Application auto–uninstall entails that applications marked as unauthorized for specific scanning profiles are first validated for a successful uninstall on a test machine. Subsequently a scheduled scan based on the scanning profile for which the application is marked as unauthorized, is configured to auto–uninstall applications.

GFI LanGuard applications inventory provides a list of all applications detected during past scans. The list is used to specify unauthorized applications. You can also manually add applications to the list. You can do this by specifying the entire name as well as a partial name, specify generic names or part of an application name. GFI LanGuard automatically scans the list of applications and detects partial names. Refer to the following sections for information about:

» Setting an application as unauthorized

» Adding new applications to the unauthorized list

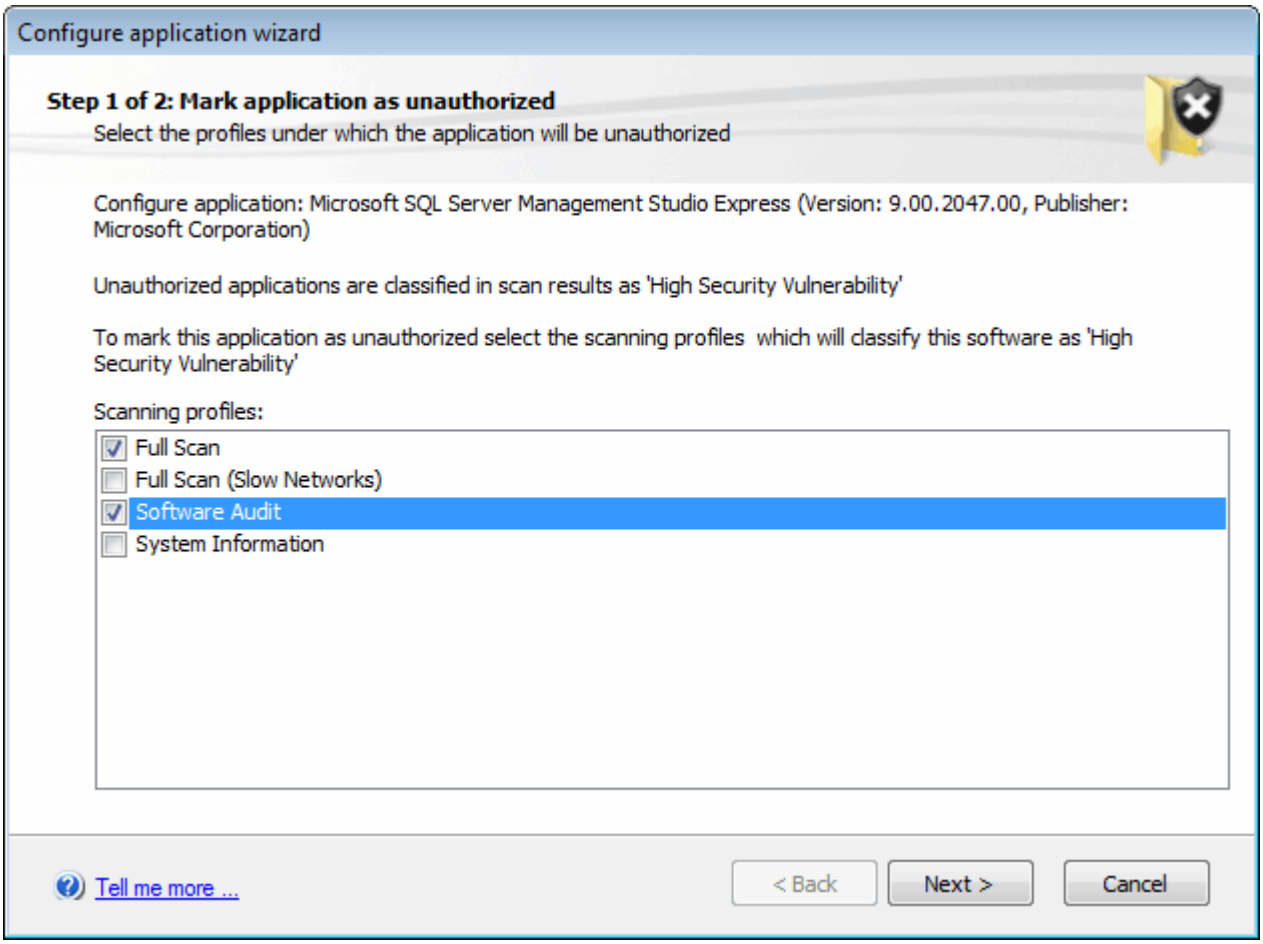
» Validating unauthorized applications for auto-uninstall

» Managing applicable scheduled scans

Setting an application as unauthorized

1. Click on **Configuration** tab > **Applications inventory** sub–node.

2. From the list of applications detected on the right, double click the application to set as unauthorized.



Screenshot 118: Unauthorized application

3. Select the scanning profile for which this application will be set as unauthorized and click **Next**.

4.GFI LanGuard can associate partial names with entries already in the list. As a result, the system will prompt you to confirm whether to apply the same changes also to applications partially have the same name.

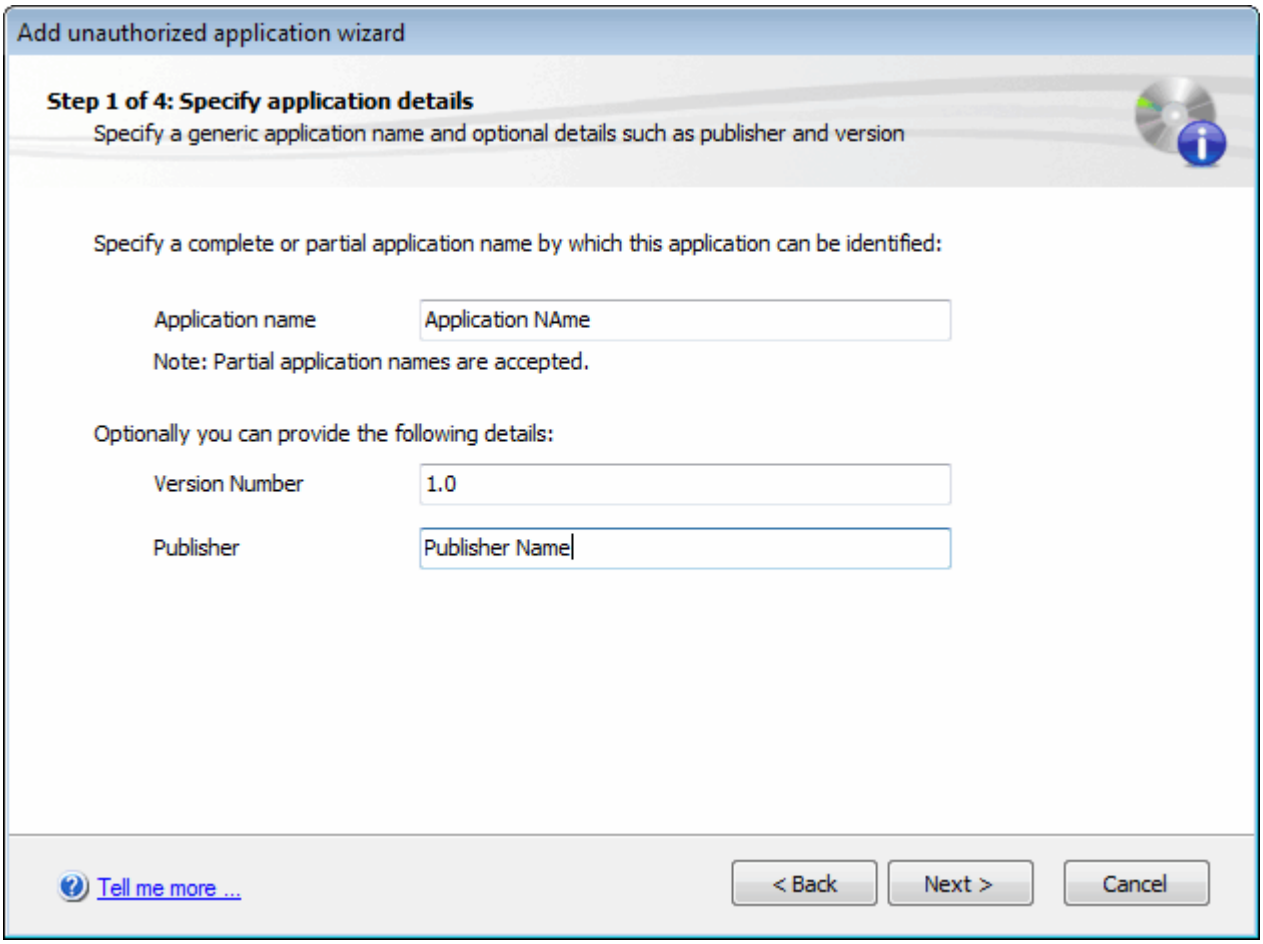
5. Click **Finish** to finalize settings.

Adding new applications to the unauthorized list

1. Click **Configuration** tab > **Applications inventory** sub–node.

2. From **Common Tasks**, click **Add a new application**.

3. In the welcome screen, click **Next**.



Screenshot 119: Applications inventory wizard

4. Specify application name. Optionally provide the version number and publisher name. Click **Next**.

5. Select the scanning profiles that will detect unauthorized applications (Example: Full Scan) and click **Next**.

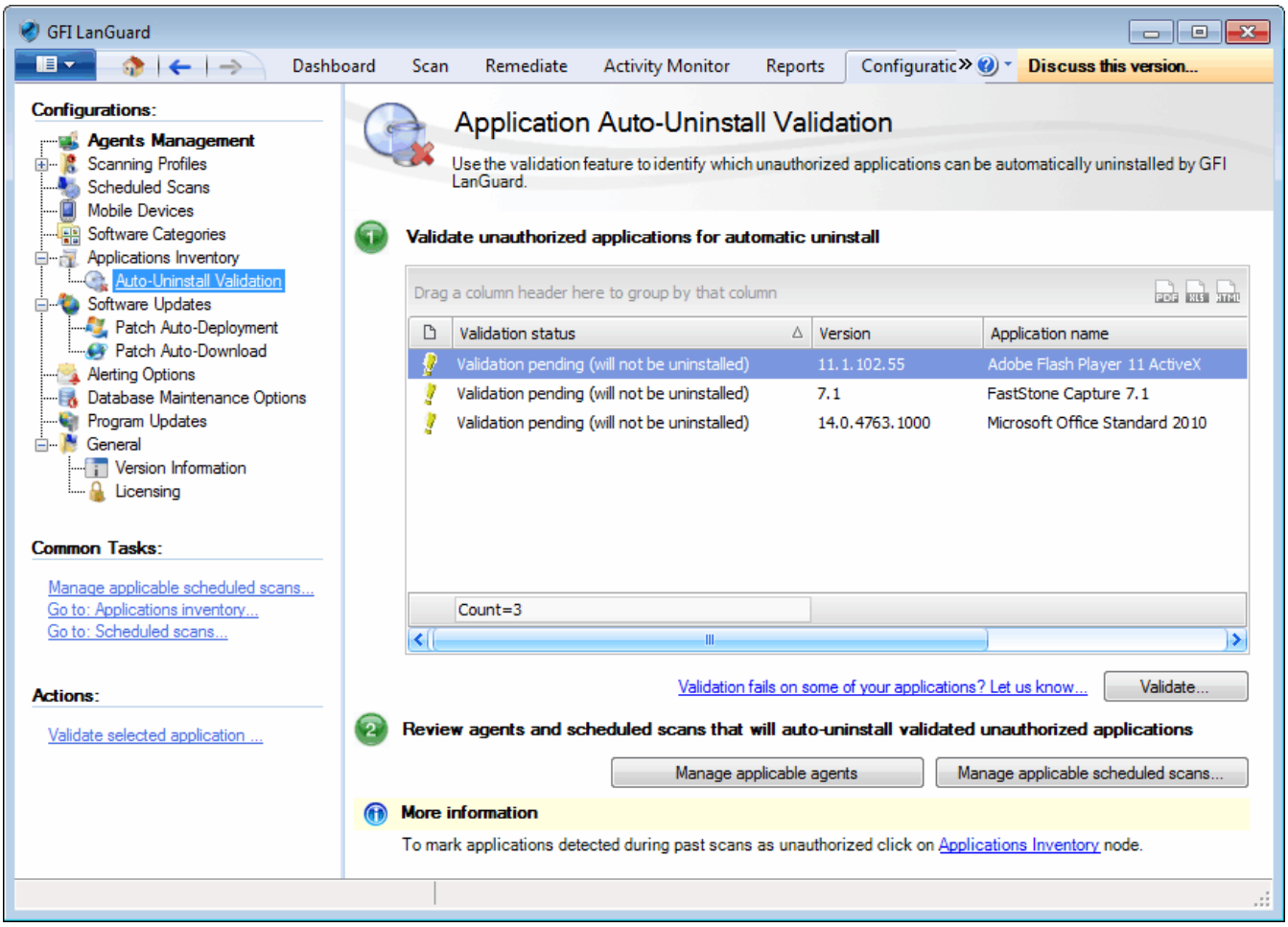
6. Specify whether changes made will effect applications, which have partial/full name match. Click **Next** to continue.

7. Review the information and click **Finish**.

Validating unauthorized applications for auto-uninstall

Application auto–uninstall validation enables you to validate the uninstallation procedure for the applications which are to be automatically uninstalled by GFI LanGuard. This is a requirement prior to the actual uninstallation process and no applications are un–installed during scans unless verified.

1. Click **Configuration** tab **> Applications Inventory > Auto–Uninstall Validation**



Screenshot 120: Application auto–uninstall validation

2. From the right pane, select an application to validate and click **Validate**.

3. In the **Application auto–uninstall validation** wizard, click **Next**.

4. Select the computer where to test the application auto–uninstall and click **Next**.

5. Provide the authentication details for the validation operation and click **Next**.

6. Review the Auto–uninstall validation wizard information and click **Start**.

Managing applicable scheduled scans

The **Manage applicable scheduled scans** button enables you to review or edit scheduled scans, which will perform the validated applications auto install. To manage a scheduled scan:

1. From the **Auto–Uninstall validation** pane, click **Manage applicable scheduled scans**.

2. From, **Manage applicable schedule scans** dialog, click one of the options described below:

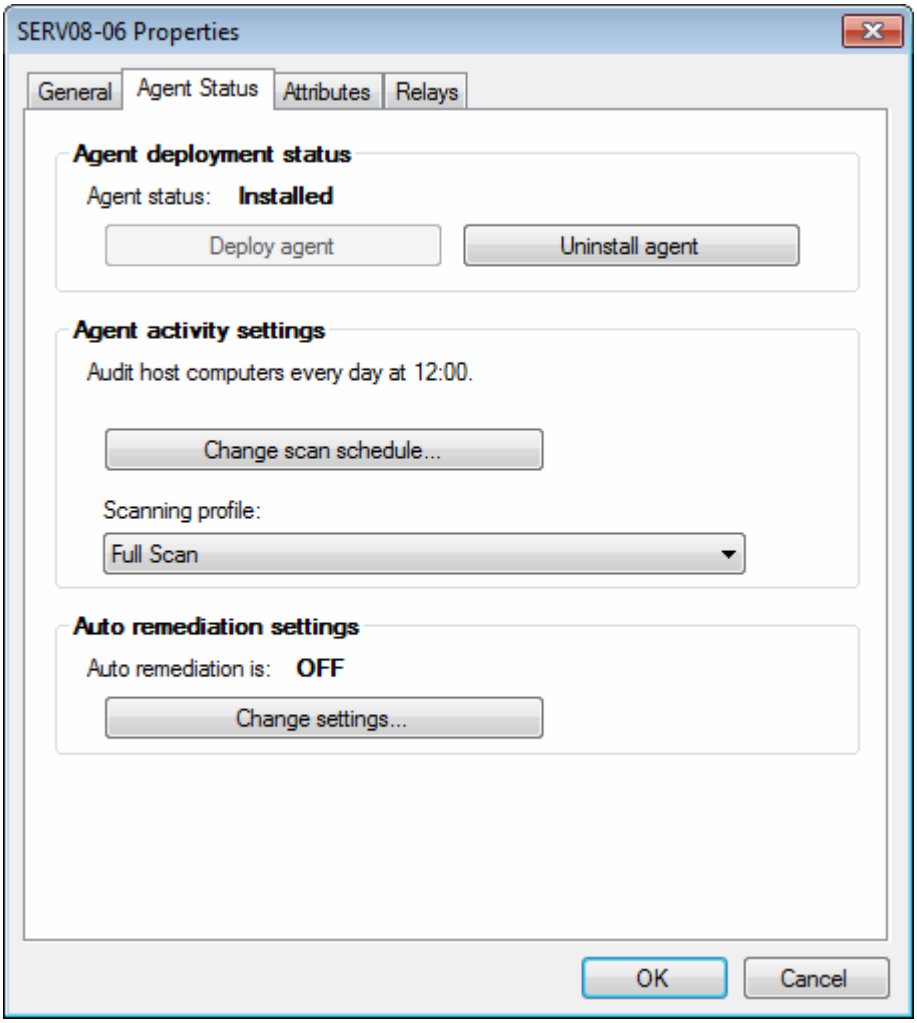
Option	Description
Edit selected scan…	Modify the selected schedule scan. For more information, refer to Editing scheduled scan settings (page 107).
Create a new scheduled scan…	Add a new scheduled scan using the new scheduled scan wizard. For more information, refer to Creating a scheduled scan (page 101).
View all scheduled scans…	Manage scheduled scans. For more information, refer to Editing scheduled scan settings (page 107).

Configuring auto-remediation options

To edit the general deployment options:

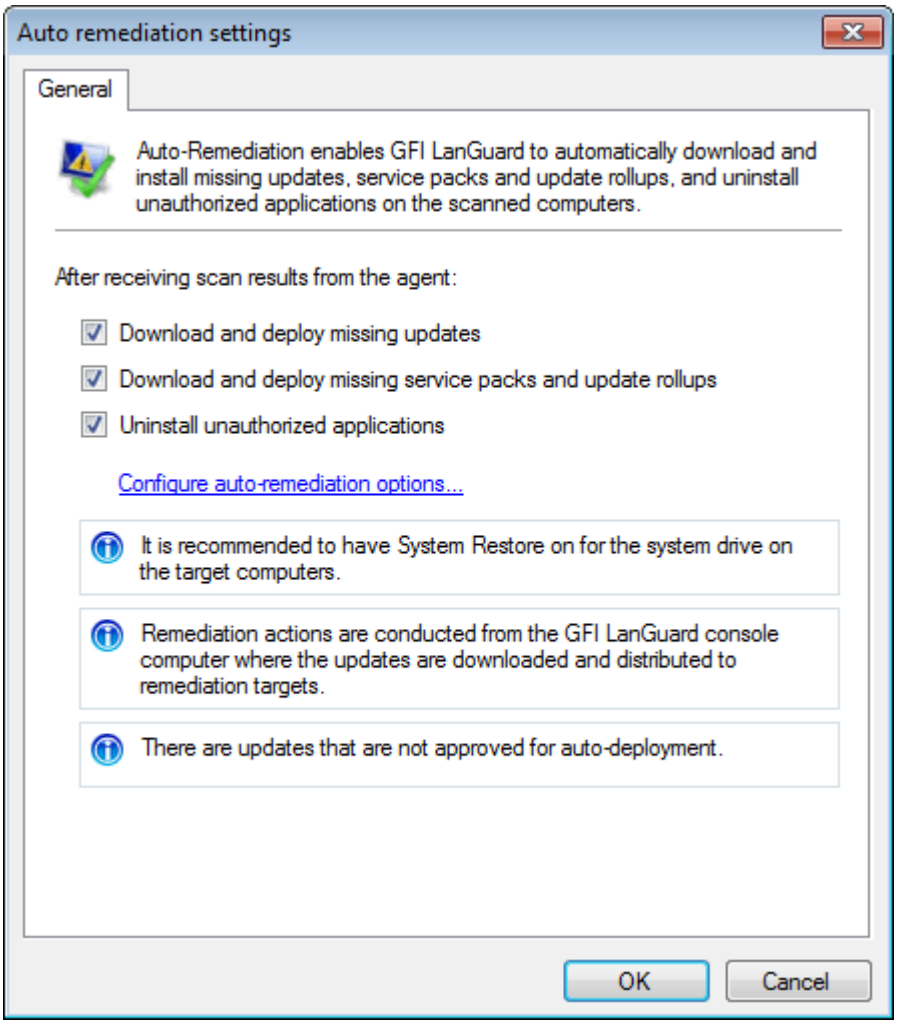
1. Launch GFI LanGuard.

2. From the computer tree, right-click a computer/computer group and select **Properties**.



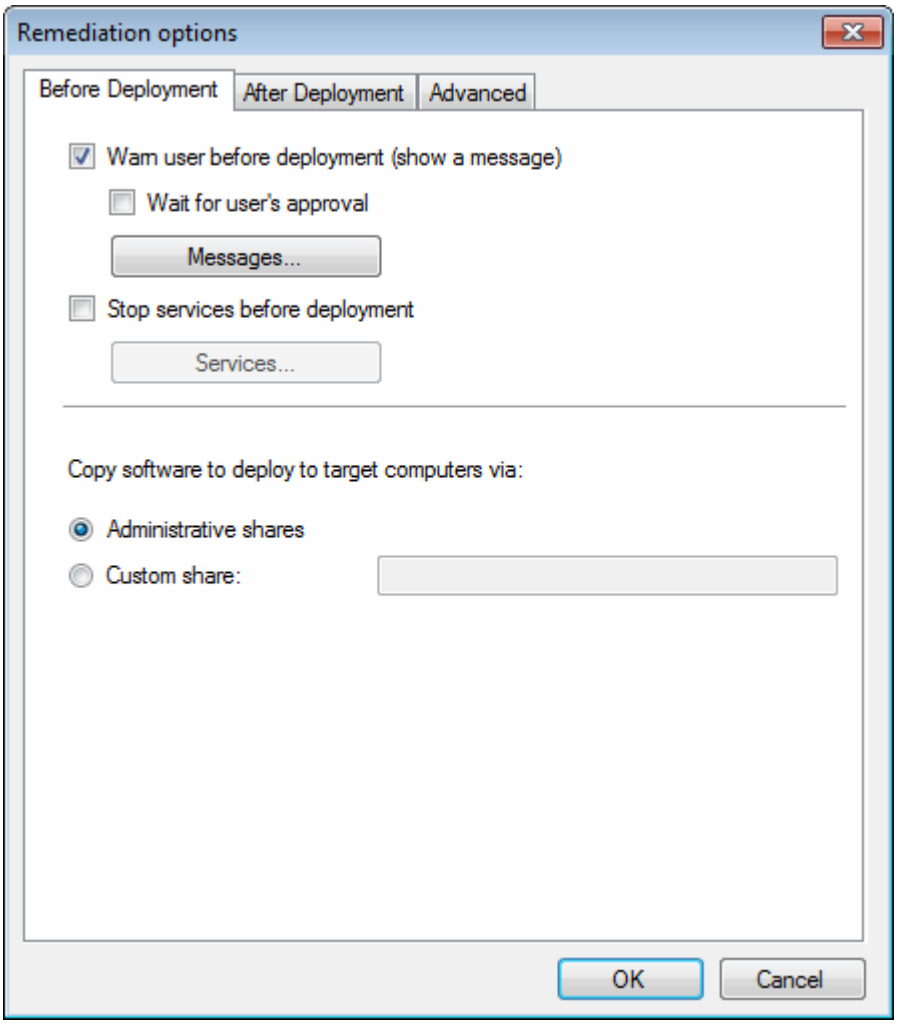
Screenshot 121: Computer properties

3. Select the **Agent Status** tab and from **Auto remediation settings**, click **Change settings...**



Screenshot 122: General auto-remediation settings

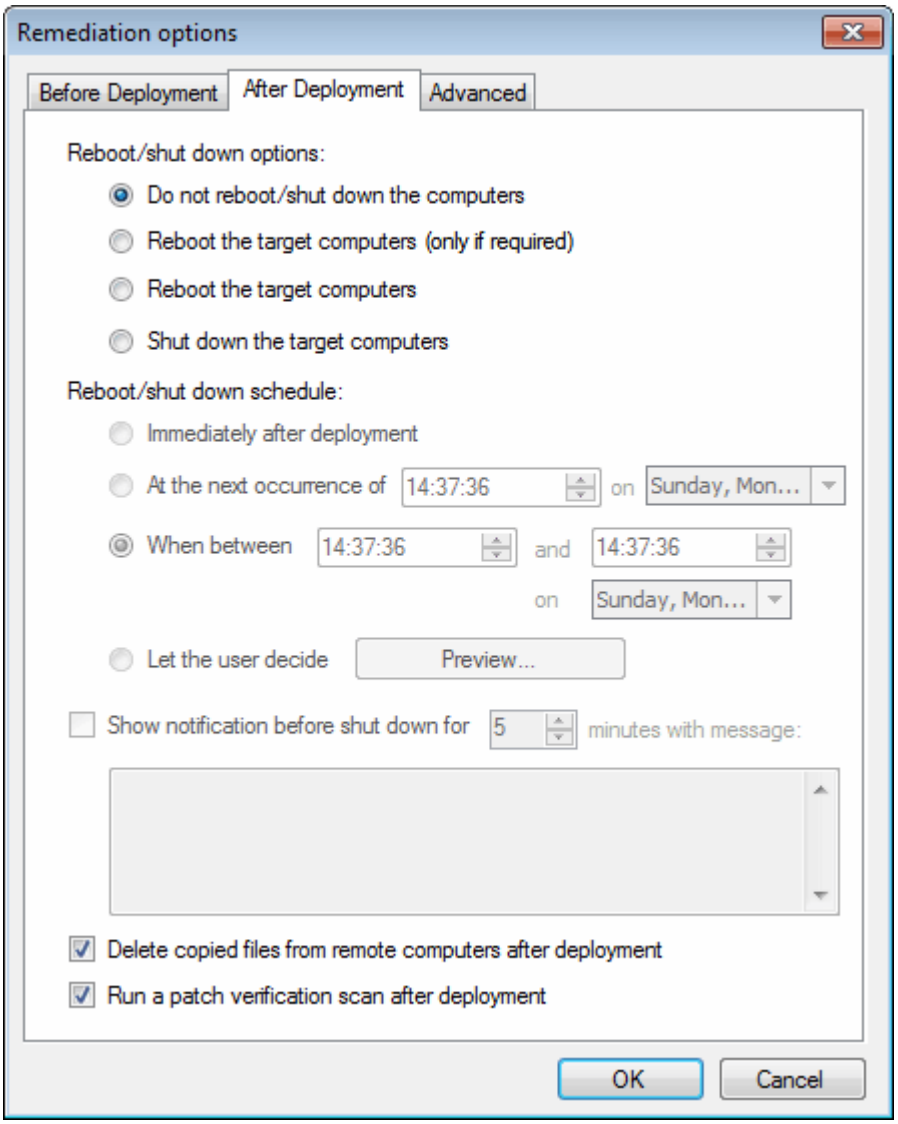
4. Select the action to take after receiving scan results from the agent. Click **Configure auto-remediation options...**



Screenshot 123: Before deployment options

5. Configure **Before Deployment** options described below:

Option	Description
Wake up offline computers	Start computers if they are turned off. For more information, refer to Configuring Wake-on-LAN on scan targets (page 178).
Warn user before deployment (show message)	Displays a message on the target machine to warn the user before deploying software.
Wait for user's approval	Wait for user's approval before deploying software.
Messages	Click **Messages** to select the end-user's computer language and define the warning message. For more information, refer to Configuring auto-remediation messages (page 180).
Administrative shares	Make a copy of the software on the default network shares.
Custom shares	Make a copy of the software in a custom share. Key–in the folder name in the text box.
Remember settings	Saves your configured settings and uses them during the next remediation job.

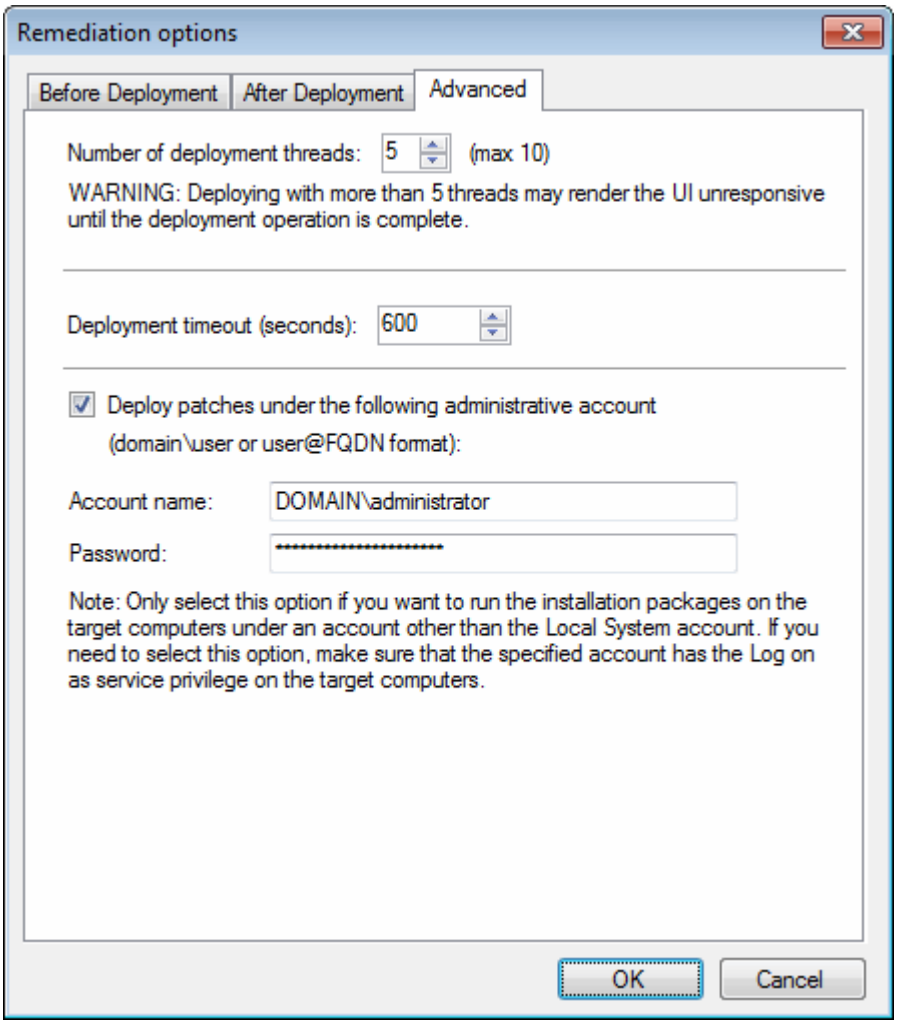


Screenshot 124: After deployment options

6. Click **After Deployment** tab. Configure **After Deployment** options described below:

Option	Description
Do not reboot/shut-down the computer	Leave scan target(s) turned on after remediating vulnerabilities, even if patches require a reboot to be installed completely.
Reboot the target computers only if required	GFI LanGuard reboots a target machine only if at least one patch requires a reboot. If no patches require a reboot, a reboot is not executed.
Reboot the target computers	Always reboots computers after remediating vulnerabilities.
Shut down the target computers	Target machine will shut down after deploying software.
Immediately after deployment	Reboots/shuts down computers immediately after remediating vulnerabilities.

Option	Description
At the next occurrence of	Specify the time when the computers reboot/shut down.
When between	This option enables you to specify time and day values. If the remediation job is completed between the specified times (start time and end time), the computer(s) will reboot/shut down immediately. Otherwise, the reboot/shut down operation is postponed until the next entrance into the specified time interval.
Let the user decide	Click **Preview** to view a screenshot of the dialog in the user manual. This dialog opens on the end-user's computer after remediating vulnerabilities. For more information, refer to Configuring end-user reboot and shut down options (page 179).
Show notification before shut down for	Shows a custom message on the end user's computer for a specified number of minutes before reboot/shut down.
Delete copied files from remote computers after deployment	Deletes the downloaded patches / service packs after they are deployed.
Run a patch verification scan after deployment	Verifies deployed patches, scanning target when the deployment process is complete. **NOTE** » If the user chooses to reboot computer after the deployment, the Patch Verification Scan will occur after the machine was restarted. » If the user chooses to shut down the computer after deployment, the computer will be restarted and the Patch Verification Scan will shut down the computer.
Remember settings	Saves your configured settings and uses them during the next remediation job.



Screenshot 125: Advanced deployment options

7. (Optional) Select **Advanced** tab. Configure the options described below:

Option	Description
Number of deployment threads	Specify the maximum number of processing threads allowed to start when deploying software updates. The number of threads determines the number of concurrent deployment operations an agent can handle.
Deployment timeout (seconds)	Specify the time (in seconds) an agent attempts to deploy an update. If the specified time is exceeded, the agent stops the unresponsive deployment and starts a new deployment thread. This feature enables you to stop the process thread so that if an update is taking longer than normal deployment time, the remediation operation continues without jeopardizing the rest.
Deploy patches under the following administrative account	Select this option to use a custom administrative account to log and deploy patches on target machines. The account selected must have Log–on as service privilege on the target computers. For more information on how to configure an account with log–on as service privilege, refer to http://go.gfi.com/?pageid=LAN_LogonService.

8. Click **OK** to apply changes.

Configuring Wake-on-LAN on scan targets

Wake-on-LAN enables GFI LanGuard to wake machines from the following states:

- Powered off
- Sleep
- Hibernated

> **IMPORTANT**
> If you have routers between the client machine and the GFI LanGuard machine, the router and the GFI LanGuard machine must be configured to allow Wake-on-LAN broadcast packets on UDP port 9.

The motherboard and the network interface card of the computer running GFI LanGuard, must support Wake-on-LAN. To configure Wake-on-LAN on a Windows® operating system:

1. Click **Start**, right click **Computer** and select **Manage**.
2. From the left panel, expand **System Tools** and click **Device Manager**.
3. Right click the **Network Interface Card** and select **Properties**.
4. From the **Power Management** tab, select the following options:
   - **Allow this device to wake up the computer**
   - **Only allow a magic packet to wake the computer**

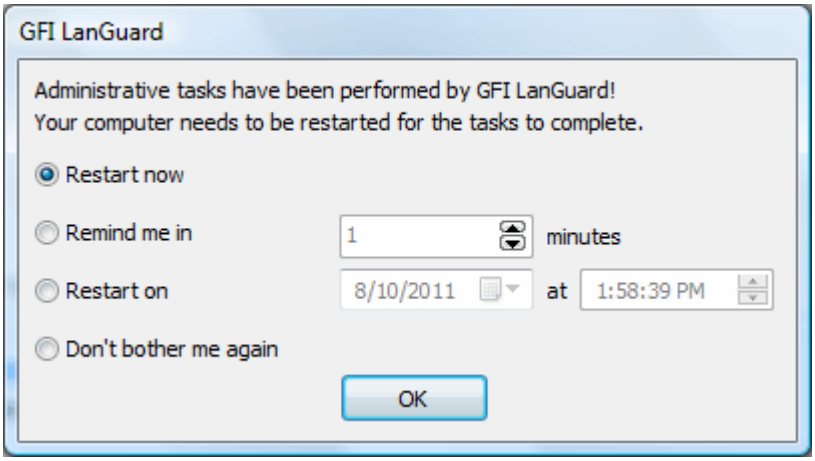
> **Note**
> **Magic Packet** is the wake up signal that is sent by GFI LanGuard to the scan target network card.

5. Click **OK**

Once the **Network Interface Card** is configured, run a **FULL** scan on the client machine. This enables GFI LanGuard to gather the required information from the client machine. For more information, refer to Manual scans (page 96).

Configuring end-user reboot and shut down options

When configuring **After Deployment** settings, in **Auto-remediation options**, you can configure GFI LanGuard to notify and let the user decide when to reboot or shut down the computer after completing an administrative task. The below dialog opens on the user's computer and enables him/her to select one of the following options:



Screenshot 126: Reboot/shut down options

The table below describes the available options:

Option	Description
Restart now	Reboots/shuts down the computer immediately after completing an administrative task.
Remind me in	Specify a time interval (in minutes), when to remind the end-user.
Restart on	Specify the date and time when the machine reboots/shuts down.
Don't bother me again	The user is not prompted again.

Configuring auto-remediation messages

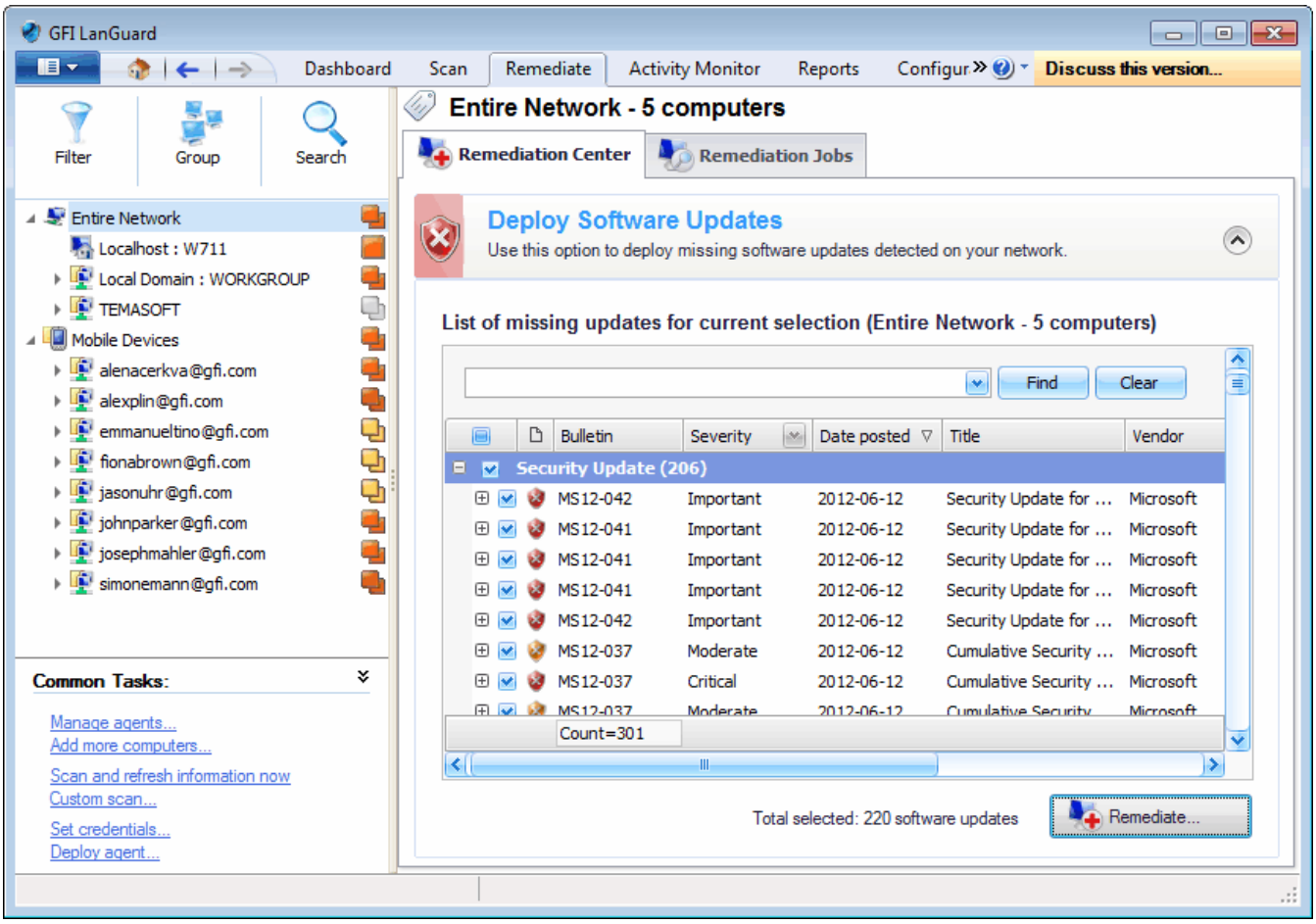
GFI LanGuard enables you to automatically display warning messages before and after remediation operations. These messages are displayed on the end-users' computer and in some cases, allows them to select after deployment options, or notify them about the operations to be carried out. You can customize predefined messages and set the language according to the scan target's computer language.

To configure warning messages:

1. Launch GFI LanGuard.

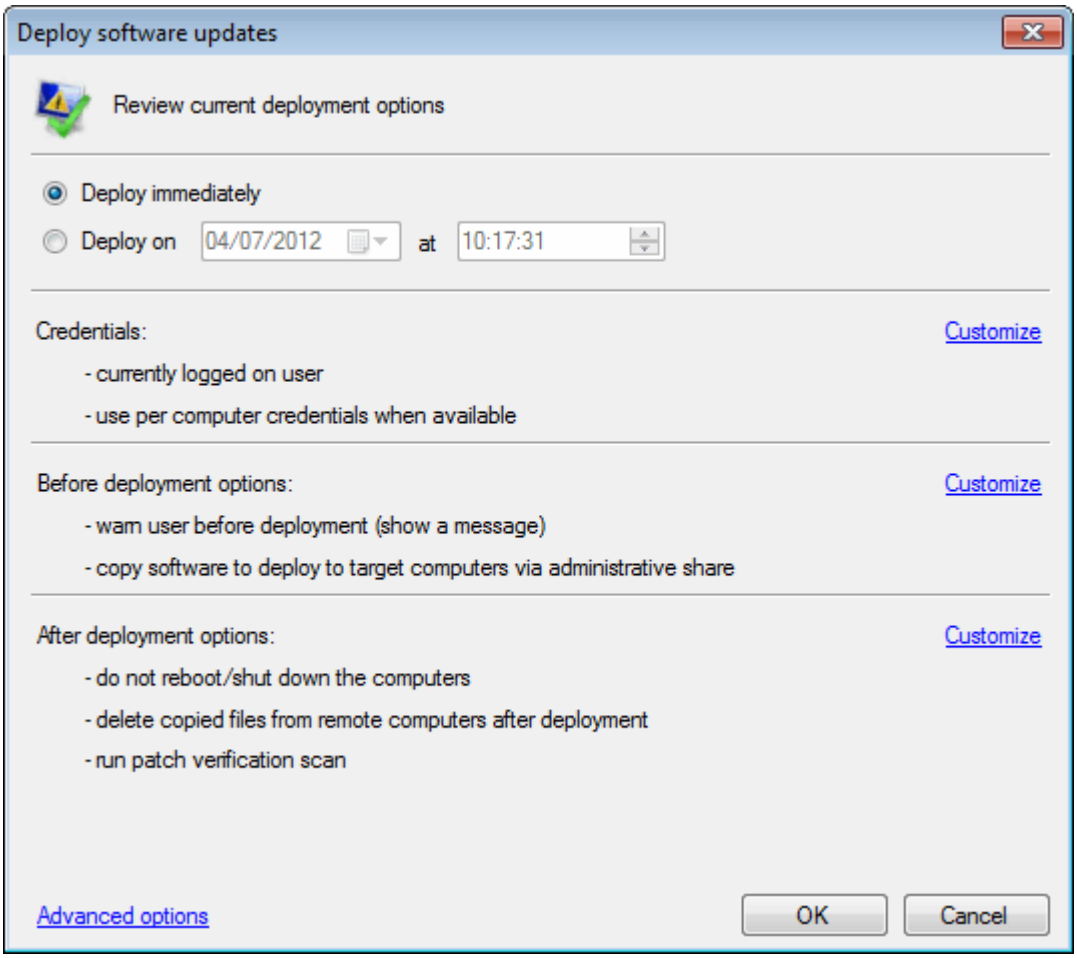
2. Click **Remediate tab > Remediation Center**.

3. From **Remediation Center**, select a remediation action, such as **Deploy Software Updates**.



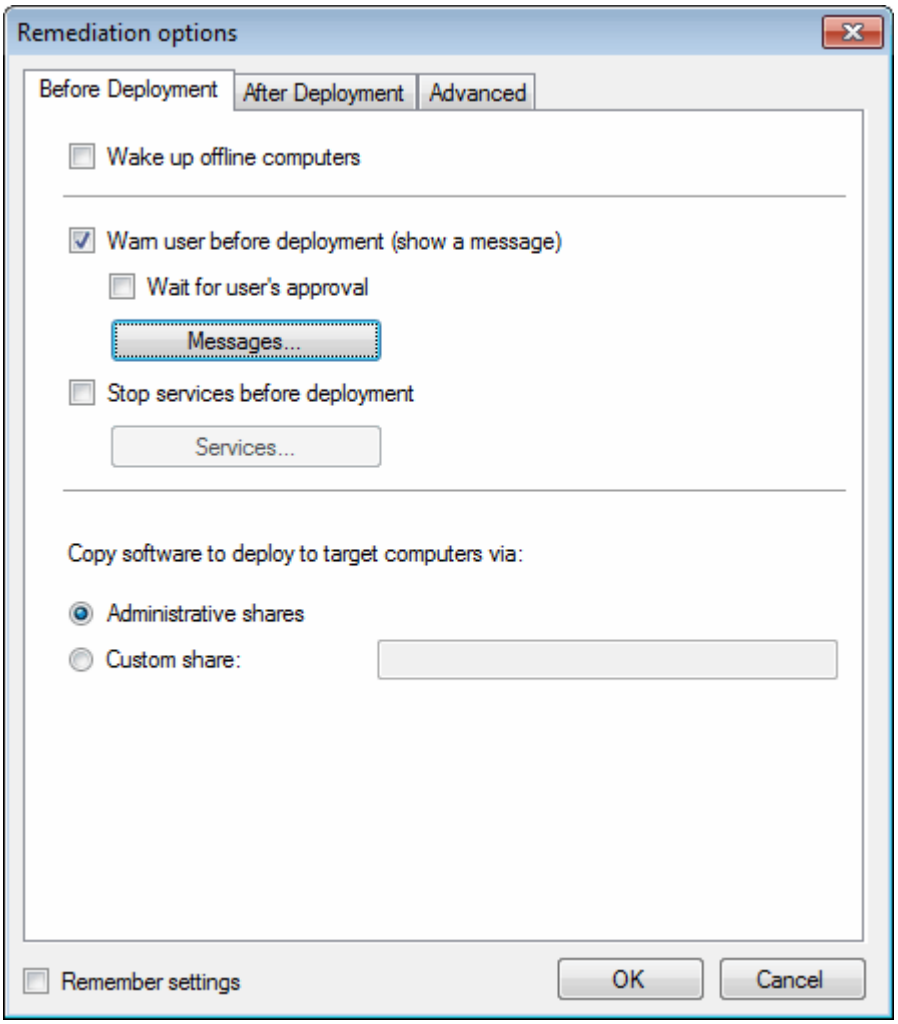
Screenshot 127: Remediation Center - Deploy Software Updates

4. Click **Remediate**.



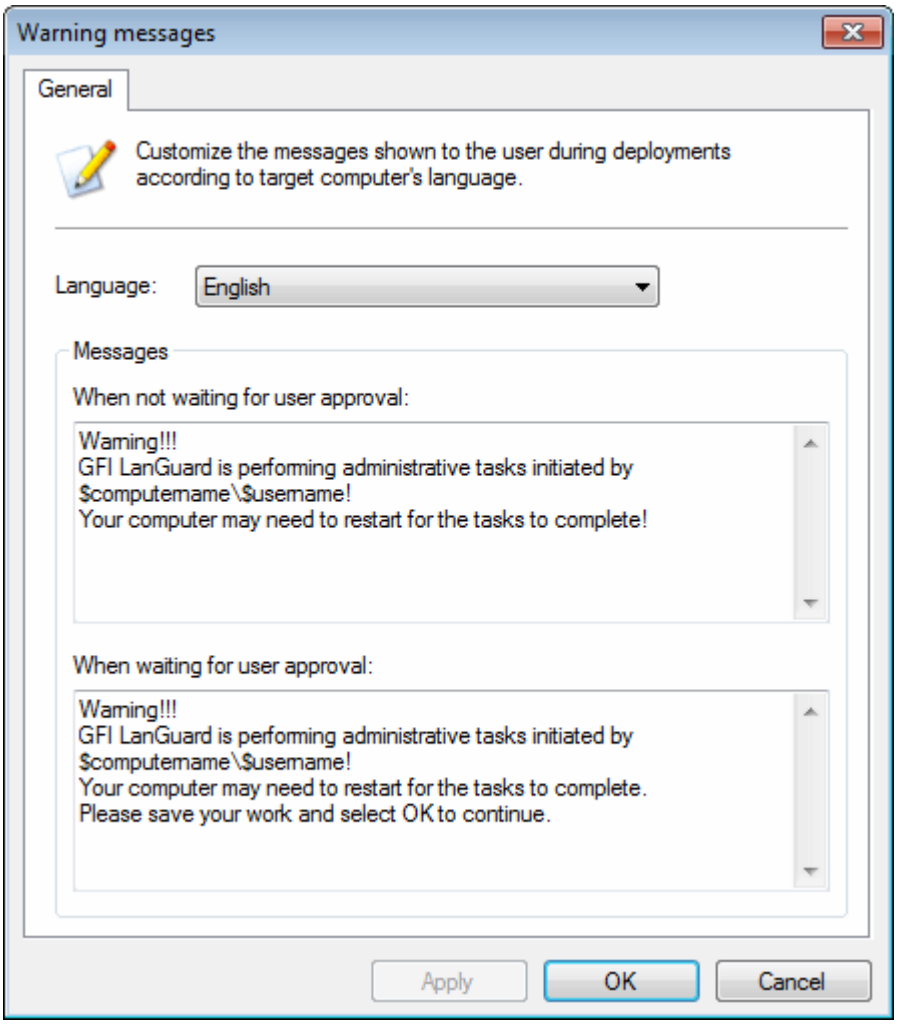
Screenshot 128: Deployment options dialog

5. Click **Advanced options**.



Screenshot 129: Before Deployment Message options

6. From the **Remediation options** dialog, click **Before Deployment tab > Messages...**.



Screenshot 130: Customizing warning messages

7. Customize any of the following options:

Option	Description
Language	Select the message language.
When not waiting for user approval	Use or customize the pre-defined message that launches on the end user's computer when GFI LanGuard is not waiting for approval.
When waiting for user approval	Use or customize the pre-defined message that launches on the end user's computer when GFI LanGuard is waiting for approval.

8. Click **Apply** and **OK**

Configuring Agent auto-remediation

In an agent–based environment, automatic remediation options can be set for every deployed agent. This enables you to configure every agent with specific auto–remediation options to suit your requirements.

To configure agent auto-remediation actions:

1. Launch GFI LanGuard.

2. Click **Configuration** tab **> Agents Management**.

3. From the right pane, right–click an agent and select **Properties**.

4. Select the **Agent Status** tab and in the **Auto remediation settings** section click **Change Settings**.

5. Select **Download and deploy missing updates** to enable automatic remediation for missing patches.

6. Select **Download and deploy missing service packs and update rollups** to enable automatic remediation for missing service packs.

7. Select **Uninstall unauthorized applications** to enable automatic remediation for unauthorized applications.

8. (Optional) Click **Configure auto–remediation options…** to further customize remediation options. For more information, refer to Configuring auto-remediation options (page 173).

9. Click **OK**

4.5.2 Manual Remediation

Apart from automatically downloading patches and service packs, GFI LanGuard can also deploy these updates network–wide as well as recall any patches that were deployed.

Both patch deployment and patch rollback operations are managed by an agent service that manages all file transfers between GFI LanGuard and remote targets. This service is installed automatically on the remote target computer during the patch deployment process.

Manual Remediation tasks:

- Review Manual Remediation important notes
- Learn more about the Remediation Center
- Deploy Software Updates
- Uninstall Software Updates
- Deploy custom software
- Uninstall Applications
- Be protected against Malware
- Connect remotely to a machine using GFI LanGuard.
- Sending Mobile Device Notifications

Manual remediation notes

1. While an infrequent occurrence, patches may be recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates such as conflict issues with present software or hardware. Examples of updates recalled by the manufacturer include patches MS03–045 and MS03–047 for Exchange that were released by Microsoft® on October 15, 2006.

2. Ensure that the NetBIOS service is enabled on the remote target computer. For more information, refer to Configuring NetBIOS (page 299).

3. A complete list of Microsoft products for which GFI LanGuard can download and deploy patches is available at http://go.gfi.com/?pageid=ms_app_fullreport

4. Non–Microsoft software update patches supported by GFI LanGuard is available at http://go.gfi.com/?pageid=3p_fullreport

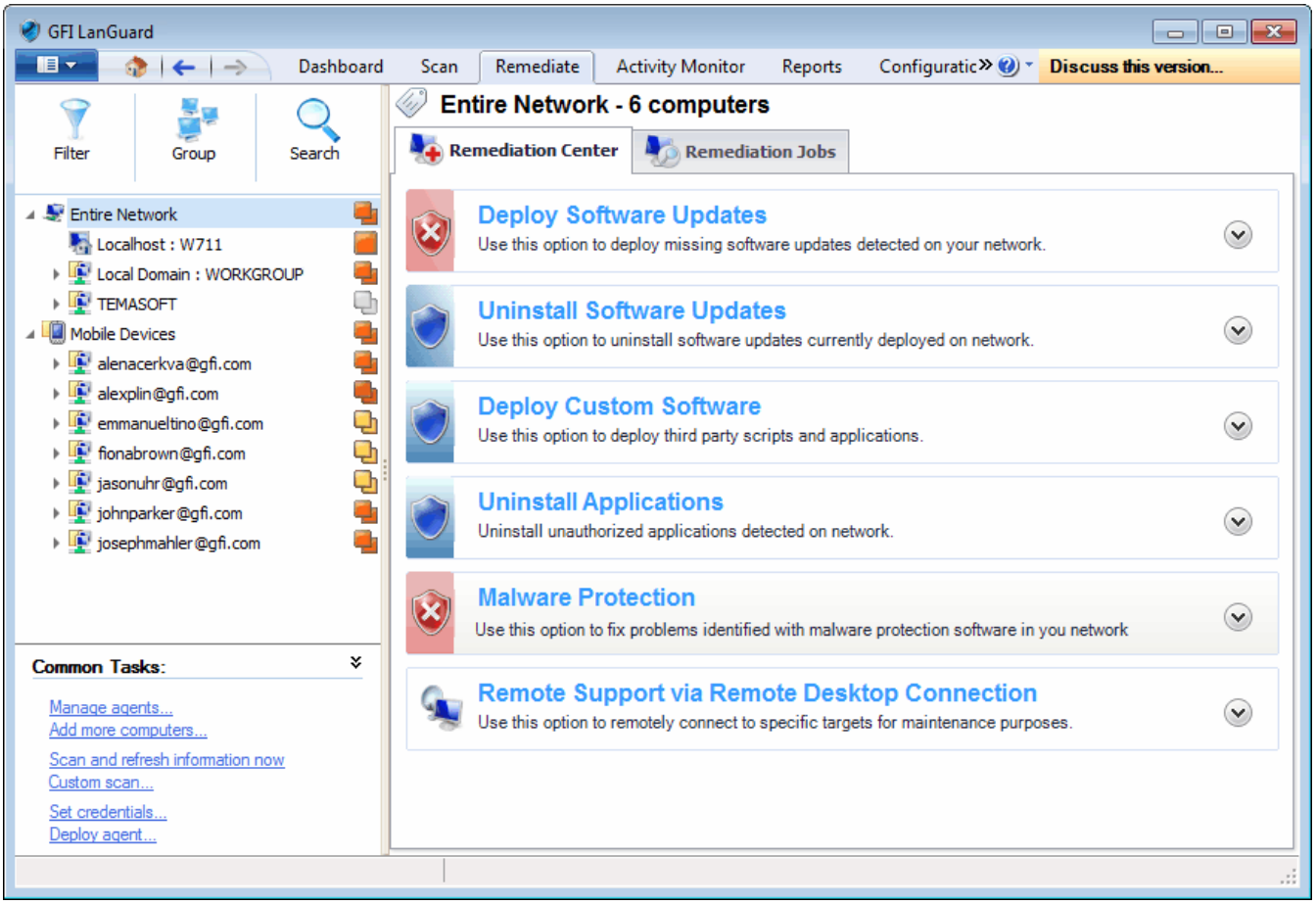
5. The complete patch management process, from detection to remediation, is supported for most of the non-Microsoft products. There is, however a small set of products that GFI LanGuard cannot update and which GFI LanGuard functionality is limited to detecting missing updates. Examples of these products are

- Apache Webserver
- MySQL
- VMware Player and Workstation

6. GFI LanGuard can be set to automatically download missing patches and service packs discovered during a network security scan. For more information, refer to Configuring missing updates auto-deployment (page 163).

Using the Remediation Center

The **Remediation Center** enables you to fix security issues found during a network scan by deploying or uninstalling applications from target machines. To access the **Remediation Center**, select **Remediate** tab > **Remediation Center**.



Screenshot 131: Remediation center

From the left panel, expand and locate a computer or a domain to perform remediation actions. The available remediation actions are described below:

Action	Description
Deploy Software Updates	Deploy missing patches discovered when auditing target computers. For more information, refer to Deploying Software Updates (page 187).
Uninstall Software Updates	Uninstall service packs from target computers. For more information, refer to Uninstalling Software Updates (page 189).
Deploy Custom Software	Deploy custom applications and scripts on target computers. For more information, refer to Deploying Custom Software (page 191).
Uninstall Applications	Uninstall applications from target computers. For more information, refer to Uninstalling Custom Applications (page 192).
Malware Protection	Perform Malware protection actions on target computers. For more information, refer to Malware Protection (page 194).
Remote Support via Remote Desktop Connection	Connect to a target machine and perform administrative tasks using remote desktop connection. For more information, refer to Using Remote Desktop Support (page 196).

Deploying Software Updates

Use the **Deploy Software Updates** feature to manually deploy:

- Missing Service Packs and Update Rollups
- Missing Security Updates
- Missing Non-Security Updates.

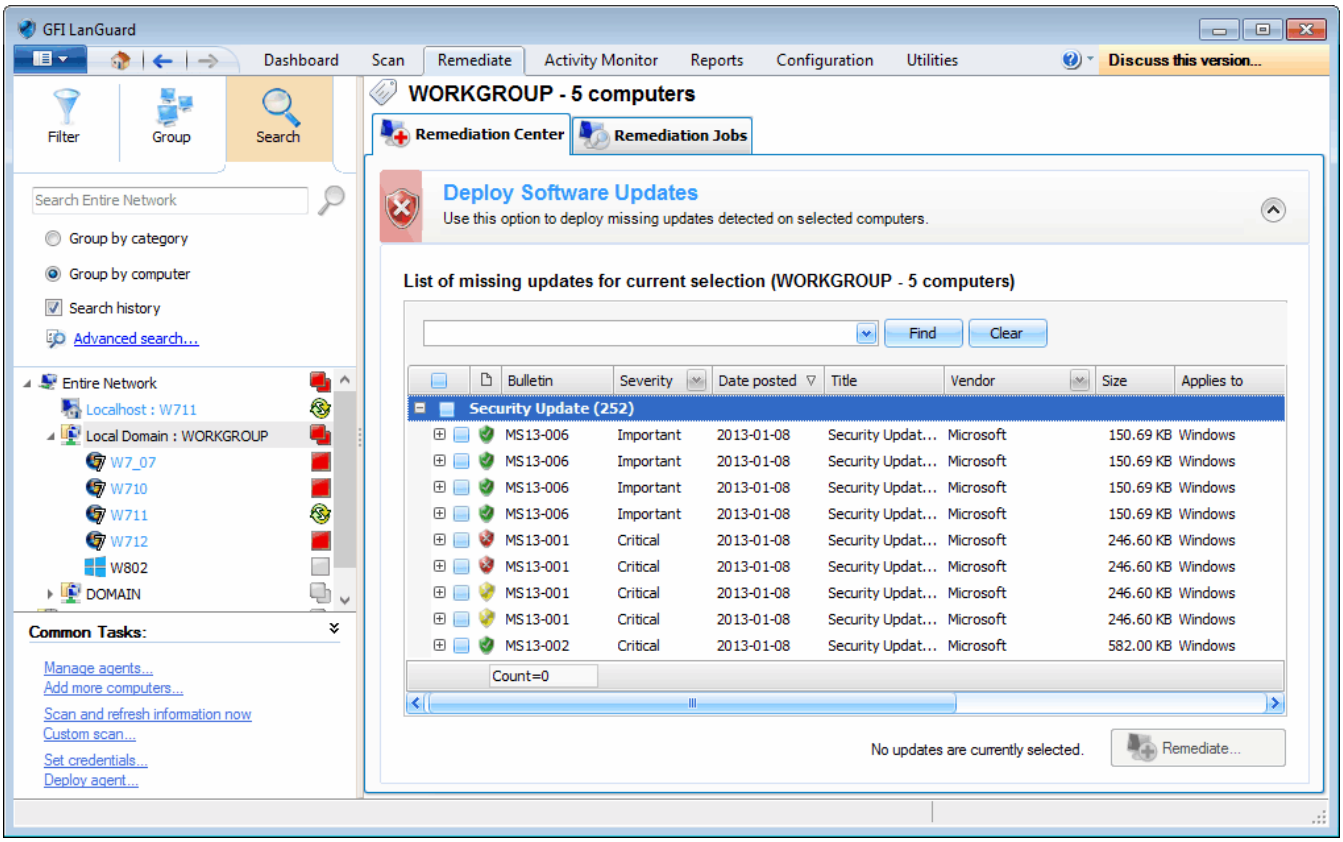
This feature enables you to specifically select the items you want to deploy and provides you with a detailed description for each.

> **NOTE**
> To view additional information about an update, right-click on an update and select **More details > Bulletin info...**

To manually deploy software updates:

1. Launch GFI LanGuard.

2. Click **Remediate** tab and expand **Deploy Software Updates**.



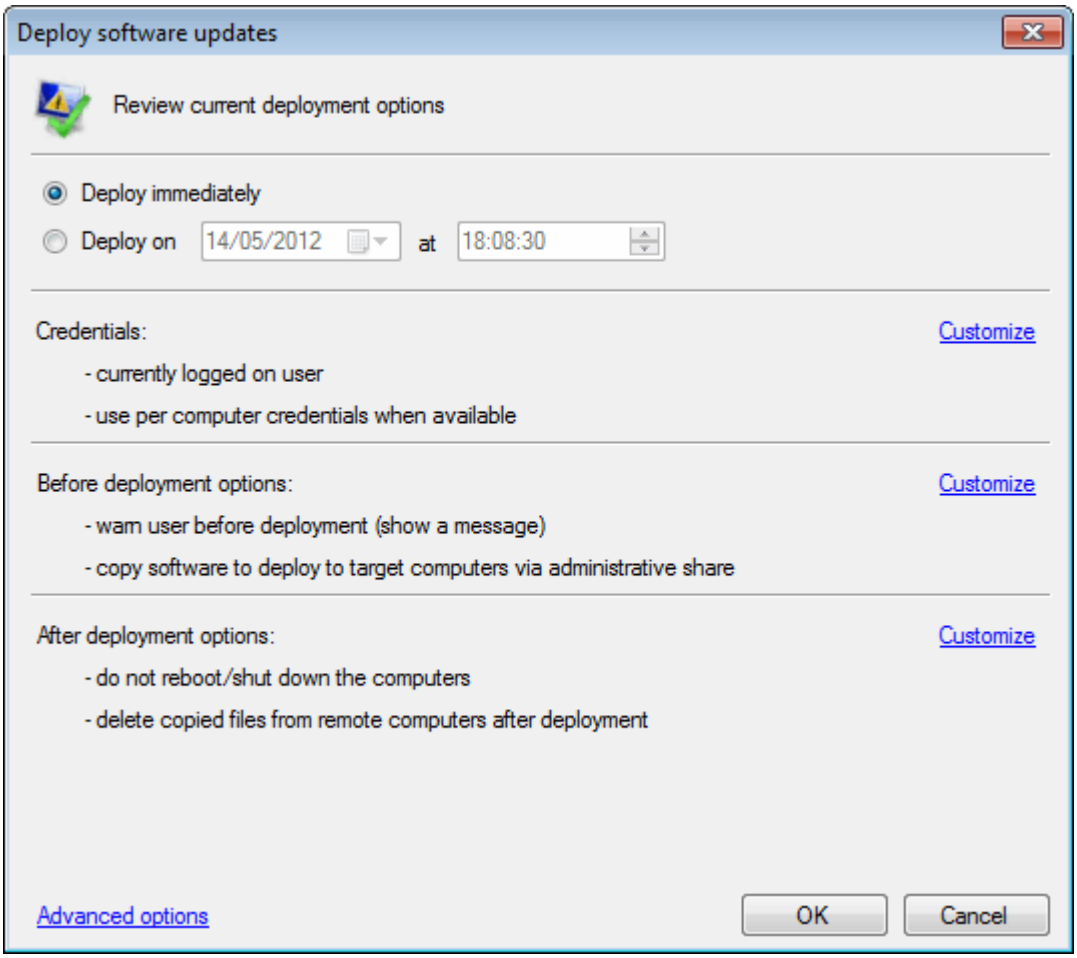
Screenshot 132: Deploying software updates

3. From the computer tree, select the computer/group where to deploy software updates.

4. From the **List of missing updates**, select the updates to deploy.

> **NOTE**
> Use the search bar to look for specific missing updates or use the filtering options for each column heading to view the required data only.

5. Click **Remediate**.



Screenshot 133: Deploy software updates options

6. The **Deploy software updates** dialog, enables you to edit deployment options before starting the deployment operation. Review the options described below:

Option	Description
Deploy immediately	Selected by default. Leave selected to deploy missing updates immediately.
Deploy on	Specify a date and time when to deploy missing updates .
Credentials	Provides you with the credentials settings for updates. Click **Customize** to change settings .
Before deployment options	Provides you with the actions taken before deploying software updates. Click **Customize** to edit the before deployment message, and the type of share created to transfer updates and scan details files.
After deployment options	Provides you with the actions taken after deploying missing software updates. Click **Customize** to configure whether the computer(s) reboot, shutdown or display a message to the end-user.
Advanced options	Click **Advanced options** to configure the: » Number of deployment threads. Maximum = 10 » Deployment timeout » Alternate credentials. Select **Remember settings** to reuse the same configuration when running the next deployment job. For more information, refer to Configuring auto-remediation options (page 173).

7. Click **OK** to start deploying updates. You are automatically taken to the **Remediation Jobs** tab where you can monitor the progress of the deployment operation.

Uninstalling Software Updates

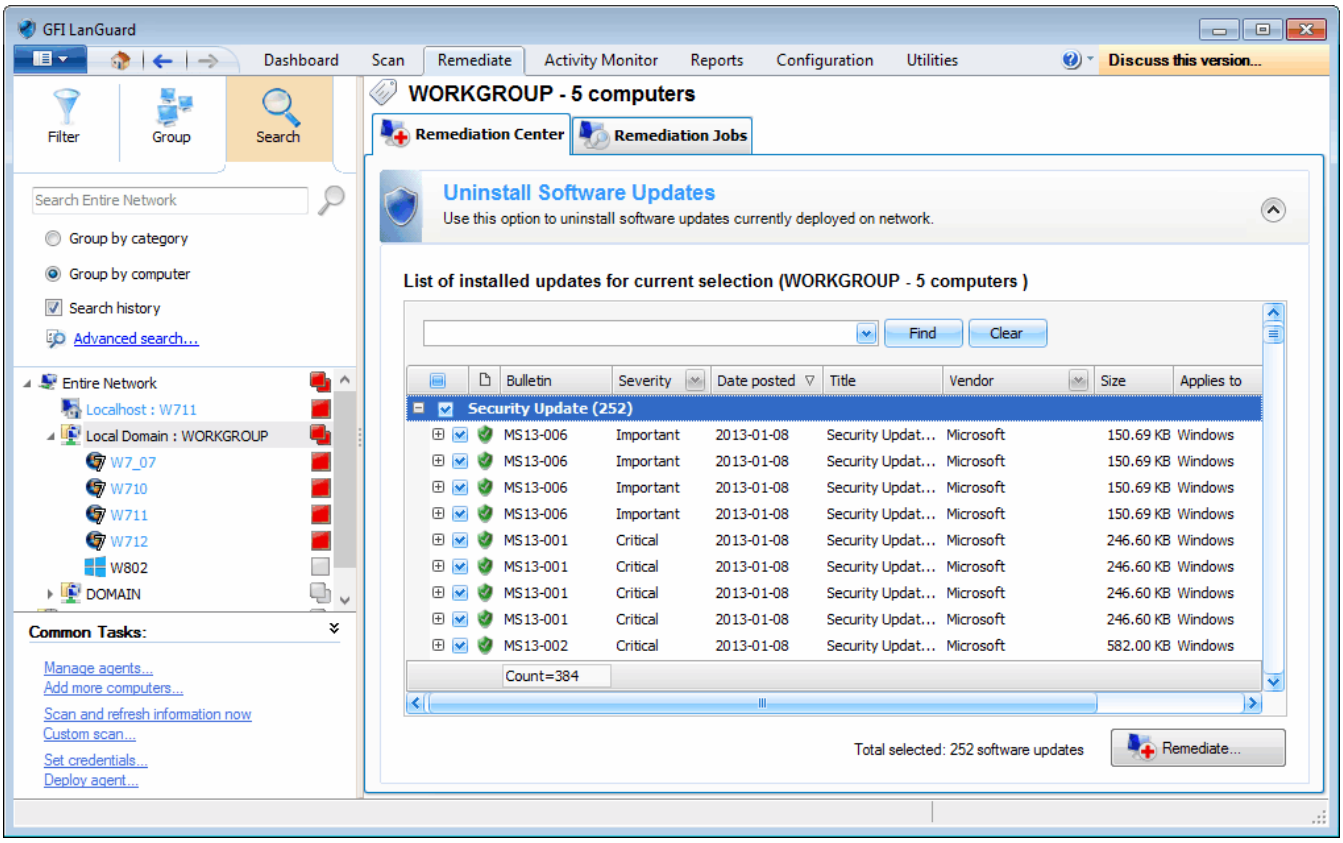
The **Uninstall Software Updates** feature enables you to manually remove:

- Installed Service Packs and Update Rollups
- Installed Security Updates
- Installed Non-Security Updates.

To manually uninstall software updates:

1. Launch GFI LanGuard.

2. Click **Remediate** tab and expand **Uninstall Software Updates**.



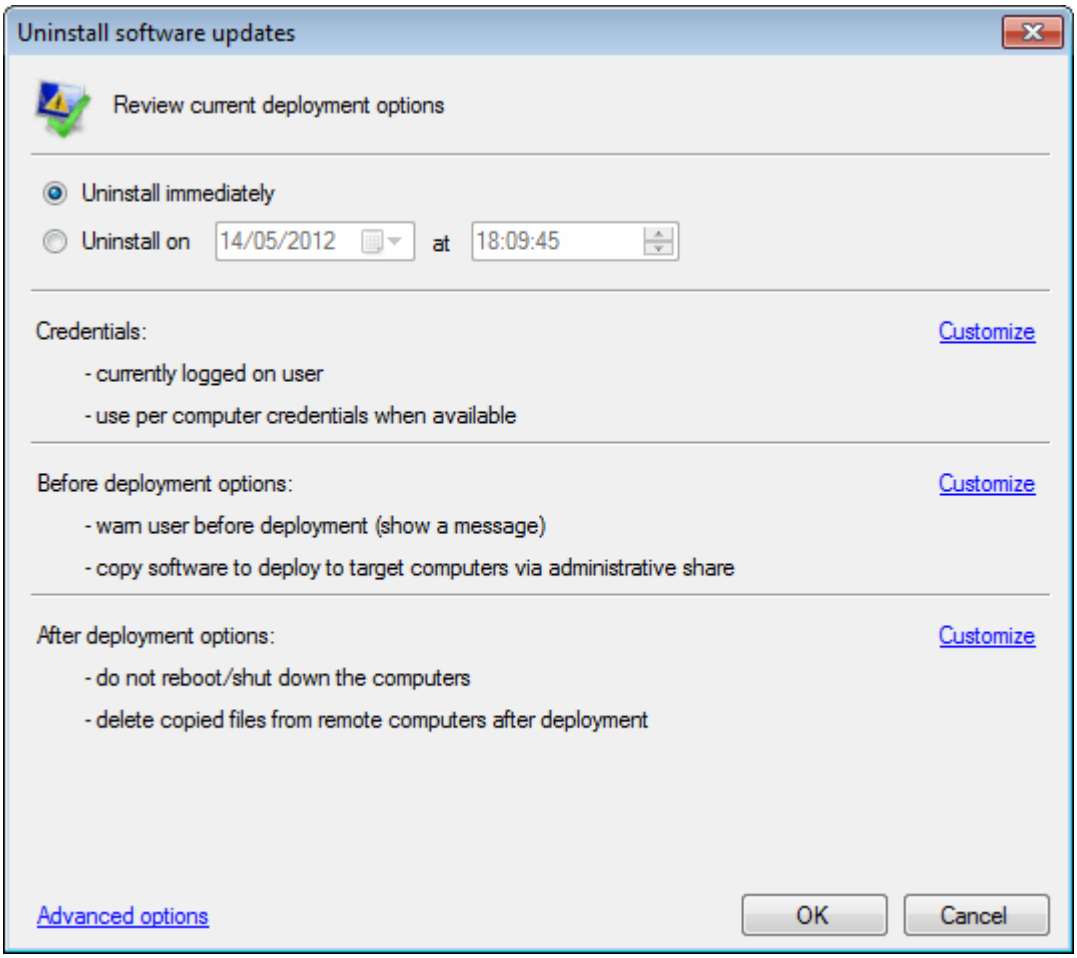
Screenshot 134: Uninstalling software updates

3. From the computer tree, select the computer/group where to uninstall software updates.

4. From the **List of installed updates**, select the updates you want to uninstall.

> **NOTE**
> Use the search bar to look for specific installed updates or use the filtering options for each column heading to view the required data only.

5. Click **Remediate**.



Screenshot 135: Uninstall software updates options

6. The **Uninstall software updates** dialog, enables you to edit uninstall options before starting the uninstall operation. Review the options described below:

Option	Description
Uninstall immediately	Selected by default. Leave selected if you want to uninstall updates immediately.
uninstall on	Specify a date and time for when updates are uninstalled.
Credentials	Provides you with the credentials settings that are used to uninstall updates. Click **Customize** to change settings and use alternate credentials.
Before deployment options	Provides you with the actions taken before uninstalling software updates. Click **Customize** to edit the before deployment message, and shares mode used to transfer updates.
After deployment options	Provides you with the actions taken after uninstalling software updates. Click **Customize** to configure whether the computer(s) reboot, shutdown or display a message to the end-user.
Advanced options	Click **Advanced options** to configure the: » Number of deployment threads. Maximum = 10 » Deployment timeout » Alternate credentials. Select **Remember settings** to reuse them when running the next deployment operation. For more information, refer to Configuring auto-remediation options (page 173).

7. Click **OK** to start uninstalling the selected updates. You are automatically taken to the **Remediation Jobs** tab where you can monitor the progress of the uninstall operation.

Deploying Custom Software

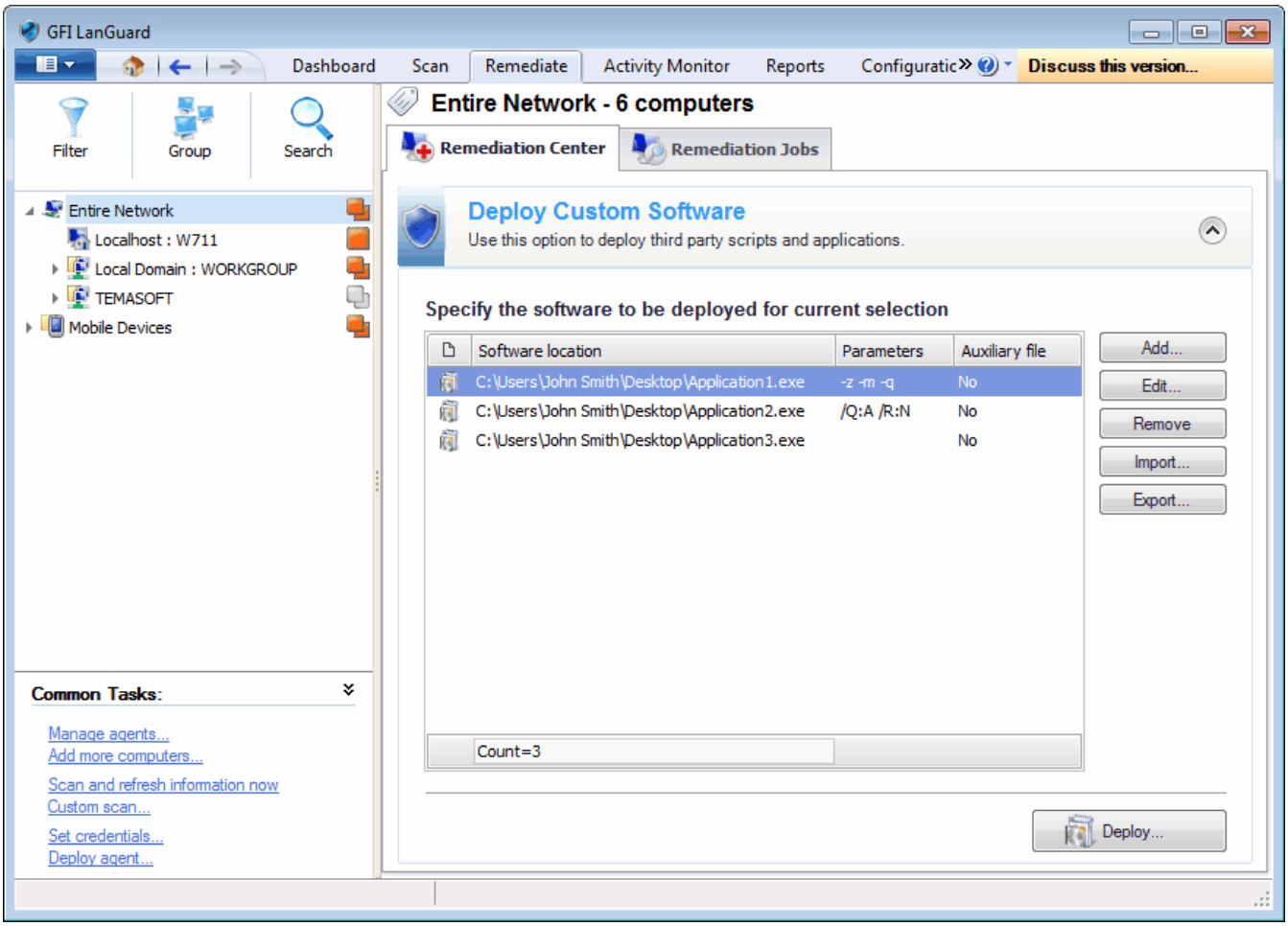
Apart from security updates and patches, GFI LanGuard also enables you to remotely deploy third party or custom software network–wide. Software that can be remotely deployed includes:

- Security applications such as antivirus/antispyware solutions and software firewalls
- Third party software updates and patches such as antivirus/antispyware signature file updates
- Custom code such as scripts and batch–files
- Desktop applications such as Microsoft® Office 2007 and more.

To specify which software to deploy:

1. Click on **Remediate** tab **> Remediation Center**.

2. From the computer tree, select the computers where the new software will be deployed and click **Deploy Custom Software**.



Screenshot 136: List of software to be deployed

3. Use the options described in below to add the applications to deploy:

Option	Description
Add	Click this button to launch the Add custom software dialog. This dialog enables you to add an application to the list and if required configure parameters.

Option	Description
Edit	Select an application and click this button to launch the Add custom software dialog. This dialog enables you to modify the existing installation parameters.
Remove	Select an application from the list and click this button to remove the application.
Import	Click this button to import the applications parameters from an XML file.
Export	Click this button to export the applications parameters to XML file.

4. Click **Deploy** and configure the options described below:

Option	Description
Deploy immediately	Deploy the selected applications immediately.
Deploy on	Deploy the selected applications on a specific date and time. Configure when to deploy the applications.
Credentials	Select the authentication method to use or specify a username and password. Select **Use per computer credentials when available**, to use the credentials specified in the computer properties. For more information, refer to Agent properties (page 77).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 173).
After deployment options	Configure the actions to perform after deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 173).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to Configuring auto-remediation options (page 173).

5. Click **OK**

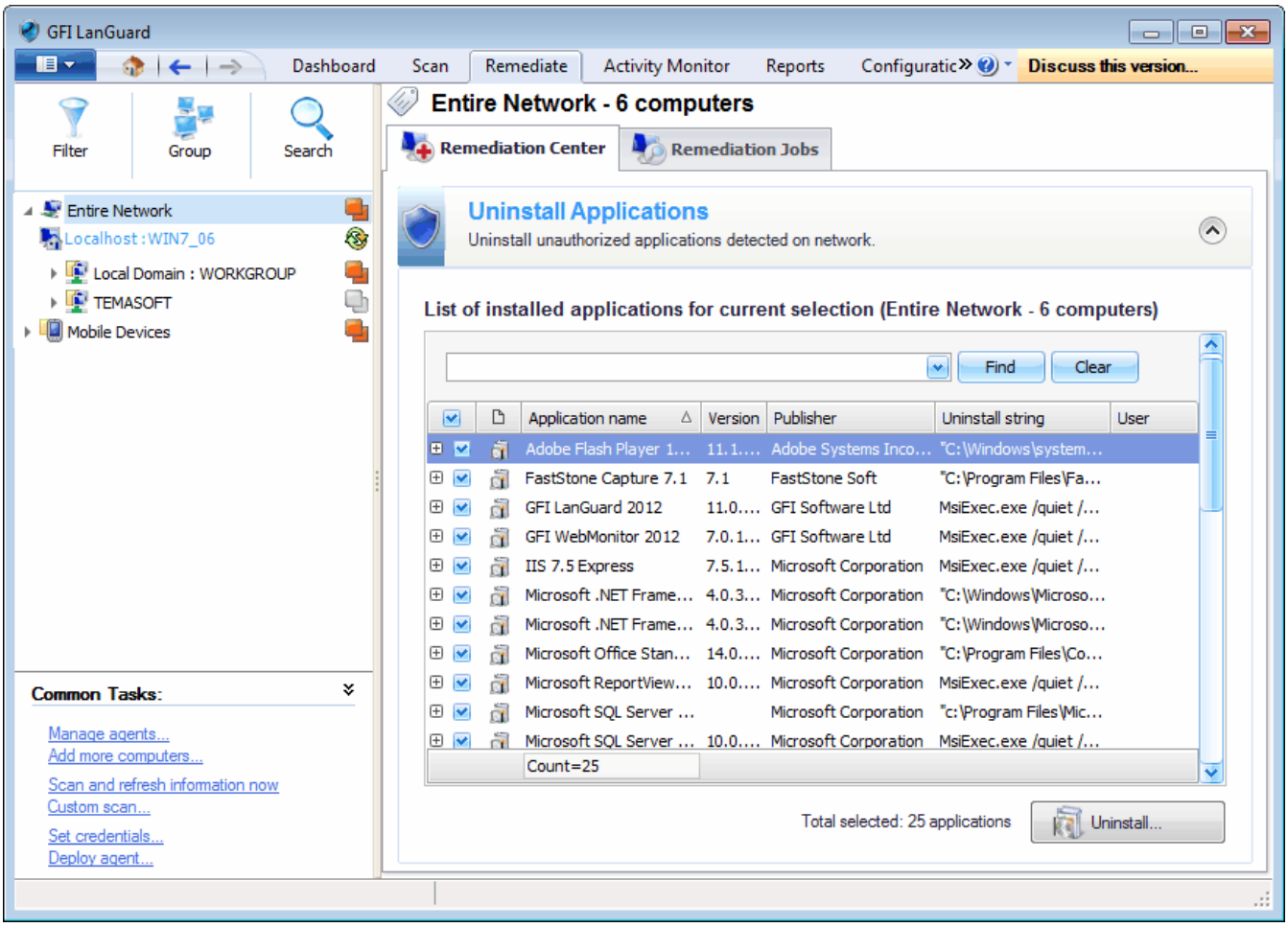
6. To view the deployment progress, click **Remediation Jobs** from the right panel.

Uninstalling Custom Applications

Using this feature, you can control the installed applications, on which computers, and uninstall any unauthorized applications present on network computers.

To uninstall applications:

1. Select **Remediate** tab **> Remediation Center** and click **Uninstall Applications**.



Screenshot 137: Uninstall applications

2. Expand the application to display the list of computers and select the computers where the application will be uninstalled.

> **NOTE**
> The list of applications displayed relies on the unauthorized applications set up for the scanning profile in use. For more information, refer to Configuring unauthorized applications auto-uninstall (page 169).

3. Repeat step 2 for all applications that will be uninstalled and click **Uninstall**.

> **NOTE**
> Key in a criteria and click **Find** to search a vulnerability. Click **Clear** to clear previous search results.

4. Configure the options described below:

Option	Description
Uninstall immediately	Uninstall the selected applications immediately.
Uninstall on	Uninstall the selected applications on a specific date and time. Configure when to uninstall the applications.

Option	Description
Credentials	Select the authentication method to use or specify a username and password. Select **Use per computer credentials when available**, to use the credentials specified in the computer properties. For more information, refer to Agent properties (page 77).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 173).
After deployment options	Configure the actions to perform after deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 173).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to Configuring auto-remediation options (page 173).

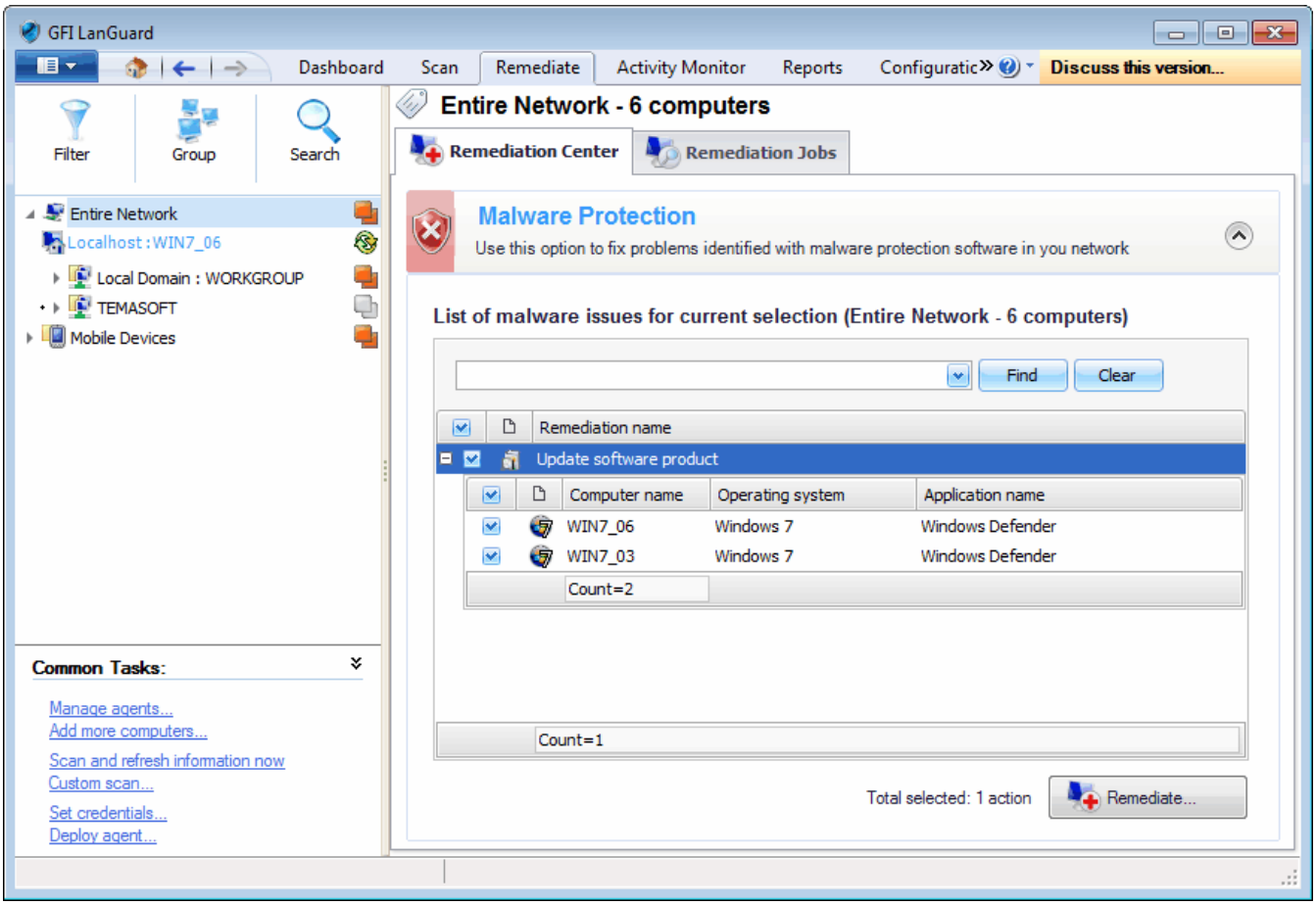
5. Click **OK**

6. To view the un–installation progress, click **Remediation Jobs** from the right panel.

Malware Protection

Use the **Malware Protection** section to remediate vulnerabilities related to malware protection identified on target computers. Amongst others, this section enables you to scan target machines for spyware, viruses and enable local firewall.

> **NOTE**
> To scan a machine for viruses and spyware, the target machine must have antivirus and antispyware installed.



Screenshot 138: Malware protection

To remediate malware protection vulnerabilities:

1. Select **Remediate** tab > **Remediation Center** and click **Malware Protection**.

2. Locate and expand the malware vulnerability and select the computers to remediate.

> **NOTE**
> Key in a criteria and click **Find** to search a vulnerability. Click **Clear** to clear previous search results.

3. Click Remediate and configure the options described below:

Option	Description
Deploy immediately	Deploy the selected applications immediately.
Deploy on	Deploy the selected applications on a specific date and time. Configure when to deploy the applications.
Credentials	Select the authentication method to use or specify a username and password. Select **Use per computer credentials when available**, to use the credentials specified in the computer properties. For more information, refer to Agent properties (page 77).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 173).

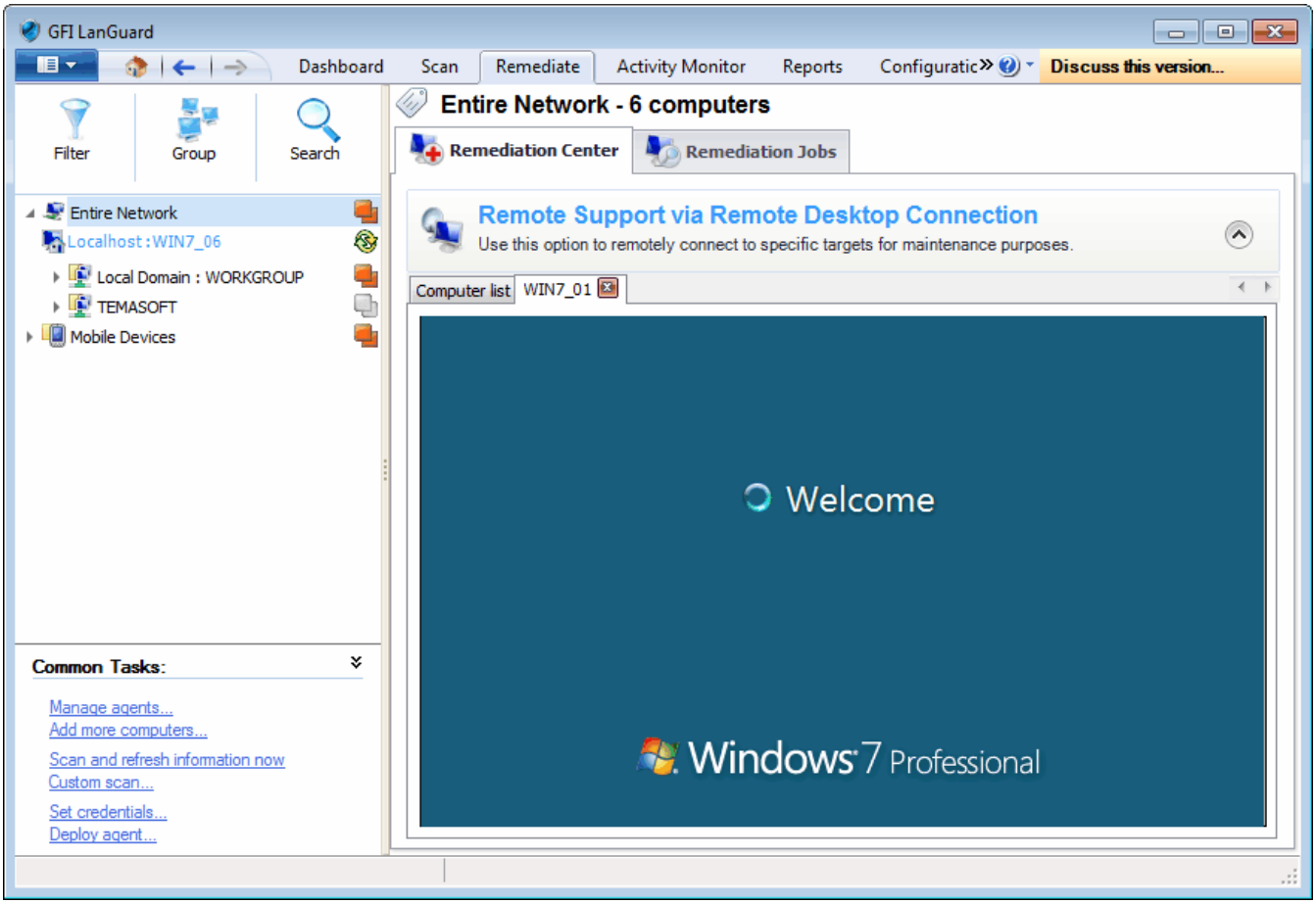
Option	Description
After deployment options	Configure the actions to perform after deploying the selected applications. For more information, refer to Configuring auto-remediation options (page 173).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to Configuring auto-remediation options (page 173).

4. Click **OK**

5. To view the action progress, click **Remediation Jobs** from the right panel.

Using Remote Desktop Support

Through Remote Support, you can control remote computers using Terminal Services and Remote Desktop Protocol. Remote Support enables you to install missing patches, service packs and custom software through a remote connection.



Screenshot 139: Remote desktop connection

To connect remotely to a target machine:

1. Click **Remediate** tab and from the left panel select a computer or domain/workgroup.

2. Expand **Remote Support via Remote Desktop Connection** from the right panel.

3. Depending on your selection, the list contains the available computers that allow remote desktop connection.

4. Double-click a machine from the list to connect.

NOTE

To disconnect a machine, select **Remediation Center > Remote Support via…**, right–click a machine from the list and select **Disconnect**.

NOTE

To disable remote connection, right click a machine and select **Disable Remote Connection**.

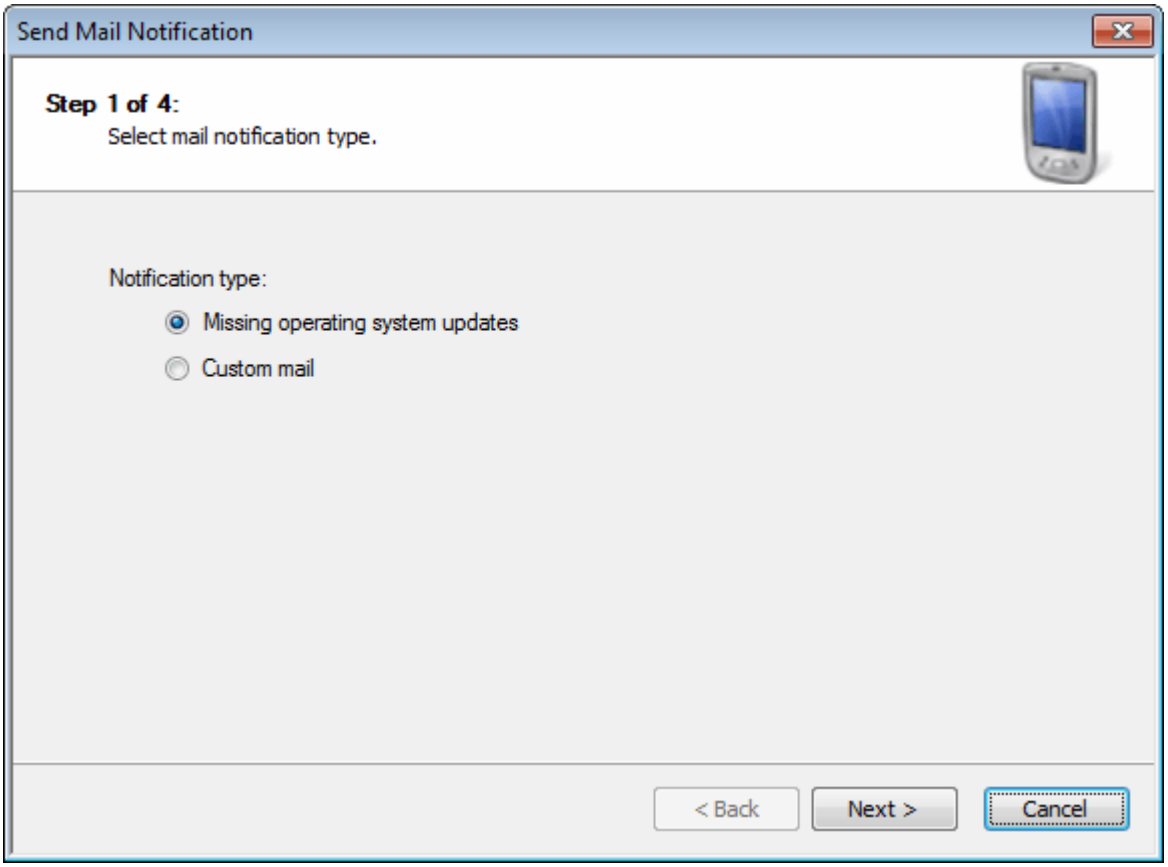
4.5.3 Sending Mobile Device Notifications

GFI LanGuard enables you to send an email notification regarding software updates for the mobile device to an email account associated with the device. The notification can either be a custom email message or a default one.

To configure mobile device alerts:

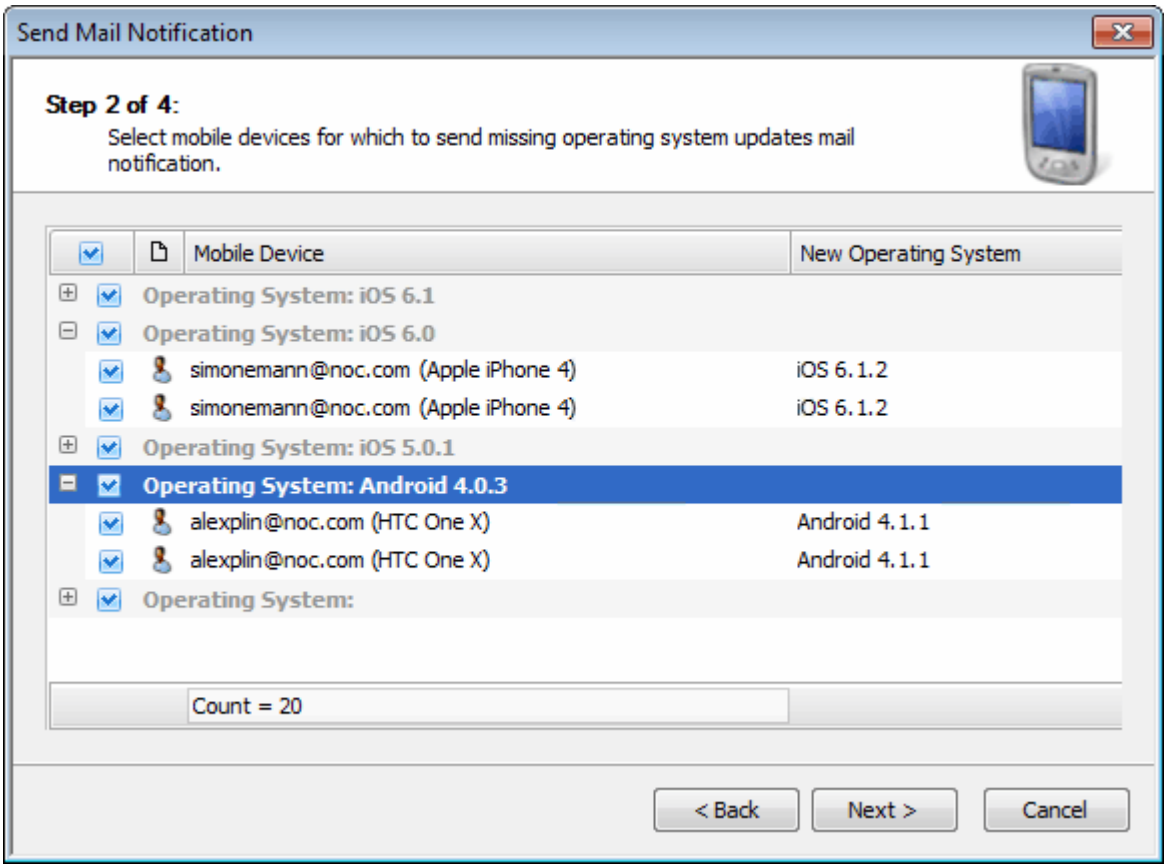
1. Click on **Dashboard** tab and from the computer tree select **> Mobile Devices**.

2. Right click on a selected account and select **Send email notification**.



Screenshot 140: Sending mail notifications: Notification type

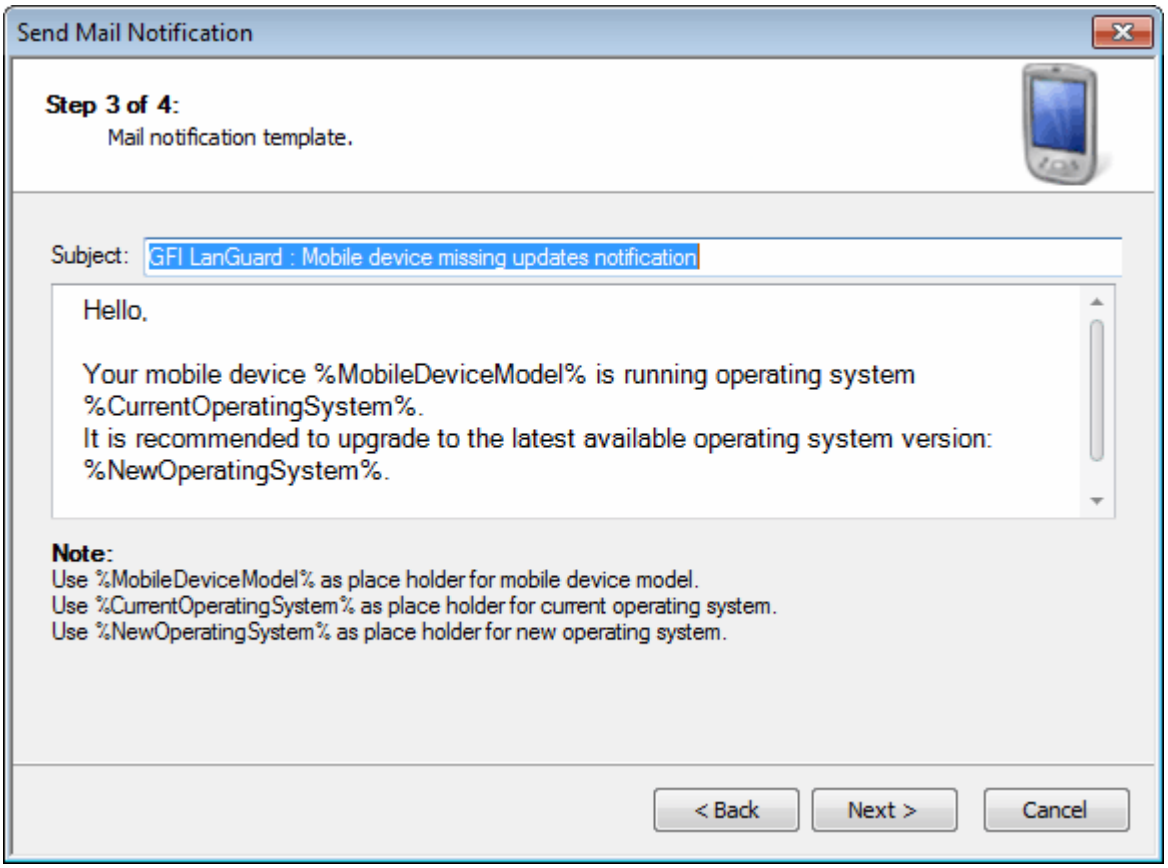
3. Select **Missing operating system updates** for a default email or **Custom mail** for a custom email.



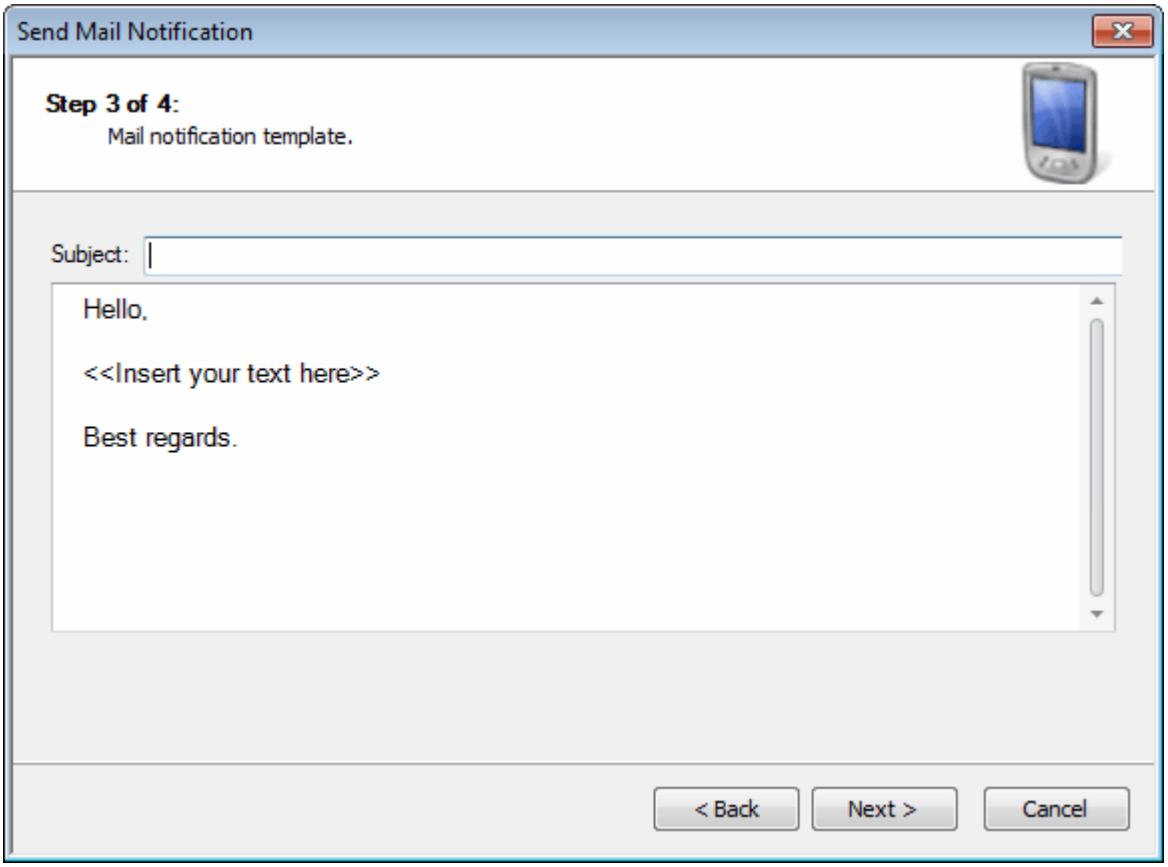
Screenshot 141: Sending mail notifications: Selecting a device

4. Select the devices for which to send a notification email for missing operating system updates and click **Next**.

5. Specify a subject and an email body if **Custom mail** is selected and click **Next** to send.



Screenshot 142: Sending mail notifications: Default notification template



Screenshot 143: Sending mail notifications: Custom notification template

4.6 Activity Monitoring

Monitoring enables you to learn more about how GFI LanGuard is performing in your infrastructure. The **Activity Monitor** tab in GFI LanGuard enables you to monitor active security scans, remediation jobs and download operations of missing updates and security definitions.

Topics in this section:

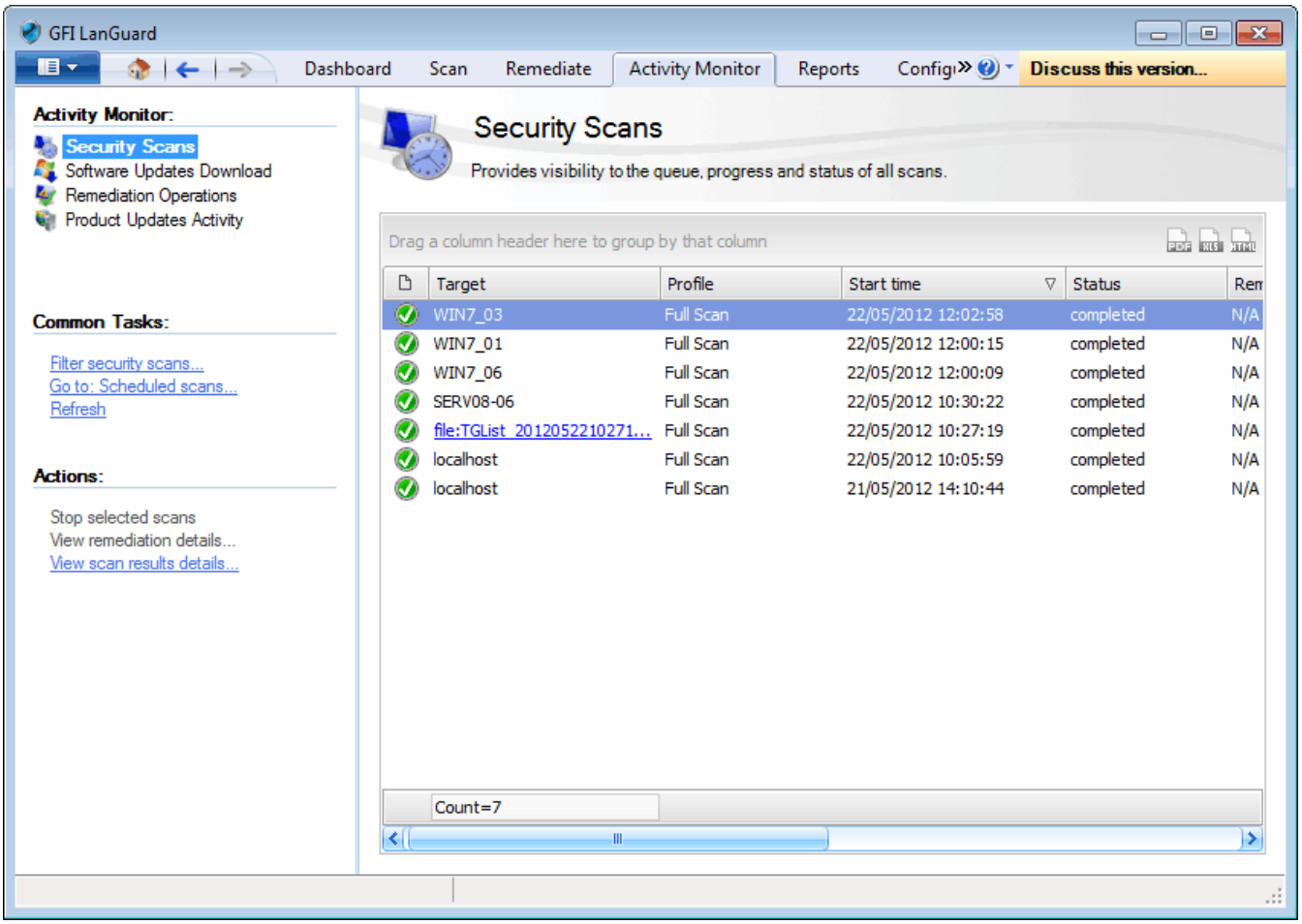
4.6.1 Monitoring Security Scans

The **Security Scans** section enables monitoring of all the security scans that are currently in progress.

To monitor active security scans:

1. Launch GFI LanGuard.

2. Click **Activity Monitor** tab and from the left panel click **Security Scans**.



Screenshot 144: Monitoring security scans

NOTE
To stop a scan right–click the security scan and select **Stop selected scans**.

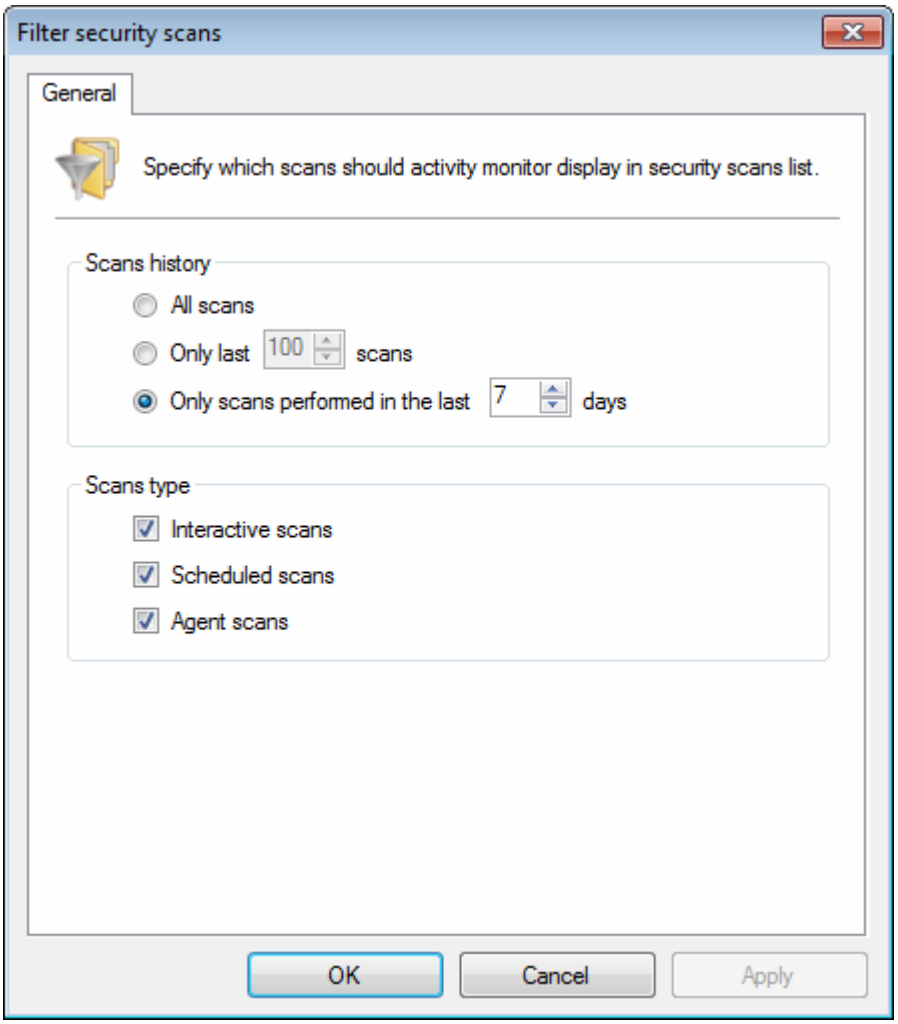
NOTE
Drag and drop a column header in the designated area to group data by criteria.

Filter Security Scans

The **Security Scan** section enables you to configure what type of scans to monitor. To configure what type of scans are displayed:

1. Launch GFI LanGuard.

2. Click **Activity Monitor** tab and from **Common Tasks**, click **Filter security scans**.



Screenshot 145: Filter security scan dialog

3. Configure the options described below:

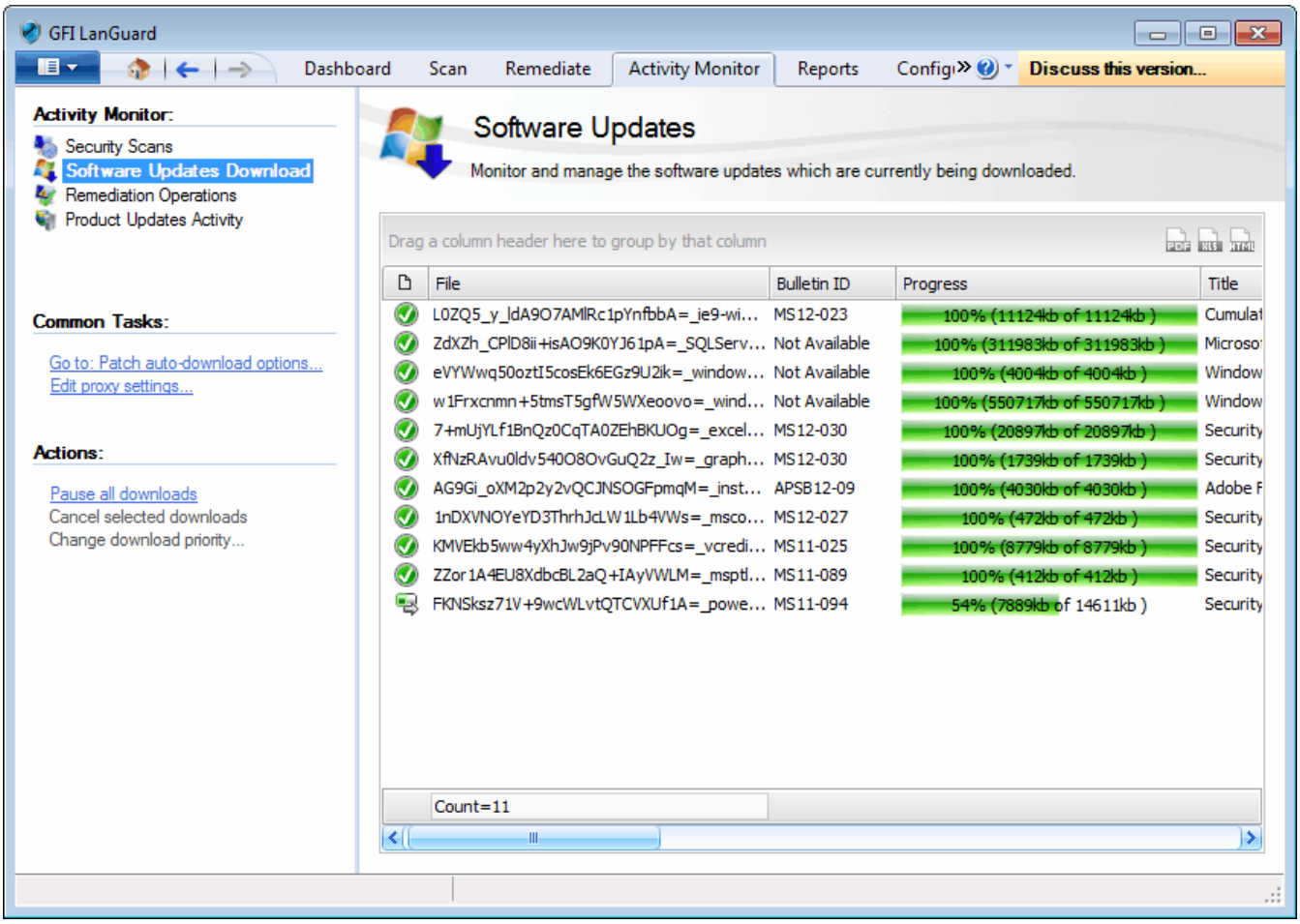
Option	Description
All scans	Displays all scans.
Only last X scans	Displays only the last X scans.

Option	Description
Only scans performed in the last X days	Displays only the scans performed in the last X days.
Interactive scans	Displays only manual scans. For more information, refer to Manual scans (page 96).
Scheduled scans	Displays only scheduled scans. For more information, refer to Scheduled scans (page 100).
Agent scans	Displays only scans performed on agent computers. For more information, refer to Starting an Agent scan manually (page 111).

4. Click **OK**

4.6.2 Monitoring Software Updates Download

The **Software Updates Download** screen enables you to monitor, pause, cancel or change priority to all the scheduled patch downloads.



Screenshot 146: Security updates download

The icon in the first column indicates the download status. The table below describes the different states:

Icon	Description
	Downloaded Update downloaded successfully.

Icon	Description
	**Downloading** Update is being downloaded.
	**Failed** An error occurred while downloading the update. Refer to Error column for more details regarding the error encountered.
	**Pending** Update is queued for download.
	**Cancelled** User cancelled update download.

Right–click an entry and select one of the options described below:

Option	Description
Configure Patch Auto–Download	Enables or disables auto–patch download and used to configure where the patches are stored. For more information, refer to Patch auto-download settings.
Edit proxy settings…	Configure the proxy settings used by GFI LanGuard to connect to the Internet. For more information, refer to Configuring Program Updates (page 240).
Change download priority…	Change the download priority. Select between, High, normal or low priority.
Cancel selected downloads	Stop and remove the selected download.
Pause all downloads	Temporarily pause all downloads.

Troubleshooting failed Software Updates

This section provides you with information about three software update errors, which are likely to cause software updates to fail from downloading and/or installing.

The table below provides you with the actual error message that you will receive if one of the errors has to occur and a possible cause and solution, for each:

Error Message	Cause	Solution
The file URL points to a different file than expected. Try re-scanning with the latest program updates	The Third-Party vendor replaces old patches with updated patches, using the same URL. GFI has no control over how Third-Party vendors replace updates and URLs.	Download the latest Product Updates manually and re-scan your targets. For more information, refer to Configuring Program Updates (page 240). **NOTE** There is a 12 to 24 hour delay between Third-Parties releasing new updates and GFI LanGuard adding support for them. During this time, you will continue to receive the error message, even though you download and scan your targets using the latest product updates.

Error Message	Cause	Solution
The repository folder is not accessible. See Configuration - Patch Auto-download	The repository folder is the location where updates are downloaded to. GFI LanGuard enables you to specify alternate repositories than the default location. This error is generally caused after specifying an invalid or inaccessible repository path (example, the given path refers to a location on a shutdown computer).	1. Manually check that you can access the folder path, using the same logon credentials. 2. Ensure that the specified path is a valid: » **Local path** - example: `C:\Share` or `C:\Folder` » **UNC path** - example: `\\NetworkShare\Folder` 3. Ensure that the path is keyed in correctly. **NOTE** For more information, refer to **Configuring Patch Auto-download settings**, from Configure Missing Updates Auto-Deployment.
Internet connection not available	The computer where GFI LanGuard is installed, does not have Internet access. There are many possible causes to this problem.	Establish an Internet connection and attempt to download the failed updates.

4.6.3 Monitoring Remediation Operations

Remediation operations can be monitored from the following places:

» Remediation Jobs sub-tab

» Remediation Operations view

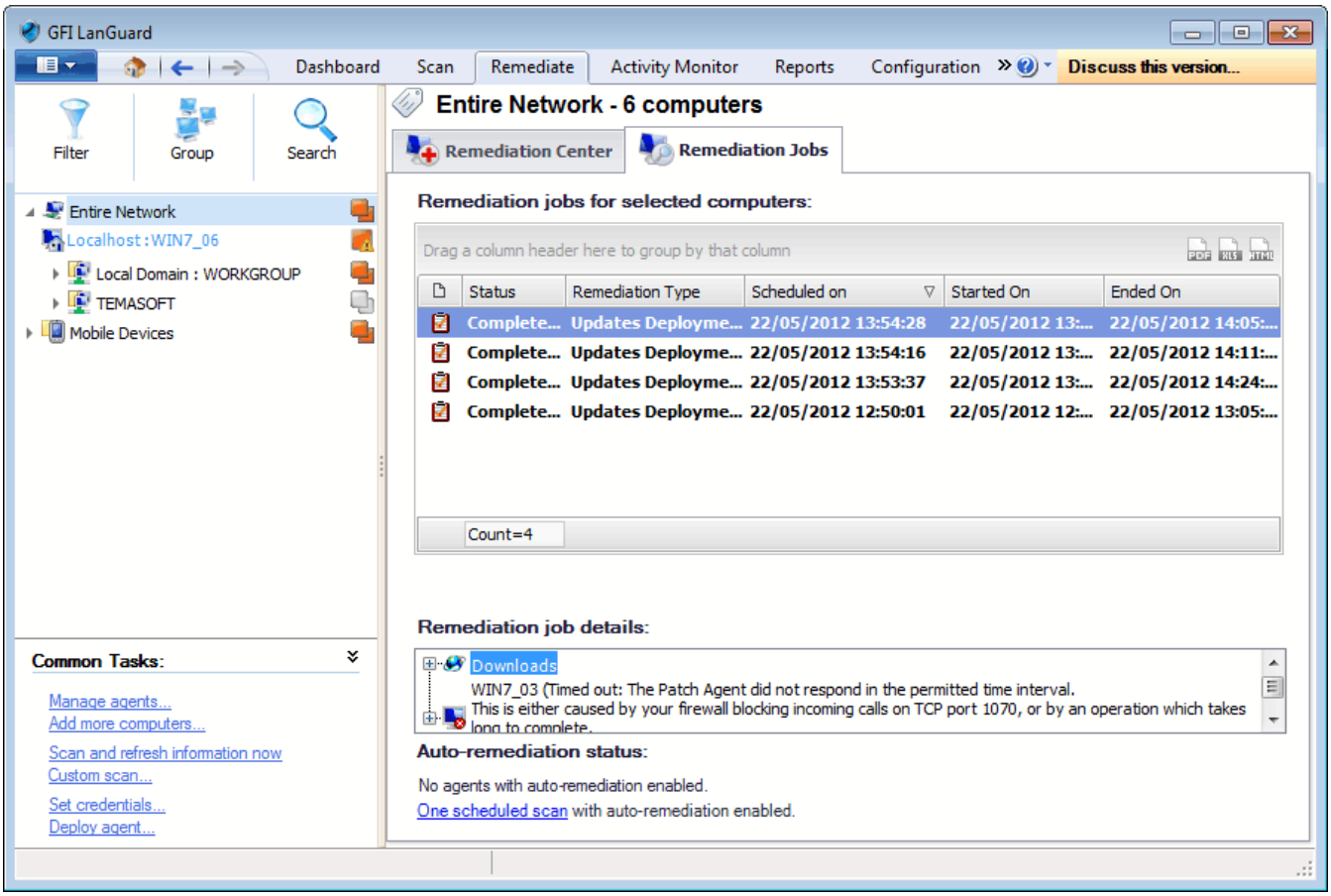
Remediation Jobs sub-tab

The **Remediation Jobs** section enables you to monitor the remediation actions currently in progress.

To view remediation jobs in progress:

1. Launch GFI LanGuard.

2. Click **Remediate** tab > **Remediation Jobs** sub-tab.



Screenshot 147: Monitoring jobs from the Remediation jobs sub-tab

3. From the computer tree, select **Entire Network** to view all the running, as well as completed operations. Select specific computers/groups to view remediation jobs history and/or remediation progress for the selected item(s).

> **NOTE**
> Right-click a remediation job and select **Cancel selected deployment** to stop the operation.

> **NOTE**
> Right-click a remediation job and select **Go to associated schedule scan** to view the pre-configured scan which triggered the remediation.

> **NOTE**
> The **Remediation job details** section provides you with granular progress details indicating the total number of files that have to be downloaded, download progress for each file and the current operation being executed as part of the remediation job.

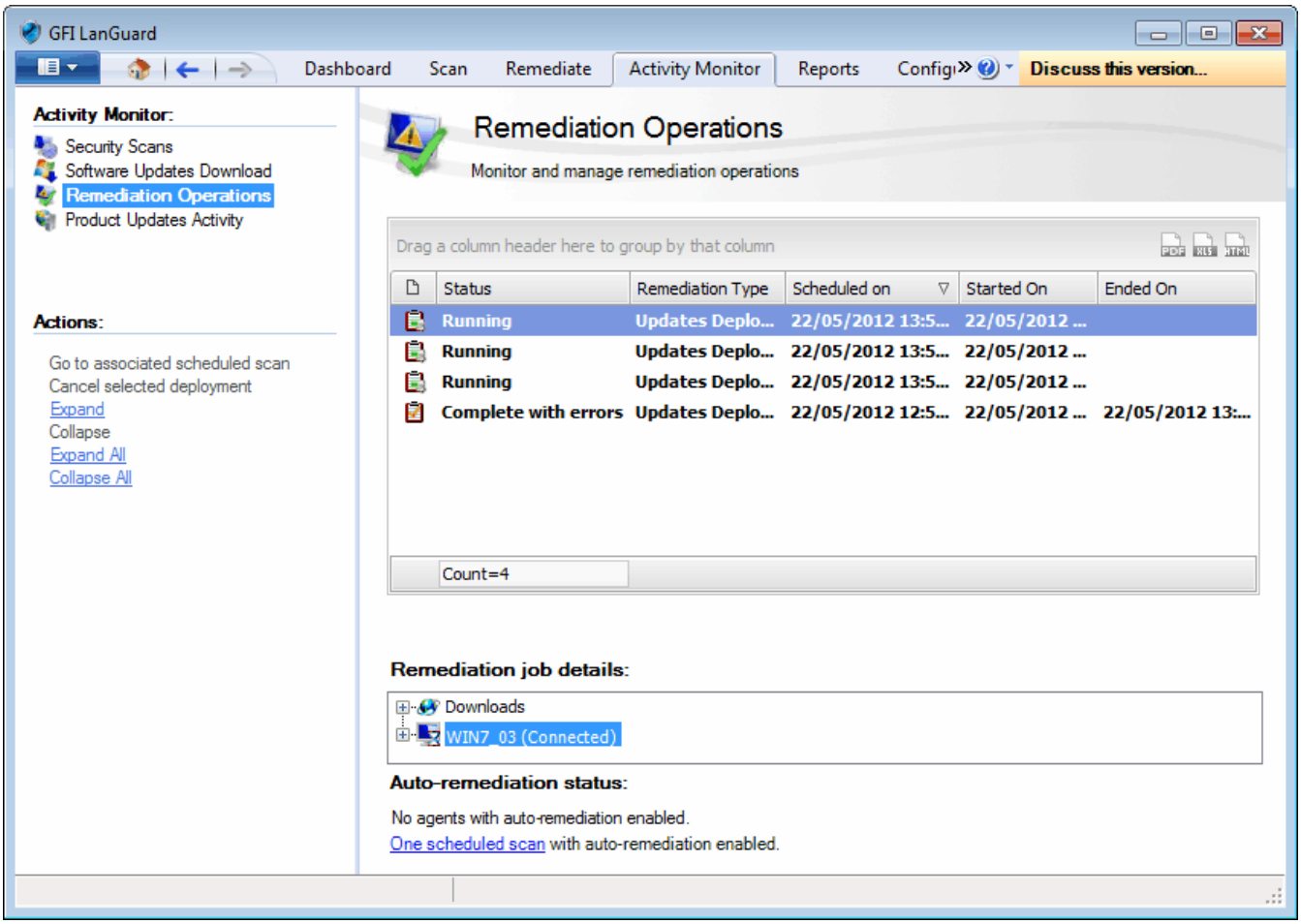
Remediation Operations view

The remediation operations screen enables you to monitor as well as cancel all the scheduled remediation features within GFI LanGuard.

To view remediation job activity:

1. Launch GFI LanGuard.

2. Click **Activity Monitor > Remediation Operations**.



Screenshot 148: Monitoring jobs from the Remediation Operations view

3. Use the view to monitor the status and history of all the running and complete remediation jobs.

NOTE

Right-click a remediation job and select **Cancel selected deployment** to stop the operation.

NOTE

Right-click a remediation job and select **Go to associated schedule scan** to view the pre-configured scan which triggered the remediation.

NOTE

The **Remediation job details** section provides you with granular progress details indicating the total number of files that have to be downloaded, download progress for each file and the current operation being executed as part of the remediation job.

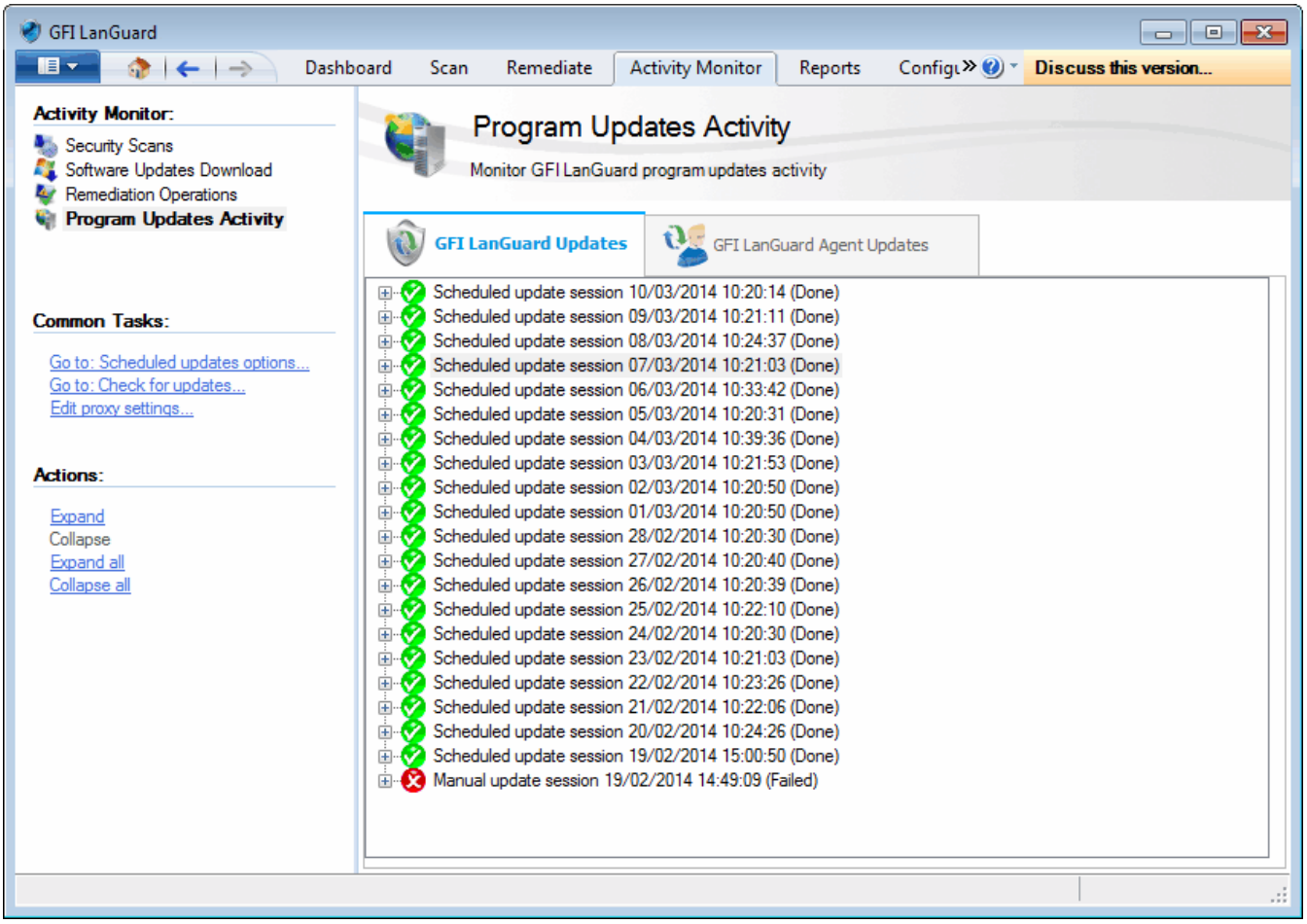
4.6.4 Monitoring Product Updates

The **Product Updates Activity** screen enables you to view a history of the product updates, performed by GFI LanGuard and the real time update activity of the GFI LanGuard agents. For more information, refer to Configuring Program Updates (page 240).

To monitor GFI LanGuard updates:

1. Click the **Activity Monitoring** tab and select **Program Updates Activity**

2. From the right pane select **GFI LanGuard Updates**.

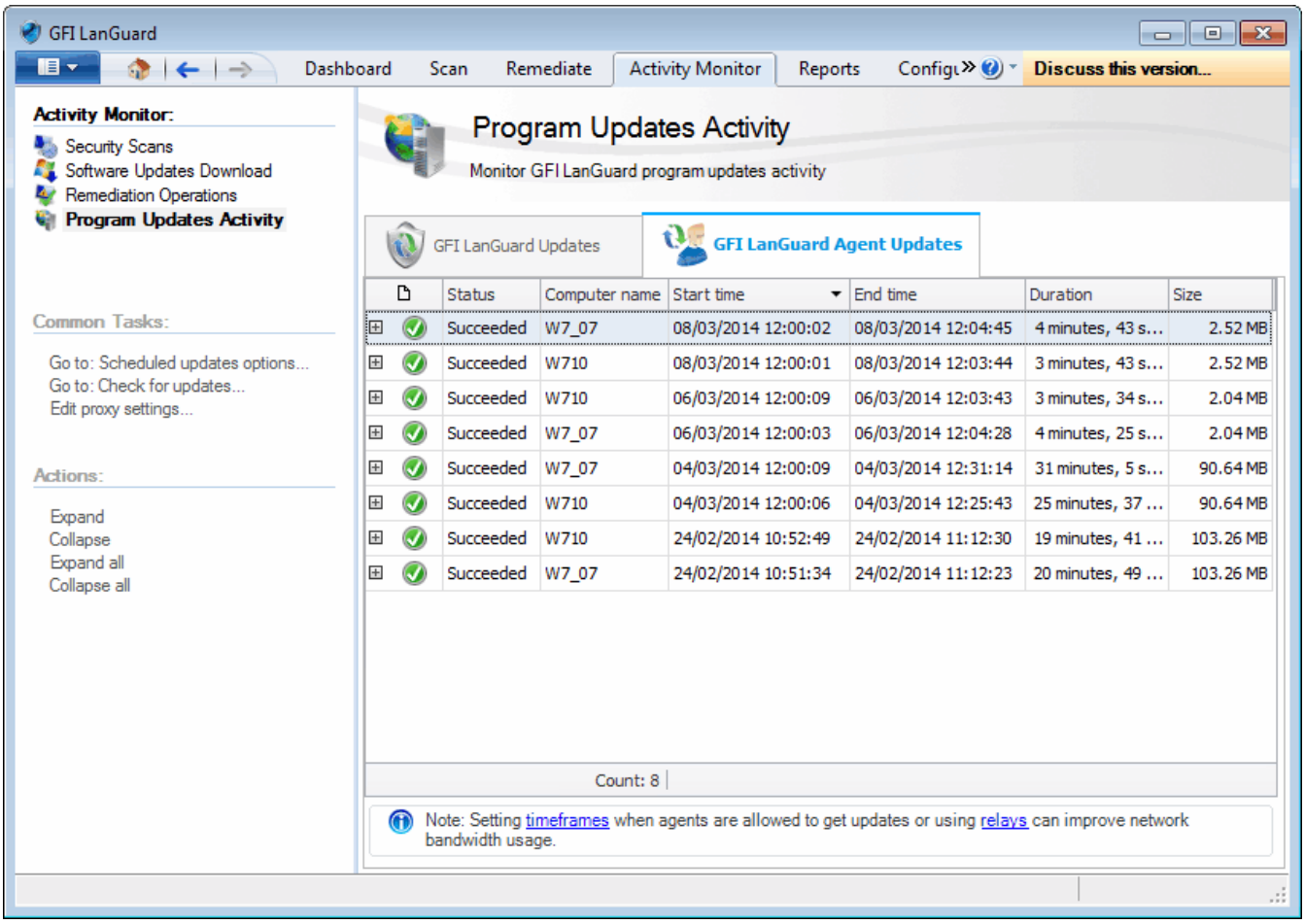


Screenshot 149: Product updates activity - GFI LanGuard Updates

To monitor GFI LanGuard Agent updates:

1. Click on the **Activity Monitoring** tab and select **Program Updates Activity**

2. From the right pane select **GFI LanGuard Agent Updates**.



Screenshot 150: Product updates activity - GFI LanGuard Agent Updates

4.7 Reporting

GFI LanGuard includes a reporting module which enables you to generate text and graphical reports based on information obtained from network security scans. This topic provides you with an overview of the available reports as well as how to create your own reports for a tailored solution. Through the Reports tab, you are able to generate technical activity reports for IT staff and also executive reports that normally contain less technical details and focus more on overall statistics.

Topics in this section:

4.7.1 Available reports

This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard.

There are two main types of reports:

» General reports - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity

» Legal compliance reports - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

General reports

To view **General** reports:

1. Click **Reports** tab.

2. Click **View**, and from the list of reports, click **General Reports**, then select any of the following reports:

Report Title	Description
Network Security Overview	An executive summary report showing: » Network vulnerability level » Most vulnerable computers » Agent status » Audit status » Vulnerability trends over time » Information on operating systems » Servers and workstations.
Computer Security Overview	An executive summary report showing: » Computer vulnerability level » Agent status » Audit status » Vulnerability trends over time » Computer summary and details.
Vulnerability Status	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by: » Computer name » Vulnerability severity » Timestamp » Category.
Patching Status	Shows statistical information related to missing and installed updates detected on your scan targets. Updates can be grouped by name, severity, timestamp, vendor and category. Use this report to get: » Missing vs. Installed updates comparison » Charts and tables displaying missing updates distribution for each item from the first and second grouping criteria » Charts and tables displaying installed updates distribution for each item from the first and second grouping criteria » Patching details for missing and installed patches.
Full Audit	A technical report showing information retrieved during an audit. Amongst others, the report contains information on: » Vulnerabilities » Open ports » Hardware and software.
Software Audit	Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on: » Antivirus » Antispyware » Applications inventory.

Report Title	Description
Scan History	An overview of the network security audits performed over time. Amongst others, the report includes information on: » Most scanned computers » Least scanned computers » Auditing status » History listing.
Remediation History	Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on: » Remediation actions per day » Remediation distribution by category » Remediation list grouped by computers.
Network Security History	Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to: » The vulnerability level » User accounts » Groups » Ports » Shares » Registry entries.
Baseline Comparison	Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on: » Registry » Installed Service Packs and Update Rollups » Missing Security/Non-Security Updates » Vulnerability level.
Mobile Devices Audit	Shows information related to detected mobile devices found during an audit. Amongst others, the report includes information on: » Vulnerability distribution by severity » Vulnerability distribution by computer » Vulnerability listing by computer.
USB Devices	Lists all USB devices found in an audit, grouped by computer.
Missing Microsoft® Security Updates	Shows statistical information related to missing Microsoft® security updates, detected on your scan targets. Select items to include in your report: » General missing updates distribution chart » Distribution table » Vulnerability list.
Missing Non-Microsoft® Security Updates	Shows statistical information related to missing non-Microsoft® security updates, detected on your scan targets. Select items to include in your report: » General missing updates distribution chart » Distribution table » Vulnerability list.
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.
Computer Summary	A summary of scan target information, including: » Operating system information » Agent status » Vulnerabilities severity.

Report Title	Description
Hardware Audit	Illustrates information related to the hardware found during an audit.
Computer Details	Provides a detailed list of computer properties, including: » MAC Address » Time to Live » Network Role » Domain » Lan Manager » Is relay agent » Uses relay agent » Attributes » Operating system » IP address.
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.
Open Ports	Lists all the open ports found during an audit. The results are grouped by port type (TCP and UDP).
Services	Lists all services found during an audit. Results are grouped by computer name.
Groups and Users	Lists all Groups and Users found during an audit. The result is grouped by computer name.
Mobile Device Policies	Lists all mobile device policies found during an audit. The result is grouped by computer name.
Unauthorized Applications	Lists all unauthorized applications installed scan targets, including: » Top Computers with Unauthorized Applications » Top Unauthorized Applications » Applications Inventory » Computers without Antivirus Installed
Antivirus Applications	Shows information related to the antivirus installed on scan targets.
New Devices	Lists all new devices found during last week audits.

Legal Compliance reports

To view **Legal Compliance** reports:

1. Click **Reports** tab.

2. From the list of reports, expand any of the following compliance reports suites:

Report Suite Title	Description
PCI DSS Compliance Reports	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. GFI LanGuard provides you with a number of reports that cater for PCI DSS compliance, including: » PCI DSS Requirement 1.4 - Installed Firewall Applications » PCI DSS Requirement 2.2.3 - Disk Encryption Applications » PCI DSS Requirement 5.2 - Antivirus Applications » PCI DSS Requirement 6.1 - Remediation History by Date » PCI DSS Requirement 12.12 - Open Trojan Ports by Host.

Report Suite Title	Description
HIPAA Compliance Reports	The Health Insurance Portability and Accountability Act (HIPAA) is a requirement of all healthcare providers that regulates the exchange of private patient data. This helps prevent unlawful disclosure or release of medical information. To help you follow HIPAA regulations, GFI LanGuard provides you with a suite of HIPAA compliance reports, including: » HIPAA 164.308(a)(1)(ii)(A) - Missing Security Updates by Host » HIPAA 164.308(a)(1)(ii)(A) - Vulnerability Distribution by Host » HIPAA 164.308(a)(4)(ii)(A) - Open Ports » HIPAA 164.308(a)(5)(ii)(D) - Audit Policy » HIPAA 164.308(a)(8) - Baseline Changes Comparison.
SOX Compliance Reports	The Sarbanes-Oxley Act (SOX) is regulation created in response to high-profile financial scandals as well as to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. GFI LanGuard provides a list of SOX compliance reports, including: » SOX 302.a - Network Vulnerability Summary » SOX 302.a - Remediation History by Host » SOX 302.a - Security Scans History » SOX 404 - Vulnerability Listing by Category » SOX 404 - Missing Security Updates by Host.
GLBA Compliance Reports	The Gramm–Leach–Bliley Act (GLBA) is an act that allows consolidation between Banks and Insurance companies. Part of the act focuses on IT network compliance for such companies. GFI LanGuard offers a list of GLBA Compliance reports, including: » GLBA 501.b - Baseline Changes Comparison » GLBA 501.b - Network Patching Status » GLBA 501.b - Open Trojan Ports by Host » GLBA 501.b - Vulnerable Hosts Based on Open Ports » GLBA 501.b - Vulnerable Hosts by Vulnerability Level.
PSN CoCo Compliance Reports	The Public Service Network - Code of Connection (PSN CoCo) is simply a list of conditions that should be met before connecting an accredited network to another accredited network. GFI LanGuard helps you monitor the status of such connections through the list of PSN CoCo Compliance reports, which include: » PSNCoCo RIS. 1 - Baseline Changes Comparison » PSNCoCo MAL. 1 - Disk Encryption Applications » PSNCoCo MAL. 1 - Installed Firewall Applications » PSNCoCo PAT. 1 - Installed Security Updates by Host » PSNCoCo PAT. 1 - Installed Security Updates by Severity.
CIPA	The Children's Internet Protection Act (CIPA) addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. GFI LanGuard Central Management Server provides a list of CIA Compliance reports including: » Req. 47 USC § 254(l)(1)(A)(iv) - Network Vulnerability Summary » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Distribution by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Category » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Severity » Req. 47 USC § 254(l)(1)(A)(iv) - Open Trojan Ports by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Network Patching Status » Req. 47 USC § 254(l)(1)(A)(iv) - Missing Security Updates by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts Based on Open Ports » Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Baseline Changes Comparison

Report Suite Title	Description
FERPA Compliance Reports	The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. GFI LanGuard provides a list of FERPA Compliance reports, including: » FERPA 20 USC 1232g (b) - Network Patching Status » FERPA 20 USC 1232g (b) - Network Security Log by Host » FERPA 20 USC 1232g (b) - Remediation History by Date » FERPA 20 USC 1232g (b) - Vulnerability Distribution by Host » FERPA 20 USC 1232g (b) - Vulnerable Hosts Based on Open Ports.
ISO/IEC 27001 & 27002 Compliance Reports	The Information technology – Security techniques – Information security management systems (ISO/IEC) standard formally specifies a management system that is intended to bring information security under explicit management control. GFI LanGuard offers an extensive list of ISO/IEC Compliance reports, including: » ISO/IEC 27001 A. 10.4 - Antivirus Applications » ISO/IEC 27001 A. 10.7.2 - Disk Encryption Applications » ISO/IEC 27001 A. 10.6.2 - Open Shares » ISO/IEC 27001 A. 10.6.2 - Services » ISO/IEC 27001 A. 10.6.2 - System Information.
FISMA Compliance Reports	The Federal Information Security Management Act (FISMA) assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. GFI LanGuard helps you be compliant to FISMA standards through the provided reports, which include: » FISMA NIST SP 800-53 AC-2 - Groups and Users » FISMA NIST SP 800-53 PM-5 - Computer Details » FISMA NIST SP 800-53 PM-5 - Computer Summary » FISMA NIST SP 800-53 SI-5 - Missing Security Updates by Host » FISMA NIST SP 800-53 SI-7 - Antivirus Applications.
CAG Compliance Reports	The Consensus Audit Guidelines (CAG) is a publication of best practice guidelines for computer security. The project was initiated as a response to extreme data losses experienced by organizations in the US defense industrial base. GFI LanGuard offers a list of CAG Compliance reports, including: » CAG CC1 - Hardware Audit » CAG CC1 - Scan History » CAG CC3 - Audit Policy » CAG CC3 - Low Security Vulnerabilities » CAG CC11 - Open Ports.
NERC CIP Compliance Reports	The North American Electric Reliability Corporation (NERC) develops standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. GFI LanGuard provides a list of NERC CIP Compliance reports, including: » NERC CIP-005 R2 - Installed Firewall Applications » NERC CIP-005 R2 - Open Ports » NERC CIP-007 R2 - Open Shares » NERC CIP-007 R2 - Services » NERC CIP-007 R2 - System Information.

4.7.2 Generating reports

GFI LanGuard ships with an extensive list of default reports. These can be used as they are, or modified to provide information precisely to your requirements.

> **NOTE**
> For more information, refer to Customizing default reports (page 219).

To generate a report:

1. Click **Reports** tab.

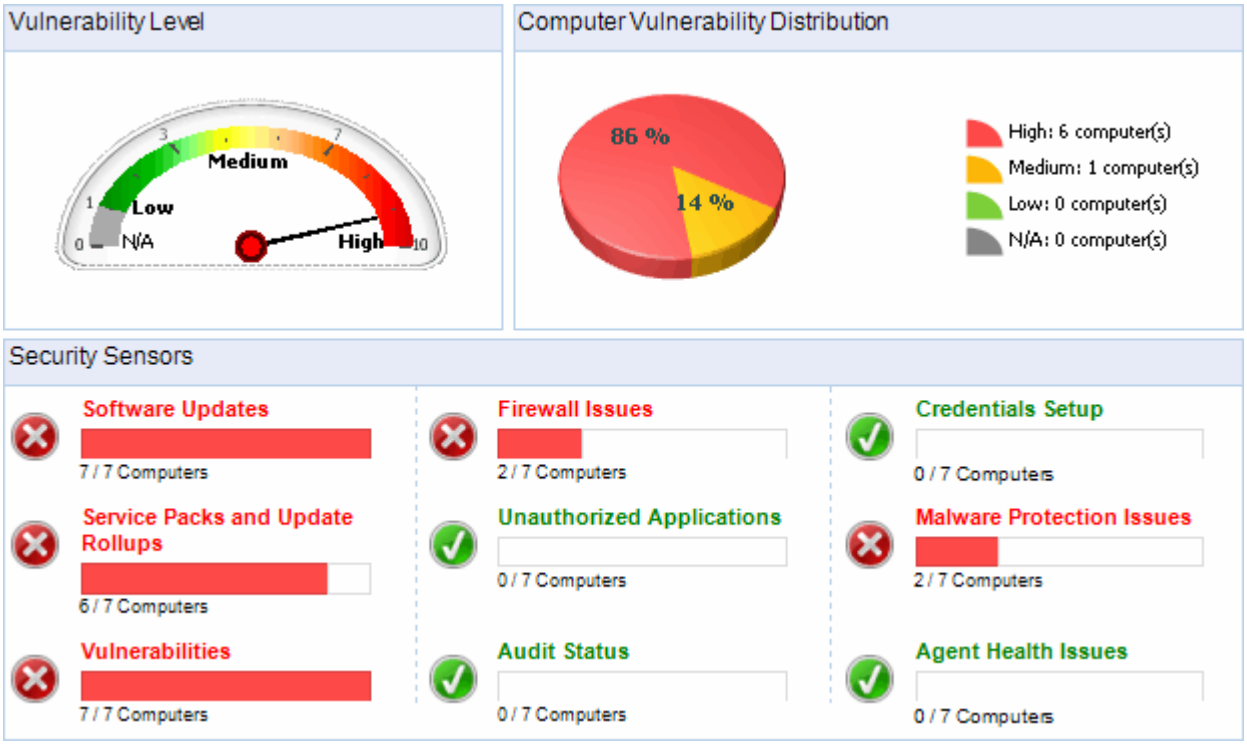
2. From the computer tree, select the computer/group you want to report on.

> **NOTE**
> Select **Entire Network** to report on all the computers listed under the computer tree.

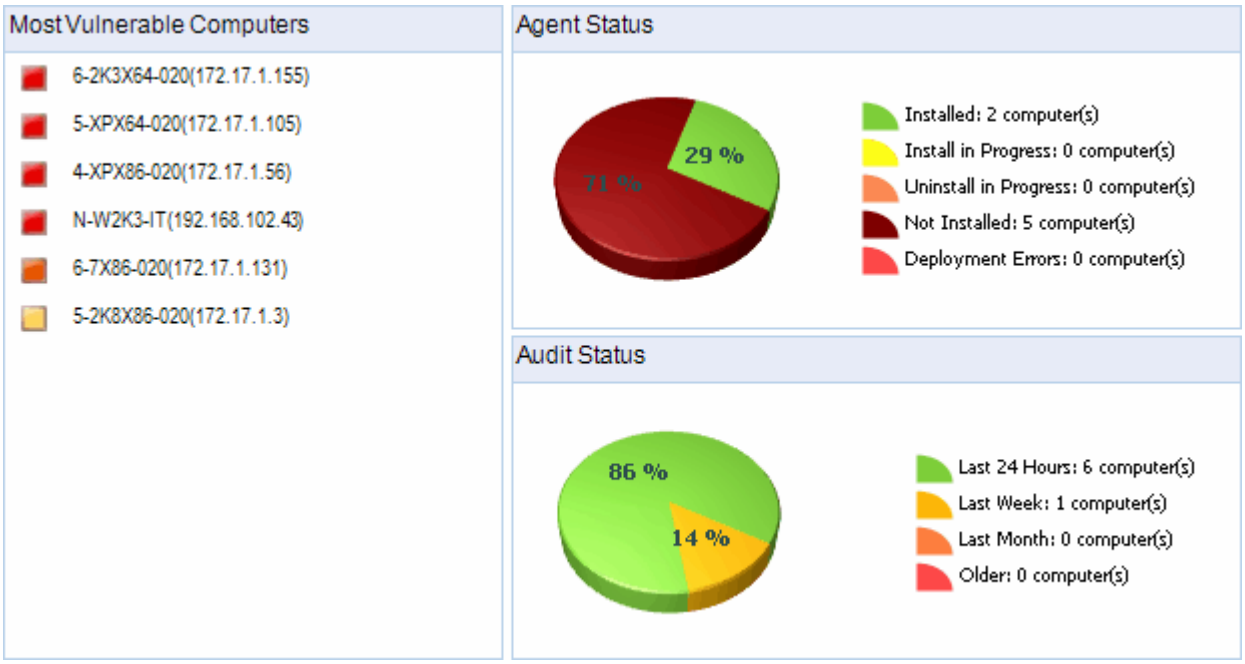
3. From the reports list, select the report you want to generate.

4. (Optional) From the right pane, click **Customize report** if changes to report items are required.

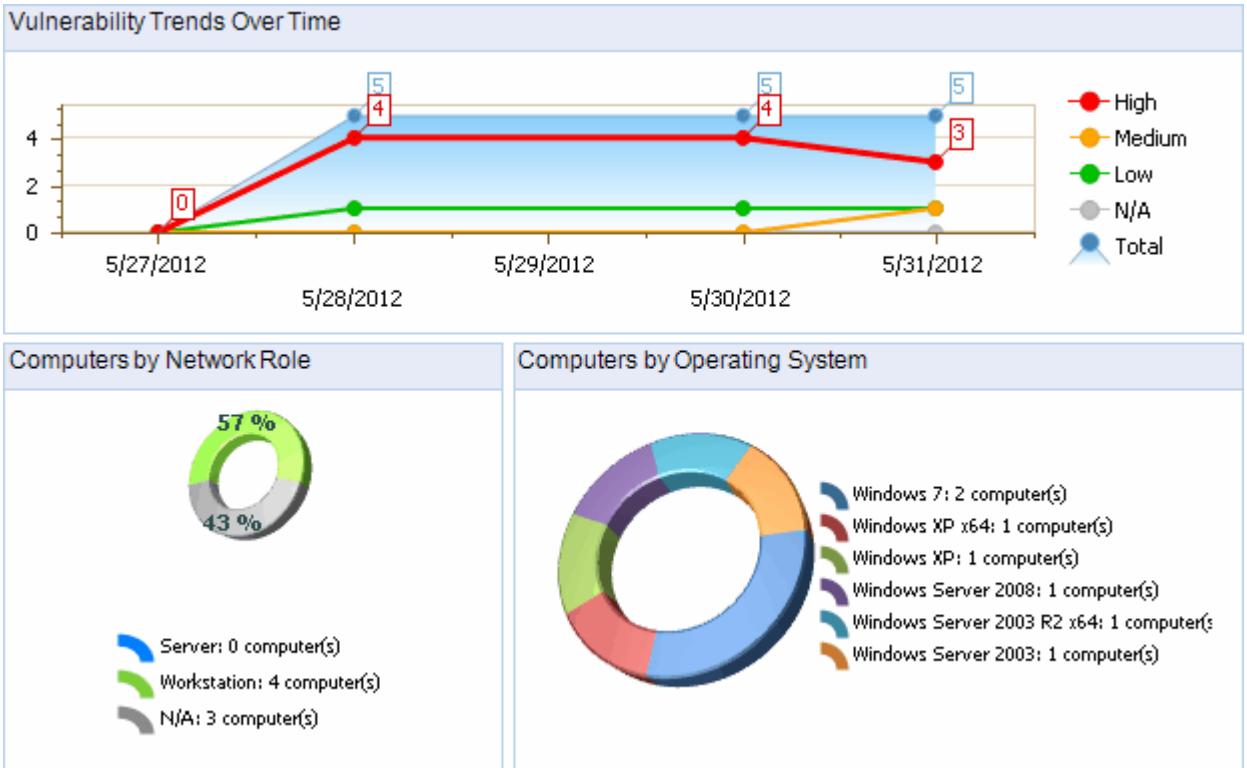
5. Click **Generate report**.



Screenshot 151: Report sample - Part 1



Screenshot 152: Report sample - Part 2



Screenshot 153: Report sample - Part 3

4.7.3 Scheduling Reports

To automate reporting tasks, GFI LanGuard enables you to generate and optionally send reports, based on a schedule. You can configure schedules for existing or custom reports.

This section contains information about:

» Creating new scheduled reports

» Configuring scheduled reports options

» Managing scheduled reports

Creating new scheduled reports

To create a new scheduled report:

1. Click **Reports** tab.

2. From **Actions**, select **New scheduled report**.

Screenshot 154: Select scheduled report template

3. From the **Report Template** section, configure the following options:

Option	Description
Schedule Report Template	Select an existing report from the drop-down menu. This enables you to create a new report based on the settings of an existing one.
Schedule Report Name	Key in a unique name for the new report.
Schedule Report Description	Optionally, key in some information about the report such as report items or schedule settings.

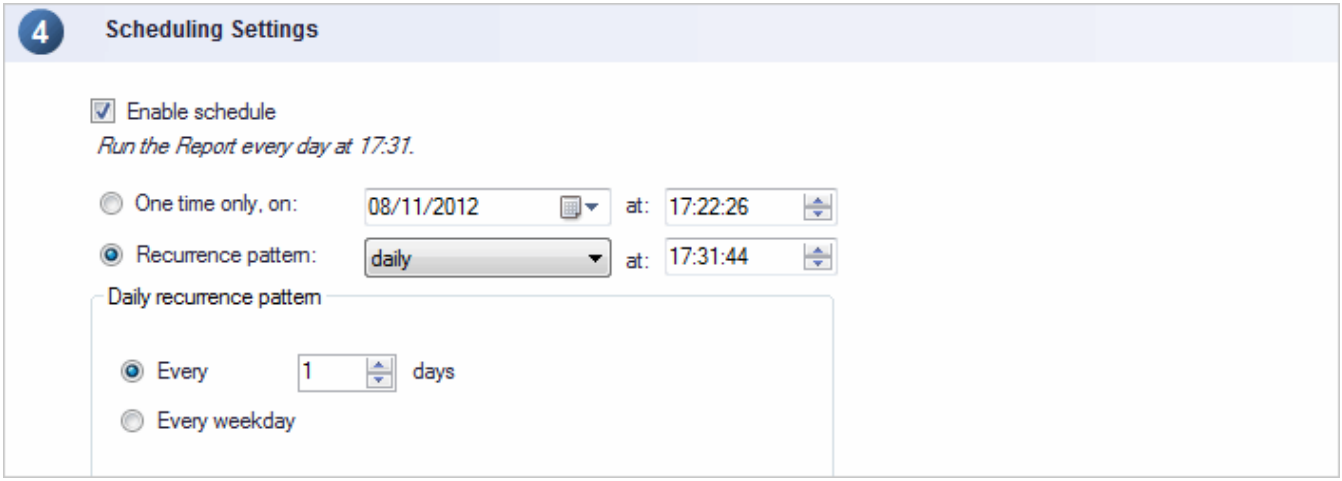
Screenshot 155: Add or remove target domains and/or computers

4. From the **Target Domains & Computers** section, configure the following options:

Option	Description
	From the computer tree, select a domain or workgroup and click **Add Domain**. The selected domains/workgroups are added to the report.
	Click **Add IP** to open the **Add IP address range** dialog. From the **Add IP address range** dialog, key in an IP range or Sub-net and click **OK**.
	Select the Domain/Workgroup/IP range you want to remove and click **Remove Domain/IP**.

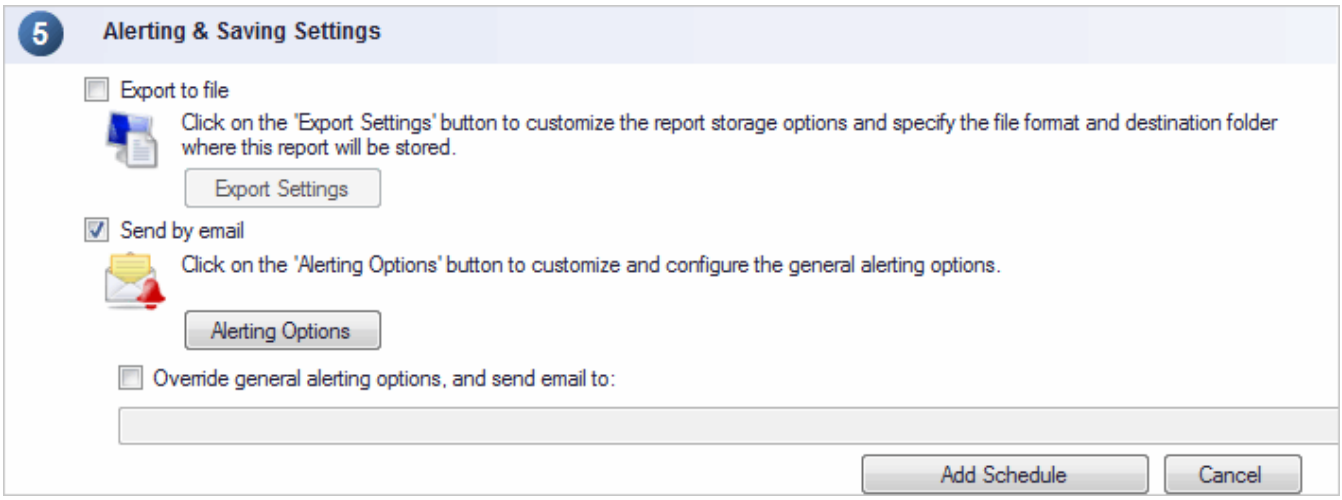
5. From the **Filter** drop-down menu, select a filter that you want to apply to the new scheduled report. This enables you to generate reports based on data pertaining to scan targets included in the filter.

> **NOTE**
> Only custom filters can be applied to scheduled reports. For more information, refer to Using the Dashboard (page 125).



6. From **Scheduling Settings**, configure the following options:

Option	Description
Enable Schedule	Select to turn on report scheduling and generate the report according to schedule settings.
One time only, on	Specify a date and time when the report is generated. This option generates the report once, on the specified date.
Recurrence pattern	Select recurrence frequency and specify the time the scheduled report is generated.



7. From **Alerting & Saving Settings**, configure the following options:

Option	Description
Export to file	Select to save the report in a folder.
Export Settings	Click **Export Settings** and from the **Scheduled Reports Storage Options** dialog, specify the folder where the report is saved and the format the report is saved in.
Send by email	Select to send report by email. The report is sent to recipients configured in Alerting Options.
Alerting Options	Click **Alerting Options** and configure alerts recipients and mail server settings. For more information, refer to Configuring Alerting Options (page 235).
Override general alerting options, and send email to	Select to use email recipients other than the ones configured in Alerting Options.

8. Click **Add Schedule** to save the report.

NOTE

Configuring scheduled reports options

To configure additional scheduled reports settings:

1. From the **Scheduled Reports** section, click **Scheduled Reports Options**.

2. Click **Alerting Options** to configure email settings to use to send reports. For more information, refer to Configuring Alerting Options (page 235).

3. Click **Storage Options** to specify the format and the location where generated reports are saved.

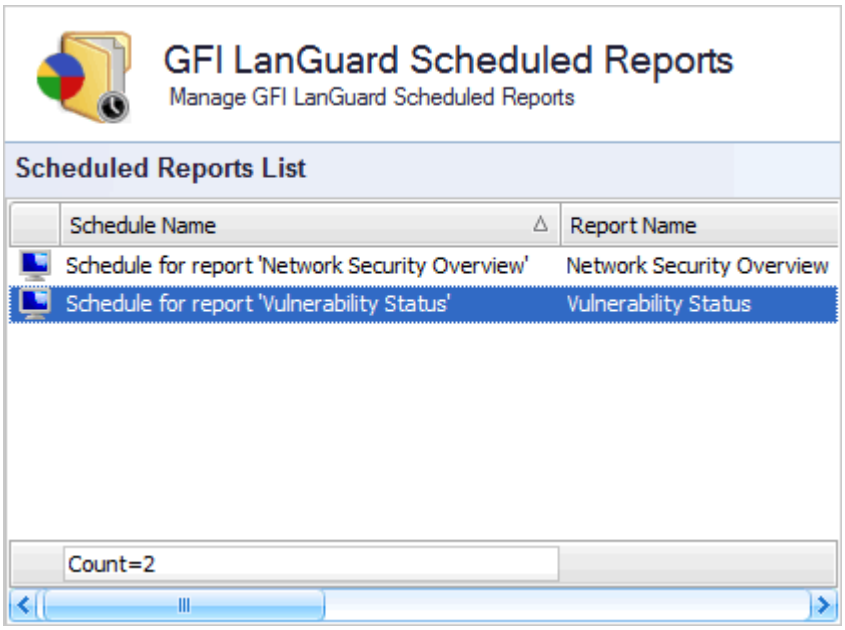
> **NOTE**
> By default, all generated reports are stored as `PDF` in: `<GFI LanGuard install directory>\Reports`.

Managing scheduled reports

To manage scheduled reports:

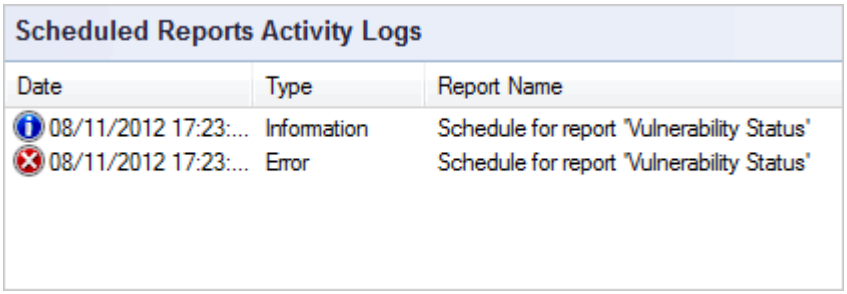
1. Click **Reports** tab.

2. From **Scheduled Reports**, click **Scheduled Reports List**.



Screenshot 156: Edit scheduled reports options

3. Double-click a report from the right pane to edit schedule report settings.



Screenshot 157: Monitor scheduled reports activity

4. Monitor schedule reports activity from the **Scheduled Reports Activity Logs** section at the bottom of the right pane.

4.7.4 Customizing default reports

GFI LanGuard enables you to create new reports based on the settings of an existing report. This saves you time and enables you to fine-tune existing reports, so that the data-set used to build the report precisely matches your requirements.

This section contains information about:

» Creating custom reports

» Customizing report logos

» Customizing Email Report Format

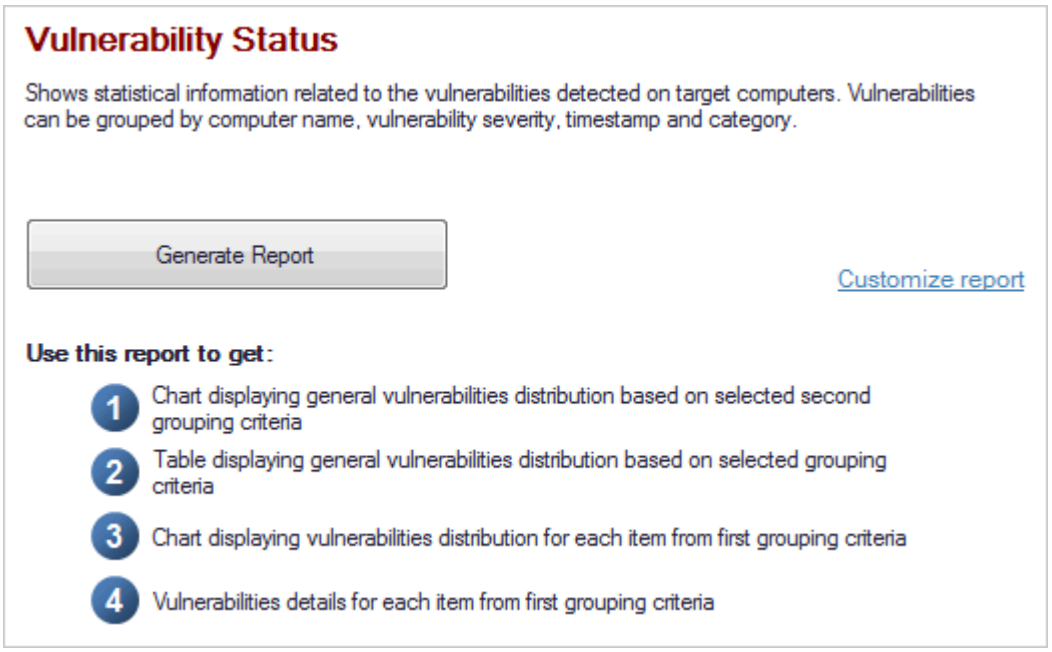
Creating custom reports

To create a custom report:

1. Click **Reports** tab.

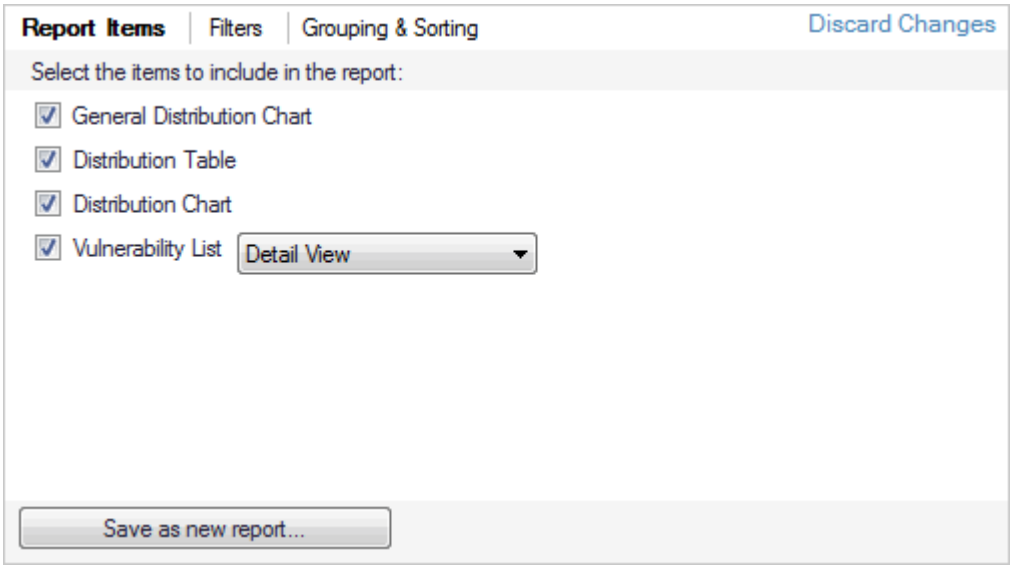
2. From the **Reports** list, select an existing report on which settings of the new reports are based on.

NOTE
Not all reports are editable.



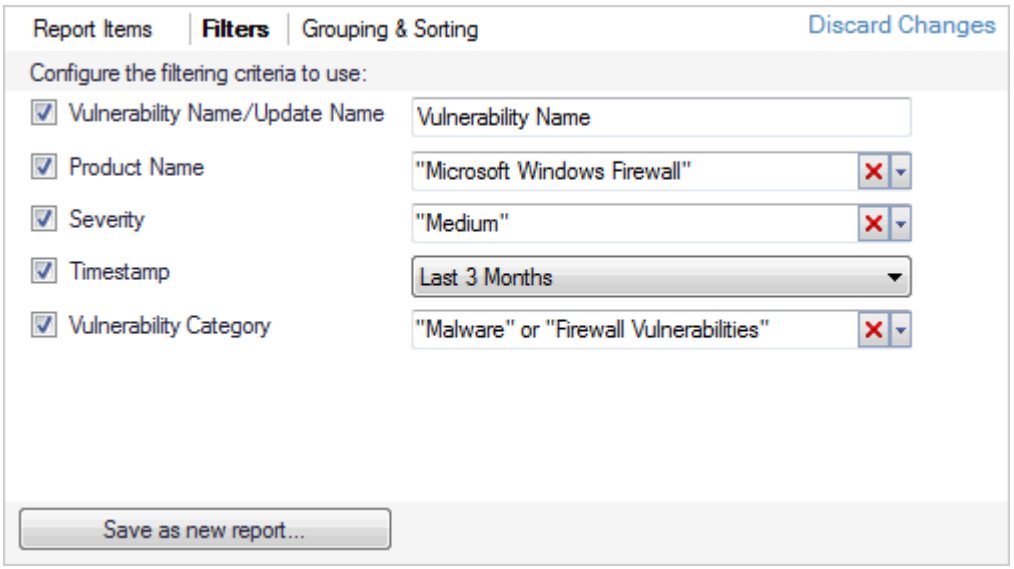
Screenshot 158: Edit report settings from the report sample preview

3. From the right pane, click **Customize report** to show advanced report options.



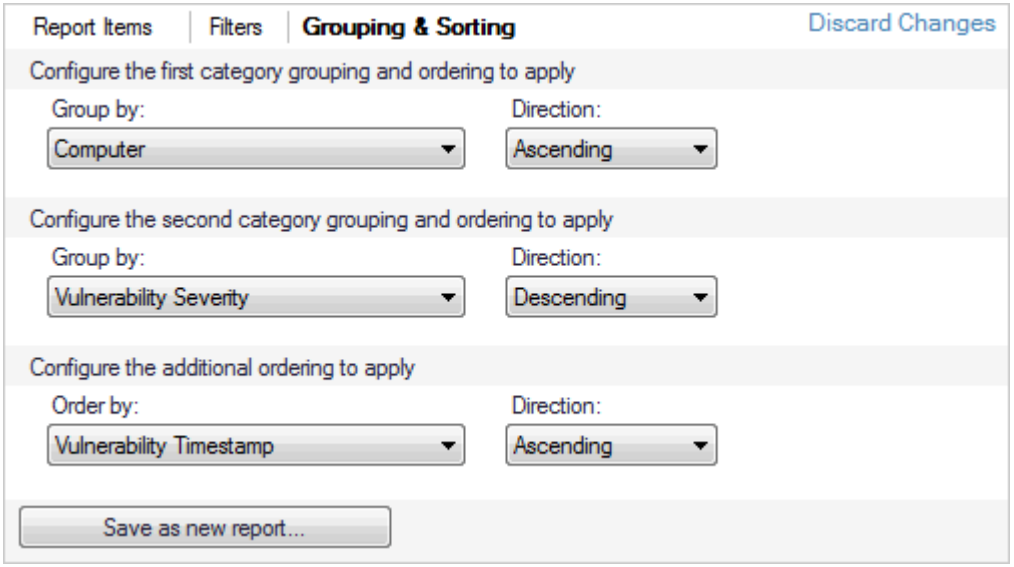
Screenshot 159: Configuring report items

4. Click **Report Items** tab and select the related items that you want to include in the report.



Screenshot 160: Configuring report filtering options

5. Click **Filters** tab and configure the available filters that relate to the report.



Screenshot 161: Configure report grouping and sorting options

6. Click **Grouping & Sorting** tab and configure:

- **First category grouping** - report information is grouped by the selected field
- **Second category grouping** - grouped information is sub-grouped by the selected field
- **Additional ordering** - order report information according to the selected field.

7. Click **Save as new report...**

8. From the **Add report** dialog, key in a name and an optional description for the new custom report. Click **OK**

Customizing report logos

GFI LanGuard enables you to use your company/custom logo in the built–in reports included in the product. Logos can be placed in the header or footer sections of the report.

Customizing Report Header Logo

1. Create / select your image.

2. Resize image to: Width = **125**, Height = **25**.

3. Rename the image to **headerlogo.png**.

4. Add custom graphics to the **logo** folder which can be found in `ProgramData\GFI\LanGuard12\Graphics\Logo`.

Customizing Report Footer Logo

1. Create / select your image.

2. Resize image to: Width = **109**, Height = **41**.

3. Rename the image to **footerlogo.png**.

4. Add custom graphics to the **logo** folder which can be found in `ProgramData\GFI\LanGuard12\Graphics\Logo`.

Customizing Email Report Format

For each scheduled email report type, there is a predefined HTML format file that includes placeholders delimited with '%' symbol (for example: %TITLE%, %NAME%). You can edit the HTML format, edit HTML style, move and delete placeholders to further customize the e mail body of generated reports. The default template location is: `<GFI LanGuard install directory> \ LanGuard 12 \ Templates \ template_mailbody.xml`.

Take into consideration that GFI LanGuard can only manage known placeholders (listed below) with their predefined role. Placeholders are usable in all scheduled report types. The table below describes the customizable placeholders:

Placeholder	Description
%TITLE%	Email title for the generated report.
%NAME%	Scheduled report name.
%DESCRIPTION%:	Scheduled report description.
%TARGET%	Targets (computers, domains) represented in the scheduled report.
%LAST_RUN%	Last run date and time of the scheduled report.
%NEXT_RUN%	Next run date and time of the scheduled report. **NOTE** This placeholder is used only for daily digest reports.
%PROFILE%	Scanning profile used whilst running the scheduled scan. **NOTE** This placeholder is used only for post–scheduled scan reports.
%DURATION%	Scheduled scan duration. **NOTE** This placeholder is used only for post–schedules scan reports.
%ITEMS_COUNT%	Collected items count. **Note** This placeholder is used only for post–scheduled scan reports.

Placeholder	Description
%AUTOREMED_ MISSINGPATCHES%	Used in the report if Auto–remediate Missing Patches option is enabled for the scheduled scan. **NOTE** This placeholder is used only for post–scheduled scan reports.
%AUTOREMED_MISSINGSPS%	Used in the report if Auto–remediate Missing Service Packs option is enabled for the scheduled scan. **Note** This placeholder is used only for post–scheduled scan reports.
%AUTOREMED_UNINSTAPPS%	Used in the report if Auto–remediate Uninstall Applications option is enabled for the scheduled scan. **NOTE** This placeholder is used only in post–scheduled scan reports.

4.7.5 Full text searching

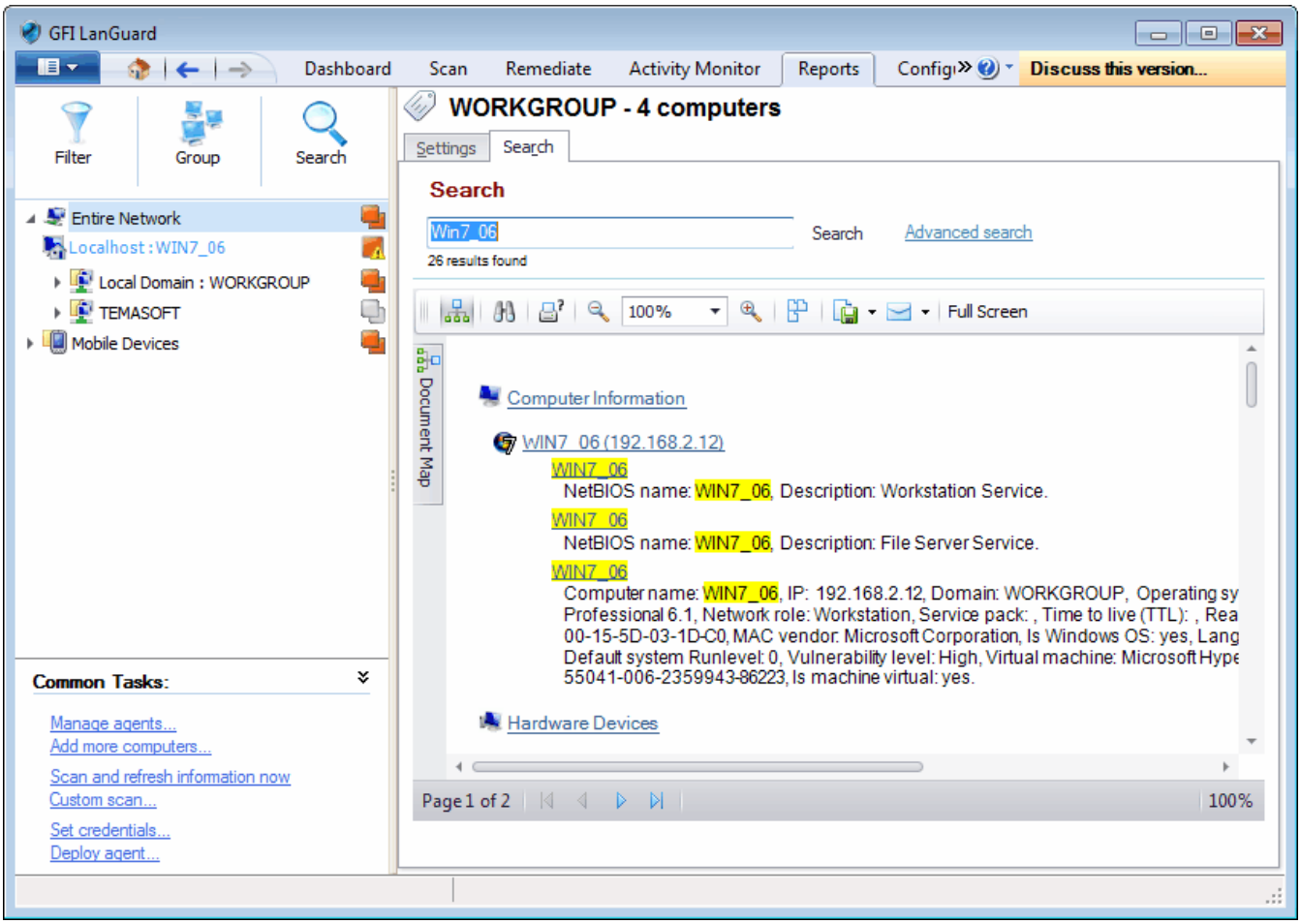
The full text search feature returns results in a structured and configurable manner. Any returned results offer clickable links for further details.

To use the full text search feature:

1. Click **Reports** tab **> Search** sub-tab.

> **NOTE**
> Search can also be accessed from **Computer tree> Search**.

2. Enter you search item and click **Search**.

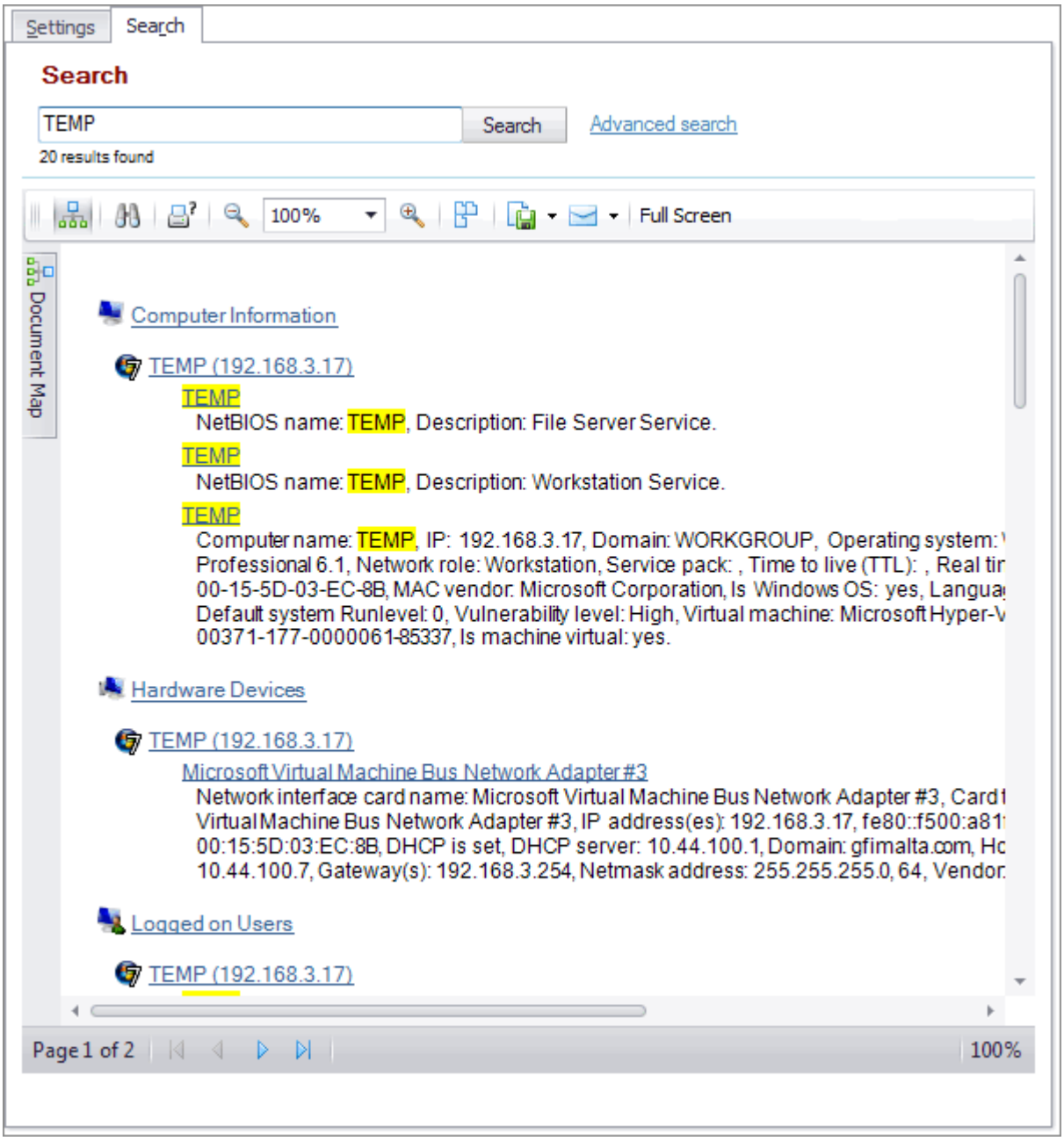


Screenshot 162: Customize the report parameters

3. (Optional) Click **Advanced search** to configure filters to narrow your search results to something more specific.

4. Analyze the search results from the results section at the bottom.

The result contains links that enable you to navigate between computers, software products and vulnerabilities. For example, you can click a missing service pack link to open the missing patches for a specific computer.



Screenshot 163: Navigate using report links

4.8 Data collected from a network audit

When auditing networks, GFI LanGuard enumerates and processes information about system patching status, hardware, software, ports and system information of each scanned machine.

For more information, refer to Interpreting scan results (page 151).

This information is collected from scan targets using the ports and protocols described in the following sections.

Topics in this section:

4.8.1 System Patching Status

GFI LanGuard shows a list of patches missing or deployed on scanned machines, including security and non-security patches of Microsoft operating systems, Mac OS X, major Linux distributions and third-party applications. Various patch management actions can then be taken based on the collected information.

For more information, refer to Missing Service Packs (page 155).

The table below displays a summary of the information gathered by the system patching status:

Data	Description	Ports	Protocol
Missing Service Packs and Update Rollups	Discovers missing Microsoft® and non-Microsoft® service packs.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Missing Security Updates	Discovers missing Microsoft® and non-Microsoft® security patches.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Missing Non-Security Updates	Discovers missing Microsoft® and non-Microsoft® patches unrelated to security.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Installed Service Packs and Update Rollups	Lists installed Microsoft® and non-Microsoft® service packs.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent
Installed Security Updates	Lists installed Microsoft® and non-Microsoft® security patches.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent

Data	Description	Ports	Protocol
Installed Non-Security Updates	Lists installed Microsoft® and non-Microsoft® patches unrelated to security.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » Windows update agent

4.8.2 Hardware

GFI LanGuard displays a hardware audit of each scanned device. In a glance you can see the hardware specification and a list of devices attached during scan.

For more information, refer to Hardware audit (page 158).

The table below displays a summary of the information gathered by the hardware audit.

Data	Description	Ports	Protocol
Network devices	Lists physical and virtual network adapters.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Local drives	Lists drives discovered on scanned target(s). Local drives include: » Hard disks » CD/DVD drives » Floppy drives	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Processors	Lists processors discovered during a scan.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Motherboards	Lists motherboards discovered during a scan.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Memory details	Returns memory information of scanned target(s), including: » Total physical memory » Free physical memory » Total virtual memory » Free virtual memory	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Storage details	Lists every storage device discovered during a scan. Storage devices include: » Hard disks » Virtual hard disks » Removable disks » Floppy drives » CD/DVD drives	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI

Data	Description	Ports	Protocol
Display adapters	Lists video cards discovered during a scan.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
USB Devices	Lists all the detected USB devices that are attached to the network/scan targets.	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI
Other devices	Lists generic devices discovered during a scan, including: » System devices/drivers » Human Interface Devices (HID) » Mouse and keyboard » Communication ports (Serial and Parallel) » Floppy disk controllers » Hard disk controllers	» TCP 139 » TCP 445 » DCOM 135 » DCOM dynamic	» SMB » File and printer sharing » Remote registry » WMI

4.8.3 Ports

GFI LanGuard displays a list of open ports found on the system after a scan.

Apart from detecting open ports, GFI LanGuard uses service fingerprint technology to analyze the services that are running behind the detected open ports. With service fingerprint, GFI LanGuard can detect if malicious software is using the detected open port.

For more information, refer to Open Ports (page 157).

The table below displays a summary of the information gathered by ports node.

Data	Description	Ports	Protocol
Open TCP ports	Checks for open TCP ports	All enabled ports in the scan profile	Windows sockets
Open UDP ports	Checks for open UDP ports	All enabled ports in the scan profile	Windows sockets

4.8.4 Software

The software audit displays the applications, divided by categories, that are installed on scanned computers . For each application, the audit displays details such as application name, publisher and version.

For more information, refer to Software audit (page 158).

The table below displays a summary of the information gathered by the software audit:

Data	Description	Ports	Protocol
General applications	Enumerates every application installed on the scan target(s).	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antiphishing applications	Lists antiphishing applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Antispyware applications	Lists antispyware applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Antivirus applications	Lists antivirus applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Backup applications	Lists backup applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Data Loss Prevention	Lists Data Loss Prevention applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Device Access Control	Lists Device Access Control applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Disk Encryption	Lists Disk Encryption applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Firewall applications	Lists firewall applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Health Agent	Lists system health monitoring applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Instant Messenger	Lists Instant Messenger applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Patch management applications	Lists patch management applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Peer To Peer	Lists Peer to Peer (P2P) applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
URL Filtering	Lists web filtering applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Virtual Machine Software	Lists virtualization software detected on your network.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Virtual Private Network (VPN) Client applications	Lists VPN client applications.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Web Browser applications	Lists web browsers.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

NOTE

For a full list of supported security applications including vendors and products, refer to http://go.gfi.com/?pageid=security_app_fullreport

4.8.5 System Information

GFI LanGuard displays various system details of scanned machines, such as information about the operating system, password and security policies and applications automatically launched at system startup.

For more information, refer to System Information (page 159).

The information gathered by the System Information node includes:

Data	Description	Ports	Protocol
Shares	Lists all shares discovered during a scan. Information includes: » Share name » Share remark » Share path » Share permissions	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Password policy	Lists the password policy configuration.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Security audit policy	Security audit policy configuration.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Registry	Lists selected information from the system registry. Amongst others, enumerated information includes: » Registry owner » Current build number » Current type » Current version » Vendor identifier » Software type	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
NetBIOS names	Lists NetBIOS names of the scanned target(s). This node includes: » Workstation service » Domain name » File server services » Browser service elections	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Computer	Lists computer identifiers including: » MAC address » Time to live » Network role » OS Serial number » Language » Machine type (physical or virtual)	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Groups	Lists local or domain/workgroup groups.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Users	Lists local or domain/workgroup users.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Logged on users	Lists locally and remotely logged on users.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Sessions	Lists the active sessions at the time of the scan.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Services	Lists every service discovered during a scan.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

Data	Description	Ports	Protocol
Processes	Lists every active process discovered during a scan.	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry
Remote TOD (time of day)	Lists the current time and uptime of the scanned target(s).	» TCP 139 » TCP 445	» SMB » File and printer sharing » Remote registry

4.9 Common Vulnerabilities and Exposures (CVE)

GFI LanGuard is CVE certified. This topic describes how CVE certification is used in GFI LanGuard.

CVE (Common Vulnerabilities and Exposures) is a list of standardized names for vulnerabilities and other information security exposures. Its aim is to standardize the names for all publicly known vulnerabilities and security exposures.

CVE is a dictionary which aim is to facilitate data distribution across separate vulnerability databases and security tools. CVE makes searching for information in other databases easier and should not be considered as a vulnerability database by itself.

CVE is a maintained through a community–wide collaborative effort known as the CVE Editorial Board. The Editorial Board includes representatives from numerous security–related organizations such as security tool vendors, academic institutions, and governments as well as other prominent security experts. The MITRE Corporation maintains CVE and moderates editorial board discussions.

About CVE Compatibility

"CVE–compatible" means that a tool, Web site, database, or service uses CVE names in a way that allows it to cross–link with other repositories that use CVE names. CVE–compatible products and services must meet the four requirements:

Compatibility	Description
CVE Searchable	A user must be able to search for vulnerabilities and related information using the CVE name.
CVE Output	Information provided must include the related CVE name(s).
Mapping	The repository owner must provide a mapping relative to a specific version of CVE, and must make a good faith effort to ensure accuracy of that mapping.
Documentation	The organization's standard documentation must include a description of CVE, CVE compatibility, and the details of how its customers can use the CVE–related functionality of its product or service.

Note

For an in–depth understanding of CVE compatibility refer to the complete list of CVE requirements available at http://go.gfi.com/?pageid=LAN_CVE_Requirements

About CVE and CAN

CVE names (also called "CVE numbers," "CVE–IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. CVE names have "entry" or "candidate" status. Entry status indicates that the CVE

name has been accepted to the CVE List while candidate status (also called "candidates," "candidate numbers," or "CANs") indicates that the name is under review for inclusion in the list.

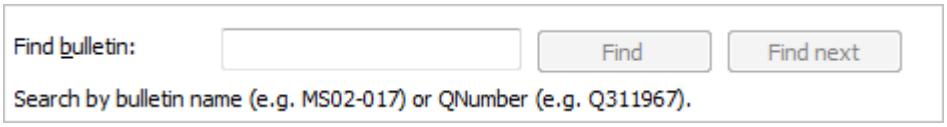
Each CVE name includes the following:

- CVE identifier number (i.e. "CVE–1999–0067").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL–ID).

> **NOTE**
> For an in–depth understanding of CVE names and CANs, refer to: http://go.gfi.com/?pageid=cvecert

Searching for CVE Entries

CVE entries can be searched from the Scanning profiles node within the Configuration tab.



Screenshot 164: Searching for CVE information

To search for a particular CVE bulletin:

1. Specify the bulletin name (for example, CVE–2005–2126) in the search tool entry box included at the bottom of the right pane.

2. Click on **Find** to start searching for your entry.

Obtaining CVE Names

CVE entry names can be obtained through the GFI LanGuard user interface from within the Scanning profiles node within the Configuration tab. By default, the CVE ID is displayed for all the vulnerabilities that have a CVE ID.

Importing and Exporting CVE Data

CVE data can be exported through the impex command line tool. For more information, refer to Using impex.exe (page 284).

5 Settings

GFI LanGuard enables you to run vulnerability scans straight out of the box – using the default settings configured prior to shipping. If required you can also customize these settings to suit any particular vulnerability management requirements that your organization might need. You can customize and configure various aspects of GFI LanGuard including scan schedules, vulnerability checks, scan filters and scan profiles.

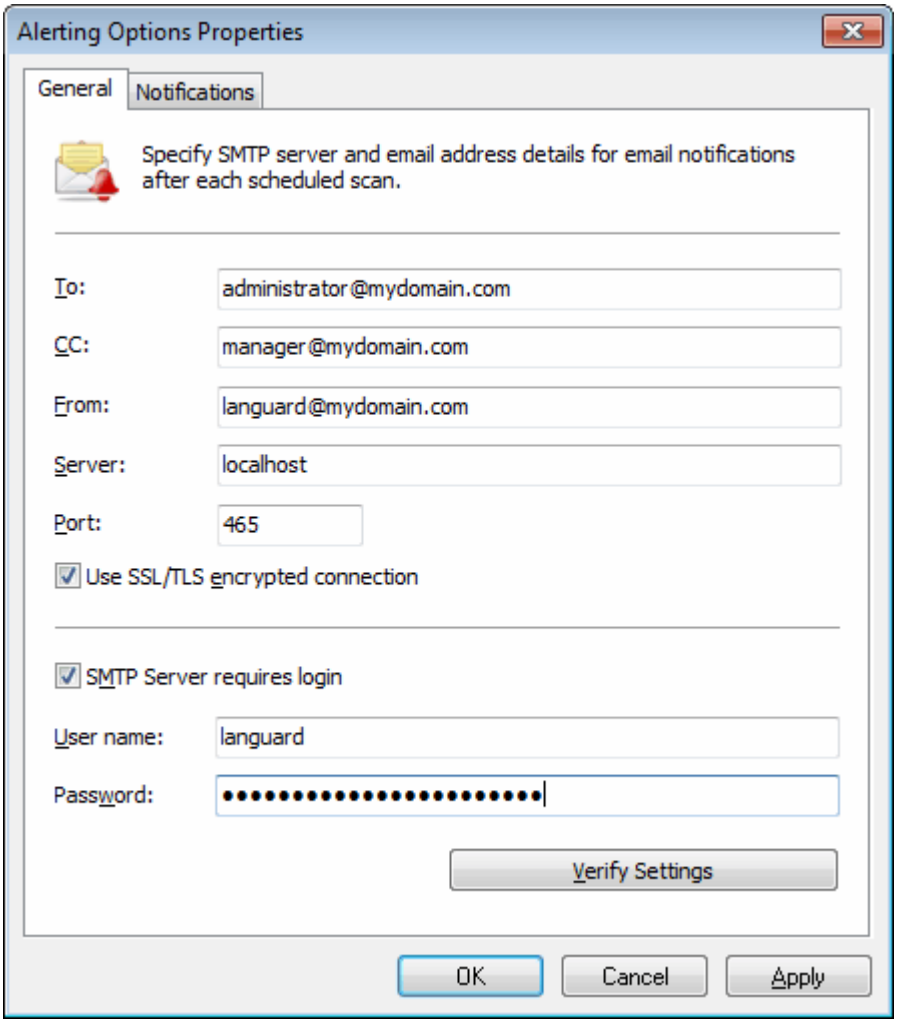
Topics in this section:

5.1 Configuring Alerting Options

To configure alerting options:

1. Click **Configuration** tab **> Alerting options**.

2. Click the link in the right pane.



Screenshot 165: Configuring Alerting Options

3. Key–in the parameters described below:

Option	Description
To	The recipient email address. Emails sent by GFI LanGuard are received by this email address.
CC	Key–in another email address in this field if you need to send a copy to another email address.
From	The sender email address. GFI LanGuard will use this email account to send the required emails.
Server	Defines the server through which emails are routed. This can be either an FQDN (Fully Qualified Domain Name) or an IP Address.
Port	Defines the IP port through which emails are routed. Default value is 25
Use SSL/TLS encrypted connection	Select this option if you have an SSL (Secure Sockets Layer Protocol) or TLS (Transport Layer Security Protocol) encrypted connection to send the required emails.

Option	Description
SMTP Server requires login	Select this option if the SMTP server requires a username and password to authenticate.

4. Click on the **Verify Settings** button to verify email settings.

5. Select **Notifications** and configure the following options:

Option	Description
Enable daily digest	Receive daily report with all changes made on the entire network. Configure the time when the daily digest email is received.
Report format	Specify the report format received by email.
Send an email on new product news	Receive an email containing new product news.

6. Click **OK**

5.2 Configuring Database Maintenance Options

GFI LanGuard ships with a set of database maintenance options through which you can maintain your scan results database backend in good shape.

For example, you can improve product performance and prevent your scan results database backend from getting excessively large by automatically deleting scan results that are older than a specific number of months.

If you are using an Access™ database backend, you can also schedule database compaction. Compaction enables you to repair any corrupted data and to delete database records marked for deletion in your database backend; ensuring the integrity of your scan results database. The following sections provide you with information about:

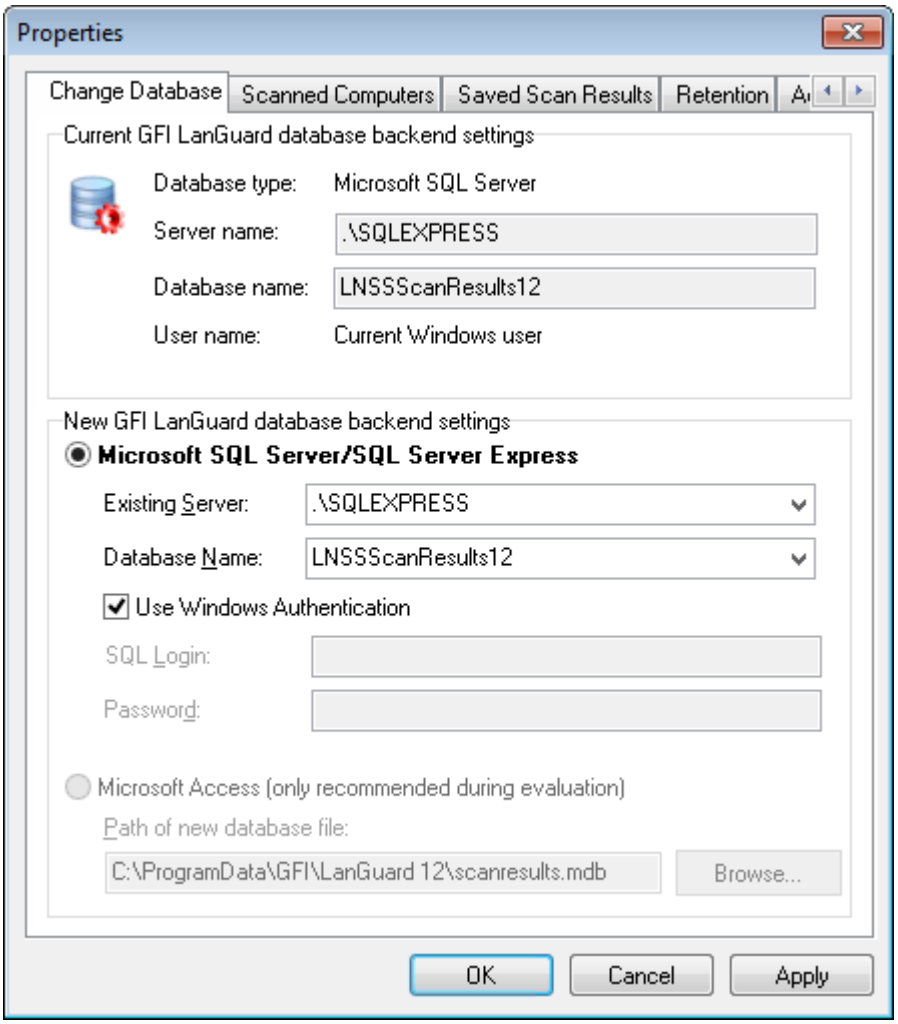
- Using SQL Server® as a database backend
- Managing saved scan results
- List scanned computers
- Configure advanced database maintenance options
- Configure database retention options

Using SQL Server® as a database backend

> **IMPORTANT**
> It is highly recommended to use SQL Server® once product evaluation is exceeded.

To store scan results in an SQL Server® database:

1. Click **Configuration** tab **> Database Maintenance Options > Database backend settings**.



Screenshot 166: SQL Server® database backend options

2. Select the **MS SQL Server** option and choose the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

3. Specify the SQL Server credentials or select the **Use Windows Authentication** option to authenticate to the SQL server using windows account details.

4. Click **OK** to finalize your settings.

> **NOTE**
> If the specified server and credentials are correct, GFI LanGuard automatically logs on to your SQL Server and create the necessary database tables. If the database tables already exist, it re–uses them.

> **NOTE**
> When using Windows Authentication credentials, make sure that GFI LanGuard services are running under an account that has both access and administrative privileges on the SQL Server databases.

5. Click **Yes** to stop all current scans.

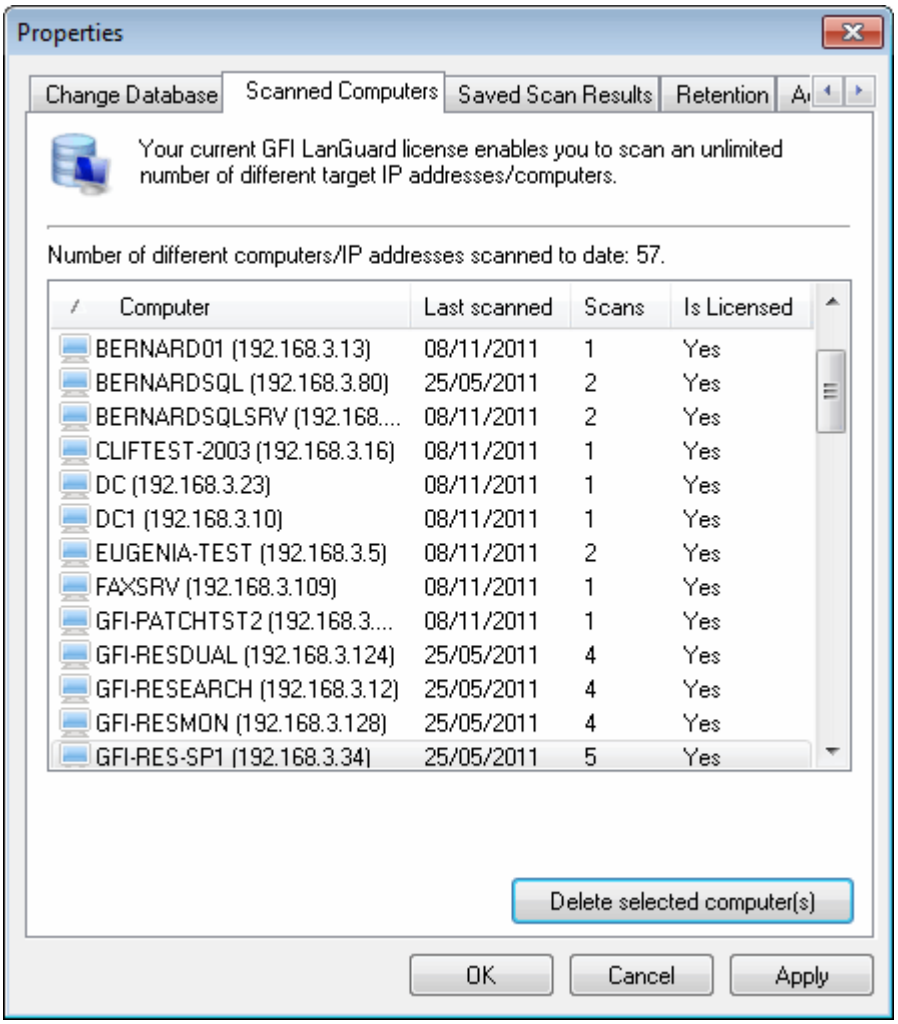
6. If the current Access™ database contains data, click **OK** to transfer all scan data to the SQL Server® database.

Managing saved scan results

Use the **Saved Scan Results** tab to maintain your database backend and delete saved scan results that are no longer

required. Deletion of non–required saved scan results can be achieved manually as well as automatically through scheduled database maintenance.

During scheduled database maintenance, GFI LanGuard automatically deletes saved scan results that are older than a specific number of days/weeks or months. You can also configure automated database maintenance to retain only a specific number of recent scan results for every scan target and scan profile.



Screenshot 167: Database maintenance properties: Managed saved scan results tab

To manage saved scan results:

1. Click on the **Configuration** tab **> Database Maintenance Options > Manage saved scan results**.

2. To delete saved scan results, select the particular result(s) and click **Delete Scan(s)**.

3. To let GFI LanGuard manage database maintenance for you, select **Scans generated during the last** to delete scan results, which are older than a specific number of days/weeks, or months or **Scans per scan target per profile in number of** to retain only a specific number of recent scan results.

List scanned computers

GFI LanGuard maintains a global list of scanned computers for licensing purposes. Any computers in excess of what is specified in the licensing information are not scanned.

GFI LanGuard enables systems administrators to delete scanned computers in order to release licenses that were previously utilized.

To delete computers previously scanned:

1. Click **Configuration** tab **> Database Maintenance Options > Manage list of scanned computers**.

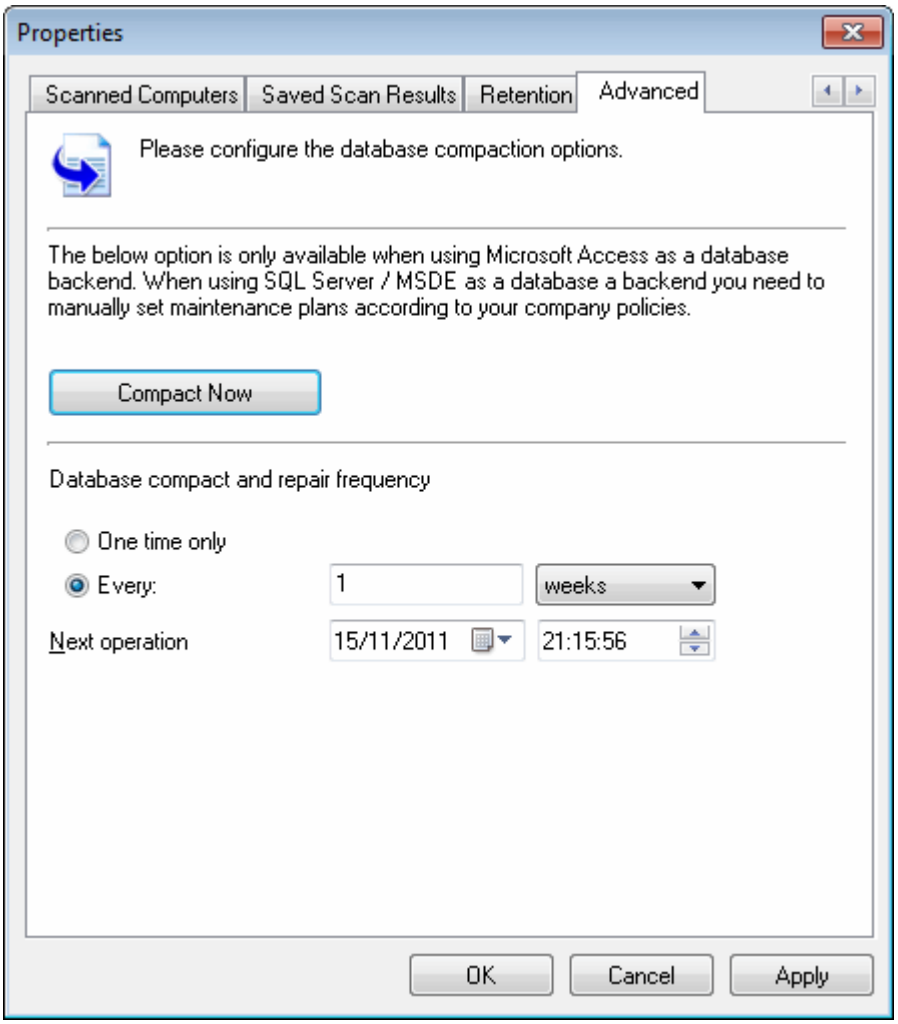
2. Select the computers to delete and click **Delete selected computer(s)**.

> **IMPORTANT**
> Deleting computers from the database is a one–way operation that will also delete all computer related data from the database. Once deleted, this data is no longer available.

Configure advanced database maintenance options

GFI LanGuard enables you to repair and compact the Access™ database backend automatically to improve performance.

During compaction, the database files are reorganized and records that have been marked for deletion are removed. In this way, you can regain used storage space. During this process, GFI LanGuard also repairs corrupted database backend files. Corruption may occur for various reasons. In most cases, a Access™ database is corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, unresponsive operations forced reboots, and so on).



Screenshot 168: Database Maintenance properties: Advanced tab

To compact and repair a Access™ database backend:

1. Click **Configuration** tab **> Database Maintenance Options > Database maintenance plan**.

2. To manually launch a repair and compact process on an Access™ database backend, click **Compact Now**.

3. To automate the repair and compact process on an Access™ database backend select:

- **One time only** - to schedule a onetime Access™ database repair and compact
- **Every** - to execute a repair and compact process on a regular schedule.

Specify the date, time and frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

Configure database retention options

Database retention options enable you to keep your database clean and consistent, by configuring GFI LanGuard to automatically delete unwanted scan results and scan history information while retaining important ones.

To configure retention settings:

1. Click **Configuration** tab **> Database Maintenance Options > Database backend settings > Retention** tab.

2. Configure the options described below:

Option	Description
Keep scans generated during the last	Keep scan results generated during the specified number of days/weeks/months.
Keep scans per scan target per profile number of	Specify the number of scan results to keep, for every scan target by every scan profile.
Never delete history	Select this option if you want to keep all scan history.
Keep history for the last	Keep scan history for the specified number of days/weeks/months.

3. Click **OK**

5.3 Configuring Program Updates

This tool enables GFI LanGuard to detect the latest vulnerabilities and maintain its scanning performance. Configure GFI LanGuard to auto–download updates released by GFI to improve functionalities in GFI LanGuard. These updates also include checking GFI web site for newer builds. Updates can be enabled/disabled by selecting the checkbox in the **Auto–download** column.

GFI LanGuard can download all Unicode languages. This includes (but is not limited to) English, German, French, Italian, Spanish, Arabic, Danish, Czech, Finnish, Hebrew, Hungarian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Portuguese/Brazilian, Russian, Swedish, Chinese, Chinese (Taiwan), Greek, and Turkish.

The following sections provide you with information about:

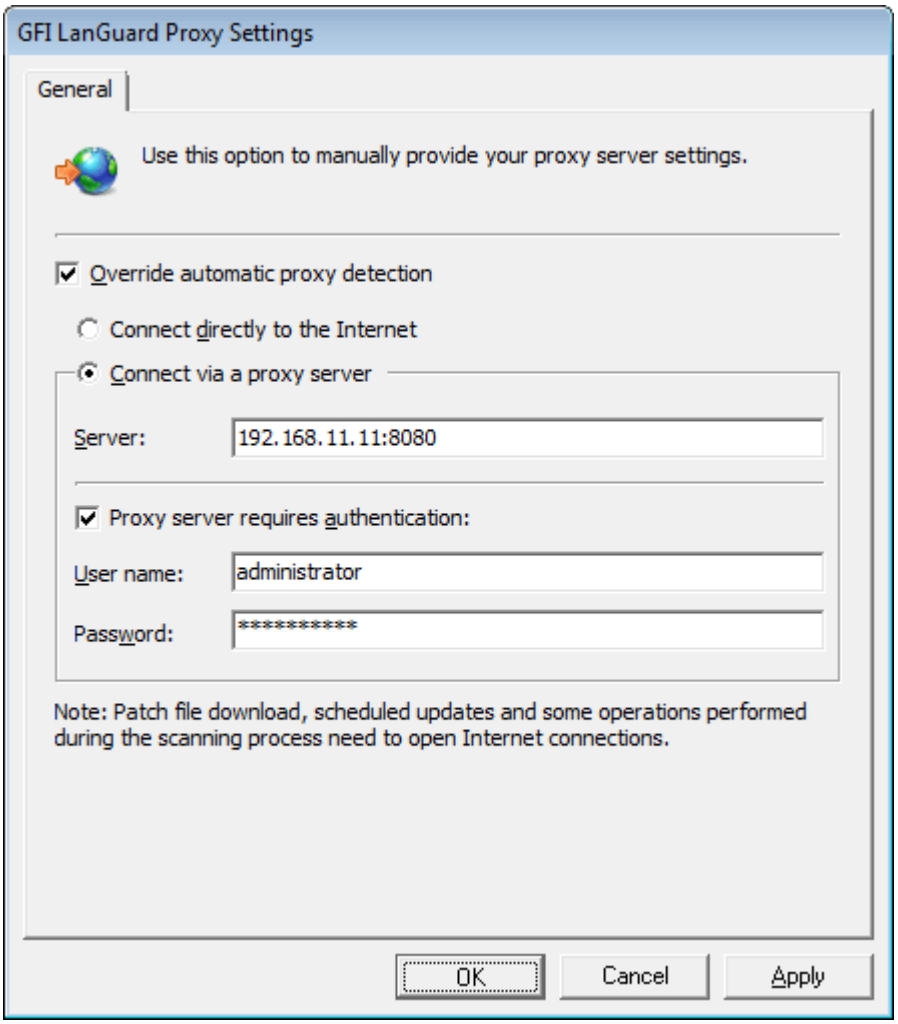
- Configuring proxy settings
- Configuring auto-update options
- Installing program updates manually

Configuring proxy settings

To manually configure proxy server settings for Internet updates:

1. Click on **Configuration** tab **> Program Updates**.

2. From **Common Tasks** select **Edit proxy settings**.



Screenshot 169: Configuring proxy server settings

3. Select **Override automatic proxy detection;** configure the options described below:

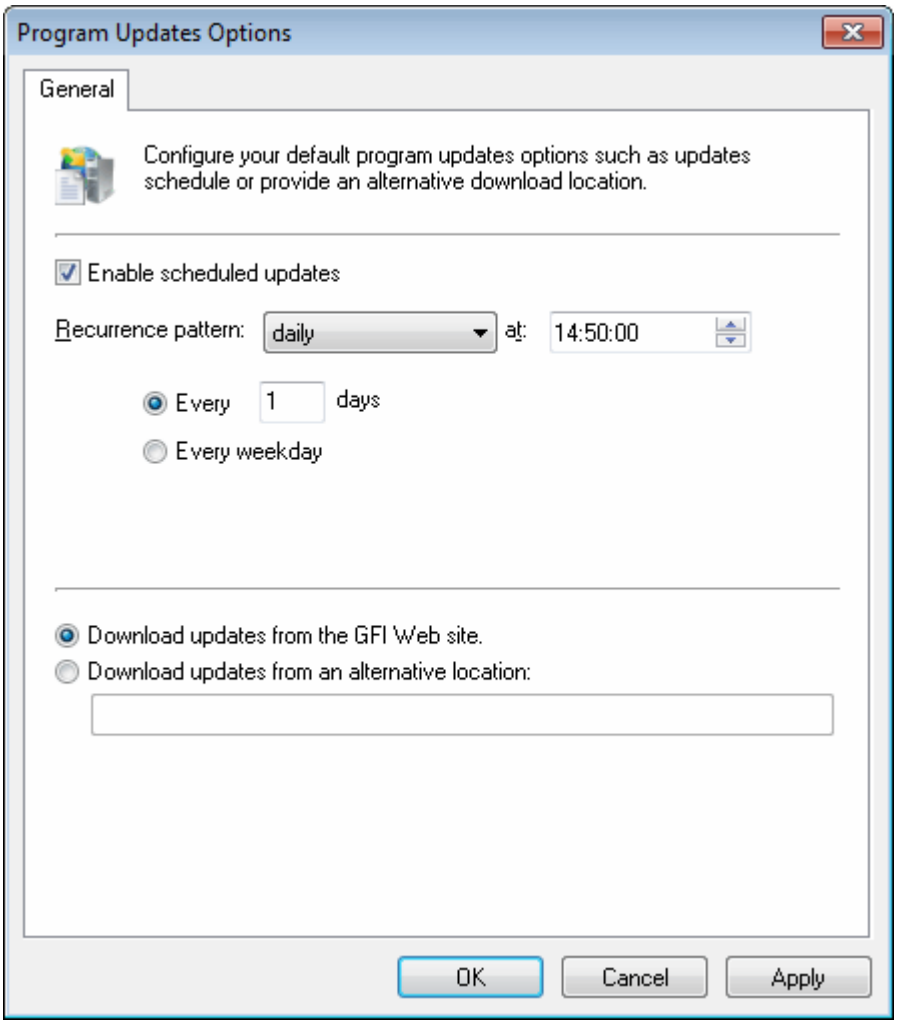
Option	Description
Connect directly to the Internet	A direct Internet connection is available.
Connect via a proxy server	Internet access is through a proxy server. Update the Server name and port number using this format <server>:<port>
Proxy server requires authentication	(Optional) Enter username and password if required by the proxy server.

4. Click **OK**

Configuring auto-update options

GFI LanGuard can check for the availability of software updates at every program startup. To disable/enable this feature

1. Click on **Configuration** tab **> Program Updates**. From **Common Tasks** select **Edit program updates options**.



Screenshot 170: Configure updates at application startup

2. Select/unselect **Check for updates at application startup** to enable/disable auto update checks at application startup.

3. Select/unselect enable scheduled updates to configure the frequency of update checks.

4. Specify whether GFI LanGuard download updates from GFI website or from an alternative location.

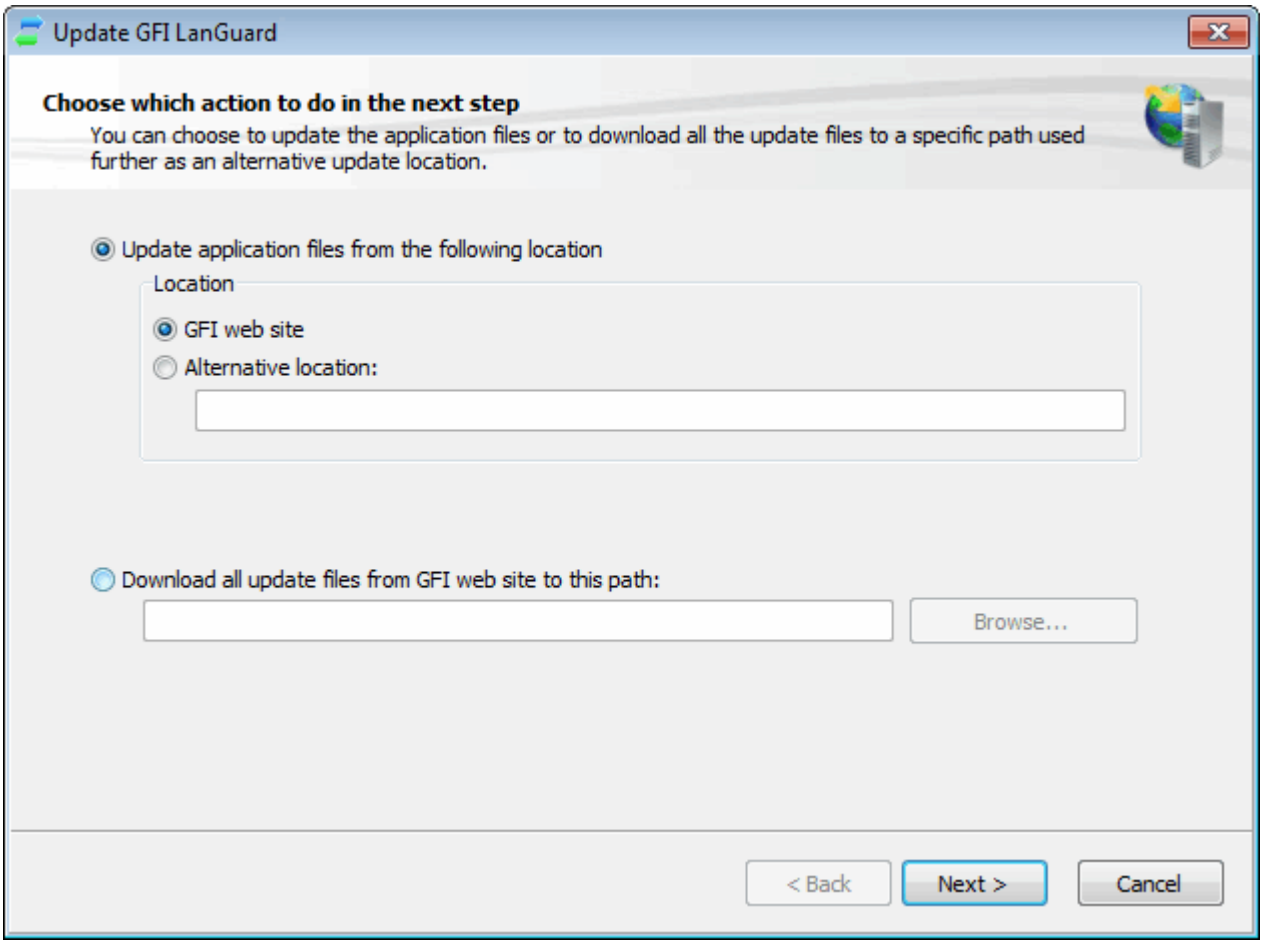
5. Click **OK**

Installing program updates manually

To start GFI LanGuard program updates manually:

1. Click on **Configuration** tab **> Program Updates**.

2. From **Common Tasks** click **Check for updates**.



Screenshot 171: Check for Updates wizard

3. Specify the location from where the required update files will be downloaded.

4. (Optional) Change the default download path, select **Download all update files…** to this path to provide an alternate download path to store all GFI LanGuard updates.

5. Click **Next** to proceed with the update.

6. Select the updates and click **Next**.

7. Click **Start** to start the update process.

> **NOTE**
> If having problems when downloading updates, check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to Gateway permissions (page 22).

5.4 Limiting Database Size

GFI LanGuard enables you to work with either Microsoft SQL Server or Microsoft SQL Server Express as database backend.

> **NOTE**
> Microsoft SQL Server Express edition is free but places limits on database size. We recommend using Microsoft SQL Server Express for GFI LanGuard deployments managing up to 2,000 computers or devices. For larger deployments, use Microsoft SQL Server Standard Edition which is not free but has an upper limit of 524 Petabytes.

NOTE

If your database reaches the limit of your SQL Server Express version, you will begin to experience errors due to the inability of the database tables to accept new data.

The following is a list with some brief information about some SQL Server Express edition versions and their size limits:

- 2008 Express - 4 GB
- 2008 R2 Express - 10 GB
- 2012/2014/2016 Express - 10 GB

5.4.1 Methods to avoid database limitation issues

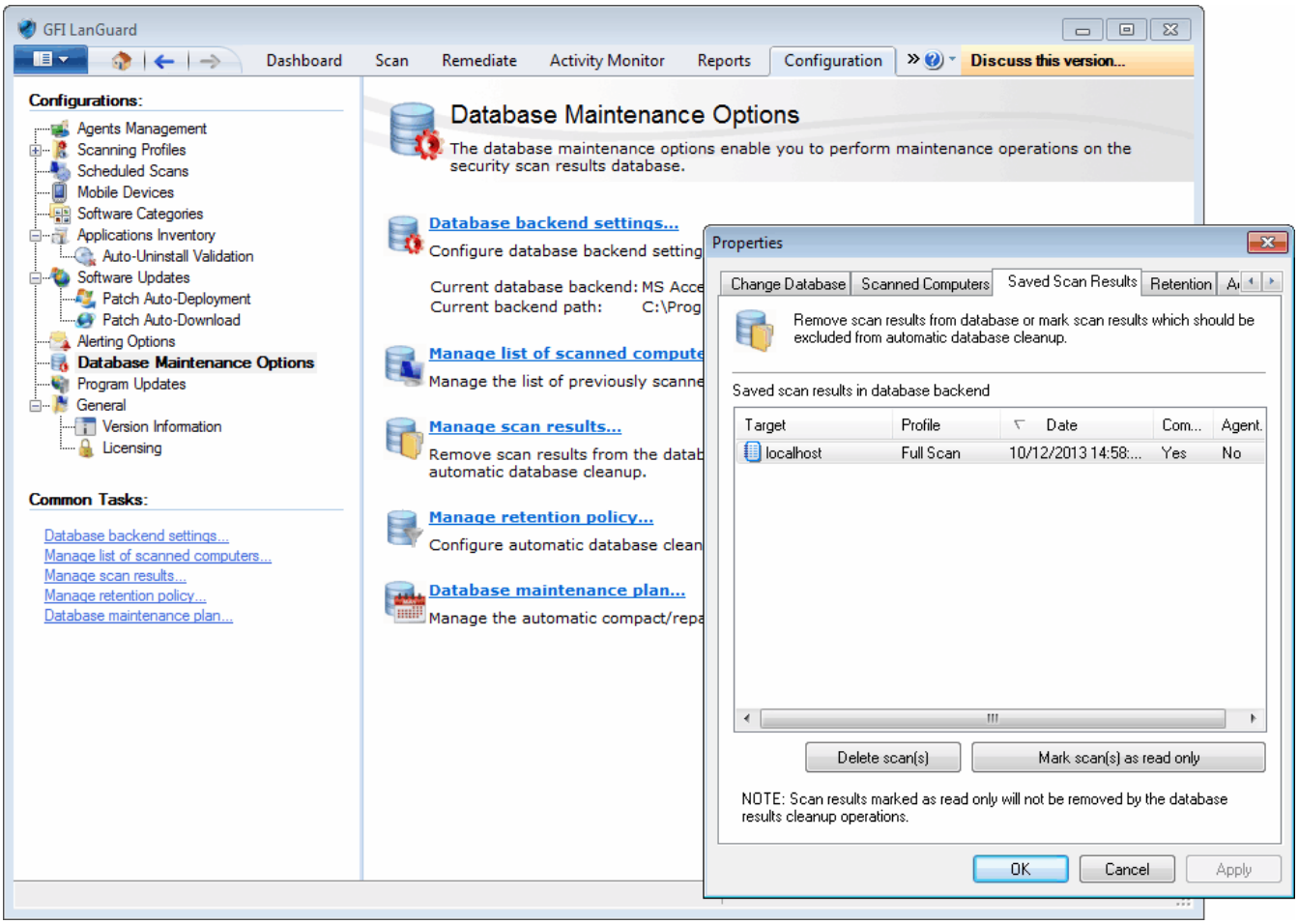
Upgrade database

- If you are currently using an Access database we highly recommend upgrading to a Microsoft SQL Server or Microsoft SQL Server Express database.
- When you migrate your database from Access to SQL Server or SQL Server Express, GFI LanGuard automatically copies your data to the new database so no data is lost.

Delete old scans manually or automatically

To delete manually:

1. Click **Configuration** tab > **Database Maintenance Options**.
2. Select **Manage Scan Results** and delete old and unneeded scans.

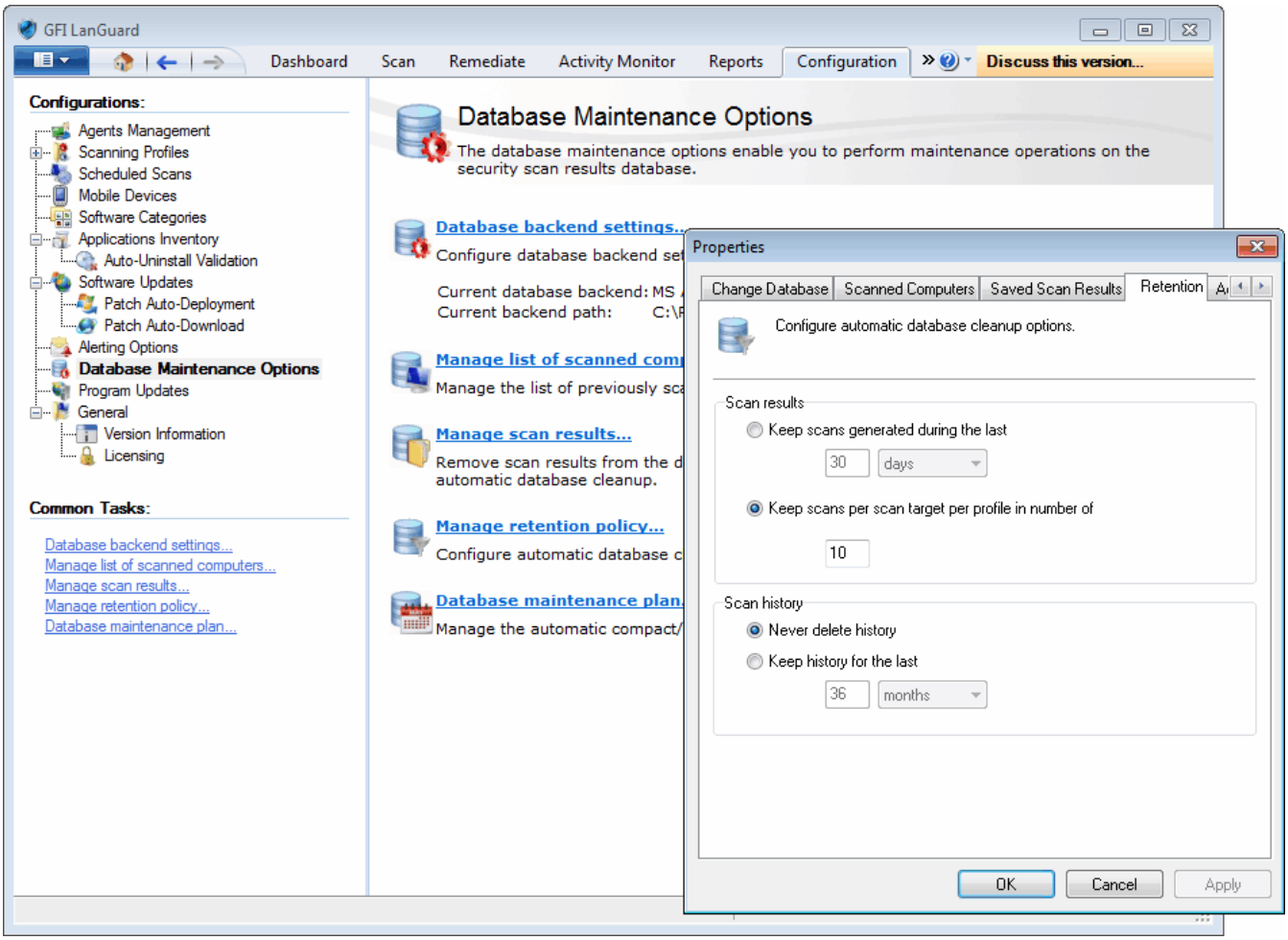


Screenshot 172: Deleting Old Scans Manually

To delete automatically:

1. Click **Configuration** tab > **Database Maintenance Options**.

2. Select **Manage Retention Policy** and set the retention policy that fits your needs.



Screenshot 173: Deleting Old Scans Automatically

Backup

To back up a Microsoft SQL Server Database use the instructions at:

http://go.gfi.com/?pageid=LAN_SQLDatabaseBackupMSDN

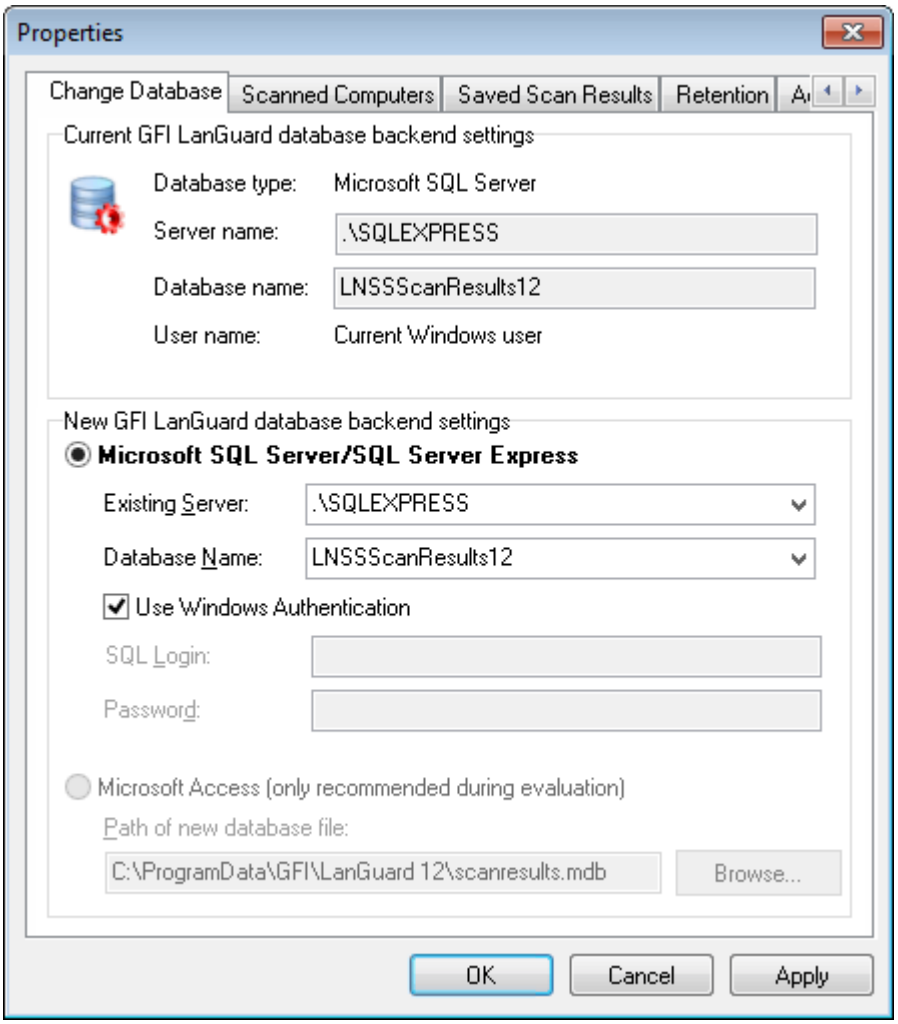
To clean-up your database:

1. Go to **Configuration > Database Maintenance Options > Database backend settings…**

2. Disconnect GFI LanGuard from the database you've backed up and you want to delete, by connecting to another temporary database (eventually Access database) .

3. Delete the database from the SQL Server using SQL Server Management Studio.

4. Go to GFI LanGuard under **Configuration > Database Maintenance Options > Database backend settings…** and reconnect to the SQL Server.



Screenshot 174: Microsoft SQL Server/SQL Server Express Database

5.5 Scanning Profile Editor

The scanning profiles that ship with GFI LanGuard are already pre–configured to run a number of vulnerability checks on selected target. You can however disable vulnerability scanning as well as customize the list of vulnerability checks executed during a scan. Scans can be modified through the **Scanning Profile Editor**.

Topics in this section:

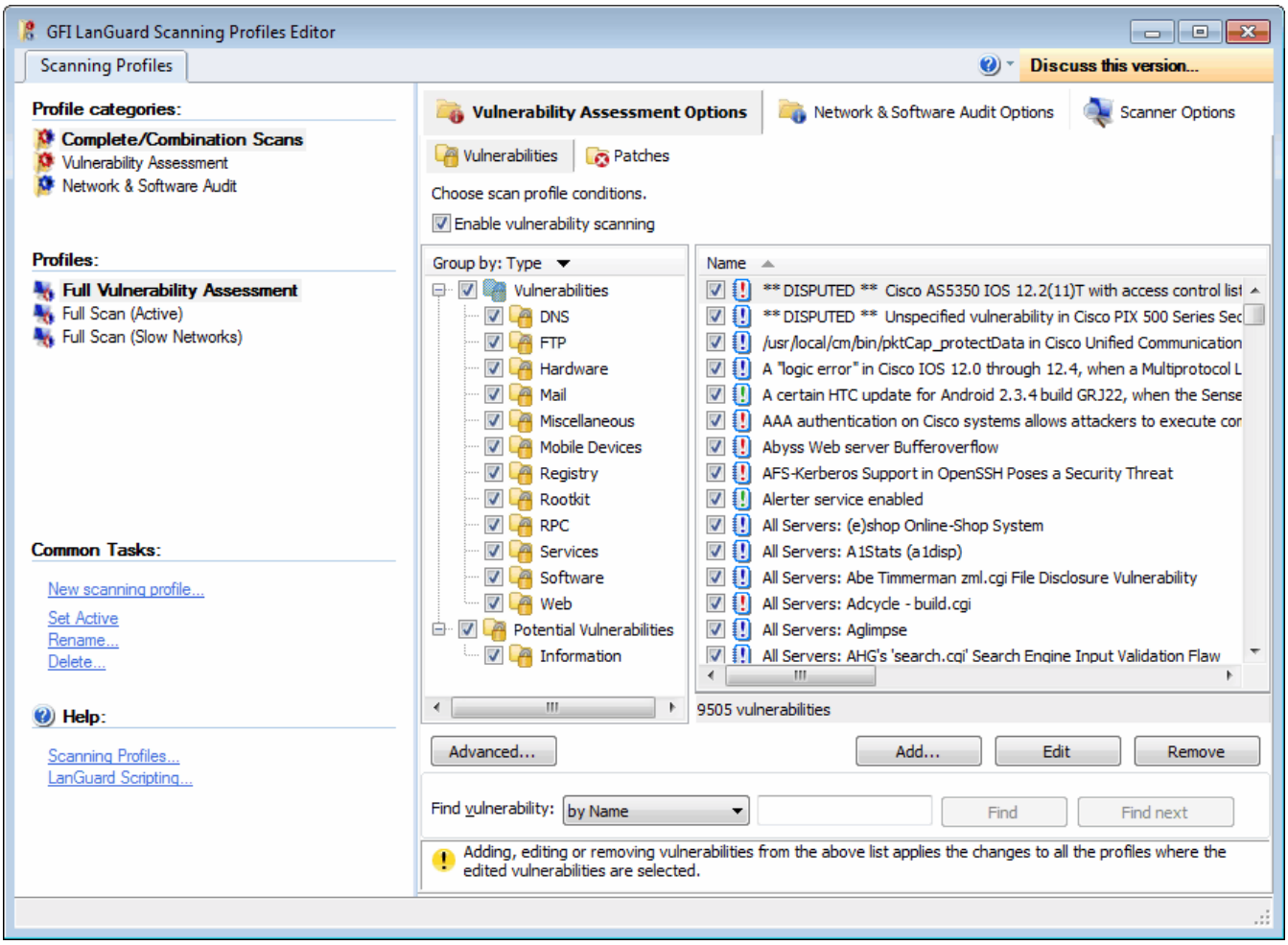
5.5.1 Create a new Scanning Profile

The **Scanning Profiles Editor** enables you to create new scanning profiles. To create a new custom scanning profile:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. In **Scanning Profiles Editor** from **Common Tasks**, click **New scanning profile**.



Screenshot 175: The Scanning Profile Editor

4. Specify the name of the new profile and optionally select **Copy all settings from an existing profile** to clone settings from an existing profile.

5. Click **OK** to save settings. The new scanning profile is added under **Profiles** in the left pane.

5.5.2 Configuring Vulnerabilities

The **Vulnerability Assessment Options** tab enables you to configure which Microsoft® /non-Microsoft® and Security/non-Security updates are checked when scanning targets with the selected profile.

The following sections provide you with information about:

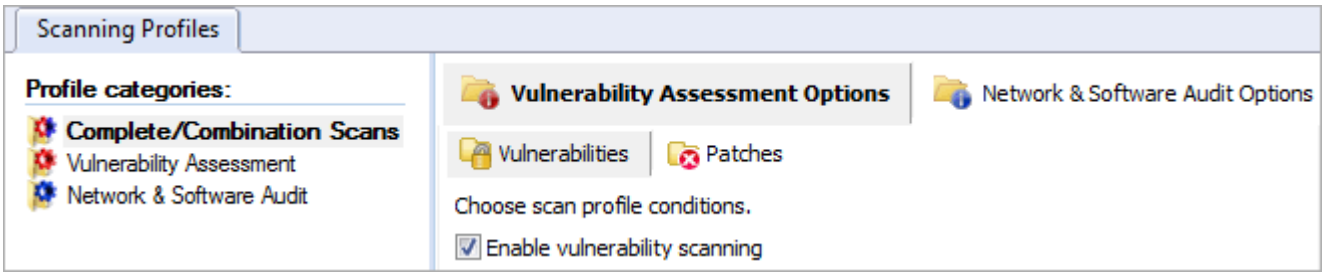
- Enabling vulnerability scanning
- Customizing the list of vulnerabilities to be scanned
- Customizing vulnerability checks properties
- Setting up vulnerability check conditions

Enabling vulnerability scanning

To enable vulnerability scanning:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.



Screenshot 176: Enabling vulnerability scanning for the selected scanning profile

3. From the **Vulnerability Assessment Options** tab, click **Vulnerabilities** sub–tab.

4. Select the scanning profile to customize from the left pane under **Profiles**.

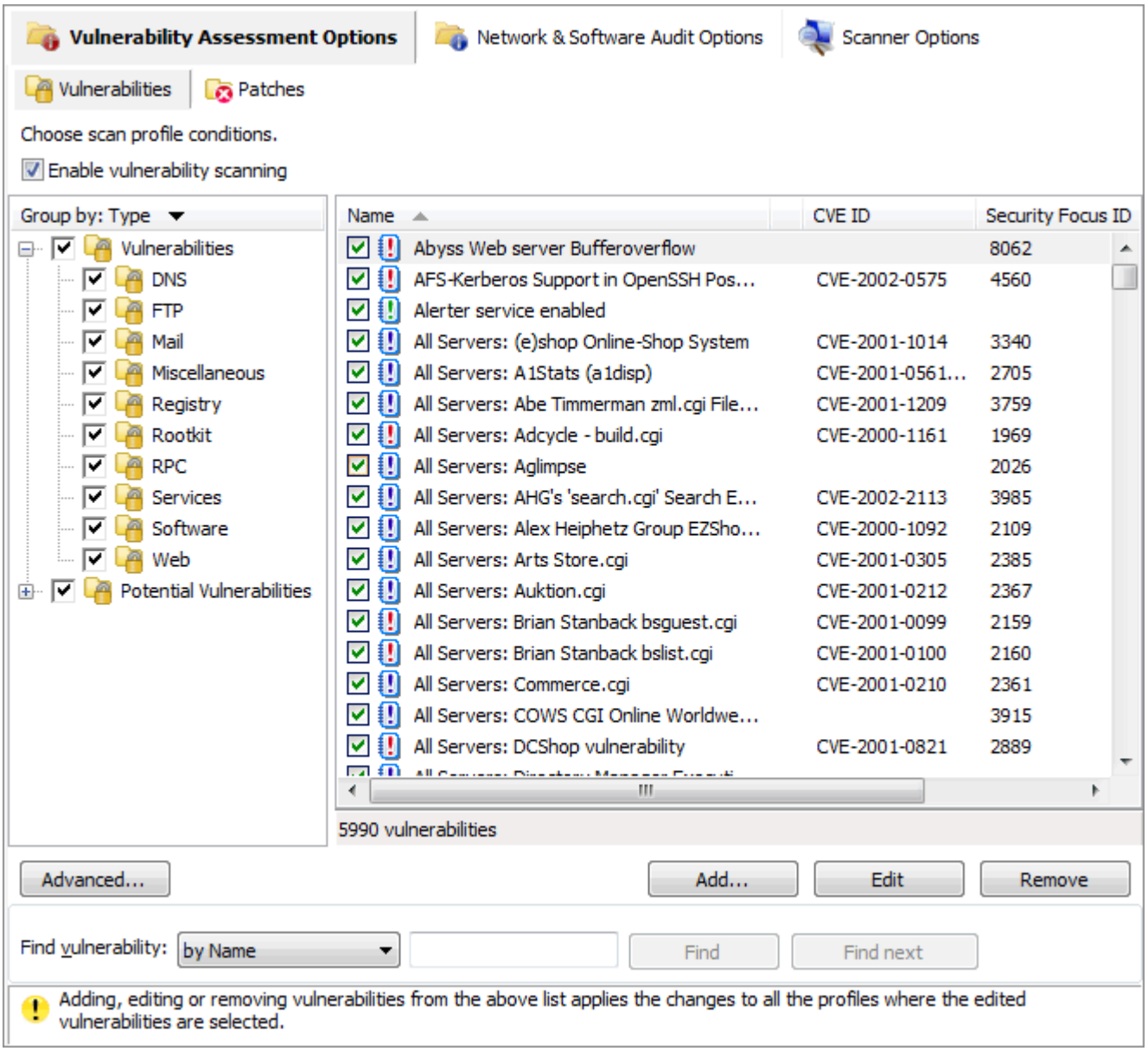
5. In the right pane, select **Enable Vulnerability Scanning**.

> **NOTE**
> Vulnerability scanning is configured on a scan profile by scan profile basis. If in a particular profile this option is not selected, no vulnerability tests will be performed in the security audits carried out by this scanning profile.

Customizing the list of vulnerabilities to be scanned

To specify which vulnerabilities will be enumerated and processed by a scanning profile during a security audit:

1. From **Vulnerability Assessment Options** tab, select the scanning profile to customize from the left pane under **Profiles**.

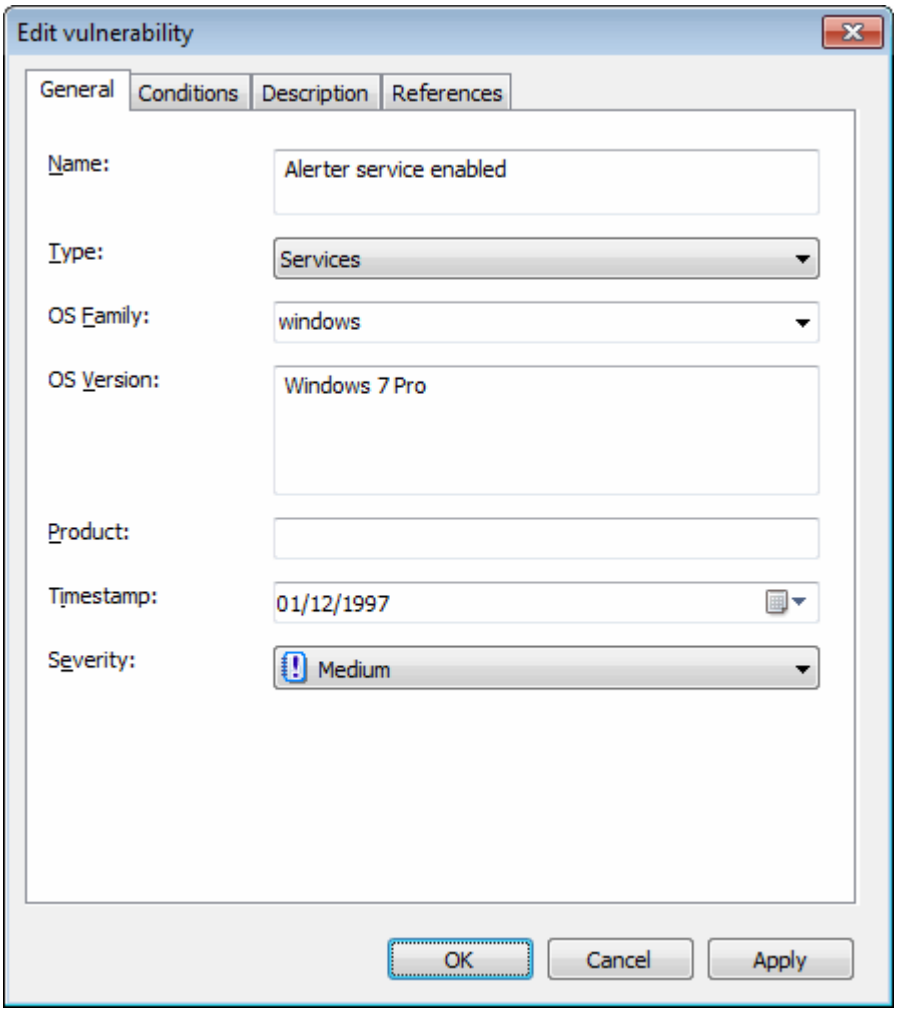


Screenshot 177: Select the vulnerability checks to be run by this scanning profile

2. In the right pane, select the vulnerability checks to execute through this scanning profile.

Customizing vulnerability checks properties

All the checks listed in the **Vulnerabilities** tab have specific properties that determine when the check is triggered and what details will be enumerated during a scan.



Screenshot 178: Vulnerability properties dialog: General tab

To change the properties of a vulnerability check:

1. Right–click on the vulnerability to customize, select **Properties**.

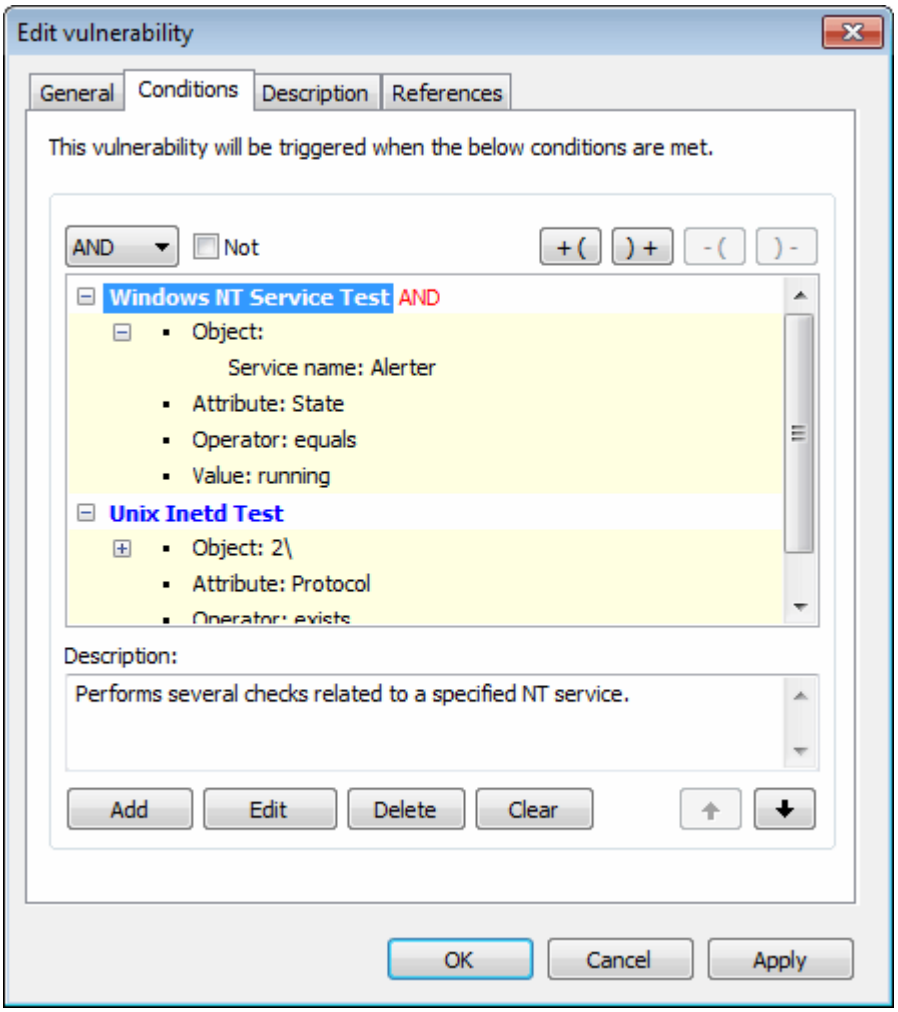
2. Customize the selected vulnerability check from the tabs described below:

Tab	Description
General	Use this tab to customize the general details of a vulnerability check including vulnerability check name, vulnerability type, OS family, OS version, Product, Timestamp and Severity.
Conditions	Use this tab to configure the operational parameters of this vulnerability check. These parameters will define whether a vulnerability check is successful or not.
Description	Use this tab to customize the vulnerability check description.
References	Use this tab to customize references and links that lead to relevant information in the OVAL, CVE, MS Security, Security Focus and SANS TOP 20 reports.

3. Click on **OK** to save your settings.

Setting up vulnerability check conditions

The **Conditions** tab enables you to add or customize conditions, which define whether the computer or network being scanned is vulnerable, or not. It is therefore of paramount importance that any custom checks defined in this section are set–up by qualified personnel that are aware of the ramifications of their actions.

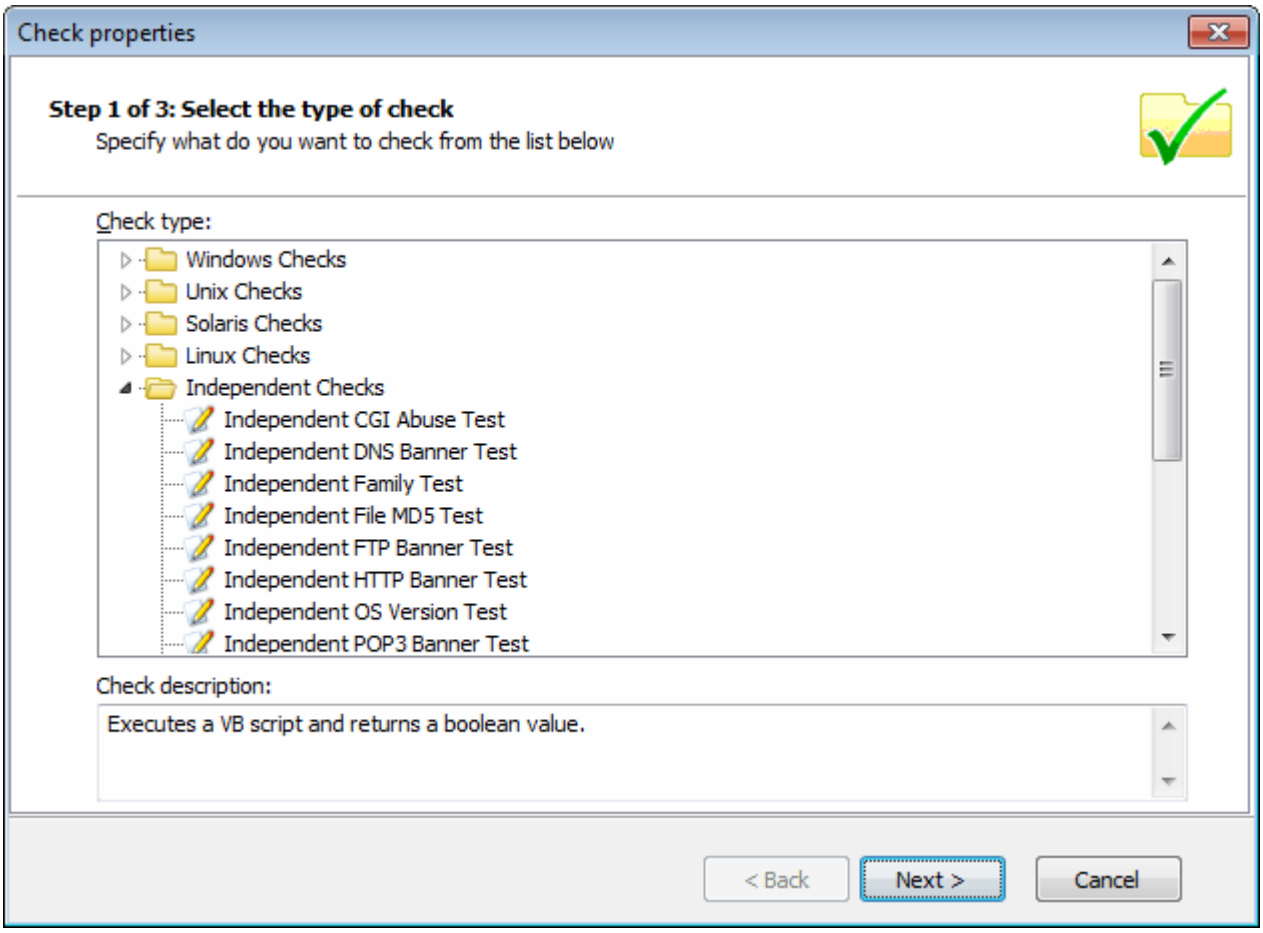


Screenshot 179: Vulnerability conditions setup tab

To add a vulnerability check condition:

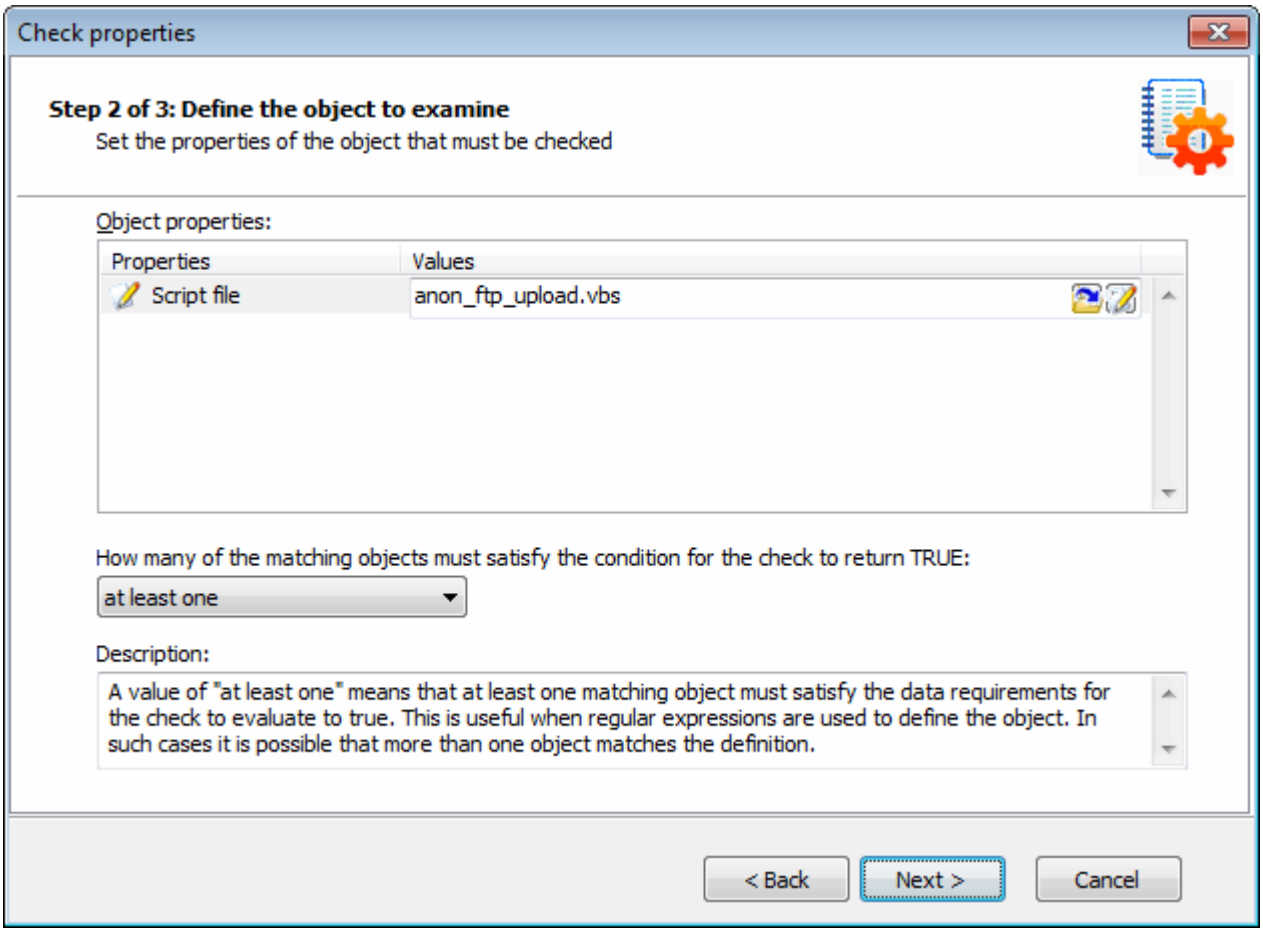
1. From **Vulnerability Assessment Options** tab **> Vulnerabilities** sub-tab, right-click a vulnerability from the list of vulnerabilities and select **Properties**.

2. From the **Edit vulnerability** dialog, click **Conditions** tab **>Add**.



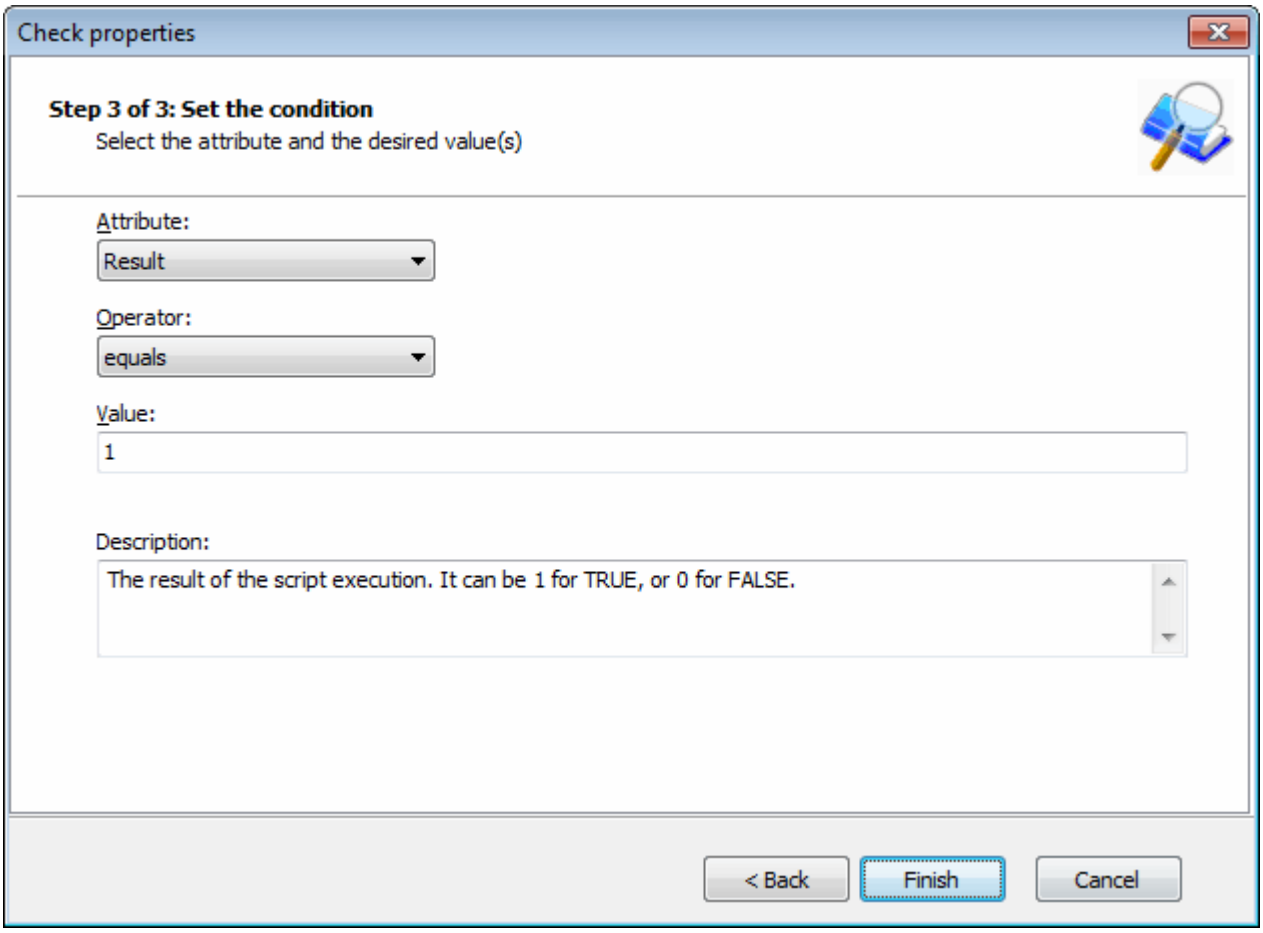
Screenshot 180: Check properties wizard - Select check type

3. Select the type of check to be configured and click **Next**.



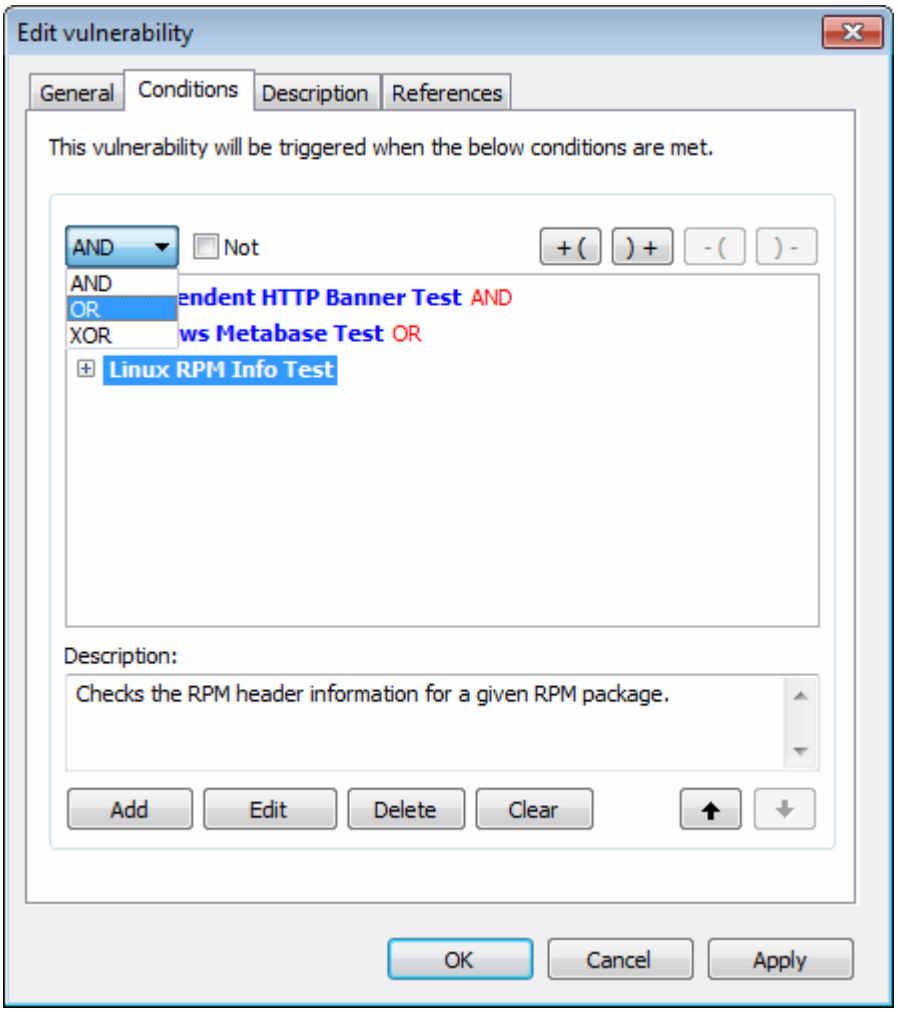
Screenshot 181: Check properties wizard - Define the object to examine

4. Define the object to examine and click **Next**.



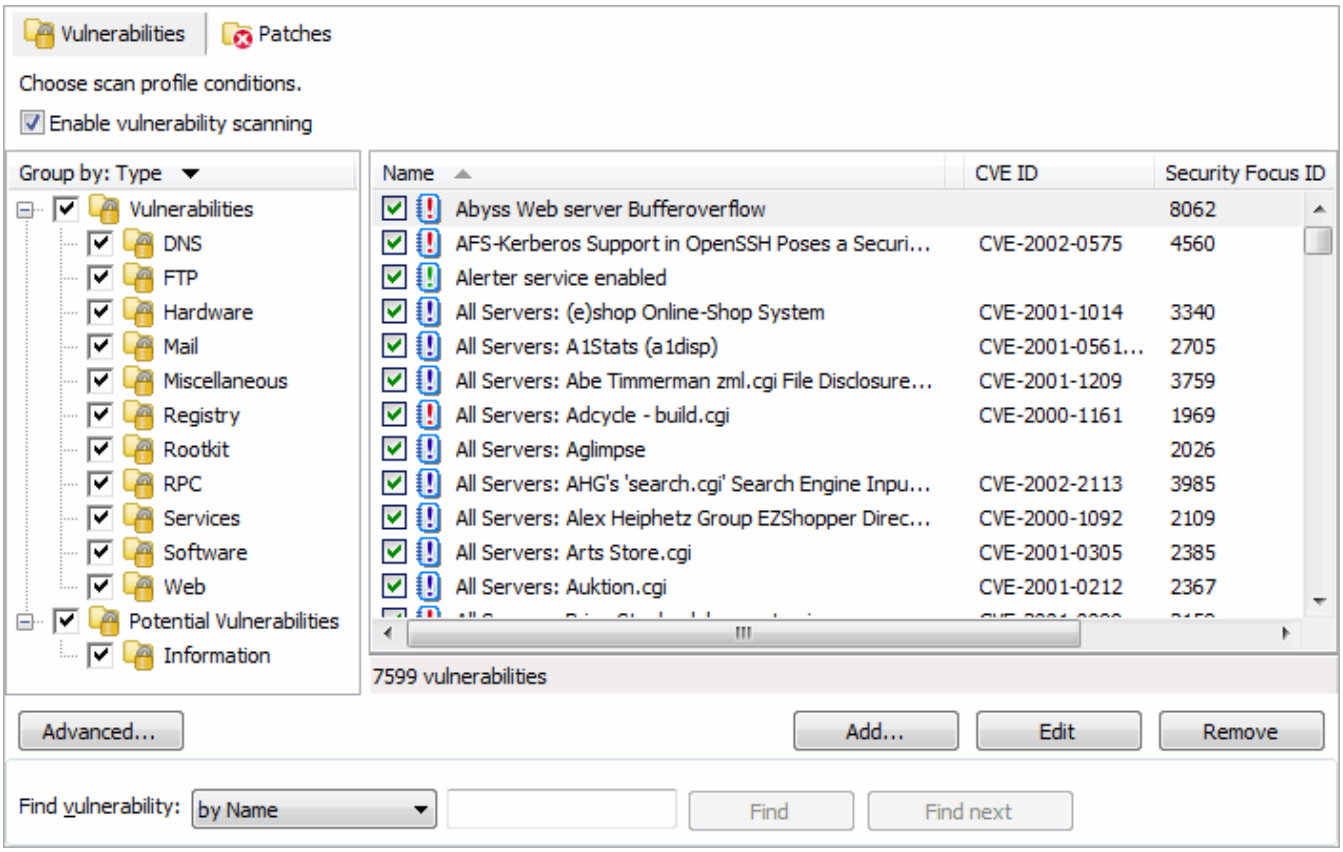
Screenshot 182: Check properties wizard - Set required conditions

5. Specify required conditions and click **Finish** to finalize your settings.



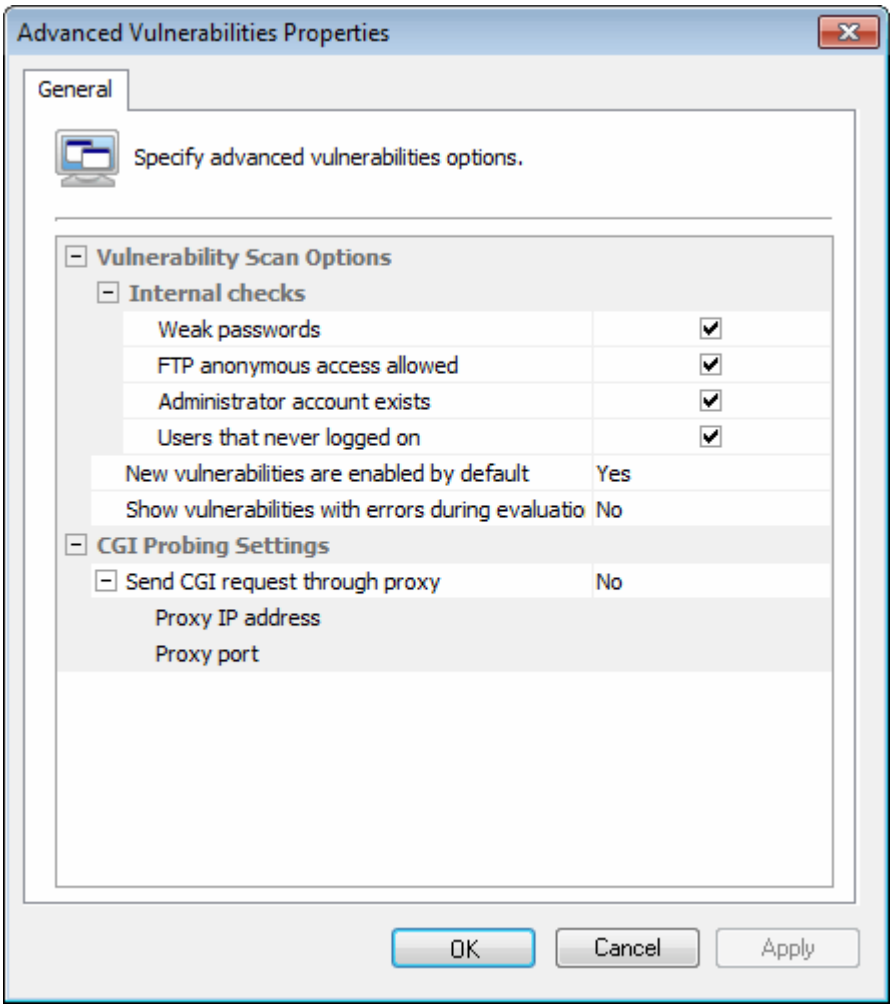
Screenshot 183: Check properties wizard - Defining conditional operators

6. If more than one condition is set up, define conditional operators and click **OK** to finalize your configuration settings.



Screenshot 184: Advanced vulnerability options

7. (Optional) Click **Advanced** in the **Vulnerabilities** tab to launch the advanced vulnerabilities scanning options.



Screenshot 185: Advanced vulnerability scanning dialogs

The options in **Advanced Vulnerabilities Options** are used to:

» Configure extended vulnerability scanning features that check your target computers for weak passwords, anonymous FTP access, and unused user accounts.

» Configure how GFI LanGuard handles newly created vulnerability checks.

» Configure GFI LanGuard to send CGI requests through a specific proxy server. This is mandatory when CGI requests will be sent from a computer that is behind a firewall to a target web server that is 'outside' the firewall. For example, Web servers on a DMZ.

The firewall will generally block all the CGI requests that are directly sent by GFI LanGuard to a target computer that is in front of the firewall. To avoid this, set the **Send CGI requests through proxy** option to 'Yes' and specify the name/IP address of your proxy server and the communication port which will be used to convey the CGI request to the target.

5.5.3 Configuring Patches

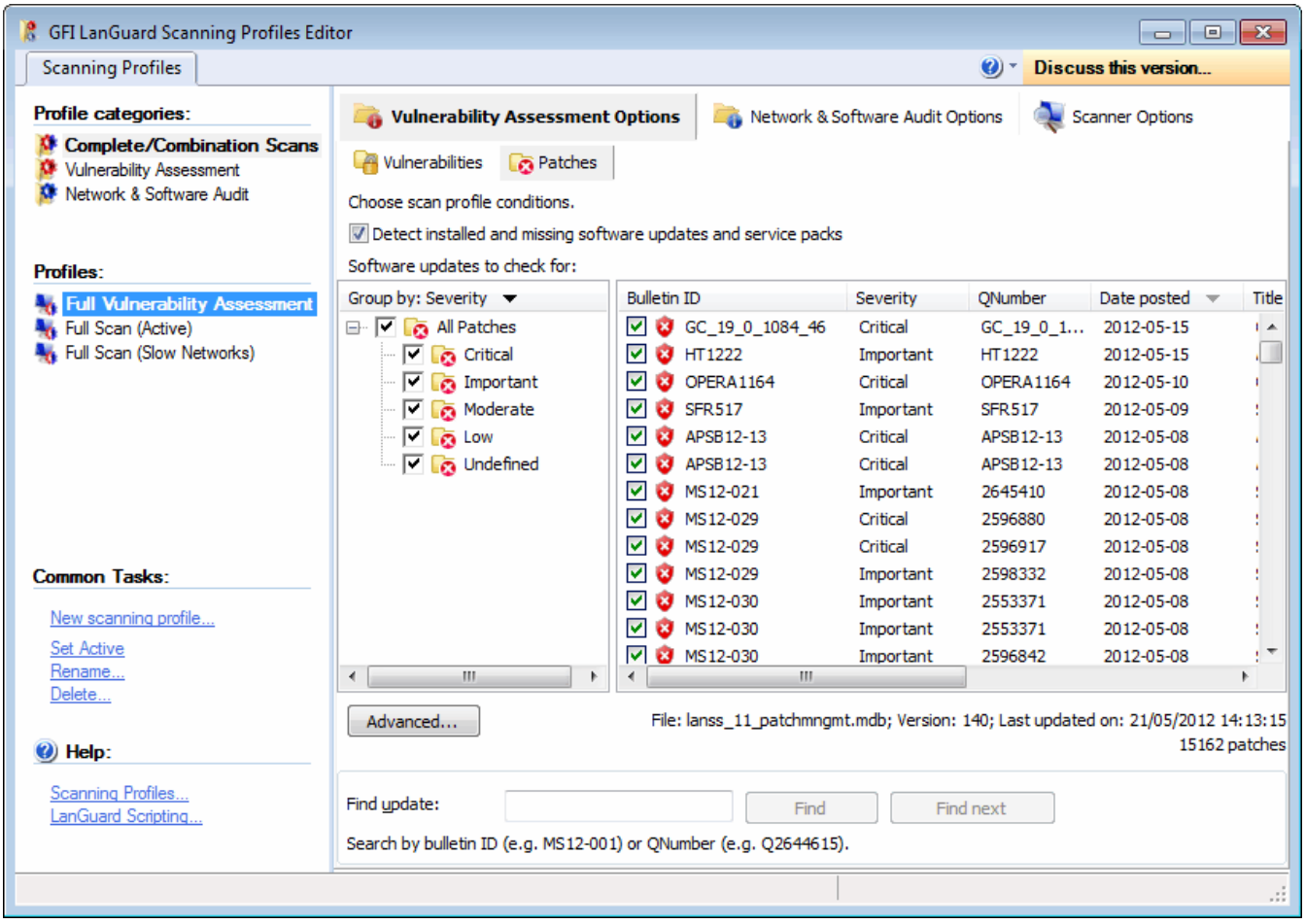
The **Patches** tab specifies the security updates checked during vulnerability scanning. The patches checked are selected from the complete list of supported software updates, included in this tab. This list is automatically updated whenever GFI releases a new GFI LanGuard missing patch definition file.

The following sections contain information about:

» Enabling/disabling missing patch detection checks

» Customizing the list of software patches to scan

Enabling/disabling missing patch detection checks



Screenshot 186: Scanning Profiles properties: Patches tab options

To enable missing patch detection checks in a particular scanning profile:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. From the **Vulnerability Assessment Options** tab, click **Patches** sub–tab.

4. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

5. In the right pane, select **Detect installed and missing service packs/patches** option.

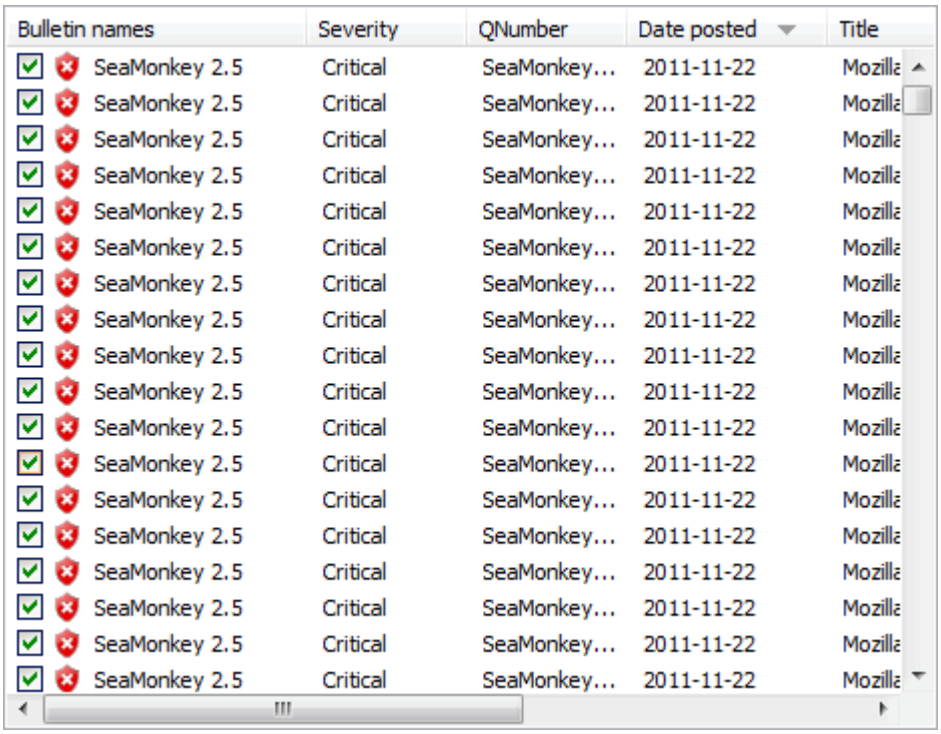
> **NOTE**
> Missing patch scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable missing patch scanning in all profiles where missing patch scanning is required.

Customizing the list of software patches to scan

To specify which missing security updates will be enumerated and processed by a scanning profile:

1. From the **Vulnerability Assessment Options** tab, click **Patches** sub–tab

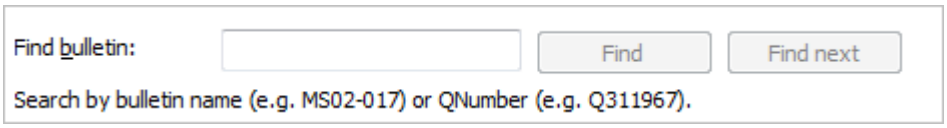
2. Select the scanning profile to customize from the left pane under **Profiles**.



Screenshot 187: Select the missing patches to enumerate

3. In the right pane, select/unselect which missing patches are enumerated by this scanning profile.

Searching for Bulletin Information

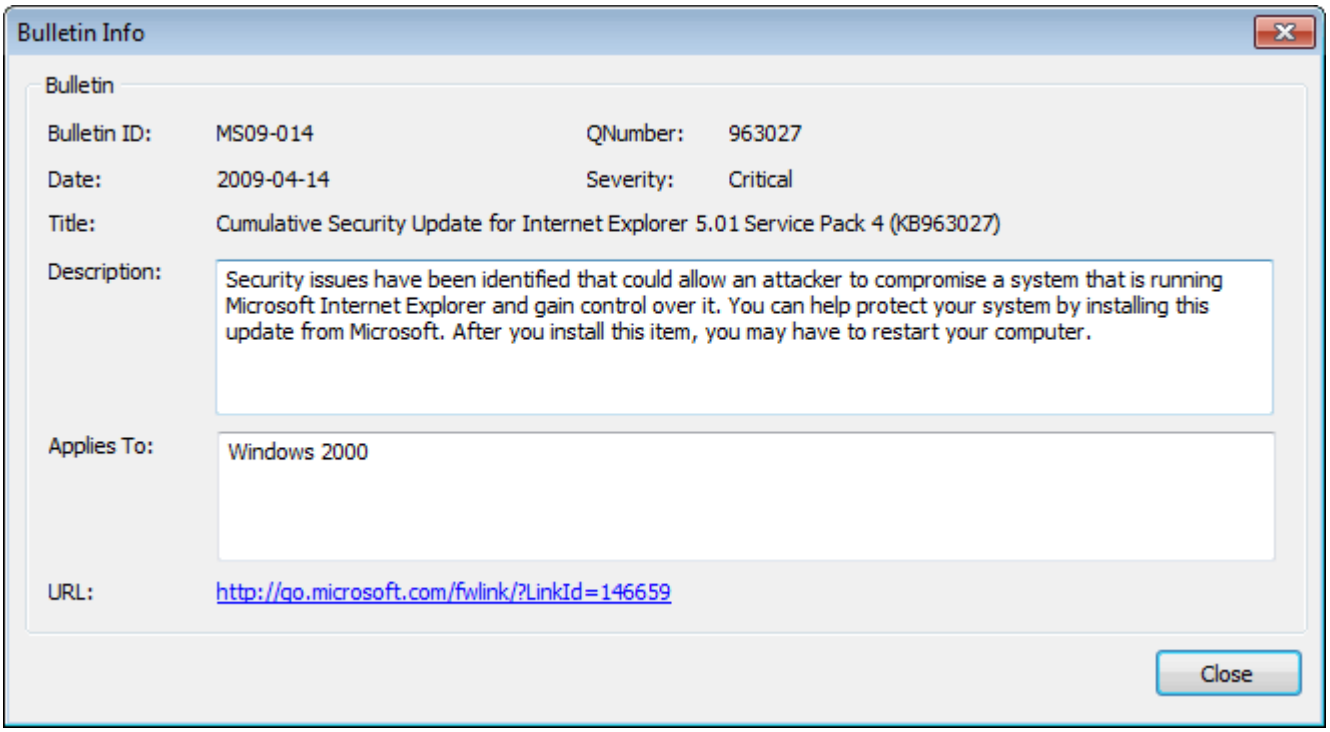


Screenshot 188: Searching for bulletin information

To search for a particular bulletin:

1. From **Vulnerability Assessment Options > Vulnerabilities > Find bulletin**, specify the bulletin name (example: MS02–017) or QNumber (example: Q311987), in the search tool entry box included at the bottom of the right pane.

2. Click **Find** to search for your entry.



Screenshot 189: Extended bulletin information

5.5.4 Configuring Network & Software Audit options

The scanning profiles that ship with GFI LanGuard are already pre–configured to run a number of network and software audit checks on selected target. You can however disable scanning as well as customize the list of network and software audits executed during a scan.

This section contains information about:

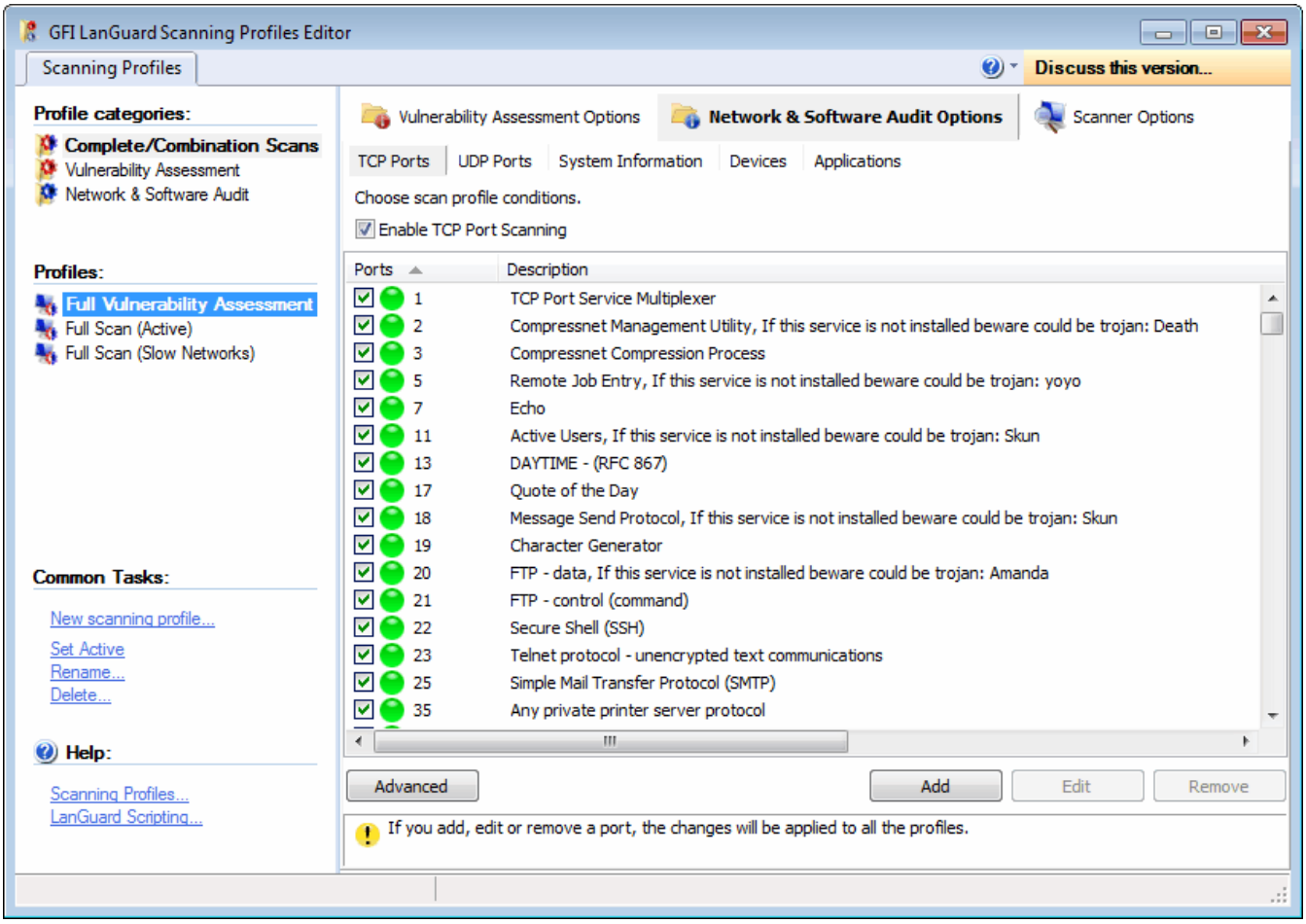
» Configuring TCP/UDP port scanning options

» Configuring System Information options

» Configuring Device scanning options

» Configuring Applications scanning options

Configuring TCP/UDP port scanning options



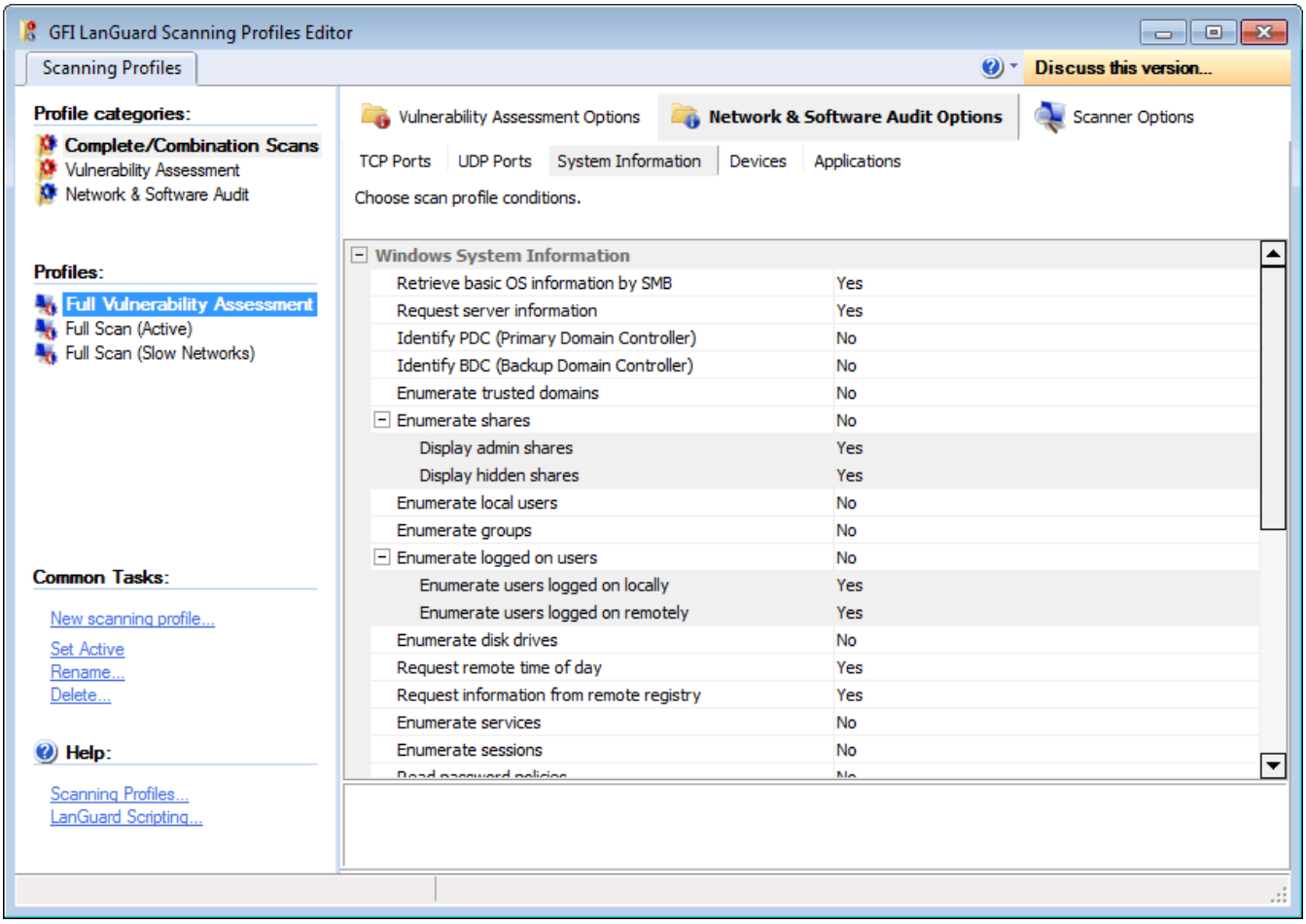
Screenshot 190: Scanning Profiles properties: TCP Ports tab options

Option	Description
Enabling/disabling TCP Port scanning	To enable TCP Port Scanning in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub–tab. 2. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 3. Select **Enable TCP Port Scanning** option.
Configuring the list of TCP ports to be scanned	To configure which TCP ports will be processed by a scanning profile: 1. From **Network & Security Audit Options** tab, click **TCP Ports** sub–tab. 2. Select scanning profile to customize from the left pane under **Profiles**. 3. Select TCP ports to analyze with this scanning profile.
Customizing the list TCP ports	1. From the **Network & Security Audit Options** tab, click **TCP Ports** sub–tab. 2. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 3. Customize the list of TCP Ports through **Add**, **Edit** or **Remove**.

NOTE

The list of supported TCP/UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles

Configuring System Information options



Screenshot 191: Scanning Profiles properties: System Information tab options

To specify what **System Information** is enumerated by a particular scanning profile:

1. From the **Network & Security Audit Options** tab, click **System Information** sub–tab.

2. Select the scanning profile that you wish to customize from the left pane under **Profiles**.

3. From the right pane, expand the **Windows System Information** group or Linux System Information group accordingly.

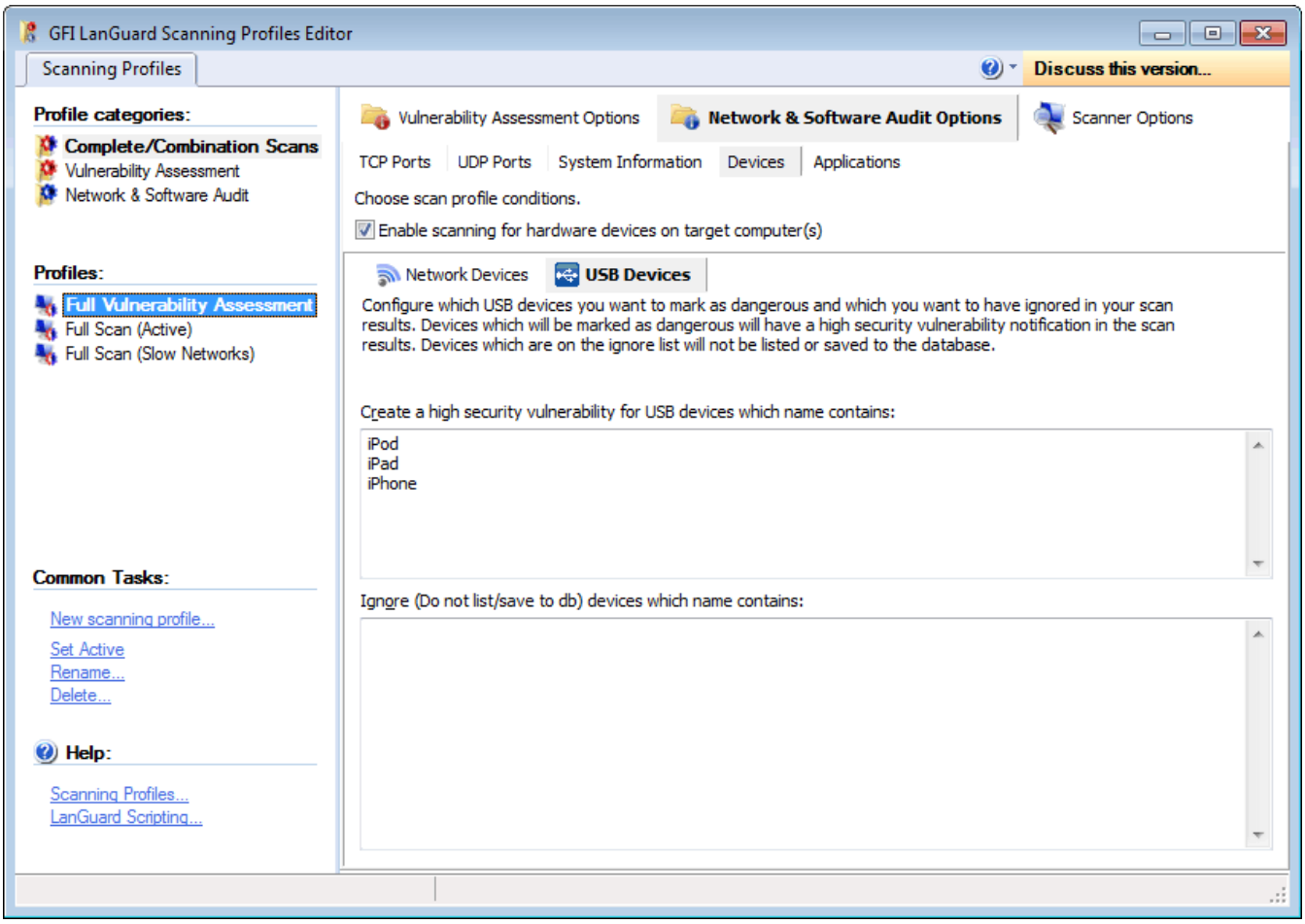
4. Select which Windows/Linux OS information is retrieved by the security scanner from scanned targets.

For example, to enumerate administrative shares in scan results, expand the **Enumerate shares** option and set the **Display admin shares** option to '**Yes**'.

Configuring Device scanning options

Use the Devices tab to enumerate network devices. Together with device enumeration, you can further configure GFI LanGuard to generate high security vulnerability alerts whenever a USB or Network device is detected.

This is achieved by compiling a list of unauthorized/blacklisted Network and USB devices that you want to be alerted.



Screenshot 192: The network devices configuration page

GFI LanGuard can also exclude from the scanning process specific USB devices that you consider safe. Such devices can be a USB mouse or keyboard. This is achieved through a safe/white list of USB devices to ignored during scanning.

Similarly you can create a separate scanning profile that enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers. In this case however, you must specify 'Bluetooth' and 'Wireless' or 'WiFi' in the unauthorized network and USB lists of your scanning profile.

All the device scanning configuration options are accessible through the two sub–tabs contained in the devices configuration page. These are the **Network Devices** tab and the **USB Devices** tab.

Use the **Network Devices** sub–tab to configure the attached network devices scanning options and blacklisted (unauthorized)/white–listed (safe) devices lists.

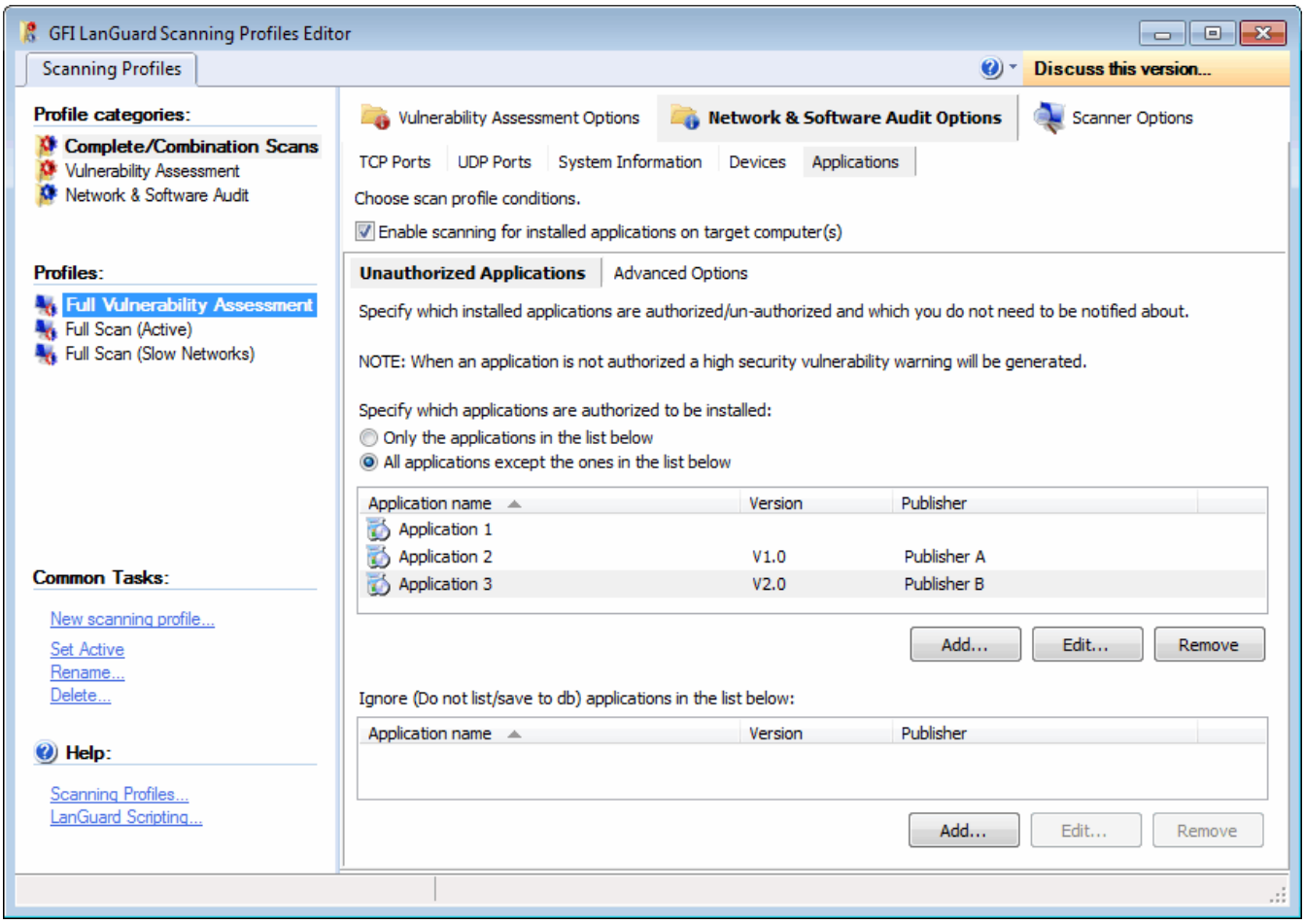
Use the **USB Devices** sub–tab to configure the attached USB devices scanning options and unauthorized/safe devices lists.

Option	Description
Enabling/disabling checks for all installed network devices	To enable network device (including USB device) scanning in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click **Devices** sub–tab. 2. Click **Network Devices** tab. 3. Select the scanning profile to customize from the left pane under **Profiles**. 4. From the right pane, select **Enable scanning for hardware devices** on target computer(s). **NOTE** Network device scanning is configurable on a scan profile by scan profile basis. Make sure to enable network device scanning in all profiles where this is required.

Option	Description
Compiling a network device blacklist/white–list	To compile a network device blacklist/white–list for a scanning profile: 1. From the **Network & Security Audit Options** tab, click **Devices** sub–tab. 2. Click **Network Devices** tab. 3. Select the scanning profile to customize from the left pane under **Profiles**. 4. In the right pane: to create a network device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under **Create a high security vulnerability for network devices which name contains**. For example, if you enter the word 'wireless' you will be notified through a high security vulnerability alert when a device whose name contains the word 'wireless' is detected. To create a network device white–list, specify which devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db)** devices which name contains. **NOTE** Only include one network device name per line.
Configuring advanced network device scanning options	From the **Network Devices** tab, you can also specify the type of network devices checked by this scanning profile and reported in the scan results. These include 'wired network devices', 'wireless network devices', 'software enumerated network devices' and 'virtual network devices'. To specify which network devices to enumerate in the scan results: 1. From the **Network & Security Audit Options** tab, click **Devices** sub–tab. 2. Click on the **Network Devices** tab (opens by default). 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Click **Advanced** at the bottom of the page. 5. Set the required options to **Yes**. Click **OK** to finalize your settings.
Scanning for USB devices	To compile a list of unauthorized/unsafe USB devices: 1. From the **Network & Security Audit Options** tab, click the **Devices** sub–tab. 2. Click **USB Devices** tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. In the right pane. specify which devices you want to classify as high security vulnerabilities in the space provided under **Create high security vulnerability for USB devices which name contains:**. For example, if you enter the word 'iPod', you will be notified through a high security vulnerability alert when a USB device whose name contains the word 'iPod' is detected. To create a USB device white–list, specify which USB devices you want to ignore during network vulnerability scanning in the space provided under **Ignore (Do not list/save to db) devices which name contains**. **NOTE** Only include one USB device name per line.

Configuring Applications scanning options

The **Applications** tab enables you to specify which applications will trigger an alert during a scan.



Screenshot 193: The applications configuration page

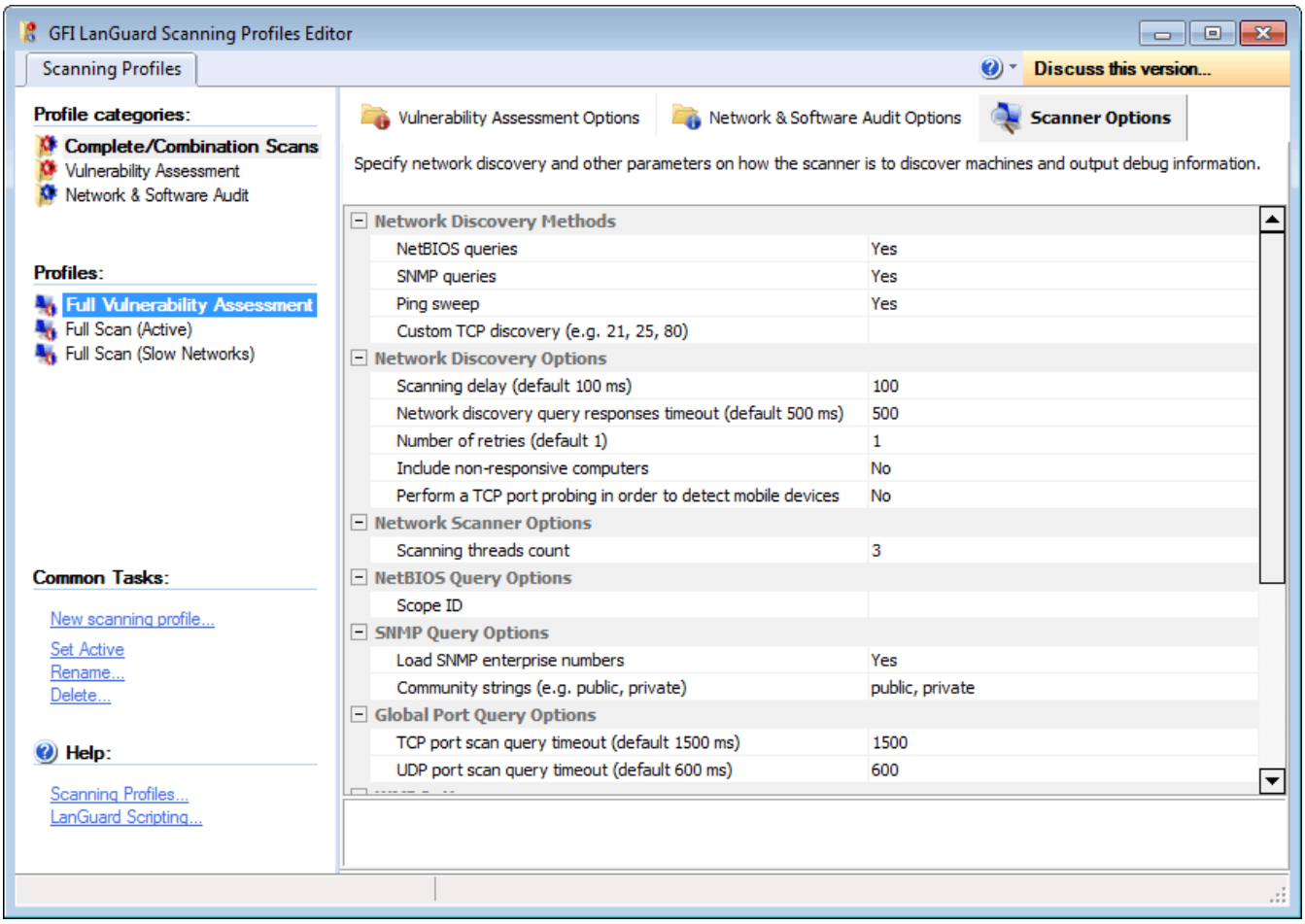
Through this tab, you can also configure GFI LanGuard to detect and report unauthorized software installed on scanned targets and to generate high security vulnerability alerts whenever such software is detected.

Option	Description
Scanning installed applications	By default,GFI LanGuard also supports integration with particular security applications. These include various antivirus and antispyware software. During security scanning, GFI LanGuard checks the correct configuration of virus scanner(s) or antispyware software and that the respective definition files are up to date. Application scanning is configurable on a scan profile by scan profile basis and all the configuration options are accessible through the two sub–tabs contained in the **Applications** tab. These are the **Unauthorized Applications** sub–tab and the **Advanced Options** sub–tab.
Enabling/disabling checks for installed applications	To enable installed applications scanning in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click on the **Applications** sub–tab. 2. Click on the **Unauthorized Applications** sub–tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Select the **Enable scanning for installed applications on target computer(s)** checkbox. **NOTE** Installed applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable installed applications scanning in all profiles where this is required.

Option	Description
Compiling installed applications blacklist/white–list	To compile installed applications blacklist/white–list: 1. From the **Network & Security Audit Options** tab, click **Applications** sub–tab. 2. Select **Unauthorized Applications** sub–tab. 3. Select the scanning profile to customize from the left pane under **Profiles**. 4. From the right pane, select **Enable scanning for installed applications on target computer(s)** checkbox. 5. Specify the applications that are authorized for installation. Select from: » **Only the applications in the list below** - Specify names of applications that are authorized for installation. These applications will be ignored during a security scan » **All applications except the ones in the list below** - Specify the names of the applications that are unauthorized for installation. Applications not in this list will be ignored during a security scan. 6. In the **Ignore (Do not list/save to db) applications from the list below** options key in applications by clicking **Add**. Any application listed is white–listed. **NOTE** Include only one application name per line.
Advanced application scanning options	GFI LanGuard ships with a default list of antivirus and antispyware applications that can be checked during security scanning. The **Advanced Options** tab enables you to configure when GFI LanGuard will generate high security vulnerability alerts if it detects certain configurations of a security application. Alerts are generated when: » No antivirus, antispyware or firewall is detected » A fake antivirus or antispyware is detected » Antivirus or antispyware definitions are not up to date » Antivirus or antispyware real–time monitoring is turned off » Antivirus or antispyware product is expired » Antivirus or antispyware product detects malware on the scanned computer(s) » Firewall is disabled » HTTP/FTP timeout when checking for product updates on remote sites. This option generates an alert if the number of seconds defined for timeout is exceeded.
Enabling/disabling checks for security applications	To enable checks for installed security applications in a particular scanning profile: 1. From the **Network & Security Audit Options** tab, click on the **Applications** sub–tab. 2. Click on the **Advanced Options** tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Select **Enable scanning for installed applications on target computer(s)** checkbox. 5. (Agent–less scans) Select **Enable full security applications audit for agent–less scans** checkbox. **NOTE** 1. Agent–less scans temporarily runs a small service on the remote computers in order to retrieve the relevant information. 2. Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required. 3. The number of supported security applications is constantly updated. Click the link available in order to get the latest version of the list. Configuring security applications – advanced options. To configure alerting triggers for installed security applications in a particular scanning profile: 1. From **Network & Security Audit Options** tab, click **Applications** sub–tab. 2. Click **Advanced Options** tab. 3. Select the scanning profile that you wish to customize from the left pane under **Profiles**. 4. Select **Enable scanning for installed applications on target computer(s)** checkbox. 5. (Agent–less scans) Select **Enable full security applications audit for agent–less scans** checkbox. 6. From the bottom–right pane, select the trigger you want to configure and choose between **Yes** or **No** from the drop down menu next to the respective alert trigger. **NOTE** Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.

5.5.5 Configuring security scanning options

Use **Scanner Options** tab to configure the operational parameters of the security–scanning engine. These parameters are configurable on a scan profile by scan profile basis and define how the scanning engine will perform target discovery and OS Data querying.



Screenshot 194: Scanning Profiles properties: Scanner Options tab

Configurable options include timeouts, types of queries to run during target discovery, number of scanning threads count, SNMP scopes for queries and more.

> **IMPORTANT**
> Configure these parameters with extreme care! An incorrect configuration can affect the security scanning performance of GFI LanGuard.

To configure scanner options:

1. From **Scanning Profile Editor > Profile categories**, select the category that contains the scanning profile you want to edit (example: **Complete/Combination Scans**).

2. From the **Profiles** section, select the scanning profile you want to edit (example: **Full Vulnerability Assessment**).

3. From the right pane, click **Scanner Options**.

4. Configure the following parameters that determine the scanning behavior of GFI LanGuard:

Parameter	Description
Network Discovery Methods	
NetBIOS queries	Enable/disable the use of NetBios queries to discover network devices.
SNMP queries	Enable/disable the use of SNMP queries to discover network devices.
Ping sweep	Enable/disable the use of Ping sweeps to discover network devices.
Custom TCP discovery	Discover online machines by querying for the specified open TCP ports.
Network Discovery Options	
Scanning delay	Key in the time interval (in milliseconds) between one scan and another.
Network discovery query responses timeout	Amount of time in milliseconds the security scanner will wait before timing out when performing a machine discovery query (NetBIOS/SNMP/Ping).
Number of retries	Number of times security scanner will retry to connect to a non-responsive machine before skipping it.
Include non-responsive computers	Run scans on all the PCs regardless of whether they are detected as being online or not.
Perform a TCP port probing in order to detect mobile devices	Perform a TCP port probing in order to detect mobile devices using known ports.
Network Scanner Options	
Scanning threads count	Key in the number of scan threads that can run simultaneously.
NetBIOS Query Options	
Scope ID	Used for NetBIOS environments requiring a specific scope ID in order to allow querying.
SNMP Query Options	
Load SNMP enterprise numbers	Specifies whether security scanner should use the OID (Object Identifier database) containing ID to Vendor map to identify the various types of devices.
Community strings	Specifies whether security scanner should use the specified community string for SNMP server detection and information retrieval.
Global Port Query Options	
TCP port scan query timeout	Amount of time in milliseconds security scanner will wait during a TCP port scan before timing out and moving on to scan the next port.
UDP port scan query timeout	Amount of time in milliseconds security scanner will wait during a UDP port scan before timing out and moving on to scan the next port.
WMI Options	
WMI timeout	Amount of time in milliseconds security scanner will wait for a reply from the remote WMI server before timing out and moving on to the next scan item.
SSH Options	
SSH timeout	Amount of time in milliseconds security scanner will wait for a SSH script to return before timing out and moving on to the next scan item.
Alternative SSH port	Alternative SSH ports to use when the default port 22 is unreachable.
Scanner activity window	

Parameter	Description
Type of scanner activity output	Activity progress modes: simple (basic progress - start / stop of operations), or verbose (more detailed information on process flow).
Display received packets	Output TCP packets in raw format as they were received by security scanner.
Display sent packets	Output TCP packets in raw format as they were sent by security scanner.
OS Information Retrieval Options	
Create custom share if administrative privileges are disabled	If administrative shares are disabled the scanner will temporarily create a custom hidden share of the form <random GUID>$. The share is used to retrieve data that helps identifying vulnerabilities and missing patches.
Start remote registry	If the remote registry service is stopped on the scanned machine, enable this option to temporarily open it during the security scanning.

5.6 Utilities

GFI LanGuard provides you with a set of network utilities that enable you to monitor network activity, gather network information and audit network devices.

Topics in this section:

5.6.1 DNS Lookup

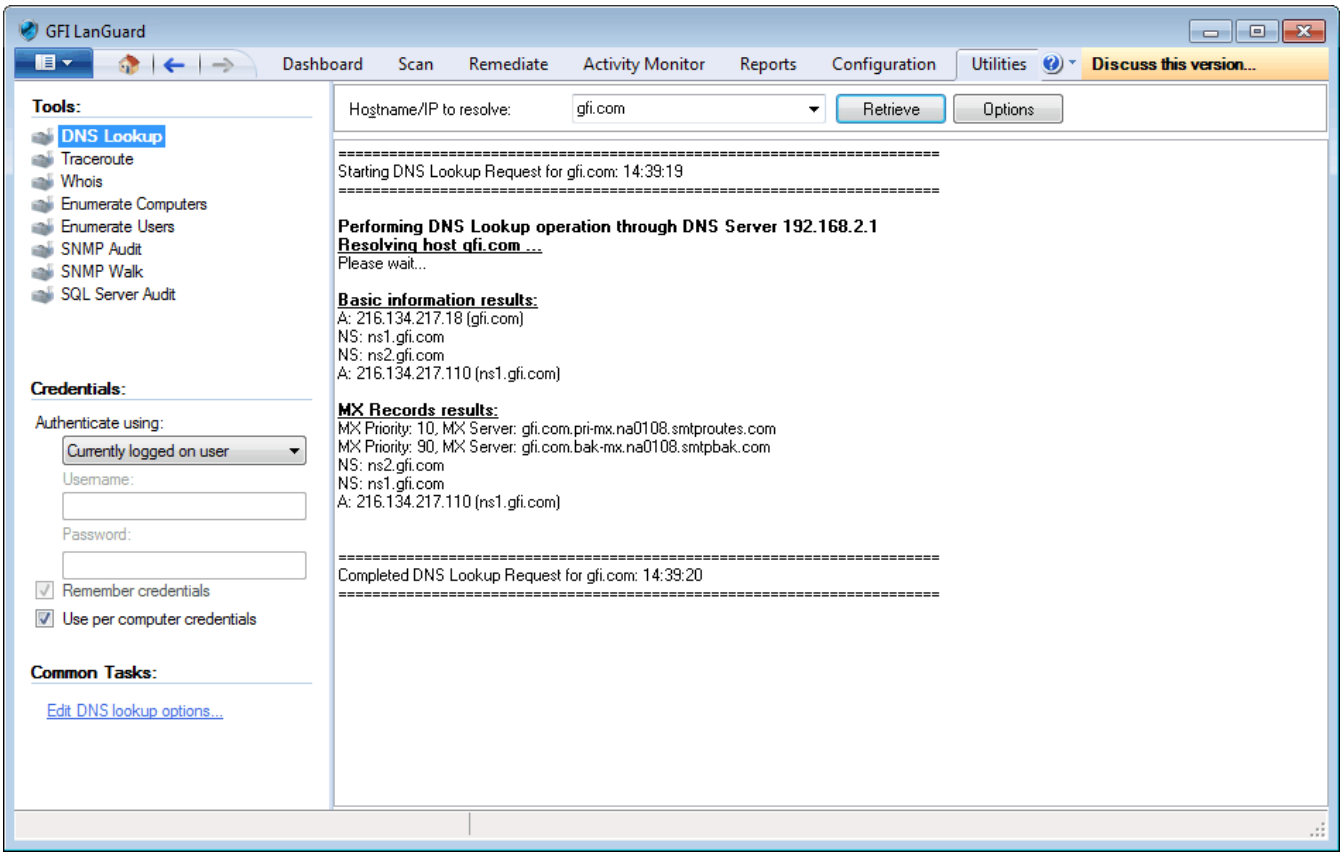
DNS lookup resolves domain names into the corresponding IP address and retrieves particular information from the target domain (for example, MX record, etc.).

To resolve a domain/host name:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **DNS Lookup** in the left pane under **Tools**.

3. Specify the hostname to resolve in **Hostname/IP to resolve**.



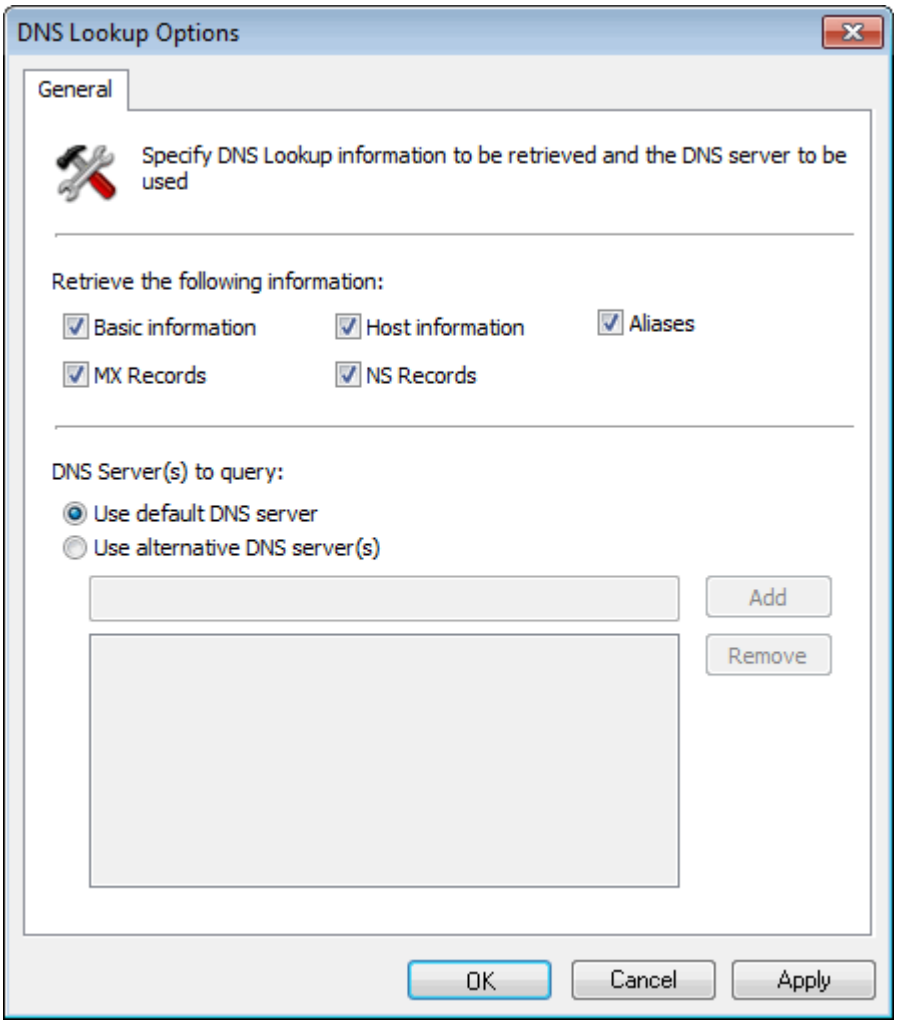
Screenshot 195: DNS Lookup tool

4. Under **Common Tasks** in the left pane, click on **Edit DNS Lookup options** or click **Options** on the right pane and specify the information described below:

Option	Description
Basic Information	Retrieve the host name and the relative IP address.
Host Information	Retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.
Aliases	Retrieve information on the 'A Records' configured on the target domain.
MX Records	Enumerate all the mail servers and the order (i.e. priority) in which they receive and process emails for the target domain.
NS Records	Specify the 'name–servers' that are authoritative for a particular domain or sub domain.

NOTE

Some DNS entries do not contain certain information for security reasons.



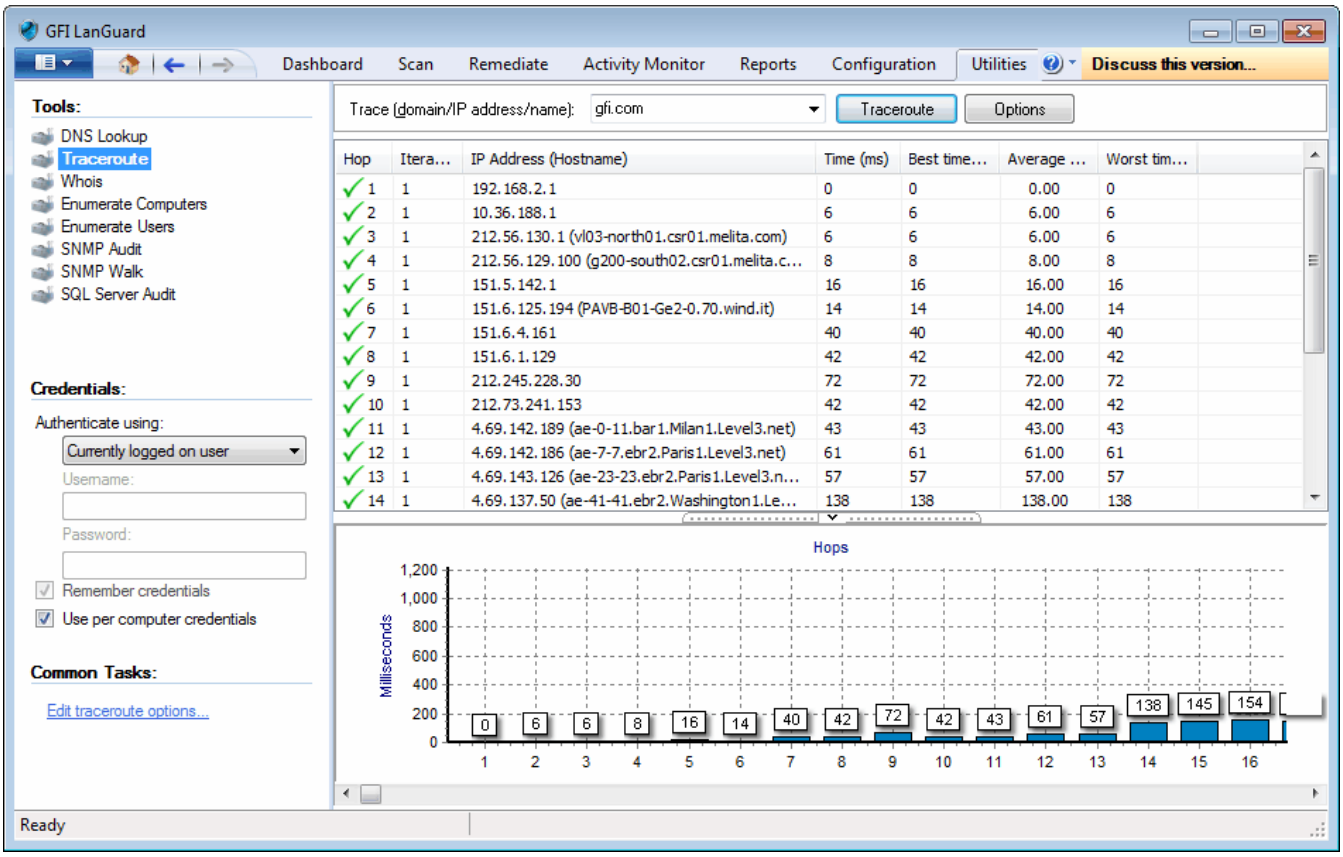
Screenshot 196: DNS Lookup tool options

5. (Optional) Specify the alternative DNS server that will be queried by the DNS Lookup tool or leave as default to use the default DNS server.

6. Click **Retrieve** to start the process.

5.6.2 Traceroute

Traceroute identifies the path that GFI LanGuard followed to reach a target computer.



Screenshot 197: Traceroute tool

To use the Traceroute tool:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **Traceroute** in the left pane under **Tools**.

3. In the **Trace (domain/IP/name)**, specify the name/IP or domain to reach.

4. (Optional) Under **Common Tasks** in the left pane, click on **Edit Traceroute options** or click **Options** on the right pane to change the default options.

5. Click on the **Traceroute** button to start the tracing process.

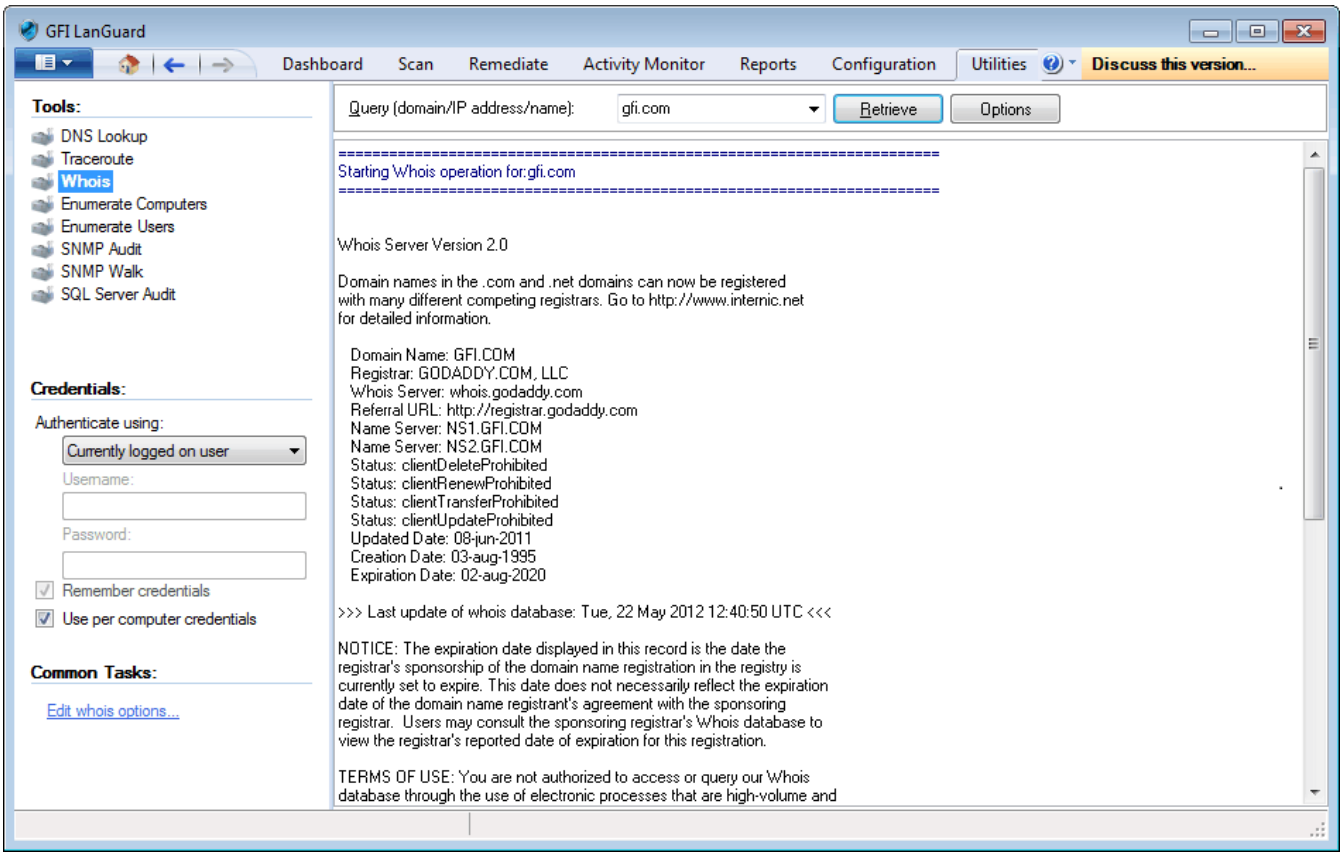
Traceroute will break down, the path taken to a target computer into 'hops'. A hop indicates a stage and represents a computer that was traversed during the process.

The information enumerated by this tool includes the IP of traversed computers, the number of times that a computer was traversed and the time taken to reach the respective computer. An icon is also included next to each hop. This icon indicates the state of that particular hop. The icons used in this tool include:

Icon	Description
✓	Indicates a successful hop taken within normal parameters.
⚠	Indicates a successful hop, but time required was quite long.
⚠	Indicates a successful hop, but the time required was too long.
✗	Indicates that the hop was timed out (> 1000ms).

5.6.3 Whois

Whois looks up information on a particular domain or IP address.



Screenshot 198: Whois tool

1. Launch GFI LanGuard.

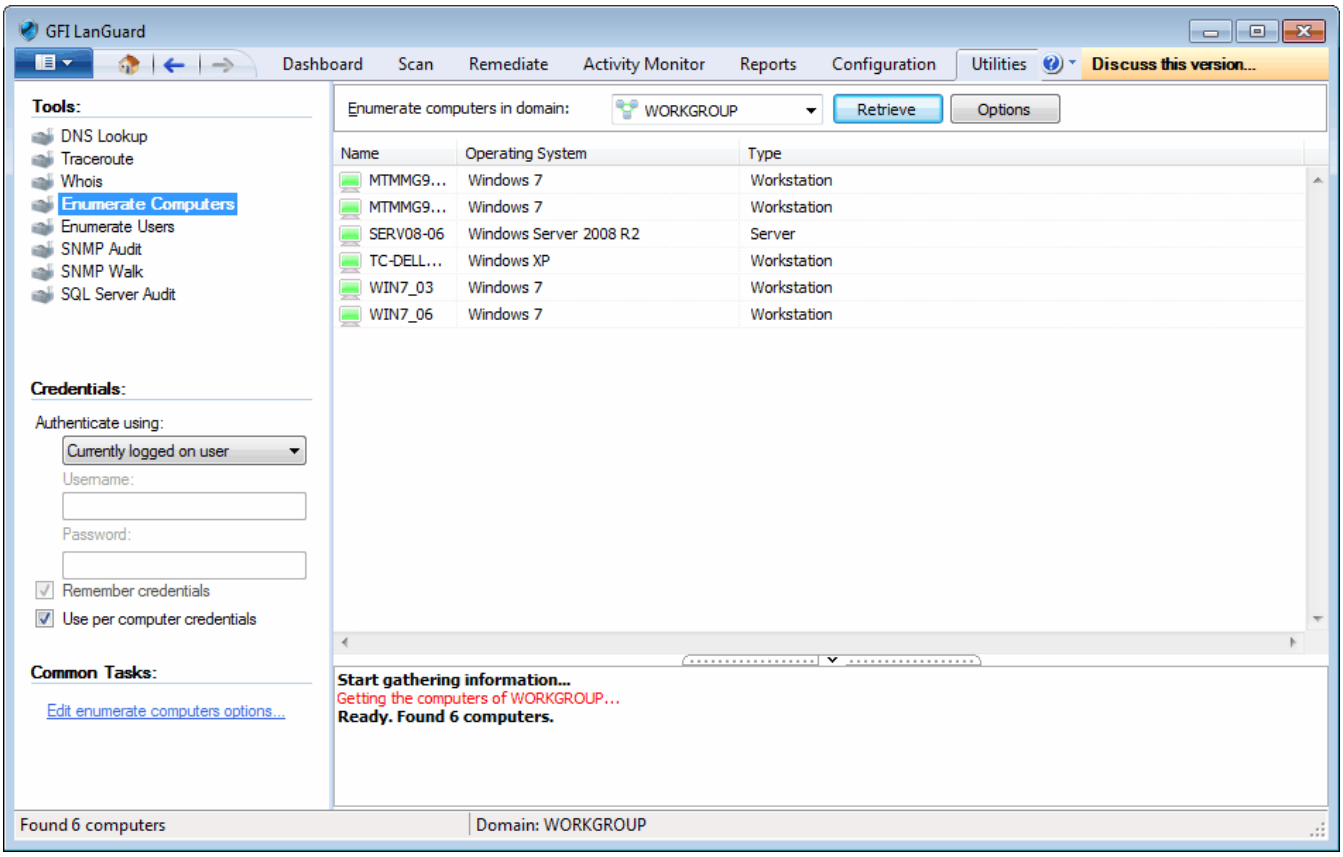
2. Click **Utilities** tab and select **Whois** in the left pane under **Tools**.

3. In **Query (domain/IP/name)** menu, specify the name/IP or domain to reach.

4. (Optional) From **Common Tasks** in the left pane, click **Edit Whois options** or **Options** on the right pane to change the default options.

5. Click **Retrieve** to start the process.

5.6.4 Enumerate Computers



Screenshot 199: Enumerate Computers tool

The enumerate computers utility identifies domains and workgroups on a network. During execution, this tool will also scan each domain/workgroup discovered so to enumerate their respective computers.

- The information enumerated by this tool includes:
- The domain or workgroup name
- The list of domain/workgroup computers
- The operating system installed on the discovered computers
- Any additional details that might be collected through NetBIOS.

Computers are enumerated using one of the following methods:

Option	Description
From Active Directory®	This method is much faster and will include computers that are currently switched off.
From Windows Explorer	This method enumerates computers through a real–time network scan and therefore it is slower and will not include computers that are switched off.

To enumerate computers:

1. Launch GFI LanGuard.
2. Click **Utilities** tab and select **Enumerate Computers** in the left pane under **Tools**.
3. In the **Enumerate computers in domain**, select the desired domain.
4. From **Common Tasks** in the left pane, click **Edit Enumerate Computers options** or **Options** on the right pane.

5. Select whether to enumerate computers from Active Directory® or Windows Explorer.

6. Click **Retrieve** to start the process.

> **NOTE**
> For an Active Directory® scan, you will need to run the tool under an account that has access rights to Active Directory®.

Starting a Security Scan

To start a security scan directly from the 'Enumerate Computers' tool, right–click on any of the enumerated computers and select Scan.

You can also launch a security scan and at the same time continue using the Enumerate Computers tool. This is achieved by right–clicking on any of the enumerated computers and selecting Scan in background.

Deploying Custom Patches

You can use the Enumerate Computers tool to deploy custom patches and third party software on the enumerated computers. To launch a deployment process directly from this tool:

1. Select the computers that require deployment.

2. Right–click on any of the selected computers and select **Deploy Custom Patches**.

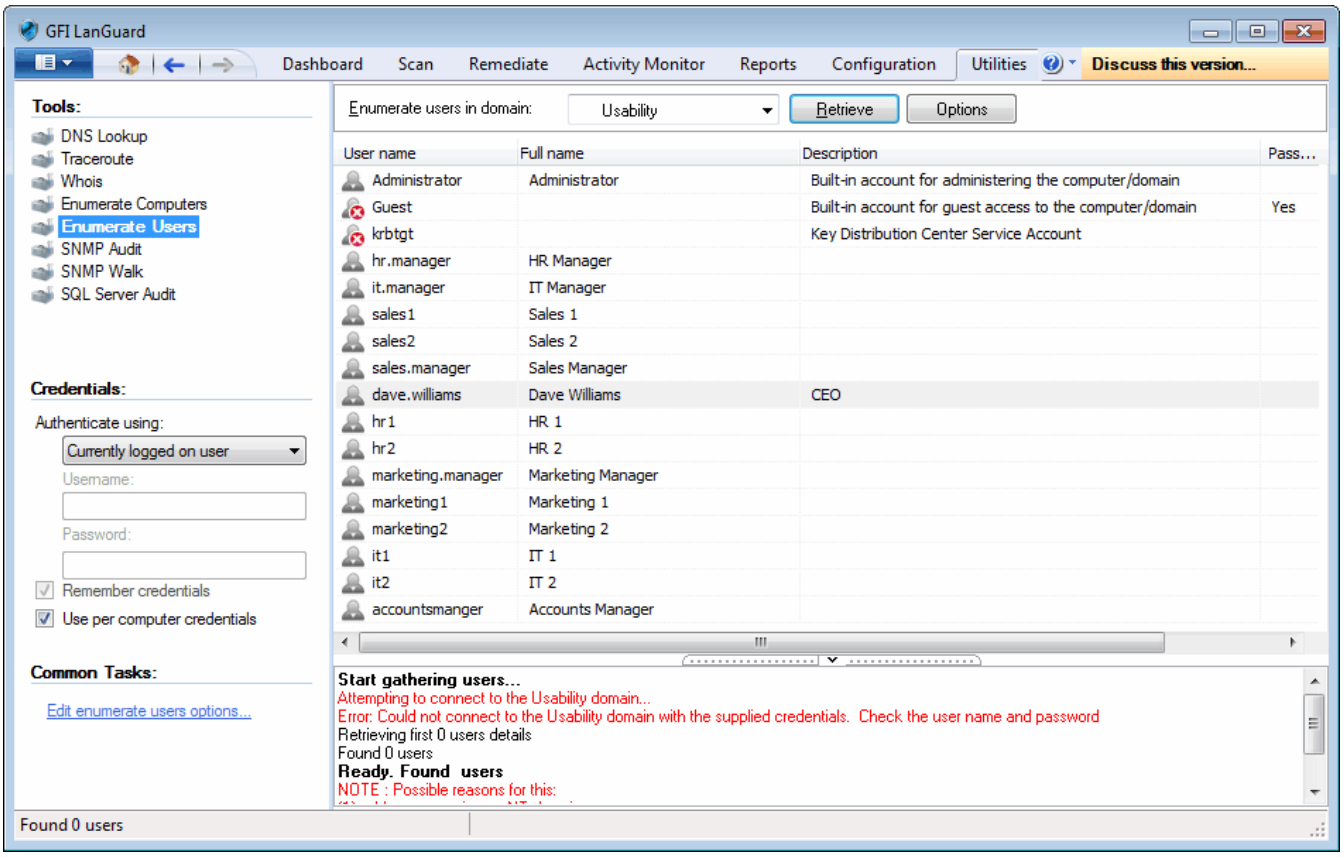
Enabling Auditing Policies

The Enumerate Computers tool also enables you to configure auditing policies on particular computers. This is done as follows:

1. Select the computers on which you want to enable auditing policies.

2. Right–click on any of the selected computers and select **Enable Auditing Policies**. This will launch the **Auditing Policies configuration Wizard** that will guide you through the configuration process.

5.6.5 Enumerate Users



Screenshot 200: The Enumerate Users tool dialog

To scan the Active Directory® and retrieve the list of all users and contacts included in this database:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **Enumerate Users** in the left pane under **Tools**.

3. In the **Enumerate users in domain** menu, select the desired domain.

4. From **Common Tasks** in the left pane, click **Edit Enumerate Users options** or **Options** on the right pane to filter the information to extract and display only the users or contacts details. In addition, you can optionally configure this tool to highlight disabled or locked accounts.

5. Click **Retrieve** to start the process.

> **NOTE**
>
> This tool can enable or disable enumerated user accounts. Right–click on the account and select **Enable/Disable account** accordingly.

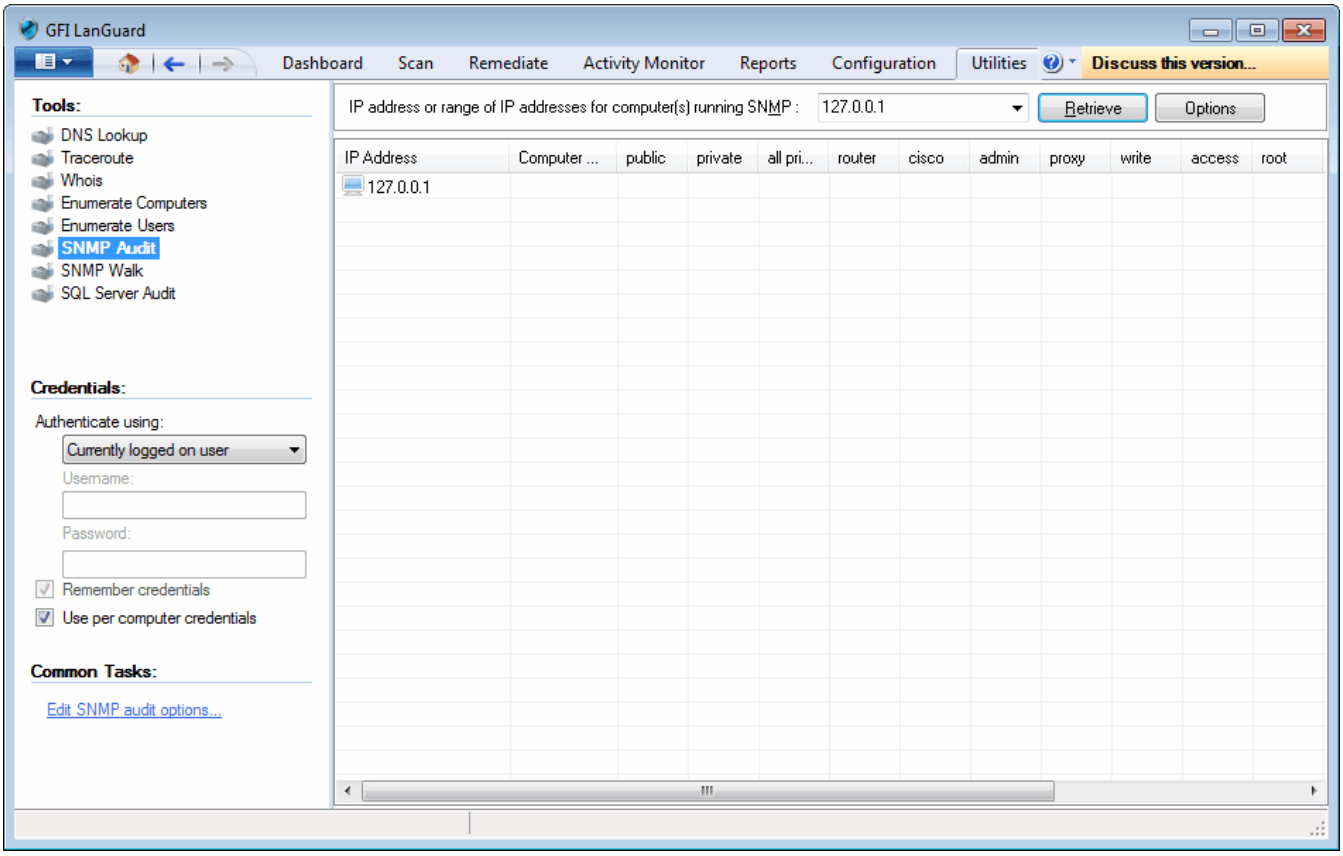
5.6.6 SNMP Auditing

GFI LanGuard uses the Simple Network Management Protocol (SNMP) to obtain information, like hardware specifications and operating system version, from network devices, such as servers, computers, printers, hubs, switches, and routers. Through SNMP, GFI LanGuard can monitor network performance, audit network usage and detect network faults.

IMPORTANT

GFI LanGuard supports SNMPv1 and SNMPv2c.

SNMPv3 and SNMP over TLS / DTLS are NOT supported.



Screenshot 201: SNMP Audit tool

This tool identifies weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary file (snmp–pass.txt).

You can add new community strings to the default dictionary file by using a text editor (for example, notepad.exe).

You can also direct the SNMP Audit tool to use other dictionary files. To achieve this, specify the path to the dictionary file from the Options dialog.

To perform SNMP audits on network targets and identify weak community strings:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **SNMP Audit** in the left pane under **Tools**.

3. In the **IP of computer running SNMP**, specify the IP to reach.

4. From **Common Tasks** in the left pane, click **Edit SNMP Audit options**, or use the **Options** button available in the top-right section of the screen, to edit the default options.

5. Click **Retrieve** to start the process.

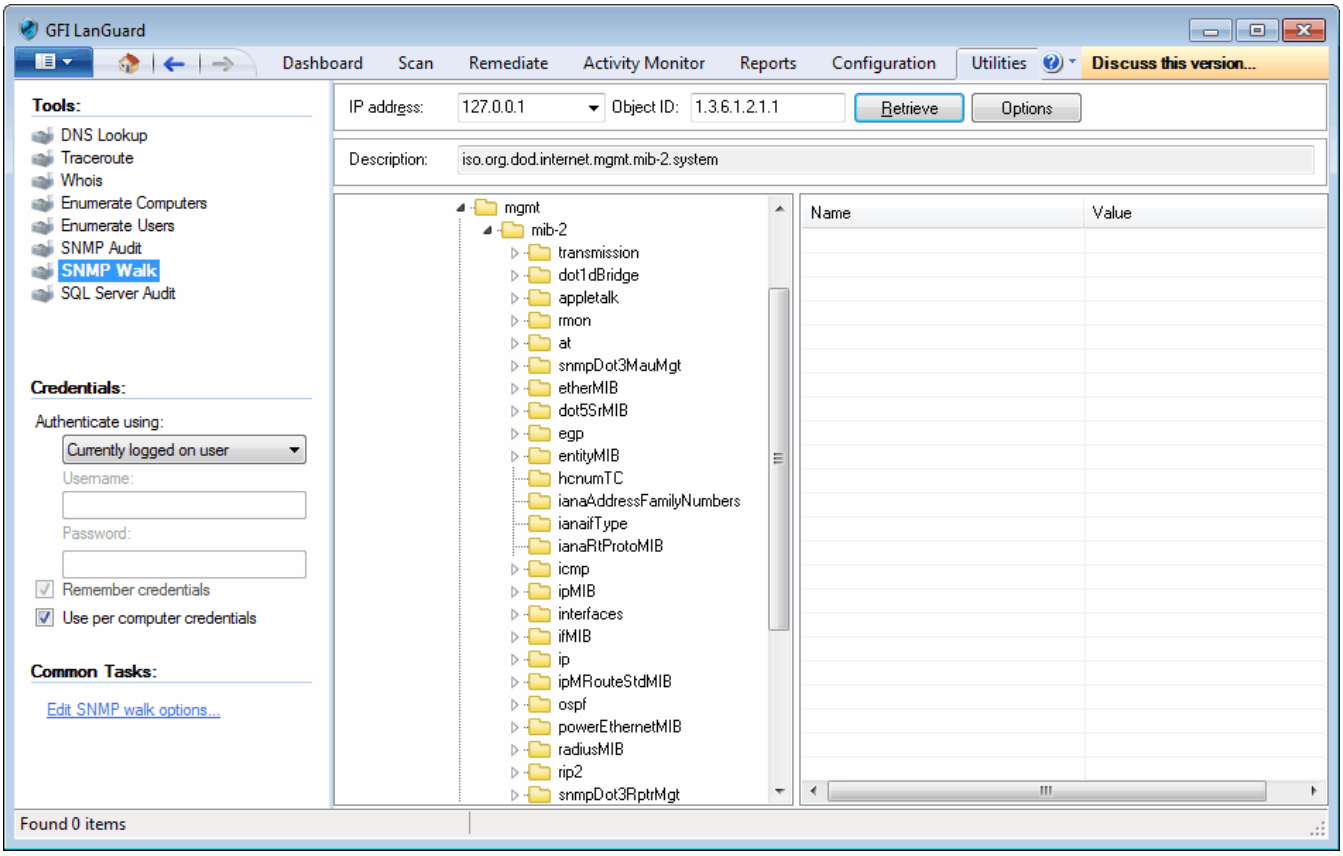
5.6.7 SNMP Walk

GFI LanGuard uses the Simple Network Management Protocol (SNMP) to obtain information, like hardware specifications and operating system version, from network devices, such as servers, computers, printers, hubs, switches, and routers. Through SNMP, GFI LanGuard can monitor network performance, audit network usage and detect network faults.

IMPORTANT

GFI LanGuard supports SNMPv1 and SNMPv2c.

SNMPv3 and SNMP over TLS / DTLS are NOT supported.



Screenshot 202: SNMP Walk tool

To probe your network nodes and retrieve SNMP information (for example, OID's):

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **SNMP Walk** in the left pane under **Tools**.

3. In the **IP address** menu, specify the IP address of the computer that you wish to scan for SNMP information.

4. From **Common Tasks** in the left pane, click **Edit SNMP Audit options**. Alternatively use the **Options** button available in the top-right section of the screen, to edit the default options, such as providing alternative community strings.

5. Click **Retrieve** to start the process.

IMPORTANT

SNMP activity is normally blocked at the router / firewall so that internet users cannot SNMP scan your network. Malicious users can use information collected through SNMP scanning to hack your network or systems. Unless this service is required, it is highly recommended to disable it.

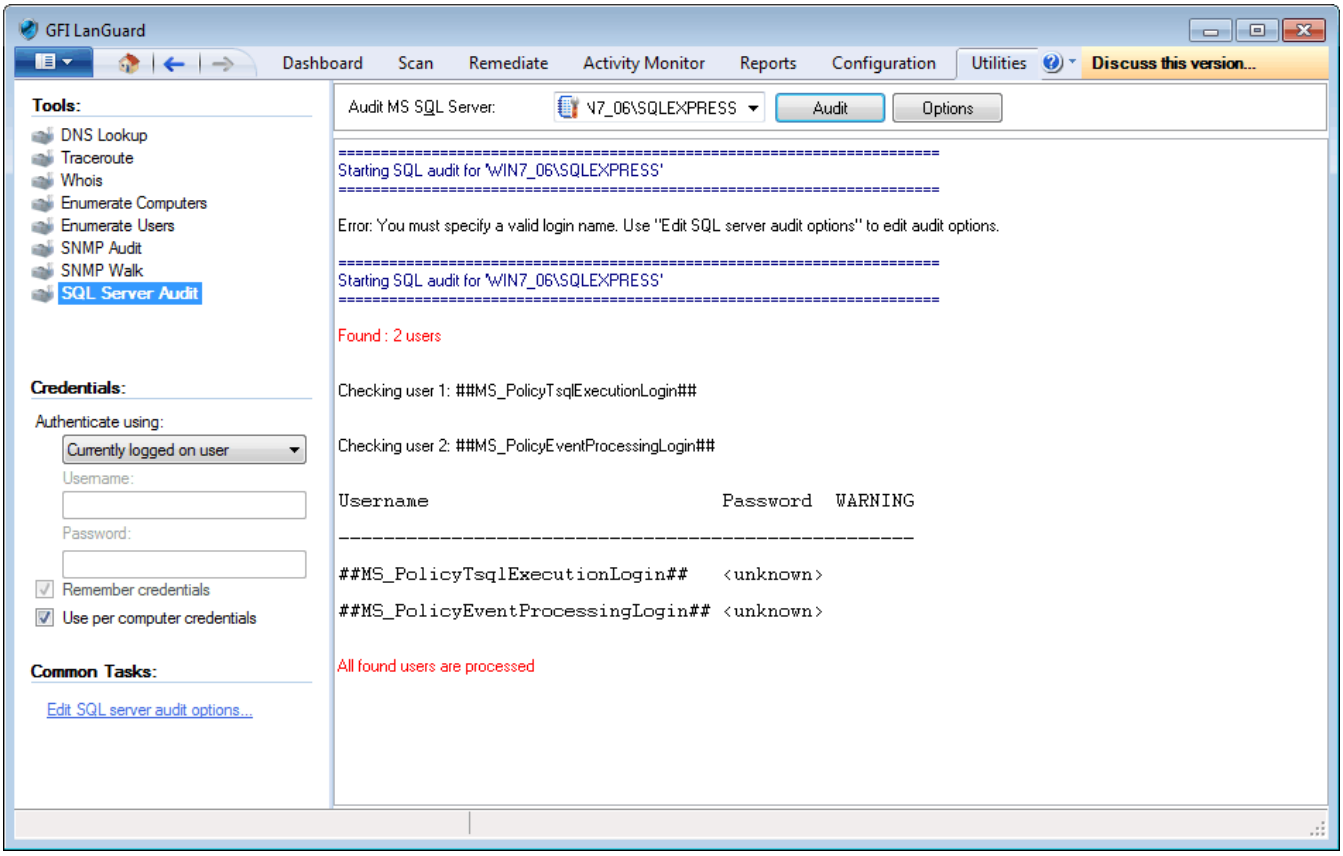
5.6.8 SQL Server® Audit

This tool enables you to test the password vulnerability of the 'sa' account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server®. During the audit process, this tool will perform dictionary attacks on the SQL Server® accounts using the credentials specified in the 'passwords.txt' dictionary file. However, you can also direct the SQL Server® Audit tool to use other dictionary files. You can also customize your dictionary file by adding new passwords to the default list.

To perform a security audit on a particular SQL Server® installation:

1. Launch GFI LanGuard.

2. Click **Utilities** tab and select **SQL Server Audit** in the left pane under **Tools**.



Screenshot 203: SQL Server® Audit

3. In the **Audit MS SQL Server** menu, specify the IP address of the SQL Server® that you wish to audit.

4. From **Common Tasks** in the left pane, click **Edit SQL Server® Audit options** or **Options** button on the right pane to edit the default options such as performing dictionary attacks on all the other SQL user accounts.

5. Click **Audit** to start the process.

5.6.9 Command Line Tools

The command line tools enable you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up the GFI LanGuard.

Use the information in this section to learn how to run patch management functions using the following CMD tools:

- Lnsscmd.exe
- Deploycmd.exe
- Impex.exe

Using lnsscmd.exe

The 'lnsscmd.exe' command line target–scanning tool allows you to run vulnerability checks against network targets directly from the command line, or through third party applications, batch files and scripts. The 'lnsscmd.exe' command line tool supports the following switches:

```
lnsscmd <Target> [/profile=profileName] [/report=reportPath]
[/reportname=reportName] [/output=pathToXmlFile] [/user=username
/password=password] [/Email [/EmailAddress=EmailAddress]] [/DontShowStatus]
[/UseComputerProfiles] [/Wake] [/Shutdown [/ShutdownIntervalStart=<hh:mm:ss>]
[/ShutdownIntervalEnd=<hh:mm:ss>]] [/?]
```

lnsscmd command switches

Switch	Description
Target	Specify the IP / range of IPs or host name(s) to be scanned.
/Profile	(Optional) Specify the scanning profile that will be used during a security scan. If this parameter is not specified, the scanning profile that is currently active in the GFI LanGuard will be used. **NOTE** In GFI LanGuard, the default (i.e. currently active) scanning profile is denoted by the word (Active) next to its name. To view which profile is active expand the **Configuration** tab > **Scanning Profiles** node.
/Output	(Optional) Specify the full path (including filename) of the XML file where the scan results will be saved.
/Report	(Optional) Directory or full file name for the output scan report.
/ReportName	(Optional) Name of the report to generate. If not specified, the report is saved with a default name.
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during security scanning. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the dashboard.
/Email	(Optional) Send the resulting report by e-mail. The e-mail address and mail server specified in **Configuration > Alerting Options** are used.
/EmailAddress	(Optional) Dependent on **/Email**. Overrides the general alerting options and uses the specified email address.
/DontShowStatus	(Optional) Include this switch if you want to perform silent scanning. In this way, the scan progress details will not be shown.
/UseComputerProfiles	(Optional) Use per computer credentials when available.
/Wake	(Optional) Wake up offline computers.
/Shutdown	(Optional) Shuts down computers after scan.

Switch	Description
/ShutdownIntervalStart	(Optional) Dependent on **/Shutdown**. The start time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutdownIntervalEnd	(Optional) Dependent on **/Shutdown**. The end time of the interval when shutdown is allowed. Use hh:mm:ss format.
/?	(Optional) Use this switch to show the command line tool usage instructions.

NOTE

Always enclose full paths and profile names within double quotes. For example, `"[path or path name]"` or `"C:\temp\test.xml"`.

The command line target–scanning tool allows you to pass parameters through specific variables. These variables will be automatically replaced with their respective value during execution. The table below describes the supported variables:

Supported variables

Variable	Description
%INSTALLDIR%	During scanning, this variable will be replaced with the path to the GFI LanGuard installation directory.
%TARGET%	During scanning this variable will be replaced with the name of the target computer.
%SCANDATE%	During scanning this variable will be replaced with the date of scan.
%SCANTIME%	During scanning this variable will be replaced with the time of scan.

Example

1. To perform a security scan on a target computer having IP address '130.16.130.1'.

2. Output the scan results to `'c:\out.xml'` (i.e. XML file).

3. Generate a PDF report and save it in `'c:\result.odf'`.

4. Send the PDF report via email to 'lanss@domain.com'

The command should be as follows:

```
lnsscmd.exe 130.16.130.1 /Profile="Default" /Output="c:\out.xml"
/Report="c:\result.pdf" /Email /emailAddress="lanss@domain.com"
```

Using deploycmd.exe

The 'deploycmd.exe' command line patch deployment tool allows you to deploy Microsoft® patches and third party software on remote targets directly from the command line, or through third party applications, batch files or scripts. The 'deploycmd.exe' command line tool supports the following switches:

```
deploycmd <target> </file=FileName> [/switches=Switches] [/username=UserName
/password=Password] [/warnuser] [/userapproval] [/stopservices]
[/customshare=CustomShareName] [/reboot] [/rebootuserdecides] [/wake] [/shutdown]
[/deletefiles] [/timeout=Timeout(sec)] [/usecomputerprofiles]
[/RebootCountdown=Time(sec)] [/RebootCountdownMessage="Custom message"]
[/RebootAtFirstOccurenceOf=Time(formatted as "hh:mm:ss")]
[/ShutDownAtFirstOccurenceOf=Time(formatted as "hh:mm:ss")] [/RebootInInterval]
[/ShutDownInInterval] [/RebootIntervalStart=Time(formatted as "hh:mm:ss")]
[/RebootIntervalEnd=Time(formatted as "hh:mm:ss")] [/?]
```

deploycmd command switches

Switch	Description
Target	Specify the name(s), IP or range of IPs of the target computer(s) on which the patch(es) will be deployed.
/File	Specify the file that you wish to deploy on the specified target(s).
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during patch deployment. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the Dashboard.
/warnuser	(Optional) Include this switch if you want to inform the target computer user that a file/patch installation is in progress. Users will be informed through a message dialog that will be shown on screen immediately before the deployment session is started.
/useraproval	(Optional) Include this switch to request the user's approval before starting the file/patch installation process. This allows users to postpone the file/patch installation process for later (for example, until an already running process is completed on the target computer).
/stopservice	(Optional) Include this switch if you want to stop specific services on the target computer before installing the file/patch. **NOTE** You cannot specify the services that will be stopped directly from the command line tool. Services can only be added or removed through the GFI LanGuard UI.
/customshare	(Optional) Specify the target share where you wish to transfer the file before it is installed.
/reboot	(Optional Parameter) Include this switch if you want to reboot the target computer after file/patch deployment.
/rebootuserdecides	(Optional Parameter) Include this switch to allow the current target computer user to decide when to reboot his computer (after patch installation).
/wake	Wakes up offline computers.
/shutdown	(Optional Parameter) Include this switch if you want to shut down the target computer after the file/patch is installed.
/deletefiles	(Optional Parameter) Include this switch if you want to delete the source file after it has been successfully installed.
/timeout	(Optional Parameter) Specify the deployment operation timeout. This value defines the time that a deployment process will be allowed to run before the file/patch installation is interrupted.
/usecomputerprofiles	(Optional) Use data from computer profiles.
/RebootCountdown	(Optional) Display a reboot countdown window for a number of seconds to the remote user before rebooting.
/RebootCountdownMessage	(Optional) Used in conjunction with **/RebootCountdown**. Displays a custom message to the remote user before rebooting the computer.
/RebootAtFirstOccurenceOf	(Optional) Reboot a computer at the first occurrence of a specified time. The time is expected in the 24 hour format "hh:mm:s s". Example, 18:30:00.
/ShutDownAtFirstOccurenceOf	(Optional) Shutdown a computer at the first occurrence of a specified time. The time is expected in the 24 hour format "hh:mm:s s". Example, 18:30:00.
/RebootInInterval	(Optional) Reboot the computer after deployment if deployment completes in the specified time interval. Otherwise wait to specify the interval manually. Requires parameters `/RebootIntervalStart` and `/RebootIntervalEnd`.

Switch	Description
/ShutdownIntervalStart	(Optional) Dependent on **/Shutdown**. The start time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutdownIntervalEnd	(Optional) Dependent on **/Shutdown**. The end time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutDownInInterval	(Optional) Shutdown the computer after deployment if deployment completes in the specified time interval. Otherwise wait to specify the interval manually.
/?	(Optional) Use this switch to show the command line tool's usage instructions.

Example

1. Deploy a file called 'patchA001002.XXX'.

2. On target computer 'TMJohnDoe'.

3. Reboot the target computer after successful deployment of the file.

The command should be as follows::

```
deploycmd TMJohnDoe /file="patchA001002.XXX" /reboot
```

Using impex.exe

The Impex tool is a command line tool that can be used to Import and Export profiles and vulnerabilities from GFI LanGuard Network Security Scanner. The parameters supported by this tool are the following:

```
impex [[/H] | [/?]] | [/XML:xmlfile [/DB:dbfile] [[/EX] [/MERGE]] | [/IM
[/ONLYNEWER]] [/PROFILES | /VULNS | /PORTS | /PROFILE:name | /VULNCAT:cat
[/VULN:name] | /PORTTYPE:type [/PORT:number]] [/SKIP | /OVERWRITE | /RENAME:value]]
```

impex command switches

Switch	Description
/H **/?** **Run impex without parameters**	Displays help information.
/XML:<xmlfile>	This parameter specifies the name of the imported or exported XML file. <xmlfile> needs to be replaced with the name of the file the profile is being exported to. **NOTE** This parameter is mandatory to import or export alerts.
/DB:<dbfile>	Where <dbfile> is the database file to be used during the import/export operation. If this is not specified the default "operationsprofiles.mdb" file will be used.
/EX	Exports data from database to XML file (Default option)
/MERGE	If this is specified when the target XML for export already exists, the file will be opened and data will be merged; otherwise the XML file is first deleted.
/IM	Imports data from XML file to database
/ONLYNEWER	When specified only vulnerabilities newer than the newest vulnerability in the database will be imported.
/PROFILES	Exports/Imports all scanning profiles.
/VULNS	Exports/Imports all vulnerabilities.

Switch	Description
/PORTS	Exports/Imports all ports
/PROFILE:<name>	Exports/Imports the specified scanning profile.
/VULNCAT:<category>	Exports/Imports all vulnerabilities of the specified category.
/VULN:<name>	Exports/Imports the specified vulnerability (/VULNCAT must be specified).
/PORTTYPE:<type>	Exports/Imports all ports of the specified type.
/PORT:<number>	Exports/Imports the specified port (/PORTTYPE must be specified).
/SKIP	If an item already exists in the target XML/database, that item will be skipped
/OVERWRITE	If an item already exists in the target XML/database, that item will be overwritten.
/RENAME:<value>	If an item already exists in the target XML/database, that item will be renamed to <value>. If /PROFILE or /VULN was specified, port information merged with that item is a port or renamed by prefixing its name with <value> in any other case.

Example 1

To import specific entries from an XML file:

```
impex /xml:regcheck.xml /vuln:"Blaster Worm" /vulncat:"Registry Vulnerabilities"
```

Example 2

To import a whole XML file:

```
impex /xml:regcheck.xml /im
```

NOTE

The Impex executable can be located in the GFI LanGuard installation folder.

NOTE

If the specified `<xmlfile>`, `<dbfile>`, `<name>`, `<category>` or `<value>` contain any space character, the whole value must be placed between double quotes. Example:

- `<xmlfile>` containing space = `"Vulnerability Checks Definitions.xml"`
- `<xmlfile>` without space = `VulnerabilityChecksDefinitions.xml`

NOTE

It is recommended that if the vulnerabilities are imported into another installed instance of GFI LanGuard; that installation will have the same build number as the one the database has been exported from.

IMPORTANT

It is highly recommended not to use the **Impex** tool if GFI LanGuard application (LanGuard.exe) or LanGuard scanning profiles (scanprofiles.exe) are running.

5.7 Script Debugger

Scripts that identify custom vulnerabilities can be created using any VBScript compatible scripting language. By default, GFI LanGuard ships with a script editor that you can use to create your custom scripts.

New checks must be included in the list of checks supported by GFI LanGuard. Use the Vulnerability Assessment tab to add new checks to the default list of vulnerability checks on a scan profile by scan profile basis. GFI LanGuard also supports Python scripting.

Topics in this section:

5.7.1 Creating custom scripts using VBscript

GFI LanGuard supports and runs scripts written in VBscript compatible languages. Use VBscript compatible languages to create custom scripts that can be run against your network targets.

Security auditing scripts can be developed using the script editor that ships with GFI LanGuard. This built–in script editor includes syntax highlighting capabilities as well as debugging features that support you during script development. Open the script editor from **Start > Programs > GFI LanGuard > LanGuard Script Debugger**.

> **NOTE**
> For more information on how to develop scripts using the built–in script editor, refer to the **Scripting documentation** help file included in **Start > Programs > GFI LanGuard > LanGuard Scripting documentation**.

> **NOTE**
> GFI does not support requests related to problems in custom scripts. You can post any queries that you may have about GFI LanGuard forums at http://forums.gfi.com/. Through this forum, you are able to share scripts, problems and ideas with other GFI LanGuard users.

Adding a vulnerability check that uses a custom VBScript (.vbs)

To create new vulnerability checks that use custom VBScripts, follow the steps described in this section:

- Step 1: Create the script
- Step 2: Add new vulnerability checks
- Step 3: Test the vulnerability check/script

Step 1: Create the script

1. Launch the Script Debugger from **Start > Programs > GFI LanGuard > LanGuard Script Debugger**.
2. Go on **File > New**.
3. Create a script. For this example, use the following sample script code.

```
Function Main
   echo "Script has run successfully"
```

```
    Main = true
End Function
```

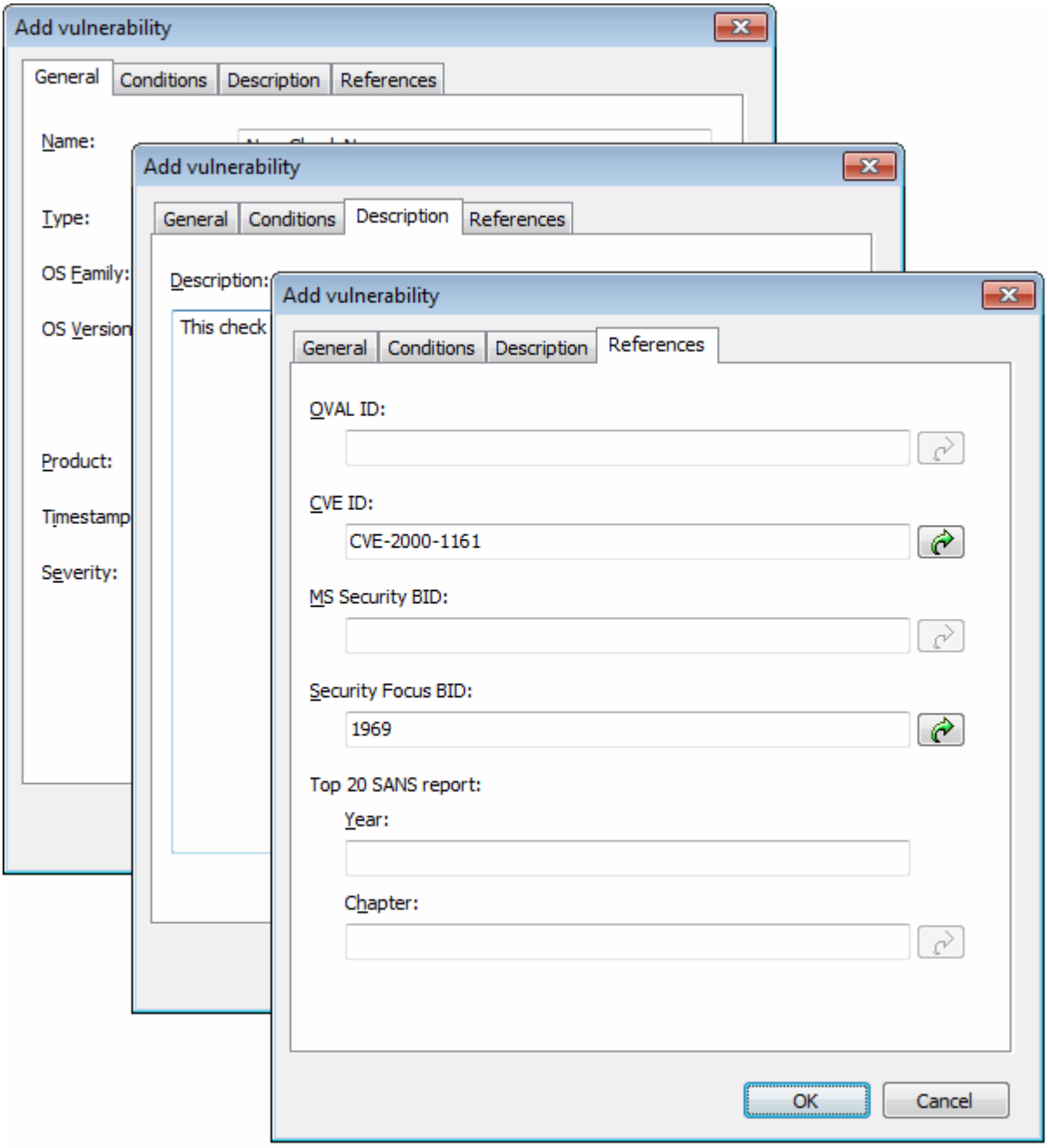
4. Save the script in `<LanGuard installation folder path> \Data\Scripts\myscript.vbs`.

Step 2: Add new vulnerability checks

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

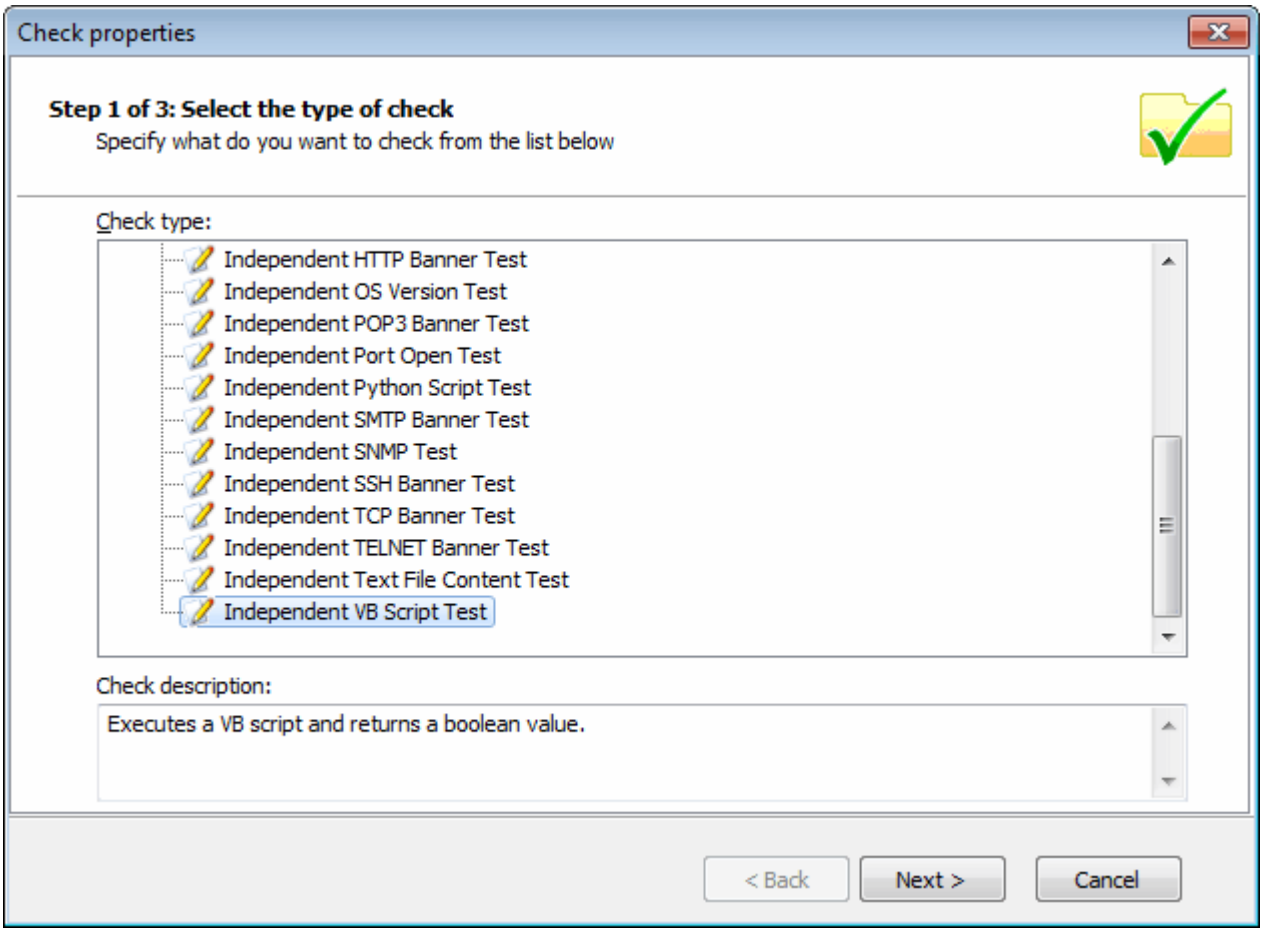
3. In the new window, add a new vulnerability by clicking **Add** under the list of vulnerability checks.



Screenshot 204: Add vulnerability dialog

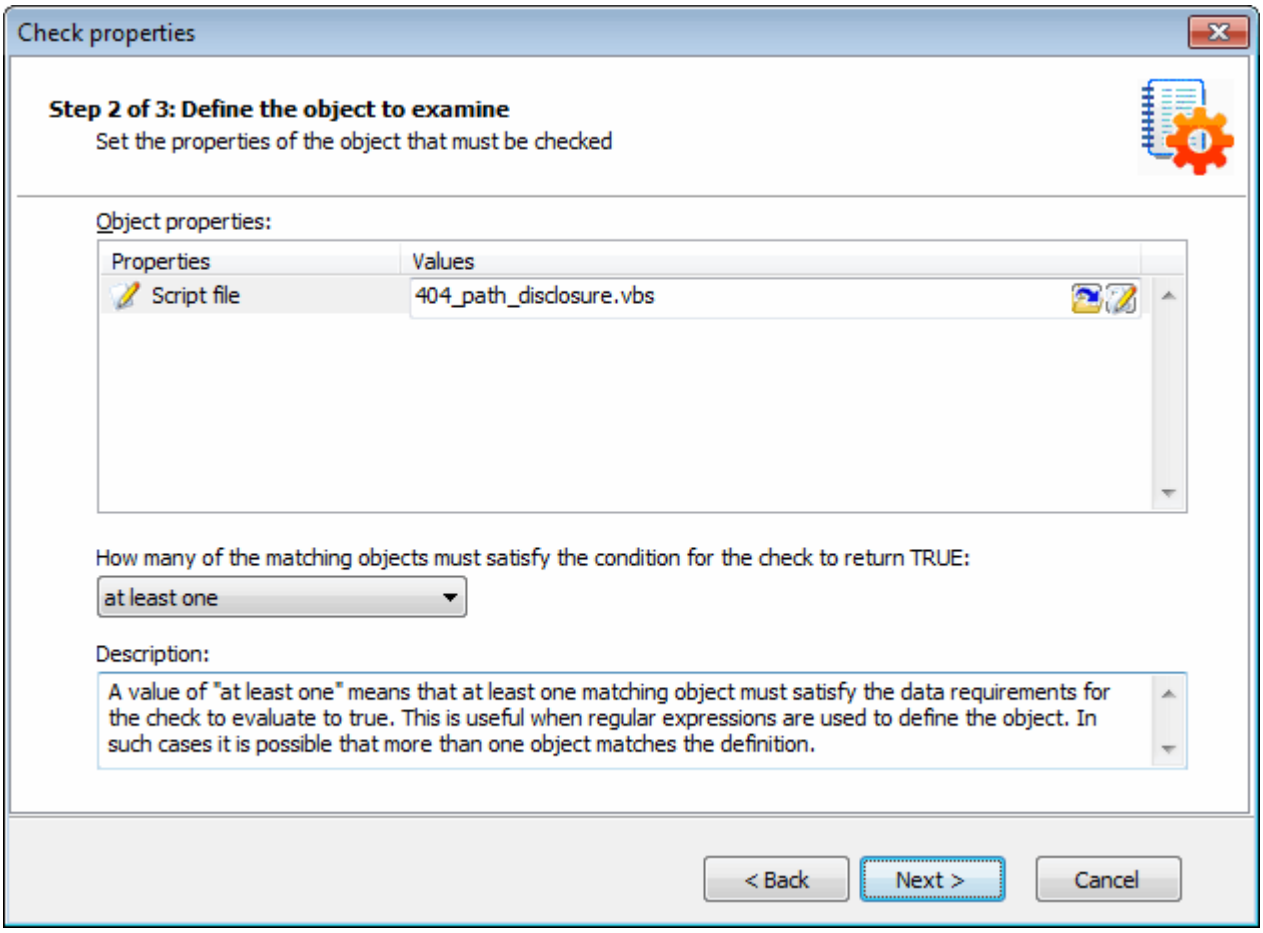
4. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

5. Click the **Conditions** tab and click on the **Add** button. This will bring up the check properties wizard.



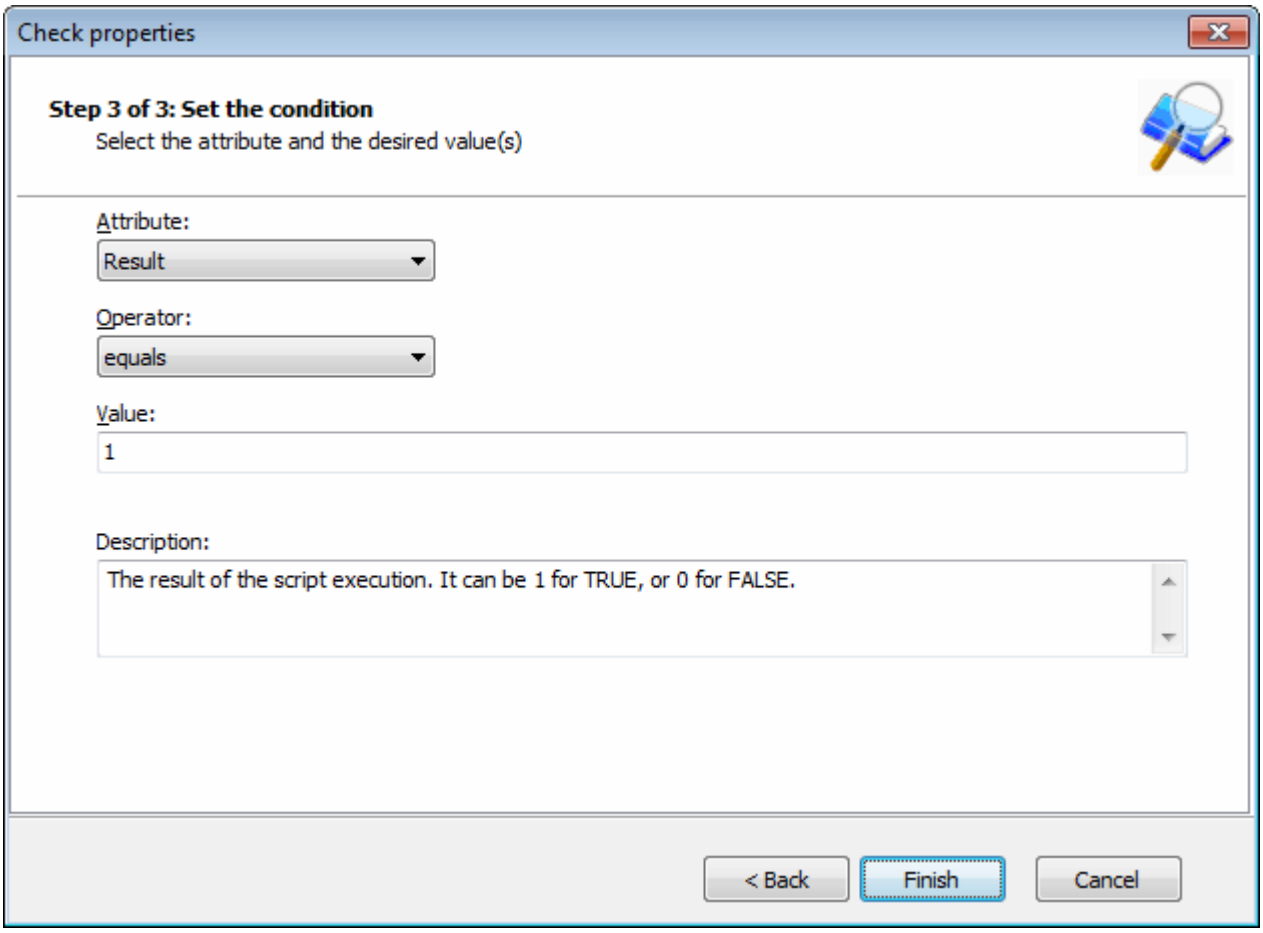
Screenshot 205: Adding vulnerability checks - Select type of check

6. Select **Independent checks > VBScript** node and click **Next**.



Screenshot 206: Adding vulnerability checks - Select VB Script file

7. Click **Choose file** and select the custom VBscript file that will be executed by this check. Click **Next**.



Screenshot 207: Adding vulnerability checks - Define conditions

8. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

9. Click **OK** to save new vulnerability check.

Step 3: Test the vulnerability check/script

Scan your local host computer using the scanning profile where the new check was added.

In **Scan** tab > **Results**, a vulnerability warning will be shown in the **Vulnerability Assessment** node of the scan results.

5.7.2 Creating custom scripts using Python Scripting

GFI LanGuard also supports a new type of vulnerability checks – Python Script Test. This type of check is available under the Independent Checks type.

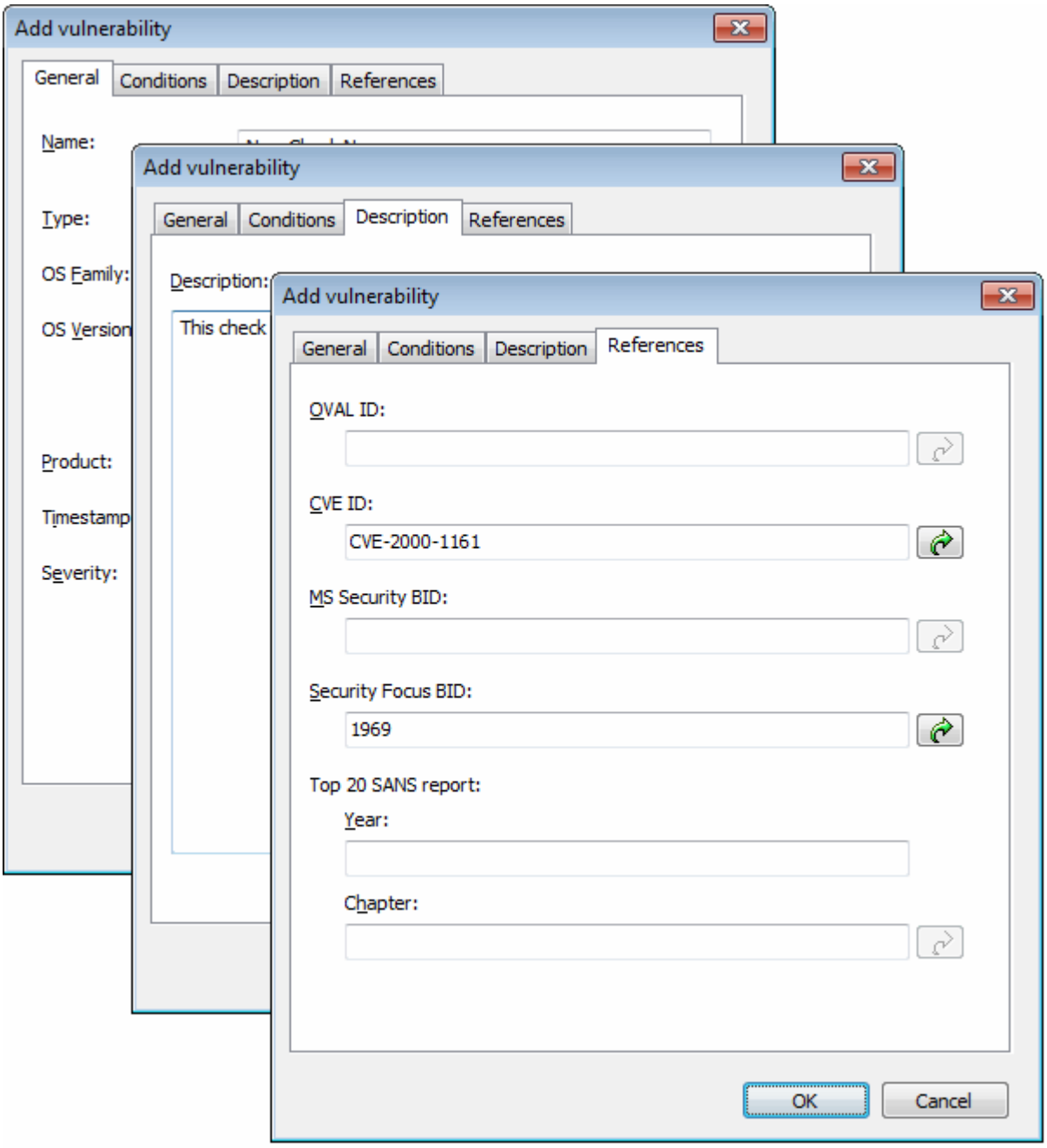
> **IMPORTANT**
> For information about Python Scripting, refer to the GFI LanGuard scripting documentation from **Start > Programs > GFI LanGuard>GFI LanGuard Scripting Documentation**.

To add a new python script check:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

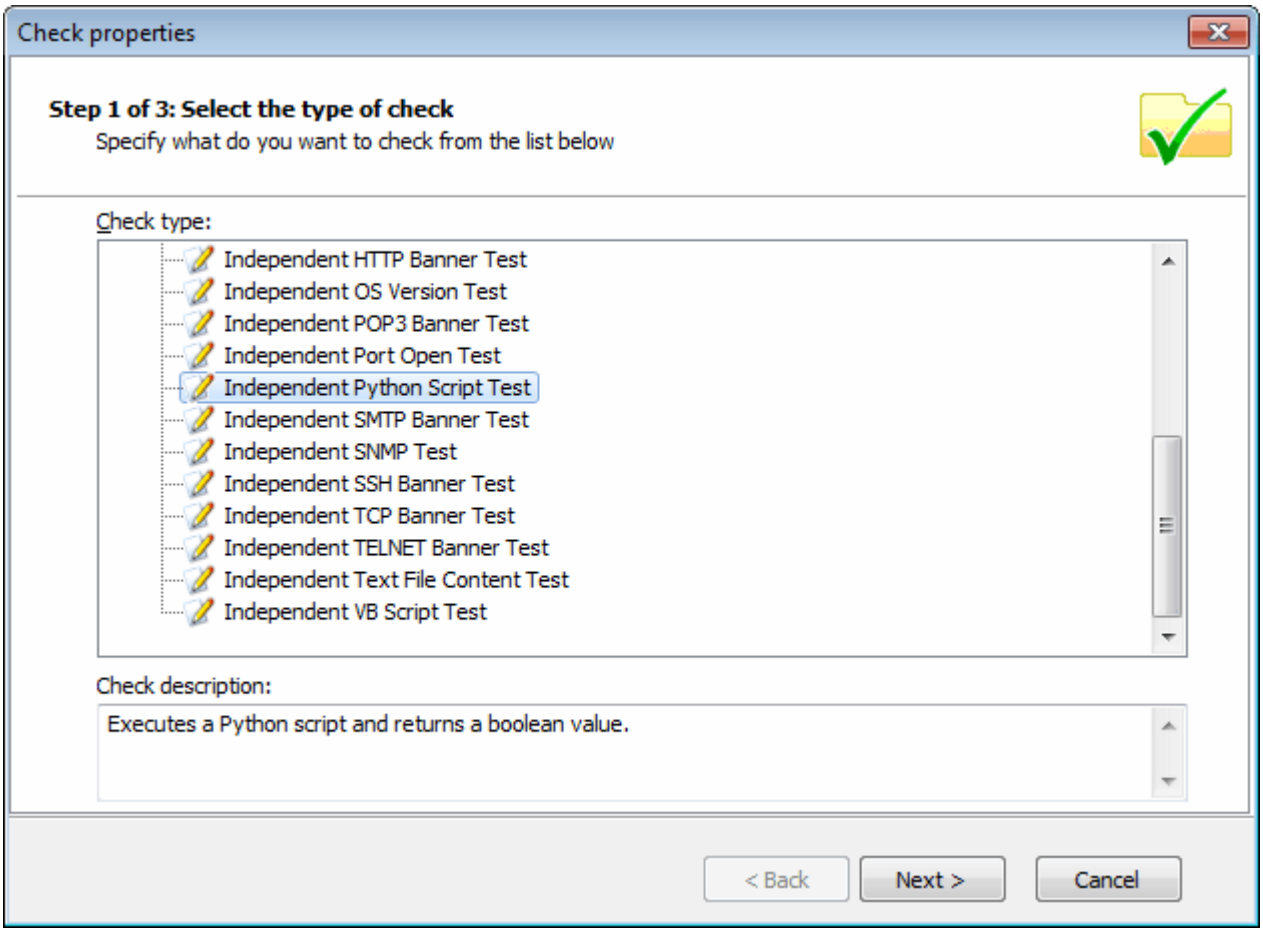
3. In the new window, add a new vulnerability by clicking **Add** under the list of vulnerability checks.



Screenshot 208: Add vulnerability dialog

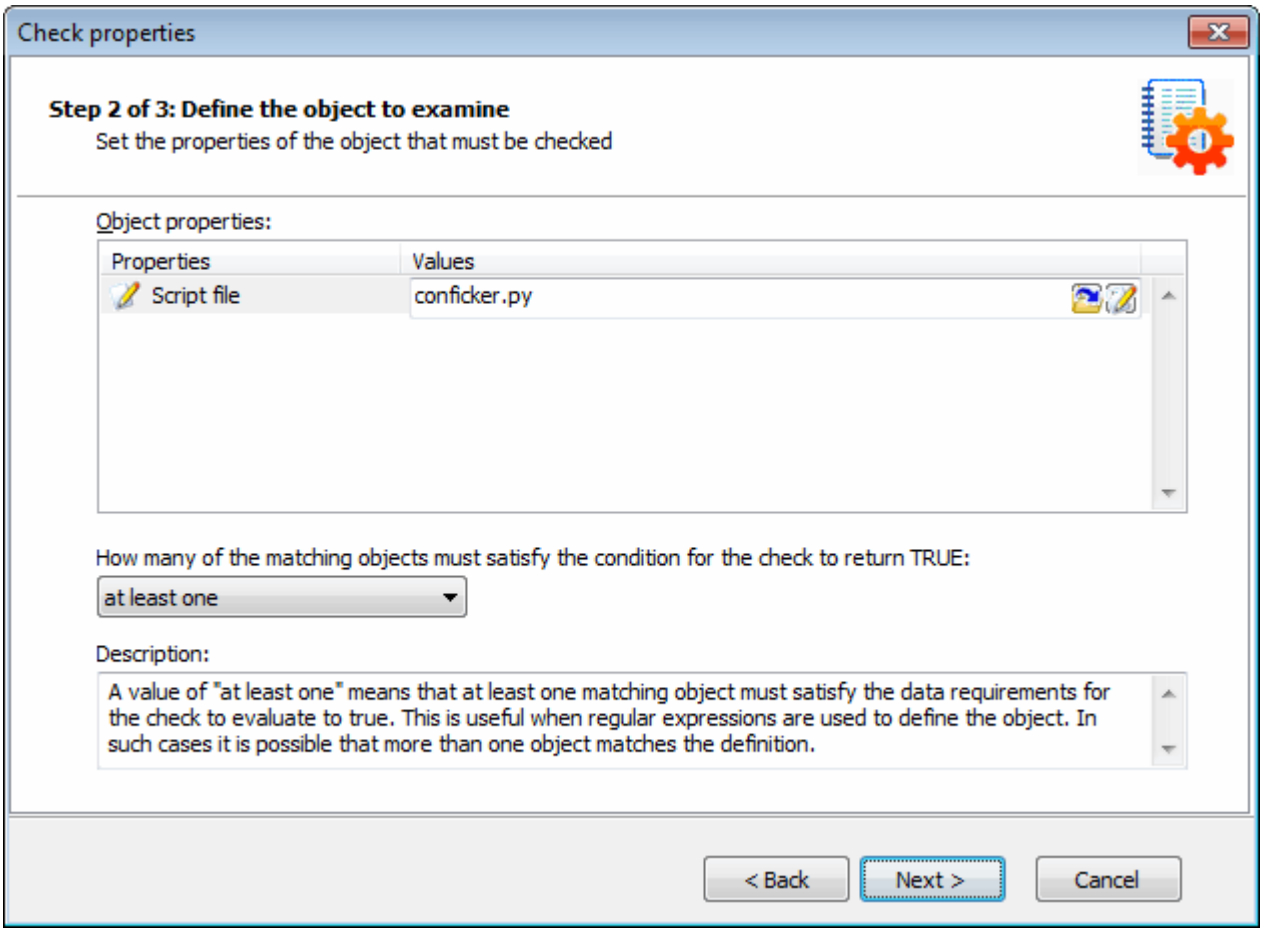
4. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

5. Click the **Conditions** tab and click on the **Add** button. This will bring up the check properties wizard.



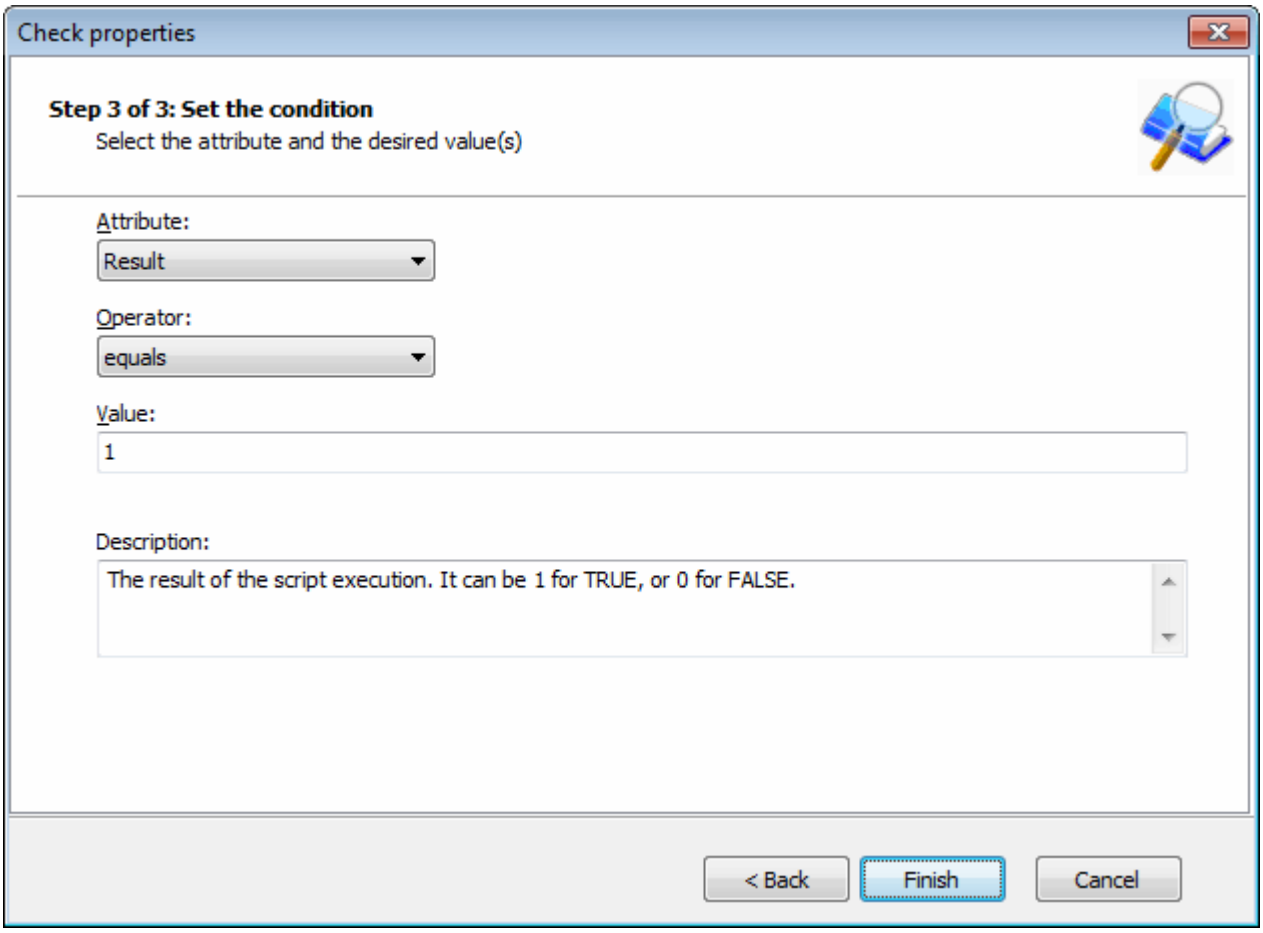
Screenshot 209: Adding vulnerability checks - Select type of check

6. Select **Independent checks > Independent Python Script Test** node and click **Next**.



Screenshot 210: Adding vulnerability checks - Select Python Script file

7. Click **Choose file** and select the custom Python Script file that will be executed by this check. Click **Next**.



Screenshot 211: Adding vulnerability checks - Defining conditions

8. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

9. Click **OK** to save new vulnerability check.

5.7.3 SSH Module

GFI LanGuard includes an SSH module which handles the execution of vulnerability scripts on Linux/UNIX based systems.

The SSH module determines the result of vulnerability checks through the UI (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target operating system.

Keywords

The SSH module can run security scanning scripts through its terminal window. When a security scan is launched on Linux/UNIX based target computers, vulnerability checking scripts are copied through an SSH connection to the respective target computer and run locally.

The SSH connection is established using the logon credentials (i.e. username and password/SSH Private Key file) specified prior to the start of a security scan.

The SSH module can determine the status of a vulnerability check through specific keywords present in the text output of the executed script. These keywords are processed by the module and interpreted as instruction for the GFI LanGuard. Standard keywords identified by the SSH module include the following:

Keyword	Description
`TRUE: / FALSE`	These strings indicate the result of the executed vulnerability check/script. When the SSH module detects a TRUE: it means that the check was successful; FALSE: indicates that the vulnerability check has failed.
`AddListItem`	This string triggers an internal function that adds results to the vulnerability check report (i.e. scan results). These results are shown in GFI LanGuard after completion of a scan. This string is formatted as follows: `AddListItem([[[[parent node]]]],[[[[actual string]]]])`
`[[[[parent node]]]]`	Includes the name of the scan results node to which the result will be added.
`[[[[actual string]]]]`	Includes the value that will be added to the scan results node. **NOTE** Each vulnerability check is bound to an associated scan result node. This means that 'AddListItem' results are by default included under an associated/default vulnerability node. In this way, if the parent node parameter is left empty, the function will add the specified string to the default node.
`SetDescription`	This string triggers an internal function that will overwrite the default description of a vulnerability check with a new description. This string is formatted as follows: SetDescription([New description])
`!!SCRIPT_ FINISHED!!`	This string marks the end of every script execution. The SSH module will keep looking for this string until it is found or until a timeout occurs. If a timeout occurs before the '!!SCRIPT_FINISHED!!' string is generated, the SSH module will classify the respective vulnerability check as failed. **NOTE** It is imperative that every custom script outputs the '!!SCRIPT_FINISHED!!' string at the very end of its checking process.

Adding a vulnerability check that uses a custom shell script

In the following example a vulnerability check is created (for Linux based targets) which uses a script written in Bash. The vulnerability check in this example will test for the presence of a dummy file called 'test.file'

Step 1: Create the script

1. Launch your favorite text file editor.
2. Create a new script using the following code:

```
#!/bin/bash
if [ -e test.file ]
then
   echo "TRUE:"
else
   echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
```

3. Save the file in `<GFI LanGuard installation folder path>..\Data\Scripts\myscript.sh`

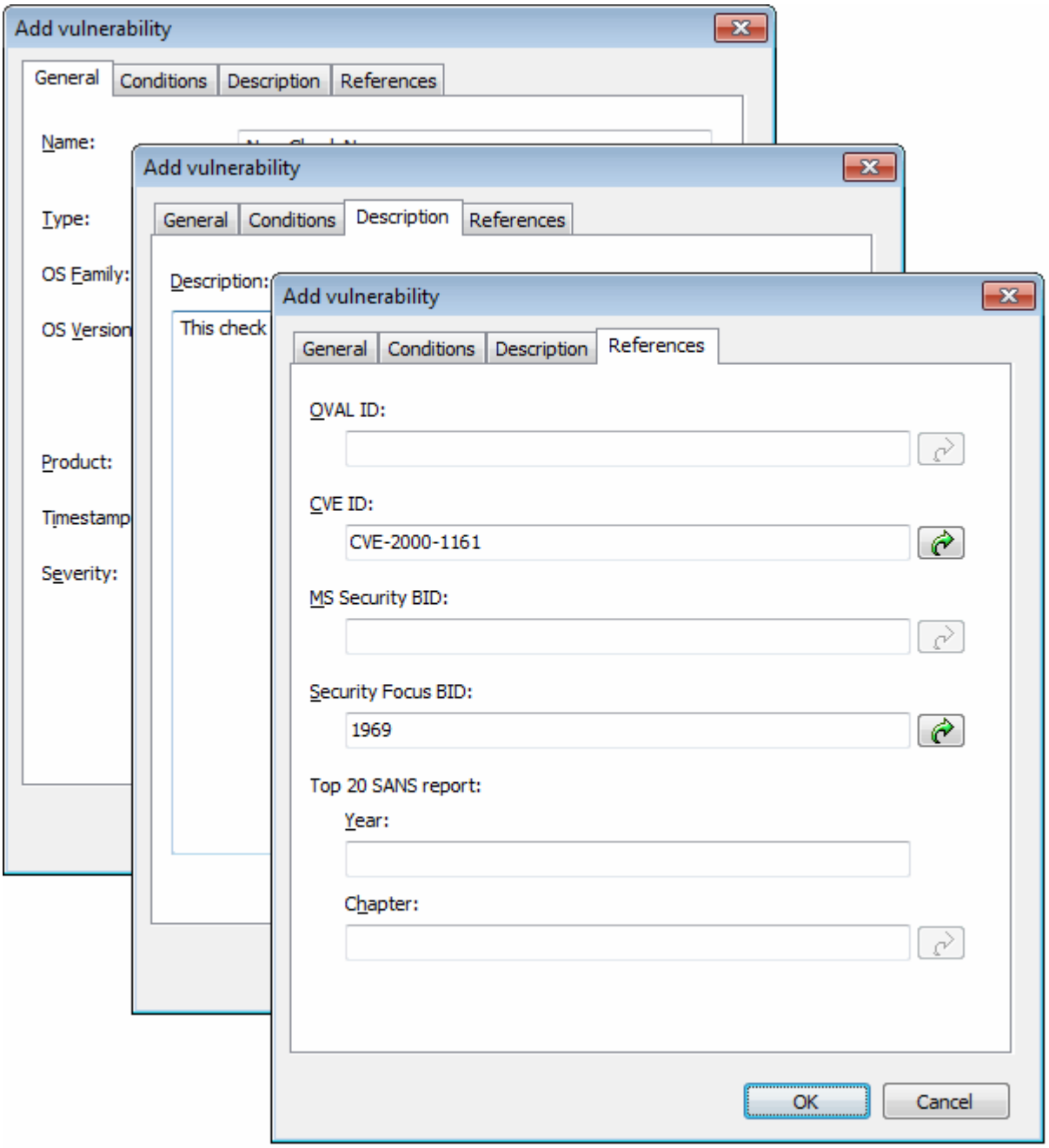
Step 2: Add the new vulnerability check

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. From the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities…).

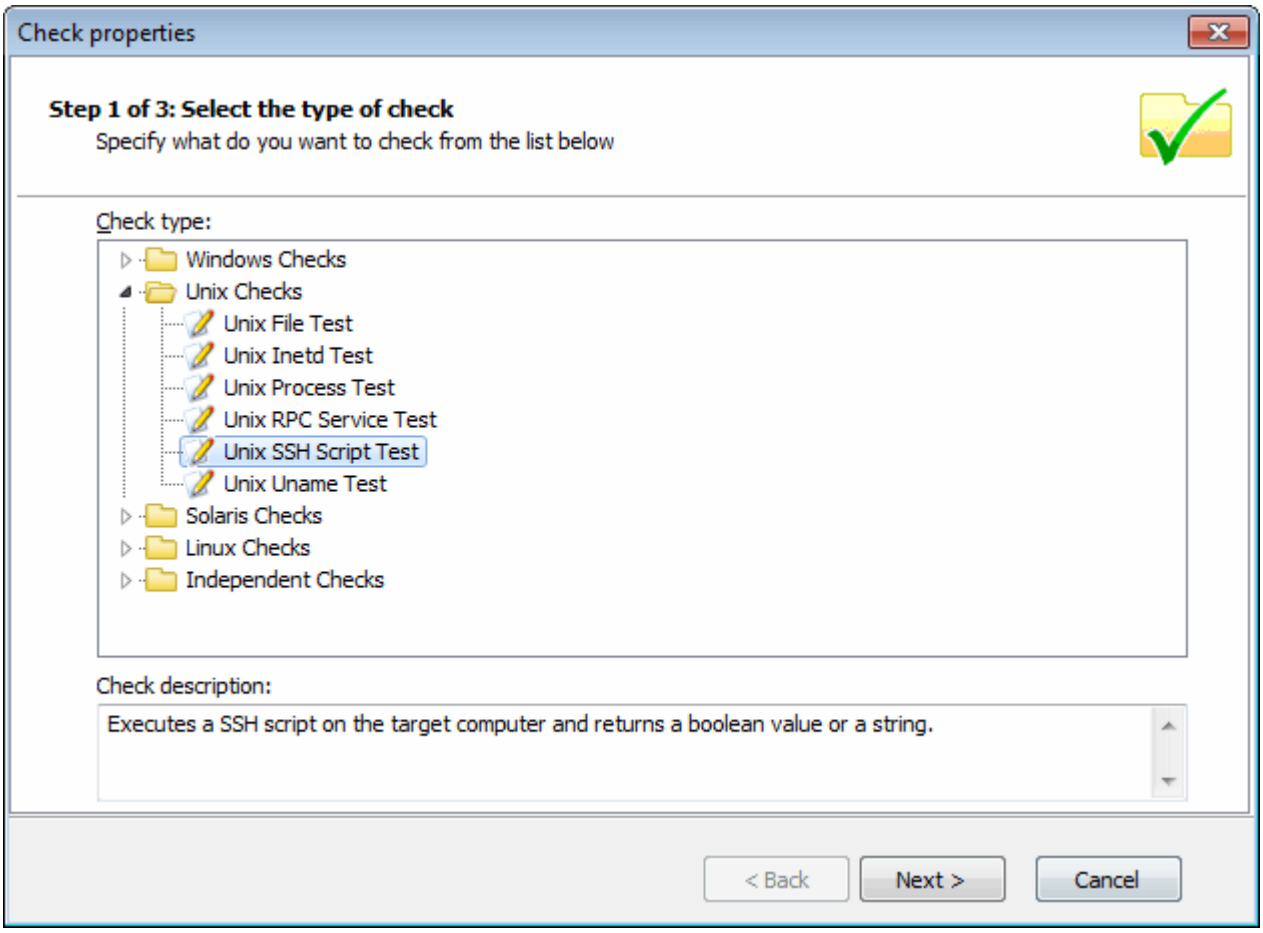
4. In the new window, add a new vulnerability by clicking **Add** in the middle pane.



Screenshot 212: Add vulnerability dialog

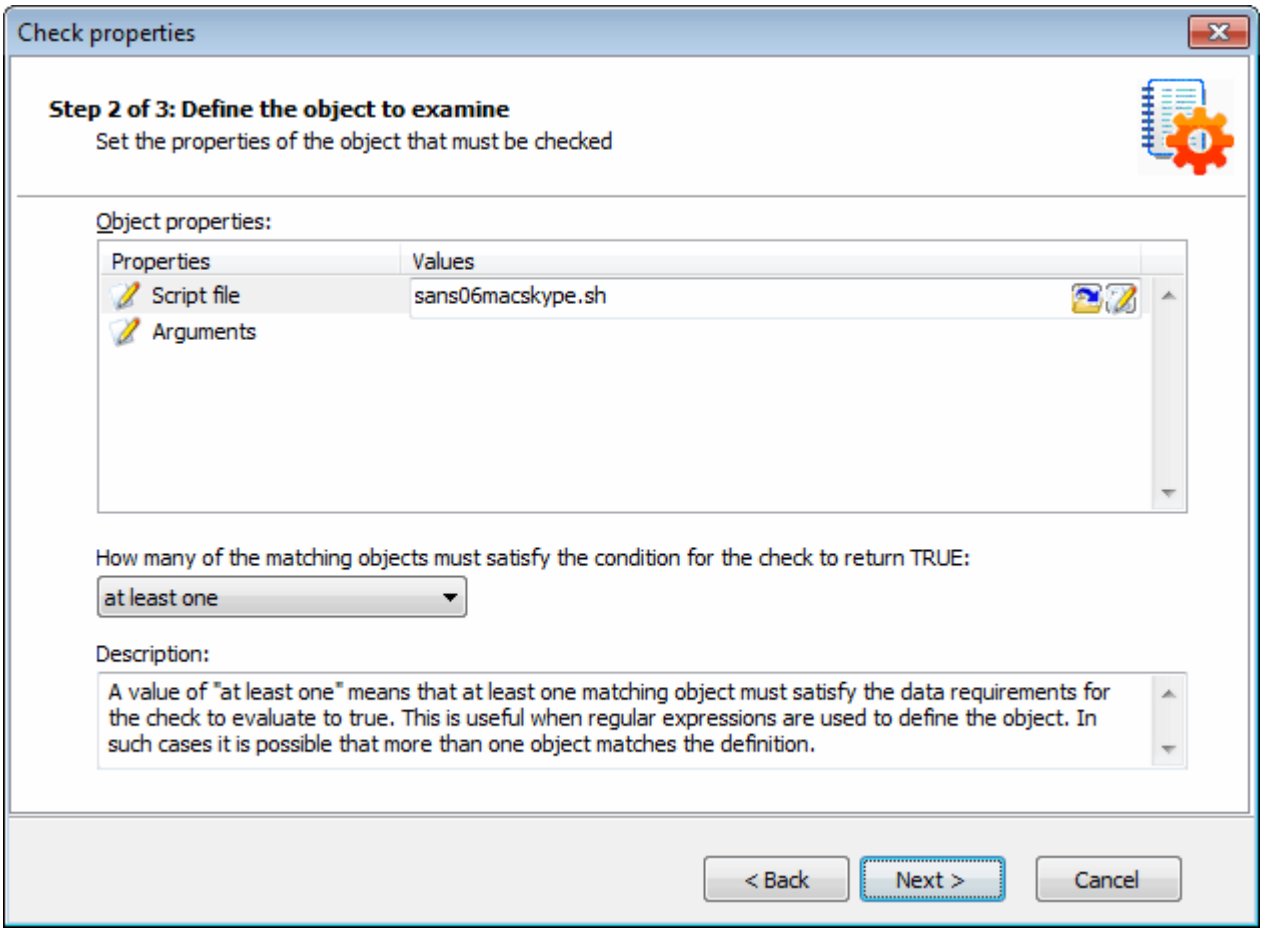
5. Go through the **General**, **Description** and **Reference** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Choose the **Conditions** tab and click **Add** button. This will bring up the check properties wizard.



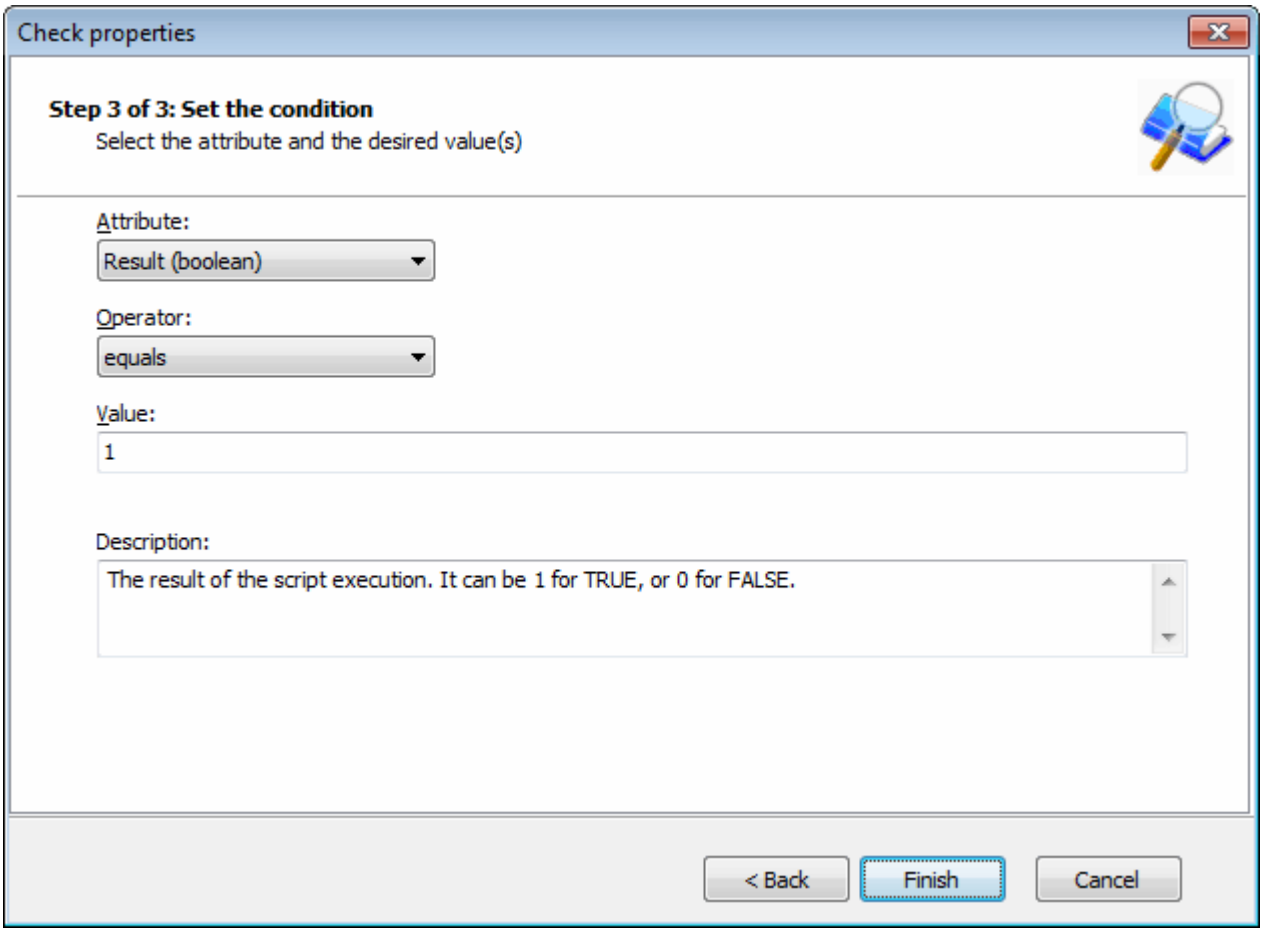
Screenshot 213: Adding vulnerability checks - Select type of check

7. Select **Unix checks > SSH Script Test** node and click on Next button to continue setup.



Screenshot 214: Adding vulnerability checks - Select SSH file

8. Click **Choose file** and select the custom SSH Script file that will execute during this check. Click **Next** to proceed.



Screenshot 215: Adding vulnerability checks - Define conditions

9. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

10. Click **OK** to save new vulnerability check.

Step 3: Test the vulnerability check/script used in the example

Scan your local host computer using the scanning profile where the new check was added.

1. Log on to a Linux target computer and create a file called 'test.file'. This check will generate a vulnerability alert if a file called 'test.file' is found.

2. Launch a scan on the Linux target where you created the file.

3. Check you scan results.

5.8 Configuring NetBIOS

To check if your scan targets are using NetBIOS:

1. Navigate to **Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**.

> **Note**
> In Windows® XP, click **Control Panel > Network Connections**.

2. Right–click on **Local Area Connection** and select **Properties**.

3. Click **Internet Protocol (TCP/IP)** and select **Properties**.

4. Click **Advanced > WINS**.

5. From the **NetBIOS setting** area, ensure that **Default** or **Enable NetBIOS over TCP/IP** are selected.

6. Click **OK** and exit the **Local Area Properties** dialog(s).

> **NOTE**
> If static IP is being used or the DHCP server does not provide NetBIOS setting, select the Enable NetBIOS over TCP/IP option.

5.9 Uninstalling GFI LanGuard

To uninstall GFI LanGuard:

1. Click **Start > Control Panel > Add or Remove Programs**.

2. Select GFI LanGuard from the list, and click **Remove**.

3. In the uninstall wizard, click **Next**.

4. Select the configuration data files to remove during un–installation and click **Next**.

5. On completion, click **Finish**.

6 Troubleshooting and support

This topic explains how to resolve issues encountered while using GFI LanGuard. These issues can be resolved using the contents of this guide. If any issues remain unresolved after reviewing the manual, check if your problem is listed below.

Refer to the following sections for information about resolving common issues and contacting our support team.

Topics in this section:

6.1 Resolving common issues

The table below provides you with solutions to the most common problems you may encounter when using GFI LanGuard:

Issue Encountered	Solution/Description
The database structure is incorrect. Do you want to delete and recreate the database?	**Description** This warning is usually encountered when trying to configure the database backend. It occurs when the database structure is corrupted. Or The database returns a timeout because the connection cannot be established. **Solution** When this message is encountered: Check that all SQL credentials are correct and there are no connectivity problems between the GFI LanGuard machine and the SQL server. It is important to note that when OK is clicked all saved scans are lost.
In **Configuration > Database Maintenance Options > Database backend settings** Microsoft Access database option is unavailable.	GFI LanGuard 12 and later versions do not support Microsoft Access databases. We recommend using Microsoft SQL Server Express which is available as a free download.

Issue Encountered	Solution/Description
Incomplete results and errors when scanning remote machines	**Description** Errors similar to the following may be encountered: » Failed to open test key to remote registry » The scan will not continue » Access Denied » Could not connect to remote SMB server. These errors may be encountered because: » The remote machine has an account similar to the one used by GFI LanGuard to log in as an administrator. » The user account used by GFI LanGuard does not have administrative privileges. **Solution** To solve this issue do one of the following: » Log on the GFI LanGuard machine and configure GFI LanGuard to use an alternate domain administrator account. » Delete the local user account on the remote machine. » Launch GFI LanGuard executable with 'Run As' using a Domain Administrator account. **NOTE** For more information, refer to http://go.gfi.com/?pageid=LAN_ProbScanningRM
GFI LanGuard program updates not working	**Description** Updates will not work if GFI LanGuard machine does not have a direct connection to the Internet. **Solution** To solve this issue do one of the following: » Configure GFI LanGuard machine to have direct Internet access. » Install another instance of GFI LanGuard on a machine with Internet access and configure GFI LanGuard to check for updates from the new installation. » Check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to Gateway permissions (page 22). **NOTE** For more information refer to http://go.gfi.com/?pageid=LAN_CheckAltUpdates
Firewall installed on GFI LanGuard is blocking connection with target computers	**Description** Scanning might slow down or be blocked if a firewall is installed on GFI LanGuard machine. **Solution** Configure the firewall to allow the following components in outbound connections: » <..\Program Files\GFI\LanGuard>*.exe » <..\Program Files\GFI\LanGuard Agent>*.exe **NOTE** For more information, refer to http://go.gfi.com/?pageid=LAN_SetBestPerformance
GFI LanGuard is failing to retrieve workgroup computers when using Enumerate Computers	**Description** GFI LanGuard uses the Windows mechanism to retrieve the machines within a workgroup. In this mechanism a Master Browser computer will create and store a list of all computers. In some cases, the Master Browser role can fail resulting in GFI LanGuard not retrieving computers information. **NOTE** To solve this issue, refer to http://go.gfi.com/?pageid=LAN_CannotEnumerate

Issue Encountered	Solution/Description
GFI LanGuard found open ports that another port scanner found closed	**Description** GFI LanGuard uses a different approach than other port scanners to detect open ports. **Solution** To view the status of a port and determine if the port is closed or opened: 1. Click **Start > Programs > Accessories > Command Prompt**. 2. Key in `netstat -an`, and press **Enter**. 3. The generated list displays all computer active connections.

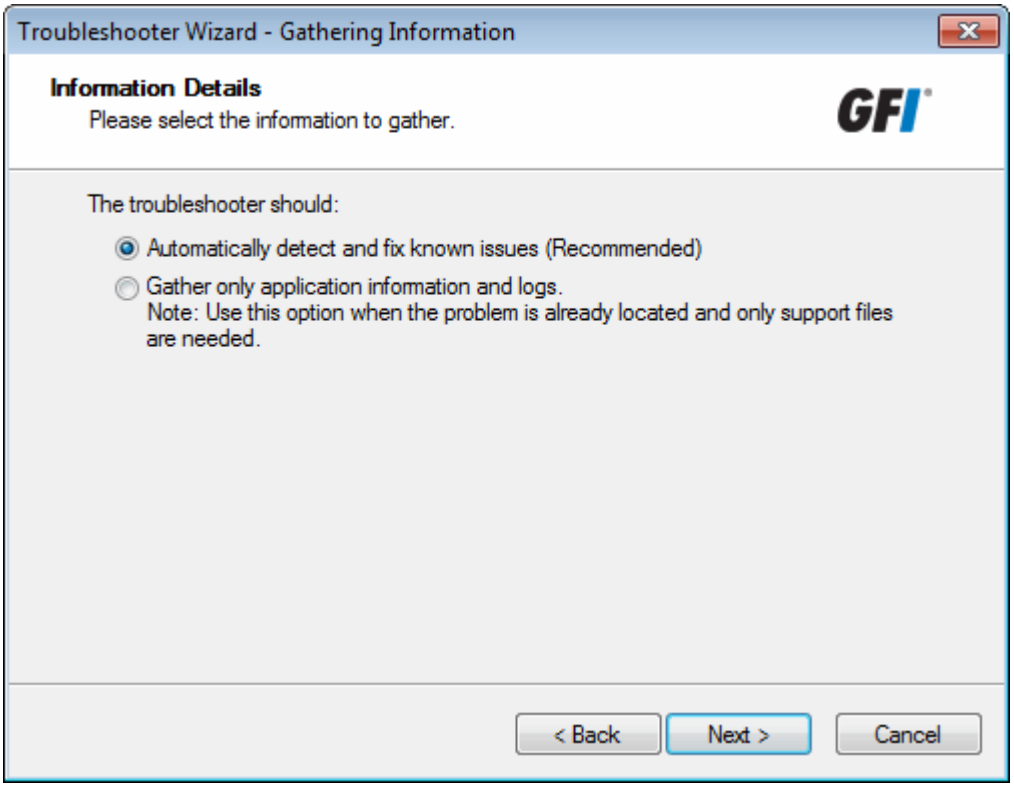
6.2 Using the Troubleshooter Wizard

The GFI LanGuard troubleshooter wizard is a tool designed to assist you when encountering technical issues related to GFI LanGuard. Through this wizard, you are able to automatically detect and fix common issues as well as gather information and logs to send to our technical support team.

To use the Troubleshooter Wizard:

1. Launch the troubleshooting wizard from the **Start > Programs > GFI LanGuard > GFI LanGuard Troubleshooter**.

2. Click **Next** in the introduction page.

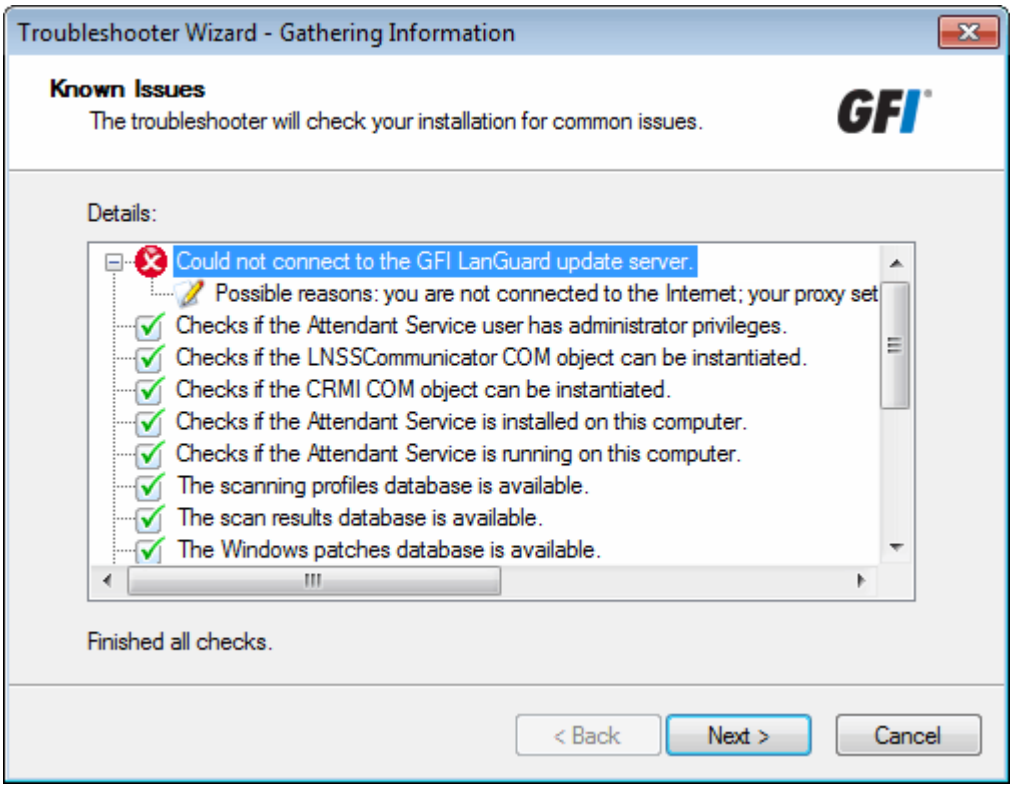


Screenshot 216: Troubleshooter wizard – Information details

3. In the Information details page select one of the following options described below:

Option	Description
Automatically detect and fix known issues	(Recommended) Configure GFI LanGuard to automatically detect and fix issues.
Gather only application information and logs	Gather logs to send to GFI support.

4. Click **Next** to continue.



Screenshot 217: Troubleshooter wizard – Gathering information about known issues

5. The troubleshooter wizard will retrieve all the information required to solve common issues. Click **Next** to continue.

6. The troubleshooter will fix any known issues that it encounters. Select **Yes** if your problem was fixed or **No** if your problem is not solved to search the GFI Knowledge base for information.

6.3 Using the Agent Diagnostics Tool

The GFI LanGuard Agent Diagnostics tool is designed to assist you in case of technical issues related to GFI LanGuard. Through this tool, you can verify agent connectivity, view error messages and obtain a a summary with all the relevant state information about the agent.

To use the Agent Diagnostics Tool:

1. Select the agent from the computer tree from the **Dashboard**.

2. Right click agent and select **Agent Diagnostics**.

3. The Agent Diagnostics Tool retrieves all the information required to solve common issues. Click **Export** to export and view the diagnostics report.

6.4 GFI Knowledge Base

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. In the event that the information in this guide does not solve your problems, next refer to the GFI Knowledge Base by visiting https://www.gfi.com/support/products/gfi-languard.

6.5 Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting http://forums.gfi.com

6.6 Requesting technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

» **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp

» **Phone**: To obtain the correct technical support phone number for your region visit: https://www.gfi.com/company/contact.htm

> **NOTE**
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on documentation@gfi.com.

7 Glossary

A

Access™

A Microsoft® desktop relational database management system included in the Microsoft® Office package. Access™ is normally used for small databases.

Active Directory™ (AD)

A technology that provides a variety of network services, including LDAP-like directory services.

Anti-spyware

A software countermeasure that detects spyware installed on a computer without the user's knowledge.

Antivirus

A software countermeasure that detects malware installed on a computer without the user's knowledge.

Apache web server

An open source HTTP server project developed and maintained by the Apache software foundation.

Applications auto-uninstall

An action that enables the auto-uninstall of applications that support silent uninstall from GFI LanGuard.

Auto-download

A GFI LanGuard technology that automatically downloads missing patches and service packs in all 38 languages.

Auto-patch management

A GFI LanGuard technology that automatically downloads missing Microsoft® updates and deploys them over the network.

Auto-remediation

A GFI LanGuard technology that automatically downloads and deploy missing patches. If an application is blacklisted in GFI LanGuard, auto-remediation will uninstall the application from the target computer during scheduled operations.

B

Backdoor program

An alternative method used to access a computer or computer data over a network.

Batch-files

A text files containing a collection of instructions to be carried out by an operating system or an application.

Blacklist

A list of USBs or Network devices names that are considered as dangerous. When a USB\Network device name contains a blacklisted entry while scanning a network, GFI LanGuard will report the device as a security threat (High security vulnerability).

Bluetooth

An open wireless communication and interfacing protocol that enables exchange of data between devices.

Bulletin Information

Contains a collection of information about a patch or a Microsoft® update. Used in GFI LanGuard to provide more information on an installed patch or update. Information includes; Bulletin id, title, description, URL and file size.

C

Common Gateway Interface (CGI)

A communication script used by web servers to transfer data to a client internet browser.

Common Vulnerabilities and Exposures (CVE)

A list of standardized names for vulnerabilities and other information security exposures. The aim of CVE is to standardize the names for all publicly known vulnerabilities and security exposures.

D

Dashboard

A graphical representation that indicates the status of various operations that might be currently active, or that are scheduled.

Demilitarized Zone (DMZ)

A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.

deploycmd.exe

A GFI LanGuard command line tool, used to deploy Microsoft® patches and third party software on target computers.

DMZ

A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.

DNS

A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

DNS Lookup tool

A utility that converts domain names into the corresponding IP address and retrieves particular information from the target domain

Domain Name System

A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

E

Enumerate computers tool

A utility that identifies domains and workgroups on a network.

Enumerate users tools

A tools which enables you to retrieve users and user information from your domain/workgroup.

Extensible Markup Language (XML)

An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.

F

File Transfer Protocol

A protocol used to transfer files between network computers.

FTP

A protocol used to transfer files between network computers.

G

GFI EndPointSecurity

A security solution developed by GFI that helps organizations to maintain data integrity by preventing unauthorized access and transfers from removable devices.

GPO

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

Group Policy Object (GPO)

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

I

ICMP pings

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

impex.exe

A Command line tool, used to Import and Export profiles and vulnerabilities from GFI LanGuard.

Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

Internet Information Services (IIS)

A set of Internet-based services created by Microsoft® Corporation for internet servers.

L

Linux

An open source operating system that is part of the Unix operating system family.

lnsscmd.exe

A GFI LanGuard command line tool that allows running vulnerability checks against network targets.

Local Host

In networking, the local host is the computer you are currently using. One can reference to the local host by using the reserved IP address 127.0.0.1. In this manual the Local host is the machine where GFI LanGuard is installed.

M

Mail server

The server that manages and stores client emails.

Malware

Composed from malicious and software, malware is a general term used for all software developed to harm and damage a computer system. Viruses, worms and Trojans are all type of malware.

Microsoft® Access™ database

A Microsoft® desktop relational database management system included in the Microsoft® Office package. Microsoft® Access™ is normally used for small databases.

Microsoft® IIS

A set of Internet-based services created by Microsoft® Corporation for internet servers.

Microsoft® Windows service packs

A collection of updates and fixes provided by Microsoft® to improve an application or an operating system.

Microsoft® WSUS

An acronym for Microsoft® Windows Server Update Services. This service enables administrators to manage the distribution of Microsoft® updates to network computers.

N

NETBIOS

An acronym for Network Basic Input/output. This system provides services to allow applications on different computers within a network to communicate with each other.

Netscape

A web browser originally developed by Netscape Communications Corporation.

O

Open Vulnerability and Assessment Language (OVAL)

A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.

OVAL

A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.

P

Patch agent

A background service that handles the deployment of patches, service packs and software updates on target computers.

Python scripting

A high-level computer programming scripting language.

R

Remote Desktop Protocol

A protocol developed by Microsoft® to enable clients to connect with the user interface of a remote computer.

S

SANS

An acronym for System Administration, Networking and Security research organization. An institute that shares solutions regarding system and security alerts.

Scan profiles

A collection of vulnerability checks that determine what vulnerabilities are identified and which information will be retrieved from scanned targets.

Script Debugger

A GFI LanGuard module that allows you to write and debug custom scripts using a VBScript-compatible language.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is a technology used to monitor network devices such as, routers, hubs and switches.

SNMP

Simple Network Management Protocol is a protocol for network management. It is used to collect information from network devices, such as servers, printers, hubs, switches, and routers.

SNMP Auditing tool

A tool that reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary.

SNMP Walk tool

A tool used to probe your network nodes and retrieve SNMP information.

Spyware

A form of malware intended to collect information from a computer without notifying the user.

SQL Server Audit tool

A tool used to test the password vulnerability of the -sa- account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server.

SQL Server®

A Microsoft® relational database management system. Microsoft® included extra functionality to the SQL Server® (transaction control, exception handling and security) so that Microsoft SQL Server® can support large organizations.

SSD

Solid State Drives are storage devices for computers. These drives use flash memory technology to provide superior performance and durability to traditional Hard Disk Drives.

SSH Module

A module used to determine the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target-s Linux/UNIX OS and which outputs results to the console in text.

T

TCP ports

Acronym for Transmitting Control Protocol. This protocol is developed to allow applications to transmit and receive data over the internet using the well-known computer ports.

Terminal Services

A service that allows connecting to a target computer and managing its installed applications and stored data.

Traceroute tool

A tool used to identify the path that GFI LanGuard followed to reach a target computer.

Trojans

A form of malware that contains a hidden application that will harm a computer.

U

UDP ports

An acronym for User Datagram Protocol, these used to transfer UDP data between devices. In this protocol received packets are not acknowledged.

Uniform Resource Locator (URL)

The Uniform Resource Locator is the address of a web page on the world wide web.

Universal Serial Bus (USB)

A Serial bus standard widely used to connect devices to a host computer.

URL

The Uniform Resource Locator is the address of a web page on the world wide web.

V

VBScript

A Visual Basic Scripting language is a high-level programming language developed by Microsoft®.

Virus

A form of malware that infects a computer. The aim of a virus is to harm a computer by corrupting files and applications. A virus is a self-replicating program and can copy itself all over the computer system.

W

Web server

A server that provides web pages to client browsers using the HTTP protocol.

White-list

A list of USBs or Network devices names that are not considered as dangerous. When a USB/Network device name contains a white-listed entry while scanning a network, GFI LanGuard will ignore the device and consider it as a safe source.

Whois tool

A tool that enables you to look up information on a particular domain or IP address.

Wi-Fi/Wireless LAN

A technology used commonly in local area networks. Network nodes use data transmitted over radio waves instead of cables to communicate with each other.

X

XML

An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.

8 Index

S

T

U

V

W