Evaluation guide

GFI LanGuard™

Network security scanner and patch management

Evaluator's guide to getting the maximum benefit out of a GFI LanGuard® trial

GFI®

Contents

Introduction

Thank you for evaluating GFI LanGuard. This document aims to help you get the maximum benefit out of your GFI LanGuard trial.

In the next sections, our guidelines will help you prove the benefits to yourself and anyone else involved in the decision-making process.

GFI LanGuard overview

GFI LanGuard is a comprehensive network management solution. It acts as a virtual security consultant helping in the following areas: patch management, vulnerability assessment, network and software auditing, asset inventory, risk analysis and compliance.

GFI LanGuard scans, analyzes and helps remediate your network. Simply stated:

- Either agent-based or agent-less, GFI LanGuard scans the network for security related issues and gathers security relevant information. It gathers information about security vulnerabilities, missing patches, missing service packs, open ports, open shares, users and groups, installed applications, and hardware inventory. GFI LanGuard integrates with over 2,500 security applications such as antivirus, anti-spyware or firewalls and reports on their status.
- With the results of the scans you can then analyze the status of your network. GFI LanGuard provides a powerful dashboard to browse and investigate the scan results. Security sensors are triggered when issues are detected. A vulnerability level is assigned to each scanned computer based on the items found during the audit and GFI LanGuard provides reports and results comparisons.
- After scanning and analyzing, GFI LanGuard assists to remediate the security issues, automating the process where possible.
- After creating a baseline scan, you can identify any differences or changes to the security and computer configurations of all the computers in the network. You can decide to take such actions as deploy missing Microsoft® and non-Microsoft security (and non-security) updates, rollback updates, deploy custom software and scripts, uninstall unauthorized applications, open remote desktop connections to scanned computers, etc. All of these actions will help to ensure your network is up-to-date and the latest patches are applied.

Why do customers purchase GFI LanGuard?

Based on our experience, the top four (4) reasons GFI customers purchase GFI LanGuard are below:

1. To minimize the risk of security breaches by:
   - scanning the network for security and vulnerability issues
   - automatically detecting and uninstalling any unauthorized applications
   - auditing software (which PCs have what software) and hardware devices on the network
   - receiving alerts and reports regarding the security environment of the network.
2. To automate patch management – detect and deploy missing patches for Microsoft and other third party applications
3. To conduct network auditing and network health monitoring
4. To aid with compliance for security regulations that require regular vulnerability assessment and patch management (e.g. PCI DSS, HIPAA, SOX, GLBA, GCSx PSN CoCo, etc.)

Installation

How to get the evaluation key

If you have not yet downloaded GFI LanGuard 2012, please download the trial here before starting.

To start the evaluation of GFI LanGuard you need to enter your free evaluation key. Entering the evaluation key will give you the full functionality of the product, limited to five IP addresses for 30 days. We sent the key to the email address that you registered with when downloading this product.

If you do not have access to the original email which included the key, please click here now to request a new evaluation key. It is completely free.

If you need to evaluate for a longer period or with more than five IP addresses, you can submit your request here.

System requirements

Before installing GFI LanGuard please check and ensure that the hardware and software requirements are met. They are listed here.

Installing GFI LanGuard 2012

Easy steps to deploy and test your GFI LanGuard 2012 installation are available in the Installation and setup guide that can be downloaded from here.

Step 1: Perform security scans

Agent-less vs. agent-based scans

GFI LanGuard can perform both agent-less and agent-based security scans. Here are some items to consider when choosing what scanning method to use:

Agent-less scans:

- No installs on client machines
- All processing is done by the central server, no resources from client machines are required
- Work on rough devices and systems where agents are not supported.

Agent-based scans:

- Have better performance due to distributed load across clients
- Work better in low bandwidth environments because the communication between server and clients is much less intensive than in the case of agent-less scans
- Better support of laptops because agents will continue to do their job when offline and when they are online they will just synchronize with the sever
- Improved results accuracy because local scans have access to more information than remote scans.

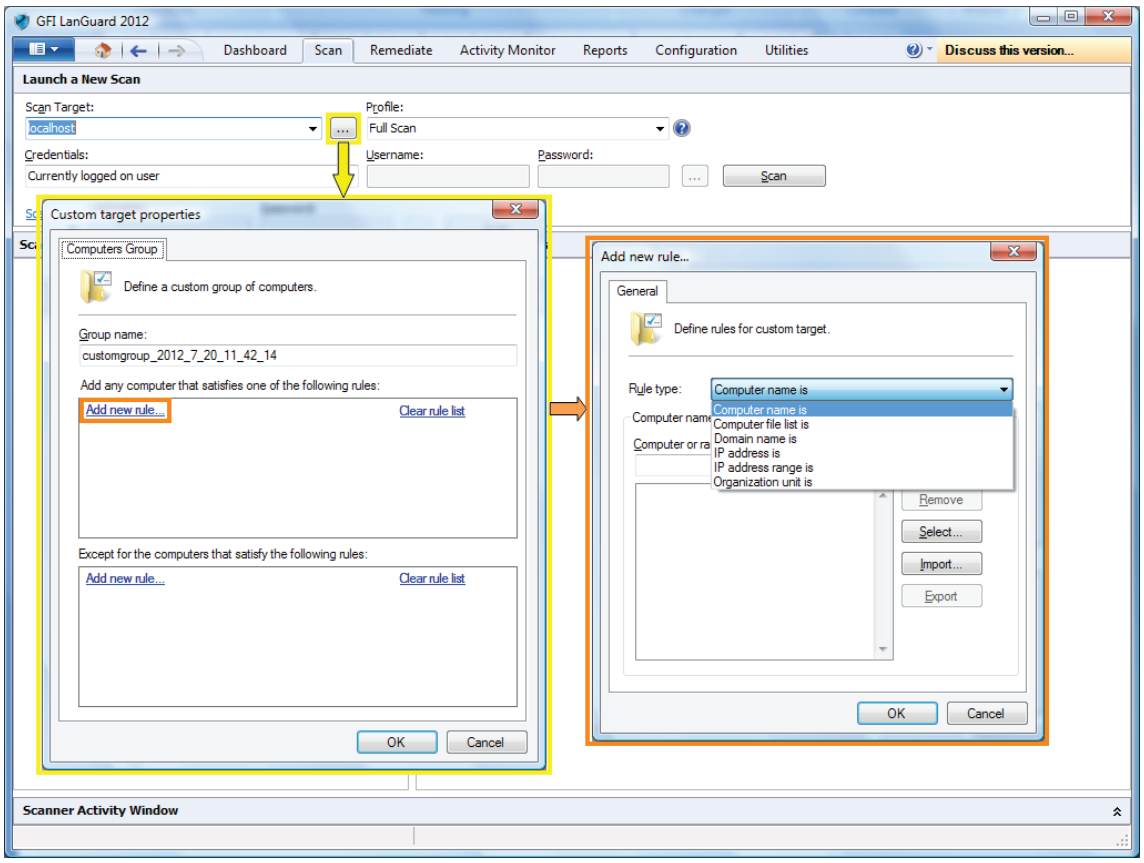
Agent-less security scans

Trigger scans and follow progress in real time

Use the Scan tab to trigger agent-less scans immediately and to follow up progress in real time. The scan target can be any combination of computer names, text files containing computer names, a single IP address and ranges of IP addresses, domain or workgroups and organizational units.

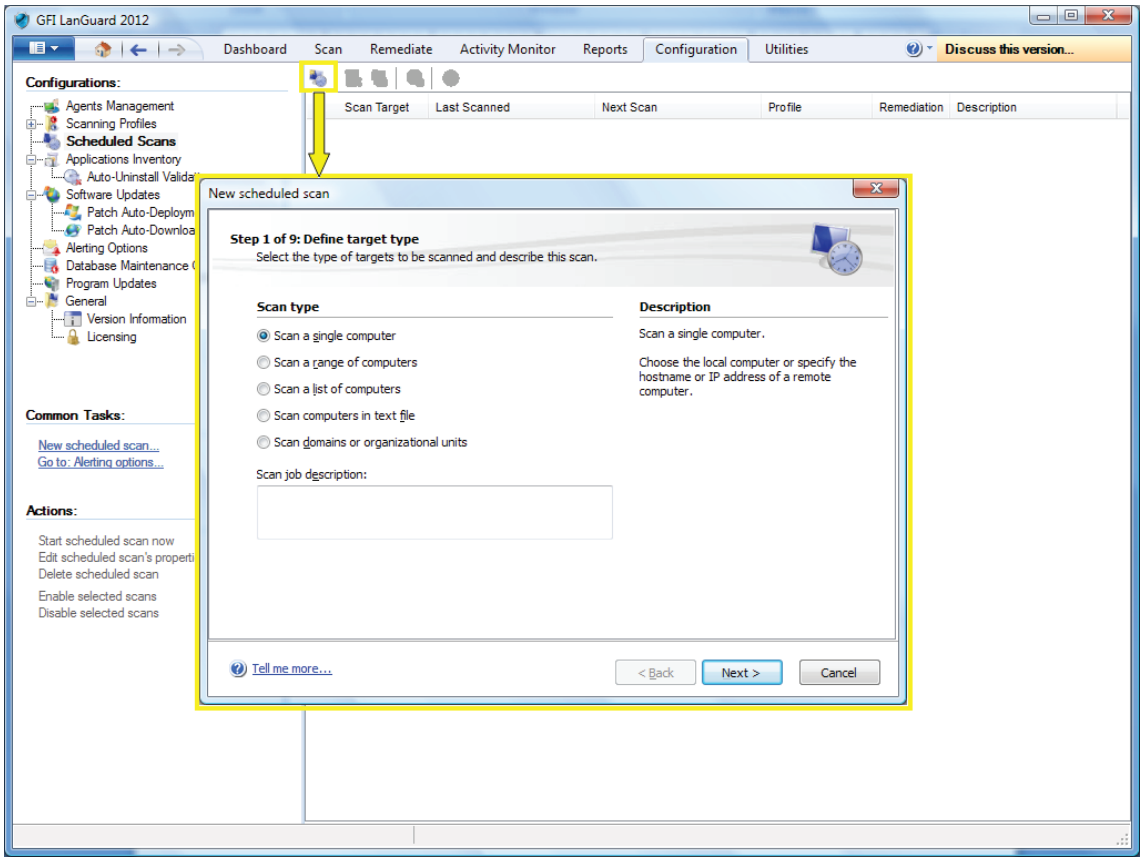
Administrative access to the remote machines is required for comprehensive security audit results.

Please note that at present, only agent-less scans are possible for Mac OS® X targets.

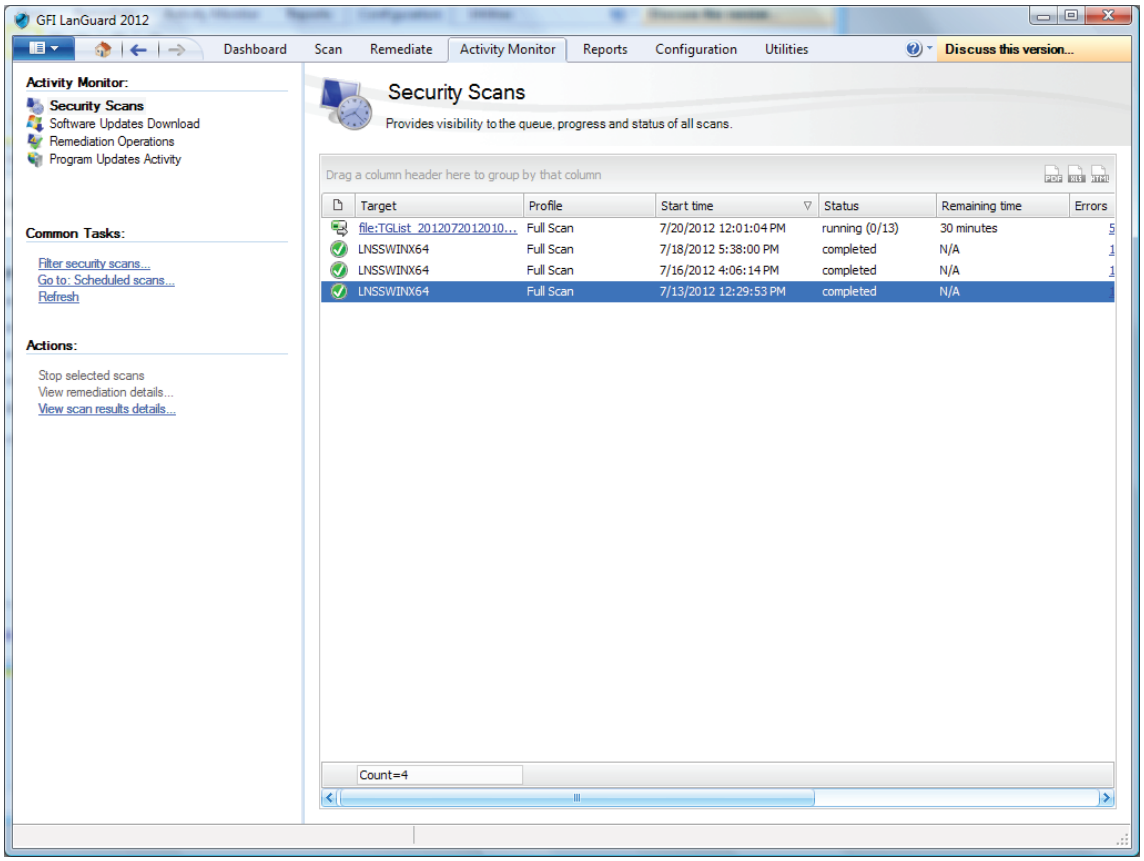


Scheduled scans

Use *Configuration* > *Scheduled Scans* to schedule agent-less scans to run on regular basis:

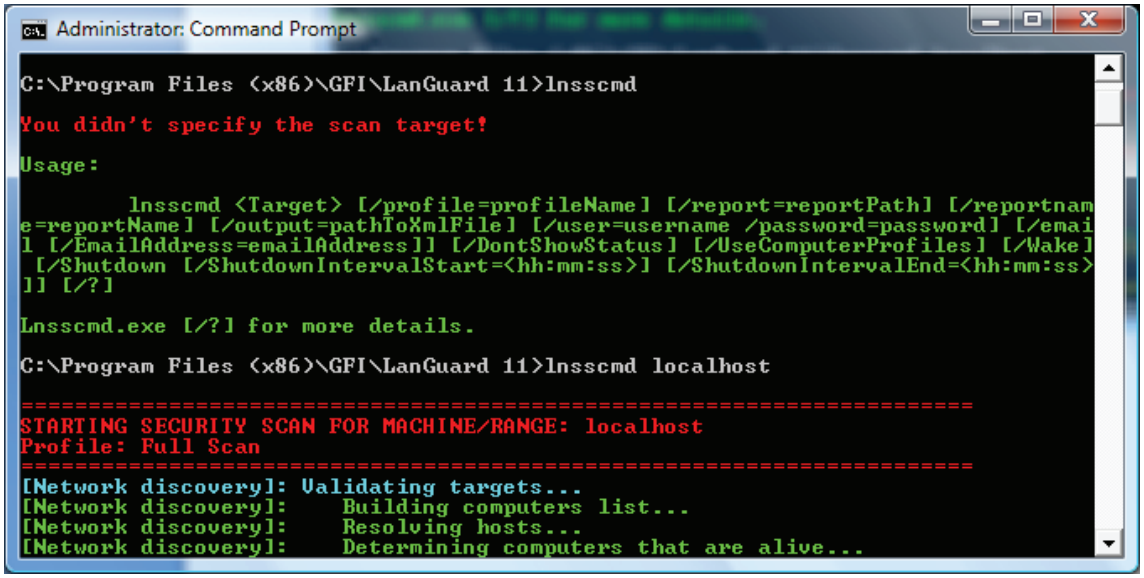


Progress of scheduled scans can be followed using *Activity Monitor* > *Security Scans*:



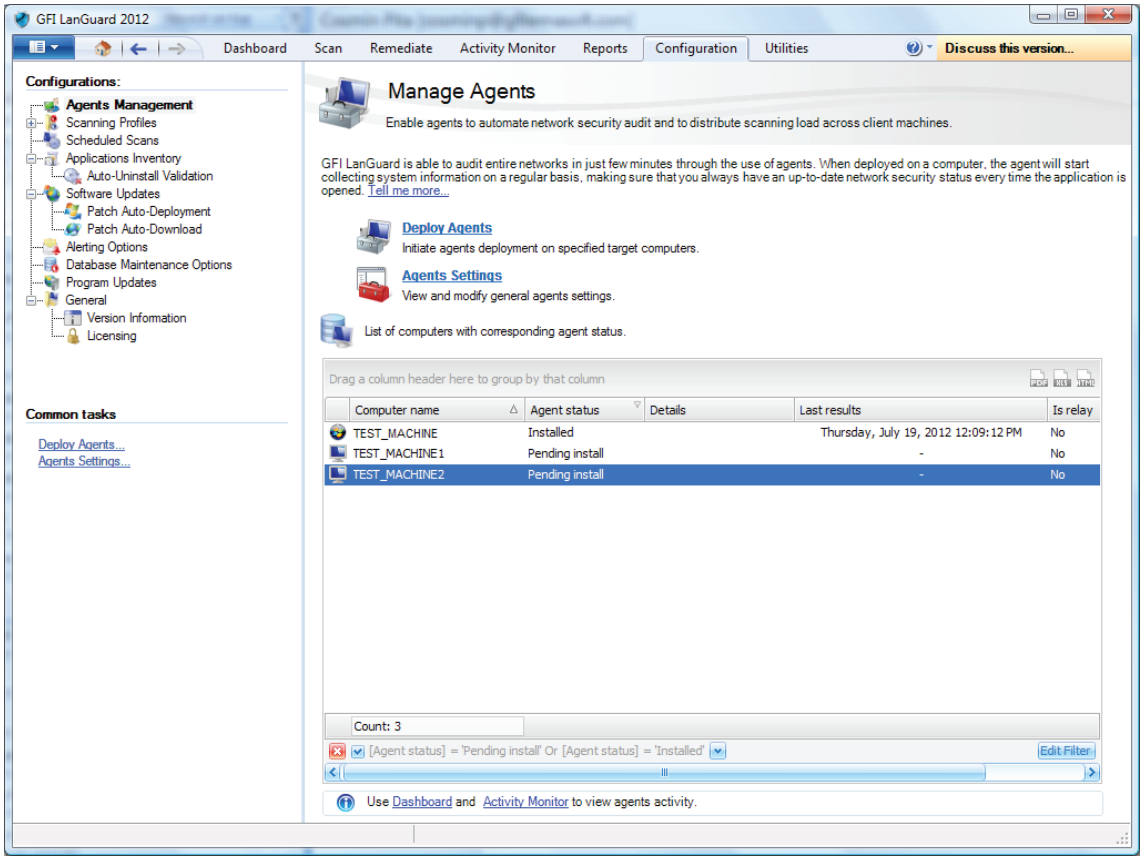
Command line scans

Use lnsscmd.exe tool to run command line scans:



Agent-based audits

One way to enable agents is to use *Configuration* > *Manage Agents* tool:



The process to enable agents is easy. Just set the list of computers or domains or organizational units where agents need to be deployed and provide credentials with administrative access to the remote machines.

GFI LanGuard will handle the deployment operation.

How agents work:

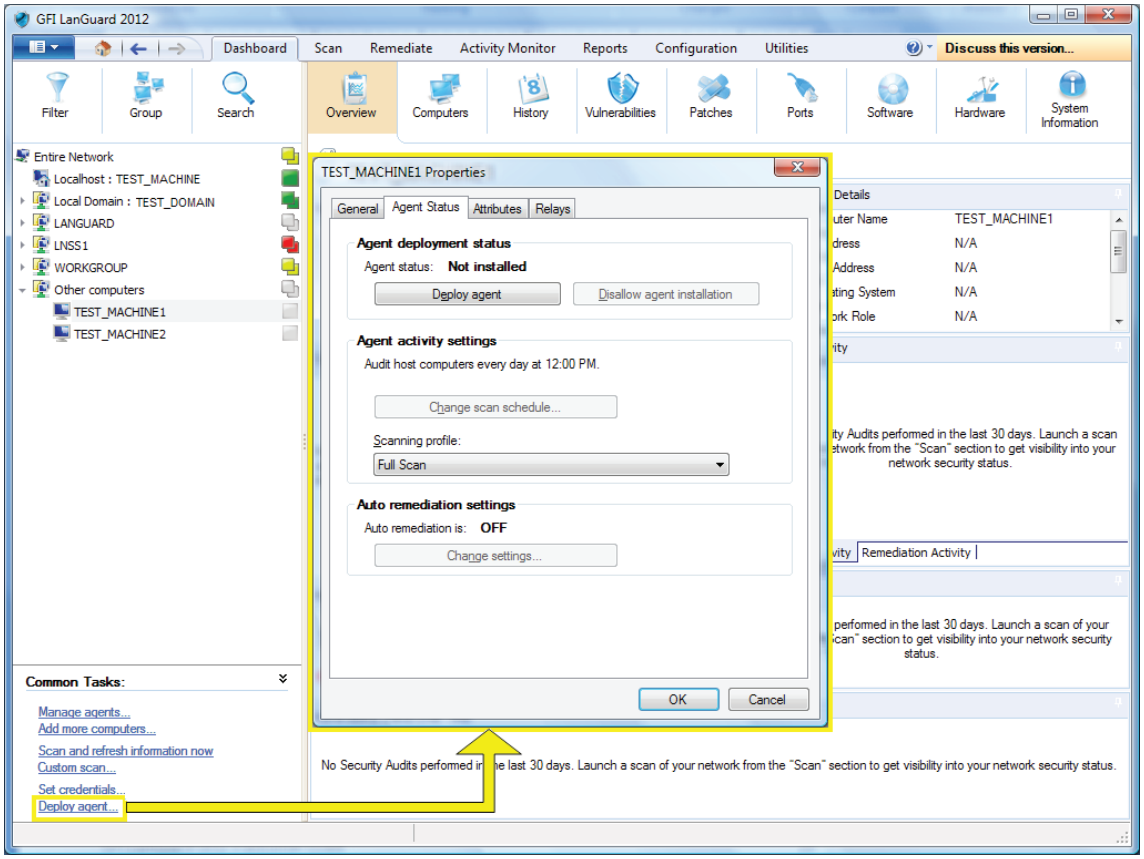
- GFI LanGuard installs the agents automatically on the selected computers
- Agents only install on Windows® systems
- By default, agents perform a full scan of their host machine once per day, but the frequency, the scan time and scanning profile can be configured
- Agents need around 25 MB RAM and 350 MB disk space
- Agents consume CPU power only when the host computer is audited. This is normally a few minutes per day and the priority of the process is below normal so that it will not interfere with the work done on that machine
- GFI LanGuard agents can be uninstalled from the main console. By default, the agents will auto-uninstall themselves if they have no contact with their server for 60 days. The number of days can be configured
- GFI LanGuard agents communicate their status to GFI LanGuard server using the TCP port 1070. The port number can be configured
- GFI LanGuard can be configured to perform network discovery automatically on domains or organizational units and install agents automatically on newly discovered machines
- GFI LanGuard automatically handles situations where agents were removed by mistake or they need to be upgraded

» An Agent may be designated a Relay Agent, which allows remediation to be performed more efficiently and using less network bandwidth for multi-site or large networks. The Relay Agent stores a local copy of the patch data (normally stored on the GFI LanGuard server) and this is used to remediate nearby computers. More information about Relay Agents can be found in the Administration and configuration manual that can be downloaded from here.

Troubleshooting agent deployment errors

If GFI LanGuard fails to deploy the agent on certain machines, you can click here for a list of possible causes.

Another way to enable and configure the agents is to use the *Dashboard* and selecting Deploy agent from the Common Tasks section:



Trigger agent-based on-demand scans

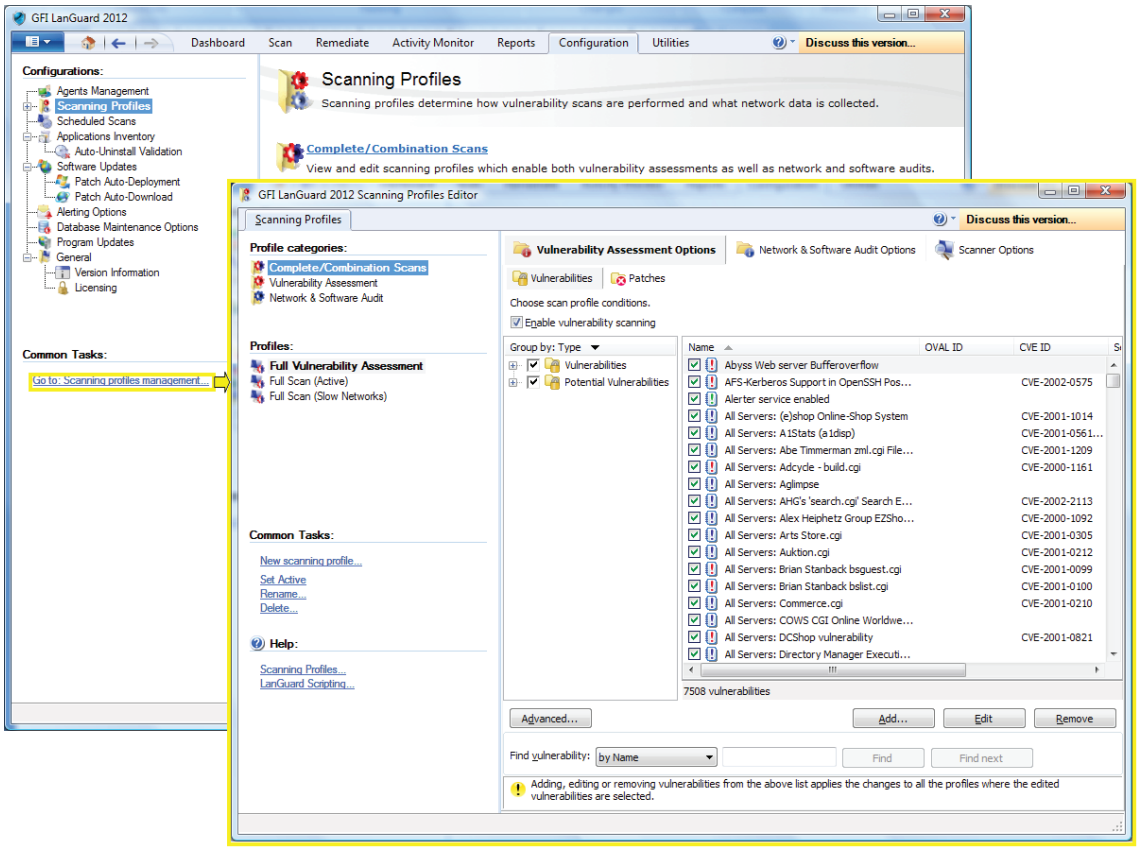
From the Scan tab only agent-less scans can be performed. Agent-based scans usually run automatically in background on the remote machines according to the audit schedule that was set (by default agents do their scan once per day).

If a refresh of the security information is required it is possible to trigger on-demand agent scans using the Scan and refresh now option from the Dashboard. More details about how the Scan and refresh now option works are available in the Triggering scans from the Dashboard section.

Scanning profiles

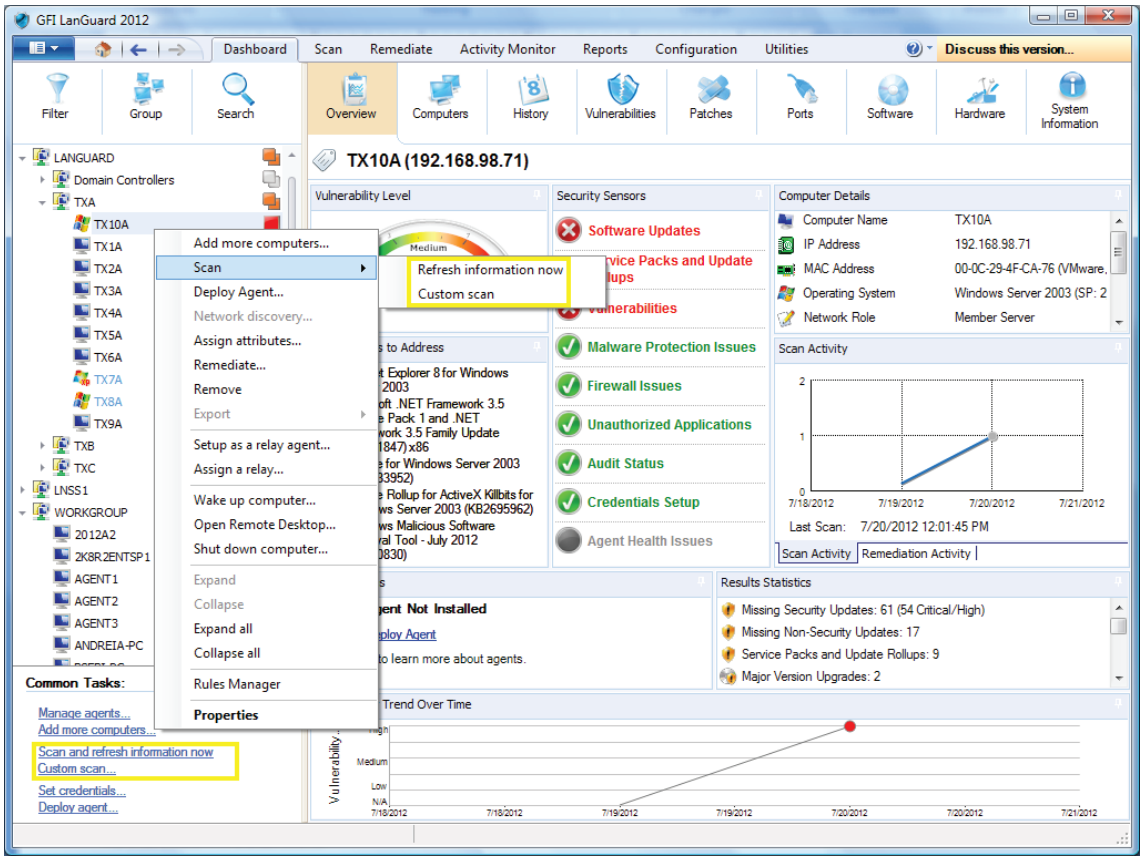
Scanning profiles determine how security scans are performed: what security issues to check for and what network data is collected. Out of the box, GFI LanGuard comes with an extensive list of predefined scanning profiles.

Use *Configuration* > *Scanning Profiles* to view, modify or create new custom scanning profiles.



Triggering scans from the Dashboard

One easy way to trigger security audits is to use the *Dashboard*. Just select the list of computers/domains/organizational units from the Dashboard tree and click on either *Scan and refresh information now* or *Custom scan* options. Both of them are available in the Common Tasks area or when right-clicking on the selected computers.



Scan and refresh information now

This option immediately triggers a security audit that runs in background for the selected computers. On the computers where the agent is installed, the scan will be performed by the agent and under the scanning profile defined for the agent. For the computers where the agent is not available an agent-less scan is scheduled to run in background using Full Scan profile. Use Activity Monitor > Security Scans to monitor both agent-based scans and agent-less scheduled scans.

Custom scan

This option will select the Scan tab with the scan target already prefilled with the list of computers that were selected in the Dashboard.

Step 2: Analyze scan results

The Dashboard

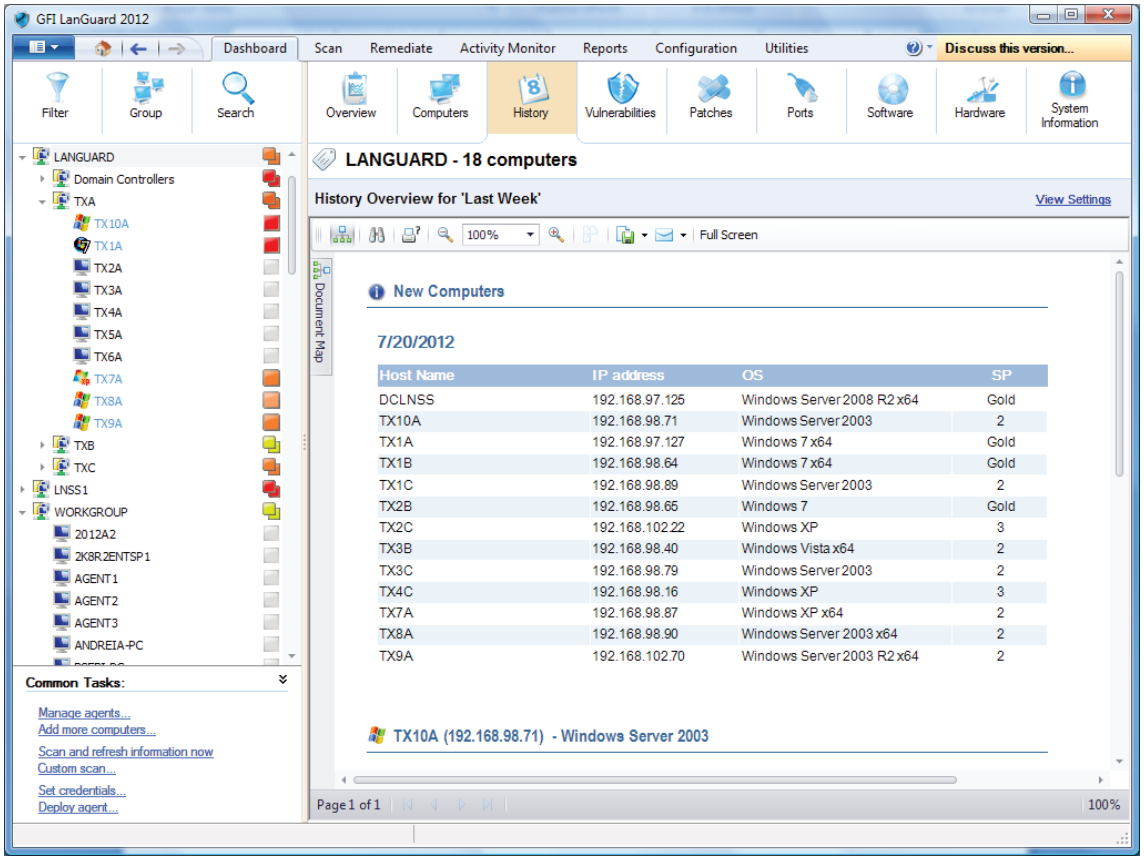
The Dashboard aggregates results from all scans, independent of the scanning profile or if the scan is agent-less or agent-based. The aim is to show instantly a complete overview of the network security status.

Starting from an executive overview that shows the most vulnerable computers, most prominent security issues, vulnerability trends, etc., users can drill down to certain computers and specific issues.

On the left hand side of the *Dashboard*, we have the computers tree, which is, by default, organized by domains and organizational units. On the right hand side, nine views are available to show information about the selected computers. The name of the views is self-explanatory: *Overview, Computers, History, Vulnerabilities, Patches, Ports, Software, Hardware* and *System Information*.

How to view relevant security changes from your network

Use the *Dashboard* > *History view* to inspect relevant security changes from your network: be notified when new devices are discovered, when new security vulnerabilities are detected, when applications are installed or removed, when services are started or stopped, when new ports are opened, when new shares are created, when new users are created, when there are hardware changes, etc.



If a valid email recipient is configured in *Alerting Options* configuration, GFI LanGuard sends by default a *Daily Digest* report containing the history view of the entire network for the last 24 hours.

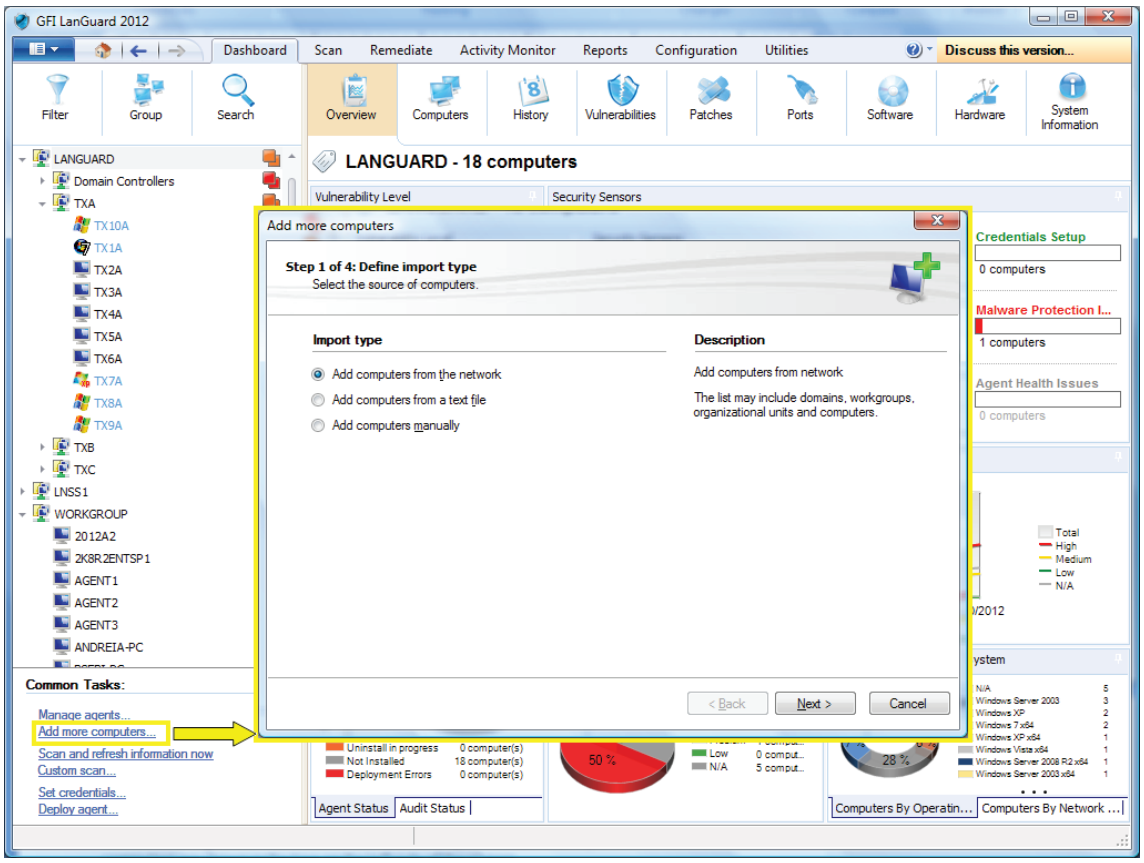
The *Reports* view also contains reports like *Baseline Comparison, Network Security History, Scan History* and *Remediation History* that can be scheduled to run on a regular basis.

How to add/view more computers in the Dashboard

Unless it is filtered, the *Dashboard* tree will show all computers managed by GFI LanGuard. This means that all devices that were discovered or fully scanned by the product.

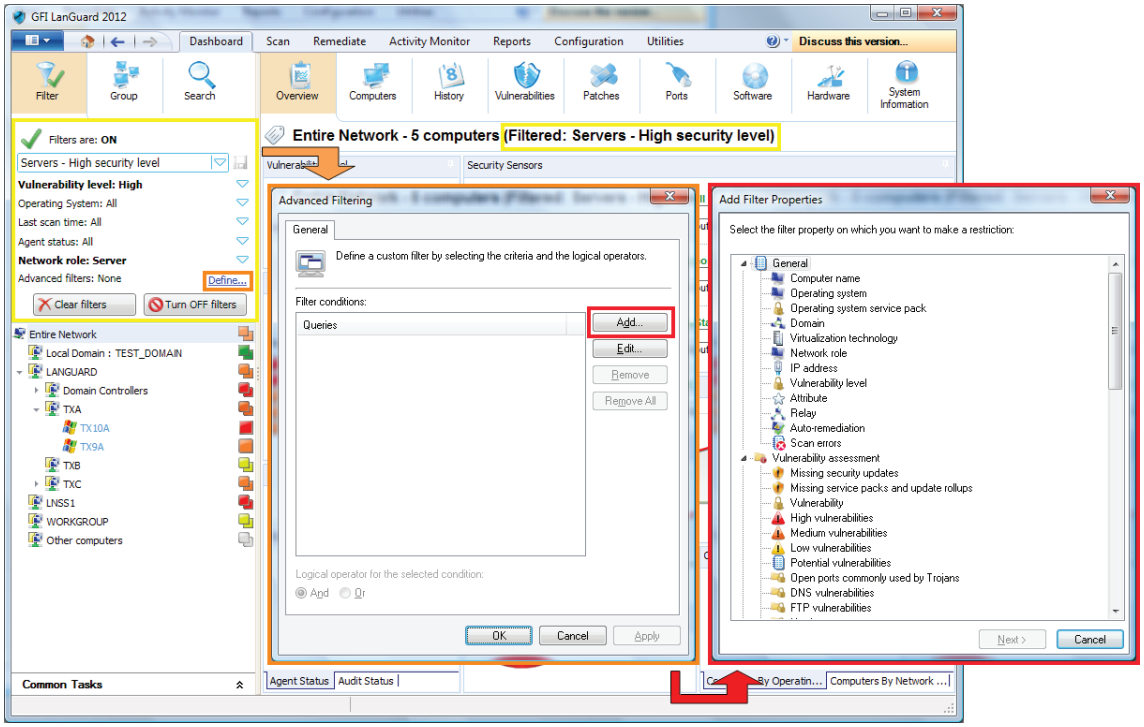
To view computers in the Dashboard one of the following operations needs to be performed:

- Scan the computers without agents by using *Scan* tab, *Configuration* > *Scheduled Scans* or command line scans
- Enable agents on the computers using *Configuration* > *Agents Management*
- Use *Add more computers*… option from the *Common Tasks* area of the *Dashboard* to add to the tree entire domains/workgroups and organizational units or a list of specific computers.



How to filter computers

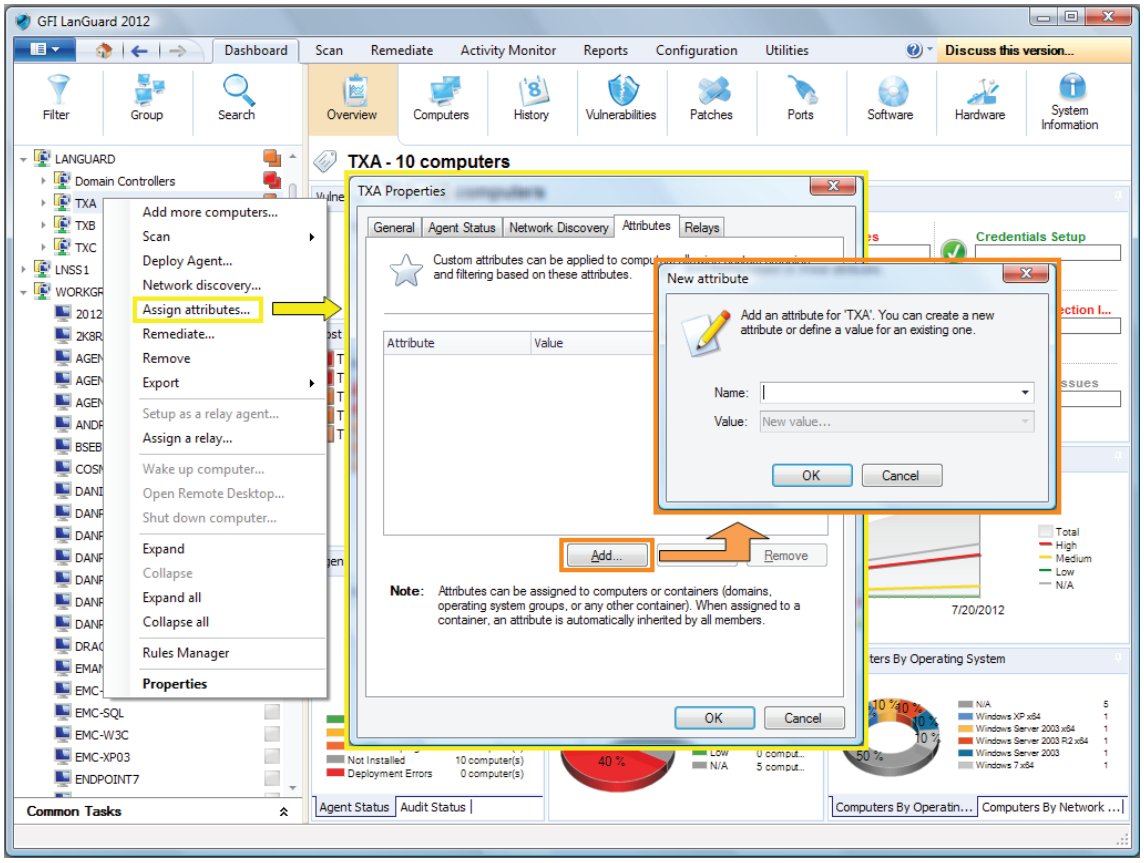
Use the filtering area which is available in Dashboard, Remediate and Reports views to filter which computers are shown in the tree on the left side of the screen:



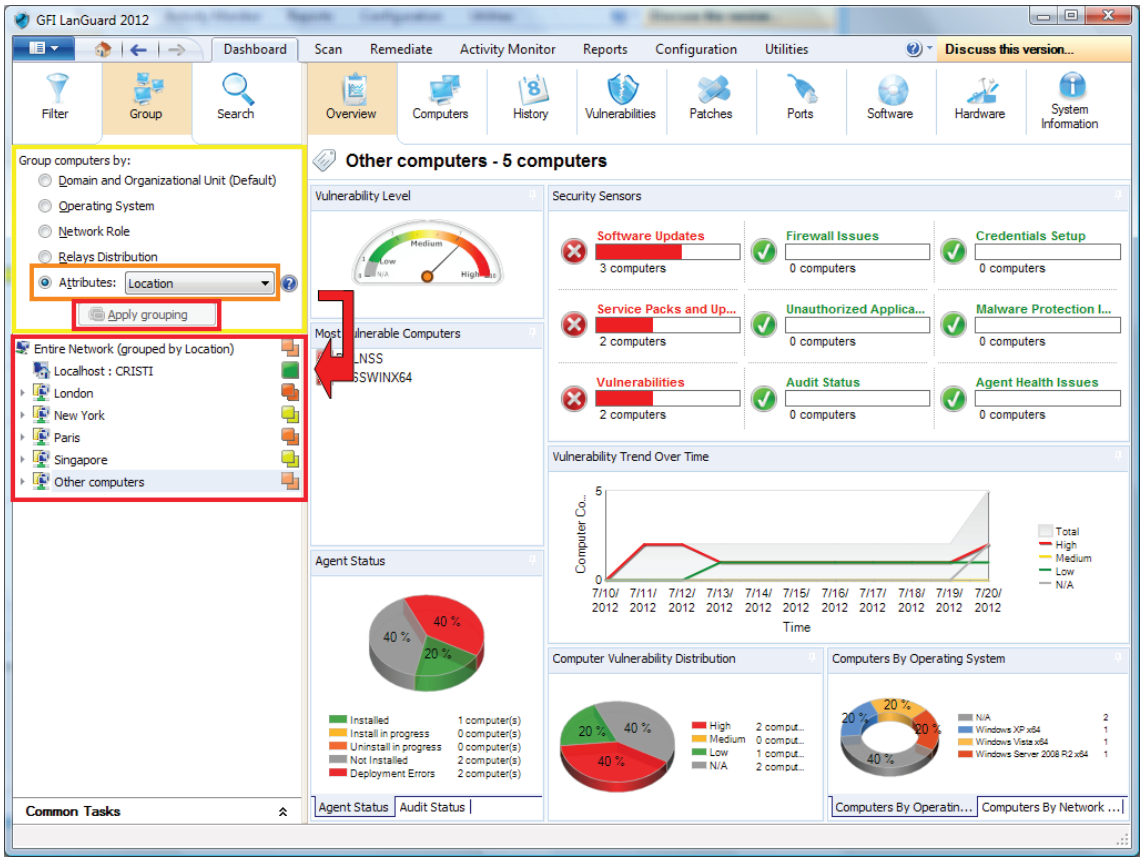
How to group computers

Computers from the tree can be grouped by predefined criteria like domains and organizational units (default grouping), operating system, network role, relays distribution or custom attributes defined by the users.

Defining custom attributes:



Then view computers by defined attributes:

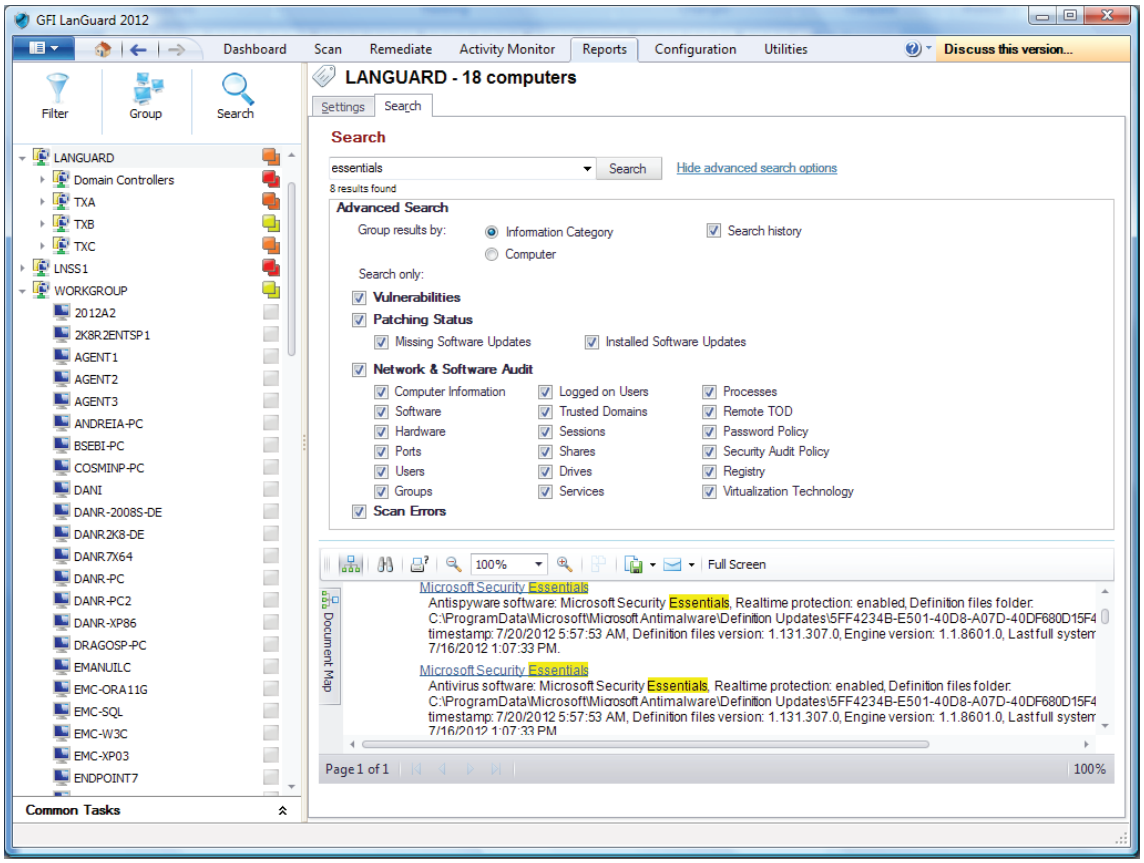


How to search for computers

If a large number of computers are managed, finding them in the computers tree might be time consuming. Use the search area available in *Dashboard, Remediate* and *Reports* views to instantly locate computers.

Full text search

Use the search area of Dashboard, Remediate and Reports views to locate information instantly in scan results based on keywords.

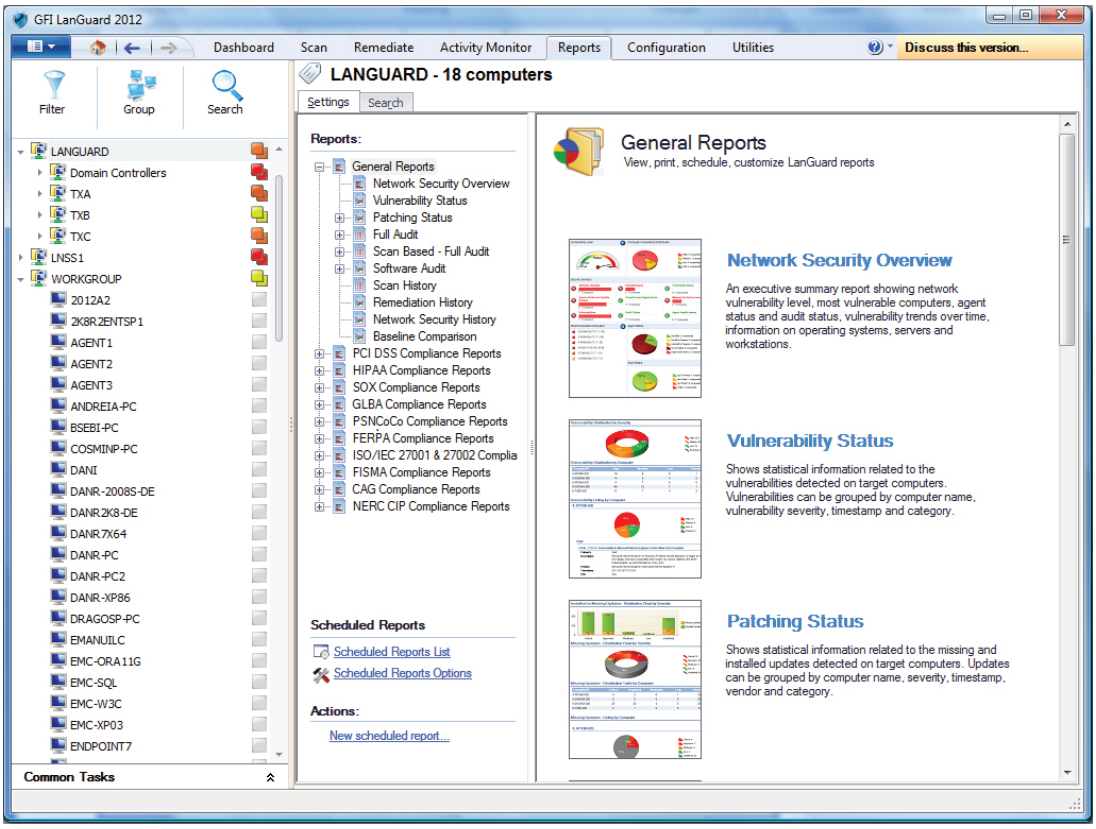


Search results can be grouped by computer or information category. It is also possible to exclude certain results (i.e., if you are interested only in installed software then you exclude the other categories of scan results like vulnerabilities, users, groups, services, etc.)

Reporting

GFI LanGuard comes with a large set of predefined executive, technical and statistical reports. All reports can be customized, rebranded, scheduled to be generated on a regular basis and exported to various popular formats like PDF, HTML, RTF, XLS, etc.

Additionally GFI LanGuard ships with a large set of reports dedicated to compliance with PCI DSS, HIPAA, SOX, GLBA, PSN CoCo, amongst others.



Step 3: Remediate security issues

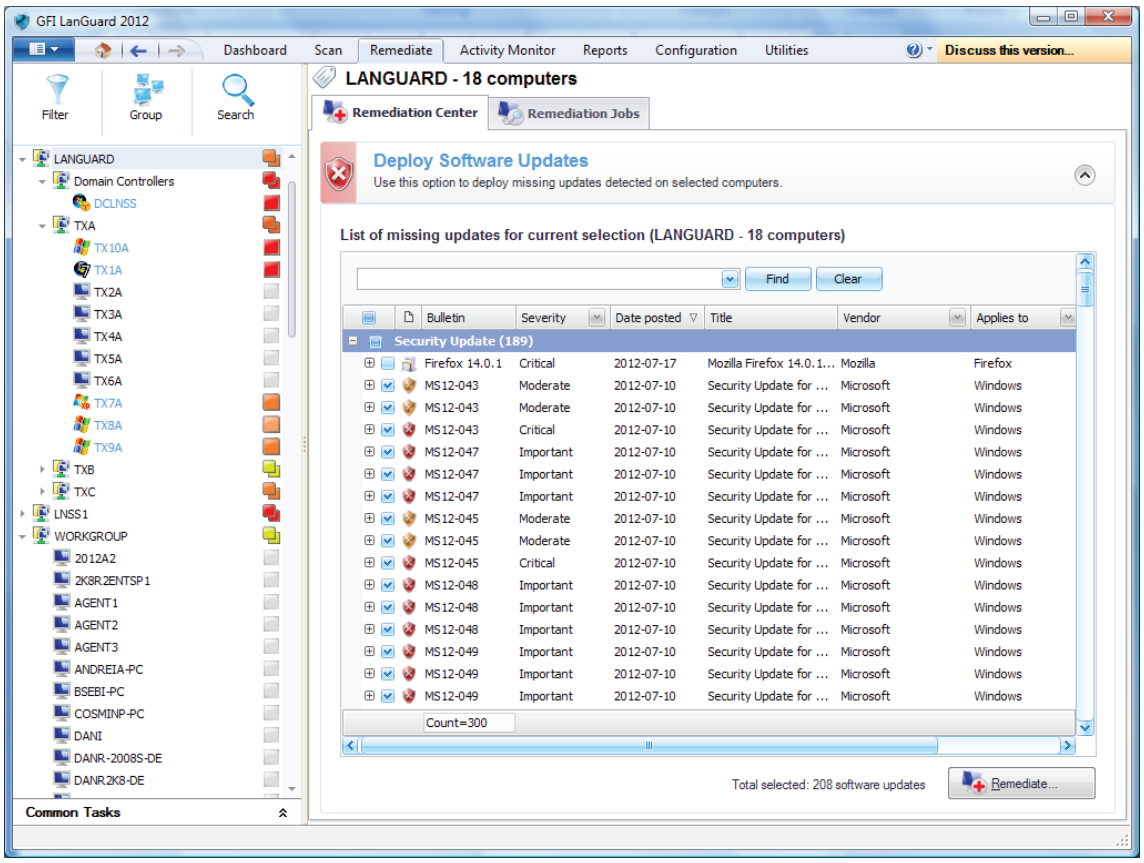
Deploy missing software updates

Use *Remediate > Remediation Center > Deploy Software Updates* to deploy missing security and non-security updates:

» Select the computers or computer groups where patches need to be deployed from the computers tree in the left part of the screen.

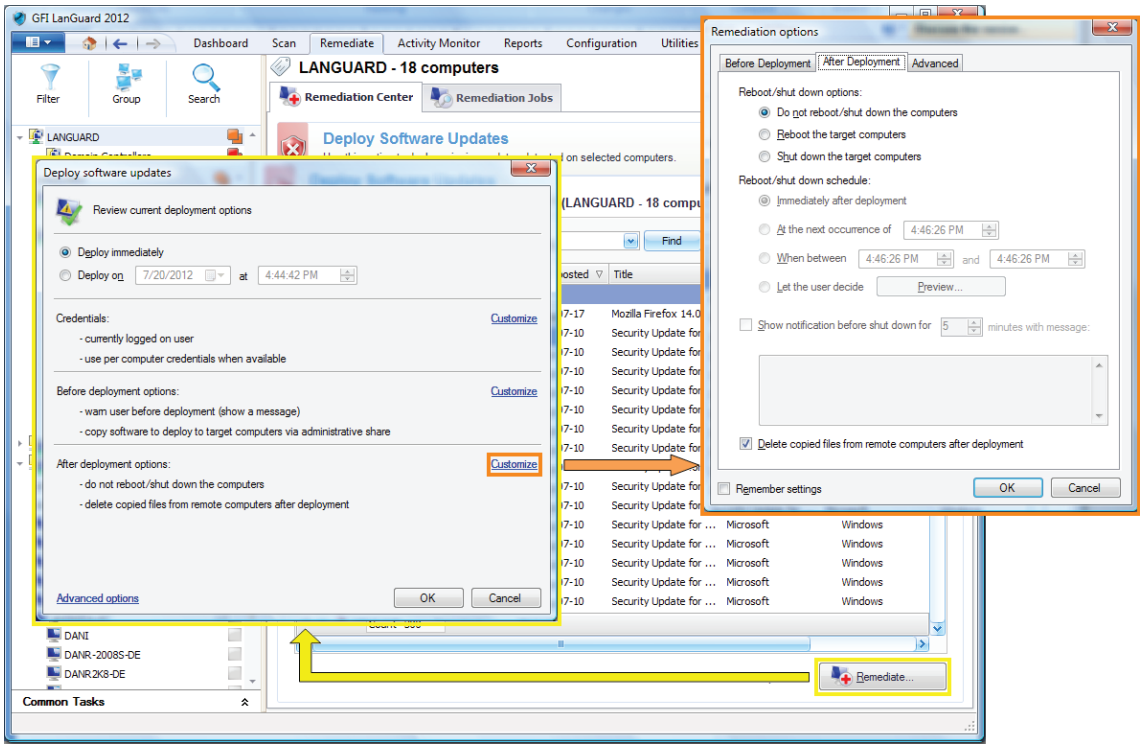
Multiple items can be selected in the computers tree using <CTRL> + click.

To locate computers more easily in large networks, computers from the tree can be filtered by a large number of criteria. See the How to filter computers section for more details.

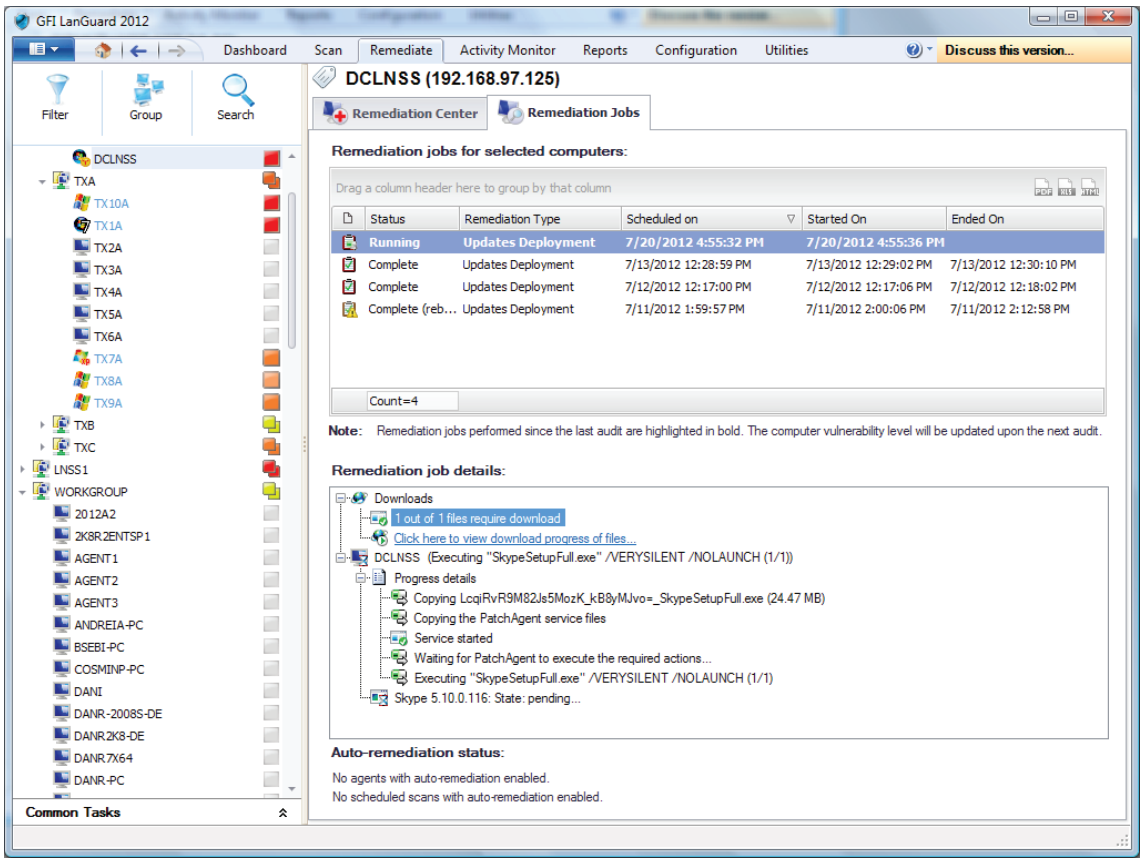


» In the *Deploy Software Updates* screen you can see all missing updates for the selected computers with details for each update on which of the selected computers is missing. It is possible to fine tune the deployment by selecting or deselecting patches or computers.

» Set up deployment schedule and reboot options.



» Start the deployment operation. Progress can be followed using *Remediate* > *Remediation Jobs*.



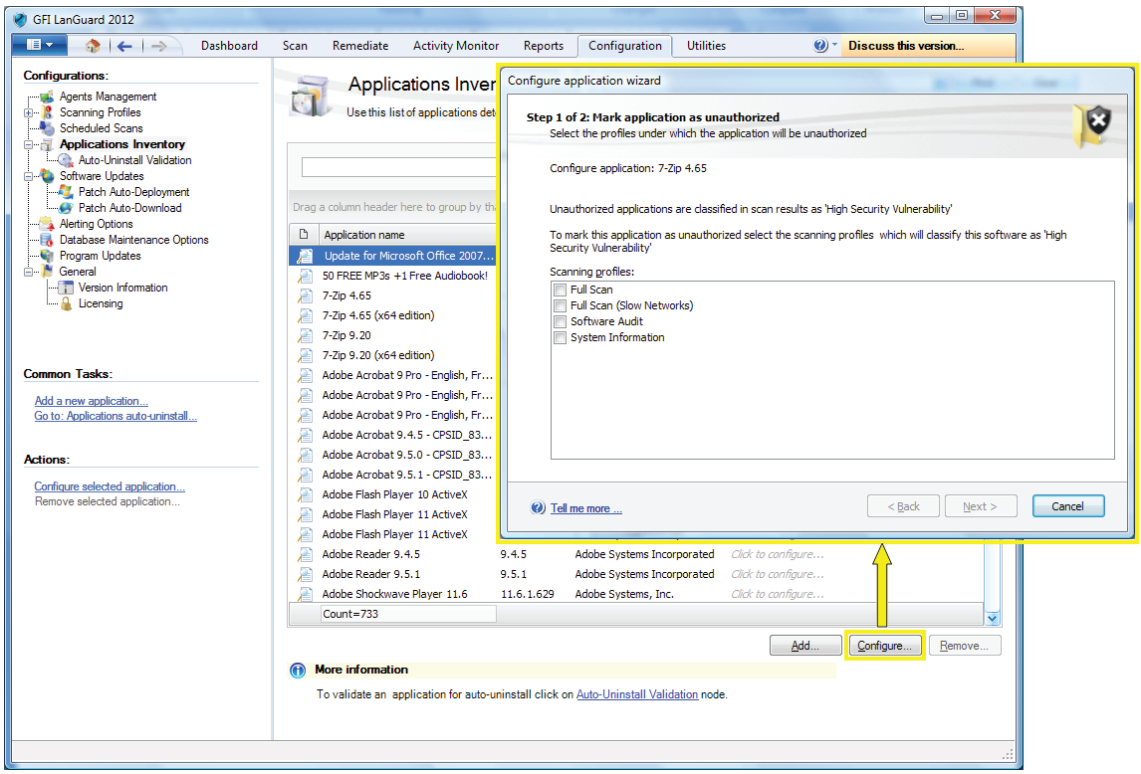
» Rescan the machines to get their security status after the deployment was done. A large number of updates require a reboot of the target machine for the deployment to complete. If an update is still seen as missing after a deployment operation, make sure the machine was rebooted.

» GFI LanGuard can be configured to automatically deploy missing updates. See Automate Remediation Operations section for more details.

Uninstall unauthorized applications

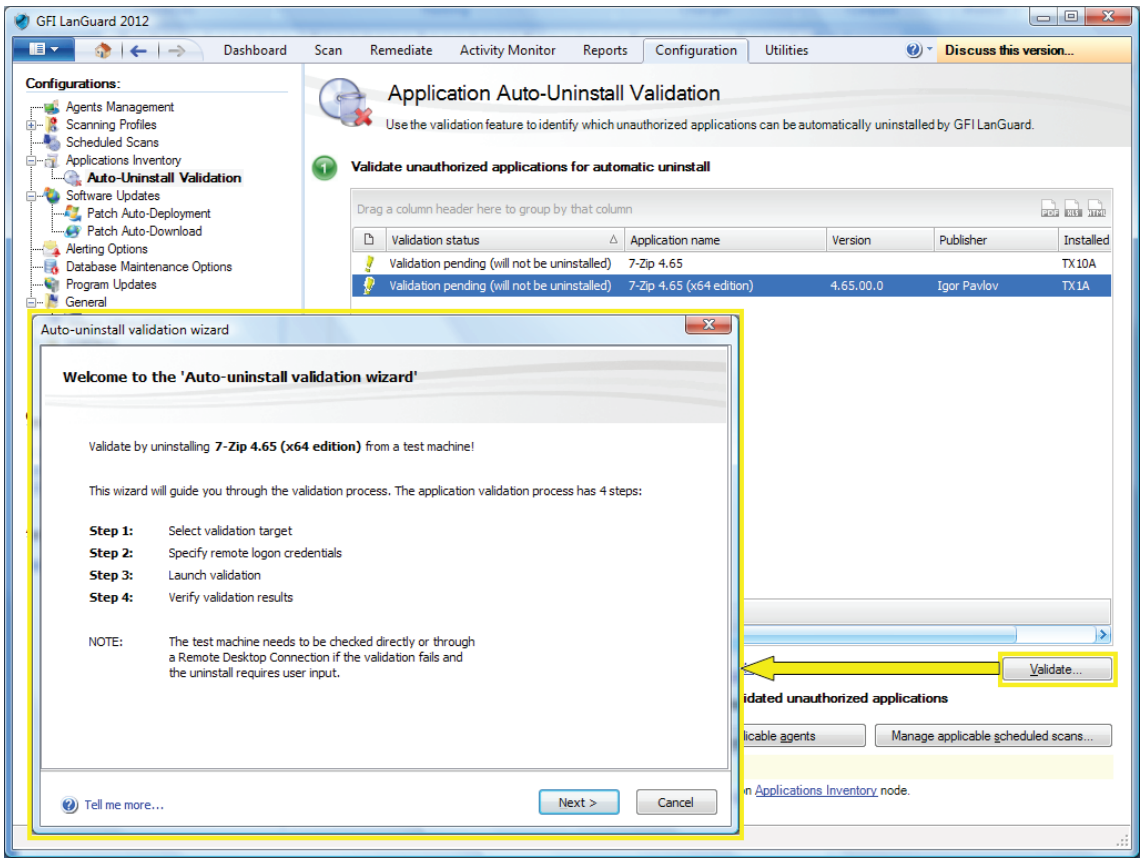
» Perform a full audit or a software audit on the network to get an inventory of installed applications. See Performing Security Scans section for more details.

» Mark unauthorized applications using Configuration > Applications Inventory. It is possible to add unauthorized applications even if they are not detected as installed in the network by using the "Add…" button.



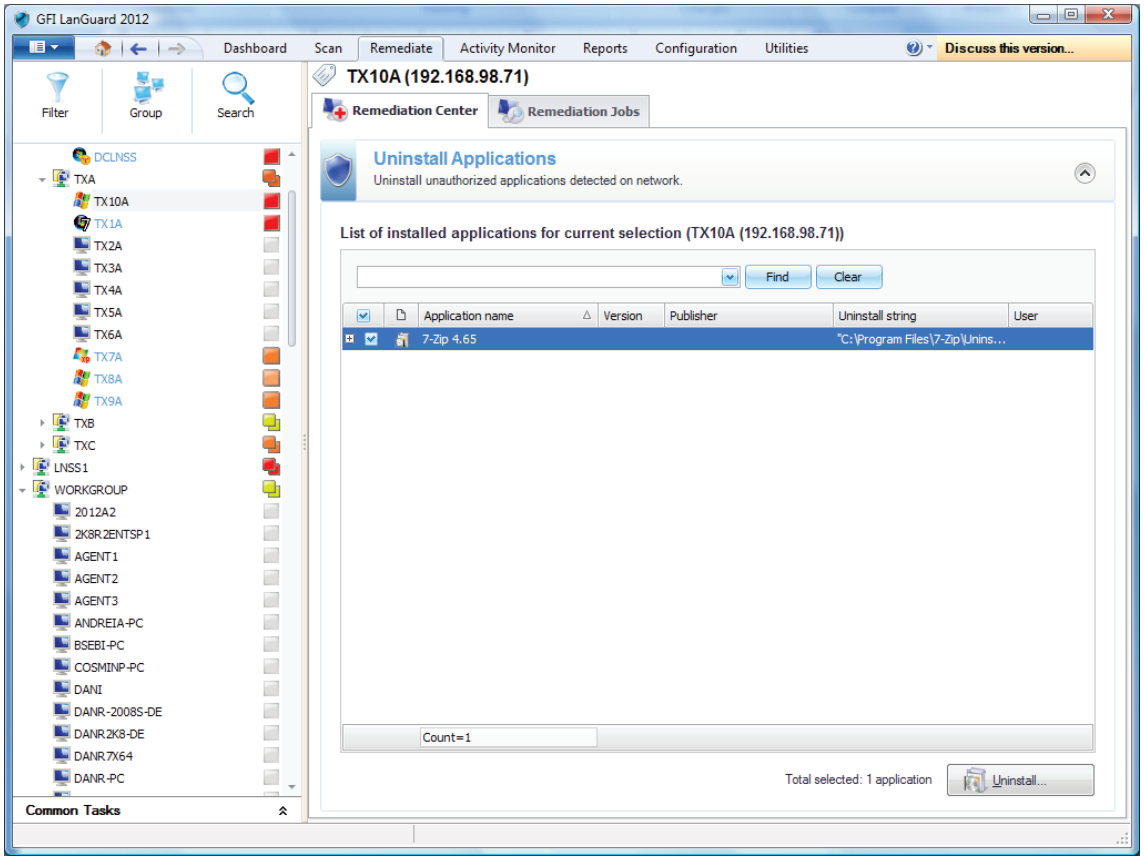
» Use Configuration > Auto-Uninstall Validation to test if GFI LanGuard is able to successfully uninstall an unauthorized application silently (no user input required on the target machine). If the validation succeeds GFI LanGuard is able and can be configured to automatically uninstall that application from the network.

Some applications do not support silent uninstall and they cannot be removed by GFI LanGuard because the uninstall process will show dialogs to the end users of the target machines, waiting for their input and interfering with their work.



» Rescan your network again to detect all unauthorized applications.

» Use *Remediate* > *Remediation Center* > *Uninstall Applications* to remove unauthorized applications from your network.



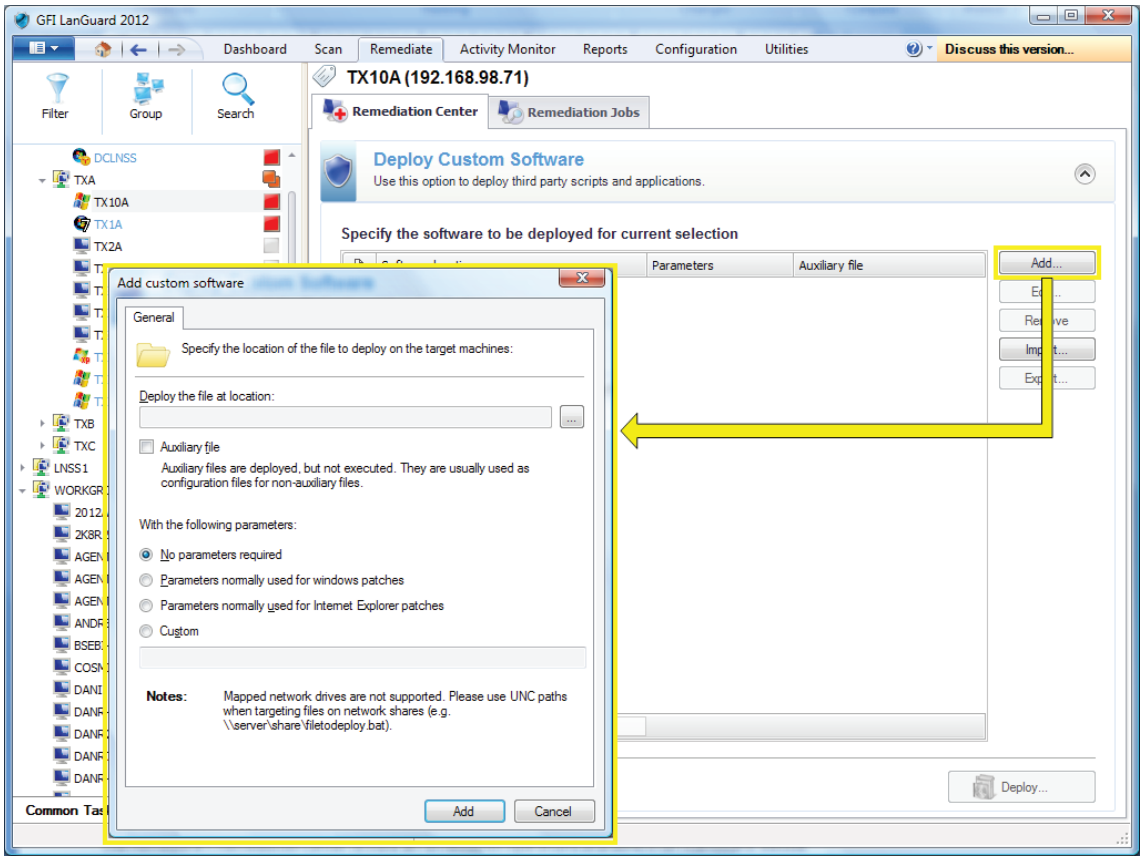
» GFI LanGuard can be configured to automatically detect and remove any unauthorized application from your network. See Automate Remediation Operations section for more details.

» Rescan the machines to get their security status once uninstall is done.

Deploy custom software

GFI LanGuard can deploy custom software and scripts network wide. Practically any piece of software that can run silently can be deployed using GFI LanGuard.

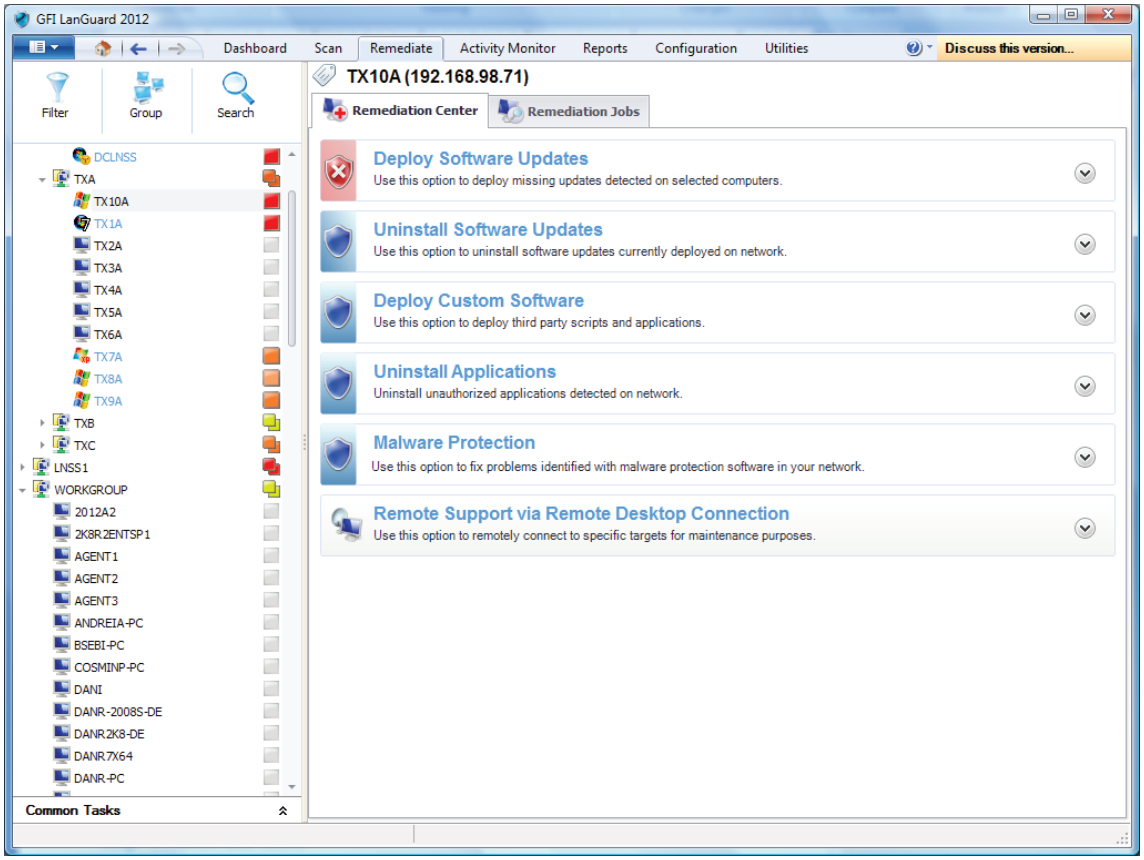
Use *Remediate > Remediation Center > Deploy Custom Software* to deploy custom software and scripts to your network. The steps to follow are pretty similar to the ones to deploy missing software updates, which is described here. The main difference is that while missing software updates are detected automatically, the custom software must be specified manually, together with parameters for silent installation and configuration files, if necessary.



Other remediation operations

Use *Remediate > Remediation Center* to view all remediation operations available in GFI LanGuard. Beside the ones mentioned in the above sections (deploy missing patches, uninstall unauthorized applications and deploy custom software), GFI LanGuard allows remediation operations like:

- Rollback patches – this option is very important when security updates that interfere with your business environment were installed
- Trigger definition updates for antivirus and anti-spyware software
- Trigger antivirus and anti-spyware scans on the remote machines
- Enable real-time protection for antivirus and anti-spyware solutions
- Turn on firewalls
- Open a remote desktop connection on the target machines to quickly solve security issues that cannot be fixed automatically.



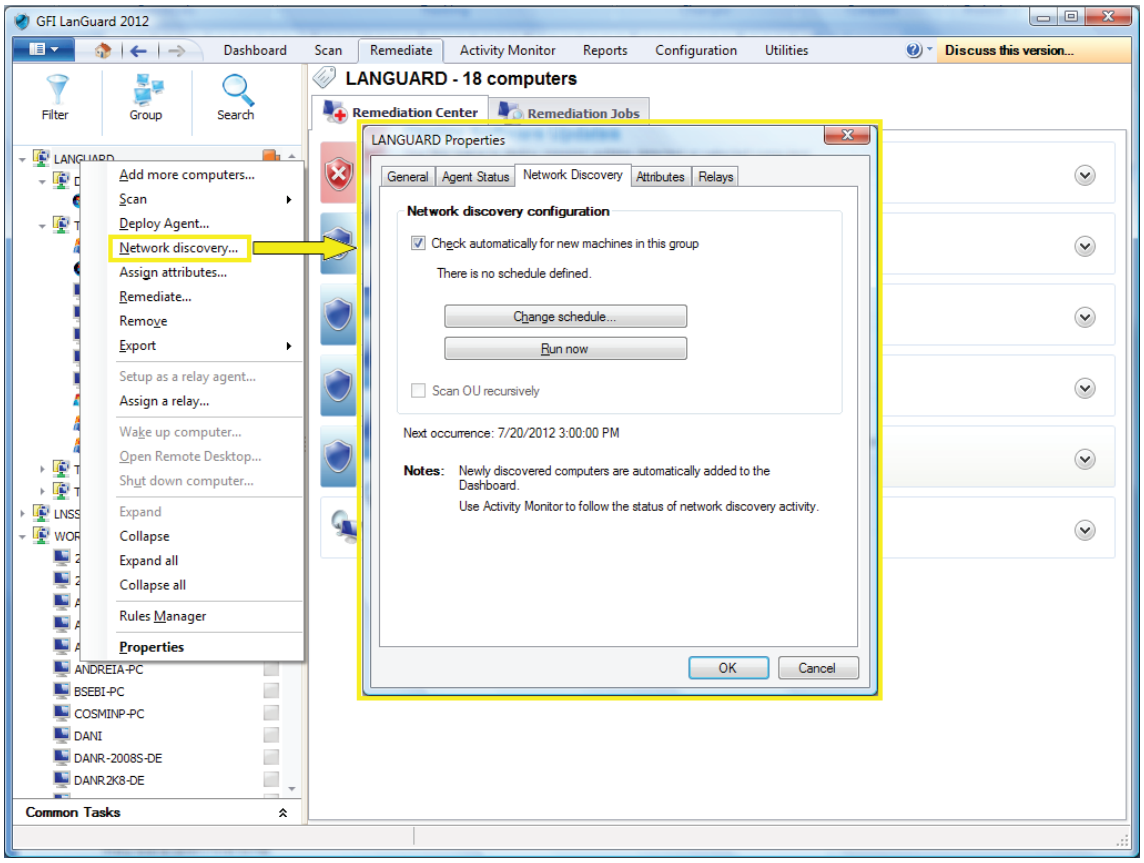
Step 4: Automate tasks

All important tasks from GFI LanGuard can be configured to run automatically on a regular basis.

Automatically discover new devices in the network

To monitor which new devices are live in the network, schedule a scan to run on regular basis under Network Discover profile.

Another simple way to automatically detect when new computers are added to a certain domain or organizational unit (OU) is to use the Dashboard. Right click on the domain/OU in the computers tree and select *Network Discovery*…



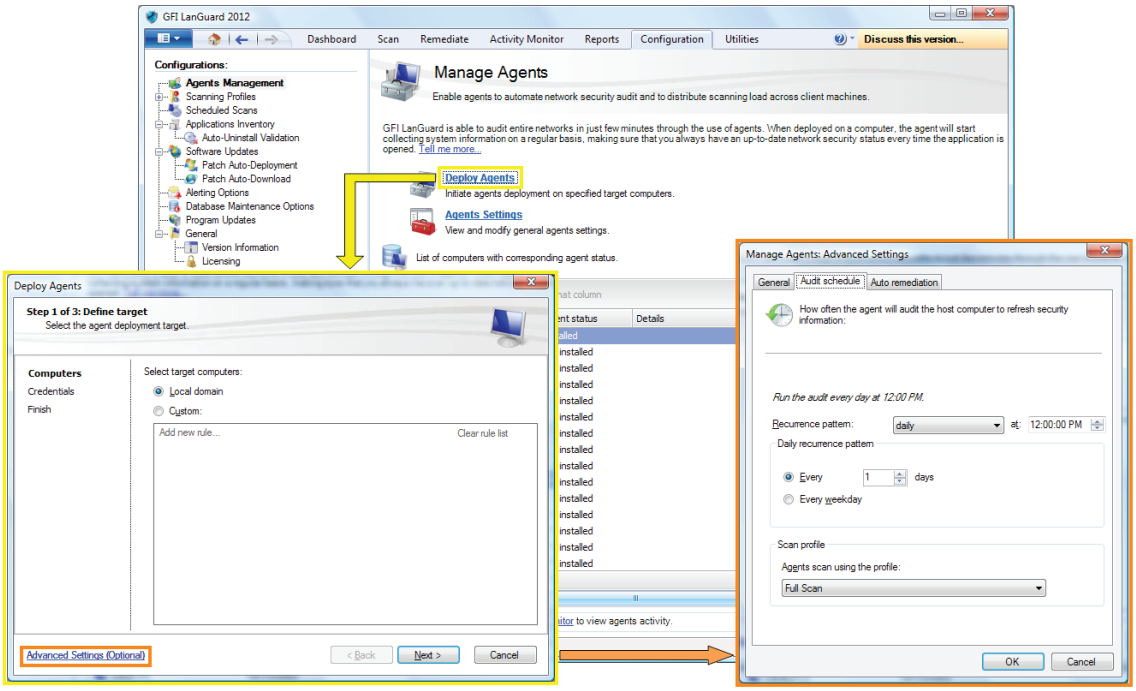
Use *Dashboard > History* view to investigate what new devices were detected in the network and when they were seen first time.

Automate security audits

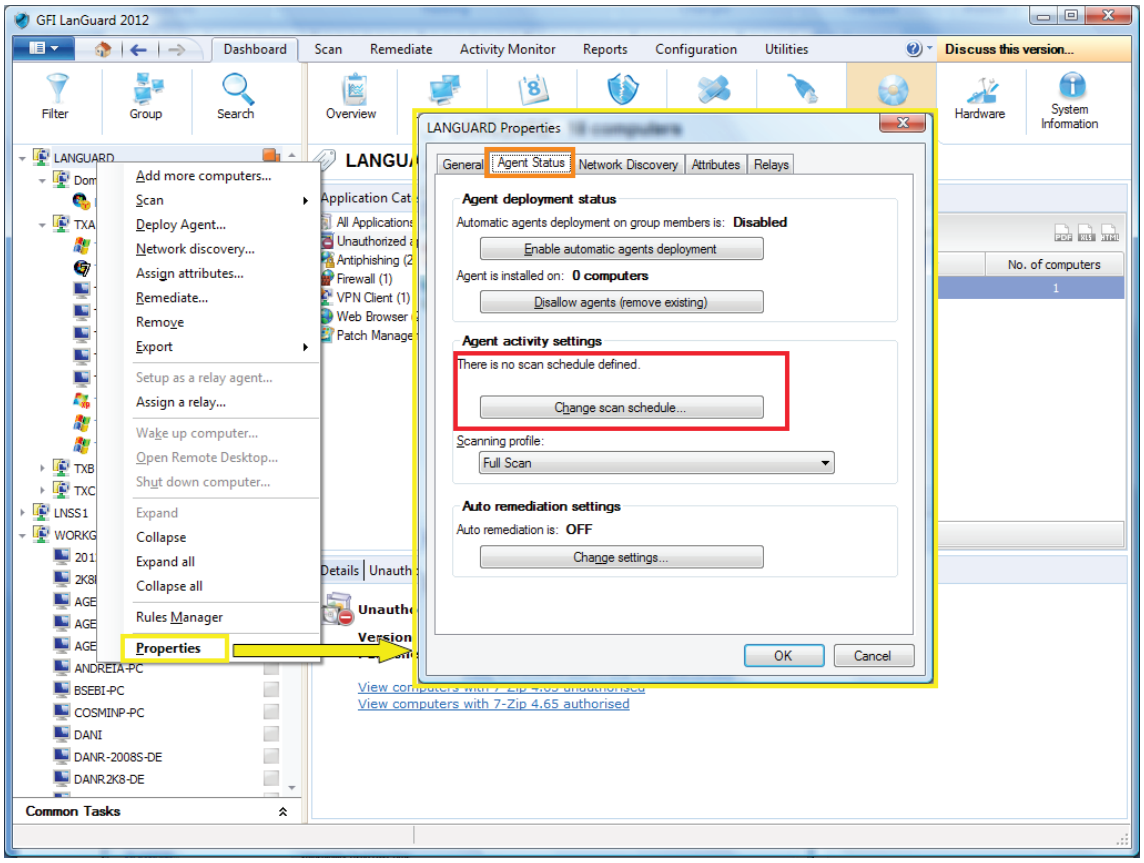
Security audits can be automated in two ways:

- Set agent-less scheduled scans to run in background on a regular basis
- Deploy agents on the target machines. By default, agents will audit the host machine once per day, but the audit schedule can be customized.

Customize audit schedule when deploying agents:

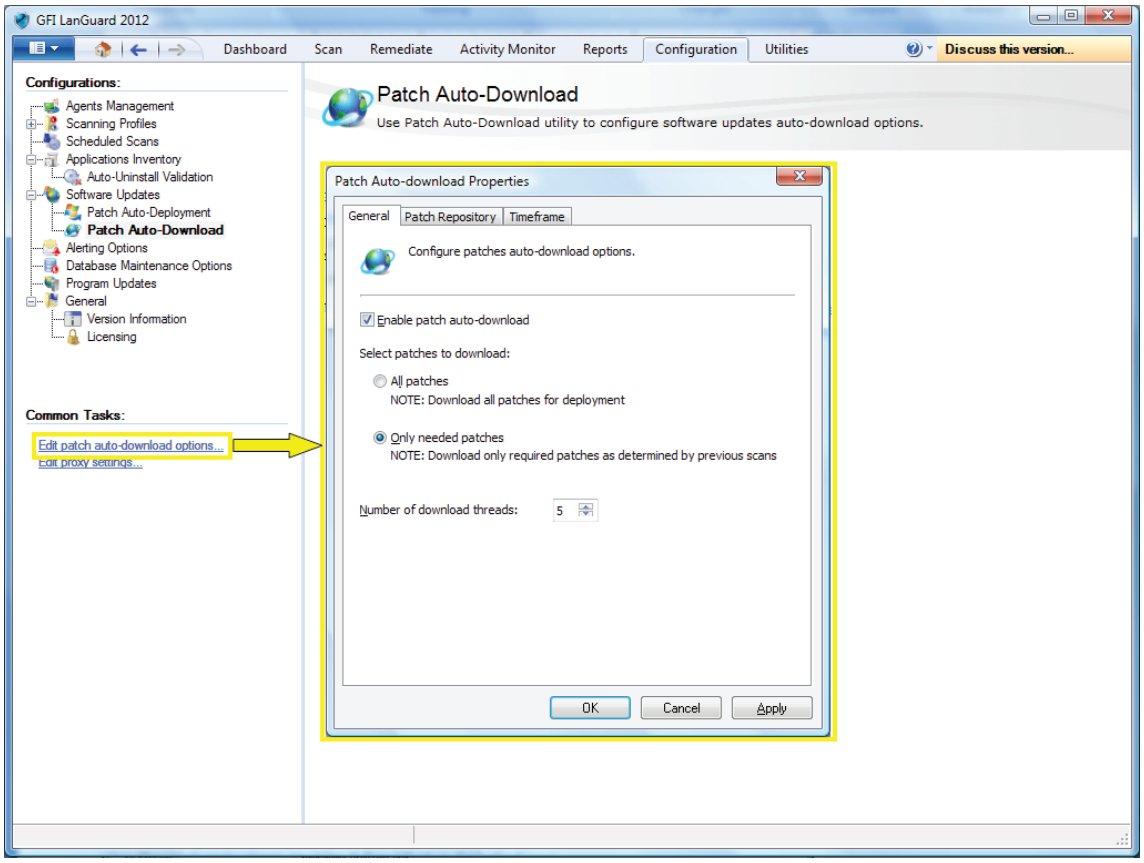


Customize audit schedule for agents using the Dashboard:



Automate patch download

Use *Configuration* > *Patch Auto-Download* to configure the product to download updates automatically so that they are available when the deployment operation starts.

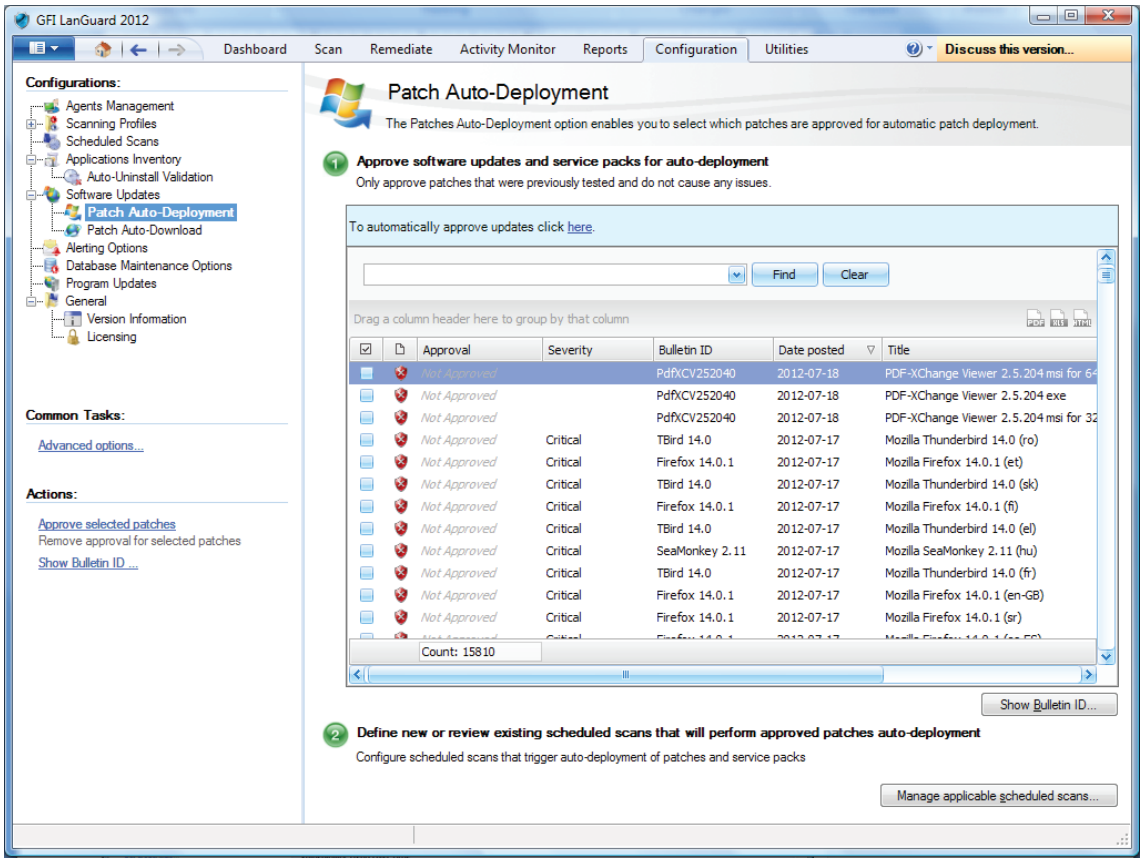


Automate remediation operations

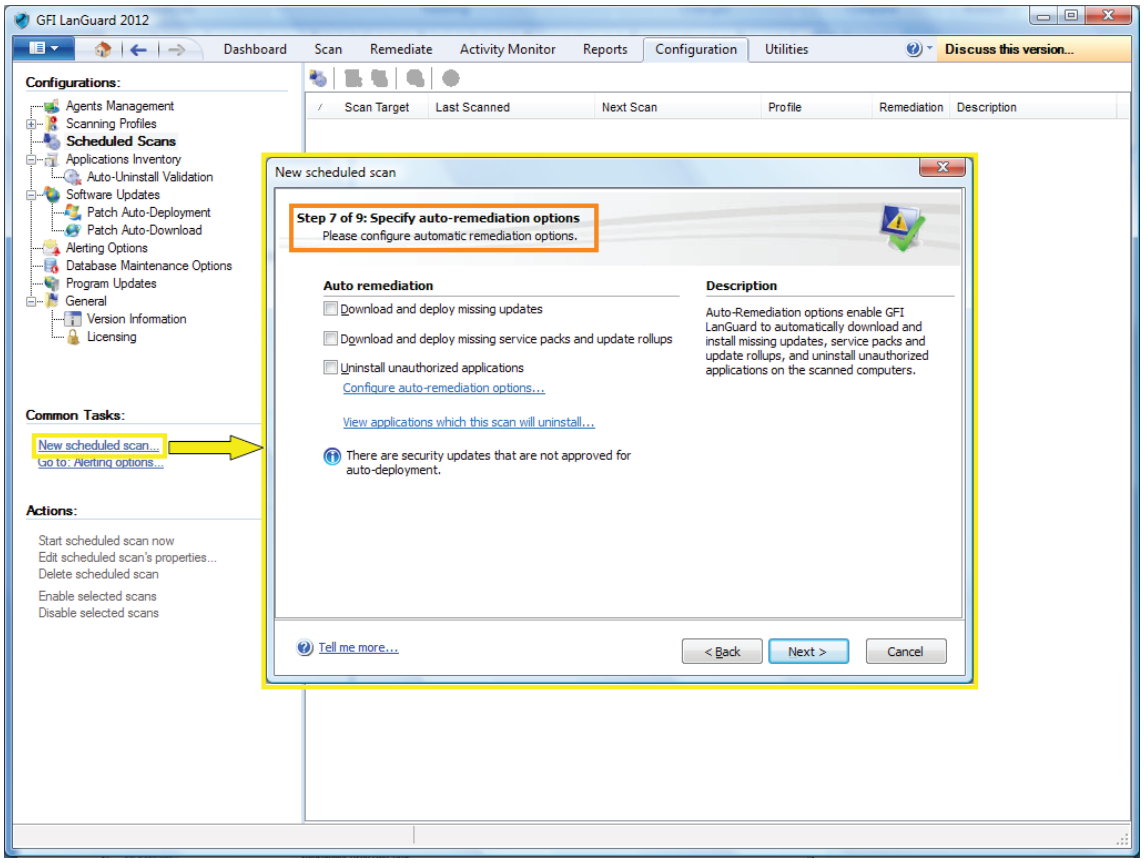
GFI LanGuard can be configured to automatically remediate certain security issues like deployment of updates and uninstall of unauthorized applications as they are detected by an agent-less scheduled scan or an agent scan.

Unauthorized applications must be defined first as described here.

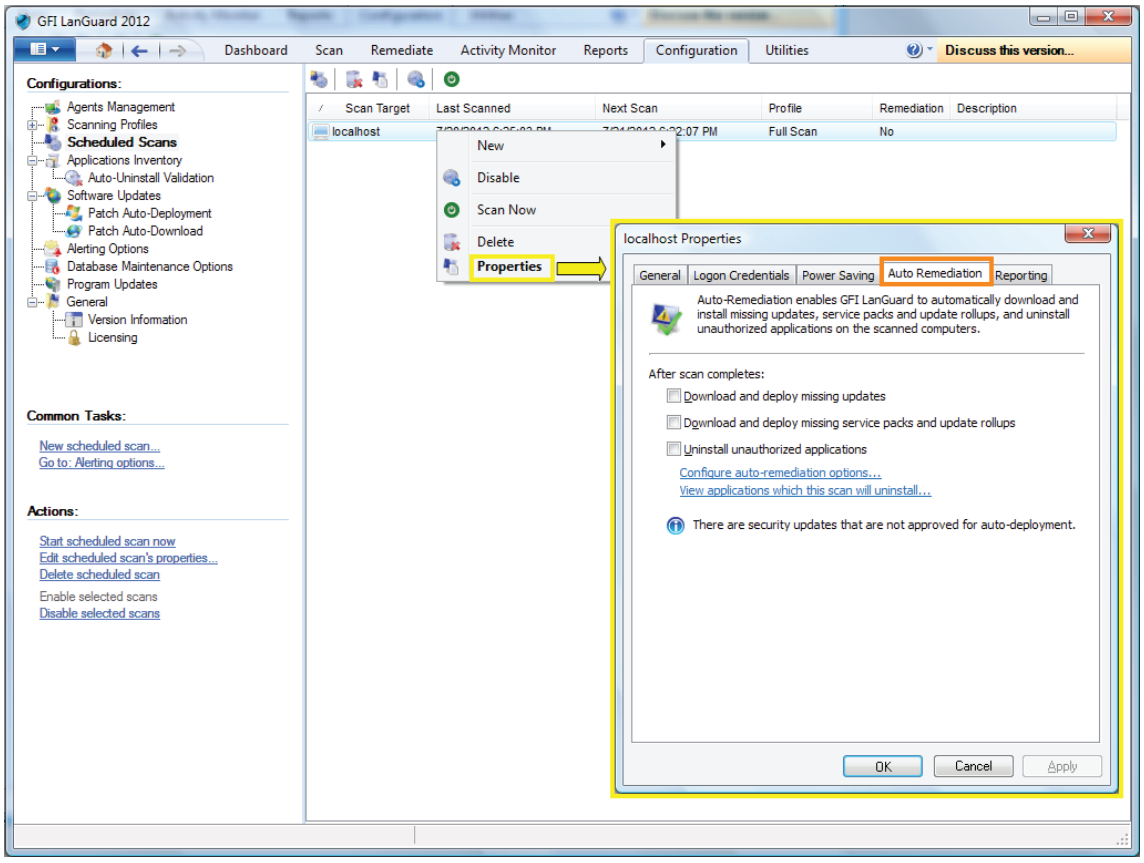
Security updates must be approved for auto-deployment using *Configuration* > *Patch Auto-Deployment* screen:



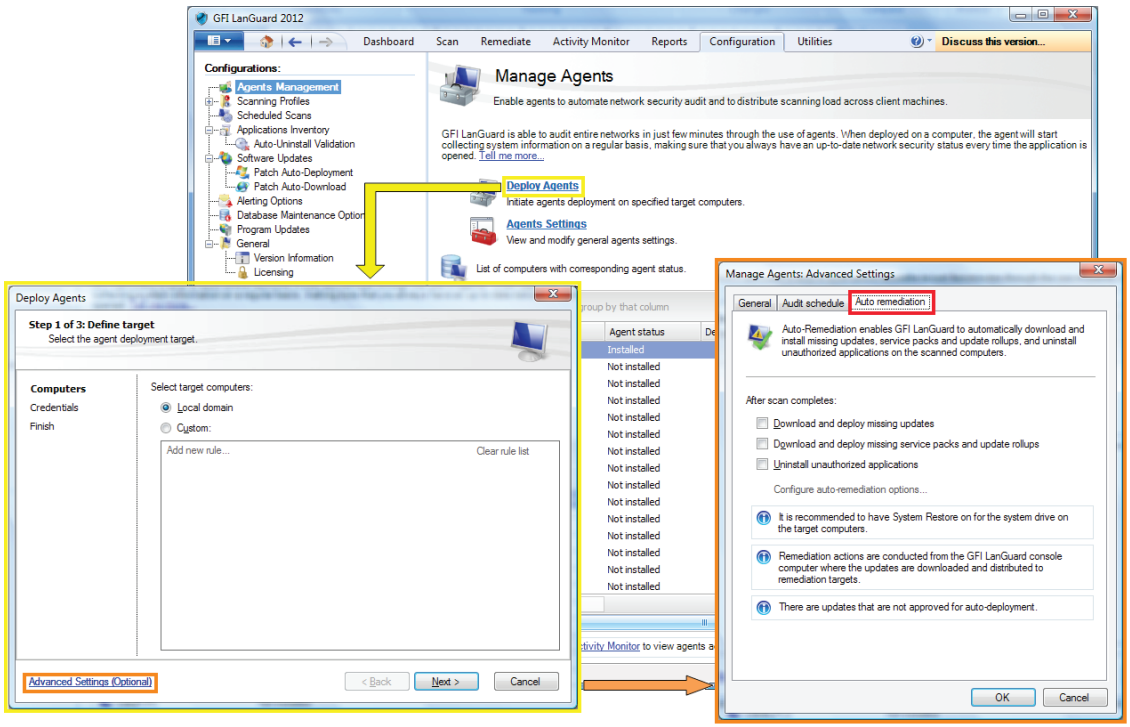
Enable auto-remediation for a new agent-less scheduled scan:



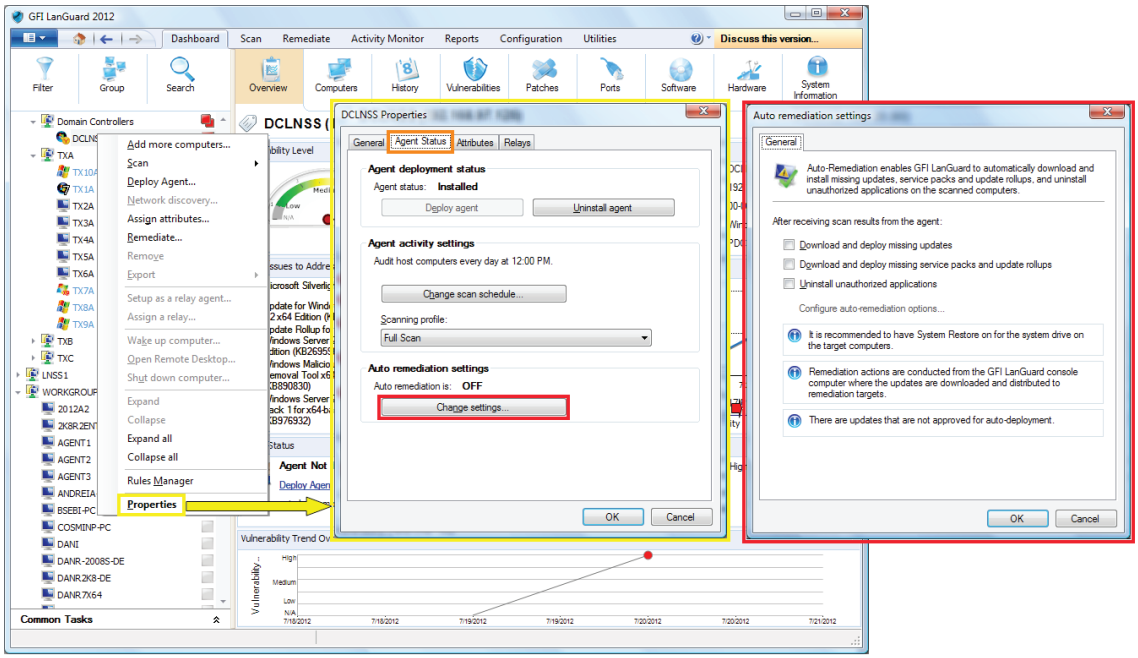
Enable auto-remediation for an existing agent-less scheduled scan:



Enable auto-remediation for agents when deploying them:

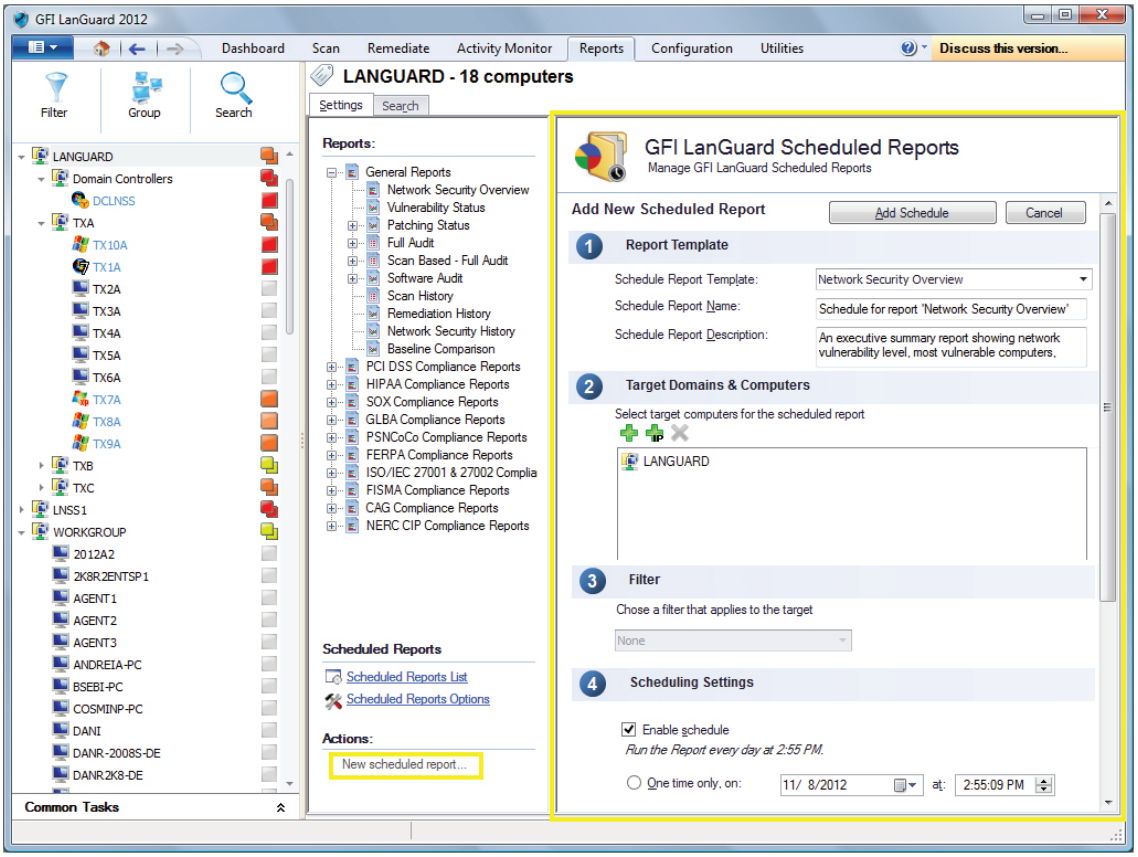


Enable auto-remediation for agent audits using the *Dashboard*:



Automate reports generation

All GFI LanGuard reports can be scheduled to be generated on a regular basis and to be automatically saved on the disk in a specified location or sent to an email recipient.



GFI LanGuard 2012 use cases

Using GFI LanGuard for vulnerability assessment

GFI LanGuard performs over 50,000 vulnerability checks on your operating system, virtual environments, network devices and installed applications using vulnerability check databases such as OVAL and SANS Top 20.

This section provides guidelines on how we recommend approaching vulnerability assessments and remediation of security issues to keep your computers secure and up to date.

» Keep GFI LanGuard up to date

- Make sure the machine that GFI LanGuard is installed on has Internet access. GFI LanGuard performs daily checks for updated information on vulnerabilities and patches
- If a proxy server is used, it can be set in the GFI LanGuard user interface > main menu > *Configuration* > *Proxy Settings*…
- If Internet access is not available on the machine where GFI LanGuard is installed, the product can be configured to get the updates from an alternative location. More details are available here.

» Perform security audits on regular basis

- New security issues are discovered every day. As their remediation requires some forward planning (i.e. machines might require a reboot, thus they will have small periods of downtime, etc.) it is better to be aware about security issues as early as possible to be able to plan for efficient remediation
- It is recommended to configure the product to automatically audit the network on a daily or weekly basis.

» Deploy missing security updates first

- The large majority of security issues can be fixed by ensuring all patches and service packs are up to date on each machine
- Service packs include a lot of security fixes so it is recommended to apply them first
- After the service packs are deployed, we recommend a rescan of the network (which will give you an updated view of the patch status of your network)
- After the rescan deploy any missing patches
- The product can be configured to deploy missing security updates automatically if pre-approved by the administrator.

» Investigate and remediate other security issues

- The results of the vulnerability assessment come with detailed description of the security issues detected and with references to external websites for additional information
- GFI LanGuard comes with tools to help address vulnerabilities by remotely uninstalling (unauthorized) software, or to enable antivirus/antispyware/firewall, or triggering definitions update for antivirus/antispyware, or to deploy custom software and scripts, or opening remote desktop connections to computers, etc.

» How to check your network security status:

- Use *Dashboard* > *Overview* to get an executive overview of the network security status, including top most vulnerable computers, vulnerability distribution and vulnerability trends
- GFI LanGuard provides a *Network Vulnerability Level*, which is calculated based on individual vulnerability levels of each machine. Each machine has a vulnerability level based on the security issues detected on it. Security issues are classified as having *High, Medium* or *Low* severity, based on CVSS scoring system as calculated by NVD

- Use *Dashboard > History* to get the list of new security issues detected, together with a list of other security sensitive configuration changes in the network
- Use *Dashboard > Vulnerabilities* to get a detailed view of vulnerabilities detected in the network
- Use *Dashboard > Patches* to get a detailed view of network patching status
- Use *Reports > Network Security Overview* report to get an executive overview of network security status
- Use *Reports > Vulnerability Status* report to get a detailed overview of network security status
- Use *Reports > Remediation History* report to get a history if security issues remediated using GFI LanGuard
- Reports can be configured to generate on a regular basis.

Using GFI LanGuard for patch management

GFI LanGuard offers on-demand or automated detection, download and deployment of missing updates, covering:

» Microsoft and Mac OS X operating systems

» Microsoft and Mac OS X applications

» Most popular and security sensitive third-party applications running on Windows platforms, including all major web browsers, Adobe products, Java runtimes and so on. Click here for full list

» Both security and non-security patches

» Rollback of patches

» Network-wide deployment of custom software and scripts (any piece of software that can run silently can be deployed using GFI LanGuard).

Click here for a set of guidelines to help you keep the network secure and up to date.

Using GFI LanGuard for asset tracking

Unmanaged or forgotten devices are a security risk. Use GFI LanGuard to find the devices you were not aware of:

» Servers and workstations

» Virtual machines

» IP-based devices such as routers, printers, switches, etc.

» Mobile devices such as iPad®, iPhone® and Android™ phones .

Click here for more details.

Using GFI LanGuard for network and software audit

GFI LanGuard provides a detailed analysis of what is happening on your network – which applications or default configurations are posing a security risk and all the information you need to know about your network such as:

» Operating systems

» Virtual machines

» Hardware and software installed

» CPU information

» HDD space

» Wireless devices

» Network adaptors

» Services

- Auditing policies
- Users and groups
- Shares
- TCP and UDP open ports.

Use *Dashboard* > *Software* to get a detailed view of all the applications installed in the network.

Use *Dashboard* > *Hardware* to check the hardware inventory of the network.

Use *Dashboard* > *System Information* to view security sensitive details about the systems present in the network.

Use ***Dashboard > History*** to get a list of security sensitive changes that happened in the network

Use *Reports* > *Software Audit* to generate a comprehensive report about the applications installed in the network.

GFI LanGuard can be used to mark, detect and **remove unauthorized applications** from the network.

GFI LanGuard integrates with over **2,500 critical security applications** of the following categories: antivirus, anti-spyware, firewall, anti-phishing, backup client, VPN client, URL filtering, patch management, web browser, instant messaging, peer-to-peer, disk encryption, data loss prevention and device access control. It provides reports on their status and **rectifies issues** by allowing operations like enabling antivirus or firewall, triggering definitions updates for antivirus or anti-spyware, uninstalling peer-to-peer applications, etc.

Using GFI LanGuard for regulatory compliance

There are more and more laws and regulations that are imposing security best practices to companies. Government institutions, companies offering financial services and healthcare are among the most affected by these regulations, but the trend is that all companies will need to be secure enough to be able to protect the privacy and data of their employees, customers and partners. Failure to comply can result in losing opportunities, legal and financial penalties or even, in extreme cases, going out of business.

Here is a list of most common security items these regulations require and where GFI LanGuard is able to help:

- Perform regular **vulnerability assessments**
- Keep the systems fully **patched**
- Ensure that **antivirus and antispyware software is installed**, running and up to date on all systems in the network
- Ensure that personal firewall is installed and turned on, on each system in the network
- Ensure that encryption software is installed throughout the network.

GFI LanGuard can be combined with other GFI Software™ products to form a suite of products dedicated to compliance:

- VIPRE® – antivirus, anti-spyware and personal firewall solution
- GFI EventsManager® – log management solution
- GFI EndPointSecurity™ – device blocking solution.

GFI LanGuard ships, out of the box, with a set of predefined reports dedicated to compliance with PCI DSS, HIPAA, SOX, GLBA and PSN CoCo amongst others. More details on PCI DSS are available **here**.

Here is a list with some of the most important standards related to IT infrastructure security:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes–Oxley Act (SOX)
- Gramm–Leach–Bliley Act (GLB/GLBA)

- Federal Information Security Management Act (FISMA)
- Family Educational Rights and Privacy Act (FERPA)
- Public Services Network – Code of Connection (PSN CoCo)
- European Union Data Protection Directive
- European Union Directive on Privacy and Electronic Communications.

Useful links

GFI LanGuard Overview

White Papers

Case Studies

Videos

System Requirements

Documentation

Support

Pricing

Awards/Reviews

GFI 4240 dec12

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus