GFI Product Manual

GFI LanGuard™

Evaluator's Guide - Getting the best benefits out of a GFI LanGuard Trial

GFI®

Document Version: 12.1

Last updated (month/day/year): 01/16/2017

Contents

1 Introduction

Thank you for evaluating GFI LanGuard. The aim of this guide is 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.

Topics in this section:

1.1 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
- Mobile device management
- Risk analysis
- Compliance

GFI LanGuard scans, analyzes and helps remediate your network.

» Regardless of an agent-based or agent-less installation, 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, smartphones and tablets used by employees and hardware inventory. GFI LanGuard integrates with over 4000 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 if issues are detected. A vulnerability level is assigned to each scanned computer, based on the audit results. GFI LanGuard also 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, for example, 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. All of these actions will help ensure your network is up-to-date and that the latest patches are applied.

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.

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 Why do customers purchase GFI LanGuard?

Based on our experience, the top five reasons GFI customers purchase GFI LanGuard are:

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 installed) 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, Mac OS, Linux systems 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 (for example, PCI DSS, HIPAA, SOX, GLBA, PSN CoCo)

5. To assess and manage security of smartphones and tablets used by employees to access company information and applications

The following topics provide real life scenarios with more insight into practical uses of GFI LanGuard:

1.3.1 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. Their remediation requires some forward planning and 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.

» 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

» Use **Reports > Mobile Device Audit** report to get an overview of what smartphones and tablets connect to the company's Microsoft Exchange servers and detect if they have outdated operating systems, with known security issues.

» Reports can be configured to generate on a regular basis

1.3.2 Using GFI LanGuard for patch management

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

- Microsoft operating systems and applications
- Apple OS X operating systems and applications
- Linux operating systems and applications. The following Linux distributions are supported: Red Hat Enterprise Linux, Fedora, Ubuntu, Suse, OpenSuse, CentOS and Debian
- Most popular and security sensitive third party applications running on Windows platforms, including all major web browsers, Adobe products, Java runtimes and so on. For a full list click here.
- 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)

1.3.3 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, access points, switches, etc.
- Mobile devices such as iPads, iPhones and Android phones

For more information, refer to Deploy custom software (page 37).

1.3.4 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
- Smartphones and tablets that connect to company's services such as Microsoft Exchange, Office 365, Google Apps and Apple Profiles Manager

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

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

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

Use **Reports > Mobile Device Audit** report to get an overview of what smartphones and tablets connect to the company's services such as Microsoft Exchange, Office 365, Google Apps and Apple Profiles Manager and detect if they have outdated operating systems, with known security issues.

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

GFI LanGuard integrates with over 4000 critical security applications of the following categories: antivirus, antispyware, 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 antispyware, uninstalling peer-to-peer applications.

1.3.5 Using GFI LanGuard for regulatory compliance

There are more and more laws and regulations that impose security specific 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 protect the privacy and data of their employees, customers and partners. Failure to comply can result in losing opportunities, legal and financial penalties and 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:

- 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)
- Children's Internet Protection Act (CIPA)
- Public Sector Network - Code of Connection (PSN CoCo)
- European Union Data Protection Directive
- European Union Directive on Privacy and Electronic Communications

1.3.6 Using GFI LanGuard for mobile device management

GFI LanGuard is able to detect smartphones and tablets that connect to the company's services such Microsoft Exchange servers, Office 365, Google Apps or Apple Profiles Manager and:

- Breakdown devices by user, manufacturer, device model, operating system, last connection time
- Perform a vulnerability assessment of the device operating system. Android, iOS and Windows Phone are supported.
- Report about operating system updates available
- Send custom email notifications to device owners.

1.4 Obtaining an evaluation key

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

To start the evaluation of GFI LanGuard enter your free evaluation key. The evaluation key gives you the full functionality of the product, limited to 25 IP addresses and 25 mobile devices for 30 days. The key is sent to the email address you registered with when downloading the product.

If you do not have access to the original email with the key, you can request a new evaluation key for free by clicking here.

If you need to evaluate for a longer period or with more than 25 IP addresses and 25 mobile devices, you can submit your request here.

2 Perform security scans

On Windows systems GFI LanGuard can perform both agent-less and agent-based security scans. At present only agent-less scans are available for non Windows based systems (Linux, Mac OS, network devices, smartphones and tablets). Below are some items to consider when choosing what scanning method to use:

Agent-less scans:

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

Agent-based scans:

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

Topics in this section:

2.1 Agent-less security scans

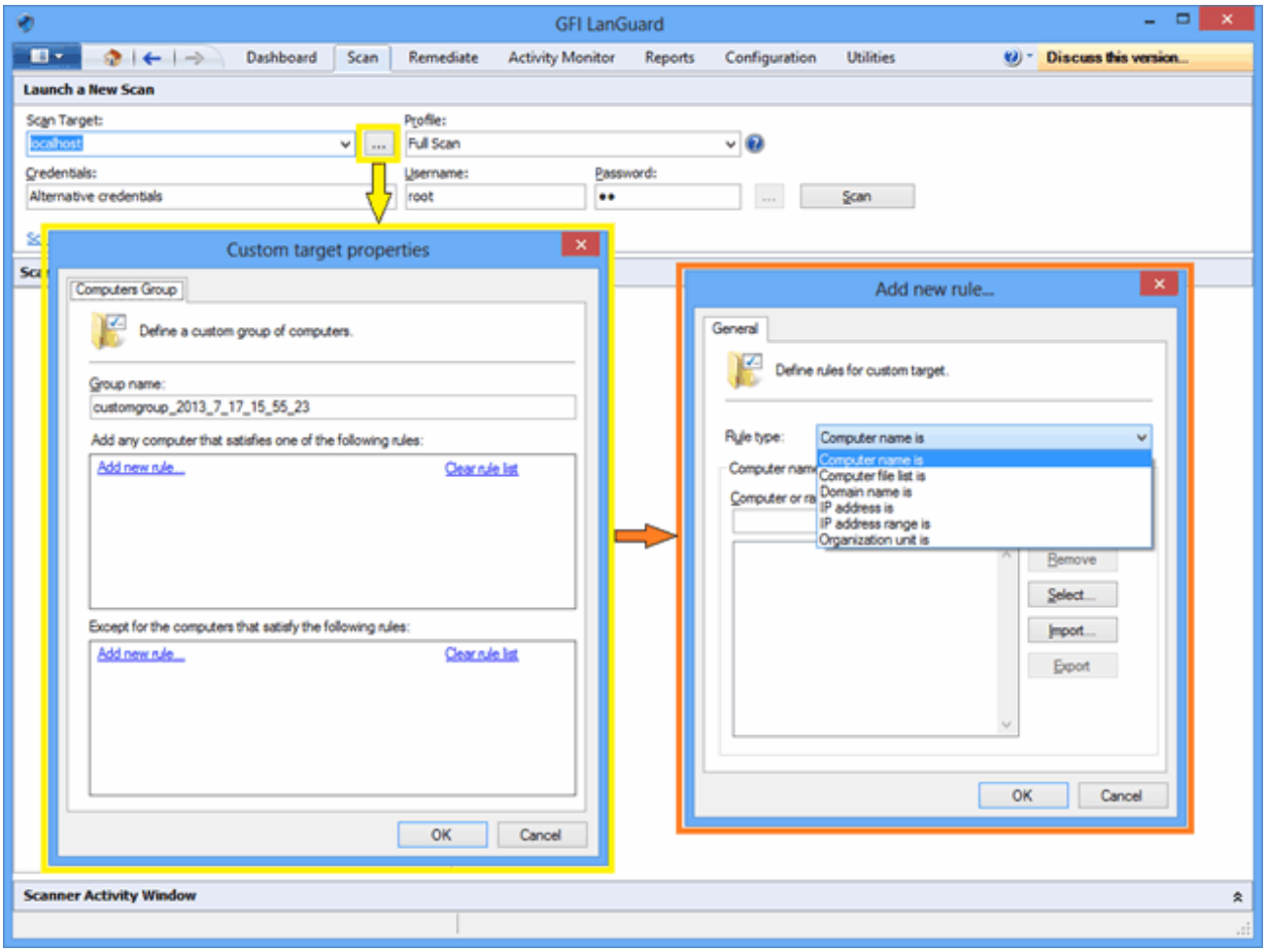
2.1.1 Trigger scans and follow progress in real time

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 the following:

- Computer names
- Text files containing computer names
- Single IP address and ranges of IP addresses
- Domain or workgroups and organizational units

NOTE

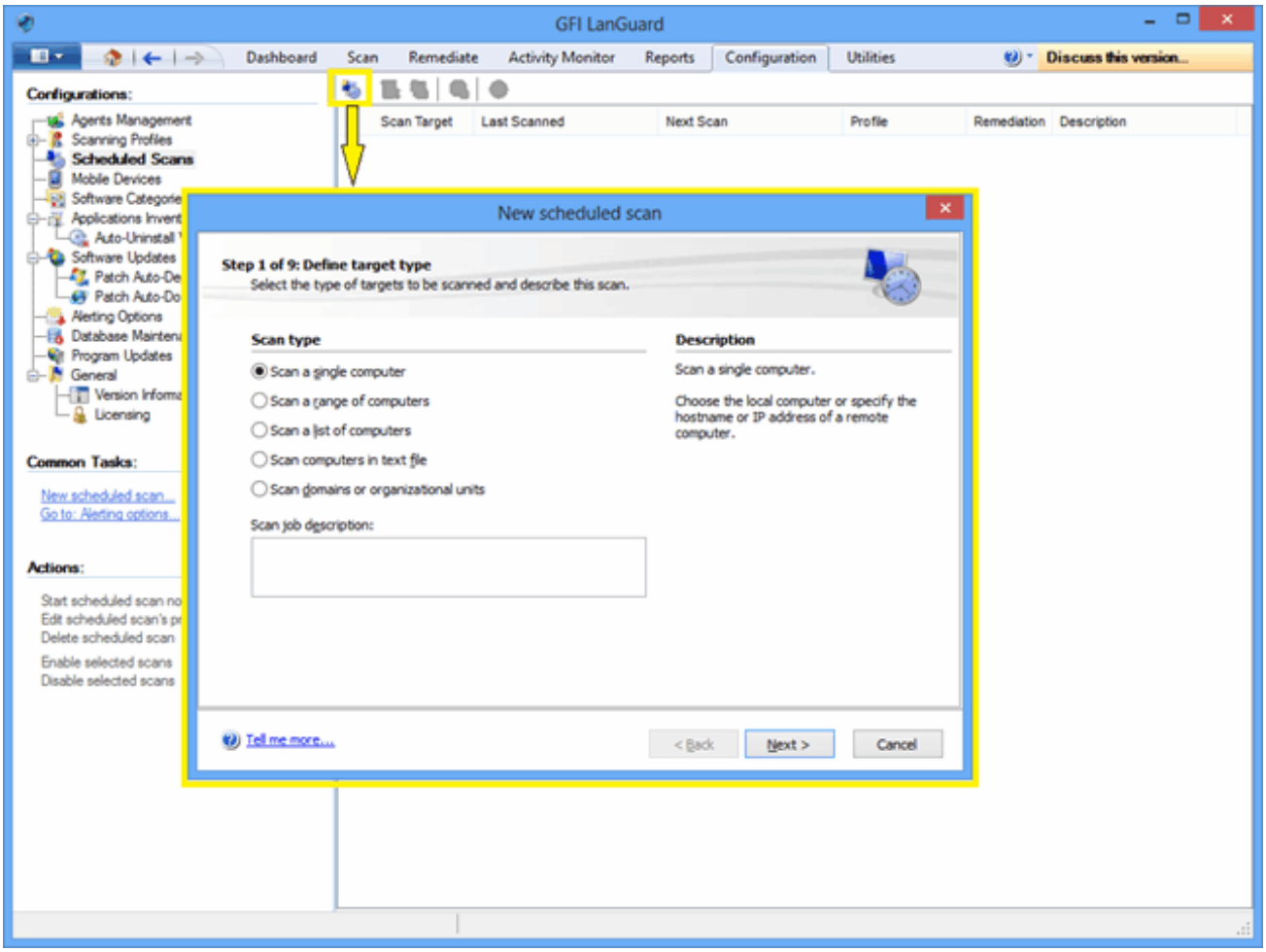
Administrative access to the remote machines is required for comprehensive security audit results.



Screenshot 1: Agent-less security scans

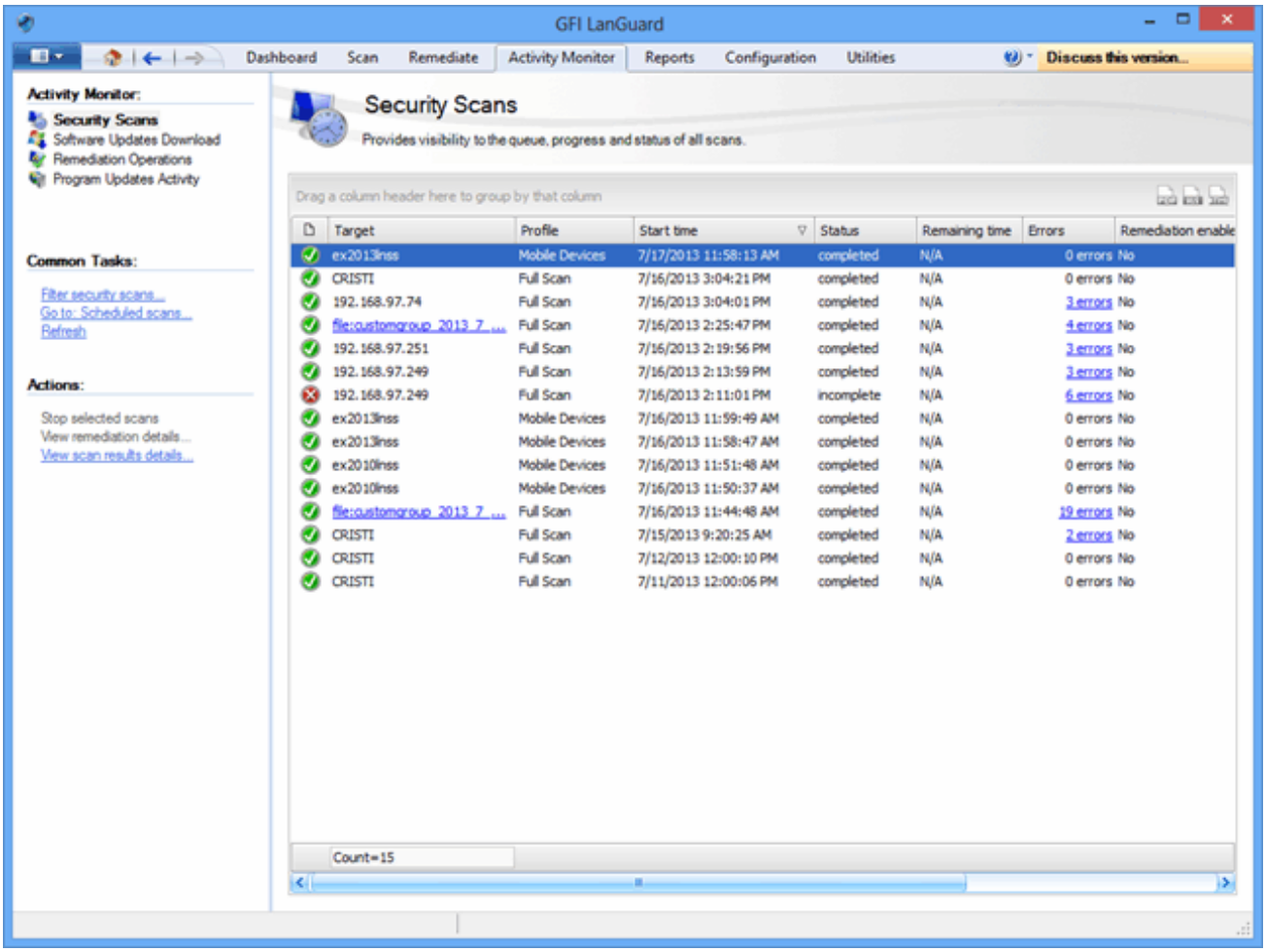
2.1.2 Scheduled scans

1. To schedule agent-less scans to run on regular basis click **Configuration > Scheduled Scans** and select the type of targets to scan.



Screenshot 2: New schedule scan

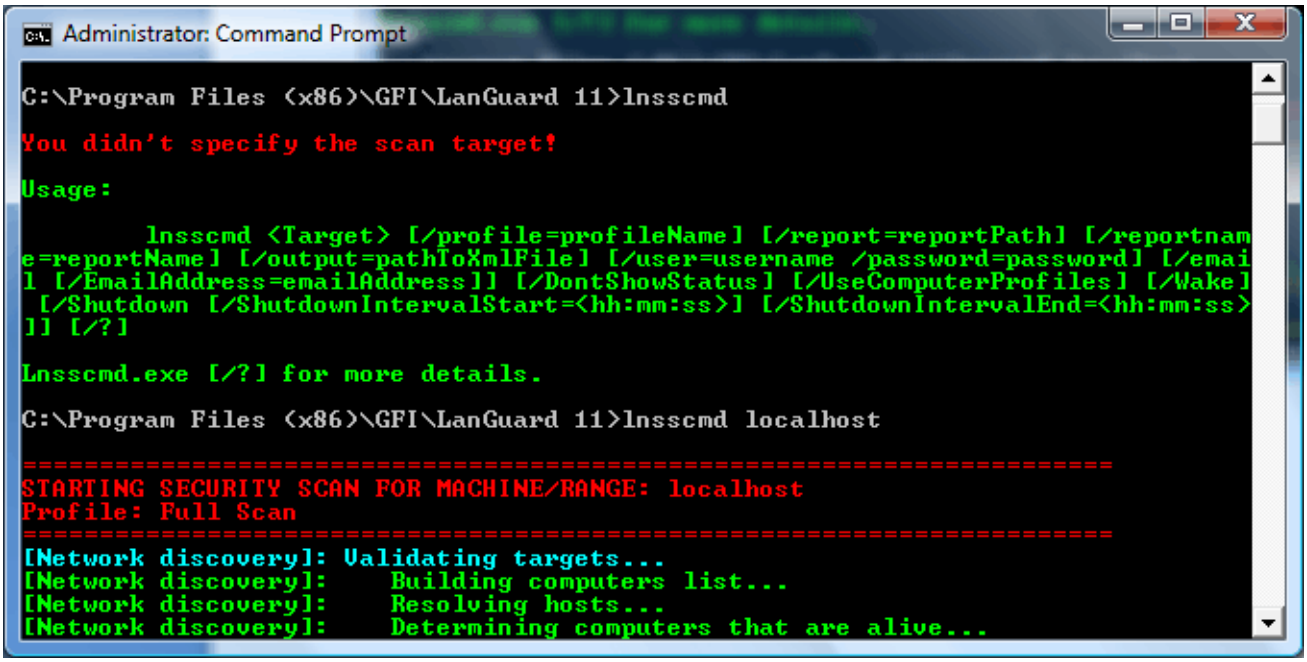
2. Progress of scheduled scans can be followed using **Activity Monitor > Security Scans:**



Screenshot 3: Security scans

2.1.3 Command line scans

1. To run command line scans use **lnsscmd.exe** tool



Screenshot 4: Command line scans

2.2 Agent-based audits

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.

What agents do:

» GFI LanGuard installs the agents automatically on the selected computers

» Agents only install on Microsoft 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 600 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.

» Agents can be uninstalled from within GFI LanGuard. 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 1072. 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.

IMPORTANT

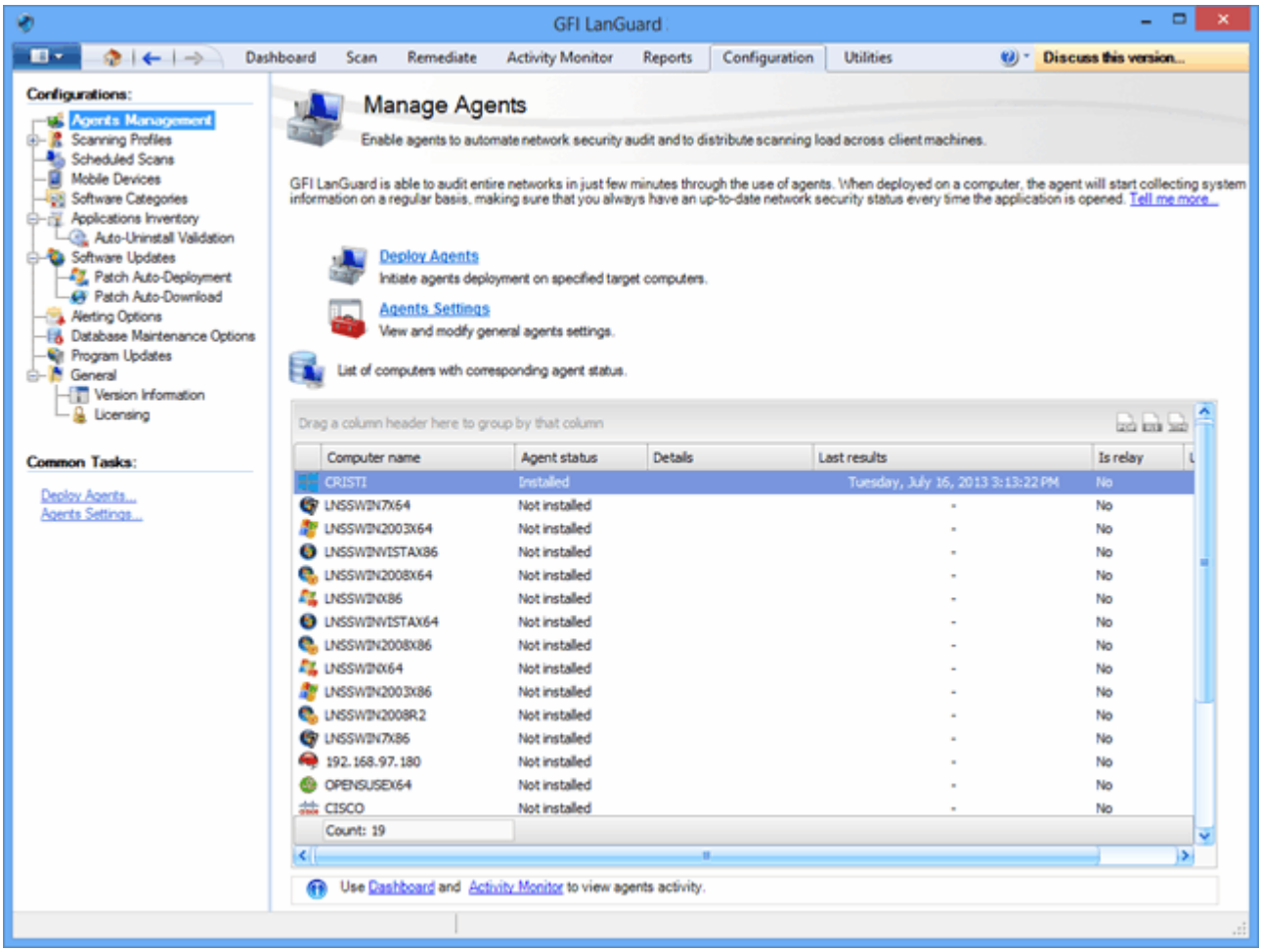
An Agent may be designated a Relay Agent, which allows remediation to be performed more efficiently and using less network bandwidth for multi-site or large networks. The Relay Agent stores a local copy of the patch data (normally stored on the GFI LanGuard server) and this is used to remediate nearby computers.

NOTE

For more information about Relay Agents refer to the Administrator Guide that can be downloaded from here.

To enable agents:

1. Click **Configuration > Manage Agents**

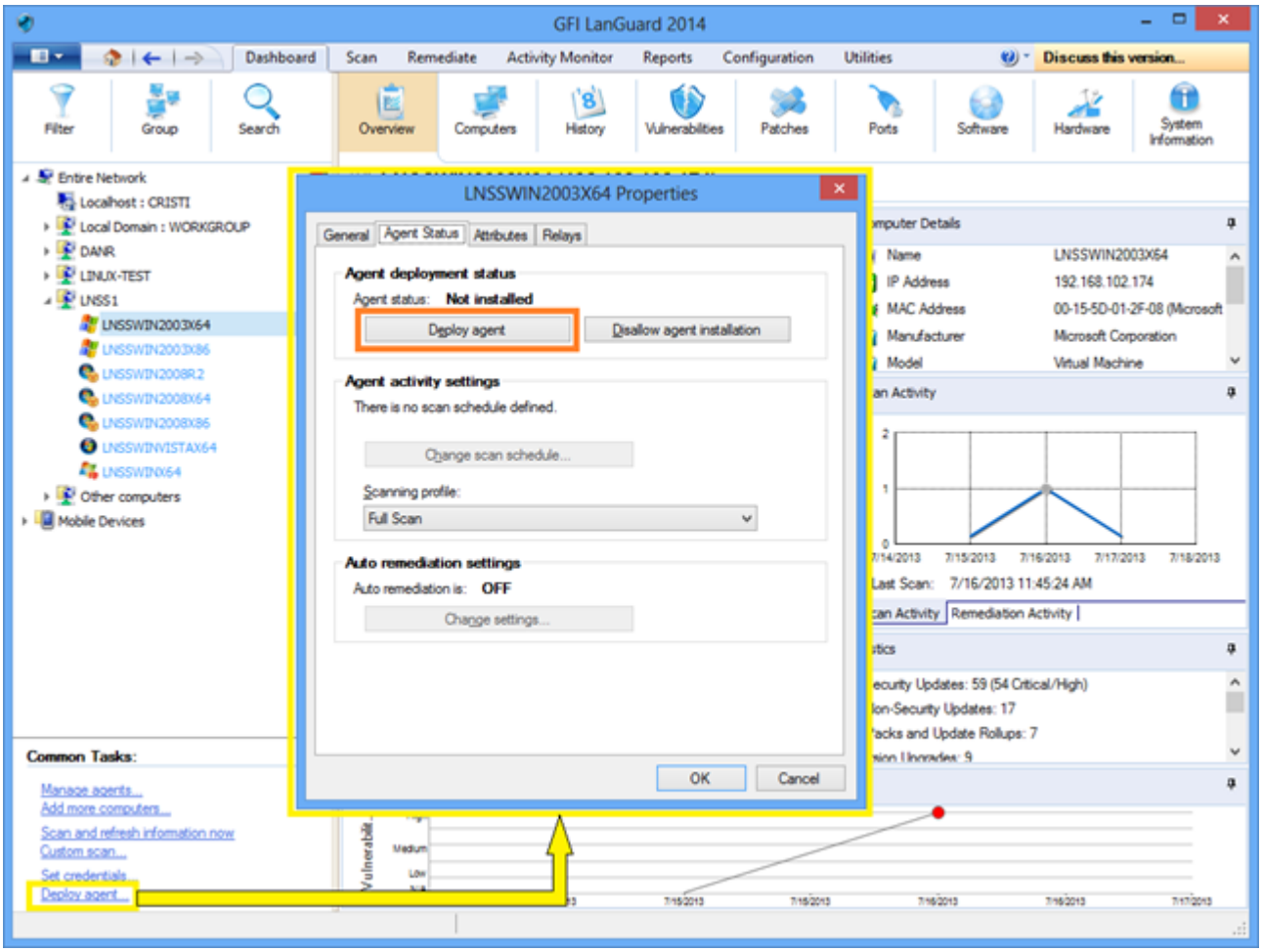


Screenshot 5: Managing agents

2.2.1 Troubleshooting agent deployment errors

For a list of possible causes in case GFI LanGuard fails to deploy agents on certain machines click here

To enable and configure agents, click **Dashboard > Overview** and select **Deploy agent…** from the **Common Tasks** section:



Screenshot 6: Deploying agent

2.2.2 Trigger agent-based on-demand scans

Agent-based scans usually run automatically in the background on remote machines according to the audit schedule that was set (by default agents do their scan once per day).

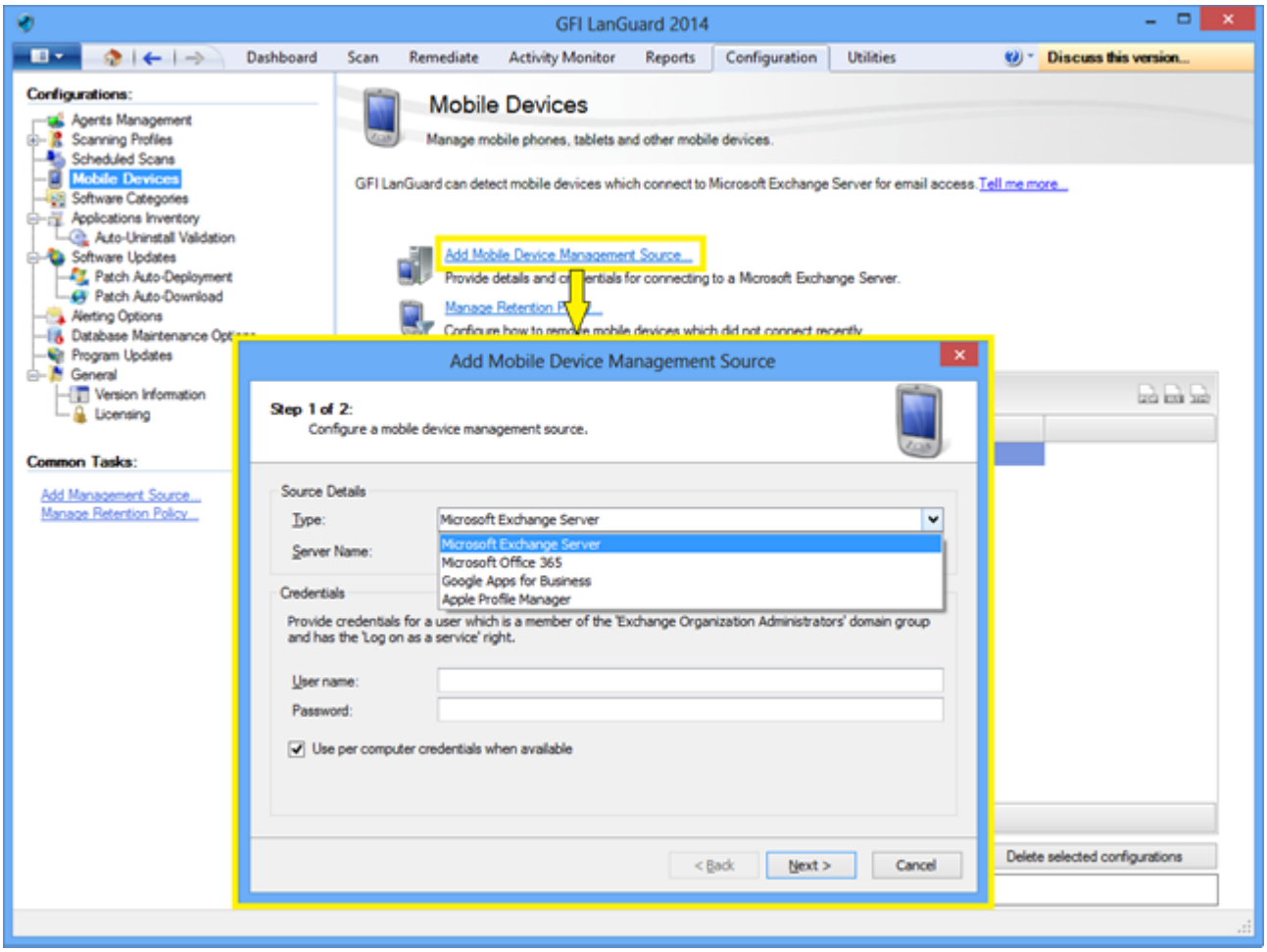
> **NOTE**
>
> If a refresh of the security information is required,you can trigger on-demand agent scans using the **Scan and refresh now** option from the **Dashboard**.

2.3 Audit smartphones and tablets

GFI LanGuard can audit smartphones and tablets that connect to the company's services (such as Microsoft Exchange, Office 365, Google Apps and Apple Profiles Manager). Use this feature to learn what mobile devices are used by your employees, what security issues they have and if there are any operating system updates that would fix those security issues.

> **NOTE**
>
> Mobile devices audit is agent-less. The supported systems are: Google Android, Apple iOS and Windows Phone.

Use **Configuration > Mobile Devices** to add or edit mobile device management sources.



Screenshot 7: Managing Mobile Devices

Mobile device scans can be monitored using **Activity Monitor > Security Scans**. Scan results for mobile devices can be seen in the dashboard or by generating reports. Mobile device audit report is dedicated to the scan results retrieved for smartphones and tablets.

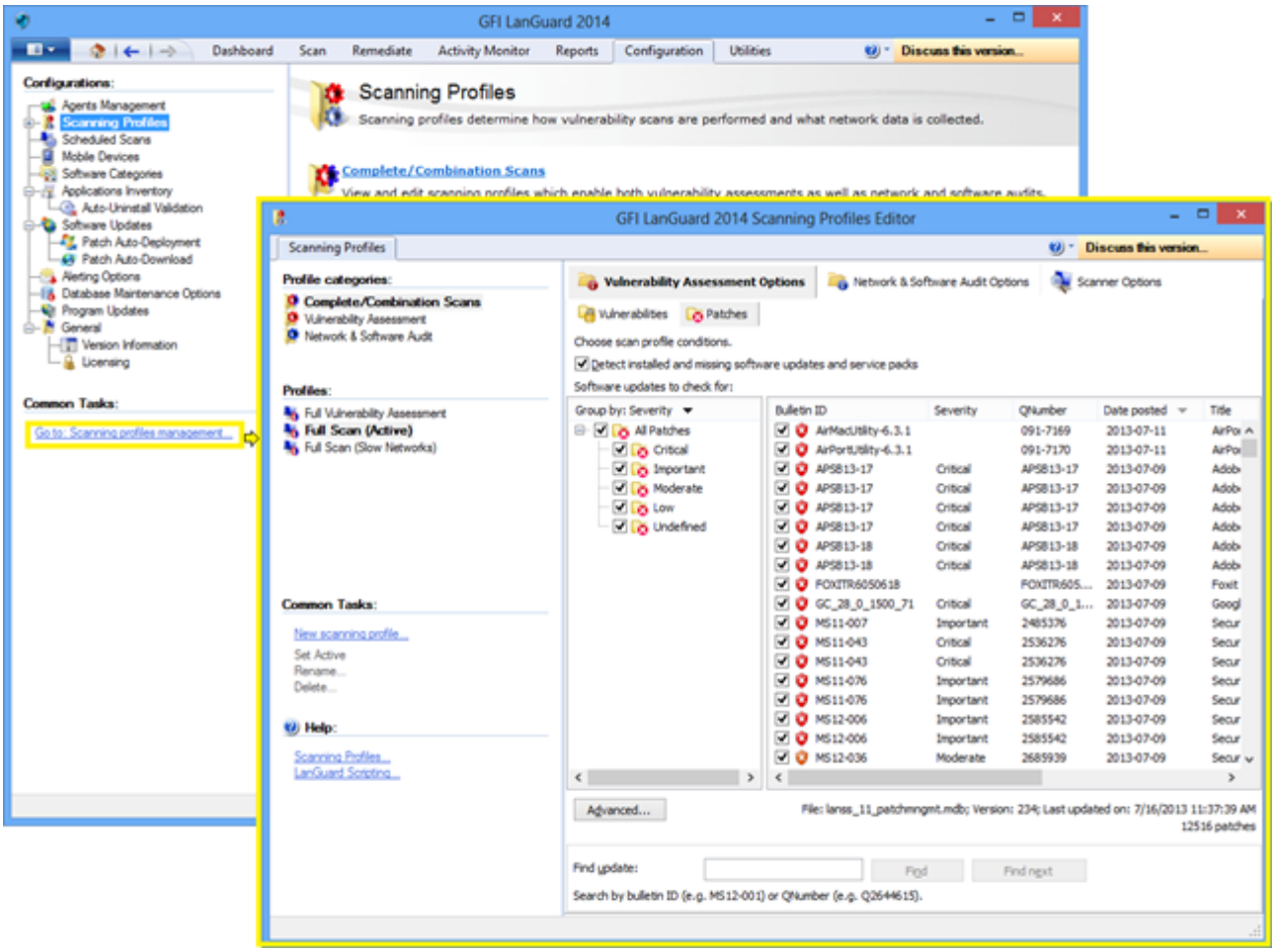
> **NOTE**
> Email notifications can be sent to mobile device owners to inform them about operating system security updates available for their device.

2.4 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.

To view, modify or create new custom scanning profiles:

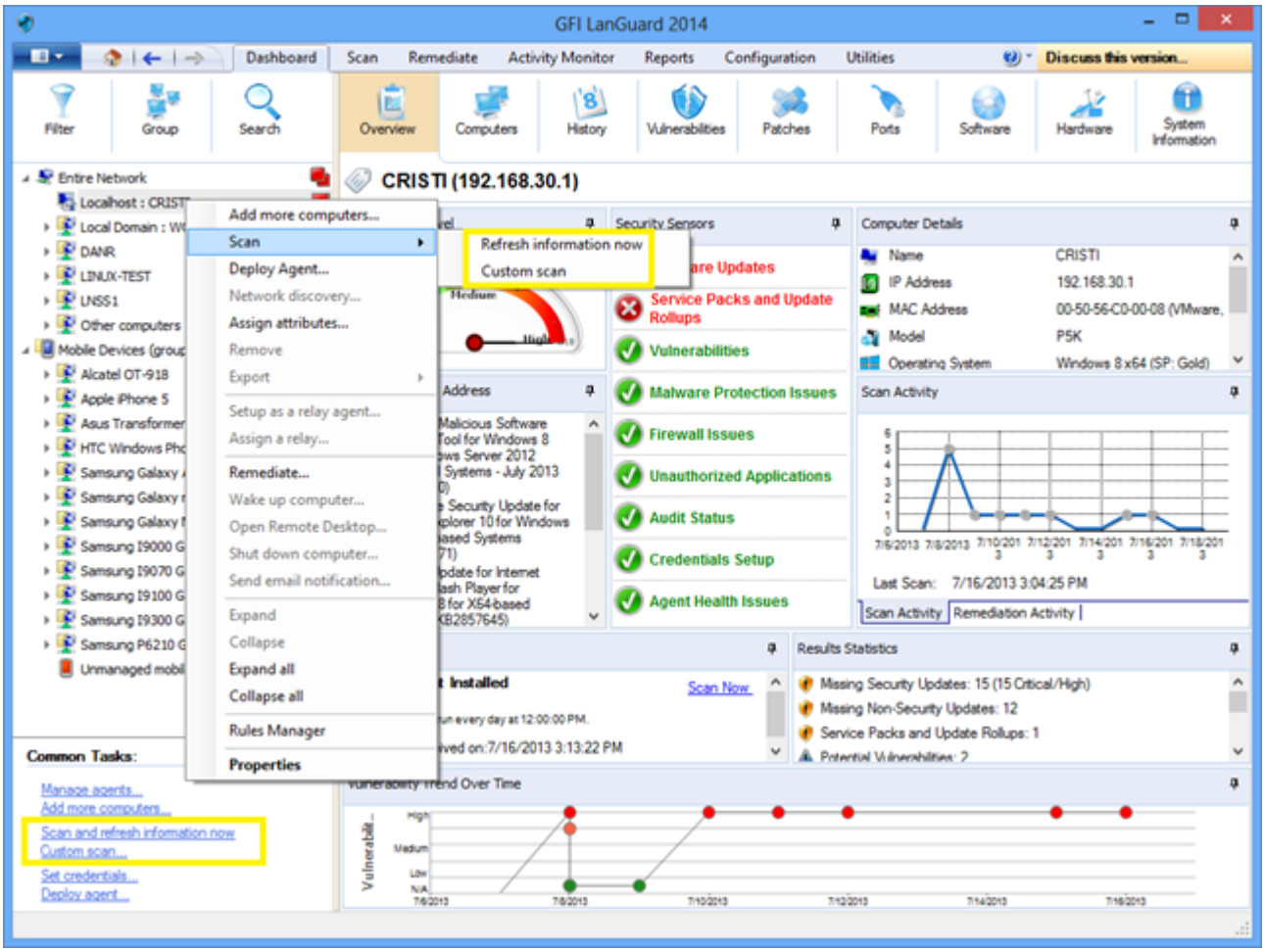
From **Configuration** select **Scanning Profiles**.



Screenshot 8: Scanning profiles

2.5 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.



Screenshot 9: Triggering scans from the dashboard

Feature	Description
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**.

3 Analyze scan results

Topics in this section:

3.1 The Dashboard

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

The executive summary shows, amongst others, the most vulnerable computers, prominent security issues, vulnerability trends. Users can also drill down to specific computers and issues.

The computer tree on the left hand side shows an organized list of domains and organizational units and mobile devices grouped by users. On the right hand side, the Dashboard section provides you with a number of views 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.

- Overview,
- Computers, History,
- Vulnerabilities,
- Patches,
- Ports,
- Software,
- Hardware,
- System Information.

Screenshot 10: The Dashboard

Section	Description
1	This section provides information about: » Filtering devices from the tree by a large number of criteria, including operating system, vulnerability level, last scan time, etc. » Grouping computers by domains and organizational units, operating systems or other custom defined attributes. Mobile devices can be grouped by user, operating system or device model. » Searching for devices by name or look for scan results containing specific keywords
2	This section provides information about how area to view and manage devices scanned and protected by GFI LanGuard: » Servers and workstations are listed under **Entire Network** node, as well as virtual machines and IP based network devices such as routers, switches, printers, etc. » Smartphones and tablets that connect to the Microsoft Exchanger servers of the company to check work email are listed under **Mobile Devices** node » The icon on the right side of the tree indicates the vulnerability level or if an audit is in progress » Computers having blue text are virtual machines » Use **<CTRL> + click** to select multiple computers
3	This section allows the user to trigger actions for the devices selected in the tree.
4	This section allows the user to select different views with statistics and scan results for the devices selected in the tree.
5	This section allows the user to view current selection of devices.
6	This section provides information about viewing statistics and scan results details for the devices selected in the tree: » Security sensors indicate how many devices are affected by different security issues » Click on the security sensors or the charts from Dashboard Overview area to drill down to more specific data

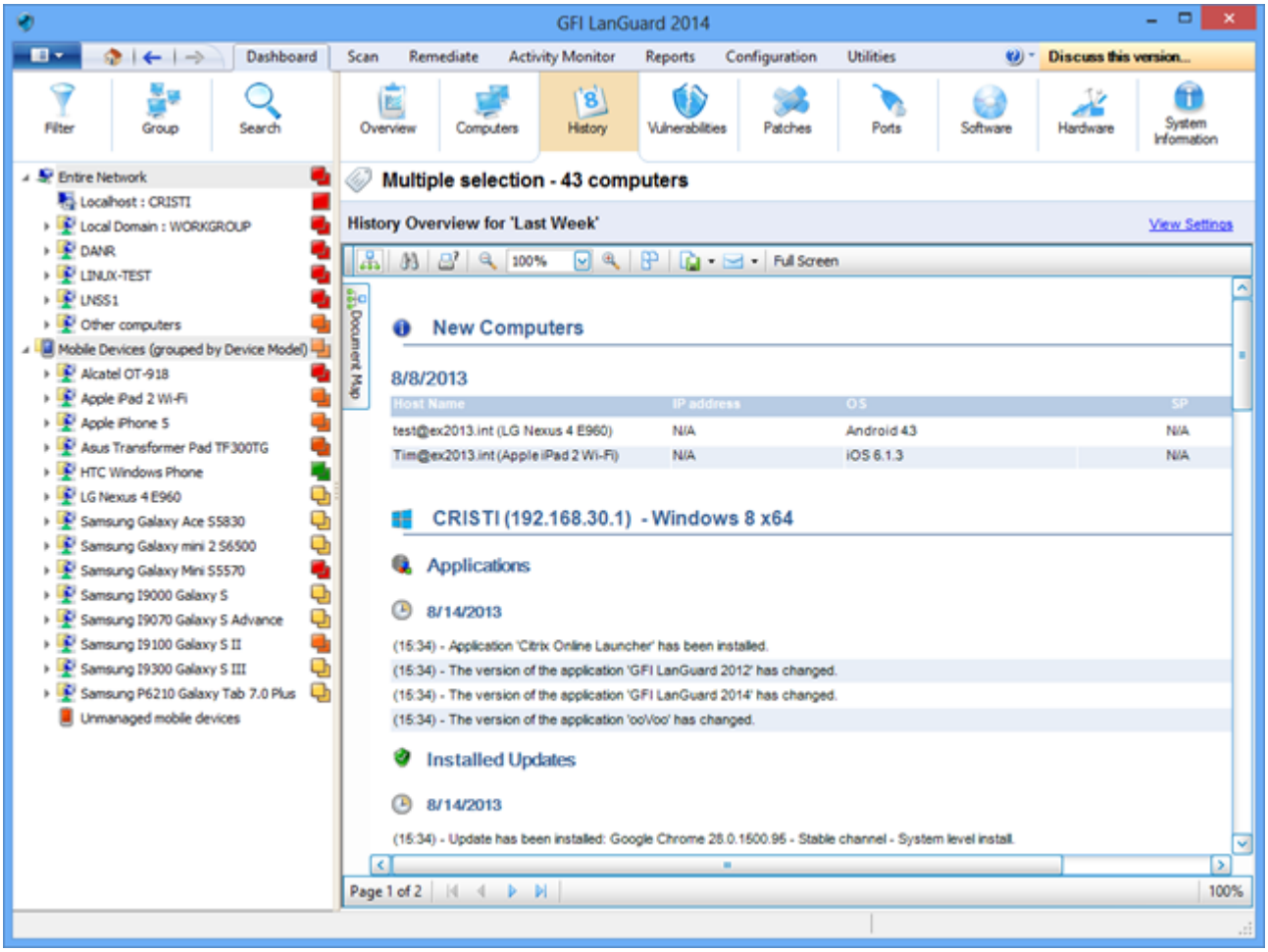
3.2 How to view relevant security changes from your network

GFI LanGuard notifies the user when:

- New devices are discovered
- New security vulnerabilities are detected
- Applications are installed or removed
- Services are started or stopped
- New ports are opened
- New shares are created
- New users are created
- Hardware changes are detected

To inspect relevant security changes from your network:

1. Click **Dashboard > History**.



Screenshot 11: Viewing security changes from your network

NOTE

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

3.3 How to add/view more devices in the Dashboard

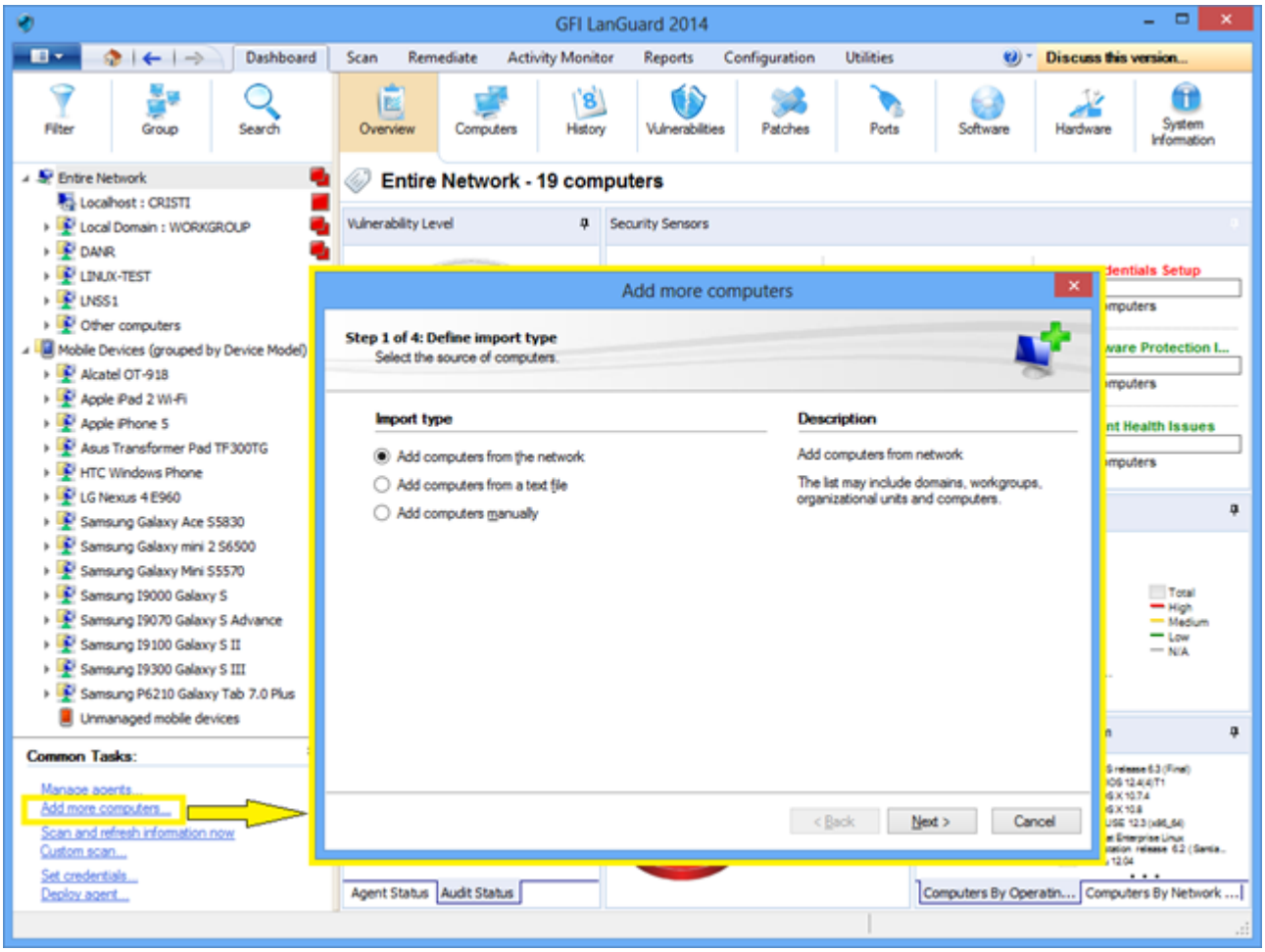
Unless filtered, the Dashboard tree shows all devices managed by GFI LanGuard. This means that all devices were discovered or fully scanned by the product.

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

1. Scan the computers without agents by clicking the **Scan** tab, **Configuration > Scheduled Scans** or command line scans.

2. Enable agents on the computers by clicking **Configuration > Agents Management**.

3. From **Dashboard** click **Add more computers...** from the **Common Tasks** area to add entire domains/workgroups and organizational units or a list of specific computers.

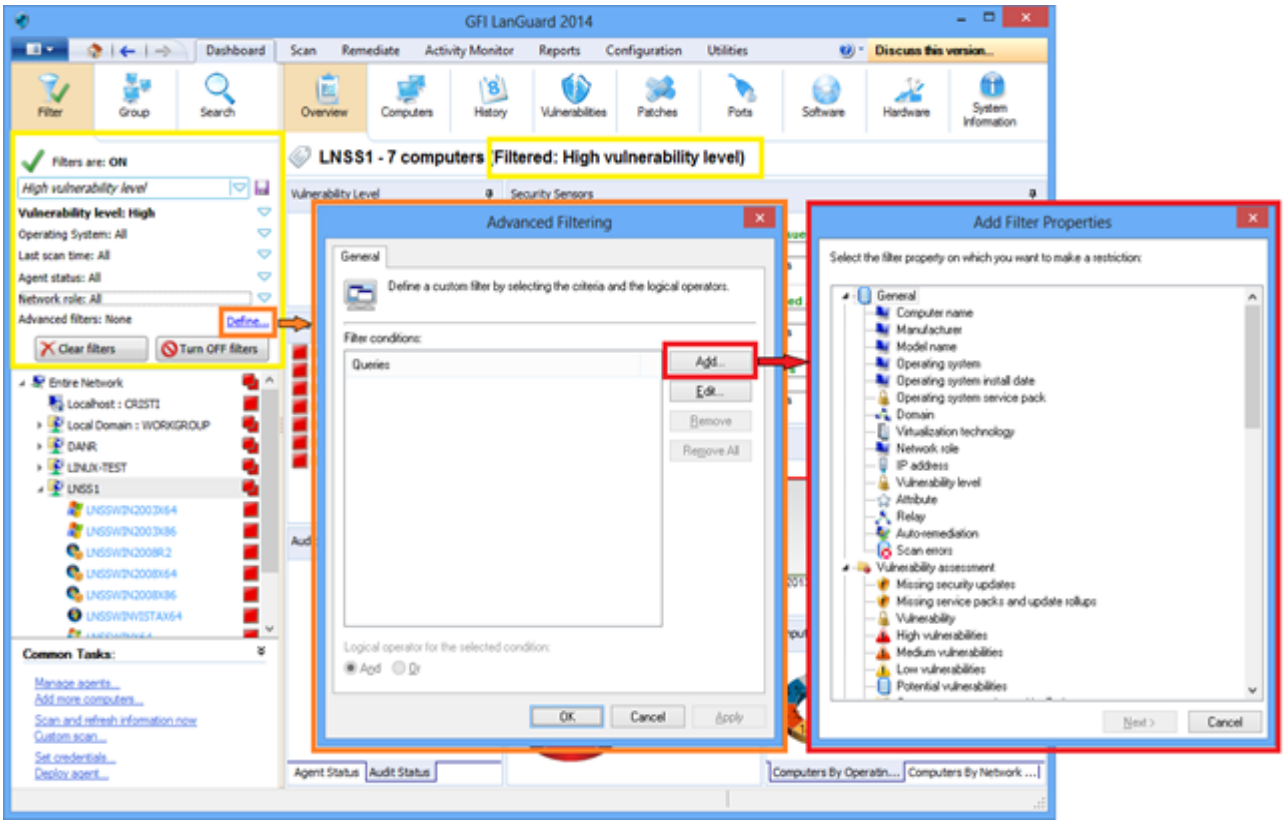


Screenshot 12: Adding and viewing computers from the dashboard

To audit smartphones and tablets use **Configuration > Mobile Devices** to add or edit mobile device management sources (provide details on Microsoft Exchange servers).

3.4 How to filter devices

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

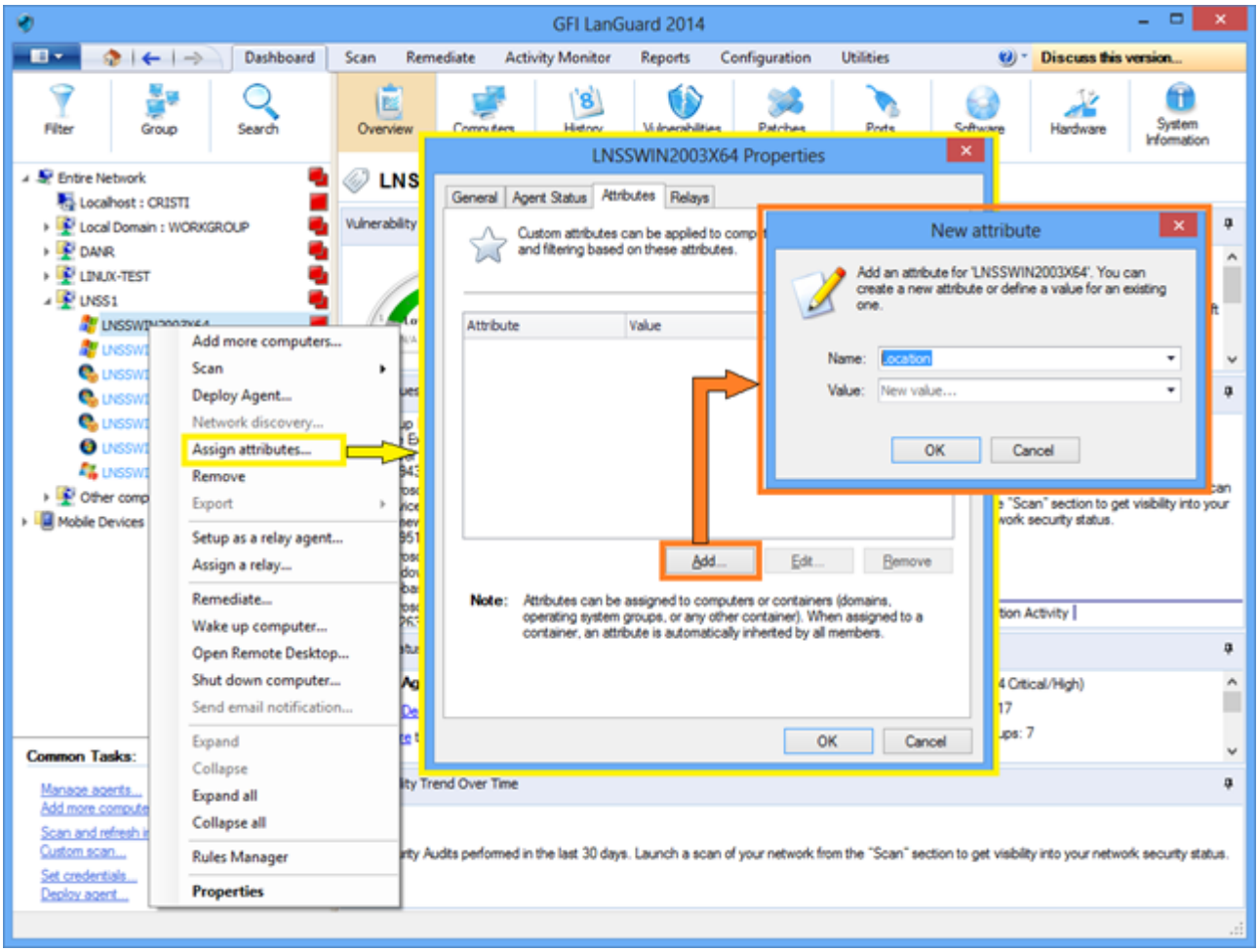


Screenshot 13: Filtering computers

3.5 How to group devices

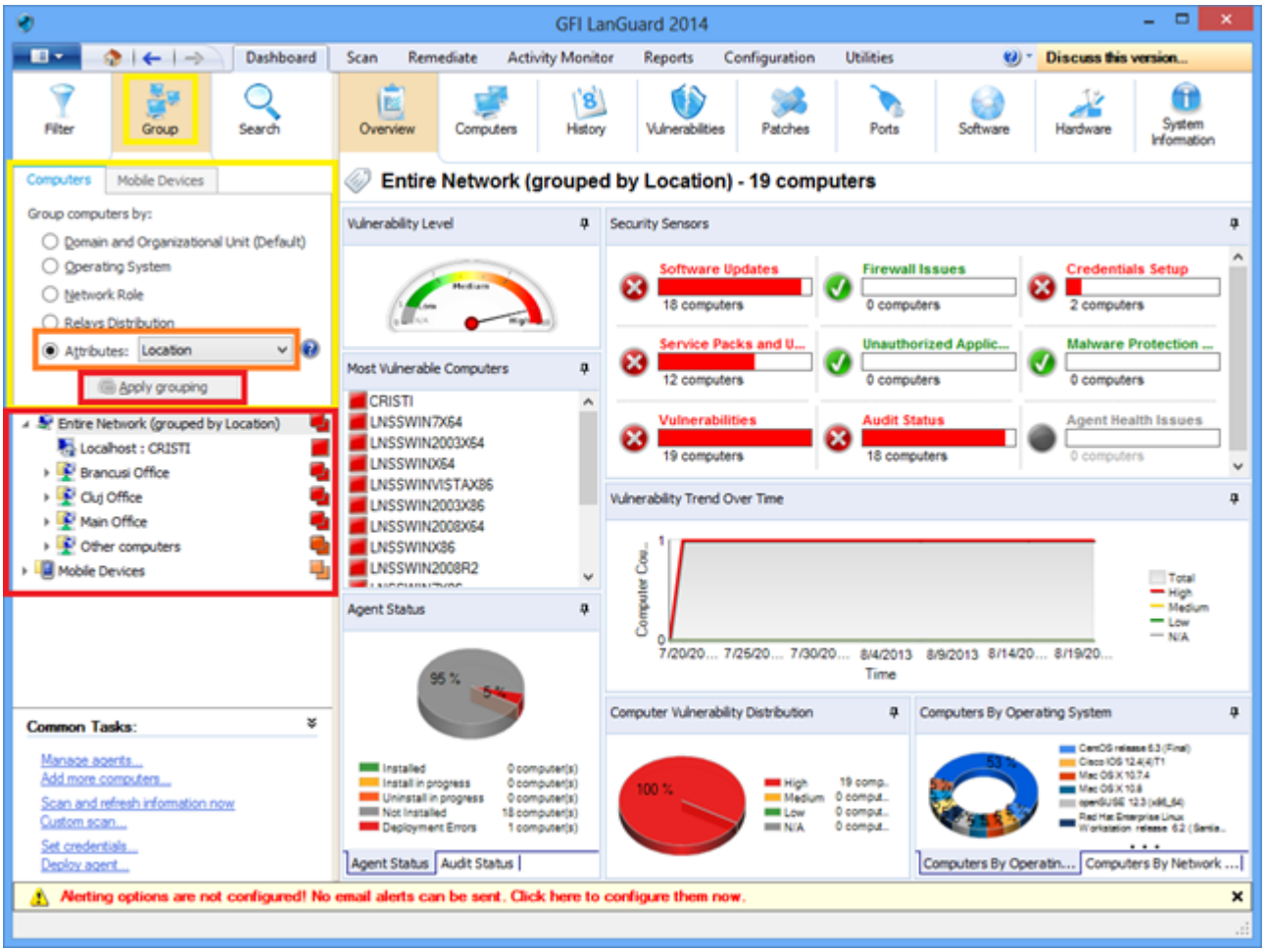
Computers from the tree can be grouped by predefined criteria like domains and organizational units (default grouping), operating system, network role, relays distribution or custom attributes defined by the users. Mobile devices can be grouped by user (default grouping), operating system, device model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

3.5.1 Defining custom attributes



Screenshot 14: Defining custom attributes

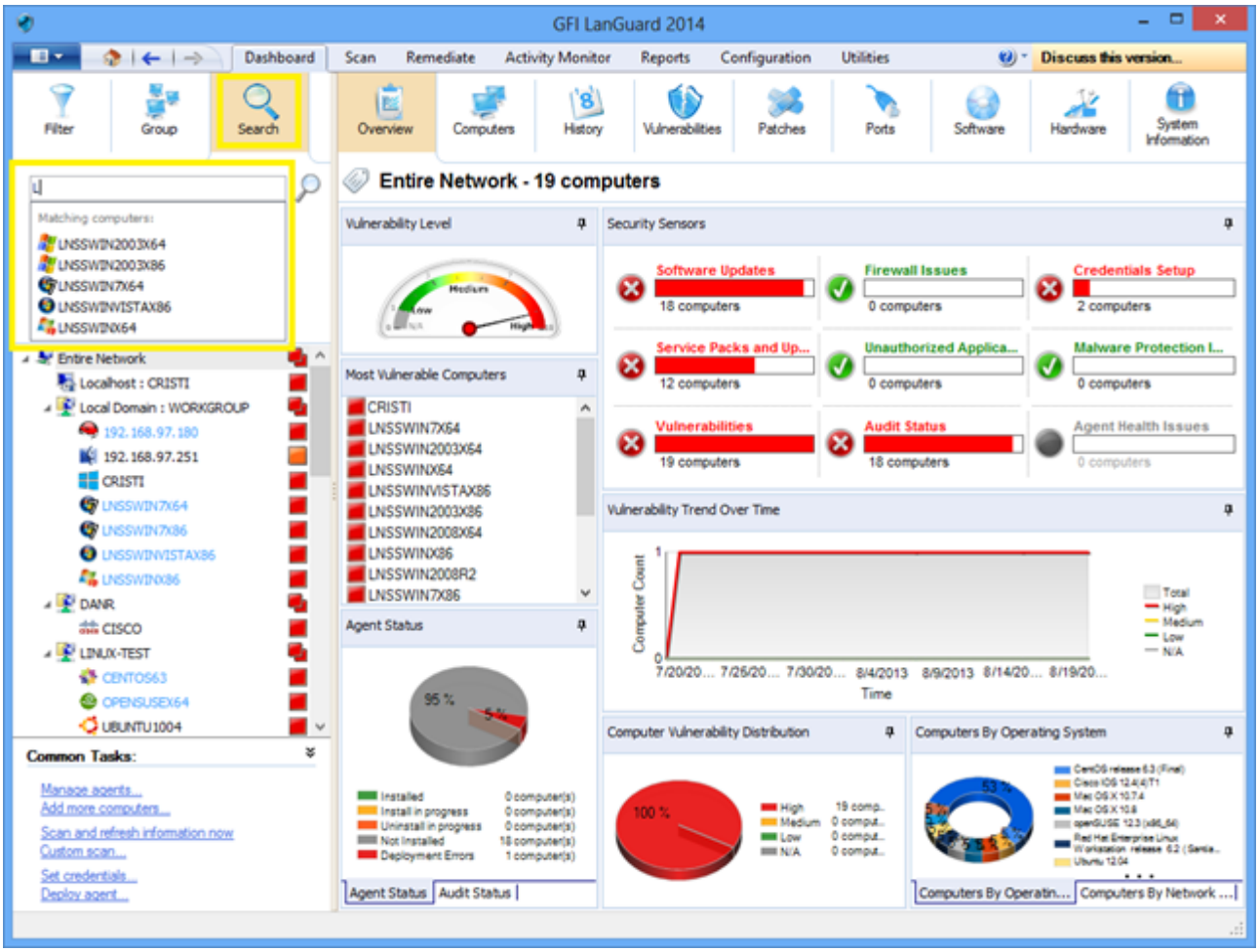
3.5.2 View computers by defined attributes



Screenshot 15: Viewing computers by defined attributes

3.6 How to search for computers

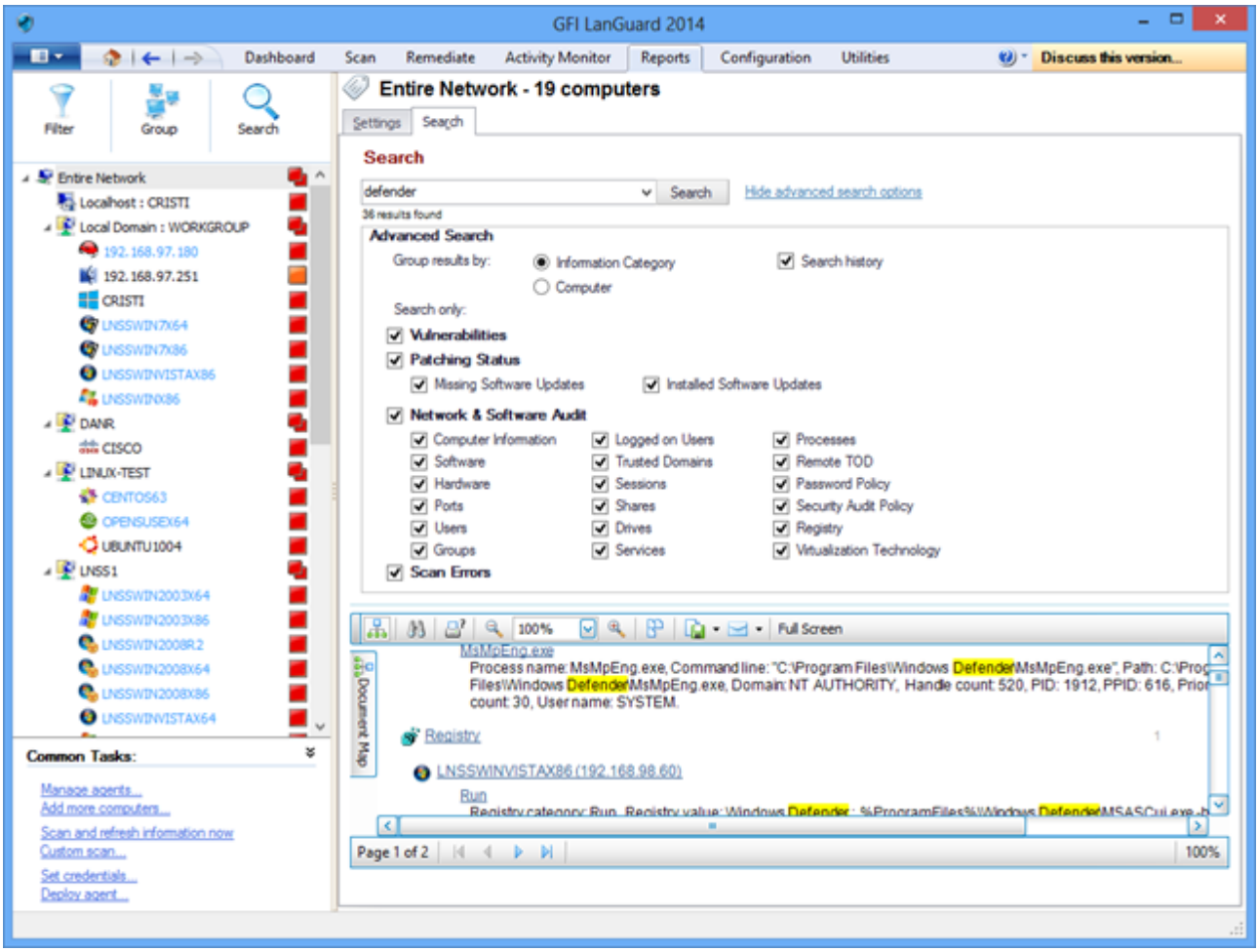
If a large number of devices are managed, finding them in the tree might be time consuming. Use the search area available in **Dashboard, Remediate** and **Reports** views to instantly locate devices.



Screenshot 16: Searching for computers

3.7 Full text search

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



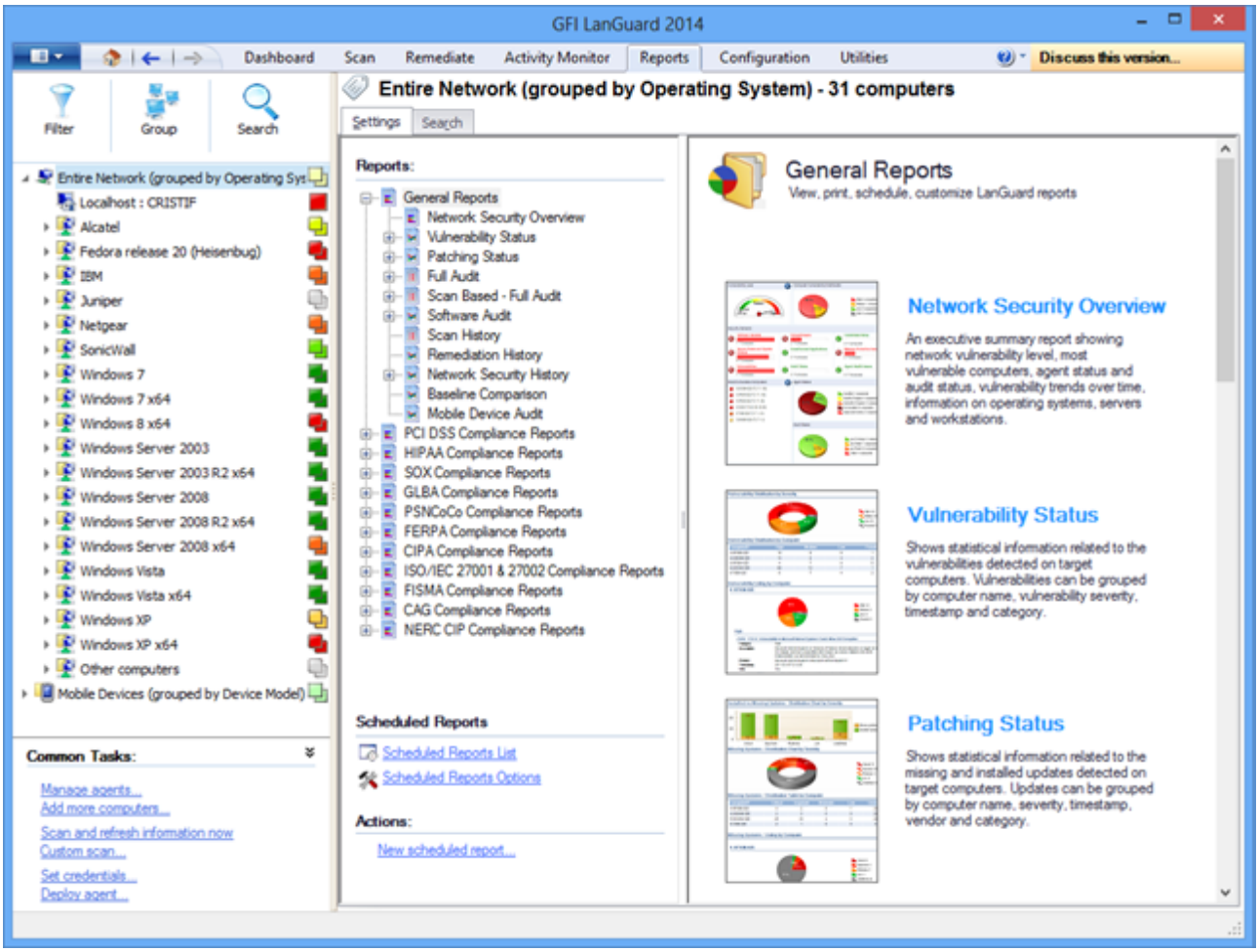
Screenshot 17: Full text searching

Search results can be grouped by a particular category. It is also possible to exclude results found in other categories.

3.8 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 amongst which PDF, HTML, RTF, XLS.

In addition,GFI LanGuard ships with a large set of reports dedicated to compliance with various standards and laws, amongst which PCI DSS, HIPAA, SOX, GLBA, PSN CoCo.



Screenshot 18: Reporting

4 Remediate security issues

Topics in this section:

4.1 Deploy missing software updates

To deploy missing security and non-security updates:

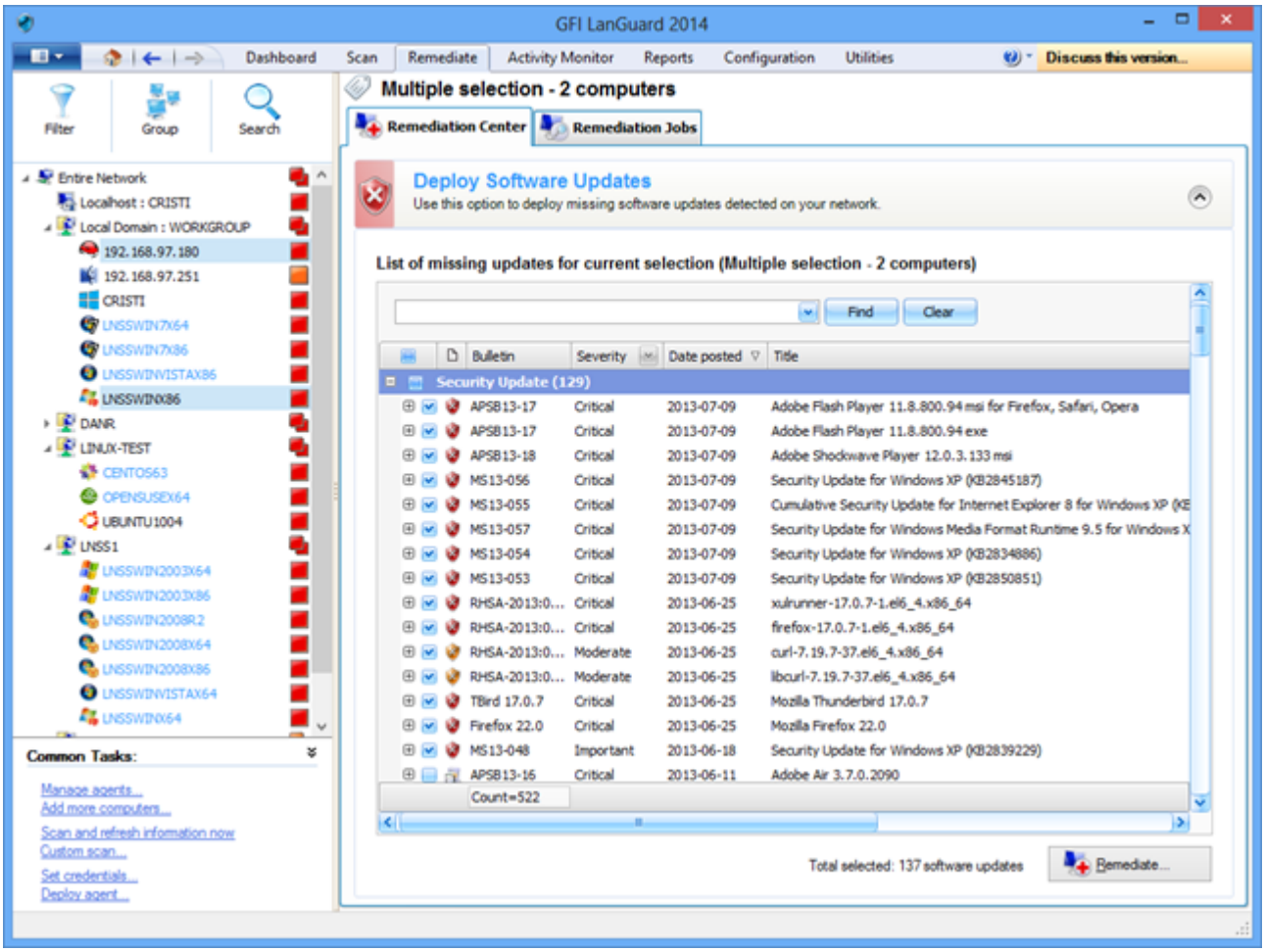
1. Click **Remediate > Remediation Center > Deploy Software Updates**

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

NOTE

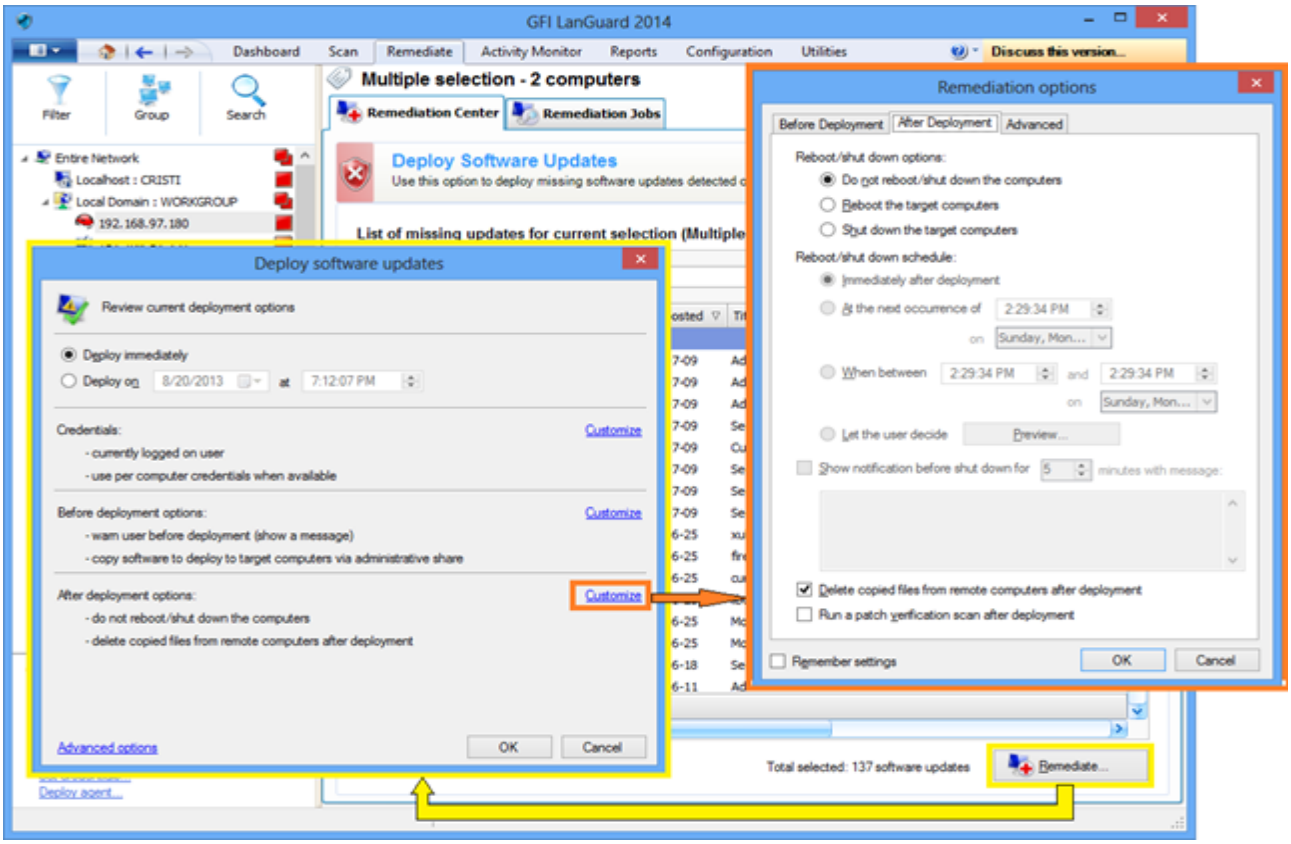
» Multiple items can be selected in the computers tree using **<CTRL> + click**.

» To locate computers more easily in large networks, computers from the tree can be filtered by a large number of criteria. For more information, refer to How to filter devices (page 24).



Screenshot 19: Deploying software updates

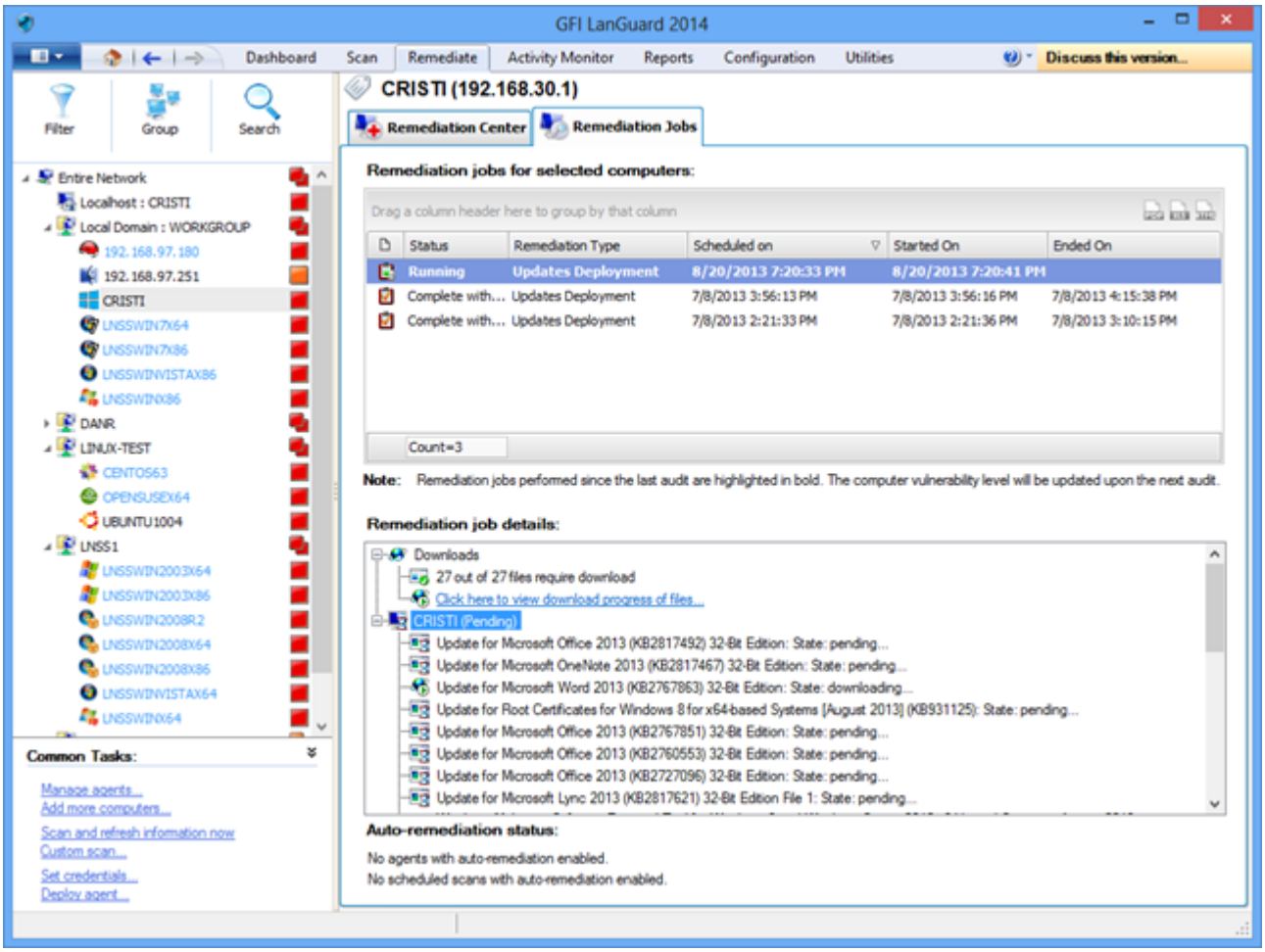
In the **Deploy Software Updates** screen you can see all missing updates for the selected computers with details for each update on which of the selected computers is missing. It is possible to fine tune the deployment by selecting or deselecting patches or computers.



Screenshot 20: Remediation options

To start the deployment operation:

1. From **Remediate** select **Remediation Jobs**.
2. From the **Deployment software options** wizard set up deployment schedule
3. From the **Remediation options** wizard select the reboot options and click **OK**.



Screenshot 21: Machines rescan

4. Rescan the machines to get their security status after the deployment was done.

NOTE

- 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.

NOTE

GFI LanGuard can be configured to automatically deploy missing updates. For more information, refer to Automate remediation operations (page 45).

4.2 Uninstall unauthorized applications

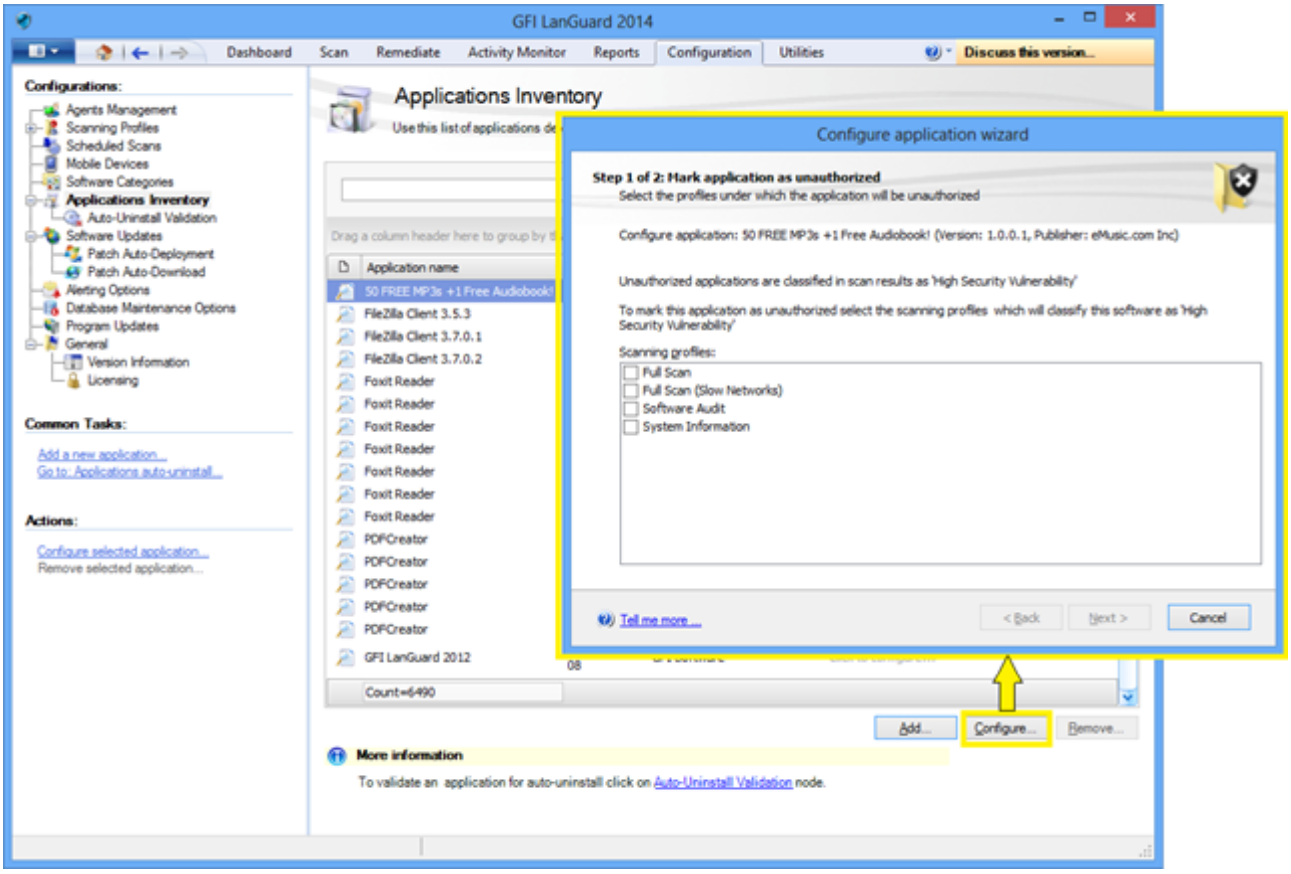
Perform a full audit or a software audit on the network to get an inventory of installed applications. For more information, refer to Perform security scans (page 11).

NOTE

It is possible to add unauthorized applications even if they are not detected as installed in the network by using the "**Add...**" button.

To mark unauthorized applications :

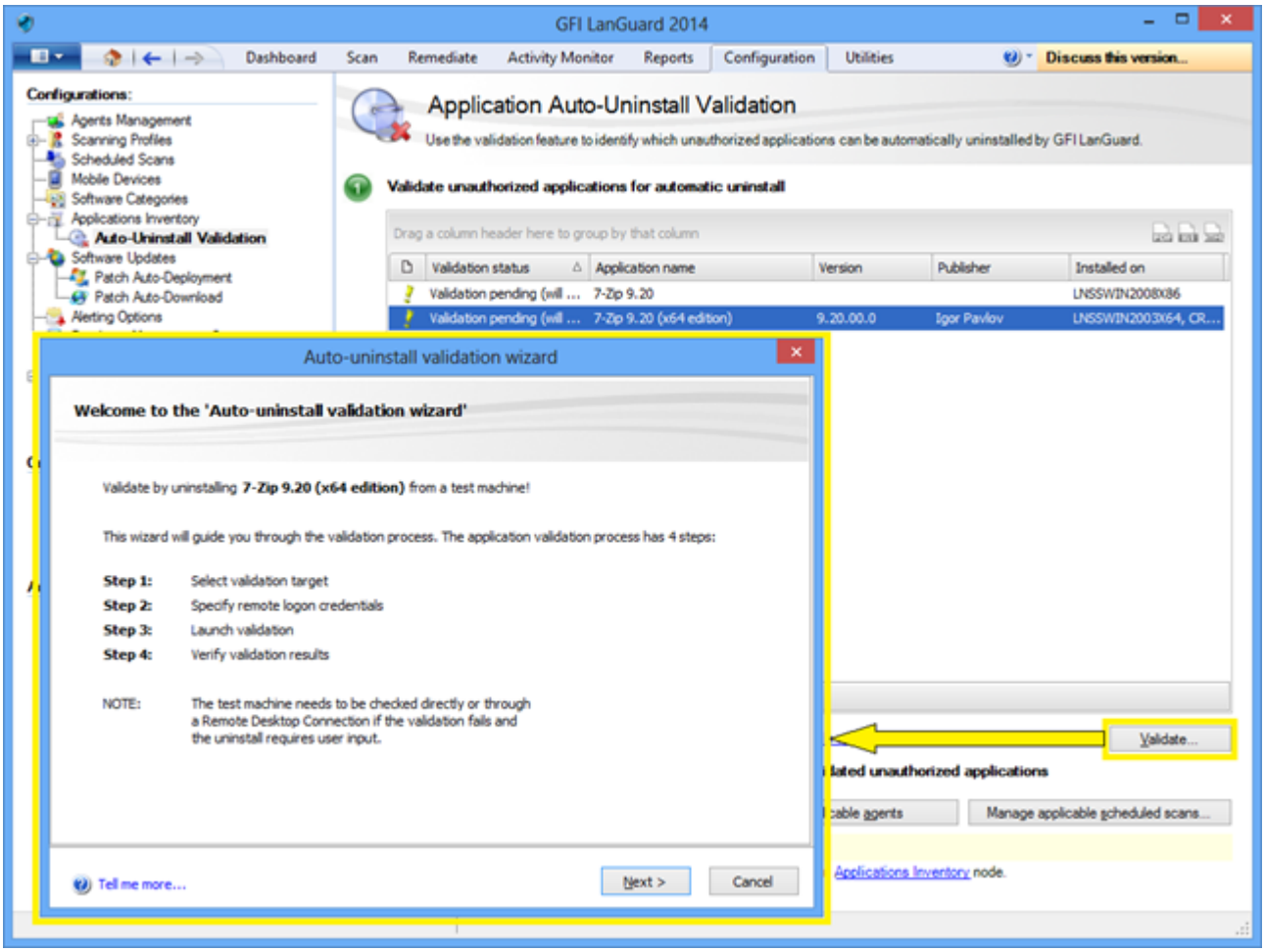
1. Click **Configuration > Applications Inventory.**



Screenshot 22: Marking unauthorized applications

2. Use **Configuration > Auto-Uninstall Validation** to test if GFI LanGuard is able to successfully uninstall an unauthorized application silently.

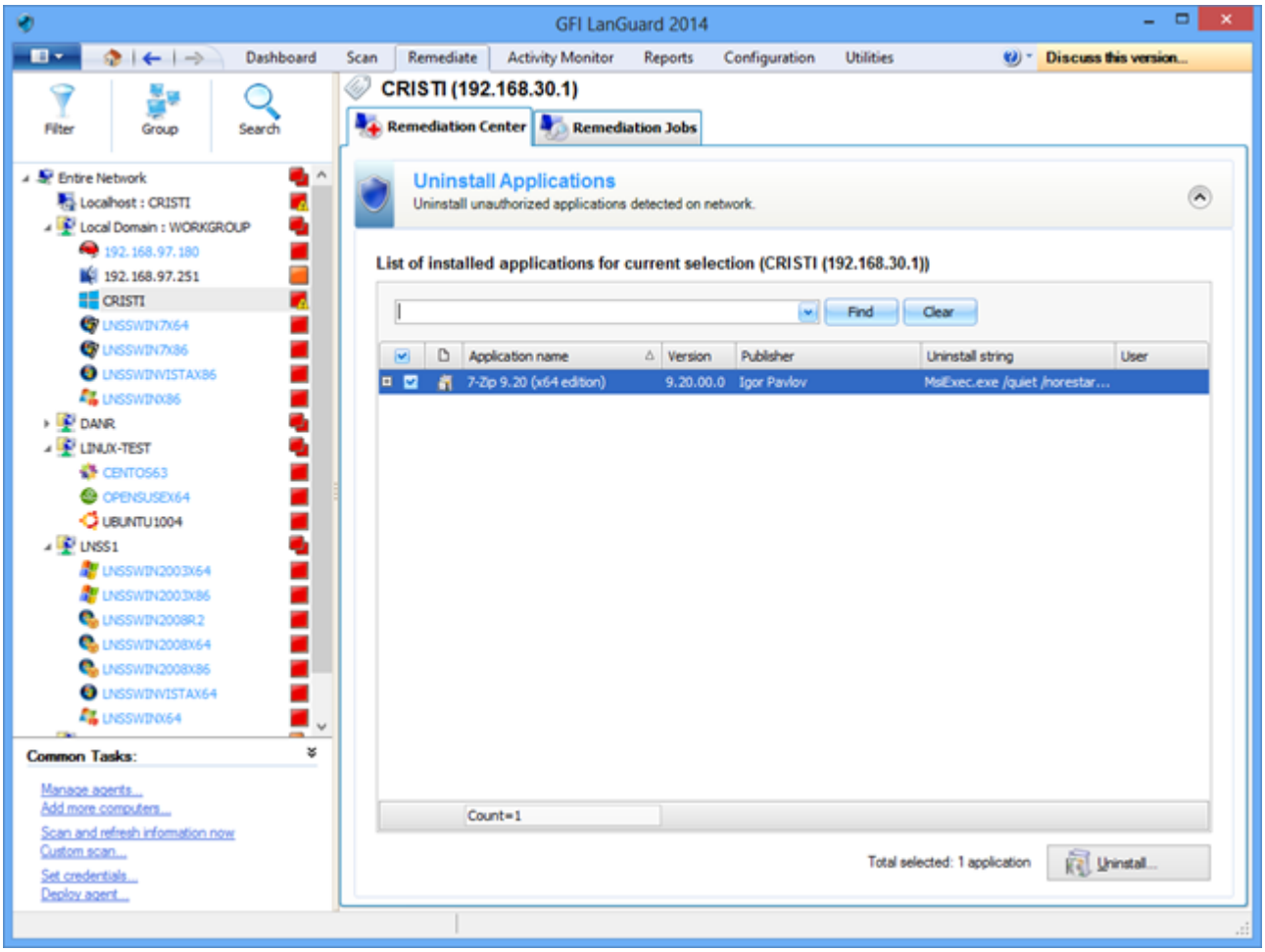
> **NOTE**
> Some applications do not support silent uninstall and they cannot be removed by GFI LanGuard because the uninstall process will show dialogs to the end users of the target machines, waiting for their input and interfering with their work.



Screenshot 23: Application auto-uninstall validation

3. Rescan your network again to detect all unauthorized applications.

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



Screenshot 24: Uninstalling applications

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

> **NOTE**
> GFI LanGuard can be configured to automatically detect and remove any unauthorized application from your network. For more information, refer to Automate remediation operations (page 45).

4.3 Deploy custom software

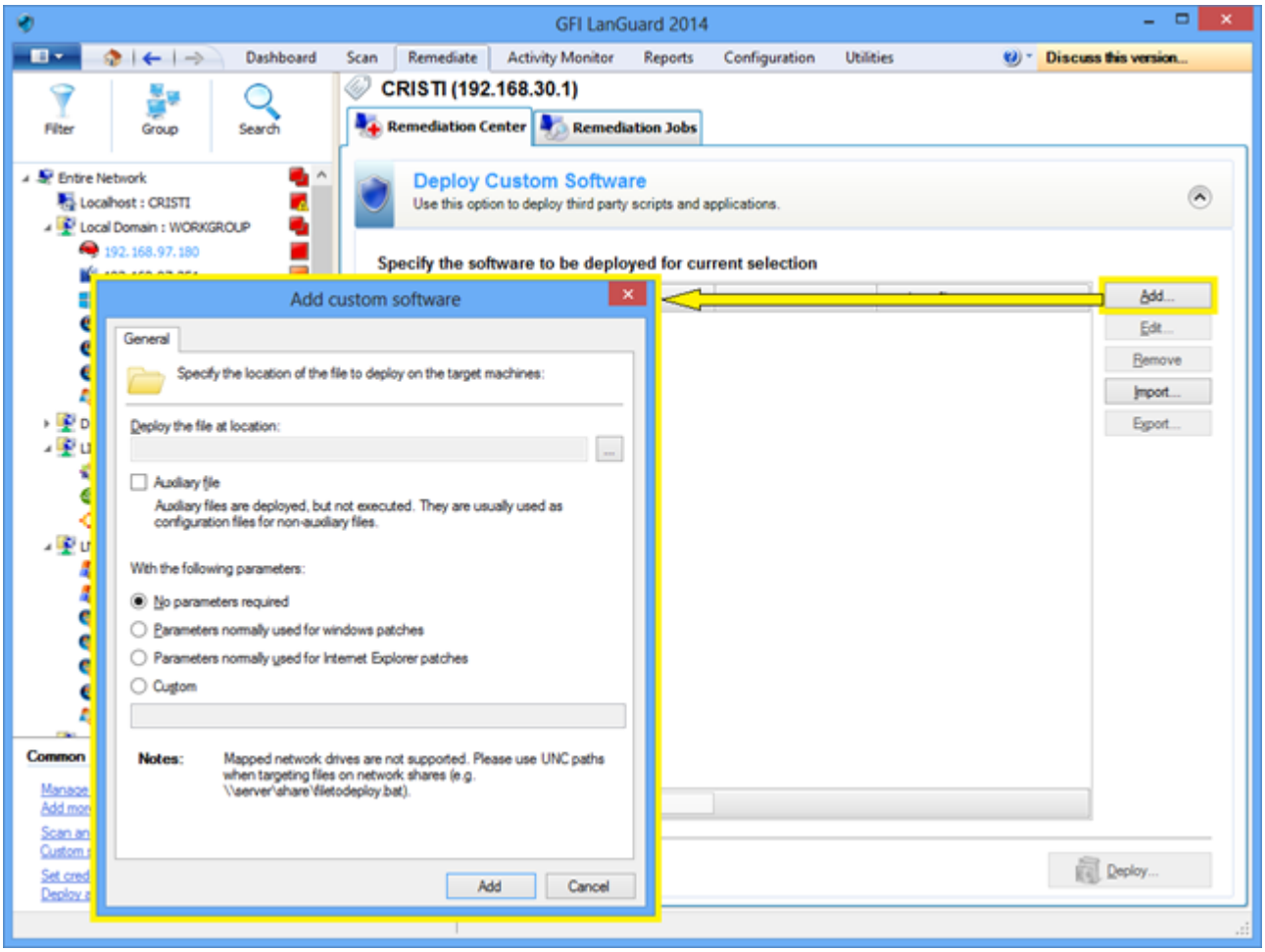
GFI LanGuard can deploy custom software and scripts network wide. Practically any piece of software that can run silently can be deployed using GFI LanGuard.

To deploy custom software and scripts to your network:

1. Click **Remediate > Remediation Center > Deploy Custom Software**

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

> **NOTE**
> Custom software must be specified manually, together with parameters for silent installation and configuration files, if necessary.

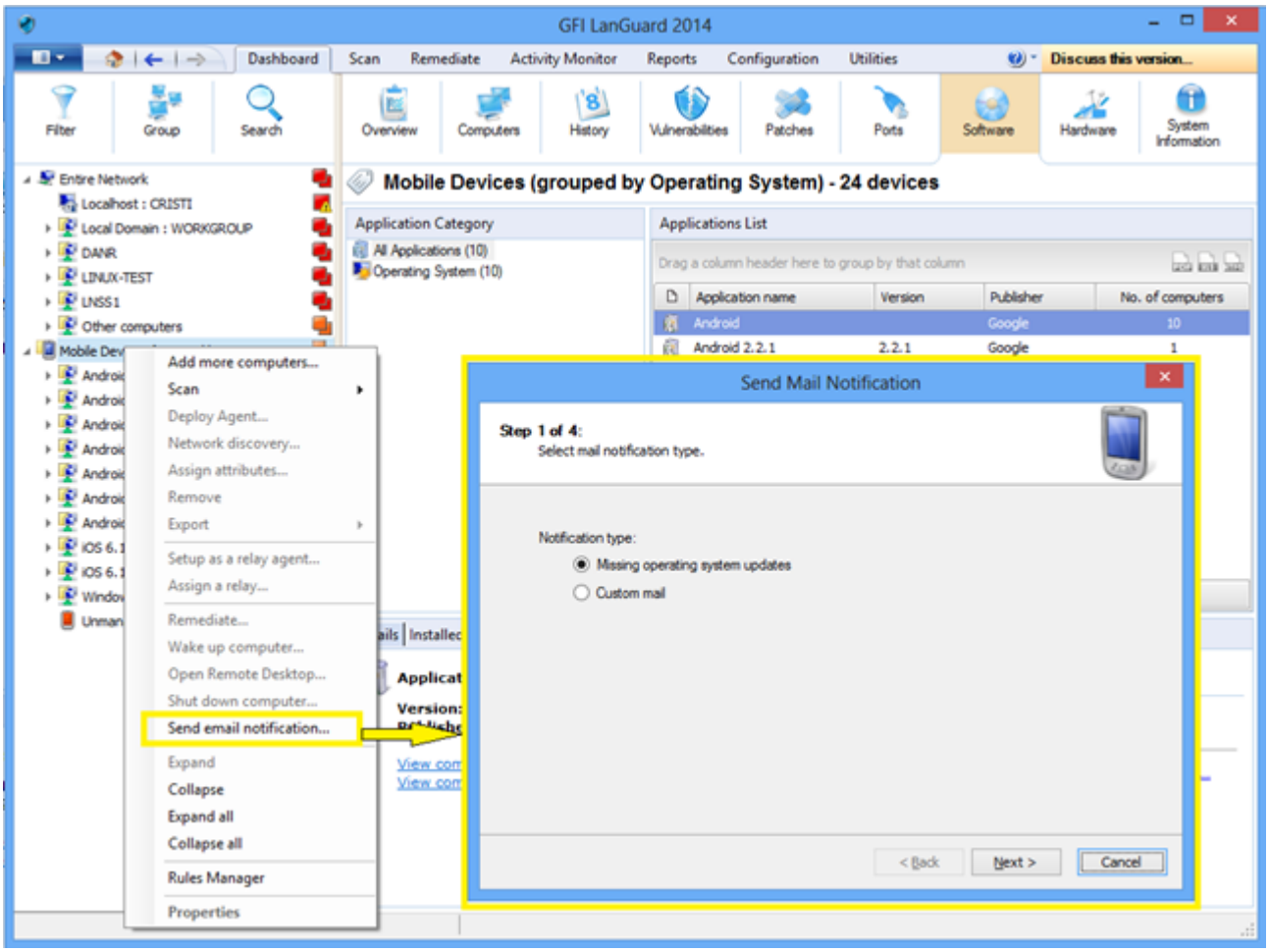


Screenshot 25: Deploying custom software

4.4 Send email notifications to mobile device owners

IT administrators can use GFI LanGuard to send custom email notifications to owners of smartphones and tablets that connect to the company's services such as Microsoft Exchange, Office 365, Google Apps and Apple Profiles Manager. A predefined email template can be used to notify device owners of the latest updates for the operating system installed on their devices.

Right click on a mobile device or a group of mobile devices in the Dashboard tree and select **Send email notification** option to send email messages to mobile device owners.



Screenshot 26: Sending Email Notifications

4.5 Other remediation operations

To view all remediation operations available in GFI LanGuard:

1. From **Remediate** select **Remediation Center**

GFI LanGuard allows remediation operations like:

» Rollback patches – this option is very important when security updates that interfere with your business environment were installed

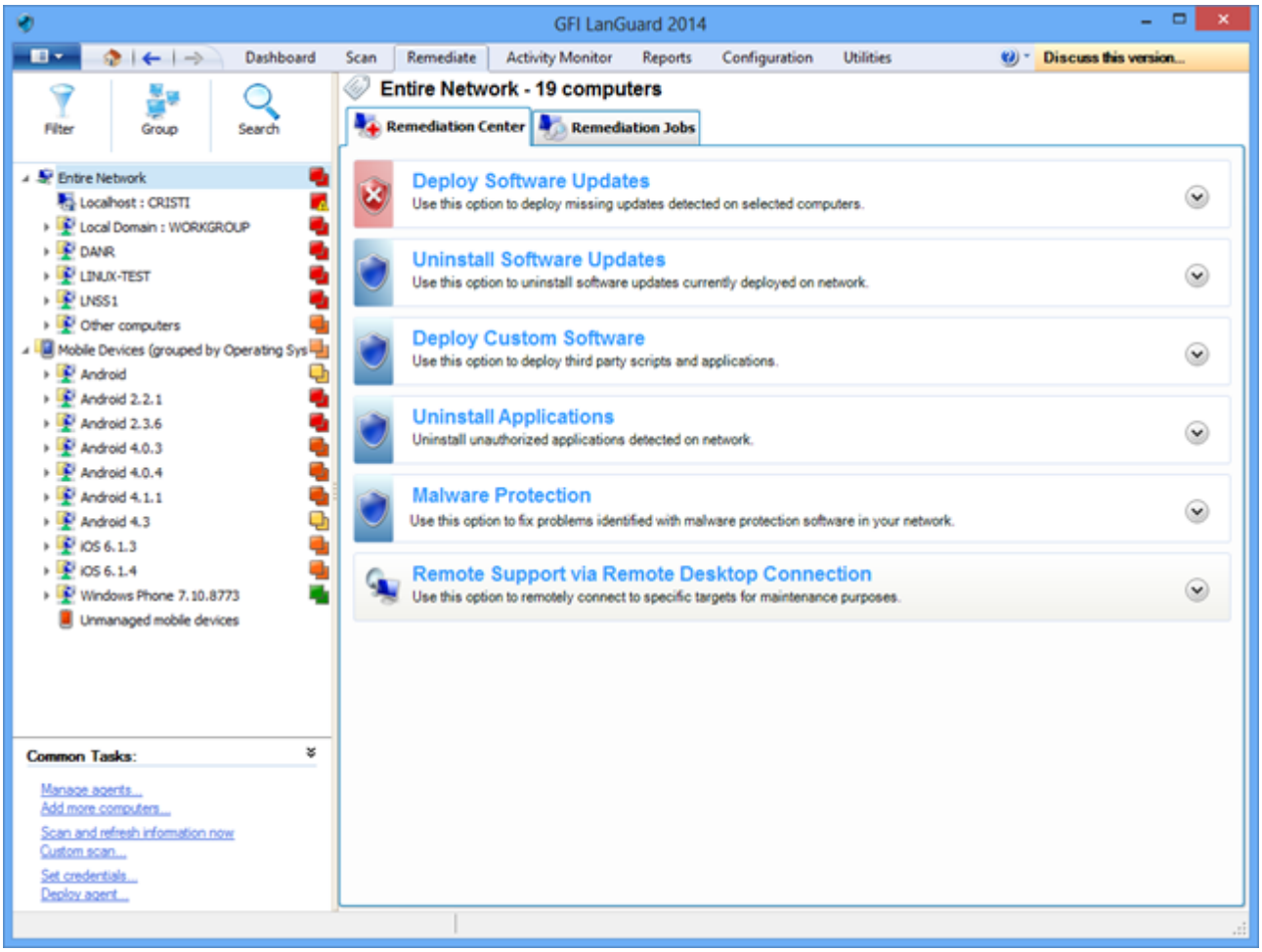
» Trigger definition updates for antivirus and antispyware software

» Trigger antivirus and antispyware scans on the remote machines

» Enable real time protection for antivirus and antispyware solutions

» Turn on firewalls

» Open a remote desktop connection on the target machines to quickly solve security issues that cannot be fixed automatically



Screenshot 27: Other remediation operations

5 Automate tasks

Topics in this section:

5.1 Automatically discover new devices in the network

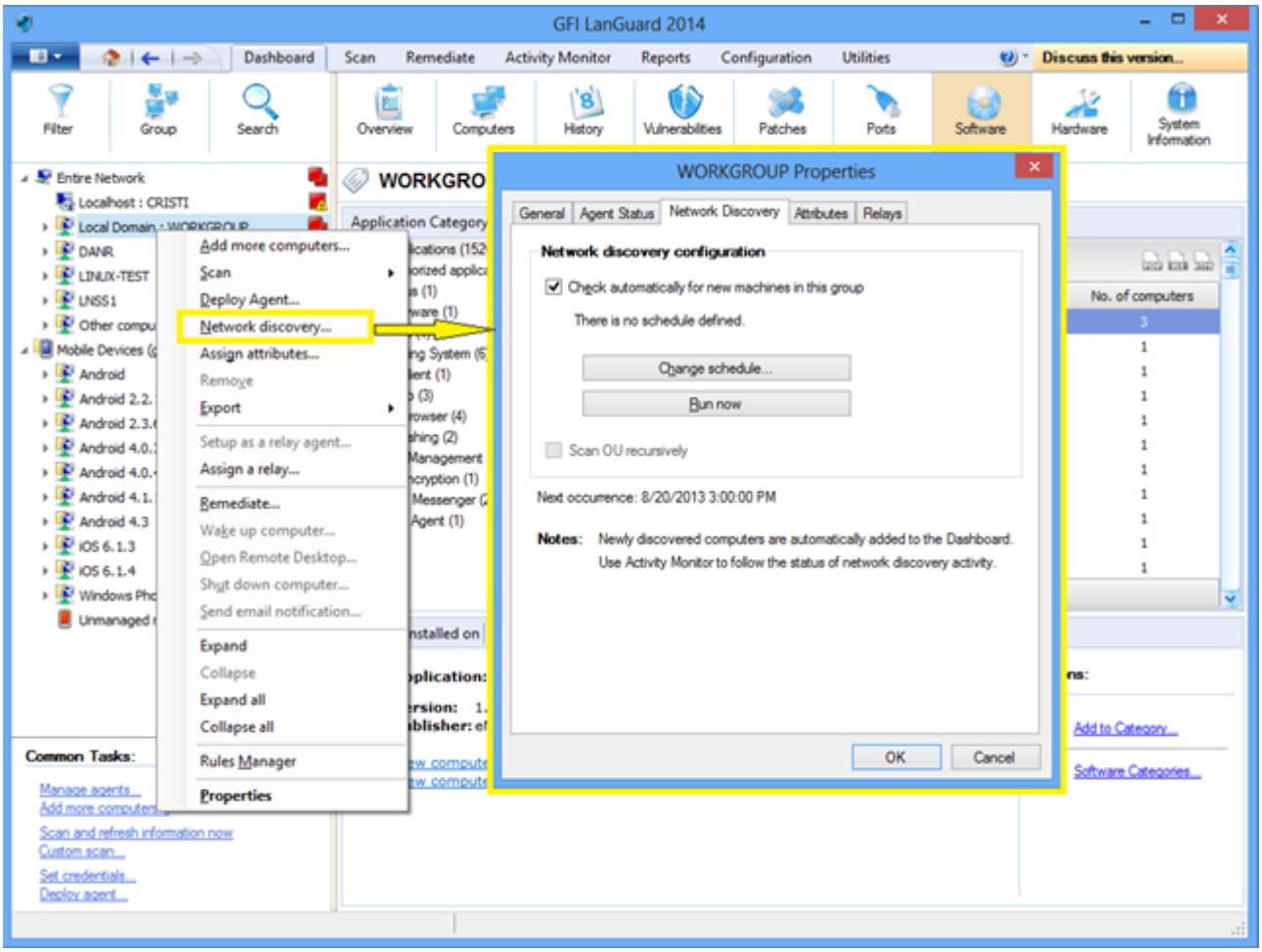
NOTE

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

» To monitor new devices that are live on the network, schedule a scan to run on regular basis under Network Discovery profile.

To automatically detect when new computers are added to a certain domain or organizational unit:

1. From **Dashboard**, right click on the domain or organizational unit in the computers tree and select **Network Discovery**…



Screenshot 28: Discovering devices

2. From **Dashboard** select **History** to investigate what new devices were detected in the network and when they were seen for the first time.

> **NOTE**
> New mobile devices are automatically detected on regular basis once a Mobile Device Management Source is defined. For more information see auditing smartphones and tablets section.

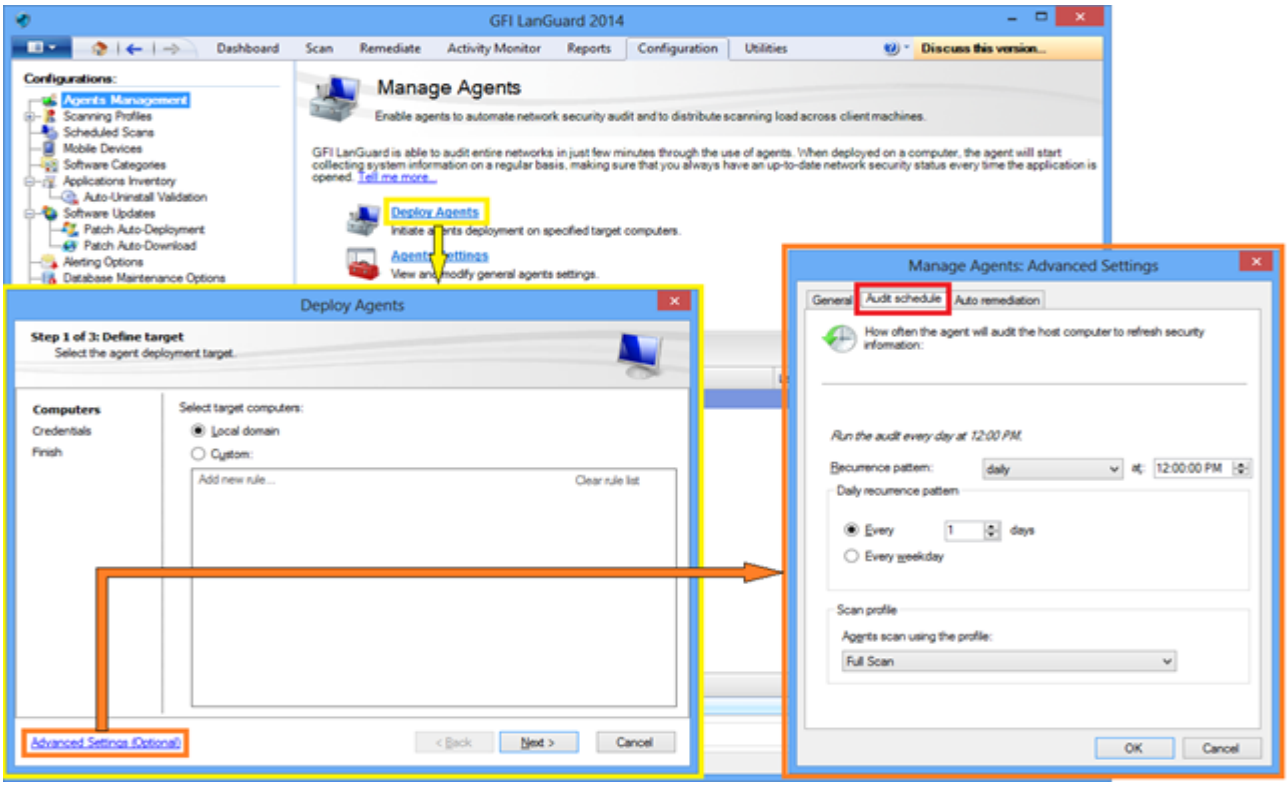
5.2 Automate security audits

Security audits can be automated in two ways:

1. Set agent-less scheduled scans to run in background on a regular basis

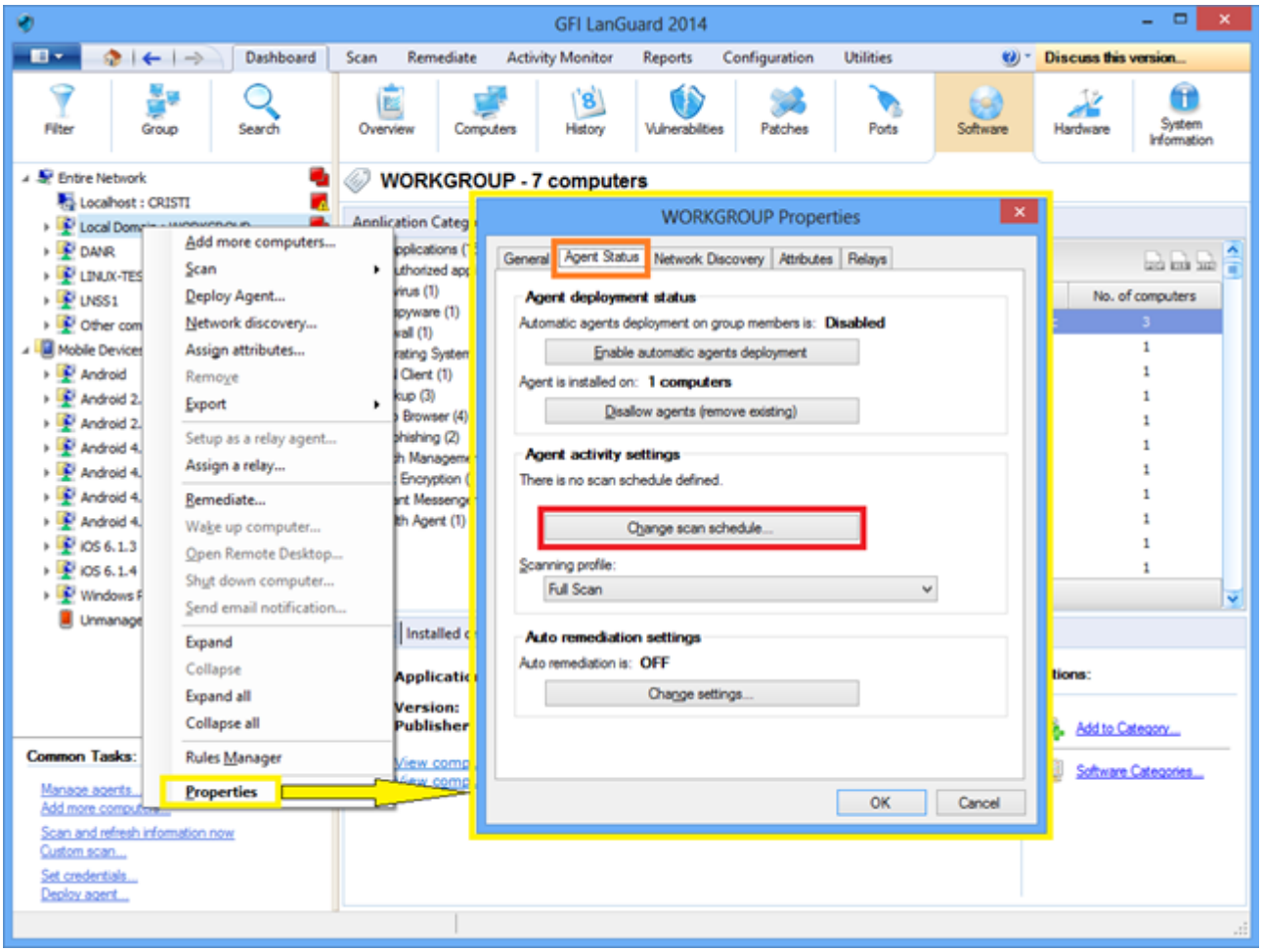
2. Deploy agents on the target machines. By default, agents audit the host machine once per day, but the audit schedule can be customized.

5.2.1 Customize audit schedule when deploying agents



Screenshot 29: Customizing audit schedule - Deploying agents

5.2.2 Customize audit schedule for agents using the Dashboard

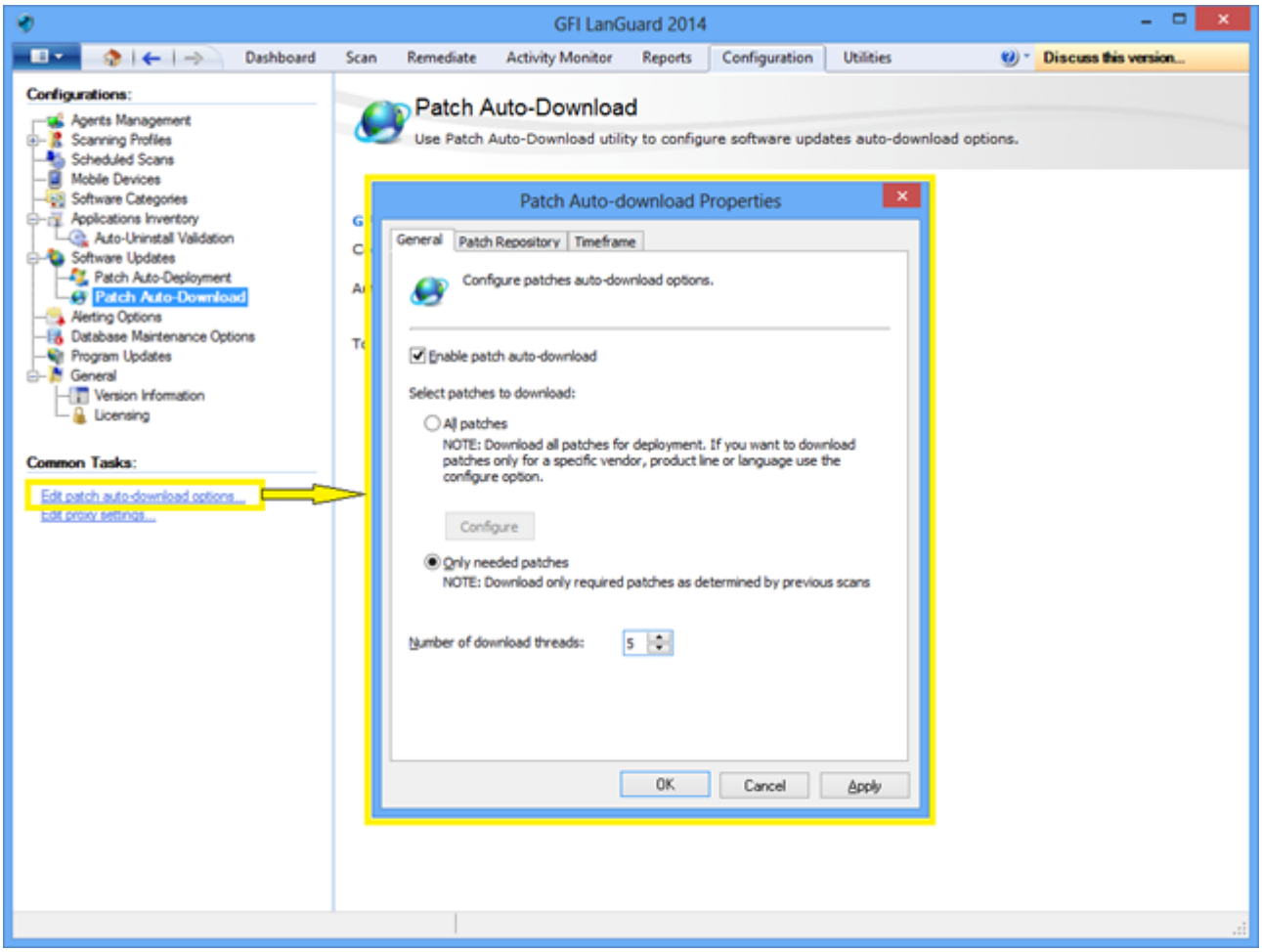


Screenshot 30: Customizing audit schedule - Using the dashboard

5.3 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. The options available are:

- Auto-download all patches
- Auto-download only patches detected as missing by GFI LanGuard
- Auto-download patches for specific vendors, products or languages.



Screenshot 31: Automating patch download

5.4 Automate remediation operations

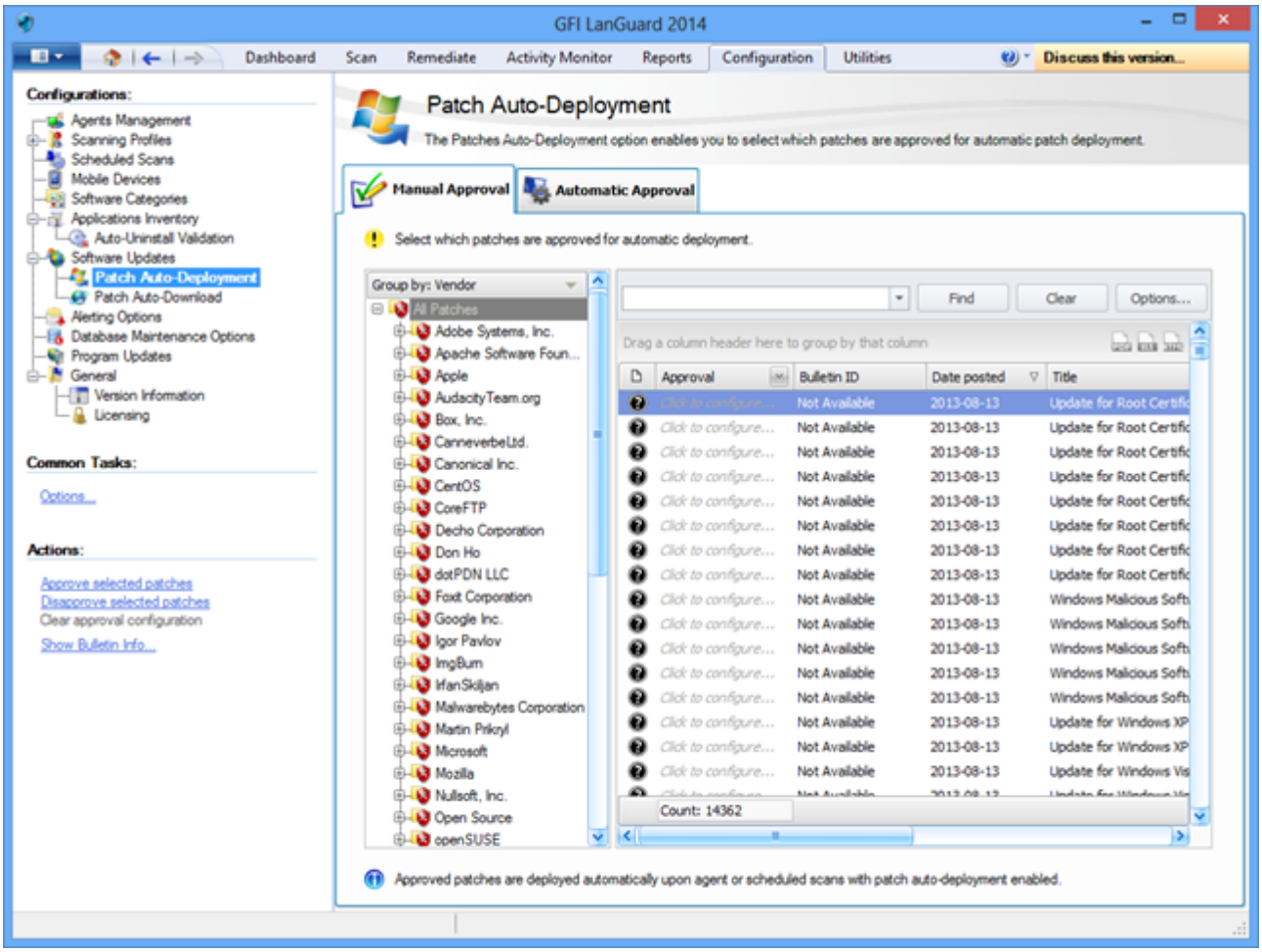
GFI LanGuard can be configured to automatically remediate certain security issues such as the deployment of updates and the uninstallation of unauthorized applications as these are detected by an agent-less scheduled scan or an agent based scan.

> **NOTE**
> Define unauthorized applications and approve security updates for auto deployment before continuing.

To approve security updates:

1. From **Configuration** select **Patch Auto-Deployment**.

2. Select the patches from the list.

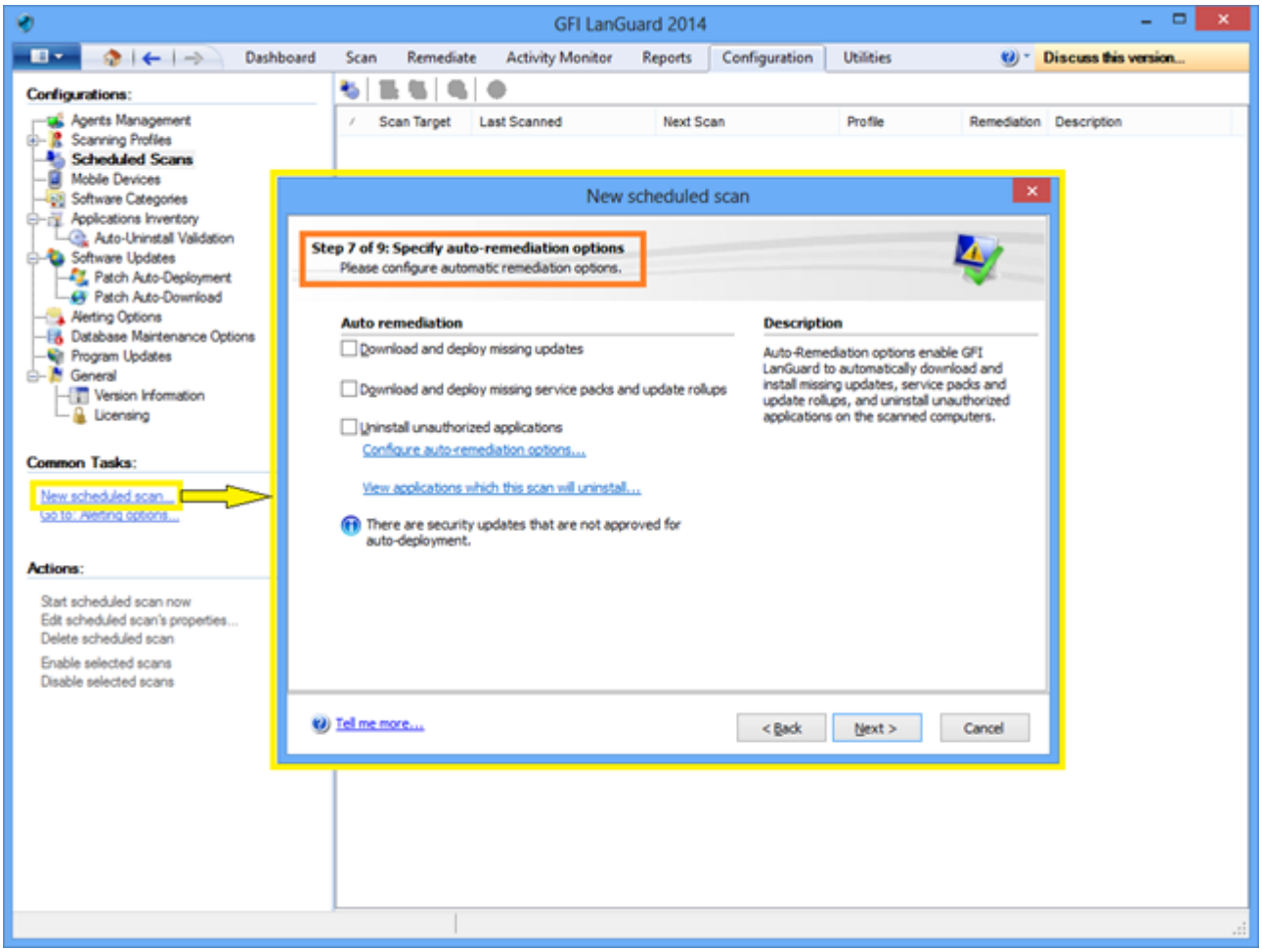


Screenshot 32: Approving security updates

To enable auto-remediation for a new agent-less scheduled scan:

1. From **Configuration > Scheduled scans > Common tasks** select **New scheduled scan**.

2. Select the auto-remediation configuration options from the wizard and click **Finish**.



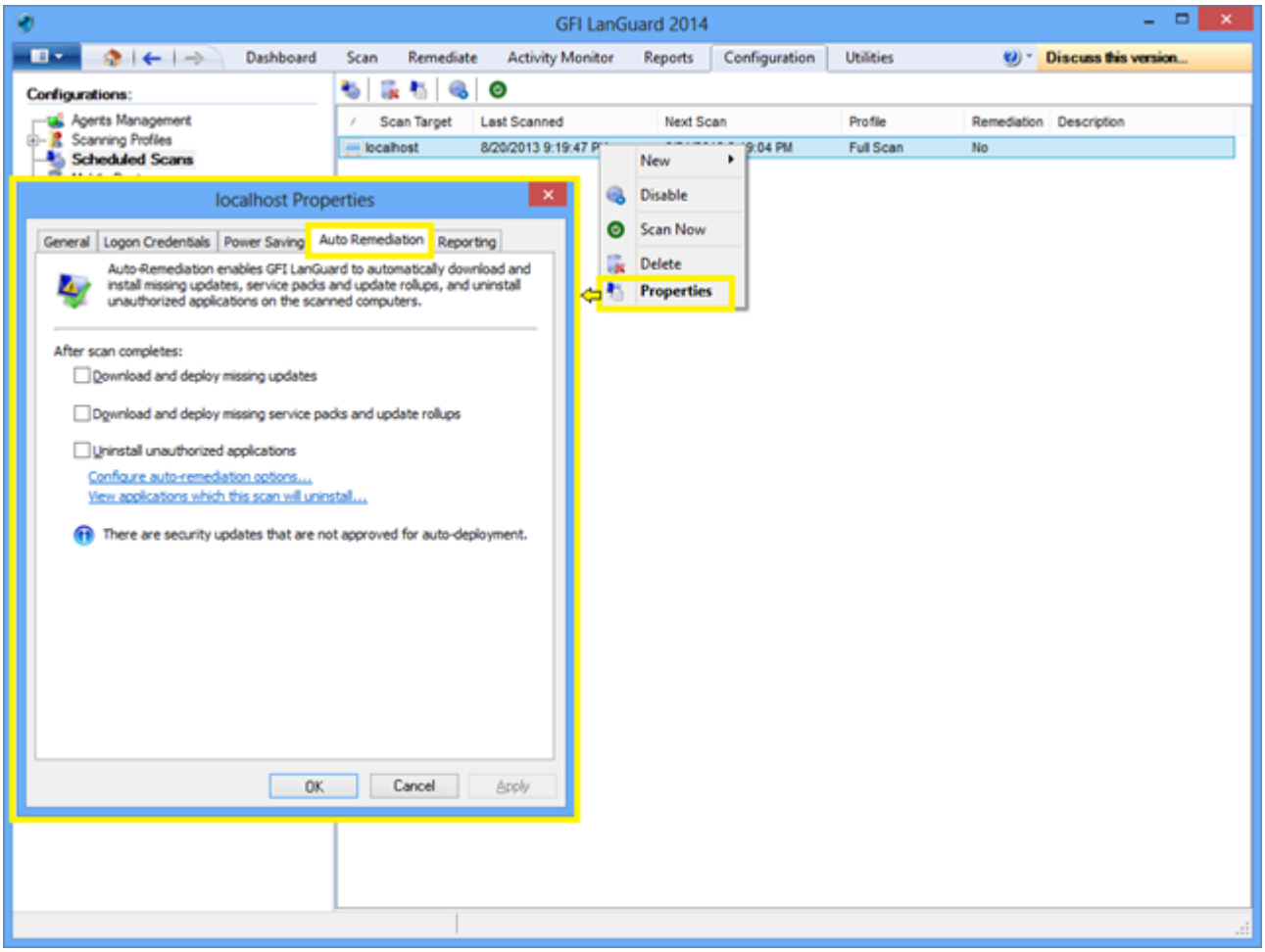
Screenshot 33: Enabling auto-remediation for new agent-less security scans

To enable auto-remediation for an existing agent-less scheduled scan:

1. From **Configuration > Scheduled scans** select the scan target.

2. Right-click on the target selected and click **Properties**. This opens the target **Properties** dialog.

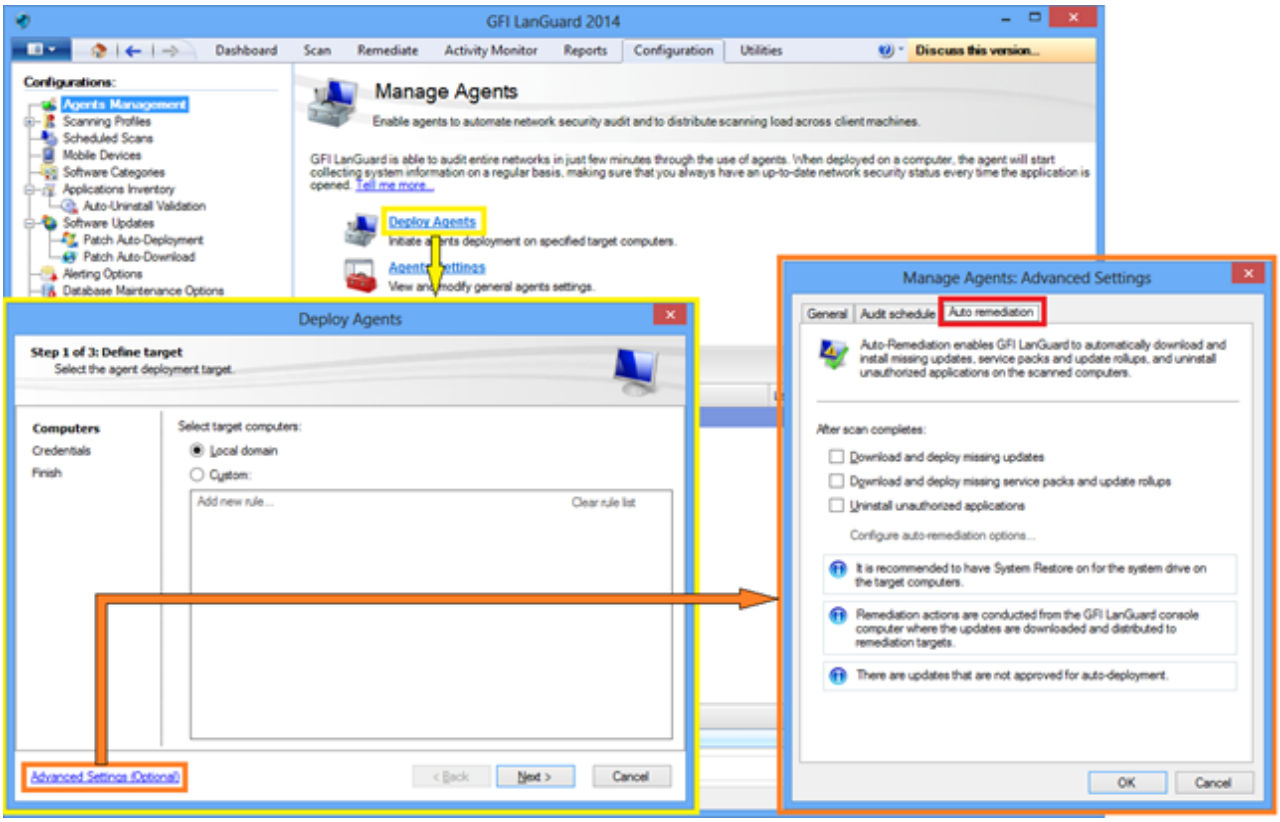
3. From the **Auto Remediation** tab, select the options from the **After scan completes** area and click **OK**.



Screenshot 34: Enabling auto-remediation for existing agent-less security scans

To enable auto-remediation for agents on deployment:

1. From **Configuration > Agents Management** select **Deploy agents**.
2. From the **Deploy Agents** wizard, select **Advanced Settings**.
3. Click the **Auto Remediation** tab and select the options from the **After scan completes** area and click **OK**.



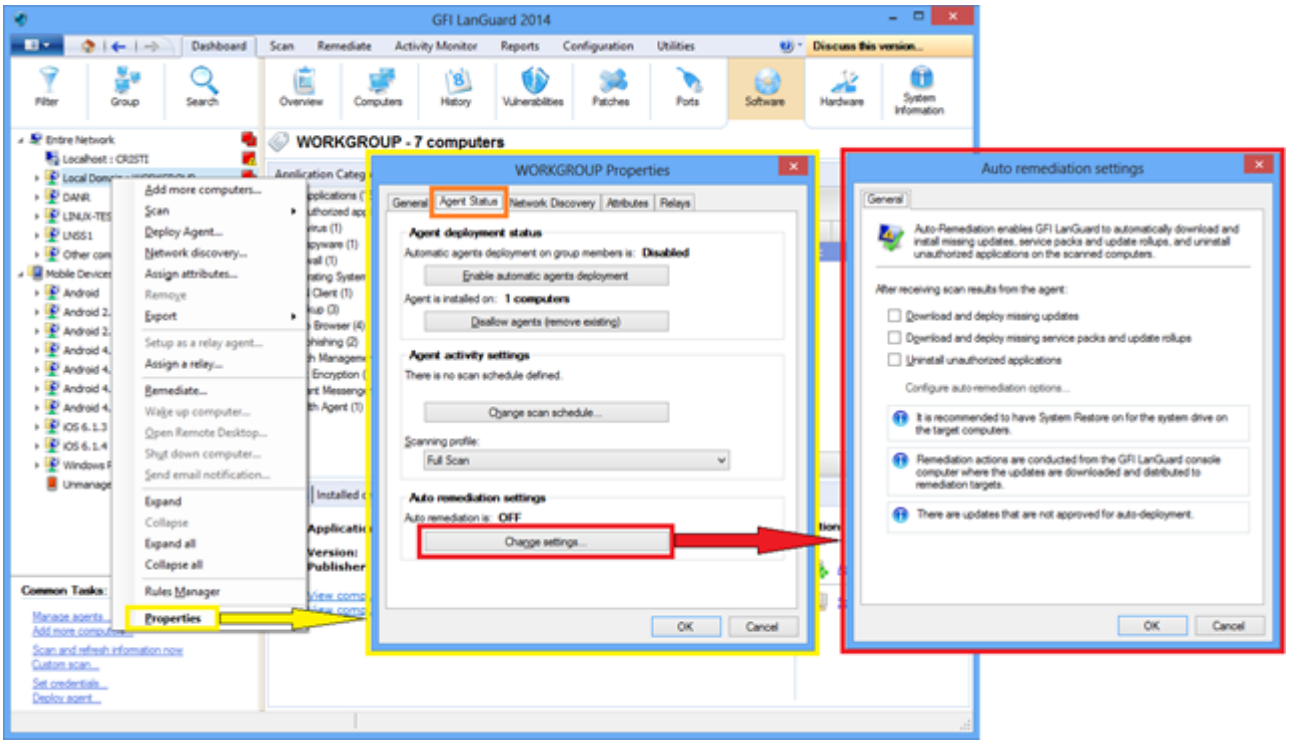
Screenshot 35: Enabling auto-remediation for agents during deployment

To enable auto-remediation for agent audits using the **Dashboard**:

1. From **Dashboard** right click an agent and click **Properties**

2. From the **Properties** dialog box, select the **Agent Status**tab

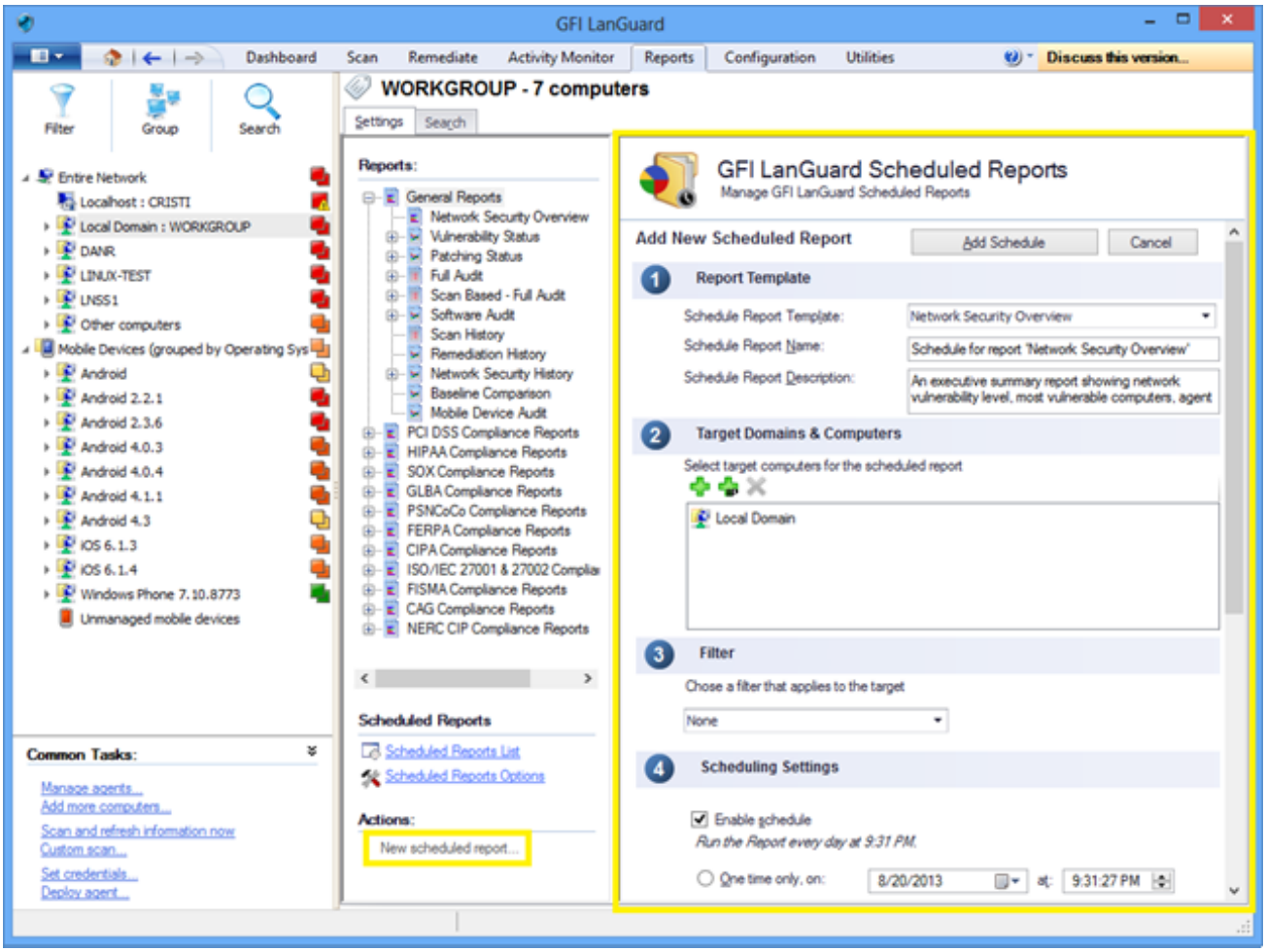
3. Click **Change settings** and select the options from the **After receiving scan results from the agent** area.Click **OK**



Screenshot 36: Enabling auto-remediation using the dashboard

5.5 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.



Screenshot 37: Automating reports generation

6 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.

7 Index