GFI Product Manual

GFI LanGuard™

GFI LanGuard Central Management Server

GFI®

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

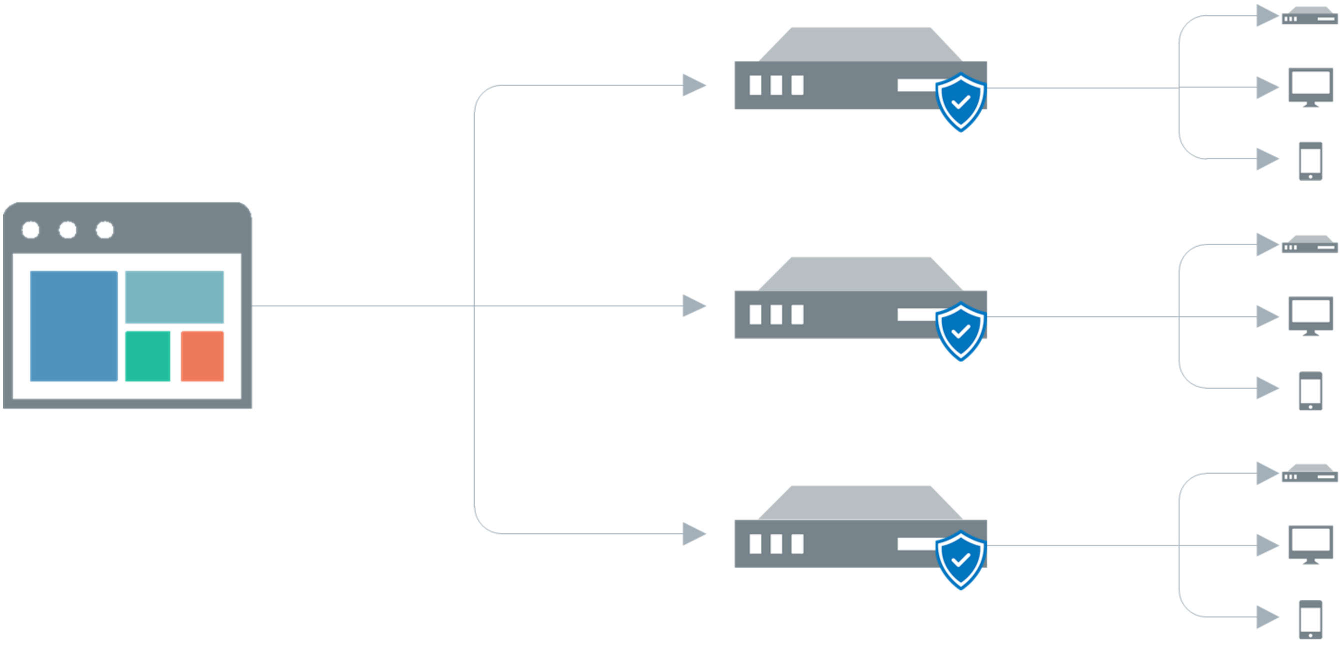
Document Version: 12.2

Last updated (month/day/year): 10/11/2017

Contents

1 GFI LanGuard Central Management Server

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



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

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

1.1 About GFI LanGuard

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

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

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

- Automatic download and remote installation of service packs and patches for Microsoft® Windows, Linux and MAC operating systems as well as third party products
- Automatic uninstallation of unauthorized software.

1.2 Installing GFI LanGuard Central Management Server

GFI LanGuard Central Management Server uses the same installation file of GFI LanGuard. Before starting the installation ensure that the system requirements are met. For more information, refer to Central Management Server system requirements (page 5).

1.2.1 Central Management Server system requirements

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

Hardware requirements

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

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

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

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

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

Supported databases

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

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

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

Firewall Ports and Protocols

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

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

Antivirus & Backup exclusions

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

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

1.2.2 Installing Central Management Server

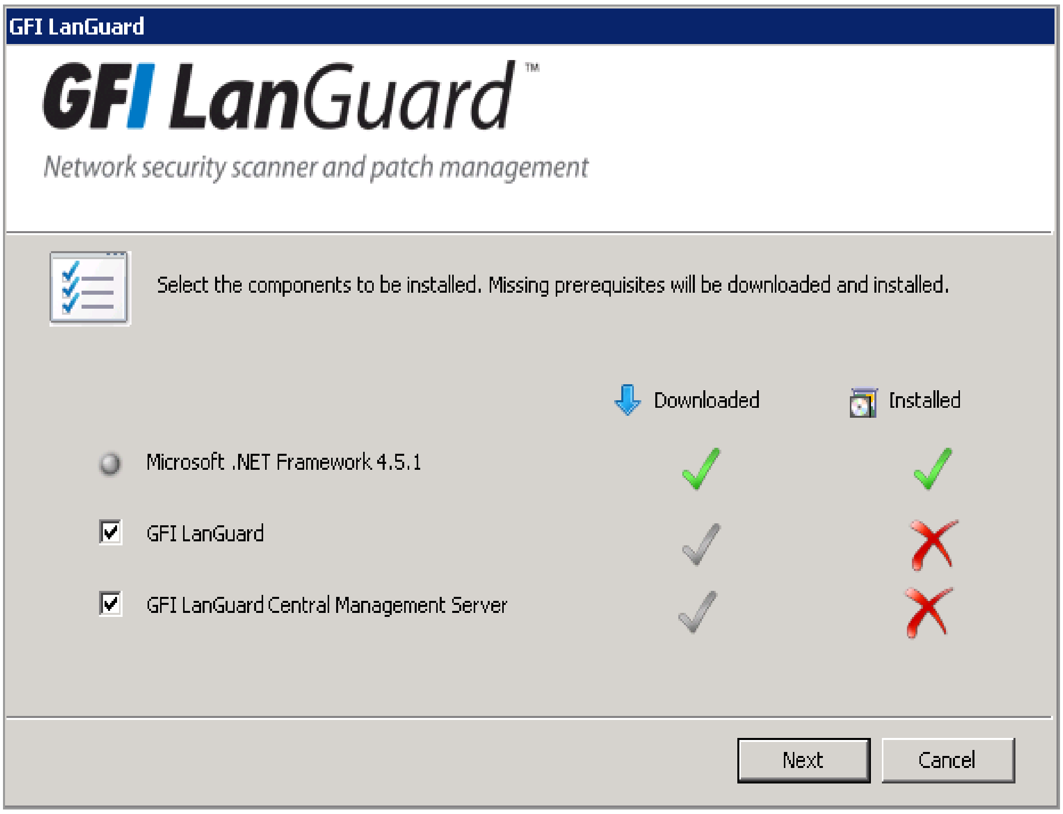
To install GFI LanGuard Central Management Server:

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

> **NOTE**
> If you are installing both GFI LanGuard and GFI LanGuard Central Management Server on the same machine, the installation wizard will first guide you to install GFI LanGuard. For step by step instructions on how to do this, refer to: http://go.gfi.com/?pageid=InstallingLanGuard

2. Launch the setup and select the installation language.

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



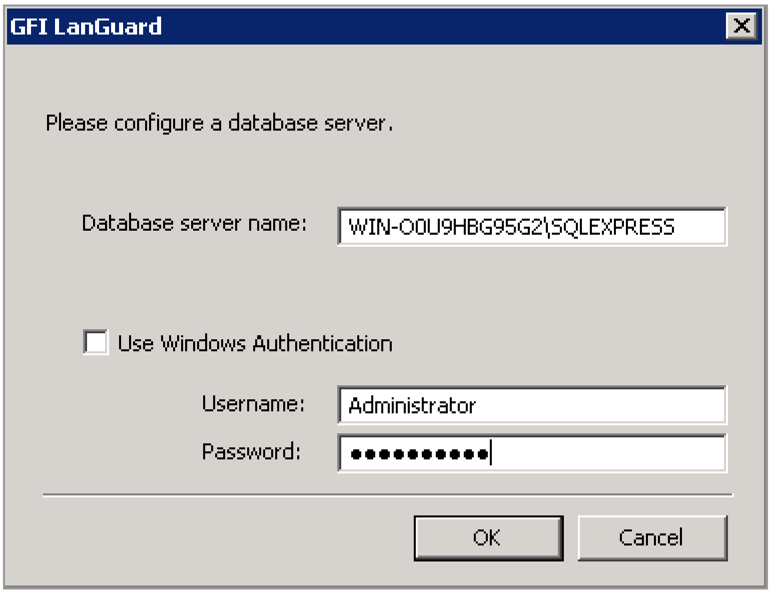
GFI LanGuard

Select the components to be installed. Missing prerequisites will be downloaded and installed.

	Downloaded	Installed
● Microsoft .NET Framework 4.5.1	✓	✓
☑ GFI LanGuard	✓	✗
☑ GFI LanGuard Central Management Server	✓	✗

Screenshot 1: Select components to be installed

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



GFI LanGuard

Please configure a database server.

Database server name: WIN-O0U9HBG95G2\SQLEXPRESS

□ Use Windows Authentication

Username: Administrator

Password: ●●●●●●●●●●●

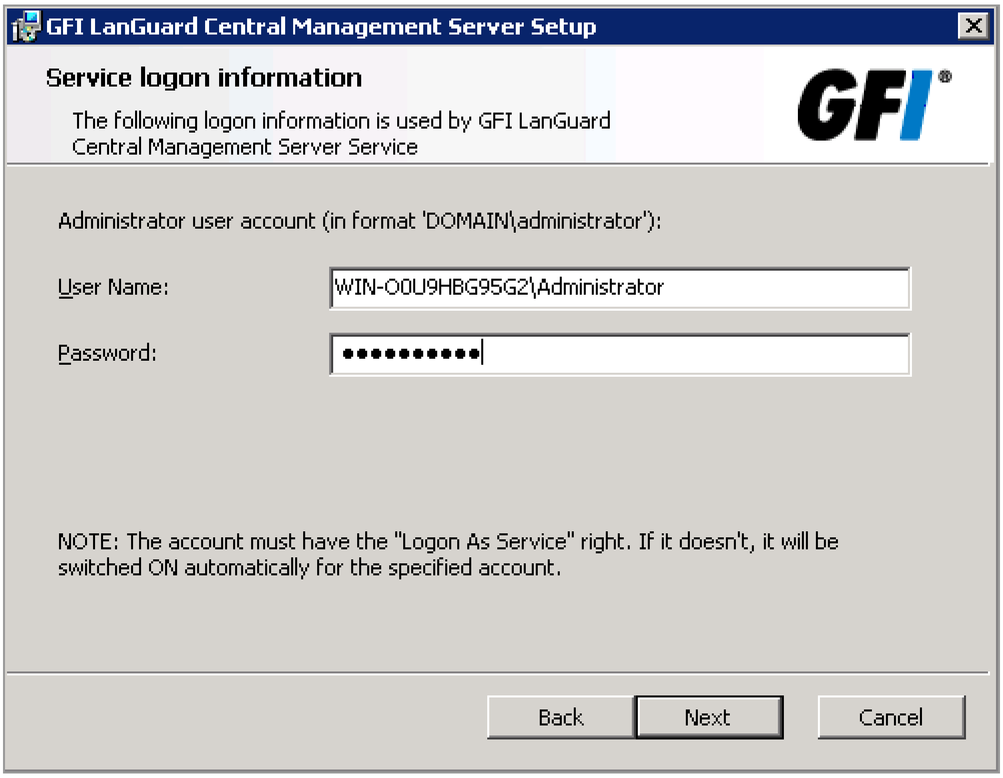
Screenshot 2: Configure the database server

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

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

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

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



GFI LanGuard Central Management Server Setup

Service logon information

The following logon information is used by GFI LanGuard Central Management Server Service

Administrator user account (in format 'DOMAIN\administrator'):

User Name: WIN-O0U9HBG95G2\Administrator

Password: ●●●●●●●●●●●

NOTE: The account must have the "Logon As Service" right. If it doesn't, it will be switched ON automatically for the specified account.

Screenshot 3: Key in credentials for the Windows service

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

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

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

1.2.3 Uninstalling Central Management Server

To uninstall GFI LanGuard Central Management Server

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

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

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

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

1.3 Configuring GFI LanGuard Central Management Server

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

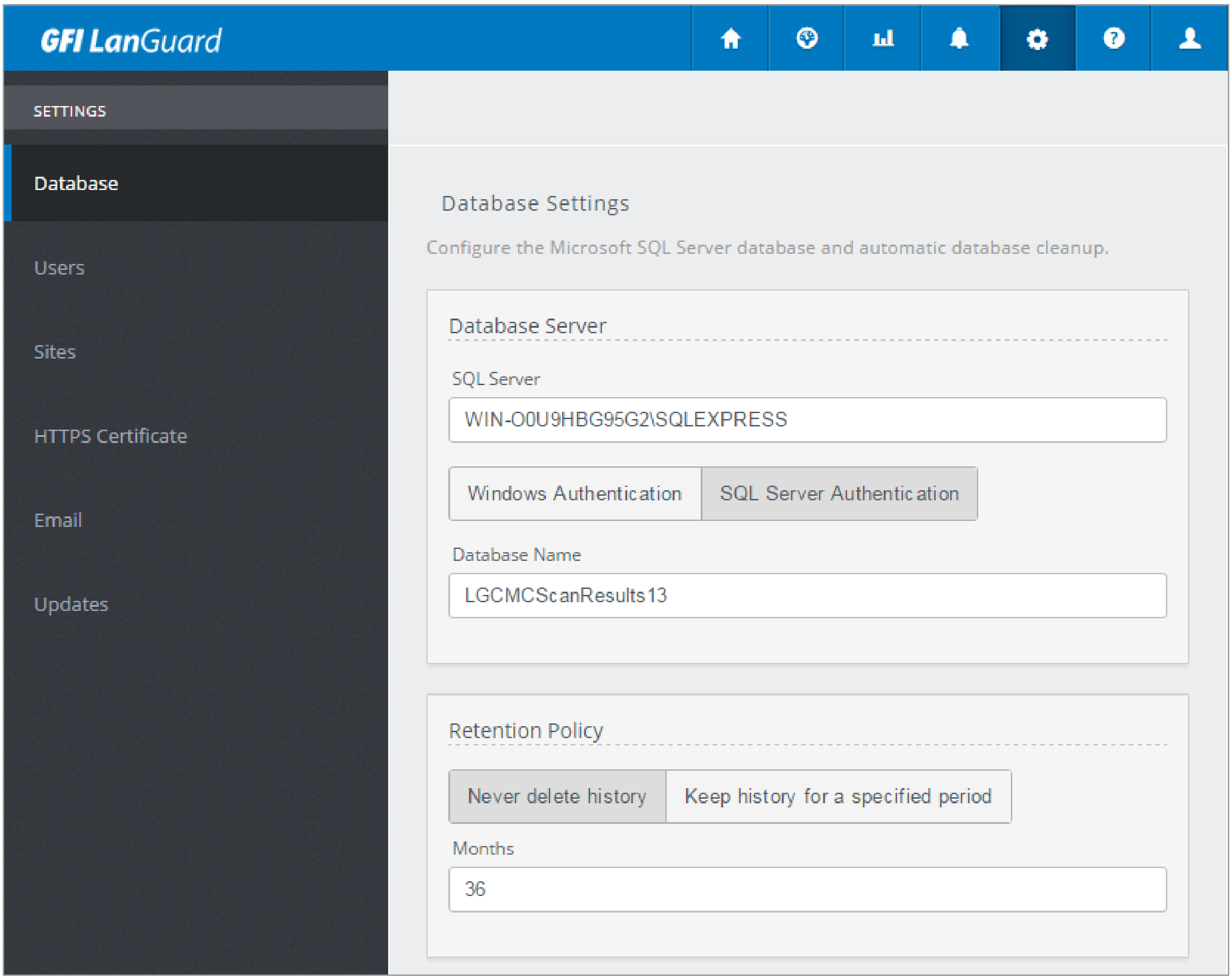
1.3.1 Configuring GFI LanGuard Central Management Server database settings

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

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

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

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



Database Settings

Configure the Microsoft SQL Server database and automatic database cleanup.

Database Server

SQL Server: WIN-O0U9HBG95G2\SQLEXPRESS

Windows Authentication | SQL Server Authentication

Database Name: LGCMCScanResults13

Retention Policy

Never delete history | Keep history for a specified period

Months: 36

Screenshot 4: Configuring Database settings for GFI LanGuard Central Management Server

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

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

1.3.2 Specifying data retention settings

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

To change data retention settings:

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

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

Select from the following options:

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

1.3.3 Configuring Central Management Server user privileges

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

GFI LanGuard Central Management Server offers the following roles:

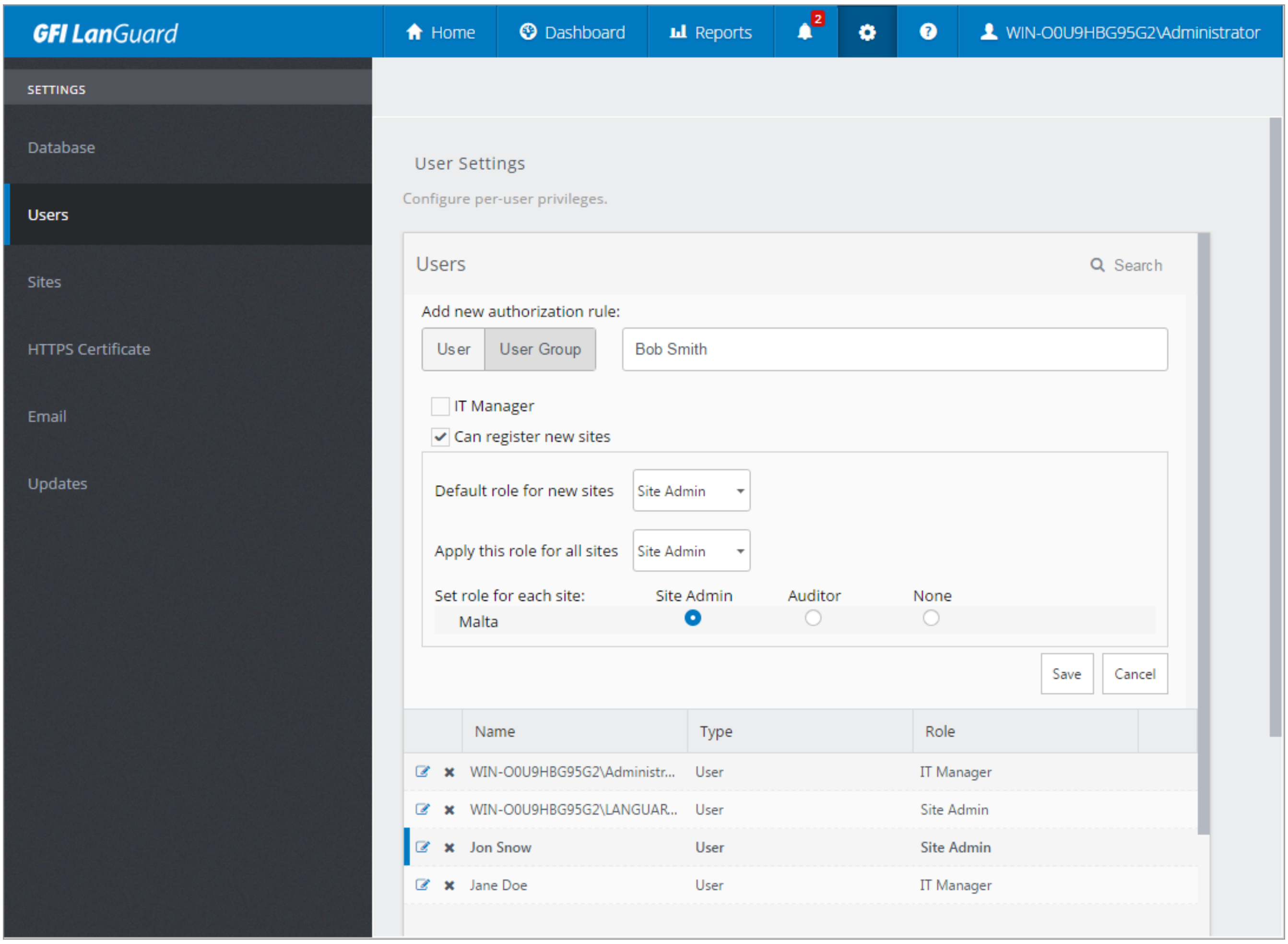
OPTION	DESCRIPTION
IT Manager	This role is made up of both the Site Admin and the Auditor roles and allows users full access to the GFI LanGuard Central Management Server.
Site Admin	Users with Site Admin rights are able to configure and manage the console.
Auditor	The auditor role permits users to access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

To add a new user:

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

2. Select **Users**.

3. Click **Add User** icon.



User Settings

Configure per-user privileges.

Users

Add new authorization rule:

User | User Group: Bob Smith

□ IT Manager

☑ Can register new sites

Default role for new sites: Site Admin

Apply this role for all sites: Site Admin

Set role for each site:	Site Admin	Auditor	None
Malta	●	○	○

Name	Type	Role
WIN-O0U9HBG95G2\Administr...	User	IT Manager
WIN-O0U9HBG95G2\LANGUAR...	User	Site Admin
Jon Snow	User	Site Admin
Jane Doe	User	IT Manager

Screenshot 5: Configuring user access rights to the GFI LanGuard Central Management Server Console

4. Select from the following options:

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

5. Click **Save**.

1.3.4 Managing GFI LanGuard sites in Central Management Server

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

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

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

Editing site details

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

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

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

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

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

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

> **NOTE**
>
> Users or groups configured in the Users area will be automatically added to these lists. For more information, refer to Configuring Central Management Server user privileges (page 11).

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

5. Click **Save**.

1.3.5 Configuring HTTPS Certificate in Central Management Server

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

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

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

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

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

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

Adding the CA Certificate as Trusted Certificate Authority

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

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

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

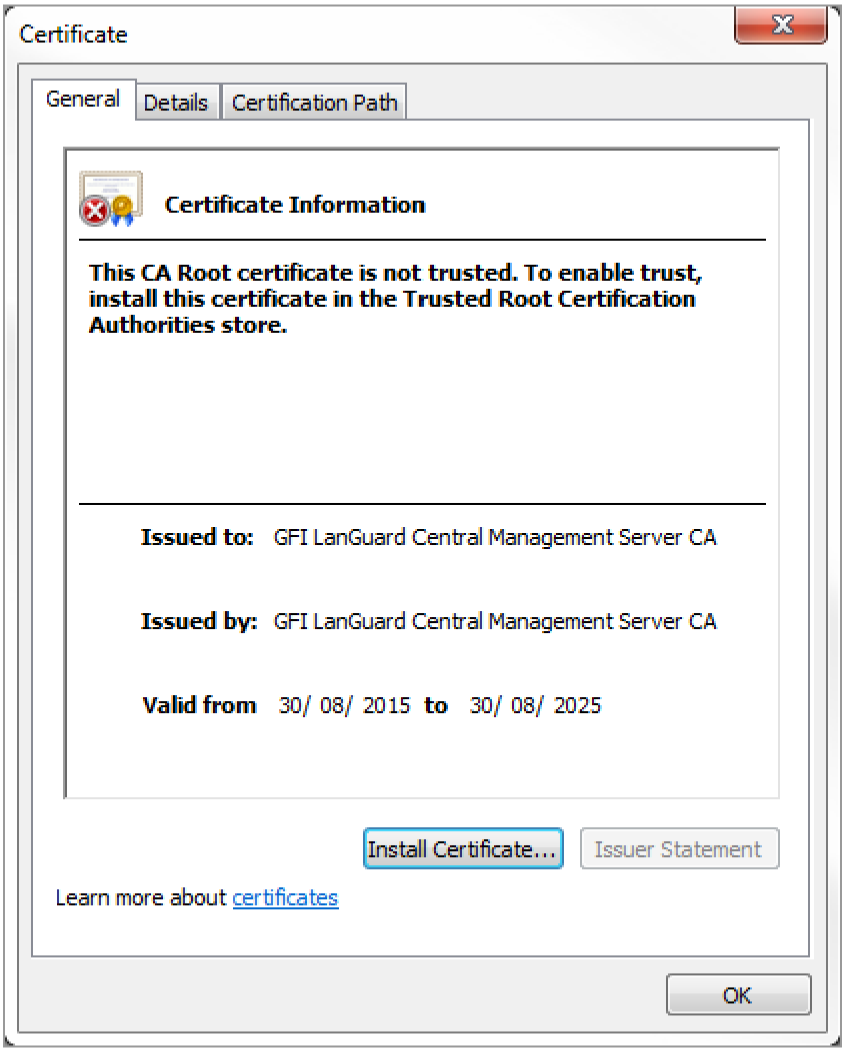
2. When you receive the certificate error in the browser, select **Continue to this website (not recommended)**.

3. Key in the authentication credentials.

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

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

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



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: GFI LanGuard Central Management Server CA

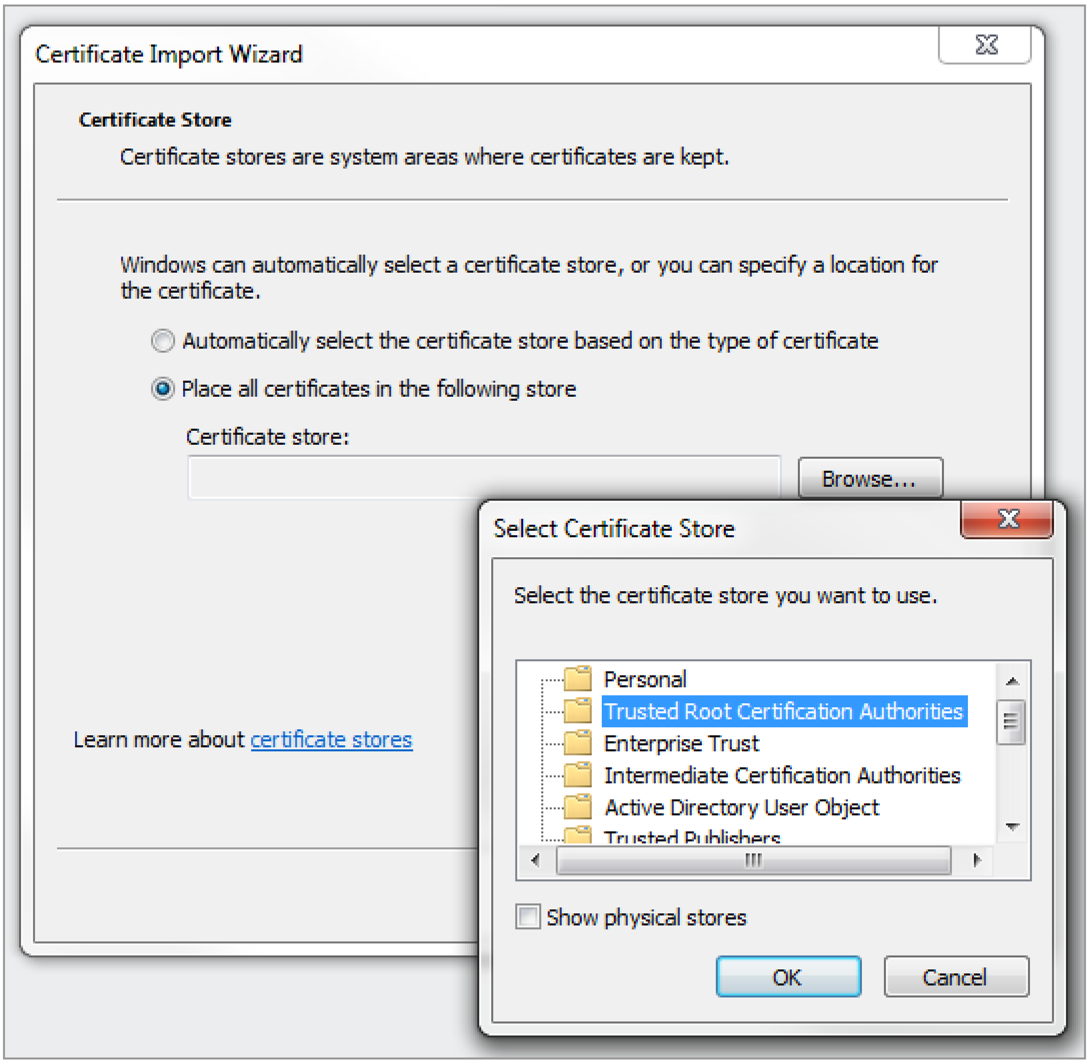
Issued by: GFI LanGuard Central Management Server CA

Valid from 30/ 08/ 2015 **to** 30/ 08/ 2025

Screenshot 6: Installing the CA Certificate

7. Click **Install Certificate…**.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Learn more about certificate stores

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

Screenshot 7: Select location for imported certificate

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

10. Click **Next**.

11. Click **Finish**.

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

For Mozilla Firefox on any operating system

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

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

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

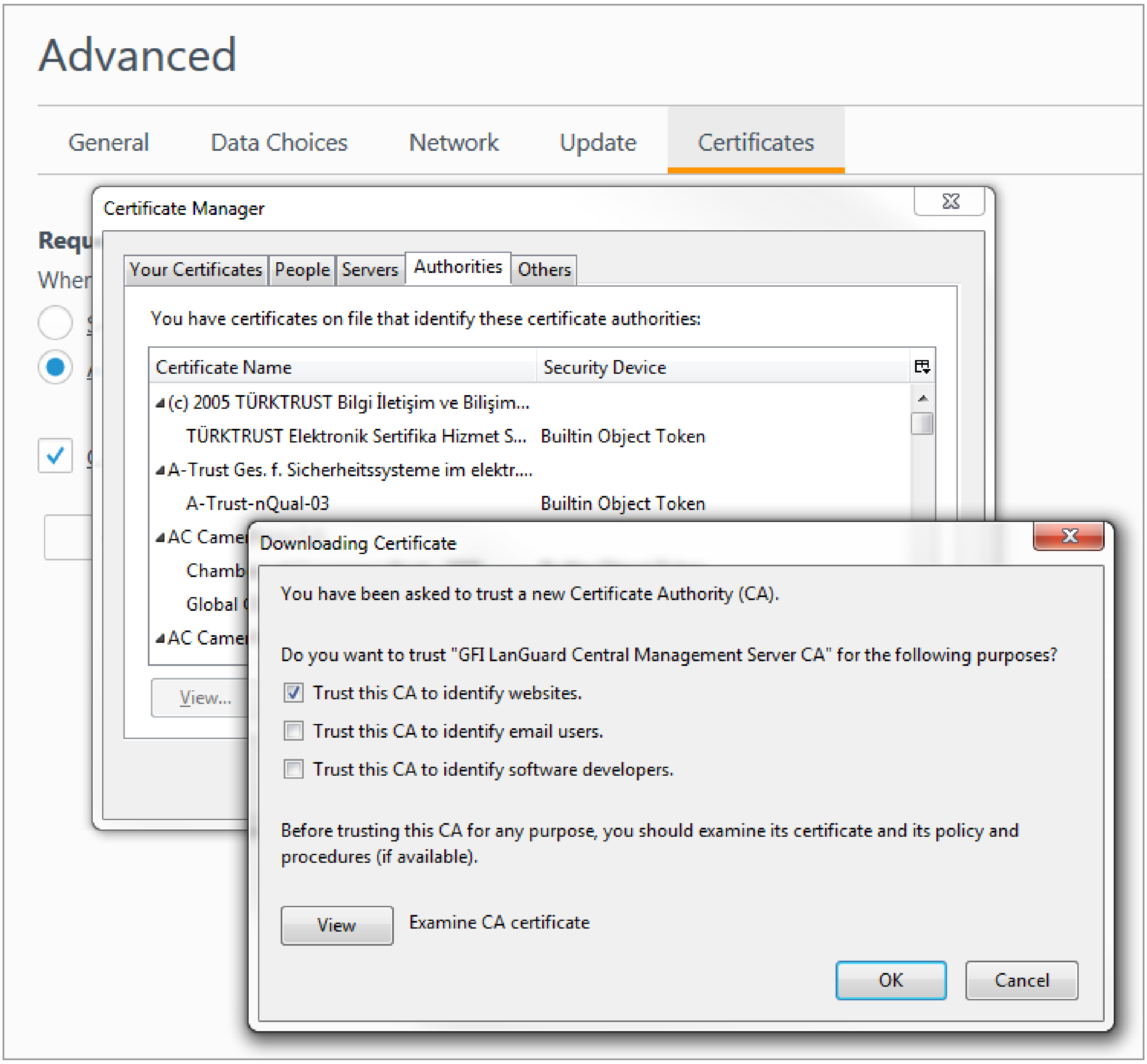
4. Key in the authentication credentials.

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

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

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

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



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
◢(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim...	
TÜRKTRUST Elektronik Sertifika Hizmet S...	Builtin Object Token
◢A-Trust Ges. f. Sicherheitssysteme im elektr....	
A-Trust-nQual-03	Builtin Object Token

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "GFI LanGuard Central Management Server CA" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Screenshot 8: Importing a trusted CA Certificate in Firefox

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

For Safari, Google Chrome and Opera on Apple OS X

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

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

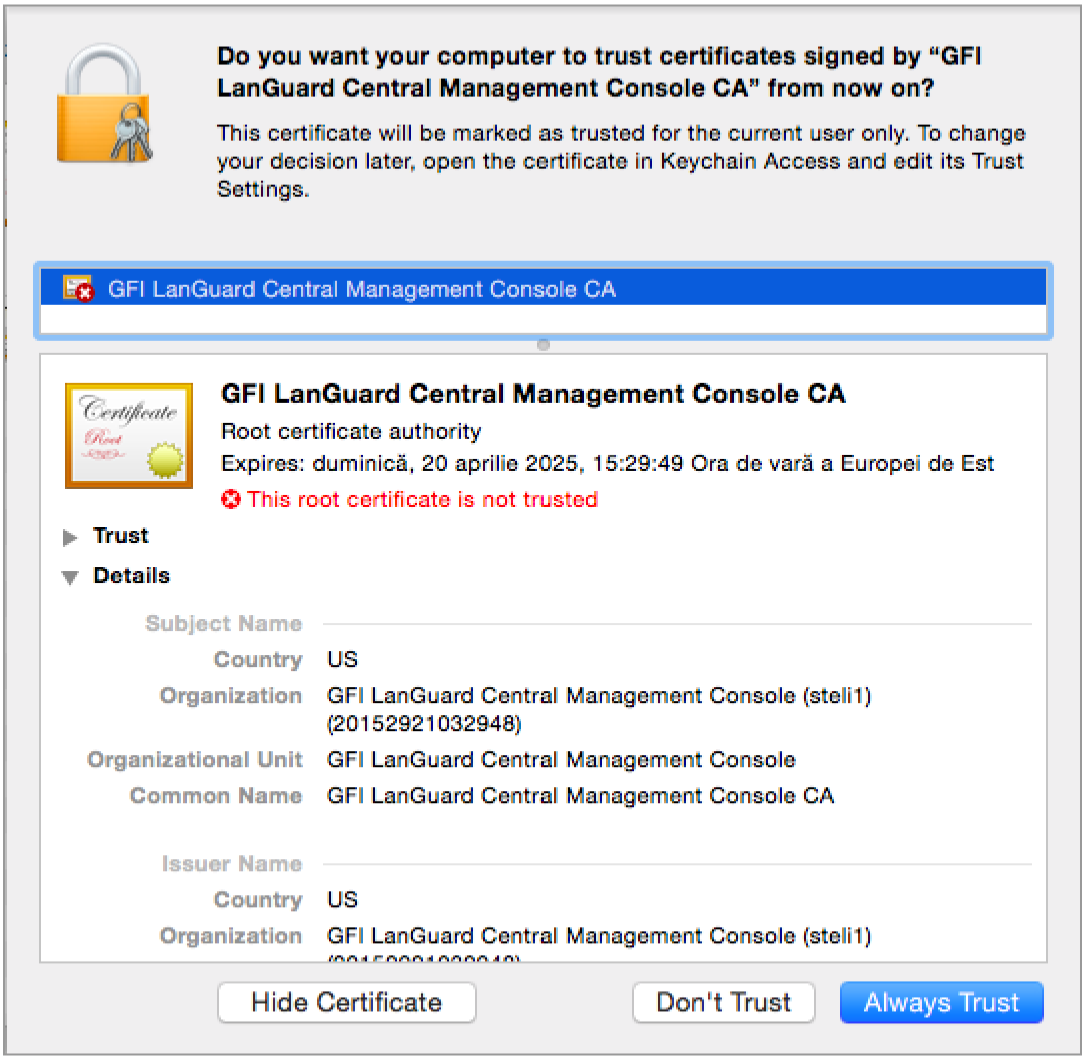
3. Key in the authentication credentials.

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

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

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

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



Do you want your computer to trust certificates signed by “GFI LanGuard Central Management Console CA” from now on?

This certificate will be marked as trusted for the current user only. To change your decision later, open the certificate in Keychain Access and edit its Trust Settings.

GFI LanGuard Central Management Console CA

GFI LanGuard Central Management Console CA

Root certificate authority

Expires: duminică, 20 aprilie 2025, 15:29:49 Ora de vară a Europei de Est

This root certificate is not trusted

▶ **Trust**

▼ **Details**

Subject Name

Country US

Organization GFI LanGuard Central Management Console (steli1) (20152921032948)

Organizational Unit GFI LanGuard Central Management Console

Common Name GFI LanGuard Central Management Console CA

Issuer Name

Country US

Organization GFI LanGuard Central Management Console (steli1) (20152921032948)

Screenshot 9: Configuring a CA Certificate in Safari, Google Chrome and Opera on Apple OS X

8. Select **Always Trust**.

Using an existing SSL certificate in Central Management Server

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

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

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

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

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

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

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

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

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

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

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

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

1.3.6 Email settings in Central Management Server

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

1. Click **Settings > Email**.

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

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

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

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

4. Click **Save**.

1.3.7 Configuring Central Management Server Updates

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

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

To configure system updates:

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

2. Configure the following:

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

3. Click **Save**.

1.4 Using the GFI LanGuard Central Management Server Console

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

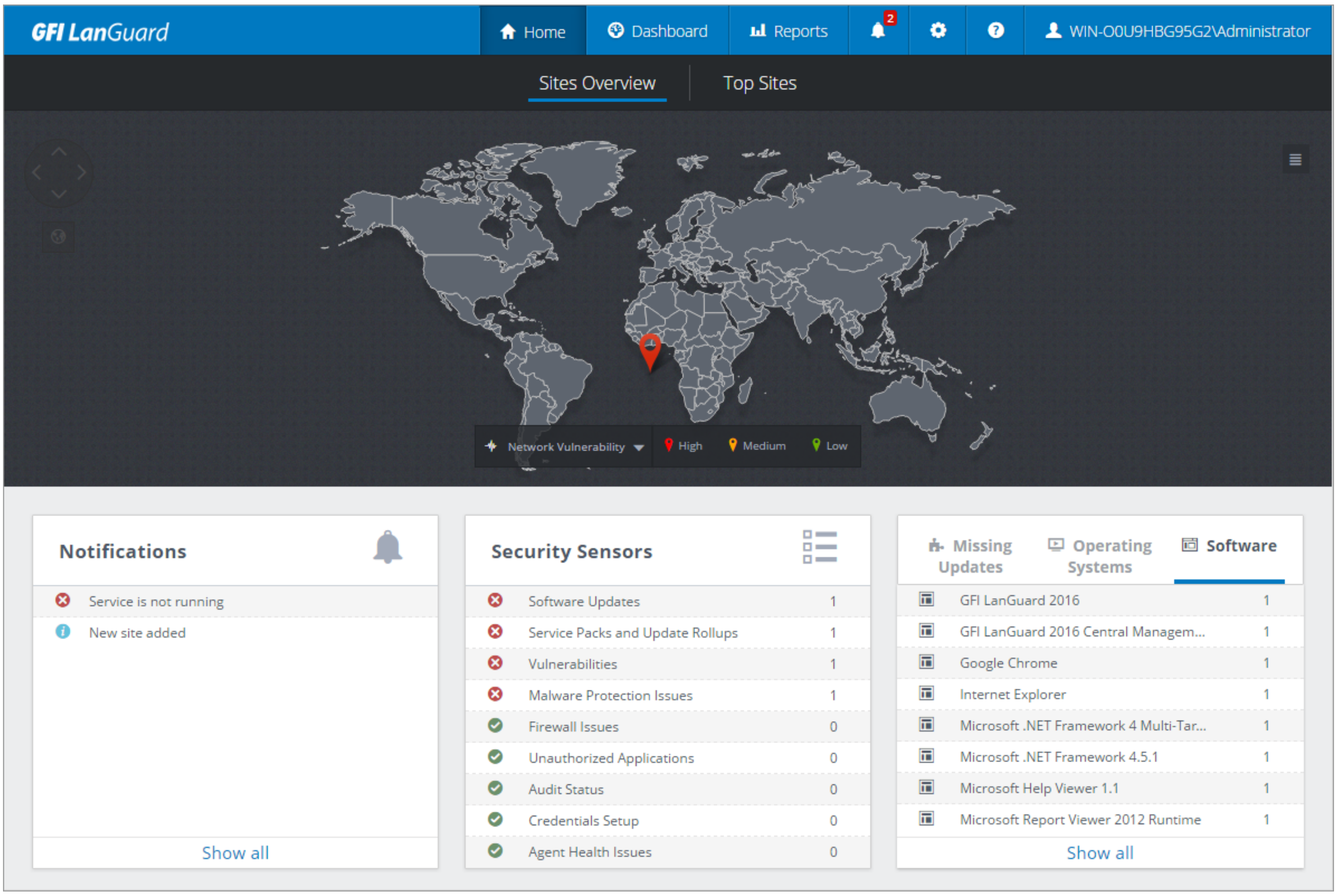
`https://<server name/IP address>:1077/Home/Home`.

Different user access rights can be granted from the settings area. For more information, refer to Configuring Central Management Server user privileges (page 11).

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

1.4.1 Central Management Server Home Page

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



Notifications

☒	Service is not running
ⓘ	New site added

Show all

Security Sensors

☒	Software Updates	1
☒	Service Packs and Update Rollups	1
☒	Vulnerabilities	1
☒	Malware Protection Issues	1
✓	Firewall Issues	0
✓	Unauthorized Applications	0
✓	Audit Status	0
✓	Credentials Setup	0
✓	Agent Health Issues	0

Missing Updates | Operating Systems | **Software**

GFI LanGuard 2016	1
GFI LanGuard 2016 Central Managem...	1
Google Chrome	1
Internet Explorer	1
Microsoft .NET Framework 4 Multi-Tar...	1
Microsoft .NET Framework 4.5.1	1
Microsoft Help Viewer 1.1	1
Microsoft Report Viewer 2012 Runtime	1

Show all

Screenshot 10: The GFI LanGuard Central Management Server Home page

Toggle between the following views:

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

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

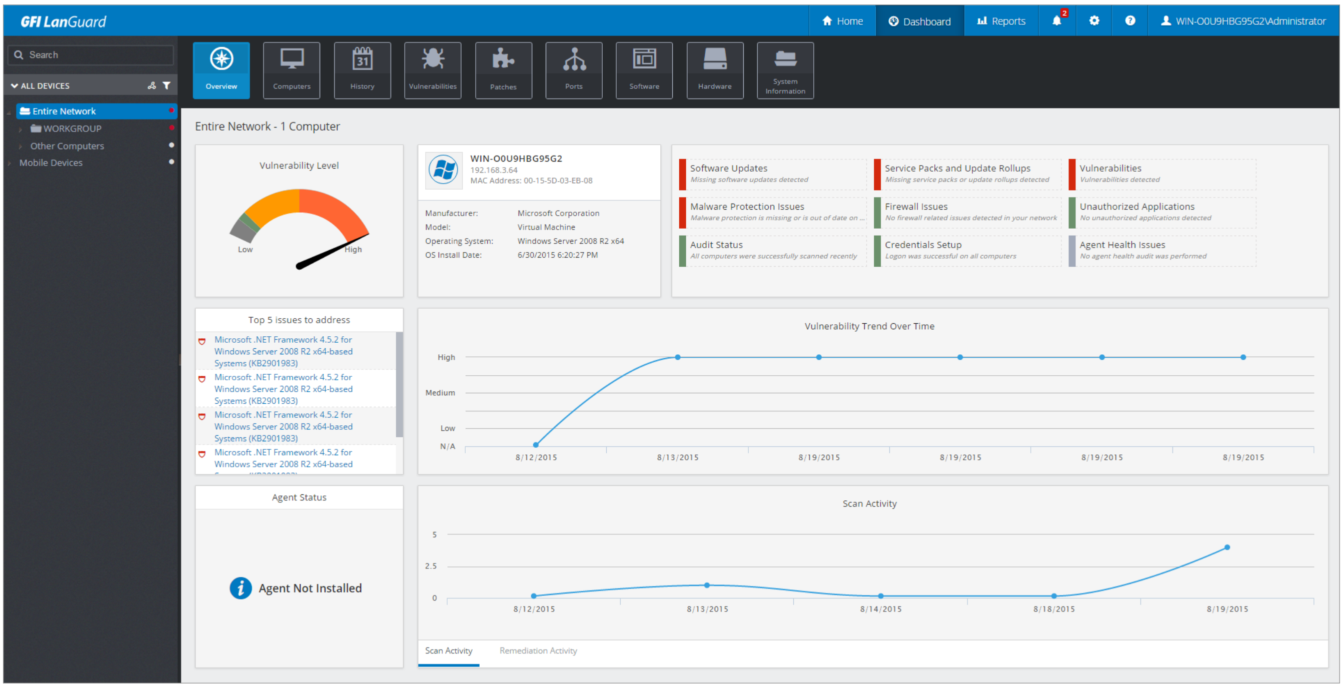
> **NOTE**
> The sites displayed by the GFI LanGuard Central Management Server represent GFI LanGuard instances that have been set up within each GFI LanGuard deployment. The GFI LanGuard Central Management Server is unable to detect any sites automatically. To view or edit details of connected sites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

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

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

1.4.2 Central Management Server Dashboards

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



Entire Network - 1 Computer

WIN-O0U9HBG95G2
192.168.3.64
MAC Address: 00-15-5D-03-EB-08

Manufacturer:	Microsoft Corporation
Model:	Virtual Machine
Operating System:	Windows Server 2008 R2 x64
OS Install Date:	6/30/2015 6:20:27 PM

- Software Updates — *Missing software updates detected*
- Service Packs and Update Rollups — *Missing service packs or update rollups detected*
- Vulnerabilities — *Vulnerabilities detected*
- Malware Protection Issues — *Malware protection is missing or is out of date on ...*
- Firewall Issues — *No firewall related issues detected in your network*
- Unauthorized Applications — *No unauthorized applications detected*
- Audit Status — *All computers were successfully scanned recently*
- Credentials Setup — *Logon was successful on all computers*
- Agent Health Issues — *No agent health audit was performed*

Microsoft .NET Framework 4.5.2 for Windows Server 2008 R2 x64-based Systems (KB2901983)
Microsoft .NET Framework 4.5.2 for Windows Server 2008 R2 x64-based Systems (KB2901983)
Microsoft .NET Framework 4.5.2 for Windows Server 2008 R2 x64-based Systems (KB2901983)
Microsoft .NET Framework 4.5.2 for Windows Server 2008 R2 x64-based

Agent Not Installed

Screenshot 11: The overview dashboard

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

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

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

1.4.3 Central Management Server Computer Tree

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

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

Saved filters can also be used to generate targeted reports. For more information, refer to Using GFI LanGuard Central Management Server Reports (page 28).

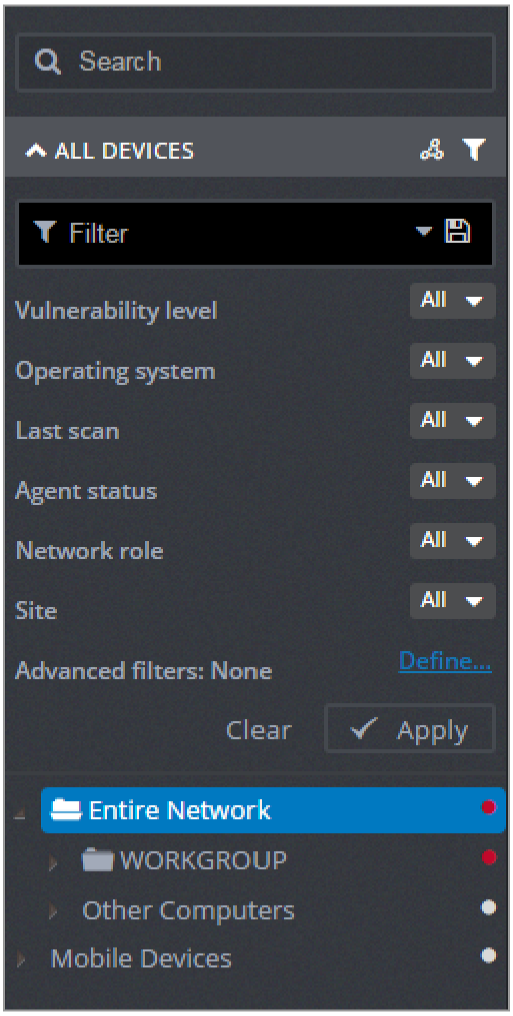
The following are functions supported by the computer tree:

- Simple filtering
- Advanced filtering
- Grouping
- Saved Filters

Simple filtering

To filter for a specific computer or group:

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



Vulnerability level All

Operating system All

Last scan All

Agent status All

Network role All

Site All

Advanced filters: None

Screenshot 12: Using a simple filter

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

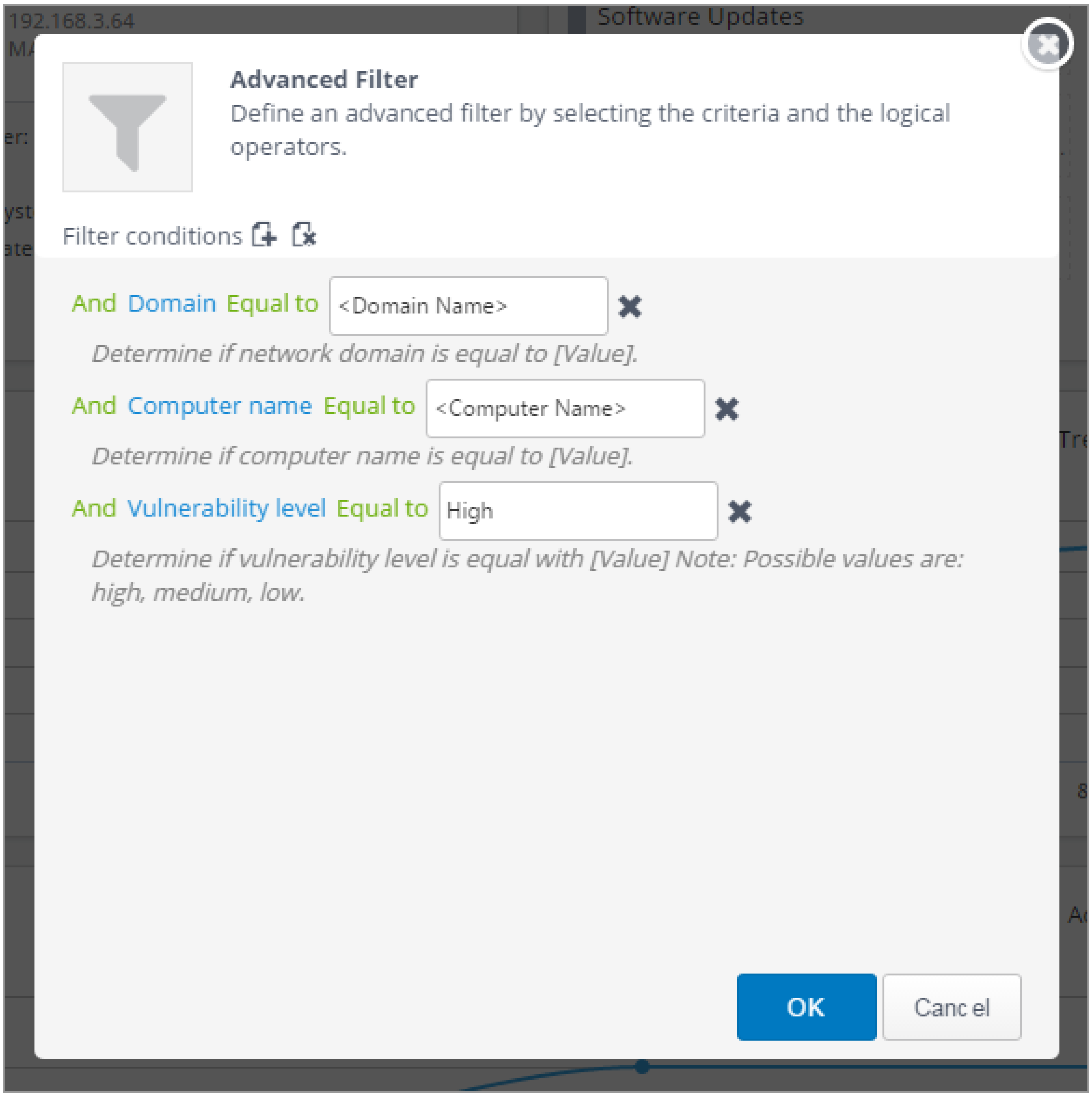
3. Click **Apply**.

Advanced filtering

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

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

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



Advanced Filter

Define an advanced filter by selecting the criteria and the logical operators.

Filter conditions

And Domain Equal to <Domain Name>

Determine if network domain is equal to [Value].

And Computer name Equal to <Computer Name>

Determine if computer name is equal to [Value].

And Vulnerability level Equal to High

Determine if vulnerability level is equal with [Value] Note: Possible values are: high, medium, low.

Screenshot 13: Using advanced filtering

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

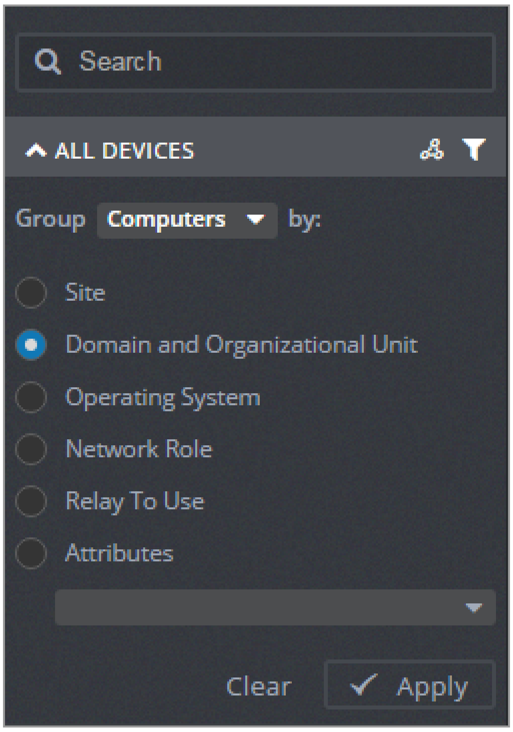
4. Select filtering conditions and key in the condition value. You can add as many as required.

5. Click **OK**

Grouping

To group machines by specific attributes:

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



Screenshot 14: Group machines by specific attributes

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

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

> NOTE
>
> If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to Using Attributes in Central Management Server (page 28).

3. Click **Apply**.

Saved Filters

Saved Filters enable you to customize views and save them to quickly find frequently accessed information. Saved filters are also used in report scheduling. For more information, refer to Scheduling a report in GFI LanGuard Central Management Server (page 33).

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

To save a new filter:

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

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

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

4. Click the **Save** icon.

Using Attributes in Central Management Server

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

Attributes are configured in separate GFI LanGuard sites. When the remote sites synchronize with GFI LanGuard Central Management Server, they appear in the attributes list. For more information on how to create and manage attributes refer to: http://go.gfi.com/?pageid=LGCMSAttributes.

1.4.4 Using GFI LanGuard Central Management Server Reports

This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard Central Management Server. New reports can be added by customizing existing reports and saving them with a new name. For more information, refer to Customizing GFI LanGuard Central Management Server Reports (page 34).

There are two main types of reports:

- General reports - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity
- Legal compliance reports - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

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

- Generating reports
- Scheduling reports

General reports

To view **General** reports:

1. Click **Reports** tab.

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

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

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

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

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

Legal Compliance reports

To view **Legal Compliance** reports:

1. Click **Reports** tab.

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

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

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

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

Generating a report in GFI LanGuard Central Management Server

To use one of the reports:

1. From the top navigation, click **Reports**.

2. Select a report category from the View menu.

3. Hover over one of the report names and click **Generate** to run the report.

Scheduling a report in GFI LanGuard Central Management Server

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

1. From the top navigation, click **Reports**.

2. Use the **View** filter on the left to select the category of reports you need.

3. Hover over a report and click **Schedule**.

4. In the **General** tab, define the following:

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

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

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

OPTION	DESCRIPTION
Choose a filter that applies to the target	Filters enable you to generate more targeted reports. For example, you can generate reports for high vulnerability issues only. Select one of the saved filters from the drop down list that apply to the currently selected report. If you have not saved any filters, this option will be grayed out. For information on how to create new filters refer to: Using the Computer Tree.
Export to file	Select this option to export the generated report. This can be saved to file or sent by email as an attachment. Use the **Report Format** drop down field to specify the format of the exported report. Available formats are *.pdf, *.rtf, *.xls, *.xlsx, *.html, *.mht and *.png
Send by email	Select this option if you want the generated report to be automatically sent as an attachment by email. GFI LanGuard Central Management Server uses configured email settings when sending reports. To view currently configured settings click **Email Setup**. For more information, refer to Email settings in Central Management Server (page 19).
Override general alerting options and send email to:	Select this option if you want GFI LanGuard Central Management Server to ignore currently configured email settings and send the generated report to a specific email addresses. Enter the email address in the available field. Separate multiple email addresses with a semi-colon.

6. Click **Save**.

Customizing GFI LanGuard Central Management Server Reports

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

To customize a report:

1. From the top navigation, click **Reports**.

2. Hover over one of the report names and click **Customize**.

3. Modify the following options:

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

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

2 Index