GFI OneGuard™

ADMINISTRATOR GUIDE

Find out how to configure GFI OneGuard in different environments, and learn how to set up advanced features.

Document Version: 2.0

Last updated (month/day/year): 10/05/2018

Contents

1 Introduction to GFI OneGuard 1
1.1 About GFI OneGuard 1
1.1.1 Benefits of GFI OneGuard 1
1.2 How it works 1
1.3 Services Offered 1

2 Getting Started with GFI OneGuard 3
2.1 GFI OneGuard system requirements 3
2.1.1 Software requirements 4
2.1.2 Hardware requirements 5
2.1.3 Firewall Ports 5
2.1.4 Antivirus and backup software 5
2.2 Planning GFI OneGuard deployment 6
2.2.1 Common deployment scenarios 6
2.3 Downloading the latest version of GFI OneGuard 6
2.4 How to install the GFI OneGuard Platform and Controller 7
2.5 Post-installation tasks 9
2.6 Upgrading to the latest version while retaining all settings 10
2.6.1 Important notes when upgrading 10
2.6.2 Upgrade Procedure 11
2.7 The GFI OneGuard Controller 11
2.7.1 Installing the GFI OneGuard Controller 12
2.8 GFI OneGuard Agents 13
2.8.1 GFI OneGuard Agent installation and removal 14
2.9 Logging into GFI OneGuard 14

3 Using the GFI OneGuard Platform 16
3.1 Home page 17
3.2 Groups and Devices 18
3.2.1 Adding new groups 20
3.2.2 Group settings 21
3.2.3 Assigning devices to groups 22
3.2.4 Moving Devices between groups 23
3.2.5 Manually running a service on devices 23
3.2.6 Renaming a group of devices 24
3.2.7 Deleting a group 24
3.2.8 Removing a managed device 24
3.3 Asset Tracking 25
3.3.1 Device hardware & software information 26
3.3.2 Customizing device login credentials 26
3.3.3 Sending a message to a device 27
3.3.4 Device service notifications 28
3.3.5 Shutting down or Restarting a device remotely 29
3.3.6 Disabling Asset Tracking 30
3.4 Patch Management 31
3.4.1 Monitoring patch deployment 31
3.4.2 Configuring Patch Management on a Group 32
3.4.3 Run Patch Services on a Device 35
3.4.4 Disabling Patch Management 36
3.5 Antivirus 37
3.5.1 Monitoring Antivirus 37
3.5.2 Configuring group antivirus protection 39

3.5.3 Device antivirus options ... 46
3.5.4 Antivirus global exclusion list ... 47
3.5.5 Disabling the Antivirus service ... 47
3.6 EndPoint Control ... 48
3.6.1 Monitoring EndPoint Control ... 49
3.6.2 Configuration ... 50
3.6.3 Adding New Rule ... 52
3.6.4 Working with Access Rules ... 56
3.6.5 Whitelist ... 57
3.6.6 Blocklist ... 59
3.6.7 Configuring encryption ... 62
3.6.8 Enabling notification ... 66
3.6.9 Temporary Access ... 66
3.6.10 Resetting the password for an encrypted device ... 69
3.7 Reports ... 70
3.7.1 Generating reports ... 71
3.7.2 Viewing and sharing generated reports ... 73
3.7.3 Custom reports ... 74
3.7.4 Scheduling reports ... 75
3.7.5 Sending reports via email ... 77
3.7.6 Deleting reports ... 77
3.8 Activity Monitor ... 78
3.9 Notifications Area ... 79

4 Settings ... 81
4.1 System settings ... 81
4.1.1 Mail server SMTP information ... 82
4.1.2 Proxy settings ... 83
4.1.3 Network Control ... 84
4.1.4 Notification Settings ... 86
4.1.5 Platform updates ... 86
4.1.6 Licensing ... 87
4.1.7 Roles and Permissions ... 88
4.1.8 Creating a new role ... 89
4.1.9 Editing an existing role ... 90
4.1.10 Role assignment ... 91
4.2 User profile settings ... 92
4.3 Controller configuration ... 93
4.3.1 Monitoring the Controller's status ... 94
4.3.2 Controller settings ... 94
4.4 How to backup GFI OneGuard configuration ... 97
4.4.1 Step 1: Stop GFI OneGuard services ... 97
4.4.2 Step 2: Backup folders ... 97
4.4.3 Step 3: Start the GFI OneGuard services ... 98
4.5 Securing Platform communications ... 98
4.6 Managing multiple domains ... 100
4.7 Controlling workgroups ... 101

5 Troubleshooting and support ... 104

6 Glossary ... 105

7 Index ... 112

1 Introduction to GFI OneGuard

1.1 About GFI OneGuard

GFI OneGuard is a delivery platform enabling network administrators to centralize, simplify and automate the process of managing security and resources on network machines. GFI OneGuard is a highly scalable solution that can be installed on-premise or in a cloud infrastructure and can support network configurations of up to 10,000 devices per instance.

For more information, refer to How it works (page 1).

GFI OneGuard ships with a free Asset Tracking service that identifies devices connected to the network where it is deployed. Other services such as patch management, antivirus and EndPoint Control can also be pushed and managed from the same console to all devices, speeding up deployment and minimizing disruption and personnel time needed to complete the work. For more information, refer to Services Offered (page 1).

1.1.1 Benefits of GFI OneGuard

GFI OneGuard resolves network problem headaches by helping System Administrators:

» Implement network security and management services using simple controls from a console accessible through an Internet browser.

» Keep software up to date through a Patch Management service. Known security holes are addressed using the latest patches provided by different software vendors.

» Protect devices from malware, avoid ransomware and potential exploits through an Antivirus service powered by Kaspersky Lab.

» Keep an inventory of the software and hardware installed in the network via an Asset Tracking feature.

» Issue relevant reports through a robust reporting engine. Reports can be generated in PDF or Excel format, manually or automatically on a schedule. Reports can be shared with users outside the organization if required.

1.2 How it works

To view an interactive slide show of how GFI OneGuard works, go to http://go.gfi.com/?pageid=OneGuardHelp#cshid=howitworks

1.3 Services Offered

GFI OneGuard is a platform software that integrates numerous services into one product. These services act as a virtual toolkit for system administrators, enabling them to perform a number of tasks remotely. These features give administrators the ability to monitor the health and stability of their networks and optimize server and workstation configurations to improve performance. Any or all of these services may be deployed in a flexible and scalable manner that best suits the unique business needs of small and medium-size businesses.

The Asset Tracking service is available to all GFI OneGuard customers. It is not a paid service and is available even if a GFI OneGuard subscription is not renewed. The other services can be purchased separately.

The current version of GFI OneGuard provides the following services:

Service	Description
Asset Tracking	This service makes an inventory of all network devices running a Windows operating system, listing hardware specifications for each device found and the installed software. When the network is scanned through the Asset Tracking service, IT staff can get a real-time view of hardware and key software status using the management console. Devices can be monitored from any location using a normal web browser.
Antivirus	Keep your network devices free from malware and viruses by using the GFI OneGuard Antivirus service which is powered by Kaspersky Lab. It provides a very powerful endpoint protection solution that can handle malware attacks that try to hijack the device and also has a very powerful disinfection engine. It is important that companies block such intrusion points in the network, checking all devices for malicious activity. If a malicious code is found running then this is deleted or blocked based on actions defined by the GFI OneGuard administrator.
Patch Management	Through the Patch Management service, GFI OneGuard assists administrators to deploy patches for software installed on different devices within the network. Manually patching each and every machine can be cumbersome and using one tool to do the job makes it much easier. All software has vulnerabilities and vendors release patches when such vulnerabilities or bugs are found. When doing so, software vendors also disclose the issues that have been fixed. Hackers make use of disclosed information to create malicious programs that attack these vulnerabilities, knowing that many organizations do not patch their software. Malicious code is generally distributed via downloads; this is why it's important that organizations always have all software updated to the latest version and also install the latest patches available. GFI OneGuard provides a single console where all the patch information can be automatically identified and deployed with a single click.
EndPoint Control	Control access to portable devices using the EndPoint Control agent of GFI OneGuard. EndPoint Control policies allow a granular control of what category of devices can be accessed by different group of users. The service also can enable encryption to be available in all USB devices as well as content awareness and file type control.

2 Getting Started with GFI OneGuard

Would you like to try out GFI OneGuard? This topic provides a quick list of actions to help you get started with GFI OneGuard.

1	**Sign up to GFI OneGuard** Go to http://go.gfi.com/?pageid=og_trial and sign up for GFI OneGuard. Follow the instructions to have your account created and download the GFI OneGuard installer. This account gives you a **free & unlimited** 30 day trial for all services and features. After the 30 days are over, you can purchase a subscription to continue using the product. If you decide not to purchase a subscription, you can continue using asset management but other scanning or remediation features will not be available.
2	**Prepare infrastructure** Decide on how to best setup your GFI OneGuard deployment, depending on your network infrastructure. For more information, refer to Planning GFI OneGuard deployment (page 6). The server where GFI OneGuard will be installed must meet or exceed the system requirements. For more information, refer to GFI OneGuard system requirements (page 3). Log into the server using an account with administrative rights.
3	**Install GFI OneGuard** Run the installer downloaded when creating your account in step 1 above. Follow the wizard steps to deploy the GFI OneGuard Platform and Controller. For more information, refer to How to install the GFI OneGuard Platform and Controller (page 7).
4	**Launch and log into the web UI** Using a supported web browser, go to http://localhost/oneguard/. Key in a domain administrator's credentials to log into the user interface. For more information, refer to Logging into GFI OneGuard (page 14).
5	**Run the post-install wizard** When launching the web UI the first time after installation, a post install wizard runs automatically to help you set up GFI OneGuard for first use. For more information, refer to Post-installation tasks (page 9).
6	**Start managing discovered devices** Devices within the network are automatically discovered by GFI OneGuard and added to the Discovered Devices area. Go to **Manage > Devices** and move discovered devices to groups to start managing them. For more information, refer to Groups and Devices (page 18).
7	**Start using the GFI OneGuard Services** Go to **Manage > Services**. The menu on the left shows the activated services. Use the right window to configure general settings and view licensing details, such as the number of devices currently being protected. For more information, refer to Services Offered (page 1). Once the services are enabled, you can run them directly from the widgets on the Home page or by going to **Manage > Devices**. Here you can run services either by group or per device.

2.1 GFI OneGuard system requirements

Computers running GFI OneGuard must meet or exceed the system requirements described below. GFI OneGuard can be installed on a physical, a virtual or a cloud environment.

2.1.1 Software requirements

Requirement	Description
64-bit operating system	Install the GFI OneGuard Platform and Controller on 64-bit versions of the following operating systems: » Windows Server 2016 Essentials, Standard or Datacenter » Windows Server 2012 R2 Essentials, Standard or Datacenter » Windows Server 2012 Essentials, Standard or Datacenter » Windows Server 2008 R2 Standard, Enterprise, Datacenter, or Itanium-based systems » Windows Server 2008 Standard or Enterprise » Windows 10 Pro or Enterprise » Windows 7 Professional, Enterprise or Ultimate » Windows Small Business Server 2011 » Windows Essential Business Server 2008 » Windows Small Business Server 2008
Fixed IP Address	The server where the GFI OneGuard Platform is installed requires a fixed IP address to ensure that no network communication breakdowns occur due to a changing address.
Domain	The server where the Platform is deployed must be joined to an Active Directory domain.
Supported browsers	The latest versions of these web browsers: » Google Chrome » Microsoft Internet Explorer 11 or Microsoft Edge » Mozilla Firefox » Safari
Internet Information Services (IIS)	Required to access the GFI OneGuard web interface. If not found, this is automatically installed by GFI OneGuard during installation.
Microsoft .NET Framework 4.5.1	Automatically installed during setup. If automatic installation fails, download setup from: https://www.microsoft.com/en-us/download/details.aspx?id=40779
ASP.NET 4.5.1	Required to access the GFI OneGuard web interface. If Microsoft® .NET framework is installed after IIS is installed, then ASP.NET is usually automatically registered. If not found, this is automatically enabled by GFI OneGuard during installation.

Supported databases

GFI OneGuard uses a database to store information retrieved from scans, audits, notifications, configuration and services data. This information is critical to the operation of GFI OneGuard and for reporting purposes. The database backend can be any of the following:

Database	Recommended Use
Microsoft SQL LocalDB	An embedded database installed automatically when installing the GFI OneGuard Platform. Adequate for small and medium installations containing up to 500 managed devices.
Microsoft SQL Server Express 2008 R2 or later editions	Recommended for networks containing up to 500 managed devices.
Microsoft SQL Server 2008 R2 or later versions	Recommended for larger networks of up to 10,000 managed devices.
Microsoft Azure SQL	A hosted database backend that is recommended for larger networks of up to 10,000 managed devices.

2.1.2 Hardware requirements

Computers hosting GFI OneGuard components must meet the following hardware requirements:

Component	Minimum requirement	Recommended minimum requirement
Processor	1.6 GHz Dual Core	2.1 GHz Quad Core
Physical Storage	2 GB hard disk space for the installation only	8 GB for the installation only
RAM	4 GB	8 GB

2.1.3 Firewall Ports

GFI OneGuard Platform communicates with Controllers and agents on managed devices using the ports below. The firewalls that control traffic between these machines need to allow requests on ports:

TCP Ports	Description
80	Listening port on GFI OneGuard Platform server, handling all Platform-Controller-Agents communications. This port can be customized from the Controller settings.
135	Remote WMI - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.
139	Remote Registry - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.
443	Listening Port on GFI OneGuard Platform server, accepting transfer of data from the Controller to the Platform.
445	Remote Registry - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.
8123	The Controller Bandwidth Saver feature listens to Agent requests on this port.

The GFI OneGuard Controller requires ICMP response on the internal network to be allowed:

» **Windows Firewall**. Ensure that in the **Windows Firewall with Advanced Security > Inbound Rules** the Rule `File Printer and Sharing(Echo Request - ICMPv4-In)` is allowed.

» **Third-party Firewalls**. These settings may vary according to the model of the firewall. Some firewalls exempt certain protocols or services. In those cases, you must enable ping. Some firewalls call the setting **Ping** or **Incoming Ping**. Others refer to it by its technical name, **ICMP Echo Reply**. Either way, allow this protocol.

2.1.4 Antivirus and backup software

Antivirus and backup scanning may cause GFI OneGuard to malfunction. This occurs when such software denies access to certain files required by GFI OneGuard.

Disable third party antivirus and backup software from scanning the installation folder of each component, which by default are:

Component	x64 default install path	x86 default install path
Platform	*..\Program Files\GFI\OneGuard*	Not supported
Controller	*..\Program Files (x86)\GFI\OneGuard*	*..\Program Files\GFI\OneGuard*
Agent	*..\Program Files (x86)\GFI\OneGuard*	*..\Program Files\GFI\OneGuard*

2.2 Planning GFI OneGuard deployment

When planning to install GFI OneGuard in your environment, there are various considerations that affect how the software gets deployed, such as network segmentation and size.

Go to http://go.gfi.com/?pageid=OneGuardHelp#cshid=deploy and fill in the form with your environment information to help you deploy GFI OneGuard.

2.2.1 Common deployment scenarios

There are many ways how to deploy GFI OneGuard. Deployment depends on various factors, such as the network infrastructure that needs to be managed, hardware considerations, number of devices to be managed, network segmentation and size.

Important notes:

» When planning the GFI OneGuard deployment, one should keep in mind that each Controller is capable of managing up to 1,000 devices. Use multiple Controllers to manage more devices.

» Controllers must always be installed within the physical network. Only the Platform component can be hosted within the cloud.

The following are some of the most common GFI OneGuard deployment scenarios:

GFI OneGuard Platform, Controller & Microsoft SQL LocalDB on same server

The most straightforward solution is to have everything on one server. This means installing GFI OneGuard Platform and Controller on the same machine. The Microsoft SQL LocalDB is installed automatically by GFI OneGuard. This solution is ideal for small installations, with a maximum of 500 devices.

GFI OneGuard Platform, Controller on one server, Microsoft SQL Server on a dedicated server

This scenario is recommended for organizations that already have a Microsoft SQL Server deployed within the network and have less than 1,000 network devices. GFI OneGuard Platform and Controller can be installed together on a machine that meets the minimum system requirements. Additional Controllers need to be installed on separate machines if the network is segmented into sub-networks or if your total number of managed devices exceeds 1,000.

GFI OneGuard Platform on a cloud service, Azure SQL & Controller on premise

GFI OneGuard Platform can be deployed in cloud-based platforms such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform. It can also be connected to a hosted SQL server such as Microsoft Azure SQL. Controllers need to be installed on machines within the physical network. The Controllers communicate with the hosted Platform. This solution is ideal for organizations that already have an existing cloud infrastructure, for organizations that want to benefit from the features of a hosted solution, or organizations that do not want to invest in new hardware.

GFI OneGuard Platform on a server, Controller on separate server & Microsoft SQL Server on dedicated server

This solution is ideal for medium sized organizations that plan for scalability and want the best performance. Additional Controllers can be added as the organization scales out.

2.3 Downloading the latest version of GFI OneGuard

To download the latest version release of GFI OneGuard:

» Go to https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-oneguard/try-now

» If you have an existing GFI Customer account, click **Login** and key in your Username and Password. Or, if you do not have a GFI Customer account, fill in the form details to register for an account.

» Next, go to the GFI OneGuard downloads page and start downloading the latest version of GFI OneGuard.

2.4 How to install the GFI OneGuard Platform and Controller

The GFI OneGuard Platform and Controller components share the same installation file. Run the installation file on a machine that meets or exceeds the GFI OneGuard system requirements. For more information, refer to GFI OneGuard system requirements (page 3).

To install the GFI OneGuard Platform, Controller or both:

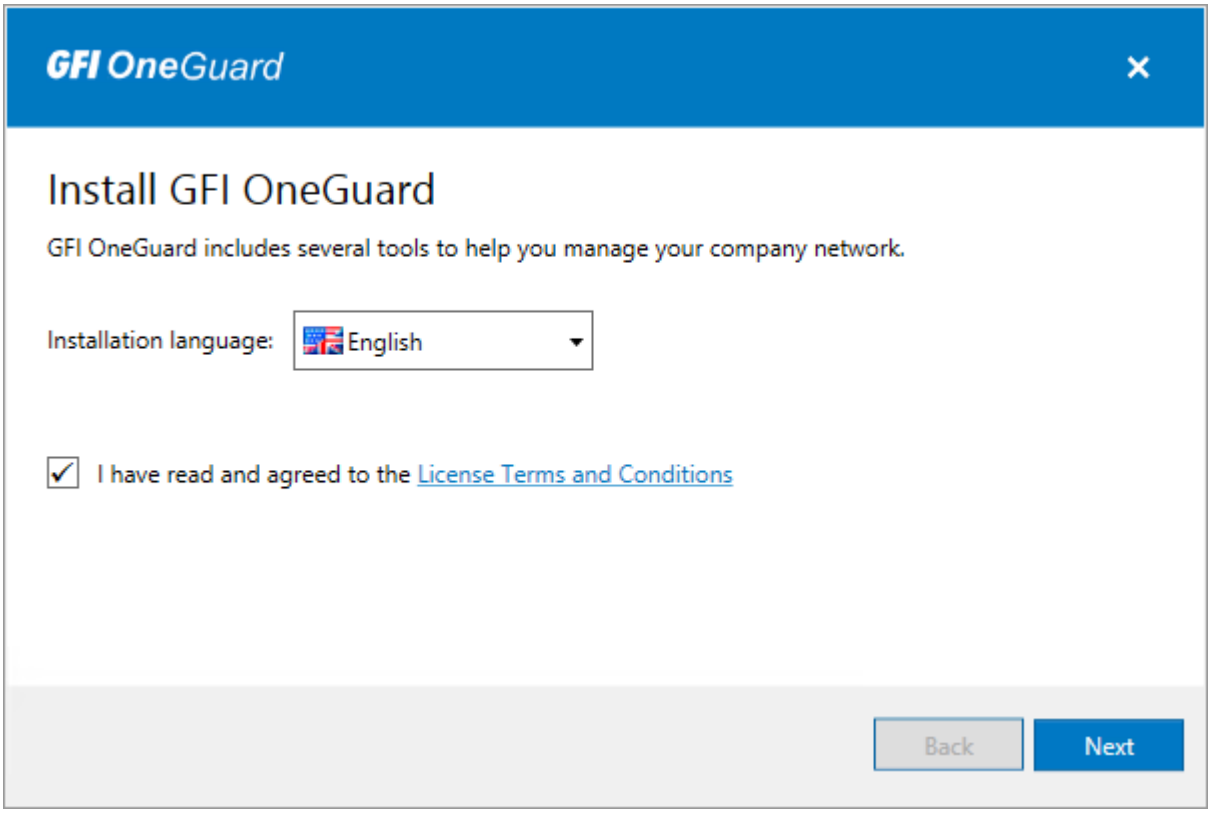
1. Go to http://go.gfi.com/?pageid=og_trial and sign up for GFI OneGuard. After your account is created, you are automatically redirected to a download page from where you can download the installation file.

2. Log in to the server using an account with administrator privileges.

3. Download the GFI OneGuard installation file to the server.

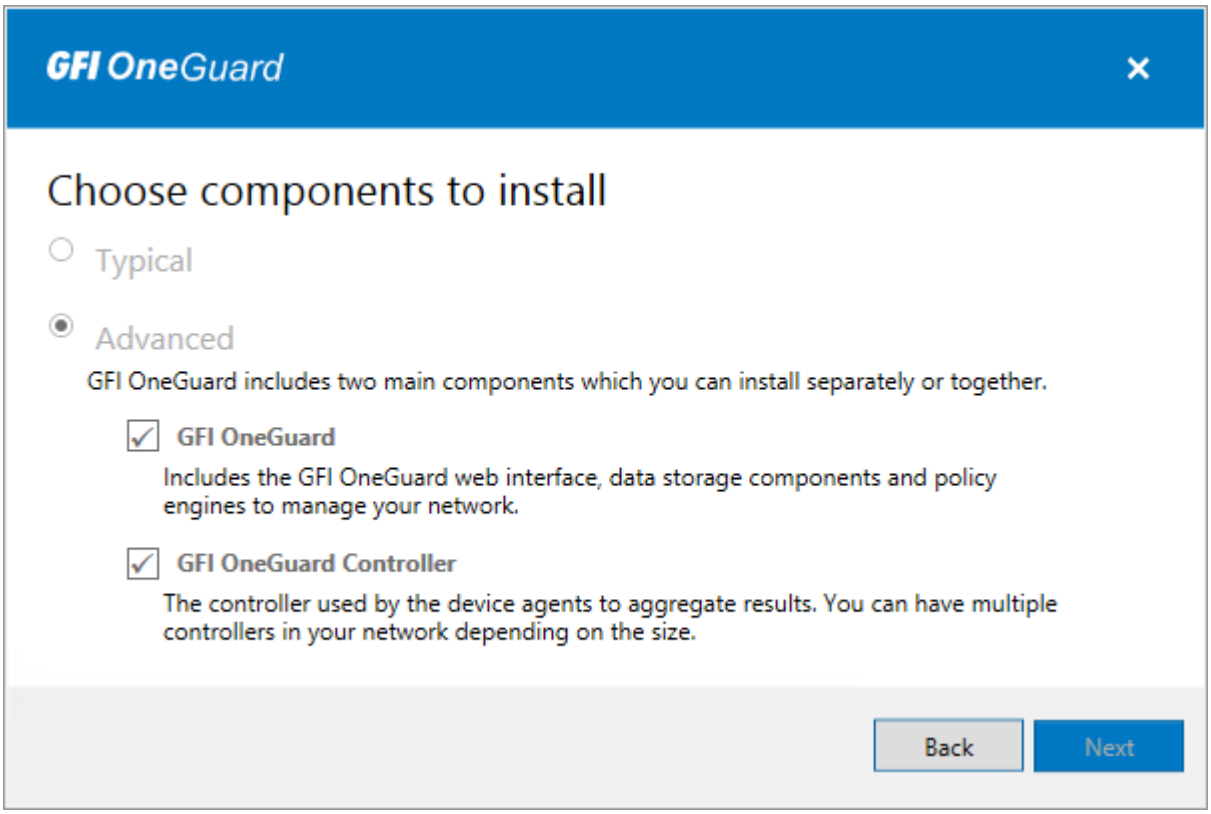
4. Before running the wizard, right-click the installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

5. Double-click the downloaded installation file.



Screenshot 1: License agreement

6. Read the license agreement and if you agree, select **I have read and agreed to the License Terms and Conditions**. You must agree to the License Terms and Conditions to proceed with the wizard. Click **Next**.

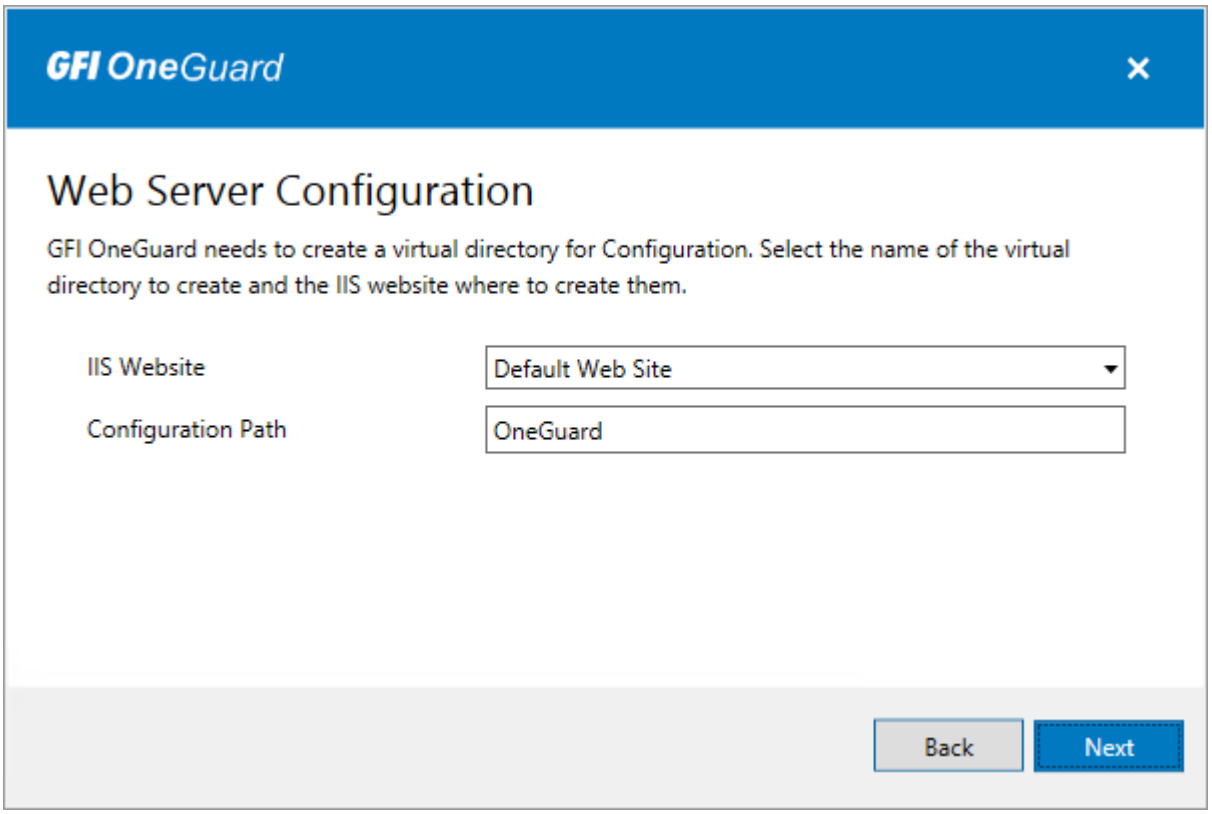


Screenshot 2: Select which components to install

7. To install both the GFI OneGuard Platform and Controller, choose **Typical**. Otherwise, click **Advanced** and select which component to install. Note that when running the installer on a 32-bit system, only the Controller can be installed. The Platform can only be installed on 64-bit systems. Click **Next**.

8. The installer verifies that the server meets the GFI OneGuard requirements. Any missing components are downloaded and installed automatically.

9. Choose the installation directory or install to the default directory. The default directory is: `C:\Program Files\GFI\OneGuard`. Click **Next**.



Screenshot 3: Configure virtual directory settings

10. Choose the **IIS Website** where to host the GFI OneGuard virtual directory and key in a name for the virtual directory, which by default is **OneGuard**. Take note of this configuration to help you identify the correct URL to use when launching the application from other computers. Click **Next**.

11. Click **Install** to start the installation.

12. Click **Finish** on install completion.

After the installation is complete, GFI OneGuard launches the post installation wizard. For more information, refer to Post-installation tasks (page 9).

2.5 Post-installation tasks

As soon as installation is complete, GFI OneGuard launches the post-installation wizard which enables you to configure basic settings that are required to start using the product.

> **IMPORTANT**
> The post install wizard only runs when GFI OneGuard is first installed and cannot be re-launched after the initial run. Some of the settings configured during this wizard cannot be altered after the initial setup, such as the database and company details. Ensure that they are properly configured first-time round.

In the login screen, enter the credentials of an administrator that is a member of the Domain Administrators group. Other domain users can be configured to access the GFI OneGuard web interface at a later stage. For more information, refer to Roles and Permissions (page 88).

When logged in, go through the following wizard steps:

Task	Description
Connect to GFI Account	GFI OneGuard needs a GFI Account to operate. Key in the credentials that you used when signing up and click **Next**. Click **Don't have an account?** to sign up for a new account with GFI Software. Click **Forgot password?** if you have forgotten the password of your existing account. This setting can be modified or entered at a later stage from **Settings > License**.
Company network details	The name of the company network that will be managed by GFI OneGuard. This will appear on the home page of the GFI OneGuard console. Note that this name cannot be changed after GFI OneGuard is up and running.
Select Administrators Group	By default, members of the Active Directory Administrators Group can access the Platform. Different levels of permissions can be assigned to different users or groups. For more information, refer to Roles and Permissions (page 88).

Database setup	Select the database where to store GFI OneGuard data. Note that this setting cannot be changed after GFI OneGuard is up and running.
	During installation, GFI OneGuard automatically installs a Microsoft SQL LocalDB database that can be used for networks of up to 1,000 devices.
	To use another existing database, such as a Microsoft SQL Server or a Microsoft Azure SQL database, click **Advanced**. For each entry shown, create a database manually on your database server and enter the connection string for each database. The connection string must be in the following form:
	`Server=<ServerAddress>\<InstanceName>; Database=<DatabaseName>; User Id=<Username>; Password=<Password>;`
	Replace the following fields as follows:
	» `<ServerAddress>` - The fully-qualified domain name or IP address of the database server.
	» `<InstanceName>` - The name of the SQL instance. This is the same instance name used when logging into the database server.
	» `<DatabaseName>` - The name of the dedicated database.
	» `<Username>` - The username of an account with full permissions on the database specified.
	» `<Password>` - The password of an account with full permissions on the database specified.
	For example:
	`Server=mydbserver.example.com\myInstance; Database=NotificationsDB; User Id=sa; Password=password123;`

Click **Finish**.

2.6 Upgrading to the latest version while retaining all settings

Learn how to upgrade GFI OneGuard to the latest version while retaining all settings.

2.6.1 Important notes when upgrading

» Upgrade is not reversible; once upgraded you cannot downgrade to the previous version.

» Backup the GFI OneGuard configuration before upgrade. For more information, refer to How to backup GFI OneGuard configuration (page 97).

» It is not necessary to upgrade the GFI OneGuard Agent on end-user machines when upgrading the GFI OneGuard server installation.

» Check that the machine being used for GFI OneGuard upgrade meets the latest system and hardware requirements. For more information, refer to GFI OneGuard system requirements (page 3).

» Log on as Administrator or using an account with administrative privileges.

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

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

2.6.2 Upgrade Procedure

1. Download the latest build of GFI OneGuard. For more information, refer to Downloading the latest version of GFI OneGuard (page 6).

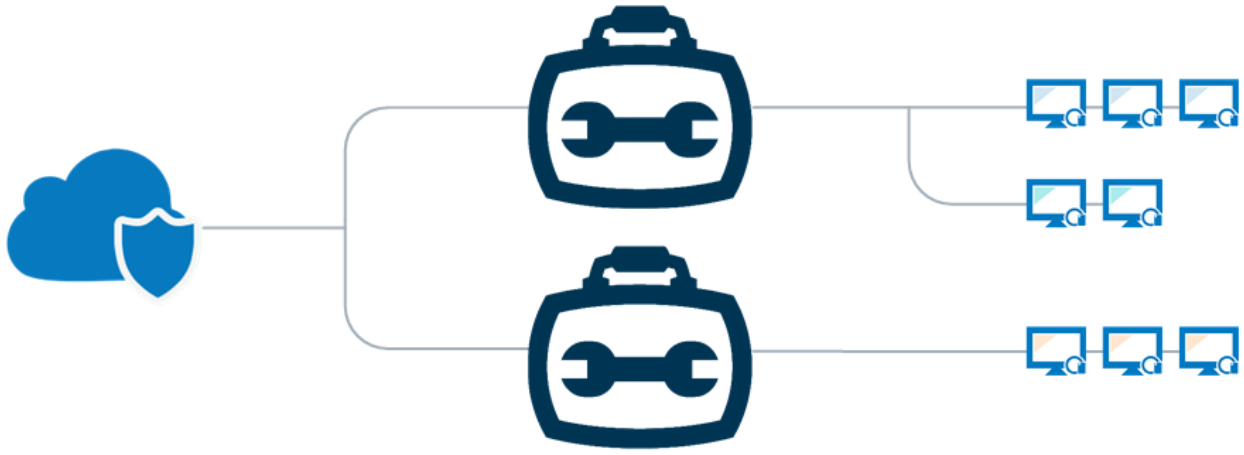
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

3. Launch the newly downloaded installer on the server where GFI OneGuard is currently installed and follow on-screen instructions to upgrade.

4. Once the upgrade completes, test your upgraded setup by logging in to GFI OneGuard Platform using your existing credentials. For more information, refer to Logging into GFI OneGuard (page 14).

2.7 The GFI OneGuard Controller

The GFI OneGuard Controller is an installable component of GFI OneGuard that manages communication between the Platform and Agents. Its main roles are to execute network discovery and to relay instructions between the Platform and the Agents that it manages. It also caches and distributes virus definitions and patches to reduce bandwidth usage and costs between the Platform and the Agents.



Screenshot 4: Multiple GFI OneGuard Controllers

All network devices managed by GFI OneGuard must communicate with at least one GFI OneGuard Controller. In typical and small installations, the Controller is installed on the same machine as the GFI OneGuard Platform and is installed automatically when choosing **Typical** deployment type when running the installation wizard.

You may also have, however, other Controllers deployed over the network, with each Controller able to communicate with both the Platform and the devices that it manages. Multiple Controllers are required when:

» A company's network is segmented in a number of sub-networks, where sub-networks cannot communicate with each other. Multiple Controllers will be required to manage the communications with the Platform of each sub-network.

» The number of Windows devices to manage exceeds 1,000. Given that a single Controller is able to handle up to 1000 devices, multiple Controllers can increase the amount of managed devices. (Note that the Platform can only manage up to 10,000 devices)

» The network is segmented in different physical and geographical sites. A Controller is deployed at each site so that communications between the Controller and the Agents are done within each individual site, minimizing communications over the internet.

» Different areas of the network are managed by different user accounts, for example when having multiple domains or having a workgroup outside your domain. Each Controller can be configured to deploy agents using a particular user account. If there is no single account that can manage all the devices connected to a Controller instance, then you need to deploy multiple Controllers and configure a different user account on each Controller.

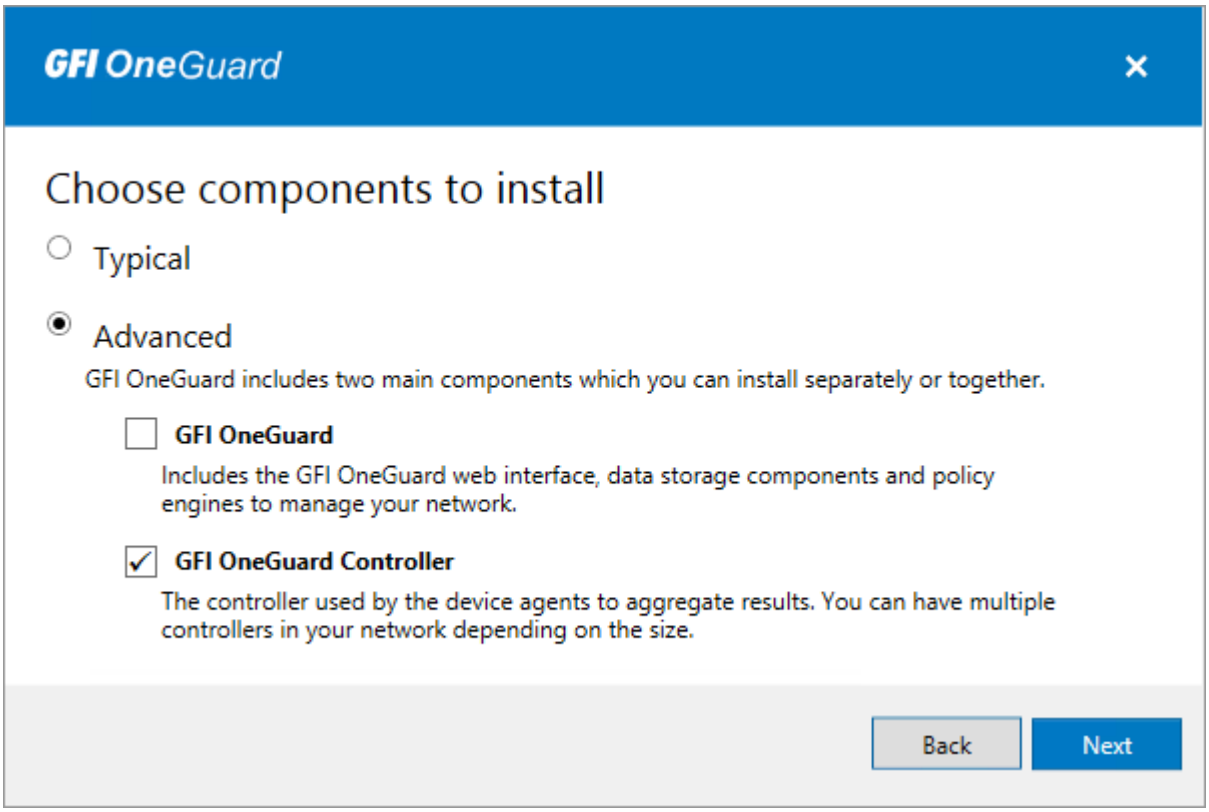
2.7.1 Installing the GFI OneGuard Controller

Controllers do not have to be installed on the same domain as the Platform and can be installed on a different site, domain or workgroup, as long as the Controller can be configured to communicate with the Platform. However, a Controller must always reside on a virtual or physical machine within the same network as the Agents connected to it.

The GFI OneGuard Platform and Controller components share the same installation file. Before starting the installation, confirm that the machine where you are going to install the Controller meets the following requirements:

Requirement	Description
Operating system	Install the GFI OneGuard Controller on any of the following 32-bit or 64-bit operating systems: » Windows Server 2016 Essentials, Standard or Datacenter » Windows Server 2012 R2 Essentials, Standard or Datacenter » Windows Server 2012 Essentials, Standard or Datacenter » Windows Server 2008 R2 Standard, Enterprise, Datacenter, or Itanium-based systems » Windows Server 2008 Standard or Enterprise » Windows 10 Pro or Enterprise » Windows 7 Professional, Enterprise or Ultimate » Windows Small Business Server 2011 » Windows Essential Business Server 2008 » Windows Small Business Server 2008
Microsoft .NET Framework 4.5.1	Automatically installed during setup. If automatic installation fails, download setup from: https://www.microsoft.com/en-us/download/details.aspx?id=40779
Network communications	The GFI OneGuard Controller can be installed on a physical or a virtual network that communicates with the Platform via an internal or external network. By default, Controller-Platform communications are done on port 80, or port 443 if using a secure connection. The Controller can also be configured to connect to the Platform via a proxy.
Antivirus and backup software	Antivirus and backup software may cause the Controller to malfunction. This occurs when such software denies access to certain files required by it. Disable third party antivirus and backup software from scanning the installation folder of the Controller, which by default is: » *..\Program Files (x86)\GFI\OneGuard* (on 64-bit systems) » *..\Program Files\GFI\OneGuard* (on 32-bit systems)

To install the Controller, run the GFI OneGuard installer and follow the wizard as described in this topic. When asked to choose the components to install, click **Advanced** and select **Controller** to install just the Controller.



Screenshot 5: Installing the Controller

When the installation is complete, the Controller is loaded and runs minimized in the system tray. If the Controller is installed on a different site, domain or workgroup than the Platform, additional configuration is required for the Controller to communicate with the Platform. For more information, refer to Controller configuration (page 93).

2.8 GFI OneGuard Agents

An Agent is a small footprint service that is automatically installed on devices that are managed by GFI OneGuard. The purpose of the Agent is to send information about the host machine to the GFI OneGuard Controller. The Controller then pushes this information to the GFI OneGuard Platform. Any actions pushed from the Platform to the managed devices are executed via the Agents. Actions can include the installation of updates for software installed on a managed device, an AV scan, or even a shutdown command. For more information, refer to How it works (page 1).

Agents can be installed on machines that meet or exceed the following requirements:

With EPC service

Requirement	Description
32-bit or 64-bit operating system	GFI OneGuard Agents can be automatically deployed on all machines running Windows operating system, from Windows 7 or newer and Windows Server 2008 or newer.
Environment	» GFI OneGuard Agents can be installed on a physical or a virtual environment within a network. » The Agent communicates with Controller via port 80 or 443. » Ensure that KB3033929 is installed - https://www.microsoft.com/en-us/-download/details.aspx?id=46148

Without EPC service

Requirement	Description
32-bit or 64-bit operating system	GFI OneGuard Agents can be automatically deployed on all machines running Windows operating system, from Windows Vista or newer and Windows Server 2003 or newer.
Environment	GFI OneGuard Agents can be installed on a physical or a virtual environment within a network. The Agent communicates with Controller via port 80 or 443.

2.8.1 GFI OneGuard Agent installation and removal

Agent installation is done automatically by the Controller when a device is added to the GFI OneGuard managed devices list in the Platform. For more information, refer to Assigning devices to groups (page 22). Installation is silent, meaning that users are not interrupted.

When devices are removed from a group, the Agents on the affected machines are automatically uninstalled. For more information, refer to Removing a managed device (page 24).

2.9 Logging into GFI OneGuard

Domain administrators where GFI OneGuard is installed can log in to the Platform to manage devices, manage services, configure software and monitor functionality.

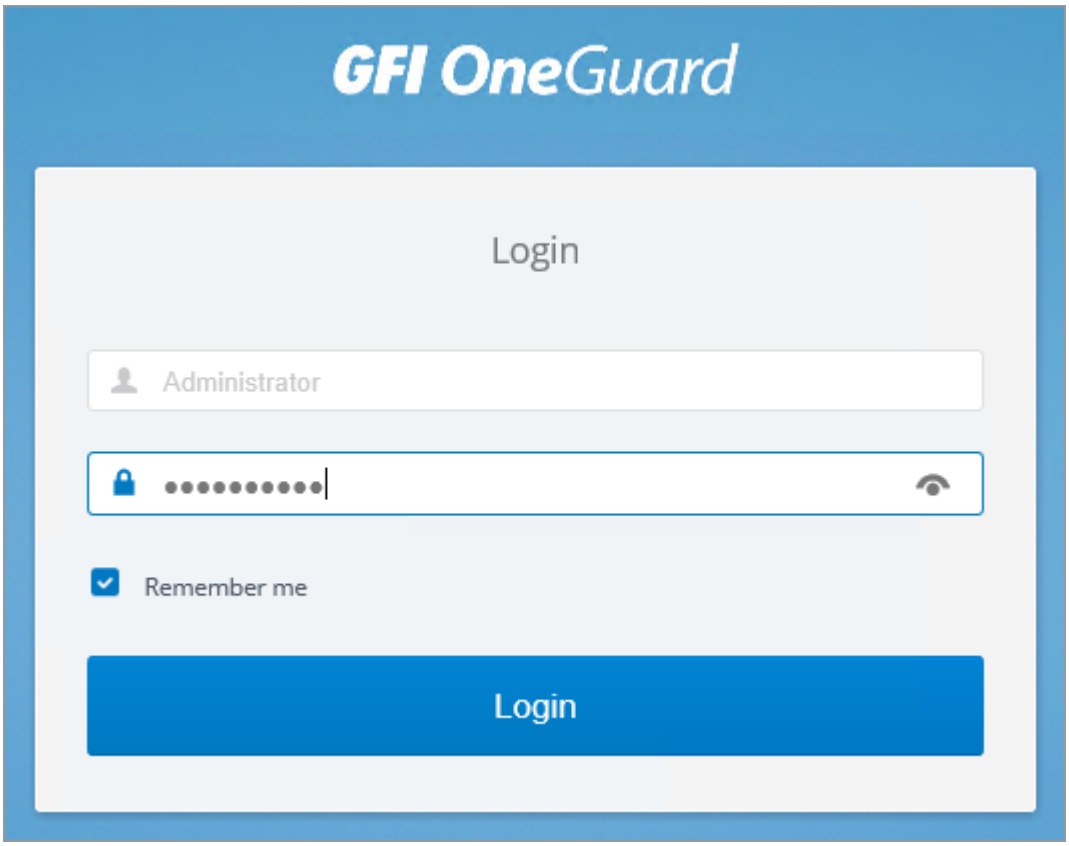
To start exploring and configuring GFI OneGuard, launch the web interface in your browser, keying in the following URL:

`http://<GFI OneGuard host name>/<GFI OneGuard virtual directory>`

Replace `<GFI OneGuard host name>` with the name of your server and `<GFI OneGuard virtual directory>` with the name that you assigned to the GFI OneGuard virtual directory during installation (default value is `OneGuard`).

For example: `http://myserver.mydomain.com/OneGuard`

If launching the Platform from the same machine where GFI OneGuard is installed, you can also use `http://localhost/OneGuard`.



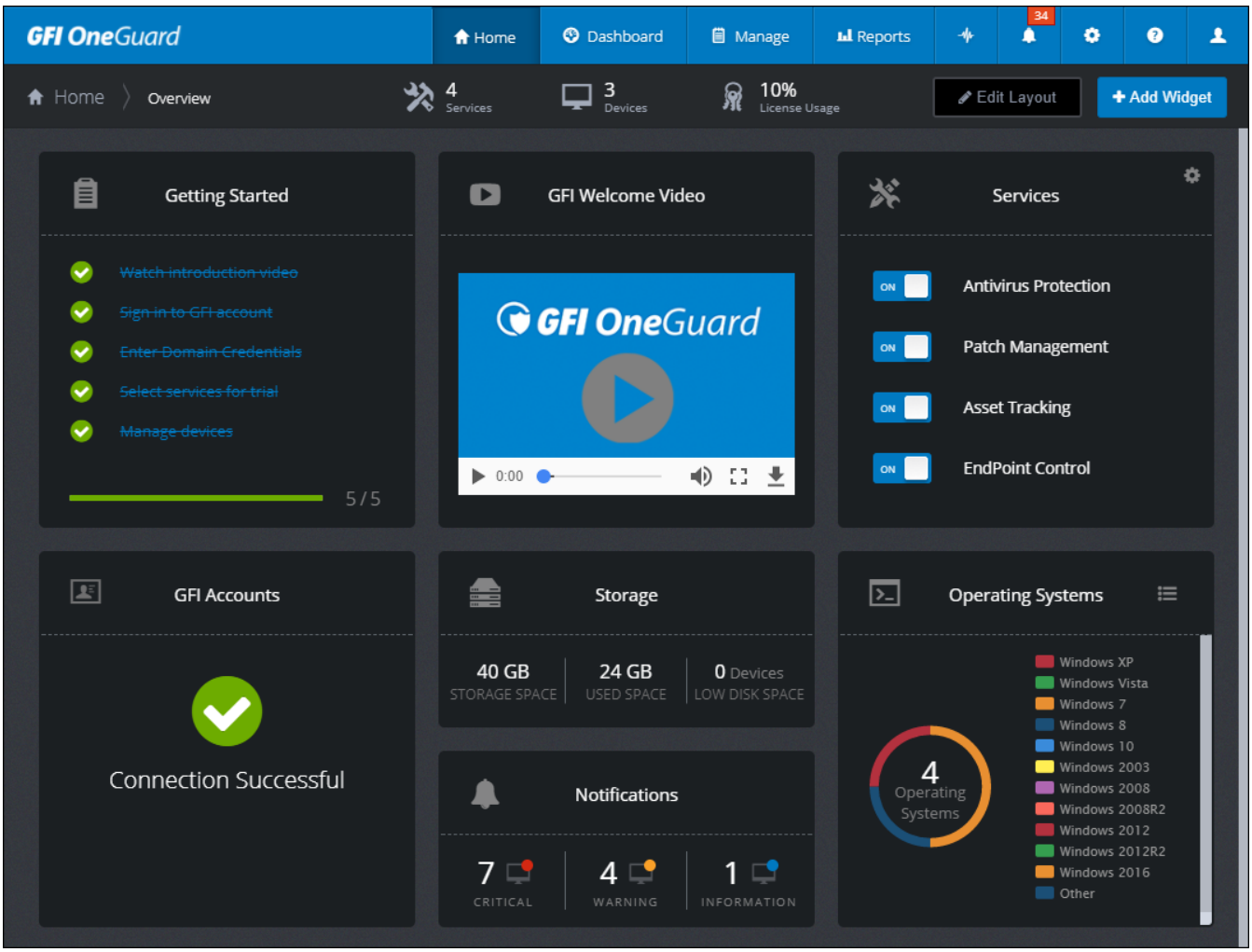
Screenshot 6: Key in credentials to login

Enter the credentials of a user with permissions to access GFI OneGuard. Usually users from the domain administrators group have access to the UI, but the permissions can be customized by installation. For more information, refer to Roles and Permissions (page 88).

> **NOTE**
> When logging in for the first time, GFI OneGuard runs the post-install wizard. For more information, refer to Post-installation tasks (page 9).

3 Using the GFI OneGuard Platform

To start using GFI OneGuard, log in to the web console from a browser on any machine on the network.



Screenshot 7: The GFI OneGuard home page

When logged in, use the top navigation bar to go to the required screen:

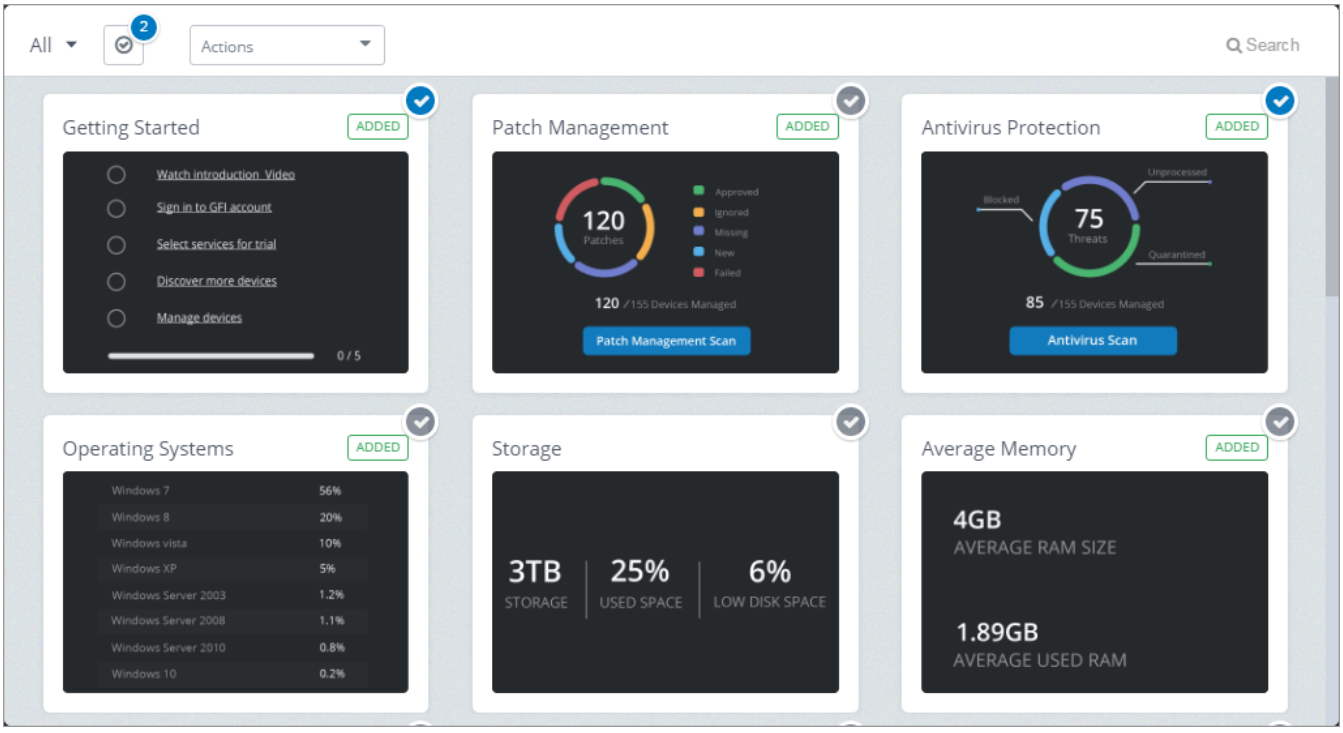
Option	Description
Home	The **Home** screen provides a high-level overview of the network status and GFI OneGuard operation. For more information, refer to Home page (page 17).
Dashboard	Provides dashboards to monitor the different services offered by GFI OneGuard: » **Patch Management** - An overview of the Patch Management service. For more information, refer to Patch Management (page 31). » **Antivirus Protection** - An overview of the Antivirus service. For more information, refer to Antivirus (page 37).
Manage	Use this node to customize and configure network devices and the services offered by GFI OneGuard: » **Devices** - Track and configure the devices managed in GFI OneGuard. For more information refer to Devices. » **Services** - View and configure services according to the plan that you purchased. For more information, refer to Services Offered (page 1).
Reports	Generate reports that provide insight on GFI OneGuard operation. For more information, refer to Reports (page 70).

Option	Description
Activity	Shows a list of jobs being done by the agents in real-time. Use the left pane to filter jobs by status. For more information, refer to Activity Monitor (page 78).
Notifications	A list of notifications issued by GFI OneGuard providing critical and important alerts that require attention. Use the left pane to filter settings by type or severity. For more information, refer to Notifications Area (page 79).
Settings	Settings related to the setup and functionality of GFI OneGuard. From the left pane choose the settings to configure and apply the necessary changes. For more information, refer to System settings (page 81).
Help	Find resources to help you use, configure and troubleshoot GFI OneGuard, such as this help system.
Profile	Use this tab to launch your profile preferences or to sign out. In the profile preferences screen, you may change your account password, the interface language and the display theme. For more information, refer to User profile settings (page 92).

3.1 Home page

The GFI OneGuard Home page offers a customizable view of all the operations and processes carried out by GFI OneGuard. The view is organized in widgets that can be moved around, added or removed according to preference. Additionally, some of these widgets enable you to perform actions directly from this dashboard, giving you total control of the network from a single console.

To move or remove a widget, click **Edit Layout** from the toolbar or click the settings icon in the upper right corner of the widget. To add a widget, click **Add Widget** from the toolbar and select from the widget menu.



Screenshot 8: Managing home page widgets

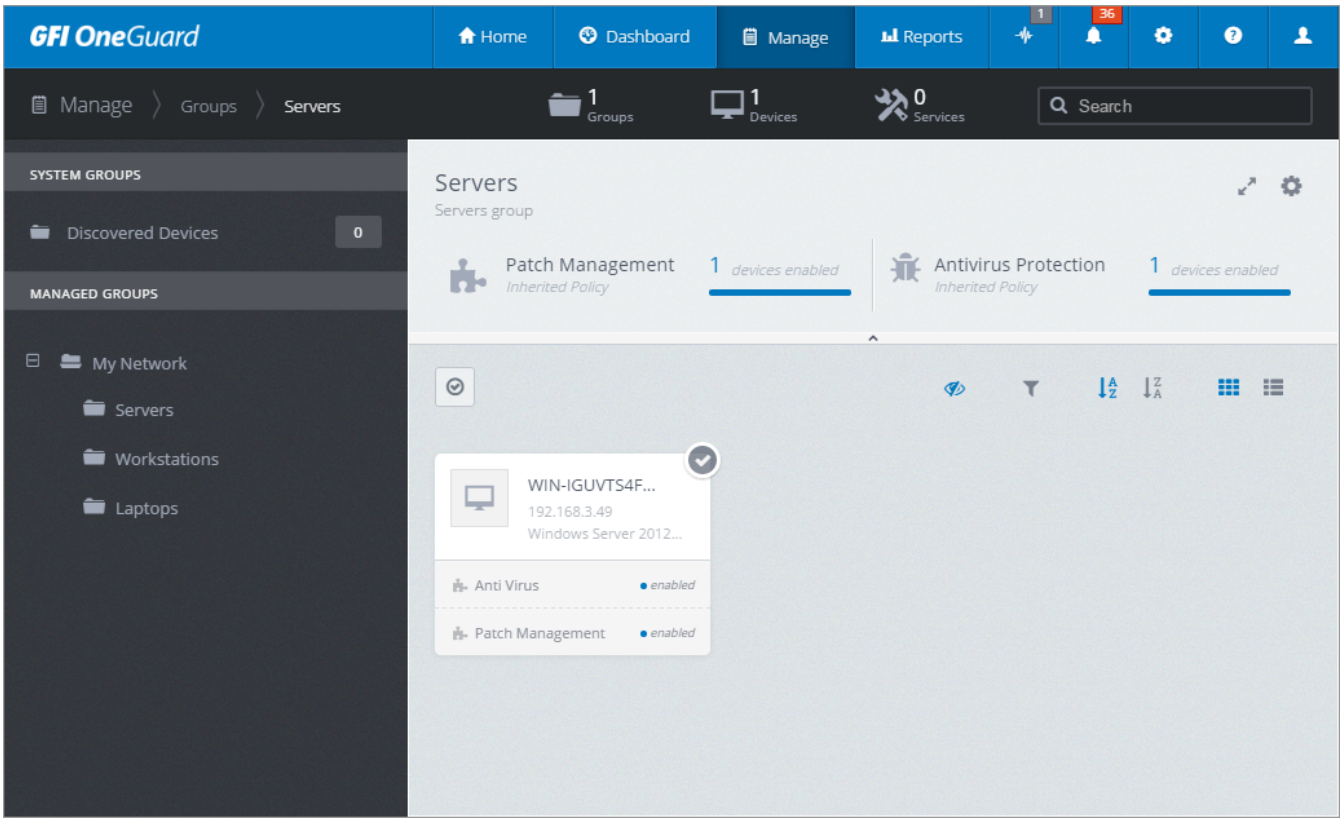
The following is a list of available widgets:

Widget	Description
Getting Started	A list of tasks to get you started with your GFI OneGuard deployment. When a task is completed it will be marked as complete. Ensure all these tasks are performed.

Widget	Description
GFI Welcome Video	A video that gives you an overview of GFI Software and the products it offers.
Services	Lists the active Services in GFI OneGuard. These depend on your subscription. You can enable or disable available services directly from this widget by simply clicking the switch next to the service.
Domain Credentials	Administrator Credentials used for any operation carried out by GFI OneGuard on client machines within int network, such as installing an Agent.
GFI Accounts	Shows the connection status of the GFI account synced with GFI OneGuard. If the connection is disabled, services will not be available.
Activity	Activity refers to jobs such as antivirus scans or patch installations. The widget shows the number of jobs that are pending, currently running or those that failed. For more information, refer to Activity Monitor (page 78).
Patch Management	This widget provides some basic information related to the Patch Management service, such as total number of patches deployed on managed devices and the Approved, Ignored or Missing patches. Click **Patch Management Scan** to run a new scan directly from the home page. For more information, refer to Run Patch Services on a Device (page 35).
Network status	Lists the number of deployed controllers, the number of managed devices and the number of devices that have been discovered but are not being managed by GFI OneGuard.
Generated reports	The number of reports generated by the system. For more information, refer to Reports (page 70).
Average Apps / Browsers	The average number of apps and browsers monitored by GFI OneGuard.
Notifications	Lists the number of notifications sent by GFI OneGuard in order of priority: Critical, Warning or Information. For more information, refer to Notifications Area (page 79).
Storage	The average hard drive storage size and the average storage usage of managed devices. The widget also shows the number of devices with low disk space.
IP/MAC Address	The number of IP and MAC addresses of devices managed by GFI OneGuard.
Product updates	Information about the current GFI OneGuard version and when it was last updated.
Ram information	The average memory size and the average memory usage of managed devices.
Operating systems	A list of the different Operating Systems on devices managed by GFI OneGuard. Toggle between a pie chart and list view using the control in the upper right hand corner of the widget.
Antivirus protection	Displays the total number of threats discovered by the Antivirus service. Click **Antivirus scan** to run a new scan directly from the home page. For more information, refer to Antivirus (page 37).

3.2 Groups and Devices

GFI OneGuard periodically scans the network to discover devices joined to it. All discovered devices can be remotely managed in GFI OneGuard. To access the list of discovered devices, from the top navigation bar, go to **Manage > Devices**.



Screenshot 9: Managing and configuring devices

The left pane contains groups in a hierarchical structure. Devices can be added to these groups to apply the group settings on the devices. Click any group to display the list of devices within that group in the right pane. Use the right pane to monitor and configure individual devices in the selected group. Use the icon bar in the right corner to filter and sort devices, show or hide configured services and to change device view.

Start by choosing a group from the left pane:

Group	Description
Discovered Devices	This group contains a list of discovered devices that are not yet managed by GFI OneGuard. To start managing these devices, drag and drop a device onto a group under **Managed Groups**. Alternatively, select one or more devices and in the actions bar, click **Move devices**. Choose the group and click **OK**.
All groups under Managed Groups	These groups contain devices that are managed by GFI OneGuard through the Agent. Each group has a custom set of settings configured and applied on all the devices that are joined to the group. The hierarchical structure allows certain settings to be inherited from parent groups. When a device is added to a group, GFI OneGuard Agents are automatically installed on that device.

IMPORTANT

When another third-party antivirus software is found on a device managed by GFI OneGuard that has antivirus protection enabled, the third-party antivirus software is automatically uninstalled by the GFI OneGuard agent. Note that this may require a reboot of the device.

Actions that can be performed on GFI OneGuard groups:

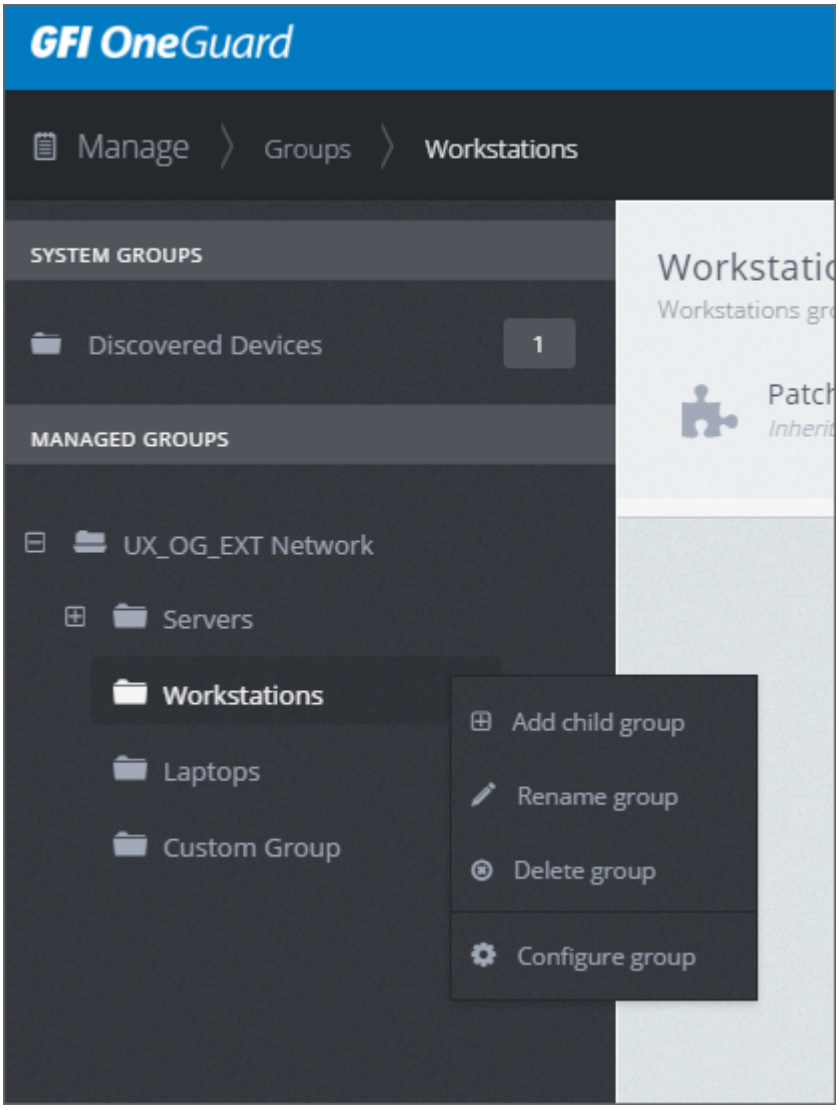
3.2.1 Adding new groups 20

3.2.2 Group settings 21
3.2.3 Assigning devices to groups 22
3.2.4 Moving Devices between groups 23
3.2.5 Manually running a service on devices 23
3.2.6 Renaming a group of devices 24
3.2.7 Deleting a group 24
3.2.8 Removing a managed device 24

3.2.1 Adding new groups

To add new groups of devices in GFI OneGuard:

1. Log in to GFI OneGuard and go to **Manage > Devices**.



Screenshot 10: Adding a child group

2. In the left pane, under **Managed Groups**, hover mouse over the group which will be the parent of the new group, click the pulldown menu arrow and click **Add child group**.

3. Key in a group name and click **OK**.

The new group is now added in the hierarchy. New groups automatically inherit the settings of the parent node. You may override the inherited settings by applying custom group settings and add devices to the group.

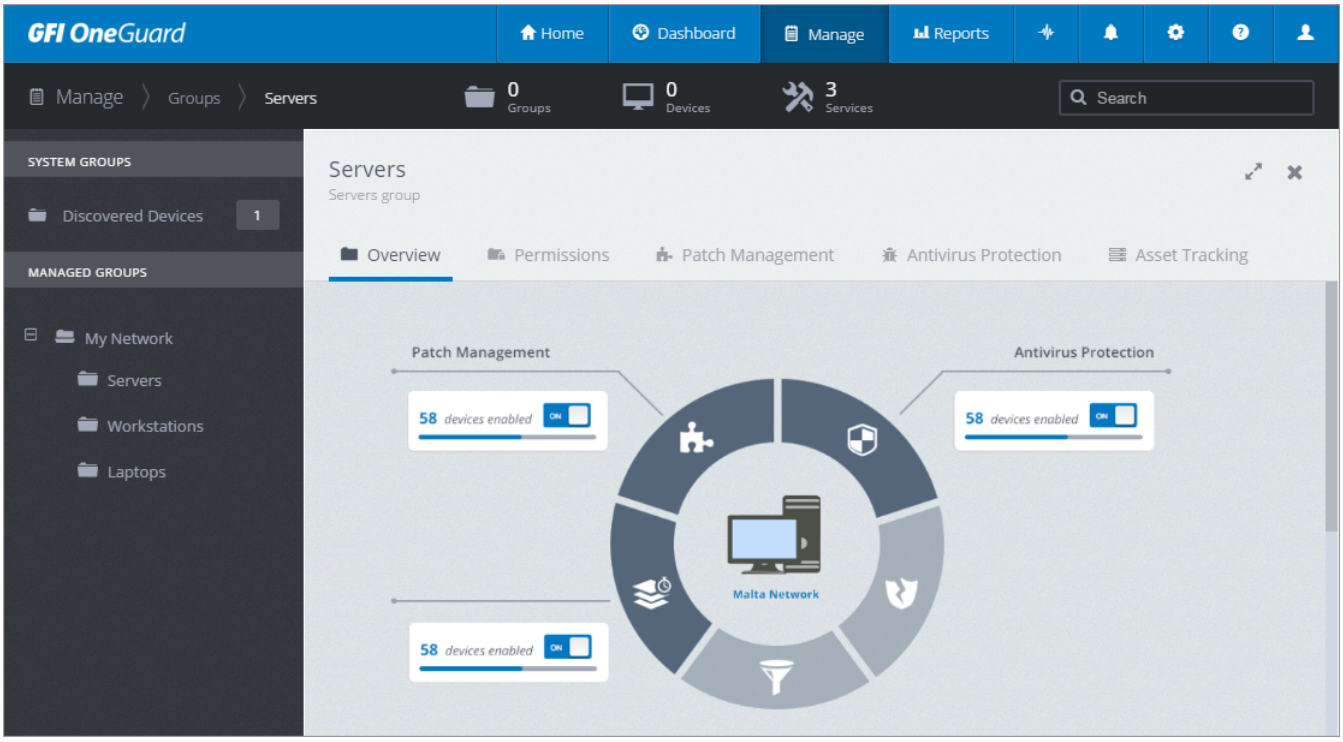
3.2.2 Group settings

In GFI OneGuard, groups are made of devices, where settings applied to them. GFI OneGuard applies the settings configured within the group to the devices that are members of that group.

To customize the settings of a group:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. From **Managed Groups**, hover mouse over the group to configure, click the pulldown menu arrow and click **Configure group**.



Screenshot 11: Configuring Group settings

3. Access the different tabs to configure settings:

Screen	Description
Overview	Shows the status of devices in this group. The Latest Notifications area displays events related to GFI OneGuard services, such as failed Agent deployments or newly discovered devices. Links to perform further actions are available on each notification, for example, when reinstalling an Agent or managing a newly discovered device.
Permissions	Displays the users that have been granted permissions to manage the selected group. Click **Roles and Permissions** to access the Roles and Permissions area and configure permissions.

Screen	Description
Patch management	Enable or disable patch management for this group using the ON/OFF switch. If enabling this feature, configure patch management options. For more information, refer to Configuring Patch Management on a Group (page 32).
Antivirus Protection	Enable or disable antivirus protection for this group using the ON/OFF switch. If enabling this feature, configure antivirus options. Depending on the action chosen, the antivirus agent gets installed or uninstalled on managed devices. When installing or uninstalling the antivirus agent, a reboot of the target computer may be required to complete the action. For more information, refer to Configuring group antivirus protection (page 39).
Asset Tracking	Enable or disable asset tracking for this group using the ON/OFF switch. If enabling this feature, specify schedule settings for when GFI OneGuard scans the network for asset information.

Certain settings have the option **Inherit policy from parent group**. When this option is selected, settings are not configurable and are inherited from the parent group. To override settings inherited from parent group uncheck the **Inherit Policy from parent group** checkbox and configure available options.

Click **Save Settings** to apply changes on all devices in the group.

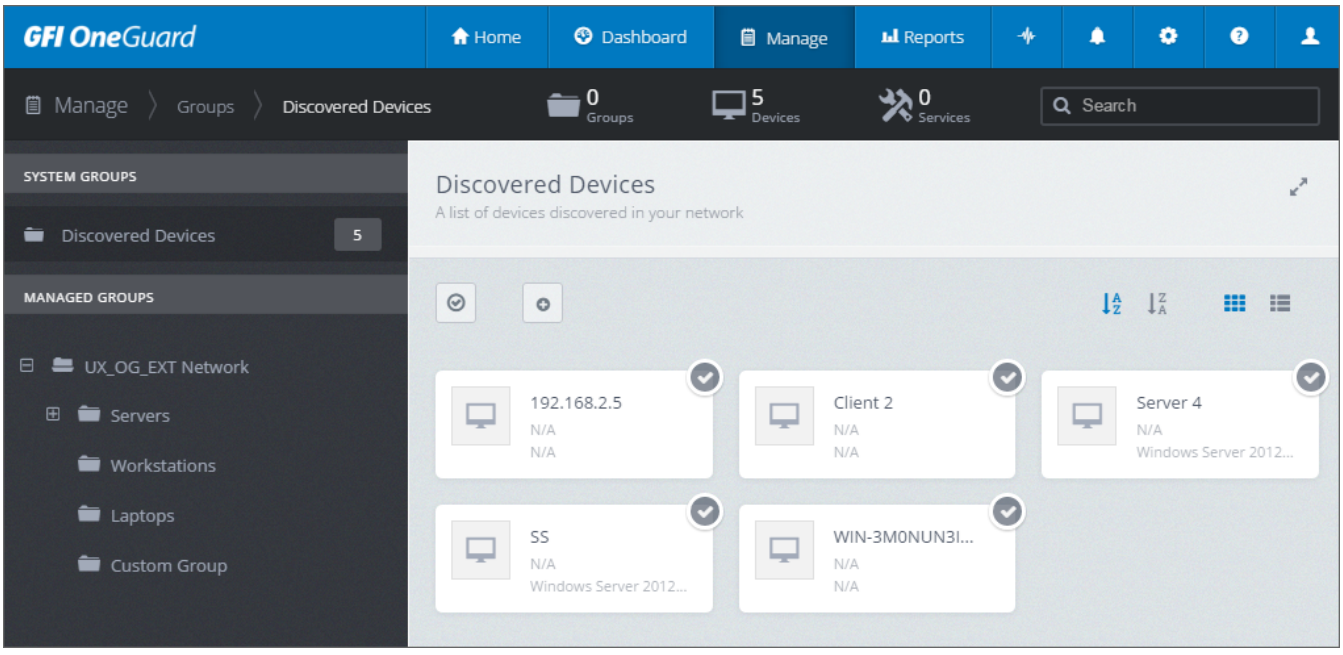
3.2.3 Assigning devices to groups

The **Discovered Devices** area contains a list of devices discovered on the network by the Controllers, but which are not managed in GFI OneGuard. To start managing your devices, add them to a group so that the devices inherit the group settings.

To add a discovered device to a group:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. Click **Discovered Devices** in the left pane to show the list of discovered devices in the right pane.



Screenshot 12: Discovered Devices List

3. Drag a device onto a group. To move multiple devices, select the devices to move and click **Move devices**. Choose the group to add the device to and click **OK**.

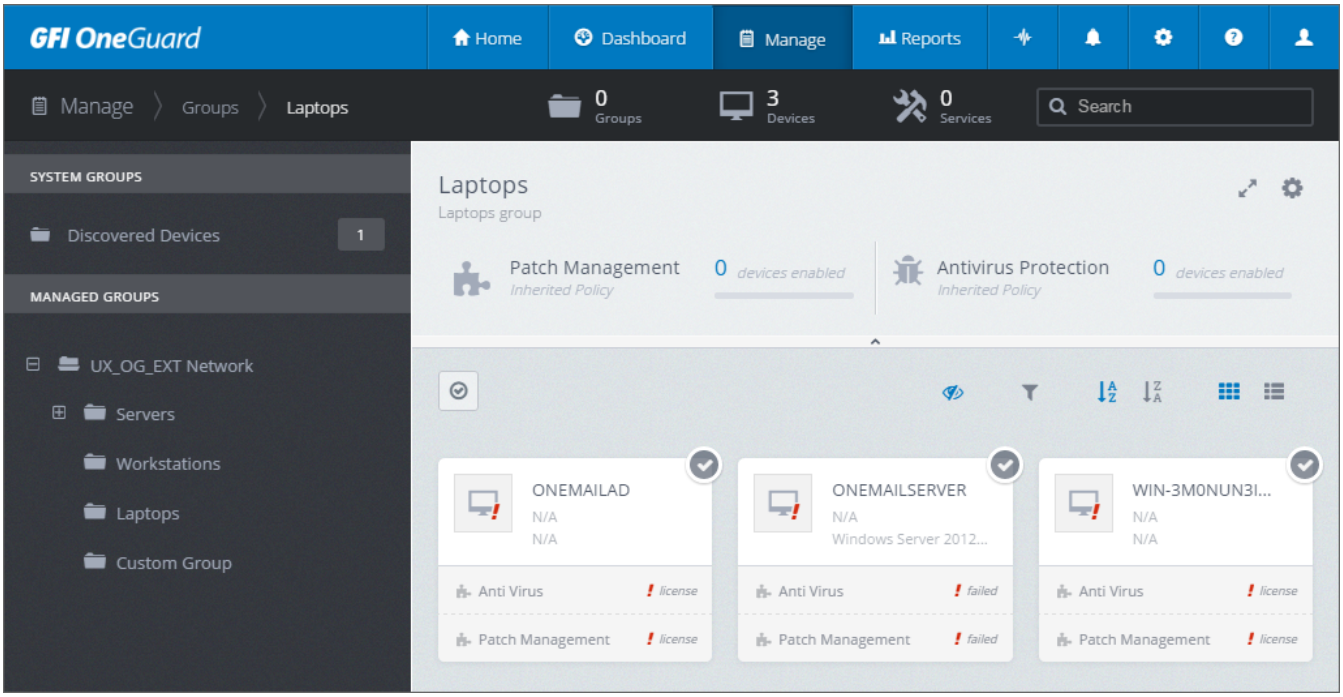
GFI OneGuard now attempts to install the agent on the device and starts applying the group settings.

3.2.4 Moving Devices between groups

To move a device from one group to another:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. From **Managed Groups**, choose the group where the device is located to show the list of devices in the group in the right pane.



Screenshot 13: Select devices to move

3. Drag device and drop it on the group where you want to move it to. To move multiple devices, select the devices to move and click **Move devices**. Choose the group to move the devices to and click **OK**.

The moved device's settings are now changed to the settings of the new group.

3.2.5 Manually running a service on devices

By default, GFI OneGuard runs services as configured in the group configuration. A service, however, can be executed on-demand on all devices within a group or on selected devices:

Running a service on all devices within a group

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. In the left pane, under **Managed Groups**, hover mouse over a group, click the pulldown menu arrow and click the service to run, for example, **Run patch scan**.

Running a service on selected devices within a group

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. Manually select desired devices. You can select all devices by clicking **Select All** icon.

3. In the right pane, click **More actions...**, then select the service to run, for example, **Run patch scan**.

To monitor the executed service, either go to the **Activity Monitor** or visit the relative dashboard from the Dashboards menu.

3.2.6 Renaming a group of devices

To rename a GFI OneGuard group of devices:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. In the left pane, under **Managed Groups**, hover mouse over the group to rename, click the pulldown menu arrow and click **Rename group**.

3. Key in the new group name and press **Enter**.

3.2.7 Deleting a group

> **IMPORTANT**
> Delete groups with caution. Settings applied to deleted groups are permanently lost and not recoverable.
> When deleting a group that contains devices, these devices are no longer managed in GFI OneGuard and are moved to the **Discovered Devices** node. It is recommended to move managed devices to a different group before deleting a group. For more information, refer to Assigning devices to groups (page 22).

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. In the left pane, click the group to delete to show the list of devices in the right pane. Move the devices to a new group before deleting the group. For more information, refer to Assigning devices to groups (page 22).

3. Hover mouse over the group to remove, click the pulldown menu arrow and click **Delete group**.

4. Click **OK** to confirm deletion.

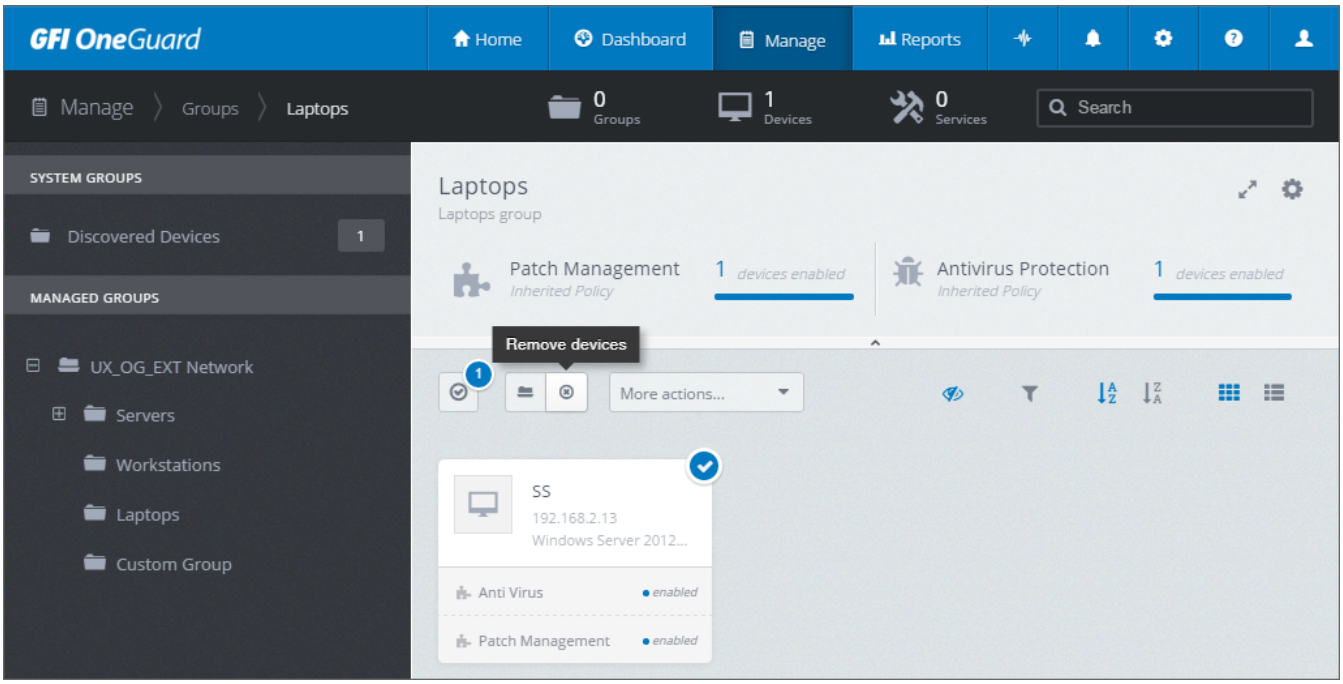
3.2.8 Removing a managed device

Devices can either be moved to a different group to apply a different policy or removed entirely from groups to stop the device from being managed via GFI OneGuard. When a device is removed from a group, GFI OneGuard Agents on removed devices are automatically uninstalled and GFI OneGuard services are not executed on that device which could leave the device in a vulnerable state.

To stop managing a device in GFI OneGuard:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. From **Managed Groups**, choose the group where the device is located.



Screenshot 14: Remove devices option

3. In the right pane select one or more devices and from the actions bar click **Remove device**.

4. Click **OK** to confirm.

Devices that are removed from a managed group are moved to the **Discovered Devices** screen and can be re-added to GFI OneGuard later. For more information, refer to Assigning devices to groups (page 22).

3.3 Asset Tracking

Managing device assets is one of the most time consuming and intensive tasks that the IT department has to carry out in any organization. Where IT staff numbers are limited, this necessary task creates a massive manpower burden if it is not automated and centralized. GFI OneGuard uses the Asset Tracking service to make an inventory of servers and workstations across the organization. Machines running a Windows operating system that are connected to the network are identified by machine name and audited, listing hardware specifications for each device found and also installed software.

The Asset Tracking service is not a paid service and is available even if a GFI OneGuard subscription is not renewed.

See also:

3.3.1 Device hardware & software information 26

3.3.2 Customizing device login credentials 26

3.3.3 Sending a message to a device 27

3.3.4 Device service notifications 28

3.3.5 Shutting down or Restarting a device remotely 29

3.3.6 Disabling Asset Tracking 30

3.3.1 Device hardware & software information

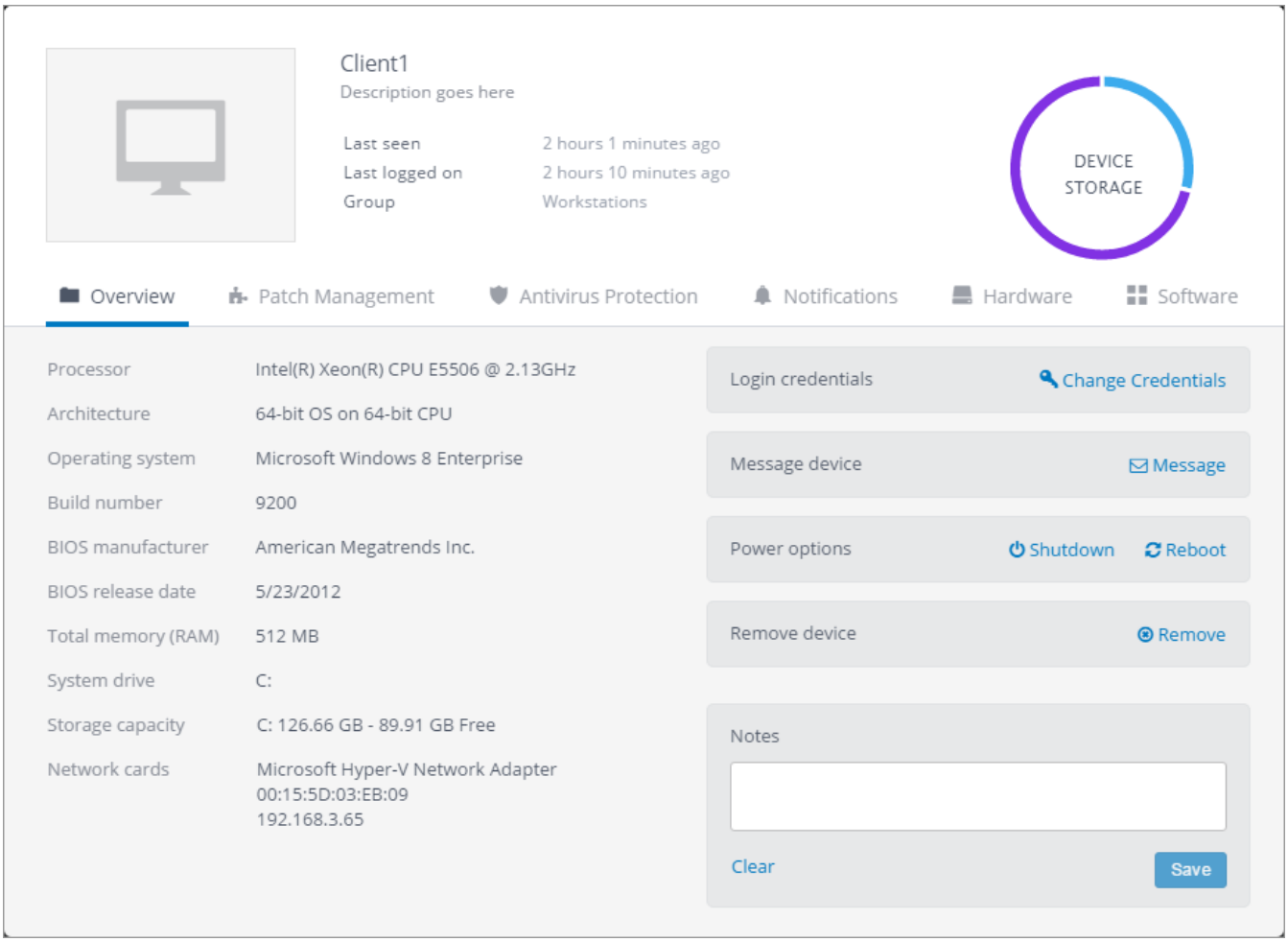
GFI OneGuard provides high-level information and system specifications of managed devices, including hardware and operating system information.

To view this information for a particular device:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. Under **Managed Groups**, click the group that contains the required device.

3. In the right pane, hover mouse over the device and click **Manage**.



Screenshot 15: Device Overview page

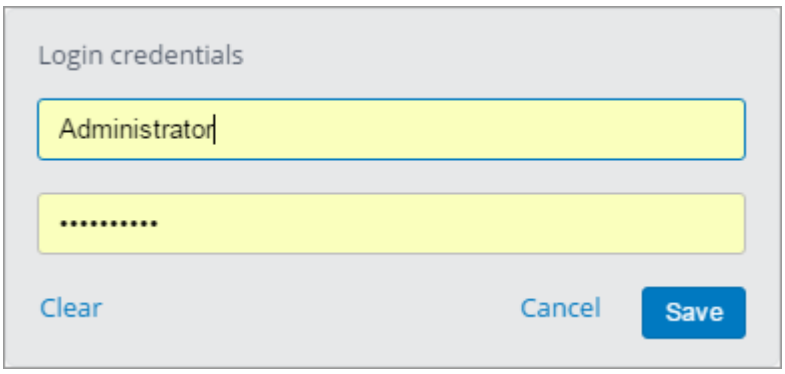
The detected device information is displayed in the left side of the **Overview** screen. Additional information can be accessed from the **Hardware** and **Software** tabs.

3.3.2 Customizing device login credentials

GFI OneGuard uses the administrative credentials configured in the Network Control settings screen to deploy and access Agents. When devices cannot be accessed using these credentials, but require a different account, a different set of credentials can be configured on each individual device. GFI OneGuard uses these custom credentials to connect, access and deploy settings to a device's agent.

To change the credentials for a particular device:

1. Log in to GFI OneGuard and go to **Manage > Devices**.
2. Under **Managed Groups**, click the group that contains the required device.
3. In the right pane, hover mouse over the device and click **Manage**.



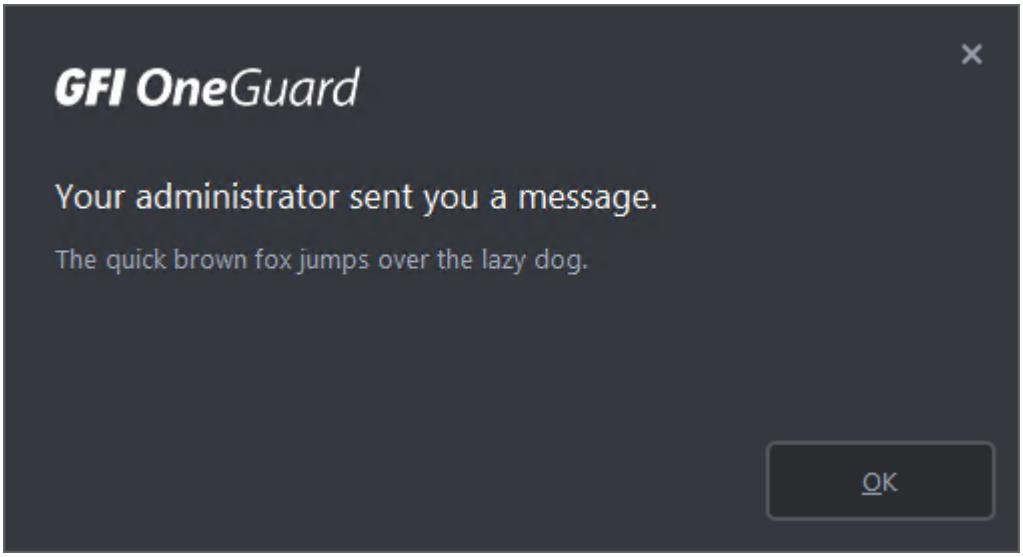
Screenshot 16: Login credentials area on Device

4. Click **Overview** tab and under **Login credentials**, click **Change credentials**.
5. Enter the username and password and click **Save**.

> **NOTE**
> To remove the custom credentials and use the default network control credentials, click **Clear** and then **Save**.

3.3.3 Sending a message to a device

When sending a message to a device, the GFI OneGuard agent loads a window on the device containing a friendly note or memo for its user.



Screenshot 17: A sample message sent by the GFI OneGuard administrator as seen by the device user

> **NOTE**
> Messages are not stored anywhere and therefore cannot be recorded or archived after transmission. Also, device users cannot reply or acknowledge receipt of message.

To send a message to a device:

1. Log in to GFI OneGuard and go to **Manage > Devices**.
2. Under **Managed Groups**, click the group that contains the required device.
3. In the right pane, hover mouse over the device and click **Manage**.
4. From the **Overview** tab, click **Message**.
5. Key in the message to send to the device. When done, click **OK** to send the message.

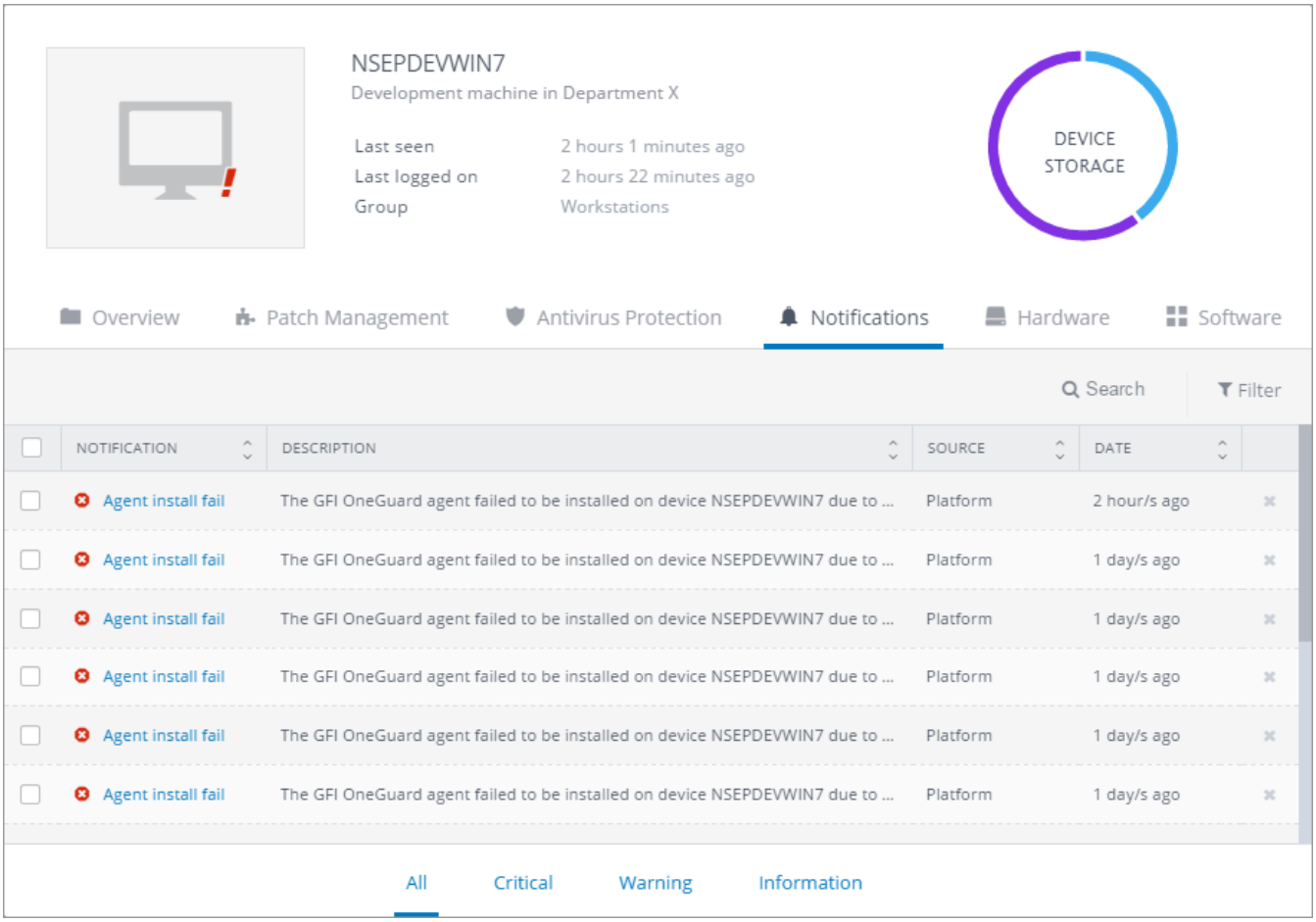
3.3.4 Device service notifications

GFI OneGuard logs all results of actions performed by all its services on all devices. This topic describes how to review a list of notifications applicable to a particular device.

> **NOTE**
> Apart from the below method, notifications for a particular device can also be reviewed from the Activity Monitor by filtering the logs by device name. For more information, refer to Activity Monitor (page 78).

To review the list of notifications for a particular device using the device card:

1. Log in to GFI OneGuard and go to **Manage > Devices**.
2. Under **Managed Groups**, click the group that contains the required device.
3. In the right pane, hover mouse over the device and click **Manage**.
4. Click **Notifications** tab to view all the notifications applicable to the device.



Screenshot 18: Viewing device notifications

To help you find notifications, use the **Search** or **Filter** controls. Click a notification to view more detailed information.

3.3.5 Shutting down or Restarting a device remotely

A GFI OneGuard administrator may remotely send a shutdown or restart command to managed devices.

> **NOTE**
> Use this feature with caution. A logged in end user cannot cancel the reboot or shutdown command.

To do this:

1. Log in to GFI OneGuard and go to **Manage > Devices**.
2. Under **Managed Groups**, click the group that contains the required device.
3. In the right pane, hover mouse over the device and click **Manage**.
4. In the **Overview** tab, under **Power Options**, click **Shutdown** or **Reboot**.

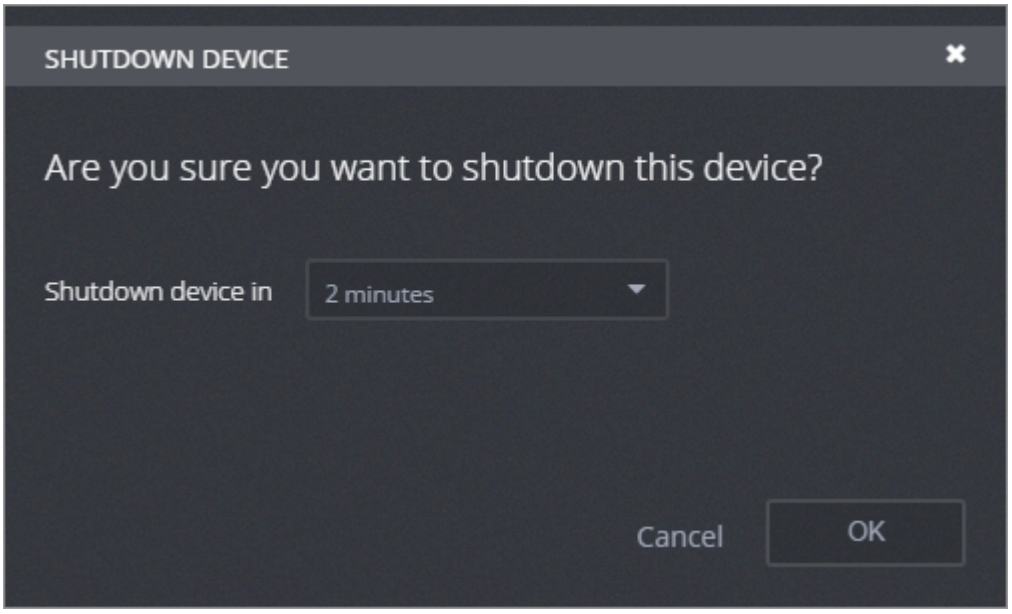
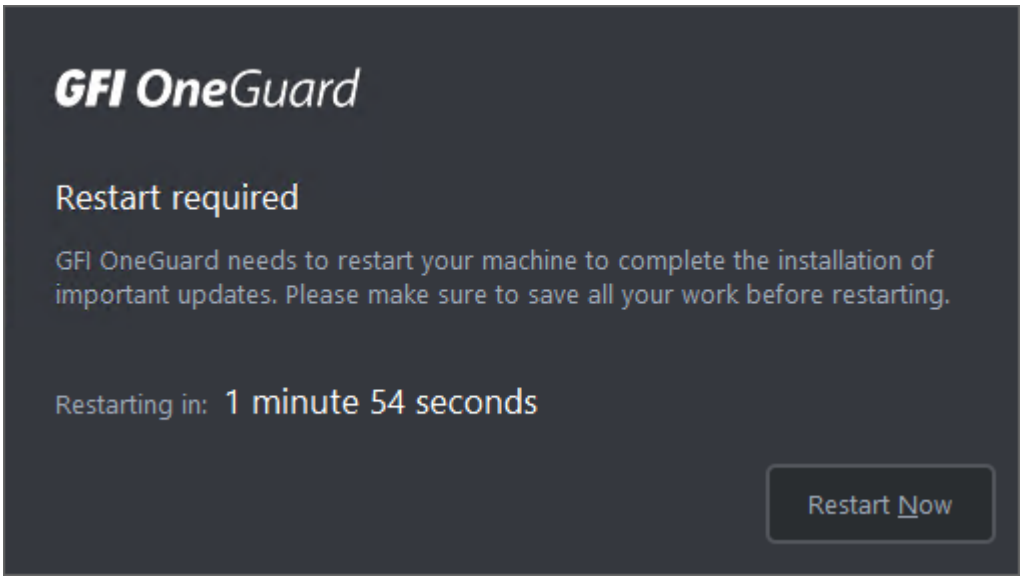


Figure 1: Set delay time for shutdown operation

5. Choose the command delay. This warns the user about the operation and gives time to finish and save work.
6. Click **OK** to confirm.



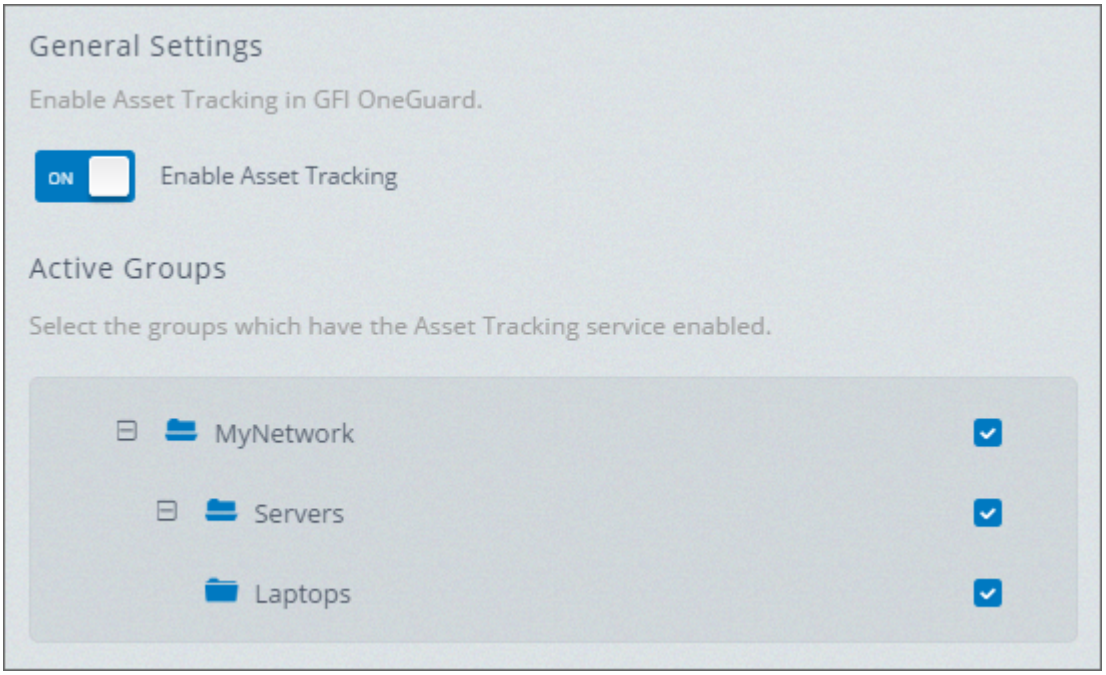
Screenshot 19: A reboot warning shown on user device

3.3.6 Disabling Asset Tracking

By default, Asset Tracking is enabled when GFI OneGuard is installed.

To disable or re-enable the Asset Tracking on the system or in individual groups:

1. Log in to GFI OneGuard and go to **Manage > Services**.



Screenshot 20: Asset Tracking service settings

2. From the menu on the left, click **Asset Tracking**.

3. In **General Settings**, click the switch to enable or disable the service from the system. You will need to confirm this action in an additional screen.

4. In the **Active Groups** area, uncheck the groups, which have the service enabled.

5. Click **Save Settings** in the top yellow bar to save your changes.

3.4 Patch Management

The patch management service in GFI OneGuard simplifies and centralizes the deployment of system and software patches on devices that are managed by GFI OneGuard. This is done by automatically downloading and remotely installing service packs and patches for Microsoft® Windows operating systems as well as third party products.

See also:

3.4.1 Monitoring patch deployment 31

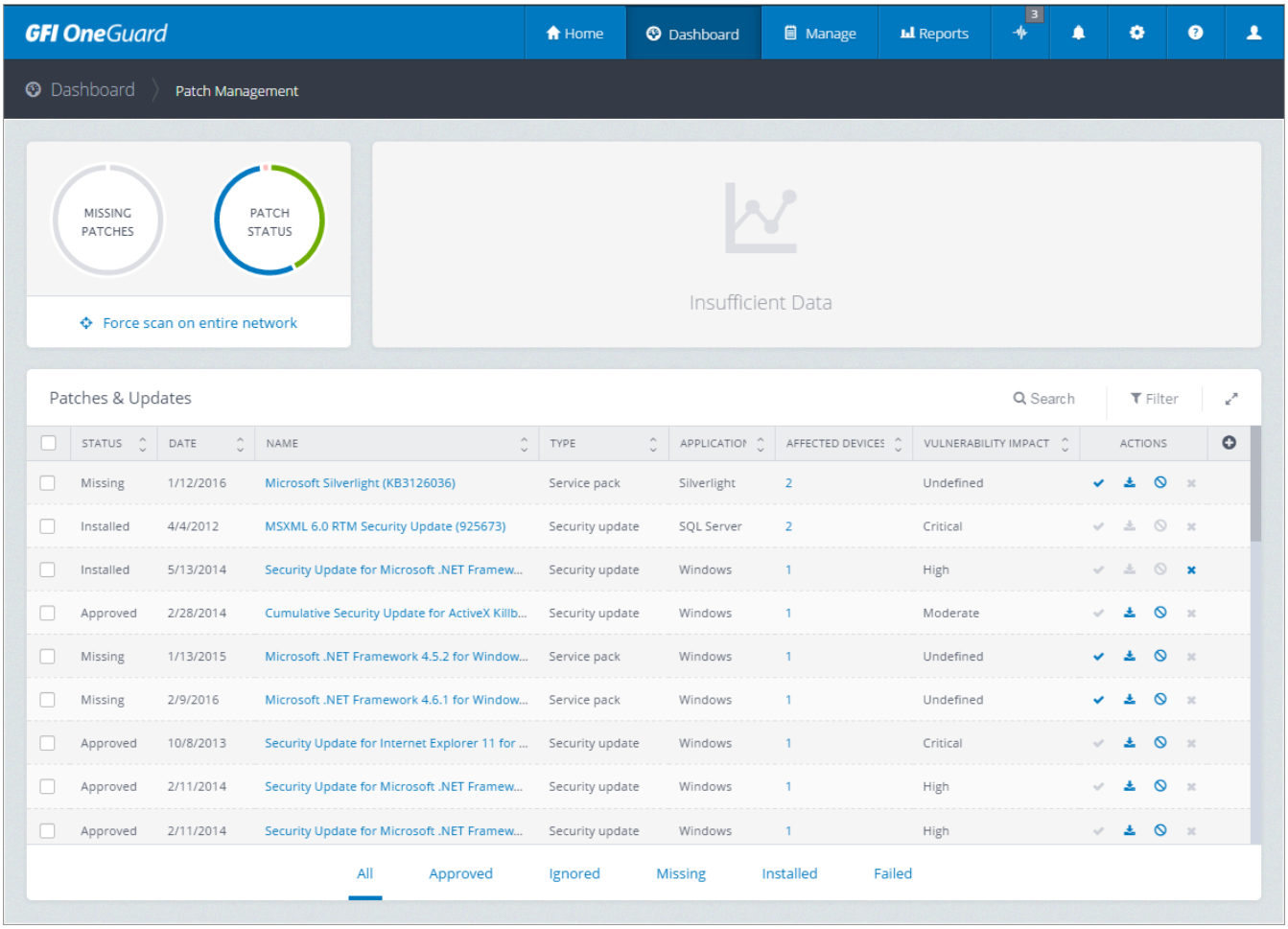
3.4.2 Configuring Patch Management on a Group 32

3.4.3 Run Patch Services on a Device 35

3.4.4 Disabling Patch Management 36

3.4.1 Monitoring patch deployment

To monitor the status of the patch management service and track the deployment of patches on devices, go to **Dashboard > Patch Management**.



Screenshot 21: The patch management dashboard

The top widgets show a graphical representation of missing patches, patch status and patch management over time.

From this dashboard you can perform the following actions:

Action	Description
Force scan on entire network	Click to force GFI OneGuard to perform a scan for devices on the entire network. New discovered devices are visible from **Manage > Devices**. For more information, refer to Groups and Devices (page 18).
Search	Key in a search term to filter the **Patches & Updates** table. Only rows that contain a field that matches the search term entered are shown.
Filter	Click to filter the list of patches and updates using the following criteria: » **Period** - select a custom date range or one of the predefined date ranges. » **Groups** - select a group from the populated list and show patches applicable to devices in that group only. » **Type** - choose from a list of available categories. » **Vendor** - select one of the available vendors from the list. » **Vulnerability Impact** - choose from the available severity ratings.
Actions	Use the actions menu to: » **Approve** - approve the patch for installation, adding it to the list of queued patches to install. » **Install** - start patch installation as soon as possible. » **Ignore** - do not install patch on device. » **Uninstall** - remove an installed patch.
Status filter	Use the status filters at the bottom of the dashboard to filter the list of patches and updates by Status.

The information is available in the format of reports that can be run at any time and schedule for recurrent patterns. For more information, refer to Reports (page 70).

3.4.2 Configuring Patch Management on a Group

Patch Management can be configured per device or on a group of managed devices. This topic describes how to configure Patch Management on a group.

Devices joined to a group inherit the group's patch management settings.

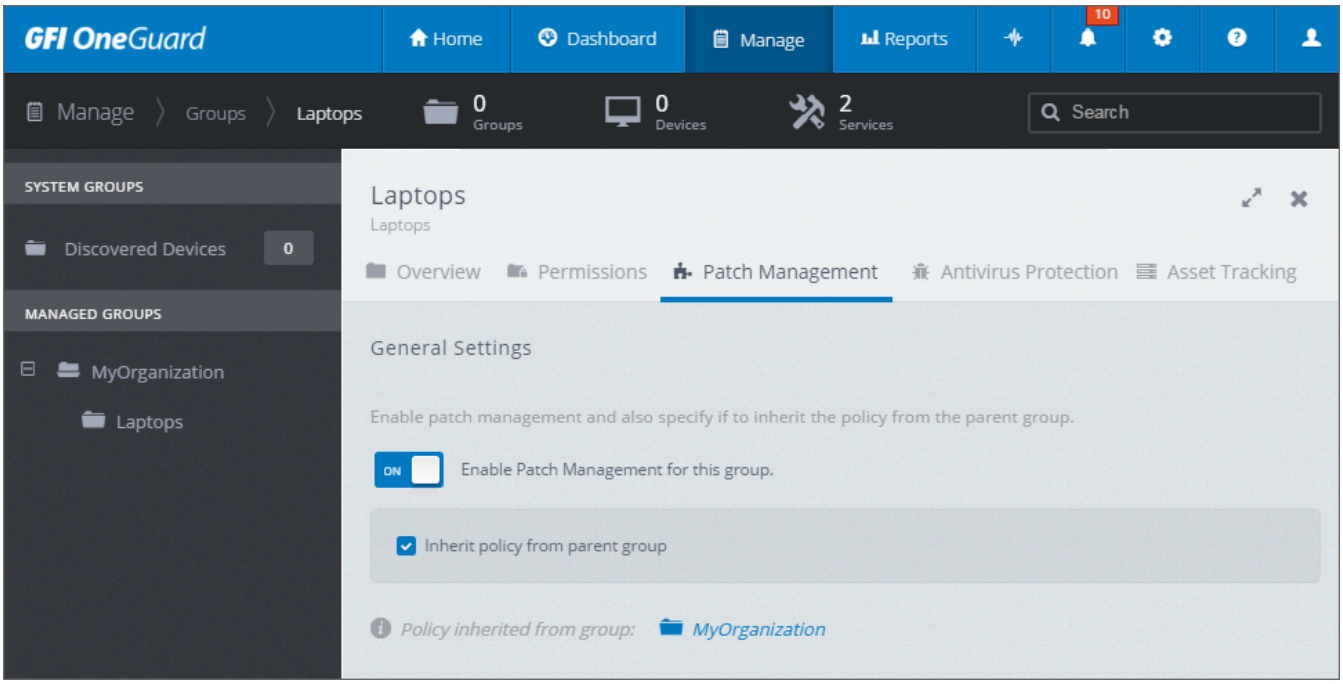
To access group patch management settings:

1. Log in to GFI OneGuard and go to **Manage > Devices**.

2. In the left pane, under **Managed Groups**, hover your mouse over the group you want to configure.

3. Click the pulldown menu arrow and select **Configure group**.

4. Go to the **Patch Management** tab to start customizing patch management settings in this group.



Screenshot 22: Enabling the patch management settings

Enabling/Disabling Patch Management

To enable or disable patch management, use the switch **Enable Patch Management for this group**.

If enabling patch management, you may proceed to configure the other settings.

If disabling patch management, no other settings need to be configured and you can click **Save Settings** to apply the change.

Inherit policy from parent group

Use this option to automatically inherit patch management settings from the parent group, according to the hierarchy shown in the **Managed Groups** section in the left pane. If this option is selected, the options below this setting are hidden.

Import or Export a Policy

You can use these options to export a policy from an existing GFI OneGuard deployment and import them into another. This is useful for example when moving your GFI OneGuard installation from one server to another.

Select from the following options:

Option	Description
Import Policy	Click to select a policy settings file from a saved location.
Export Policy	Use this option to save the currently configured settings to a desired location.

Patch Scanning and Installation scheduling

Use the scheduler to configure how frequent GFI OneGuard scans managed devices for missing patches.

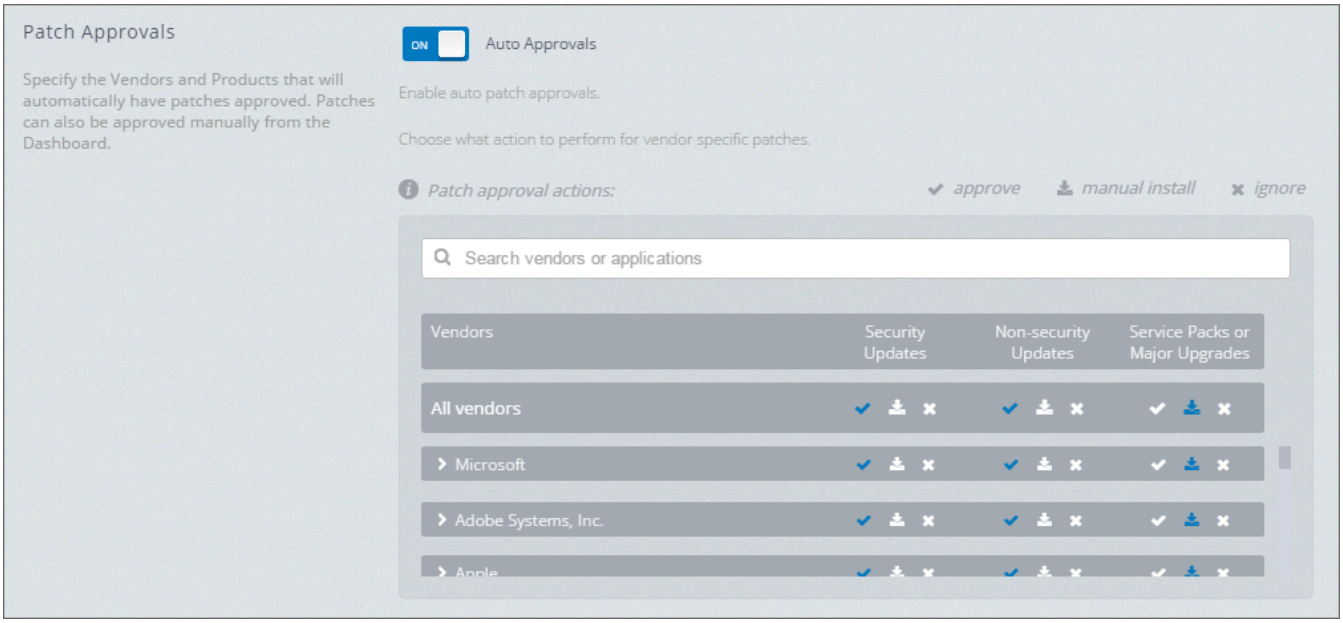
Configure also other patch scanning options:

Option	Description
Run scan immediately when new patch definitions are detected	When new software or system patches are available, GFI OneGuard runs a scan immediately, overriding the schedule configured.
Install approved patches immediately if a patch installation is missed	Approved patches are automatically installed on managed devices when a patch installation is missed.
Restart devices automatically after patch installation is complete	Instructs GFI OneGuard to attempt device restart after installing patches.

> **NOTE**
> GFI OneGuard automatically installs approved missing patches when a scan completes.

Patch approvals

Use this area to maintain a list of actions for patches issued by specific vendors. When a patch by a vendor is available, GFI OneGuard runs the action configured here. For example, GFI OneGuard can automatically approve and install the patch.



Screenshot 23: Group patch approvals area

To enable this feature, switch **ON** the **Auto Approvals** option. When this option is disabled, all patches to deploy must be manually approved for deployment one-by-one. To do this, go to **Dashboard > Patch Management** and review, approve and install missing patches from the **Patched & Updates** table. For more information, refer to Monitoring patch deployment (page 31).

In the **Vendors** table, configure the approval action for each vendor and for each software product issued by that vendor. Choose the action to take for **Security updates**, **Non-Security updates** and for **Service Packs or Major Upgrades**. The possible actions are:

Option	Description
Approve	Patches are automatically downloaded and installed on devices.
Manual install	Mark software updates for manual download. You will be able to manually approve downloaded patches from the home page.
Ignore	Patches are not downloaded and not installed on devices.

The **All vendors** role defines the action to take by default on all vendors and software. When an action in this row is chosen, the action of all vendors and software is automatically set to the action chosen.

Notifications

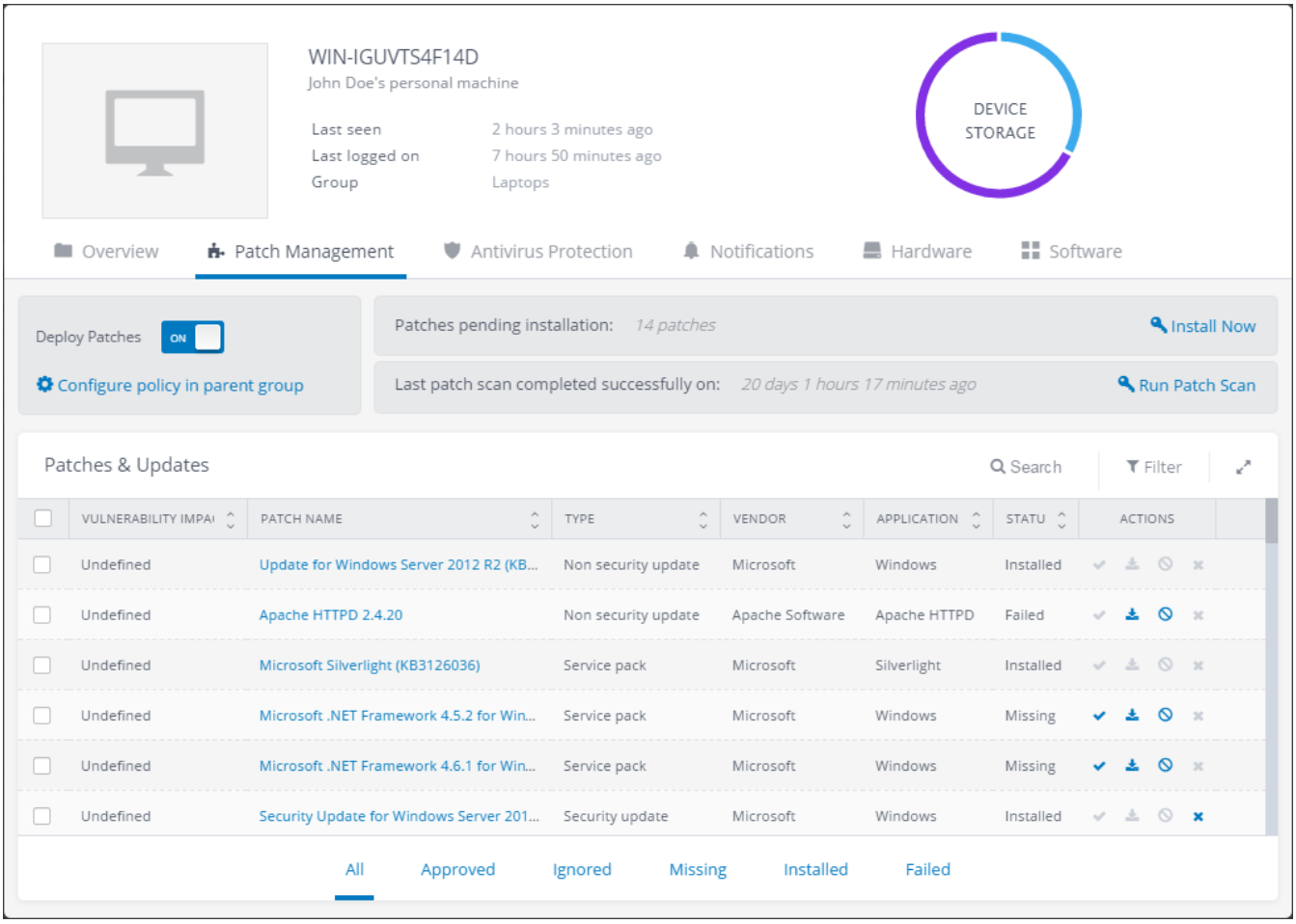
Configure system alerts and email notifications based on the status of patch availability and deployment.

Notification type	Description
Alerts	Choose to enable or disable system alerts shown in the top navigation bar.
Send an email alert when a patch fails to install	Send an email notification when a patch fails to install. The notification can either be sent to all users that have access to the group or to a custom email address list.

3.4.3 Run Patch Services on a Device

Patch management services, such as a Patch scan, can be executed on a single device. To monitor and configure patch management services on a specific device:

1. Log in to GFI OneGuard and go to **Manage > Devices**.
2. In the left pane, under **Managed Groups**, click the group that contains the required device.
3. In the right pane, hover over the device and click **Manage**.
4. Go to **Patch Management** tab.



Screenshot 24: Running a Patch Scan on a device

5. Select from the following options:

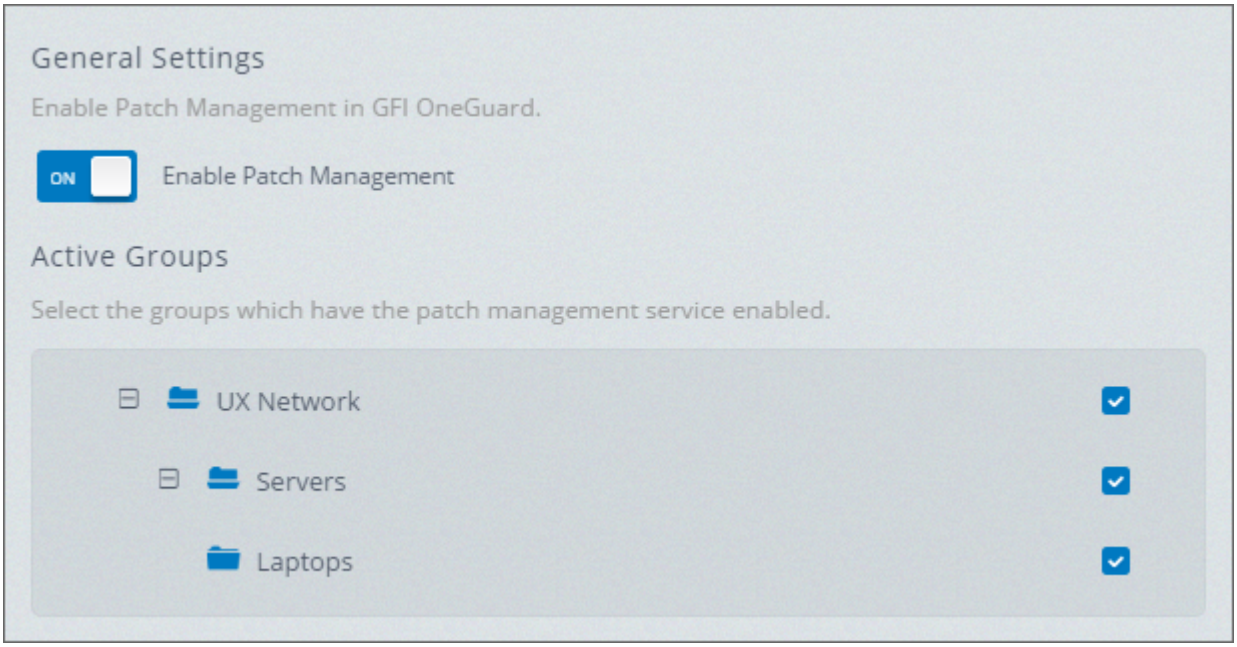
Service	Description
Deploy Patches	Click the switch to enable or disable patch management scanning and install missing patches on the selected device.
Configure policy in parent group	Click this link to go the group settings page where you can configure patch management on the group the selected device belongs to. For more information, refer to Configuring Patch Management on a Group (page 32).
Install now	Installs pending patches on the selected device.
Run Patch Scan	Runs a scan for missing patches on the selected device.
Search	Searches through the list of patches and updates. Click on **Search** and key in the term to search for in any of the available fields. The list is filtered in real-time to show only patches and updates that contain the keyed in term.
Filter	Click to narrow the list of patches and updates by the following criteria: » **Type** - choose from a list of available categories. » **Vendor** - select one of the available vendors from the list. » **Vulnerability Impact** - choose from the available severity ratings.
Actions	For each patch listed, choose the action to take on the chosen device: » **Approve** - approve the patch for installation, adding it to the list of queued patches to install. » **Install** - Start patch installation as soon as possible. » **Ignore** - Do not install patch on device. » **Uninstall** - remove an installed patch. Note that not all patches support uninstallation.
Status filter	Use the status filters at the bottom of the patch management tab to filter the list of patches and updates by status.

Go to the **Activity Monitor** to monitor the progress of actions performed in this screen.

3.4.4 Disabling Patch Management

If included with the license or when evaluating the software, the Antivirus service is enabled by default. To disable or re-enable the Patch Management on the system or in individual groups:

1. Log in to GFI OneGuard and go to **Manage > Services**.



Screenshot 25: Patch Management service settings

2. From the left pane, click **Patch Management**.

3. In **General Settings**, click the switch to enable or disable the service from the system. You will need to confirm this action in an additional screen.

4. In the **Active Groups** area, uncheck the groups, which have the service enabled.

5. Click **Save Settings** in the top yellow bar to save your changes.

3.5 Antivirus

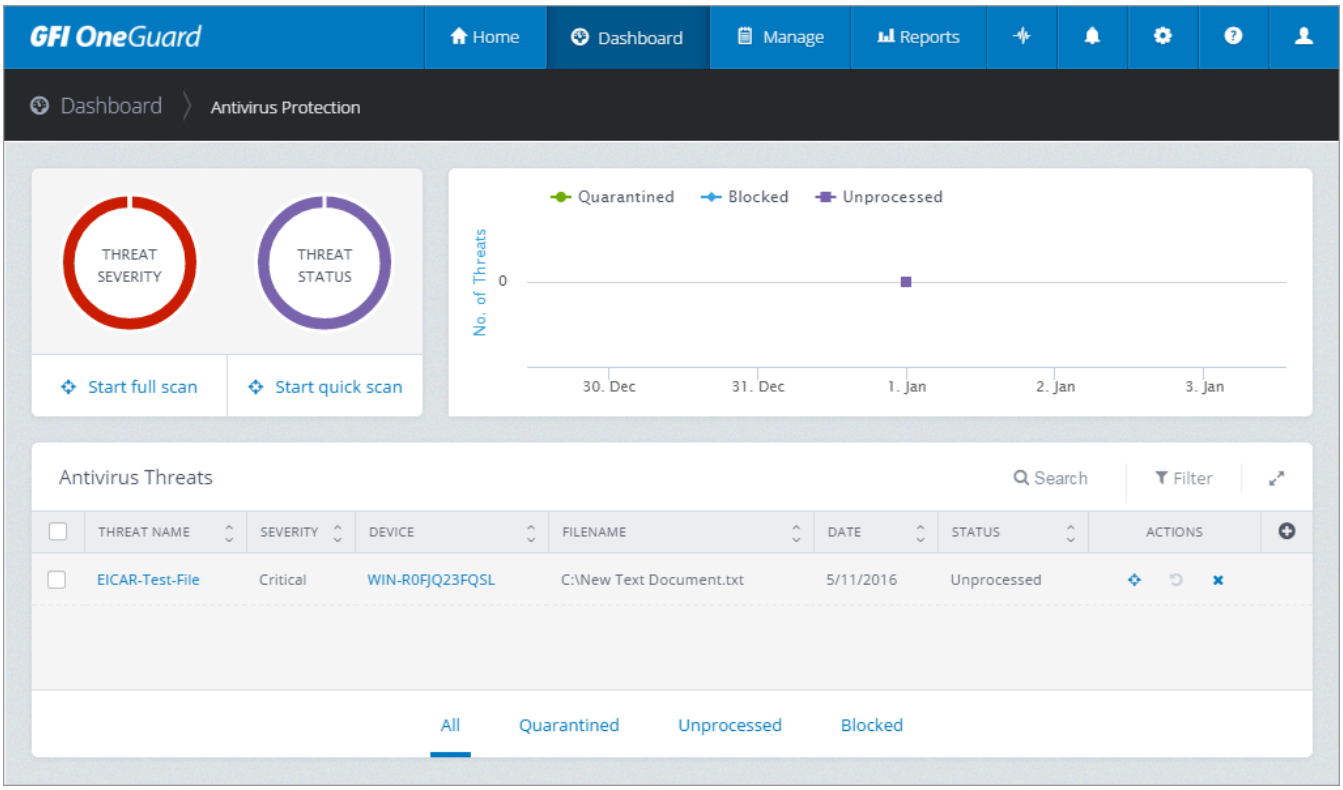
The Antivirus service in GFI OneGuard centralizes antivirus protection measures across the whole network. Powered by Kaspersky Lab, the service scans managed devices for malicious activity automatically. Any malicious code detected by GFI OneGuard is deleted or blocked based on actions defined by the administrator.

See also:

3.5.1 Monitoring Antivirus 37
3.5.2 Configuring group antivirus protection 39
3.5.3 Device antivirus options 46
3.5.4 Antivirus global exclusion list 47
3.5.5 Disabling the Antivirus service 47

3.5.1 Monitoring Antivirus

To monitor the status of the antivirus protection service and track threat history on devices, go to **Dashboard > Antivirus Protection**.



Screenshot 26: The antivirus management dashboard

The top widgets show a graphical representation of threat severity, threat status and antivirus detection over time.

From this dashboard you can perform the following actions:

Action	Description
Start Full Scan	Forces GFI OneGuard to perform a full antivirus scan for devices on the entire network.
Start Quick Scan	Forces GFI OneGuard to perform a quick antivirus scan for devices on the entire network. Quick scan may not detect some malware, but it can still inform you about a virus if your computer is infected.
Search	Key in the terms to search for in the Antivirus Threats table. Any fields matching the keyed in term are returned in real time.
Filter	Narrow the list of Antivirus Threats through the following criteria: » **Period** - select a custom date range or one of the predefined date ranges. » **Severity** - filters threats by their severity. Choose from the available severity types.
Actions	Use the **Actions...** drop down or the **Actions** column to perform one of the following: » **Rescan** - Select an item in the list of threats and rescan for viruses. » **Restore** - Restores a quarantined item. » **Delete** - Deletes the identified threat from the device.
Threat filter	Filter the Antivirus Threats list by the action performed by GFI OneGuard.

The information is available in the format of reports that can be run at any time and schedule for recurrent patterns. For more information, refer to Reports (page 70).

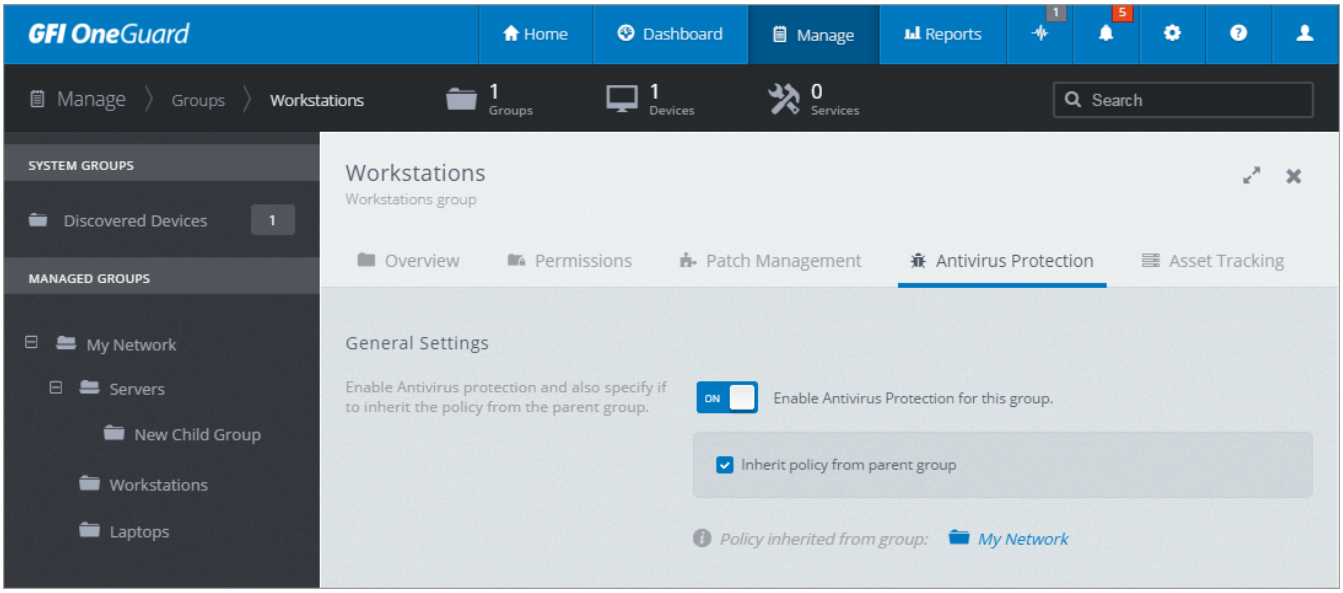
3.5.2 Configuring group antivirus protection

The Antivirus service offered by GFI OneGuard can be configured per device or on a group of managed devices. This topic describes how to configure Antivirus protection on a group.

Devices joined to a group inherit the antivirus protection settings configured on that group.

To access group antivirus settings:

1. Login to GFI OneGuard and go to **Manage > Devices**.
2. In the left pane, under **Managed Groups**, hover your mouse over the group you want to configure.
3. Click the pulldown menu arrow and select **Configure group**.
4. Go to the **Antivirus Protection** tab to start customizing settings in this group.



Screenshot 27: Configuring Antivirus Protection policy

Enabling/Disabling Antivirus Protection

To enable or disable antivirus protection, use the switch **Enable Antivirus Protection for this group**.

If enabling antivirus protection, you may proceed to configure the other settings.

If disabling antivirus protection, no other settings are need to be configured and you can click **Save Settings** to apply the change. If the antivirus service was previously installed and the antivirus service is then disabled, then the antivirus agent gets uninstalled from the affected devices.

> **NOTE**
> When installing or uninstalling the Antivirus, a reboot of the target computer may be required to complete the action.

> **IMPORTANT**
> When another third-party antivirus software is found on a device managed by GFI OneGuard that has antivirus protection enabled, the third-party antivirus software is automatically uninstalled by the GFI OneGuard agent. Note that this may require a reboot of the device.

Inherit policy from parent group

Use the **Inherit policy from parent group option** to automatically inherit settings from the parent group, according to the hierarchy shown in the **Managed Groups** section in the left pane. If this option is selected, the options below this setting are hidden.

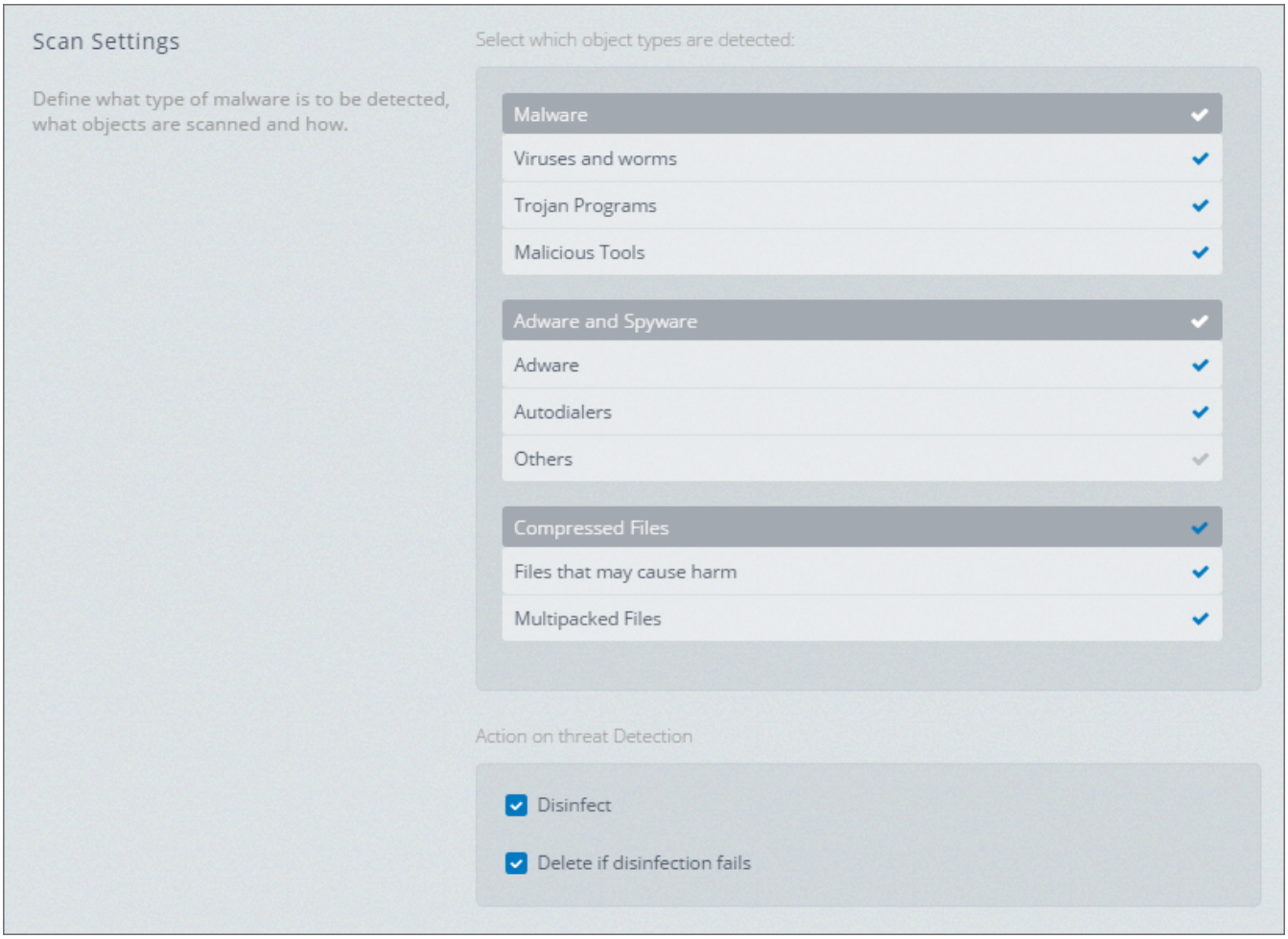
Import or Export a Policy

You can use these options to export a policy from an existing GFI OneGuard deployment and import them into another. This is useful for example when moving your GFI OneGuard installation from one server to another.

Select from the following options:

Option	Description
Import Policy	Click to select a policy settings file from a saved location.
Export Policy	Use this option to save the currently configured settings to a desired location.

Scan Settings



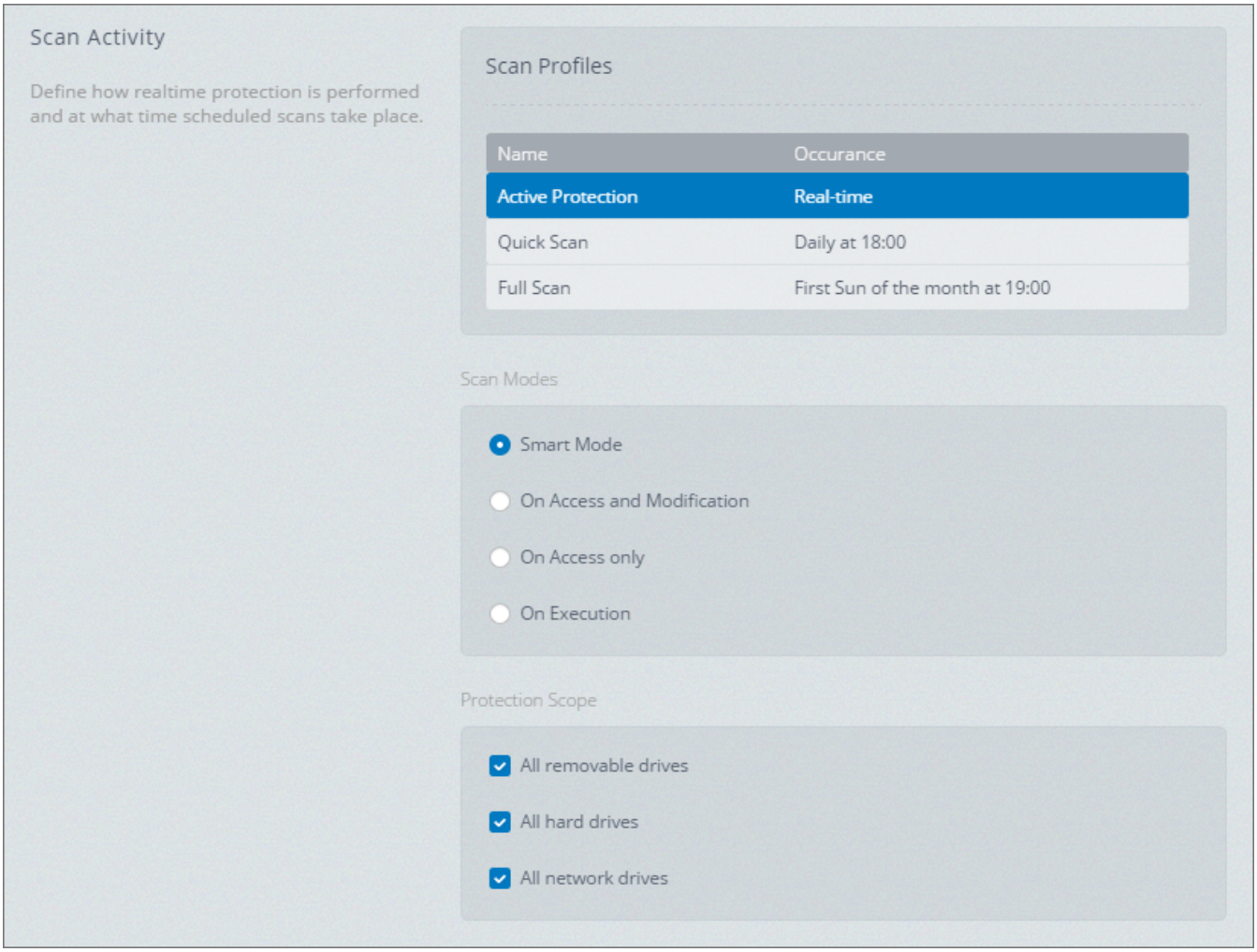
Screenshot 28: Antivirus scan settings

In the Scan Settings area, configure how this policy scans for antiviruses:

Option	Description
Select which object types are detected	Use this area to select which security scans to perform on devices within this group and the types of malicious or potentially risky files that are detected by GFI OneGuard. Select the check mark next to the desired scan type.
Action on threat detection	Specify the actions taken by the antivirus service when a potentially infected file is detected. Select from the following options: » **Disinfect** - When this option is selected, the Antivirus service attempts to disinfect any detected objects. » **Delete if disinfection fails** - Select this option to delete any detected objects that GFI OneGuard failed to disinfect.
Security Level	Move the slider to select your preferred level of protection from security threats. When switching between levels, options in the collapsed **Advanced Settings** area change accordingly. Available options are: » **High** - This setting offers the maximum protection and is recommended for organizations operating in industries where risk from threats is high. » **Medium** - This is the default protection setting and is recommended for most users since it offers a balance between protection and performance. » **Low** - This offers high performance but a minimum protection level. » **Custom** - Expand **Advanced Settings** and configure a list of custom options related to antivirus scanning.
File types to scan (shown when viewing Advanced Settings)	Use this setting to specify the types of files to include in a scan. Select from: » **All files** - scans all files (opened, executed or saved) regardless of extensions and formats. Selected by default. » **Files scanned by format** - The GFI OneGuard Antivirus analyzes inner file headers to detect file format (for example, text file, executable file, etc.). If the component detects that the file cannot be infected, the file will not be scanned for viruses. If the file of the detected format can be infected, the file will be scanned for viruses. » **Files scanned by extension** - The GFI OneGuard Antivirus analyzes files depending on their extensions (for example, files with extensions .com, .exe, .sys, .bat, .dll, etc.) to determine the file type.
Heuristic Analysis (shown when viewing Advanced Settings)	If you want GFI OneGuard Antivirus to use heuristic analysis, select the Heuristic Analysis checkbox and use the slider to set the intensity of a scanning process: » **Deep Scan** » **Medium Scan** » **Light Scan** » **Off**
Scan Compound Files (shown when viewing Advanced Settings)	Select which types of compressed files to scan: » **Archives (compound files, such as .doc and .xls)** » **Installation Packages** » **Embedded OLE Objects**

> **NOTE**
> It is recommended to use the default setting in most scenarios since that gives the best level of security while not heavily impacting systems performance.

Scan Profiles



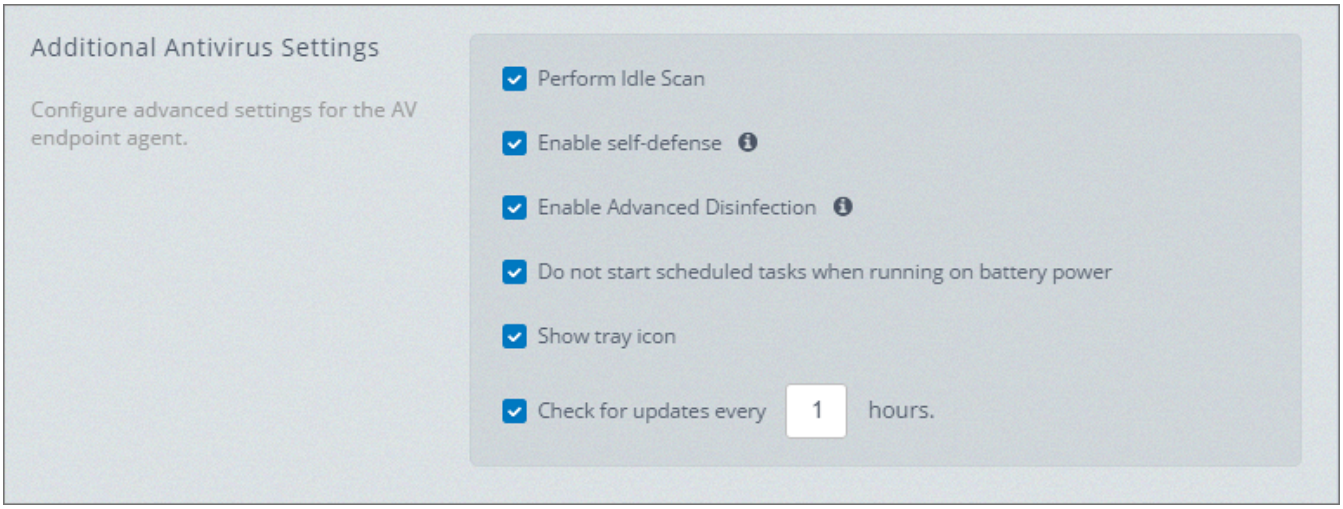
Screenshot 29: Antivirus scan activity

Select one of the available 3 profiles that provide real time antivirus protection. Modify settings for the selected profile as described below:

Profile	Description
Active Protection (Default profile)	Active protection is ongoing protection where a threat is blocked not only when a scan is run but also if a user downloads, opens or executes an infected file. In the **Scan Modes** area, select a scan mode from the following options: » **Smart Mode** - GFI OneGuard Antivirus decides whether or not to scan files after file analysis performed by the user, by an application on behalf of the user or by the operating system. For example, when working with a Microsoft Office document, Smart Mode scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned. » **On Access and Modification** - GFI OneGuard Antivirus scans files each time they are accessed or modified. » **On Access only** - GFI OneGuard Antivirus scans files only the first time when they are accessed. » **On Execution** - GFI OneGuard Antivirus scans *.exe items when these are executed. In the **Protection Scope** area, select any of the following options: » All removable drives » All hard drives » All network drives

Profile	Description
Quick Scan	Select this option to have GFI OneGuard Antivirus periodically check objects loaded on system startup, the system memory and boot sectors. Quick scan may not detect some malware, but it can still inform you about a virus if your computer is infected. Configure the frequency of quick antivirus scans. The default schedule is set to run daily at 18:00. Modify the schedule using the **Occurrence**, **Day** and **Time** controls as required.
Full Scan	If this option is selected, GFI OneGuard Antivirus scans the operating system, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives. Configure the frequency of full antivirus scans. By default, full scans are set to run on the first Sunday of every month at 18:00. Modify the schedule using the available controls as required.

Additional Antivirus Settings

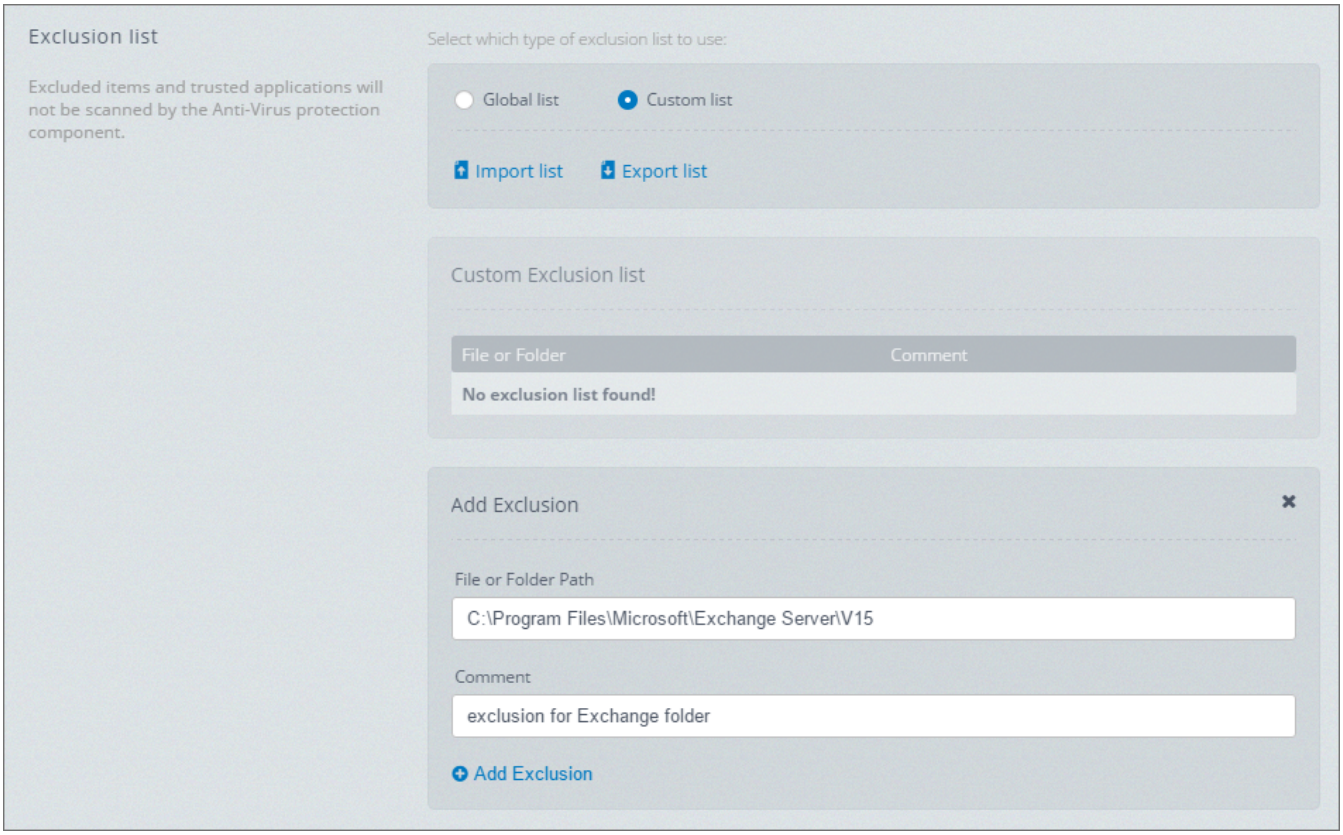


Screenshot 30: Antivirus additional settings

Configure advanced settings for the AV endpoint agent.

Options	Description
Perform Idle Scan	GFI OneGuard Antivirus scans machines only when a computer is idle and not busy.
Enable self-defense	Self-defense is a feature that protects the antivirus agent itself from malicious attacks, such as applications that block the antivirus agent from scanning the system.
Enable Advanced Disinfection	Advanced disinfection is a feature that allows a special disinfection process to be performed on active malware.
Do not start scheduled tasks when running on battery power	Enables energy conservation mode. When enabled, the following tasks are not run, even if scheduled: » Updates » Full Scans » Quick scans
Show tray icon	When enabled, a GFI OneGuard Antivirus icon is displayed in the Windows system tray.
Check for updates every 1 hours	GFI OneGuard Antivirus agent checks for definition updates at an interval which is set to 1 hour by default.

Group Exclusion list

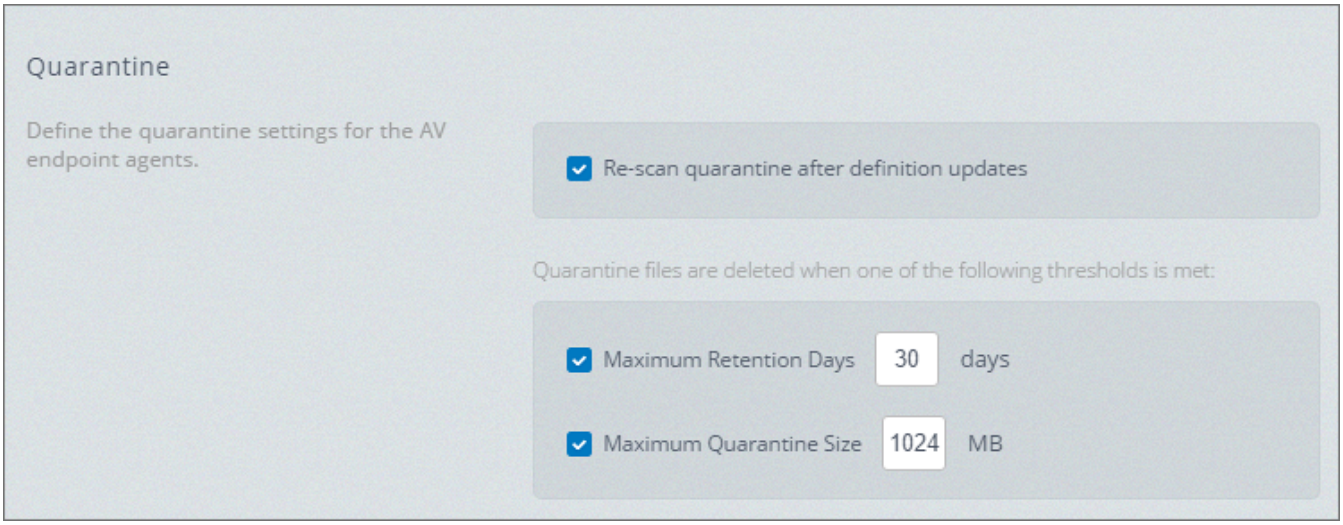


Screenshot 31: Antivirus custom exclusion list

You can configure a list of items and trusted applications that will be excluded from Antivirus scanning and protection. GFI OneGuard provides the following exclusion options:

Options	Description
Global list	Select this option to instruct GFI OneGuard to use the global list set in **Manage > Services > Antivirus Protection**. For more information, refer to Antivirus global exclusion list (page 47).
Custom list	GFI OneGuard gives you the option to import a custom list of exclusions or specify custom file or folder exclusions. To create a custom exclusion manually, click **Add file/folder**. Key in a file name or the path of a folder to exclude from scanning, for example `invoice.xls` or `C:\Program Files\GFI`. You can also use wildcard character ***** to match various patterns, for example use `*.xls` to exclude all files with an XLS extension or use `c:\dir\*.abc` to exclude all files with an ABC extension in c:\dir\. In the **Comment** field, type an optional description on why this file or folder is excluded. Click **Add Exclusion** to add the exclusion entry.

Quarantine



Screenshot 32: Antivirus quarantine settings

Use this area to define quarantine settings enforced by the antivirus service endpoint agents.

Option	Description
Re-scan quarantine after definition updates	Select to run an antivirus scan on quarantined items each time antivirus definitions are updated.
Maximum Retention Days	Set a retention value in days to specify for how long a period to keep infected files quarantined before deleting them.
Maximum Quarantine Size	Set a retention value to specify the threshold f in hard disk space to keep infected files quarantined before deleting them.

Notifications

Configure system alerts and email notifications based on antivirus related tasks carried out by GFI OneGuard.

Notification type	Description
Alerts	Choose to enable or disable email notifications when the below situations are encountered by the antivirus agent.
Send an email when a Quarantined file is added	Instructs GFI OneGuard to send an email notification when a file is added to the quarantine list.
Send an email when an Unprocessed file is found	Instructs GFI OneGuard to send an email notification when the antivirus agent cannot process an infected file. This situation is typically encountered when the infected file is unavailable (for example, file located on a removable drive without write privileges).
Send an email when a Blocked file is found	Use this option to instruct GFI OneGuard to send an email notification when a file is moved to the antivirus backup. The antivirus agent performs this action when a file is found to contain malware.
Users who have access	When checked, notifications are sent to the users that have access to the group. To specify custom recipients who receive the group's notifications, uncheck this option and specify custom email addresses.

3.5.3 Device antivirus options

Anti virus tasks, such as anti-malware scans and definition updates can be performed and managed centrally from the GFI OneGuard at either group-level or on a single device.

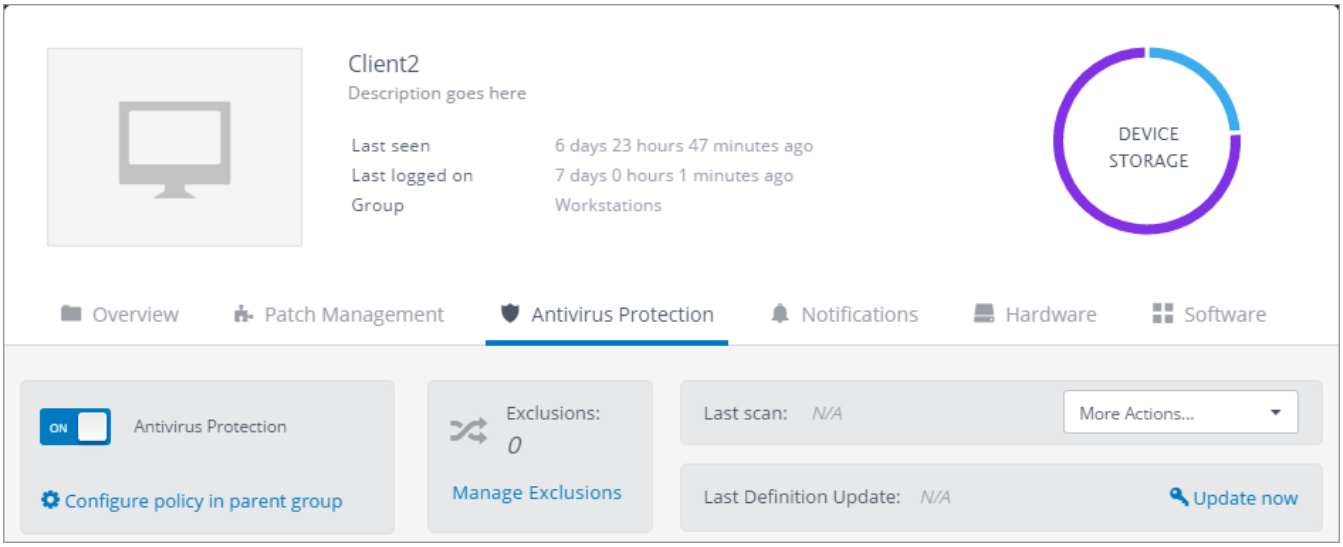
To run and configure the antivirus service on a specific device:

1. Login to GFI OneGuard and go to **Manage > Devices**.

2. In the left pane, under **Managed Groups**, click the group that contains the required device.

3. In the right pane, hover over the device and click **Manage**.

4. Go to **Antivirus Protection** tab.



Screenshot 33: Managing Antivirus services on a device

5. Select from the following options:

Service	Description
Antivirus Protection	If the antivirus service is enabled by the parent group, use this switch to disable antivirus protection on the selected device only. Note that if the antivirus is disabled at device level, the antivirus agent is left installed on the affected device and still counts towards your antivirus license count.
Configure policy in parent group	Click to configure antivirus settings on the parent group, from which this device inherits its antivirus protection configuration. For more information, refer to Configuring group antivirus protection (page 39).
Manage Exclusions	Click to configure a list of files or folder to be excluded from antivirus scans on the selected device. To configure an exclusion list: 1. Click **Add File/Folder**. 2. Key in a file name or the path of a folder to exclude from scanning, for example `invoice.xls` or `C:\Program Files\GFI`. You can also use wildcard character ***** to match various patterns, for example use `*.xls` to exclude all files with an XLS extension or use `c:\dir\*.abc` to exclude all files with an ABC extension in c:\dir\. 3. In the **Comment** field, type an optional description on why this file or folder is excluded. 4. Click **OK**. The excluded file or folder is added to the list. 5. Click **OK** to confirm.
More Actions	» **Run Quick Scan** select to run a quick antivirus scan on the specific device. » **Run Full Scan** select to run a full antivirus scan on the specific device.

Service	Description
Update now	Click to let GFI OneGuard check if there are any new definitions which need to be deployed on the selected device.
Antivirus Threats	The bottom area of the card shows a list of discovered threats, their severity, status and other information. Click on a threat to view more information about it. Use the **Actions...** drop down or the **Actions** column to carry out one of the following actions: » **Rescan Threat** - Rescans the file for viruses. » **Restore File** - Restores the selected file. » **Delete Threat** - Deletes the identified threat from the device.
Threat filter	Use the filters at the bottom of the tab to filter the detected threats by action.

Go to the **Activity Monitor** to watch the progress of actions performed in this screen.

3.5.4 Antivirus global exclusion list

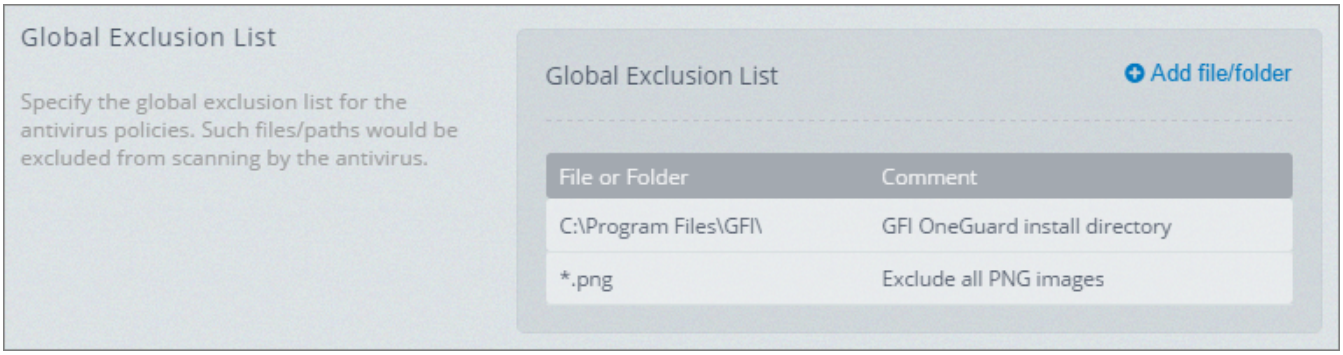
You can configure a list of items and trusted applications that will be excluded from Antivirus scanning and protection. A device group can either have a custom exclusion list applicable to it only, or the group can be configured to use a global list.

To add exclusions to the Global exclusion list.

1. Login to GFI OneGuard and go to **Manage > Services**.

2. From the the left pane, click **Antivirus Protection**.

3. Scroll down to the **Global Exclusion List** section.



Screenshot 34: The global antivirus exclusion list

4. Click **Add file/folder**.

5. Key in a file name or the path of a folder to exclude from scanning, for example `invoice.xls` or `C:\Program Files\GFI`. You can also use wildcard character ***** to match various patterns, for example use `*.xls` to exclude all files with an XLS extension or use `c:\dir\*.abc` to exclude all files with an ABC extension in c:\dir\.

6. In the **Comment** field, type an optional description on why this file or folder is excluded.

7. Click **Add Exclusion** to add the exclusion entry.

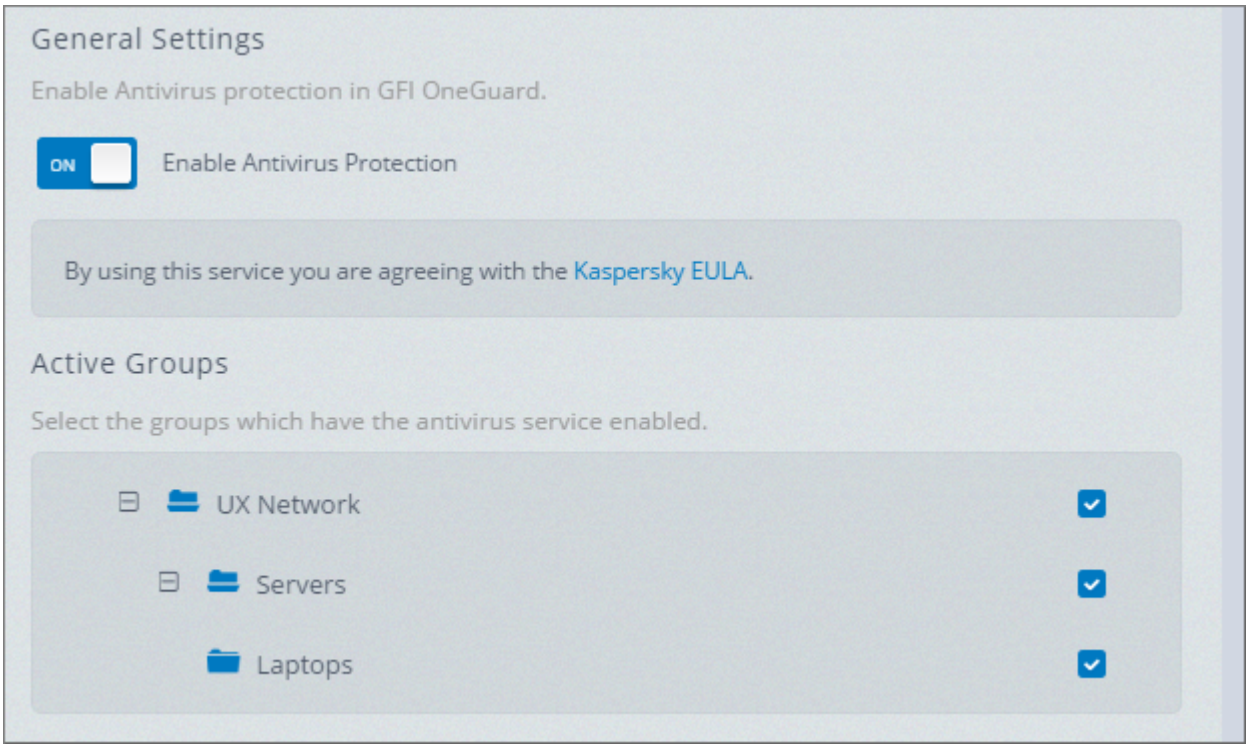
8. Repeat steps 4 to 7 to add more entries to the list.

9. On completion, click **Save Settings** to save and apply changes.

3.5.5 Disabling the Antivirus service

If included with the license or when evaluating the software, the Antivirus service is enabled by default. To disable or re-enable the Antivirus service on the system or in individual groups:

1. Login to GFI OneGuard and go to **Manage > Services**.



Screenshot 35: Antivirus service settings

2. From the left pane, click **Antivirus Protection**.

3. In **General Settings**, click the switch to enable or disable the service from the system. You will need to confirm this action in an additional screen.

4. In the **Active Groups** area, uncheck the groups, which have the service enabled.

5. Click **Save Settings** in the top yellow bar to save your changes.

3.6 EndPoint Control

The EndPoint Control service gives administrators full control of which files can be accessed on devices controlled by GFI OneGuard.

To control access, GFI OneGuard automatically installs a tamper-proof, hidden agent on the machines in your network. This agent delivers protection against users, even those with admin rights. This feature enables IT admins to remain in complete control in any scenario.

See also:

3.6.1 Monitoring EndPoint Control 49
3.6.2 Configuration 50
3.6.3 Adding New Rule 52
3.6.4 Working with Access Rules 56
3.6.5 Whitelist 57
3.6.6 Blocklist 59
3.6.7 Configuring encryption 62

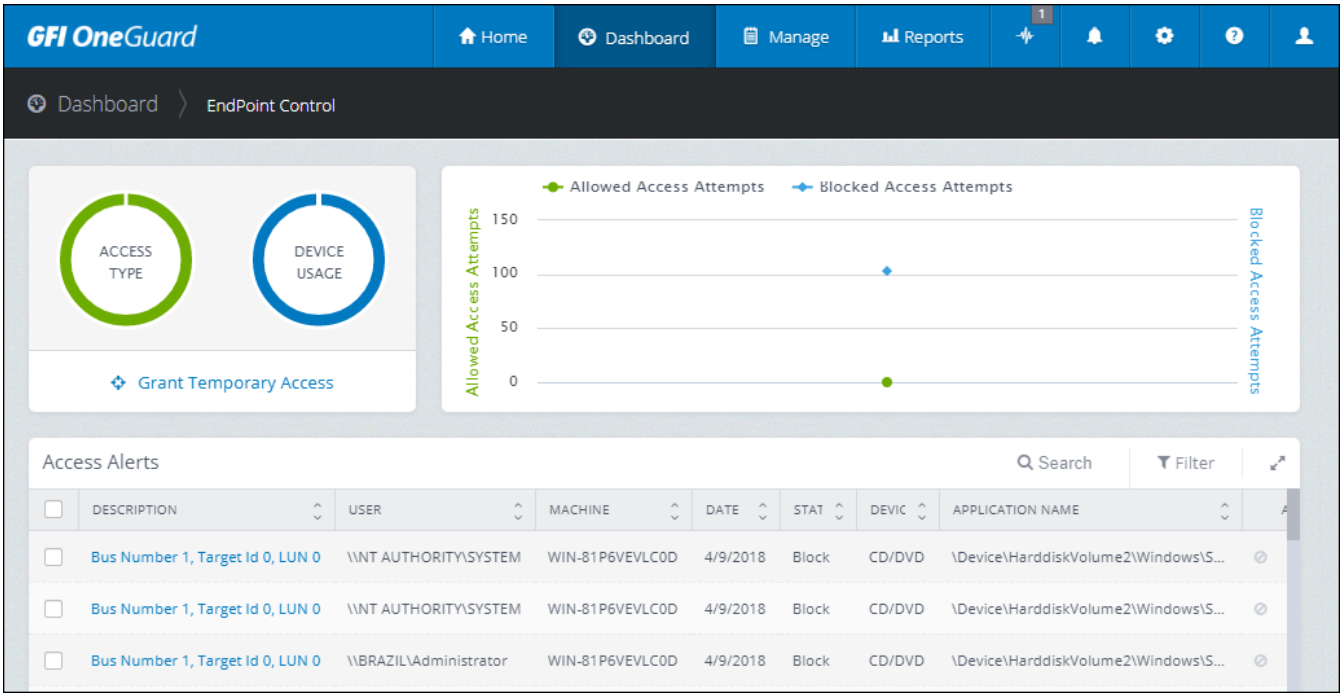
3.6.8 Enabling notification 66
3.6.9 Temporary Access 66
3.6.10 Resetting the password for an encrypted device 69

3.6.1 Monitoring EndPoint Control

GFI OneGuard EndPoint Control brings a dashboard that offers administrator an overview of devices usage and a table that shows the details of every device accessed showing the user, the application, the data and the status of blocked or allowed for every access.

The information is available in the format of reports that can be run at any time and schedule for recurrent patterns. For more information, refer to Reports (page 70).

To monitor the status of the EndPoint Control service and track usage history of devices, go to **Dashboard > EndPoint Control**.



Screenshot 36: The EndPoint Control dashboard

The top widgets show a graphical representation of device usage over time, displaying allowed access attempts and blocked access attempts. The graph offers a good overview of trend user behavior regarding attempts to break policy rules.

The lower widget shows a table with the access alerts in chronological order. The widget displays the user, machine, category, time and application used when the device was allowed or blocked.

From this dashboard you can perform the following actions:

Action	Description
Grant Temporary Access	EndPoint Control enables administrators to grant temporary access to users. The Temporary Access feature allows time-limited access to peripherals like a USB or CD/DVD blocked by an EndPoint Control policy. This feature can be used to give flexibility and manage exceptions without compromising security. For example, when a guest room that provides limited access to external clients needs to be used to hold a short conference. For more information, refer to Temporary Access (page 66).
Search	Key in the terms to search for in the Access Alerts table. Any fields matching the term are returned in real time.
Filter	Narrow down you search the following criteria: » **Period** - select a custom date range or one of the predefined date ranges. » **Device** - filters entries based on the computer or device used. » **Users** - filter entries based on the user. » **Application** - filters entries based on the application detected by EndPoint Control.
Delete alerts	Click the icon in the action column to delete the alert from the table.

3.6.2 Configuration

The GFI OneGuard EndPoint Control service can be configured per device or on a group of managed devices. This topic describes how to configure EndPoint Control protection for a group.

Devices joined to a group inherit the protection settings configured on that group.

To access group EndPoint Control settings:

1. Login to GFI OneGuard.
2. Go to **Manage > Devices**.
3. In the left pane, under **Managed Groups**, hover your mouse over the group you want to configure.
4. Click the pulldown menu arrow and select **Configure group**.
5. Go to the **EndPoint Control** tab to start customizing settings in this group.

Enabling/Disabling EndPoint Control

Use the switch **Enable EndPoint Control policy for this group** to enable or disable EndPoint Control protection.

When EndPoint Control is enabled, you may proceed to configure the other settings.

When EndPoint Control is disabled, no other settings configuration are needed and you can click **Save Settings**. When the EndPoint Control service is disabled the EndPoint agent gets uninstalled from the affected devices.

Inherit policy from parent group

Use the **Inherit policy from parent group option** to automatically inherit settings from the parent group, according to the hierarchy shown in the **Managed Groups** section in the left pane. If this option is selected, the options below this setting are hidden.

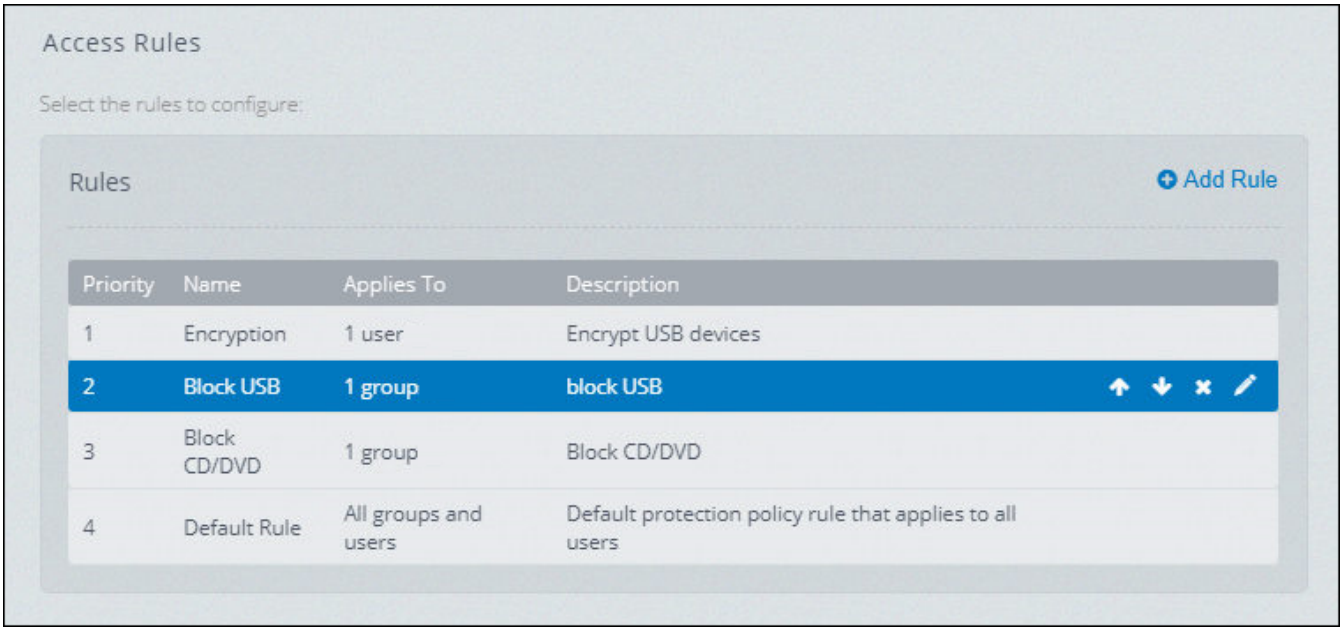
Import or Export a Policy

You can use these options to export an EndPoint Control policy from an existing GFI OneGuard deployment or group and import them into another. This is useful for example when moving your GFI OneGuard installation from one server to another, or setting up policies for different groups.

Select from the following options:

Option	Description
Export Policy	Use this option to save the currently configured settings to the desired location. By default, an XML file is saved on the Download folder. Take note of the name and location to import the policy. The file can also be renamed and moved to another location if required.
Import Policy	Click to select a policy settings file from a saved location. Browse to the folder where the policy was exported and select the XML file with the policy settings.

Access Rules



Screenshot 37: Access Rules order

The Access Rules policy define Endpoint Control rules based on users and groups and set the priority of rule execution.

Rules are executed from top to bottom and once a match is found the other policies are no longer applied. Thus, it is advisable to place the most specific rules to block on top and leave a default rule on the bottom that ensures the access to every device that should be used in the network.

For more information, refer to Working with Access Rules (page 56).

Policy Checker

Screenshot 38: Policy Checker displays the policy applied to a user

The policy Checker allows you to verify which rule applies to a particular user. Enter the name of a user or group and click **Check User**. The name of the rule applied to the user is displayed next to **Applying Policy**.

Click **Clear Results** to erase the actual result and start a new check.

3.6.3 Adding New Rule

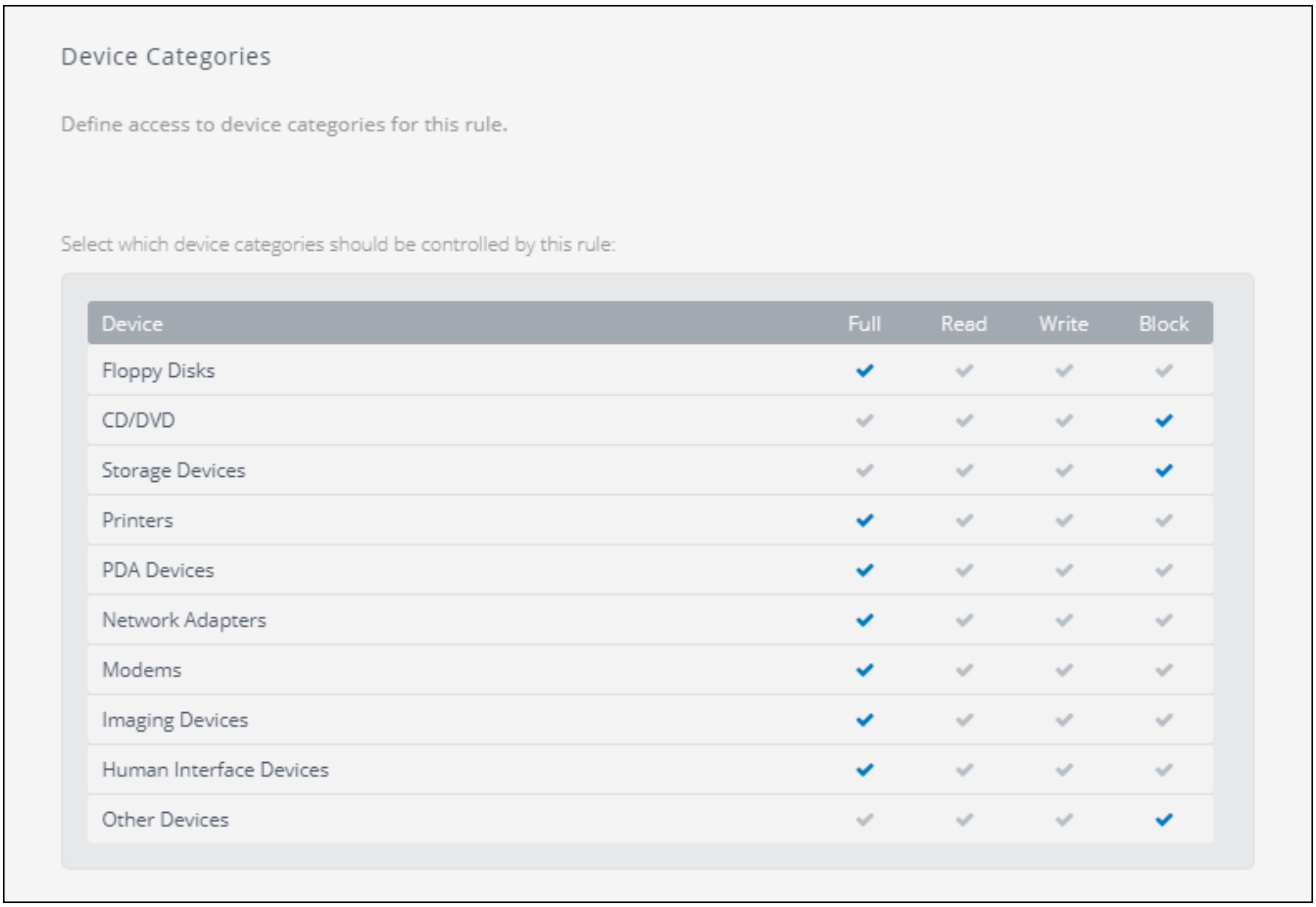
EndPoint Control agent uses Access Rules to establish which devices are allowed and which devices are blocked.

> **NOTE**
> For a machine running in terminal services, the GFI OneGuard EndPoint Control policies based on users may not work properly. Hence, in such scenario, it is suggested to simply use the default rule that applies to all users.

To add a rule:

1. Login to the GFI OneGuard Platform.
2. Go to **Manage > Groups**.
3. Locate the group you want to edit in the left pane, hover the mouse over the group and click **Manage**.
4. Go to **Services > EndPoint Control**.
5. Under **Access Rules** click **Add Rule**.
6. Type a **Rule name** that should be unique and an optional **description**.
7. Select the users or groups that inherit the configuration of this rule under **Users/Groups**. Start by typing all or part of a user or group name to populate the list of options available.

> **NOTE**
> Members of the Domain Administrators groups are automatically part of the Power Group users and are exempt from every policy. Remove the user from the Domain Administrator group or create a new policy and apply the policy to the Administrator group.

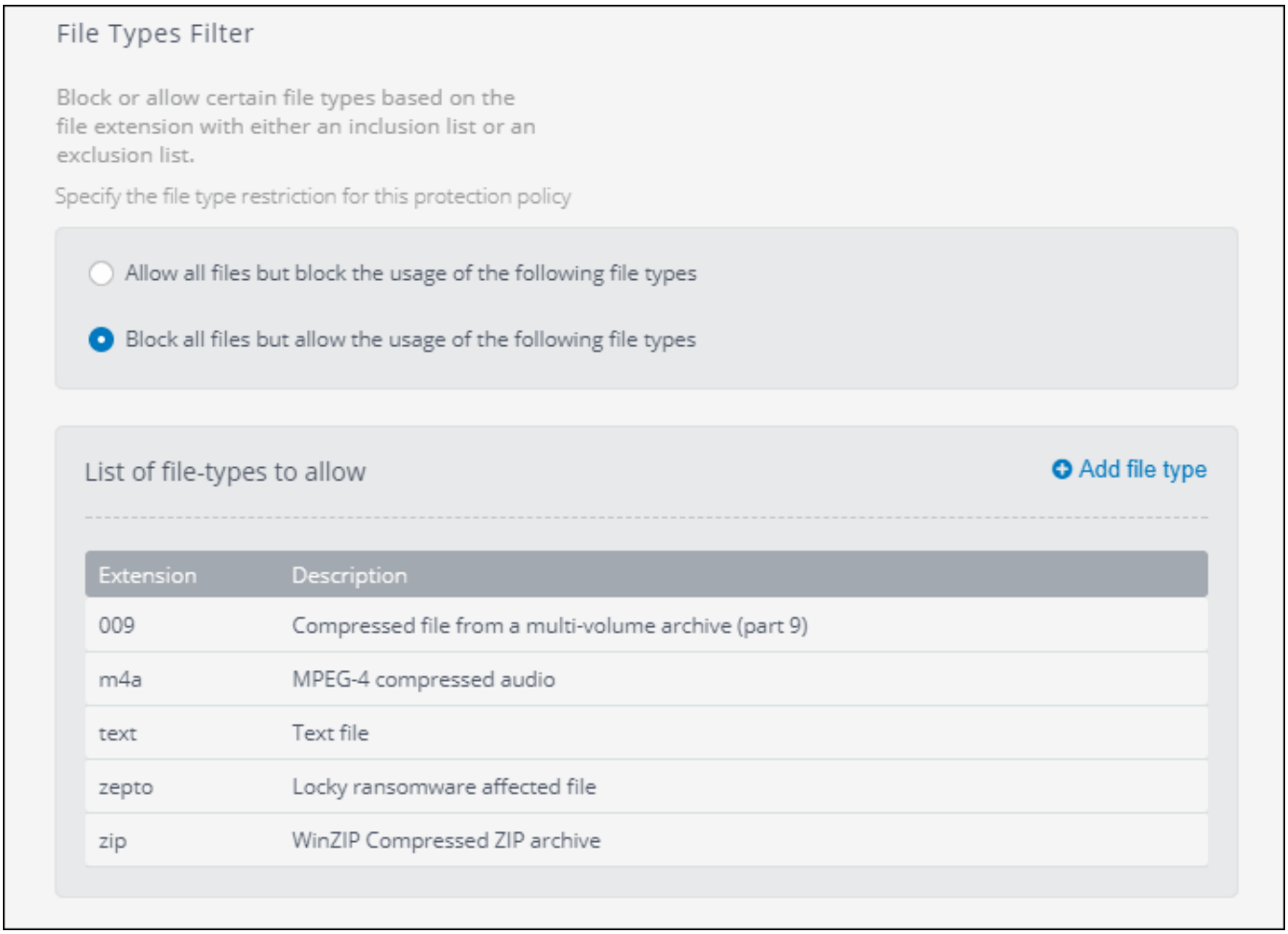


Screenshot 39: Permission granted to device

8. Under **Devices Categories**, configure the access to device categories for this rule. The available permissions are:

Permission	Description
Full	User has full permissions to the files present in the device.
Read	User can see and read the files present in the device, but cannot edit, delete or save files on the device.
Write	User can read and edit the files in the devices, but cannot execute or delete files.
Block	User does not have any permission and access to the device is blocked.

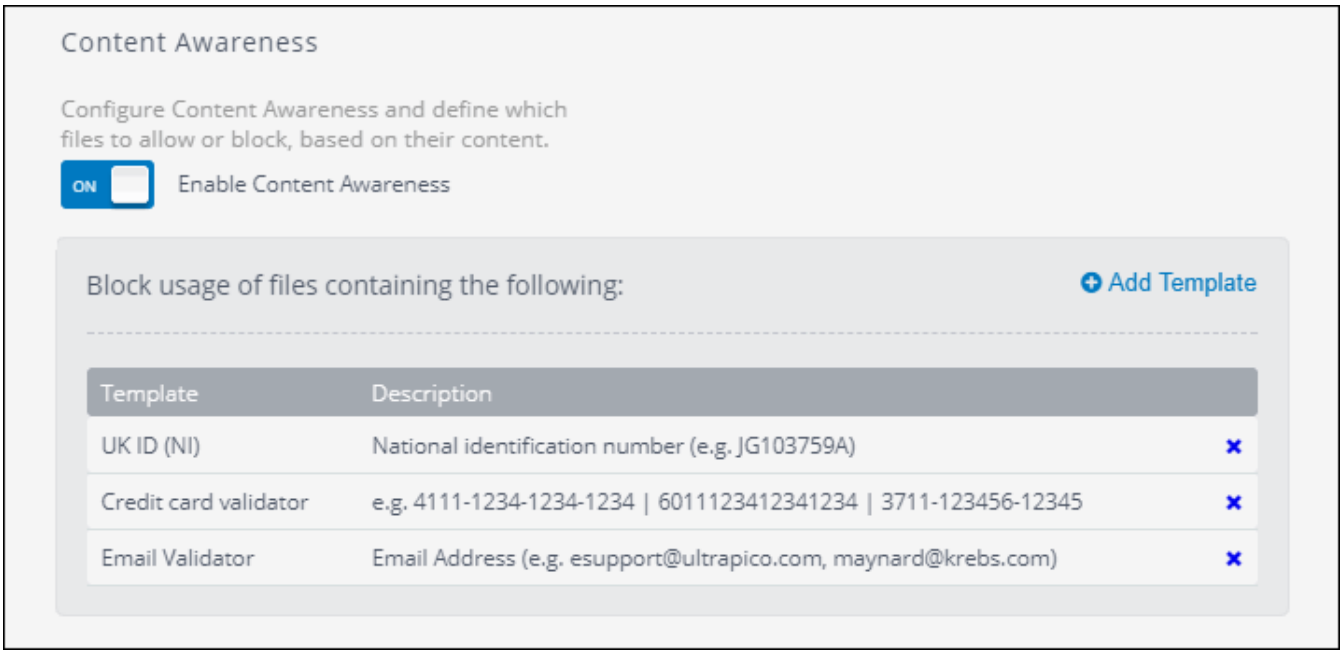
9. Repeat the operation above to grant permissions to **Connectivity Ports**.



Screenshot 40: Allow or block file types

10. Specify the file type restriction under **File Type filter**. These options are related to the List of file types. The options are:

Options	Description
Allow all files but block the usage of the following file types	Select this option to allow all file types except the files present in the File type list.
Block all files but allow the usage of the following file types	Select this option to block all files types except the files present in the File type list.



Screenshot 41: Content awareness options

11. Turn on or off **Enable Content Awareness**. Content Awareness enables you to specify the file content restrictions for a particular protection policy. The content awareness feature looks into files transiting the endpoints via removable devices and it identifies content based on pre-configured and custom regular expressions and dictionary files.

12. Select which file options define the threshold file size to process and how to handle archives. The options are:

Option	Descriptions
Ignore files larger than the following maximum file size	Select this option to enhance the speed of the scanning process passing without scan files large than the specified maximum size.
Block files large than the following maximum file size	Select this option to enhance security and block files that exceed the specified maximum size.

13. Specify the maximum file size to ignore or block.

14. Specify inside how many levels EndPoint Control should verify inside archives. The higher the number more security is added, but the scanning of files consumes more time.

15. Turn on or off the option to **Enable Device Encryption**. For more information, refer to Configuring encryption (page 62).

16. Use the **Blocklisted Devices** to specify devices that are always blocked. Use either the global blocklist or a custom list of blocked devices specifically for this rule. For more information, refer to Blocklist (page 59).

17. Use the **Whitelisted Devices** to specify devices that are always allowed. Use either the global whitelist or a custom list of allowed devices specifically for this rule. For more information, refer to Whitelist (page 57).

18. Slide **Alerts** to enable or disable notifications. When notifications are turned on, the following options are available:

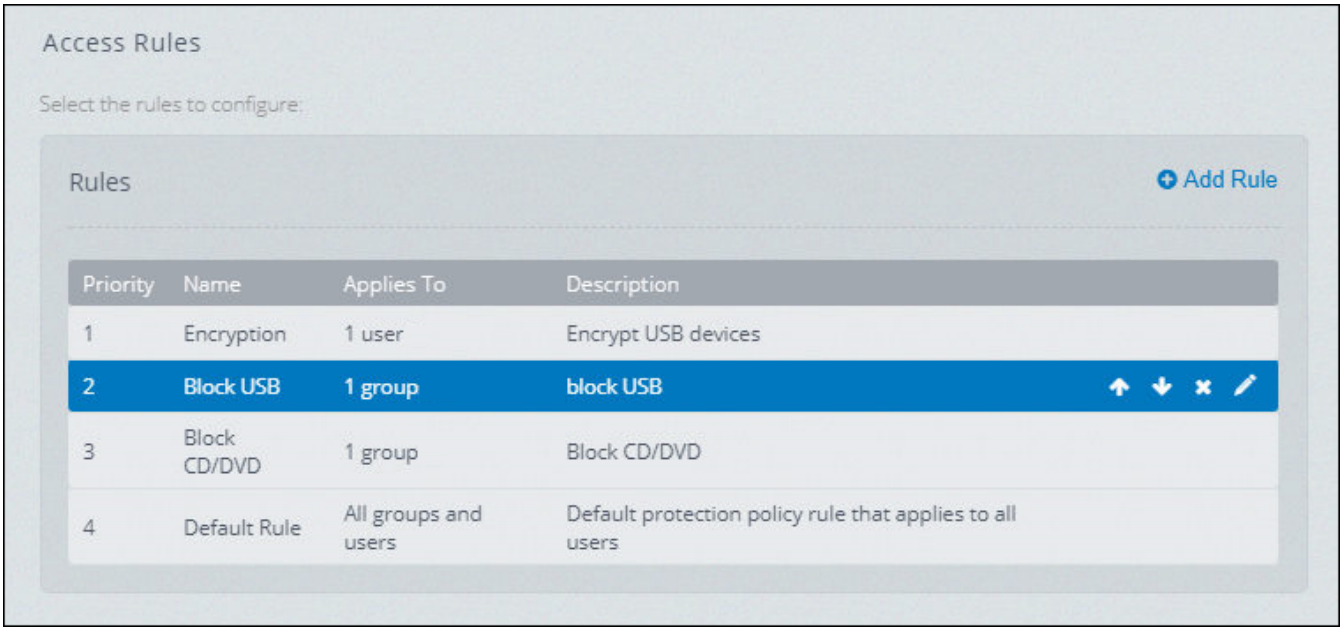
Option	Description
Send an email when Error Events occur	An alert is sent when an error occurs. For example, an agent is not responding.
Send an email when Violation Events occur.	An alert is sent on occasion of an access violation. For example, an invalid password or an agent stopped maliciously.
Send an email when Encrypted Device Mount Events occur	A notification is sent when a new encrypted device is mounted.
Send an email when Blocked Events (Full or Read) occur	An email is sent every time that a user tries to access a device that should be blocked.
Send an email when Access Events occur	An email is sent every time that a user accesses an allowed device.
Specify recipients you want to receive the digest.	By default, all administrators are set to receive the alerts. This option can be altered and new recipients can be added.

19. Click **Apply**.

3.6.4 Working with Access Rules

The Access Rules policy defines Endpoint Control rules based on users and groups and sets the priority of rule execution.

Rules are executed from top to bottom. Once a match is found, the policies below it are not applied. Thus, it is advisable to place the most specific, restrictive rules to block on top and leave a default rule on the bottom. It ensures access to every device that should be used in the network.



Screenshot 42: Access Rules list

> **NOTE**
> For a machine running in terminal services, the GFI OneGuard EndPoint Control policies based on users may not work properly. Hence, in such scenario, it is suggested to simply use the default rule that applies to all users.

Changing the priority

The priority of a rule is important to determine which rule is applied to a user or device. Once a rule is matched, the rules below it in the list are ignored.

To re-order the priorities:

1. Login to GFI OneGuard.
2. Go to **Manage > Groups**.
3. Locate the group you want to edit and click **Manage**.
4. Go to **Services > EndPoint Control**.
5. Under the **Access Rules** section locate the rule you want to move. Click the up arrow icon to increase the priority and the down arrow icon to decrease the priority.

Editing a rule

To modify an existing rule:

1. Login to GFI OneGuard.
2. Go to **Manage > Groups**.
3. Locate the group you want to edit and click **Manage**.
4. Go to **Services > EndPoint Control**.
5. Under the **Access Rules** section locate the rule you want to edit and click the  icon.
6. Make the modifications required. For more information, refer to Adding New Rule (page 52).
7. Click **Apply**.

Deleting a rule

To delete an existing rule:

1. Login to GFI OneGuard.
2. Go to **Manage > Groups**.
3. Locate the group you want to edit and click **Manage**.
4. Go to **Services > EndPoint Control**.
5. Under the **Access Rules** section locate the rule you want to delete and click the  icon.

3.6.5 Whitelist

Use the **Whitelisted Devices** to specify devices that are always allowed.

The whitelist allows the administrator to have policies that block the use of various categories and ports, while ensuring that the devices listed are always allowed.

You can use either the global whitelist or a custom whitelist to allow devices:

Type	Description
Global Whitelist	Can be set at service level and can affect all groups or devices when selected. To create a global whitelist go to **Manage > Services > EndPoint Control**.
Custom Whitelist	Can be set at group or device level and affects only the group of devices where it is created. To create a custom whitelist go to **Manage > Devices > EndPoint Control**.

The procedure to add a device to a whitelist is the same for the global and custom whitelist and consists of two steps:

Step 1: Obtain the Hardware ID

GFI OneGuard relies on the information stored in the Device Manager of the computer to which a device is plugged-in to obtain the hardware information and applies policies accordingly.

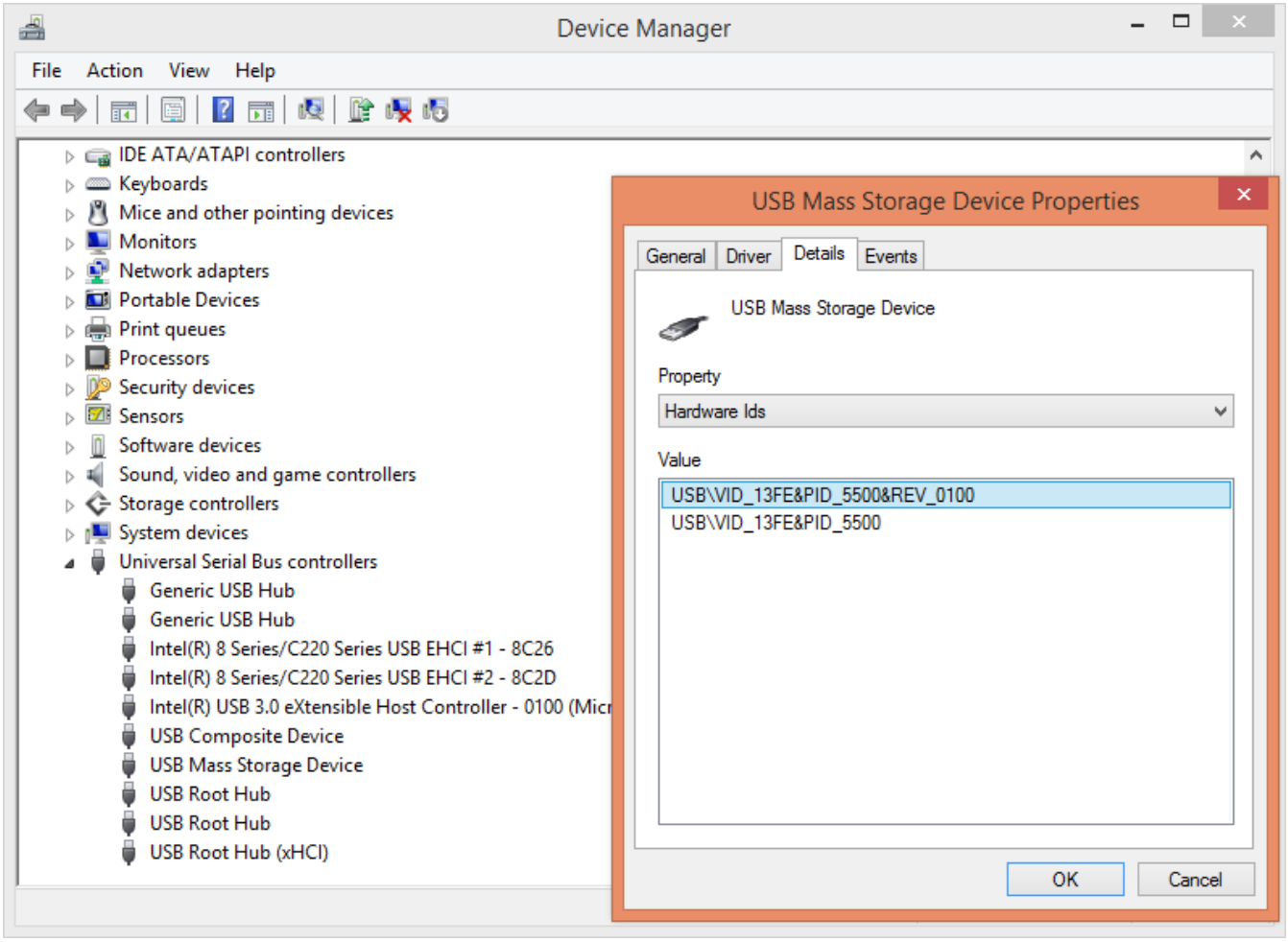
To obtain the hardware ID:

1. Open the **Panel Control** on the machine that the device is plugged.

2. Go to **Hardware and Sound > Device and Printers > Device Manager**.

3. Expand the category, right-click the device and select **Properties**.

4. Open the **Details** tab.



Screenshot 43: Device Manager showing hardware Ids

5. Under property select **Hardware Ids**.

6. Copy the items displayed in the **Value** textbox. By default more that one item is listed. The longer value on top is the one with more details and should be used.

Step 2: Add Hardware ID to exceptions to the Whitelist

1. Login to the GFI OneGuard Platform.

2. Go to **Manage > Devices**.

3. Select the entire Network or a specific group.

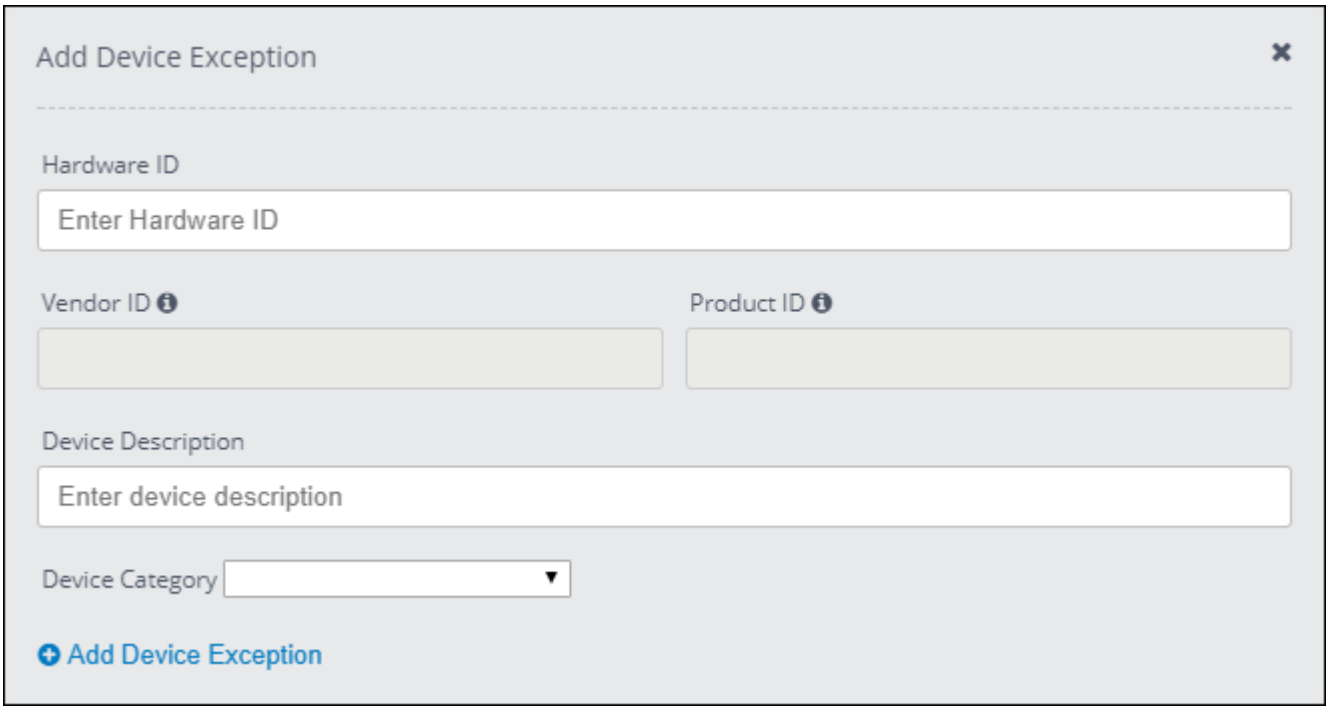
4. Go to **Services > EndPoint Control**

5. Click **Add Rule**.

6. Under **Whitelisted Devices** select the type of whitelist:

Type	Description
Global Whitelist	Set at platform level and applicable to all groups.
Custom Whitelist	Set at group level and applicable to all devices that have the specific policy applied.

7. Click **Add Device Exception**.



Screenshot 44: Options available to add a device to exception list

8. Enter the following information:

Field	Description
Hardware ID	Paste the Hardware ID copied in the previous step. Vendor ID and Product ID are automatically populated.
Device Description	Enter a description of the devices included in the list.
Device Category	Select a category from the drop-down list.

9. Click **Add Device Exception**.

3.6.6 Blocklist

Use the **Blocklisted Devices** to specify peripherals that are always blocked. The blocklist allows the administrator to have policies that allow the use of various categories and ports, while ensuring that the devices listed are always blocked.

You can use either the global blocklist or a custom blocklist to block devices:

Type	Description
Global Blocklist	Can be set at service level and can affect all groups or devices when selected. To create a global blocklist go to **Manage > Services > EndPoint Control**.
Custom Blocklist	Can be set at group or device level and affects only the group of devices where it is created. To create a custom blocklist go to **Manage > Devices > EndPoint Control**.

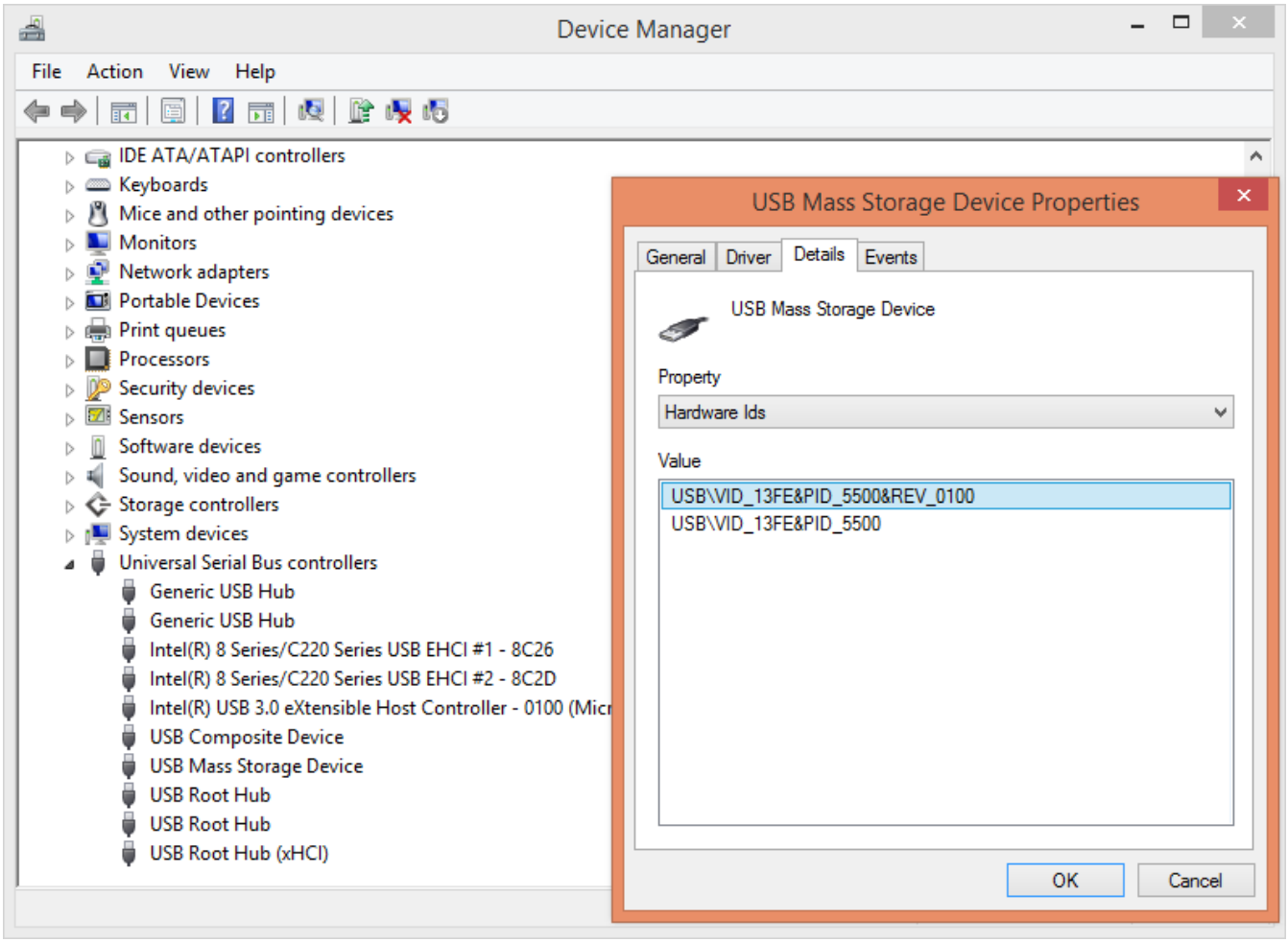
The procedure to add a device to a blocklist is the same for both the global and custom blocklist and consists of two steps:

Step 1: Obtain the Hardware ID

GFI OneGuard relies on the information stored in the Device Manager of the computer to which a device is plugged-in to obtain the hardware information and applies policies accordingly.

To obtain the hardware ID:

1. Open the **Panel Control** on the machine that the device is plugged.
2. Go to **Hardware and Sound > Device and Printers > Device Manager**.
3. Expand the category, right-click the device and select **Properties**.
4. Open the **Details** tab.



Screenshot 45: Device Manager showing hardware Ids

5. Under property select **Hardware Ids**.

6. Copy the items displayed in the **Value** textbox. By default more that one item is listed. The longer value on top is the one with more details and should be used.

Step 2: Add Hardware ID to exceptions on the Blocklist

1. Login to the GFI OneGuard Platform.

2. Go to **Manage > Devices**.

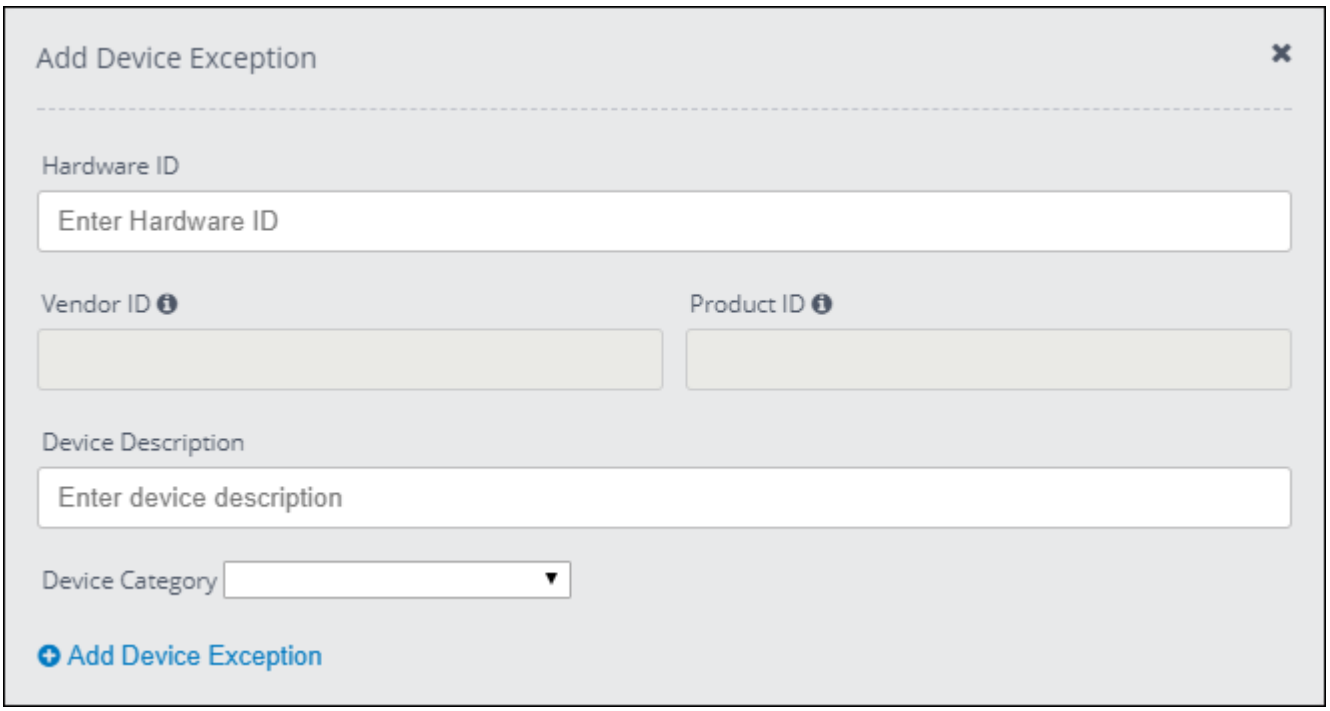
3. Select the entire Network or a specific group.

4. Go to **Services > EndPoint Control**.

5. Under **Blocklisted Devices** select the type of blocklist:

Type	Description
Global Blocklist	Set at platform level and applicable to all groups.
Custom Blocklist	Set at group level and applicable to all devices that have the specific policy applied.

6. Click **Add Device Exception**.



Screenshot 46: Options available to add an device to exception list

7. Enter the following information:

Field	Description
Hardware ID	Paste the Hardware ID copied in the previous step. Vendor ID and Product ID are automatically populated.
Device Description	Enter a description of the devices included in the list.
Device Category	Select a category from the drop-down list.

8. Click **Add Device Exception**.

3.6.7 Configuring encryption

Encryption plays an important role in security because it ensures that information that could be intercepted by non-authorized third-parties is not accessible. Peripherals like USB sticks can be easily misplaced and cause facilitated data loss.

GFI OneGuard EndPoint Controls enables you to configure settings specifically catered to encrypted devices, ensuring that only users with the necessary clearance can get access to the data stored in a device.

Screenshot 47: Encryption methods available

There are two types of encryption available:

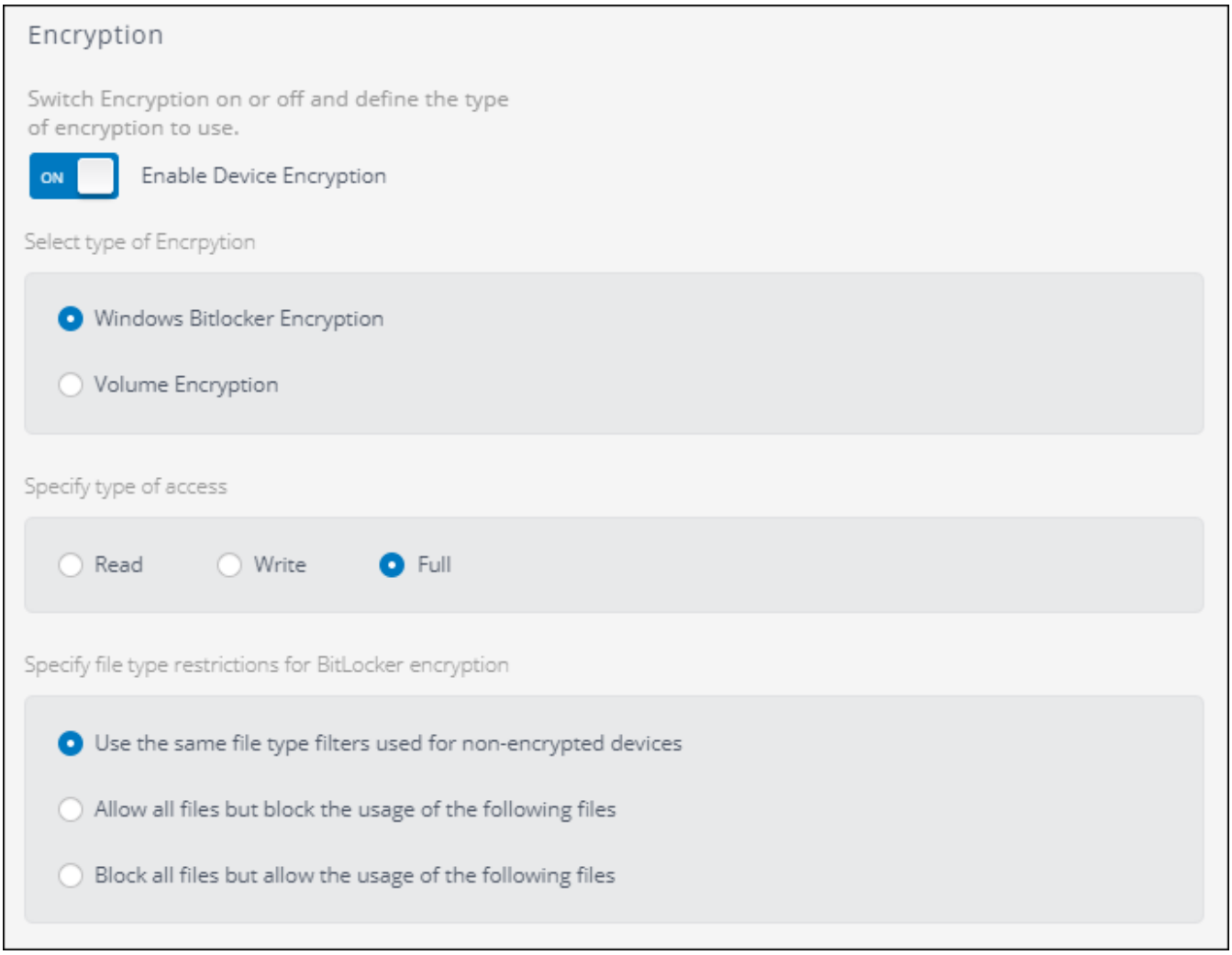
- Microsoft BitLocker
- Volume Encryption

Configuring Microsoft BitLocker

GFI OneGuard can detect storage devices encrypted with Microsoft BitLocker. When this option is selected, the encryption is performed by the operating system. This option only enables you to configure different permissions on such devices.

To enable Microsoft BitLocker detection:

1. Login to the GFI OneGuard Platform.
2. Go to **Manage > Devices**.
3. Select the entire Network or a specific group.
4. Go to **Services > EndPoint Control**
5. Click **Add Rule**.
6. Under Encryption Turn On **Enable Device Encryption** and check **Windows BitLocker Encryption**.



Screenshot 48: BitLocker encryption options

7. Specify the type of access the user should have to the device. The options are:

Option	Description
Read	User can open the files, but cannot edit or delete them.
Write	User can open and edit files. Users cannot run executable files.
Full	Full permissions including running executable files.

8. Specify the type of restrictions for file types. The options are:

Option	Description
Use the same file type used for non-encrypted devices	When this option is select the settings for the file type filtering used in the policy is applied.
Allow all files but block the usage the following files	This option overwrites the file type settings of the policy and allows all the files except those listed.

Option	Description
Block all files but allow the usage the following files	This option overwrites the file type settings of the policy and blocks all the files except those listed.

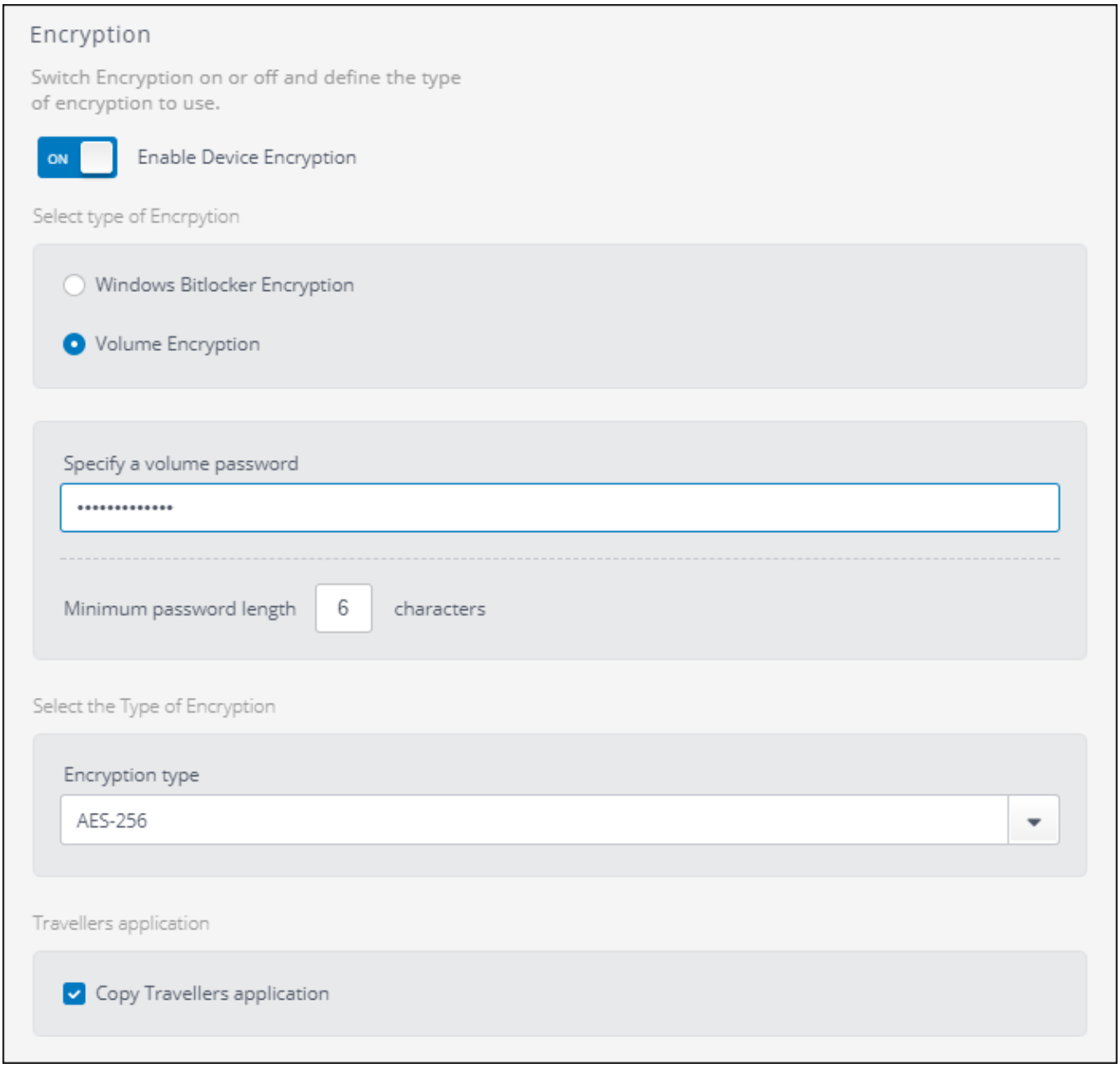
9. Click **Apply**.

Configuring Volume Encryption

Volume Encryption enables you to encrypt the contents of USB devices using AES 256 encryption. When volume encryption is enforced, users must provide a password to encrypt or access storage devices data.

To enforce Volume Encryption on installed agents:

1. LLogin to the GFI OneGuard Platform.
2. Go to **Manage > Devices**.
3. Select the entire Network or a specific group.
4. Go to **Services > EndPoint Control**
5. Click **Add Rule**.
6. Under Encryption Turn On **Enable Device Encryption** and check **Volume Encryption**.



Screenshot 49: Volume encryption options

7. Enter a password under **Specify a volume password**. This is the administrator password that is required to reset a password of a device if the user loses it.

8. Enter a numeral under **Minimum password length**. That value is applied when the user enter a password when encrypting a new device.

9. Select the Type of Encryption. The options are:

Option	Description
AES-128	This encryption algorithm is less secure, but uses less disk space for the encryption and the process of initial encryption is completed in less time. A better option for devices with little disk space.
AES-256	This encryption algorithm is more secure, but uses more disk space for the encryption and more time for the initial encryption. A better option when security is a concern and there is enough disk space.

10. Check the option to **Copy Travellers application** to enable this feature. The Traveler Application enables users to access encrypted content when they are away from the office and in locations where the EndPoint Control agent is not installed.

11. Click **Apply**.

3.6.8 Enabling notification

EndPoint Control allows administrators to enable notification. Alerts and notifications are crucial features of EndPoint Control operation. They allow you to take action immediately after a threat is detected.

Too many notifications can lead to important warns to get ignored. Use the evaluation period to test and find the right volume of notification required. In a production environment, it may be advisable to enable only part of the alerts till the right balance is found.

To turn on notification:

1. Login to GFI OneGuard admin console.

2. Go to **Manage > Groups**.

3. Locate the group you want to edit and click **Manage**.

4. Go to **Services > EndPoint Control**.

5. Locate the policy you want to receive notification and click **Edit**.

6. Browse to **Notification**.

7. Slide **Alerts** to Enable or disable notifications.

8. Check the types of alerts you want to enable. The following options are available:

Option	Description
Send an email when Error Events occur	An alert is sent when an error occurs. For example, an agent is not responding.
Send an email when Violation Events occur	An alert is sent on occasion of an access violation. For example, an invalid password or an agent stopped.
Send an email when Encrypted Device Mount Events occur	A notification is sent when a new encrypted devices is mounted.
Send an email when Blocked Events (Full or Read) occur	An email is sent every time that a user tries to access a device that was blocked.
Send an email when Access Events occur	An email is sent every time that a user accesses an allowed device.
Specify recipients you want to receive the digest	By default all administrator is set to receive the alerts. New recipients can be added to the list.

9. Click **Apply**.

3.6.9 Temporary Access

EndPoint Control enables administrators to grant temporary access to users. The Temporary Access feature allows time-limited access to peripherals like a USB or CD/DVD blocked by an EndPoint Control policy.

This feature can be used to give flexibility and manage exceptions without compromising security. For example, when a guest room that provides limited access to external clients needs to be used to hold a short conference.

When temporary access is granted, permissions and settings in the protection policy applicable to the target computer are temporarily overridden by the rules of the temporary access.

> **NOTE**
> File Type filtering and Content awareness settings are overridden during the time the temporary access is active.

There is not a standard procedure for administrator and user to exchange temporary access request and the unlock code. An email or any other communication means available in your organization can be used. The administrator should advise network users the best way to exchange the request and code with security.

The Temporary Access is granted for a limited time and is valid only during the time specified in the Temporary Access Settings.

> **NOTE**
> Be aware of time zone differences that can be present between the GFI OneGuard console and the end user device. Time settings on the remote computer are used.

The request for temporary access is composed of three steps:

1. Requesting temporary access to a protected device.
2. Granting temporary access to a protected device.
3. Entering the Access code into the device.

Step 1: Requesting temporary access to a protected device

The first step is to obtain a temporary access code from the device:

1. From the computer tray, right-click the GFI OneGuard agent icon .
2. Click **EndPoint Control Temporary Access**.

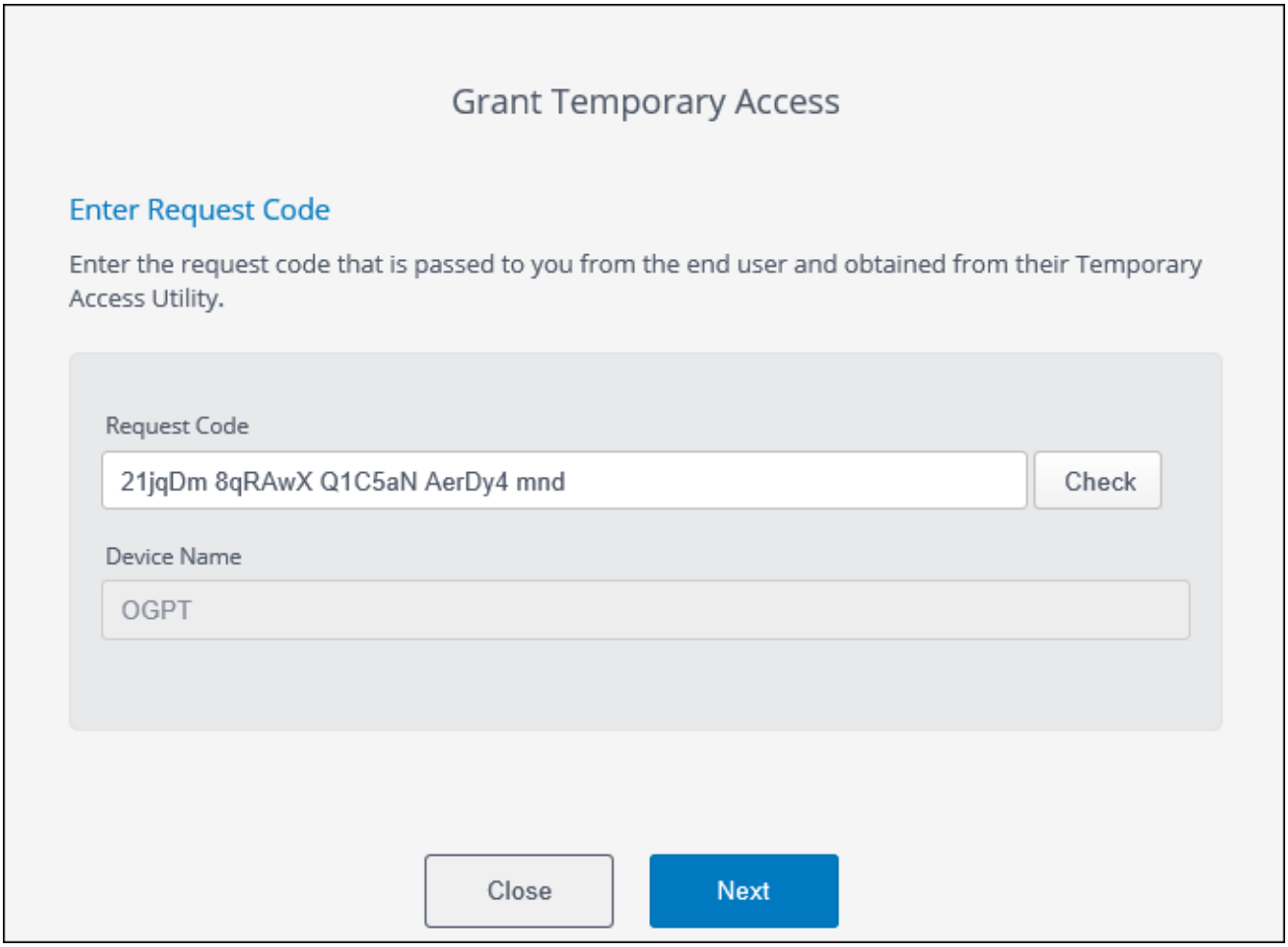
Screenshot 50: Temporary Access request form

3. Copy the **Request code** string and send it to the administrator together with the machine name.

Step 2: Granting temporary access to a protected device

Once the administrator receives the request for temporary access, the next step is to grant the access from the GFI OneGuard platform:

1. Login to the GFI OneGuard Platform.
2. Go to **Dashboard > EndPoint Control**.
3. Click **Grant Temporary Access**.



Screenshot 51: Grant Temporary Access window.

4. Paste the string sent by the user under the **Request Code** textbox and click **Check**.
5. The Device Name should appear. Click **Next**.
6. Enter the number of minutes to grant access for under the **Unlock the usage of device for:**
7. Select the start and end date and time that the request is valid under the **From:** and **To:** fields.
8. Check which categories have allowed access. Click **Next**.
9. Copy the **Unlock Code** and send to the user. Click **Finish**.

Step 3: Entering the Unlock Code into the device

Once the administrator sends back the Unlock code, insert it into the GFI EndPoint Control Temporary Access windows.

To insert the unlock code:

1. From the computer tray, right-click the GFI OneGuard agent icon .
2. Click **EndPoint Control Temporary Access**.

Screenshot 52: Unlock code inserted into the Temporary Access window

3. Insert the code sent by the administrator under **Unlock code**.
4. Click **Unlock**.

3.6.10 Resetting the password for an encrypted device

When using volume encryption to secure the device, a password is created to encrypt the device for the first time. If the user loses or forgets this password, the administrator can reset it using the **Reset User Password** tool.

Two different passwords are used in this process, and it is important to distinguish between them:

Password type	Description
Recovery password	The password used by the administrator to create the Encryption policy.
New user password	The password used by the administrator to reset a user's password. This password is used to decrypt the device's contents.

The **Reset User Password** can be used on any computer. You just need the encrypted device and the tool running on the same computer.

Screenshot 53: Reset User Password tool interface

To reset the password for an encrypted device:

1. Download the tool from http://go.gfi.com/?pageid=OG_PasswordRecoveryTool

2. Right-click the **PasswordRecoveryTool.zip** file and choose **Properties**. From the General tab, click **Unblock** and then **Apply**.

3. Extract the files from the compressed folder.

4. Double-click **passrecovery.exe**.

5. Select the device from the **Encrypted devices:** list.

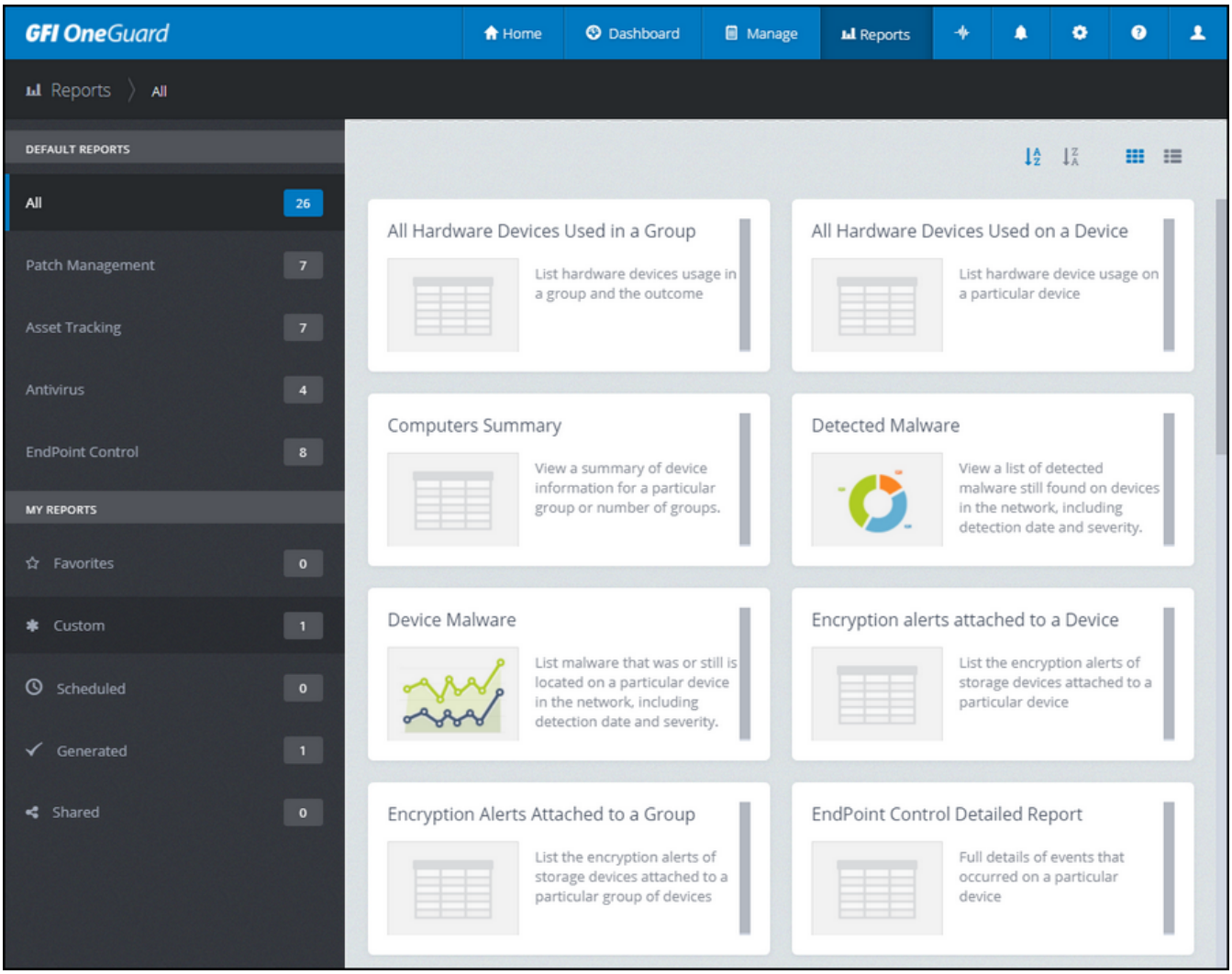
6. Enter the recovery password set by the administrator when creating the policy.

7. Type the new password for the device twice.

8. Click **Reset**.

3.7 Reports

GFI OneGuard ships with a suite of predefined reports, covering the functionality of the services provided. Each and every report can be customized as required, and generated immediately or saved as a new report.



Screenshot 54: List of all default reports.

To view the list of reports, go to the **Reports** tab. The menu on the left is divided in two sections:

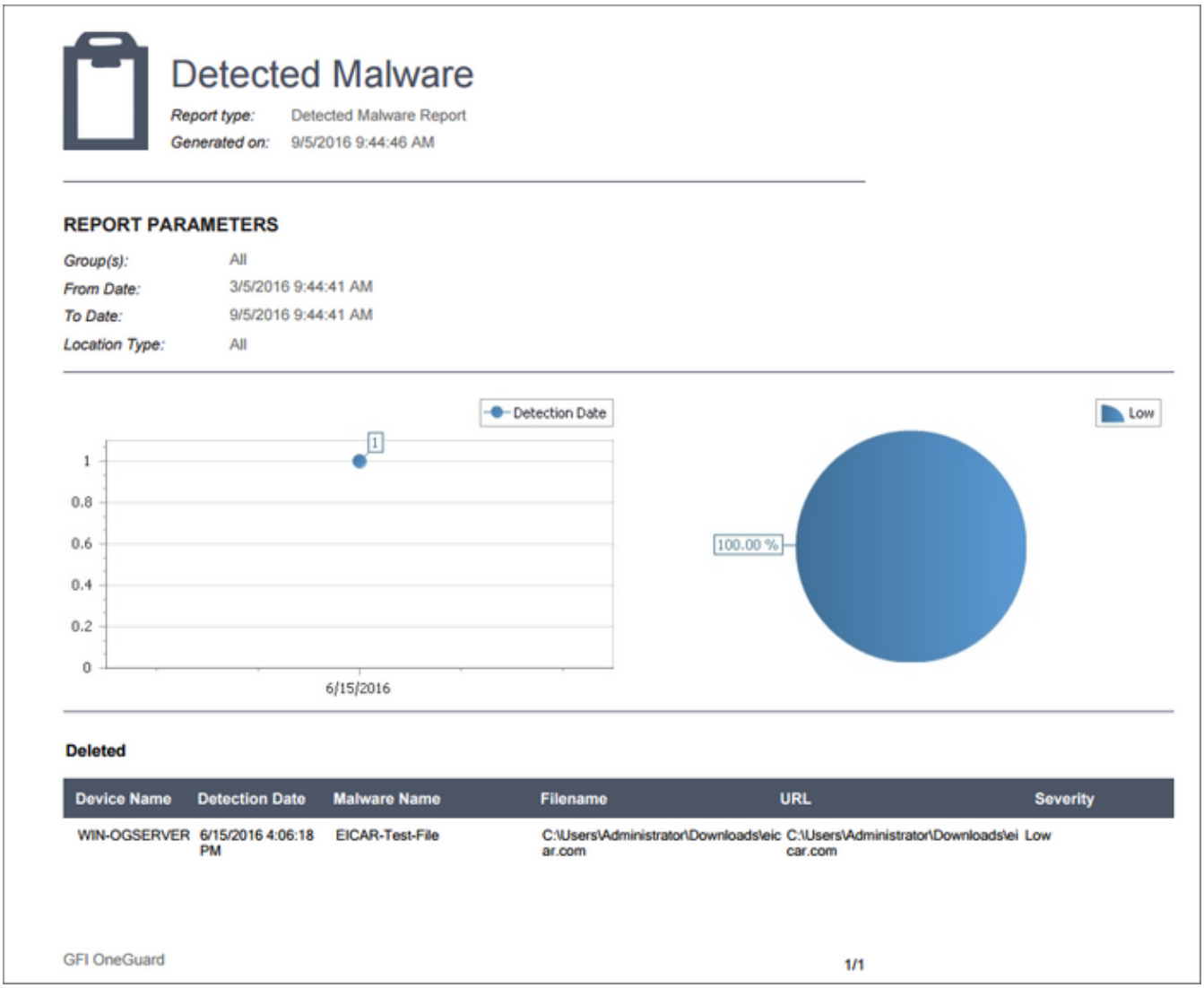
Default Reports: The Default Reports node host the reports for the services used by GFI OneGuard. Click the **All** option to see all the available default reports or in any individual service to see the reports related to it.

My Reports: Include the following report categories:

Report	Description
Favorites	List of reports added to the favorite list. Lunch a report and click **Add to favorites** to add it to this list.
Custom	Shortcut to pre-configured reports. Launch a report and customize its settings. Click **Save Report** to save the report to this category for easy access. For more information, refer to Custom reports (page 74).
Schedule	Any reports scheduled to run at a future date are automatically added to this list. For more information, refer to Scheduling reports (page 75).
Generated	All generated reports are available here. These include scheduled reports and one-off reports generated on-demand. . For more information, refer to Generating reports (page 71).
Shared	Any report shared with other users can be viewed here. For more information, refer to Viewing and sharing generated reports (page 73).

3.7.1 Generating reports

Generate reports to have an output file that you can download or print.



Screenshot 55: A report generated by GFI OneGuard

To generate a report:

1. Login to GFI OneGuard and click **Reports**.

2. Hover over the desired report and click **Generate**.

3. To generate and download a report without customizing settings, click the **Generate** button on the new screen. Alternatively edit the settings to customize the report.

4. From the **General** tab, configure report parameters. The parameters available may vary between different report types. The following table describes common parameters across reports:

Option	Description
Name	Rename the reports to easily remember the changes made.
Description	Add a description of the report being generated.
Group	Select the groups to be included in the report. Separating the report by groups keeps the report smaller and can help to organize the information by sectors.

Option	Description
Date	Set the cut-off date that the report should cover. Choose either a relative time period with respect to the date when the report is generated, for example, choose **Last 7 days** to show data for a week prior to the date when report is generated. Alternatively, choose a **Custom** date range with custom from and to dates. Limiting the date range helps to keep the reports into a manageable size.
Location	Select a particular location to be included in the report. Options are quarantine, blocked and deleted.
Format	Select a format for the output of the report. The available options are PDF and XLS (Microsoft Excel).

5. Reports also can also be scheduled or set to be sent via email.

6. When all data is configured, the report can be saved for future use. Click **Save Report** to save the changed made on the report. The saved report will be available in the **Custom** node of the **Reports** screen.

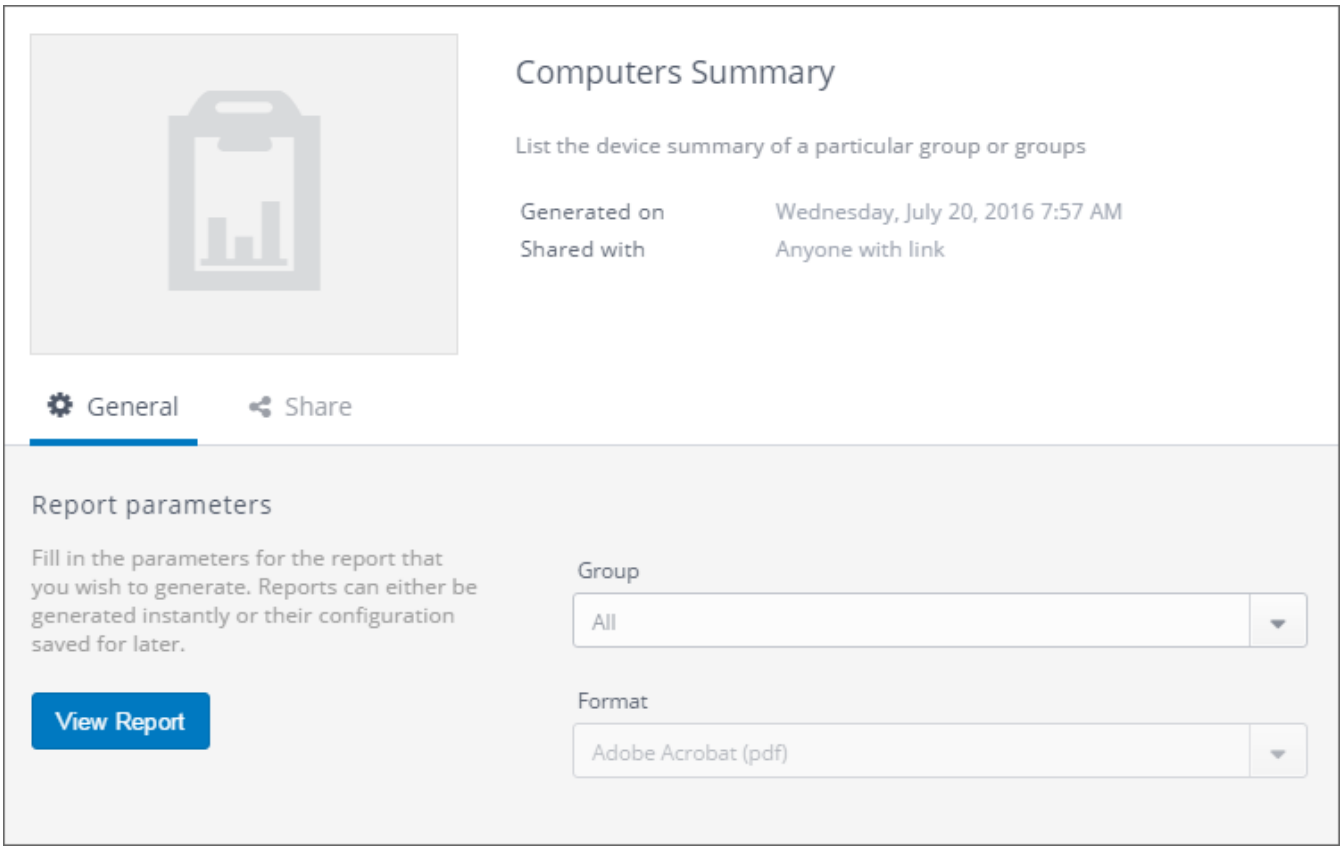
7. Click **Generate** to create the report. The new report will be made available under the **Generated** node of the **My Reports** section when generation is complete.

3.7.2 Viewing and sharing generated reports

Generated reports can be viewed, shared or downloaded. To access a generated report:

1. Login to GFI OneGuard and click **Reports**.

2. Click **Generated** in the left pane.



Screenshot 56: Accessing a generated report

3. Hover over a desired report and click **View Details**.

4. Select from the following actions:

Action	Steps
View reports	Under the **General** tab, click **View Report** to open the report in an Internet browser.
Download reports	Click the download icon  in the top right corner to download a copy of the report. The format of the download depends on the format indicated in the report settings. Default reports are set to PDF.
Share reports	GFI OneGuard can be configured to create a unique link to a report to allow it to be shared with others. To Share a Report: 1. Under the **Share** tab turn on the **Share Link**. A link for the report is displayed. 2. Select with whom to share the link. • Anyone with the link. • Anyone with access to the same instance of GFI OneGuard. 3. Copy the **Link to Report** and send it to whom you want to share the report with. Instruct the person to paste the link in a browser and the report is automatically downloaded on their computer. Shared reports are available under the **shared** node of **My Reports**.

3.7.3 Custom reports

Custom reports are pre-configured reports with custom data filters that are readily available whenever required.

To access the list of custom reports, from the left pane go to **My Reports > Custom**.

Creating a custom report:

1. Hover over a default report that will serve as the basis of your scheduled report and click **Generate**.

2. Specify a report name by clicking on the report name at the top and keying in the custom name. Report names must be unique.

3. Click on the report description underneath the name and key in a friendly description of the report to help you understand the aim of the report.

4. From the **General** tab, configure report options. The options available may vary between different report types. The following table describes common options across reports:

Option	Description
Name	Rename the reports to easily remember the changes made.
Description	Add a description of the report being generated.
Group	Select the groups to be included in the report. Separating the report by groups keeps the report smaller and can help to organize the information by sectors.
Date	Set the cut-off date that the report should cover. Choose either a relative time period with respect to the date when the report is generated, for example, choose **Last 7 days** to show data for a week prior to the date when report is generated. Alternatively, choose a **Custom** date range with custom from and to dates. Limiting the date range helps to keep the reports into a manageable size.
Location	Select a particular location to be included in the report. Options are quarantine, blocked and deleted.
Format	Select a format for the output of the report. The available options are PDF and XLS (Microsoft Excel).

5. Reports can also be scheduled or sent via email.

6. Click **Save Reports** to save the changes made as a custom report.

Generating a custom report:

To generate a custom report, go to **Reports > My Reports > Custom**. Hover over the desired report and click **Generate** to open the report card. Click **Generate** to initiate report generation.

Editing a custom report:

To generate a custom report, go to **Reports > My Reports > Custom**. Hover over the desired report and click **Generate** to open the report card. Review the **General**, **Schedule** and **Mail** tabs, and apply the required changes. Click **Save Report**.

Deleting a custom report:

To delete a custom report, go to **Reports > My Reports > Custom** and click **Generate** on the report to delete. Click the bin icon  in the top right hand corner. Click **OK** to confirm deletion.

> **IMPORTANT**
> Deleted reports are permanently removed and are not recoverable.

3.7.4 Scheduling reports

GFI OneGuard reports enable you to generate reports on a pre-defined schedule to automate the generation of reports that are required on regular basis. Scheduled reports are sent via email to a custom list of email addresses at a particular frequency.

To open the list of scheduled reports, from the left pane go to **My Reports > Scheduled**.

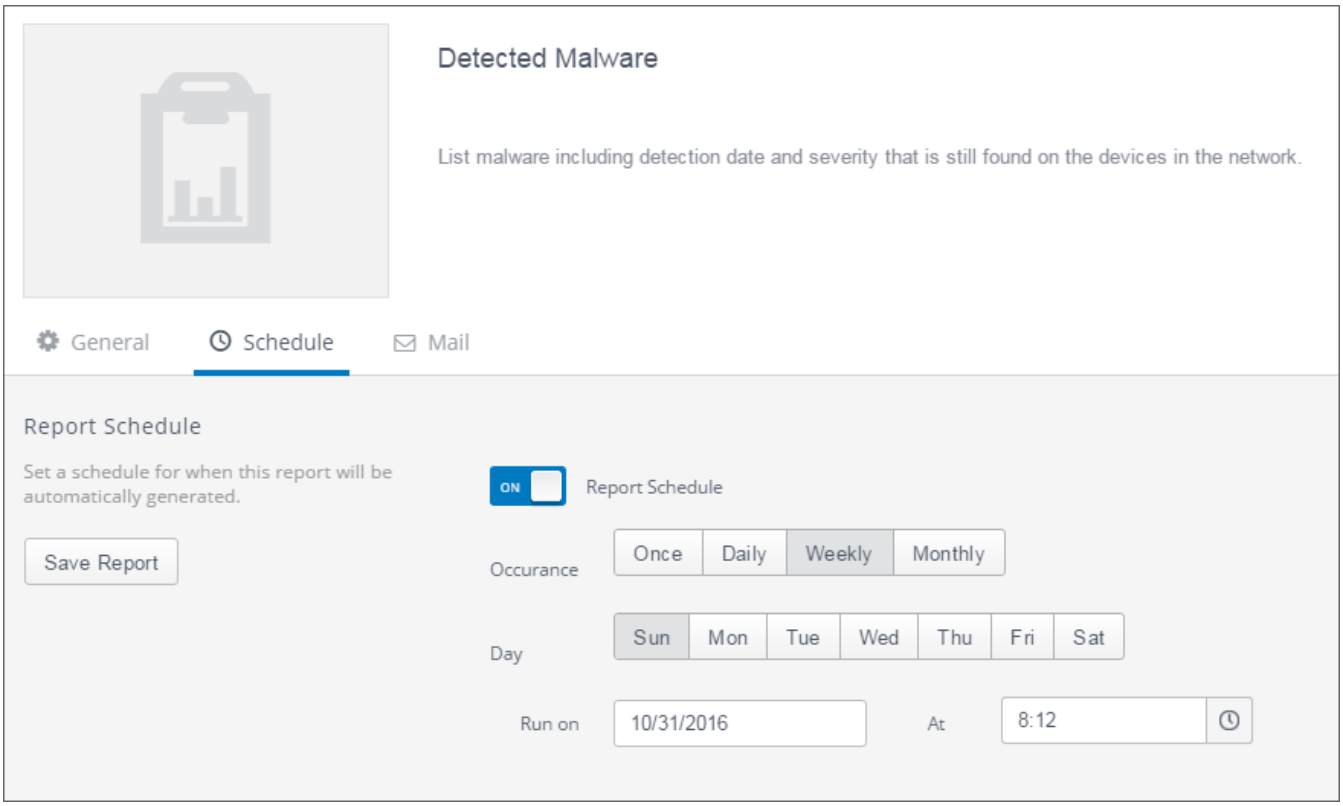
Creating a scheduled report

1. Hover over a default or a custom report that will serve as the basis of your scheduled report and click **Generate**.

2. Specify a report name by clicking on the report name at the top and keying in the custom name. Report names must be unique.

3. Click on the report description underneath the name and key in a friendly description of the report to help you understand the aim of the report.

4. From the **General** tab, configure report options to define the data and metrics for the report. When done click the **Schedule** tab.



Screenshot 57: Schedule reports settings.

5. Turn on **Report Schedule**.

6. In the **Occurrence** field, choose how frequent the scheduled report is to be generated. Select the interval and configure the appropriate schedule:

Occurrence interval	Description
Once	Generates a one-time report. Choose the date and time when to generate the report.
Daily	Generates the report every day. Choose the time of day when to generate the report.
Weekly	Generates the report every seven days. Choose the day of the week and the time when to generate the report.
Monthly	Generates the report once every month. Choose a particular first or last weekday of the month and the time when to generate the report.

7. Click **Save Report**.

The reports are generated on the configured schedule and will be available in the **Generated** tab. You can also send the scheduled reports via email.

Modifying a scheduled report

To modify any of the settings of a scheduled report, for example the report data or the frequency of the report, go to **My Reports > Scheduled** and click **Generate** on the report to edit. Customize settings from the **General** or **Schedule** tabs and when ready, click **Save Report**.

Deleting schedule reports

To delete a scheduled report, go to **My Reports > Scheduled** and click **Generate** on the report to delete.

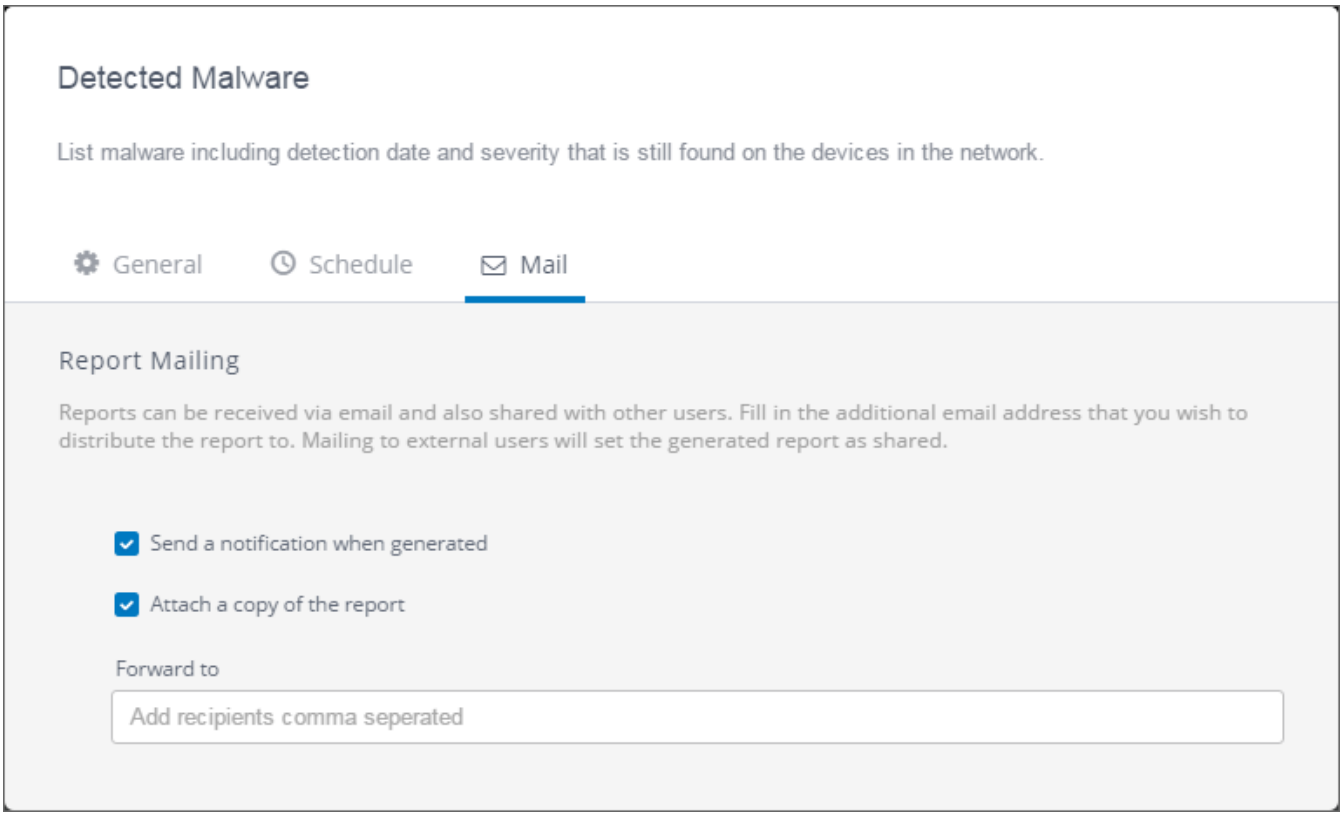
Click the bin icon in the top right hand corner. Click **OK** to confirm deletion.

> **IMPORTANT**
> Deleted reports are permanently removed and are not recoverable.

3.7.5 Sending reports via email

This topic describes how to configure GFI OneGuard to send generated reports via email:

1. Login to GFI OneGuard and click **Reports**.
2. Hover over a default, custom or scheduled report and click **Generate**.
3. Click the **Mail** tab.



Screenshot 58: Sending a report via email

4. Select **Send a notification on report generation** to send an email when the report is generated.
5. Optionally, you may select **Attach a copy of the report** to add the generated report as an attachment to the email.
6. Add the recipients in the **Forward to** field. Separate multiple recipients using a comma.
7. To generate and send the report immediately, go to the **General** tab and click **Generate**. Alternatively, if this report is part of a schedule, go to the **General** tab and click **Save Report** so that when the report gets generated, it also gets sent via email.

3.7.6 Deleting reports

Generated and custom reports can be deleted at any time.

> **NOTE**
> Default reports cannot be deleted.

To delete a report:

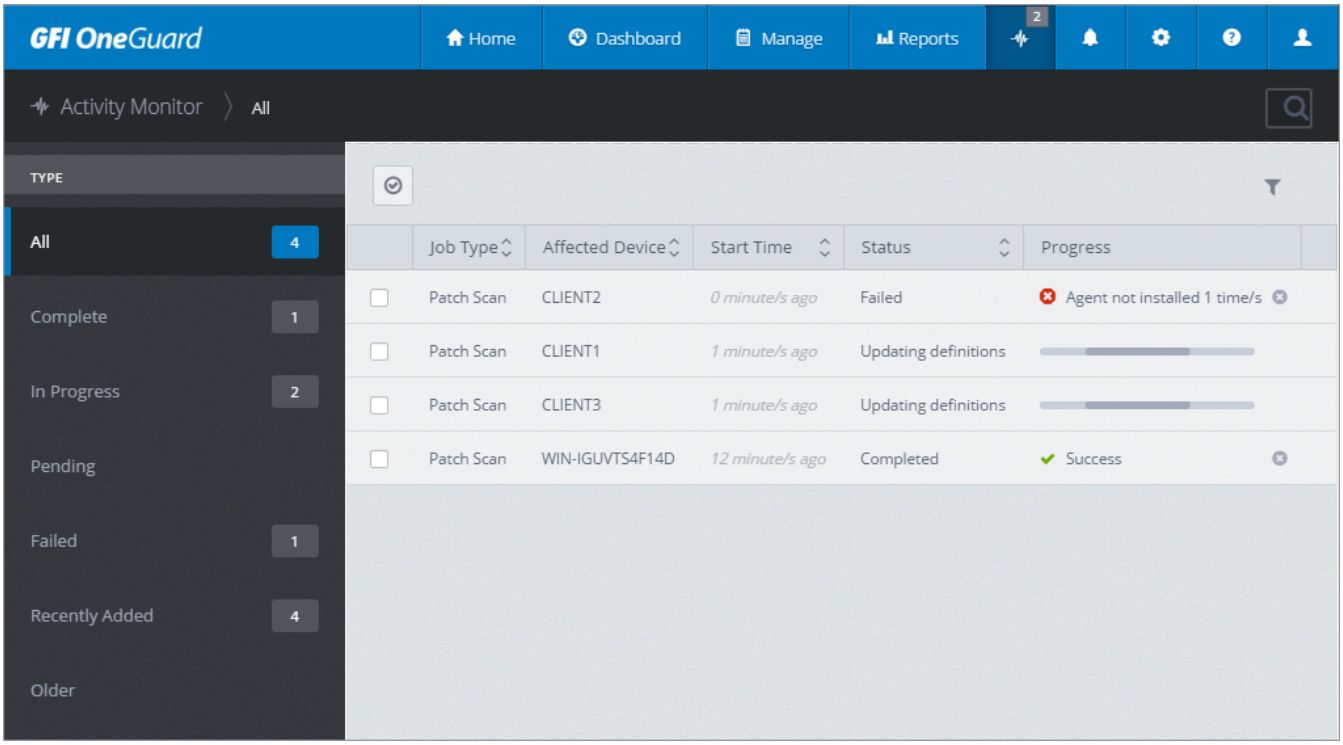
1. Open the report to delete by clicking **Generate**.

2. Click the bin icon in the top right hand corner.

> **IMPORTANT**
> Deleted reports are permanently removed and are not recoverable.

3.8 Activity Monitor

The Activity Monitor is a dashboard offering a view of tasks performed by GFI OneGuard in various states. This dashboard helps identify and fix issues in real-time. To open the Activity Dashboard, login to GFI OneGuard and click the icon from the top navigation.



Screenshot 59: The GFI OneGuard Activity Dashboard

The dashboard offers the following views:

View	Description
All	Shows all tasks performed by GFI OneGuard.
Complete	Lists tasks that are completed successfully.
In Progress	Displays tasks currently in progress.
Pending	Lists pending jobs.
Failed	Shows a list of jobs that failed. Jobs are classified as failed after 10 unsuccessful attempts.

View	Description
Recently Added	Displays recently added jobs.
Older	A history of all the jobs performed by GFI OneGuard.

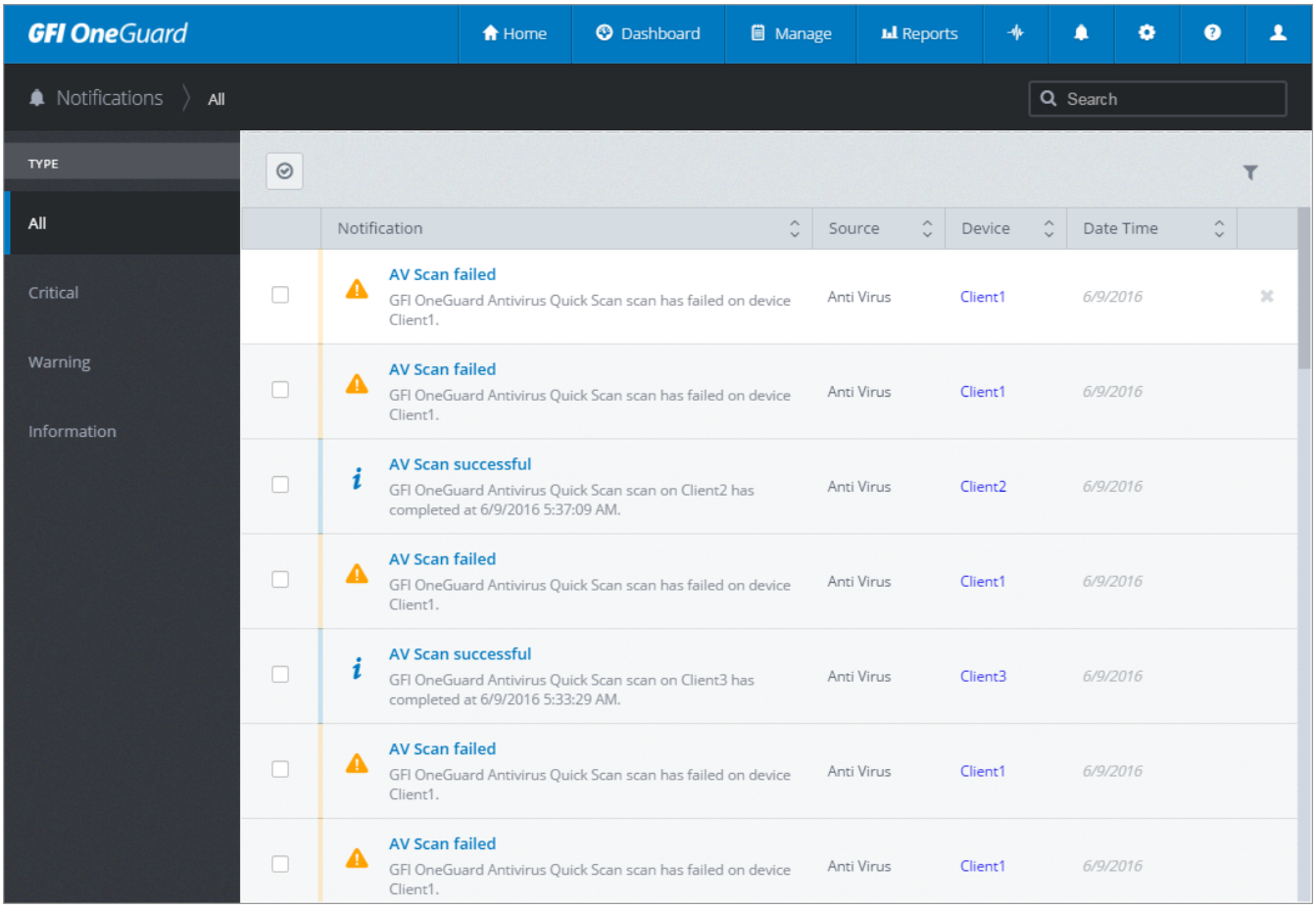
For each of these views you can select jobs either one by one or all at once and remove them from the lists by clicking **Delete** or the delete icon .

You can use the available filters to search for particular jobs. To open the filter, click . Select from the following:

Filter	Description
Job Type	Click the drop down list to select from the available job type options. The list refreshes automatically.
Status	Click the drop down list to select from the available job status options. The list refreshes automatically.
Device	Enter a device name to display information about a particular device. This filter shows devices with a name that matches the sequence of characters entered.

3.9 Notifications Area

In the notifications area you can view system generated notifications for events related to GFI OneGuard services. To access this area, from the top navigation, click .



Screenshot 60: The Notifications area

Perform the following actions:

Action	Description
Type	Use the menu on the left to filter notifications by type. Available filters: **All**, **Critical**, **Warning** or **Information**.
Select all	Click  to select all notifications.
Select single item	To select specific notifications, select the checkbox next to the desired notification.
Delete	Use the **Delete** button to remove selected notifications.
Mark as read	Select unread notifications and use this action to mark them as read.
Mark as unread	Select read notifications and use this action to mark them as unread.
Advanced Filter	Use the advanced filter to sort the view by period, source, group, device name and read or unread.

4 Settings

This topic contains information about the following advanced system settings for the GFI OneGuard Platform and GFI OneGuard Controller:

4.1 System settings 81
4.1.1 Mail server SMTP information 82
4.1.2 Proxy settings 83
4.1.3 Network Control 84
4.1.4 Notification Settings 86
4.1.5 Platform updates 86
4.1.6 Licensing 87
4.1.7 Roles and Permissions 88
4.1.8 Creating a new role 89
4.1.9 Editing an existing role 90
4.1.10 Role assignment 91
4.2 User profile settings 92
4.3 Controller configuration 93
4.3.1 Monitoring the Controller's status 94
4.3.2 Controller settings 94
4.4 How to backup GFI OneGuard configuration 97
4.4.1 Step 1: Stop GFI OneGuard services 97
4.4.2 Step 2: Backup folders 97
4.4.3 Step 3: Start the GFI OneGuard services 98
4.5 Securing Platform communications 98
4.6 Managing multiple domains 100
4.7 Controlling workgroups 101

4.1 System settings

Log in to the GFI OneGuard Platform and click **Settings** to configure important operational settings. From the left pane choose the settings to configure and apply the necessary changes.

On completion, save and apply all settings by clicking **Save Settings** in the yellow toolbar.

Section	Description
SMTP Settings	Enter your mail server SMTP information to enable GFI OneGuard to send email notifications.
Proxy Settings	If the server on which GFI OneGuard is installed, connects to the internet through a proxy server, configure the proxy details in this node.

Section	Description
Network Control	Settings related to GFI OneGuard Controllers, how these communicate with the Platform and credentials used to deploy Agents on discovered devices.
Notifications settings	A list of users and email addresses that receive email notifications when key events occur.
Platform updates	Monitor and configure how GFI OneGuard downloads and installs updates issued by GFI Software for the Platform.
Licensing	Review and configure information related to your GFI OneGuard license.
Roles & Permissions	Roles can be granted permissions to various functions within GFI OneGuard. Configure different roles and assign users or groups to these roles to enable them to use or configure GFI OneGuard.

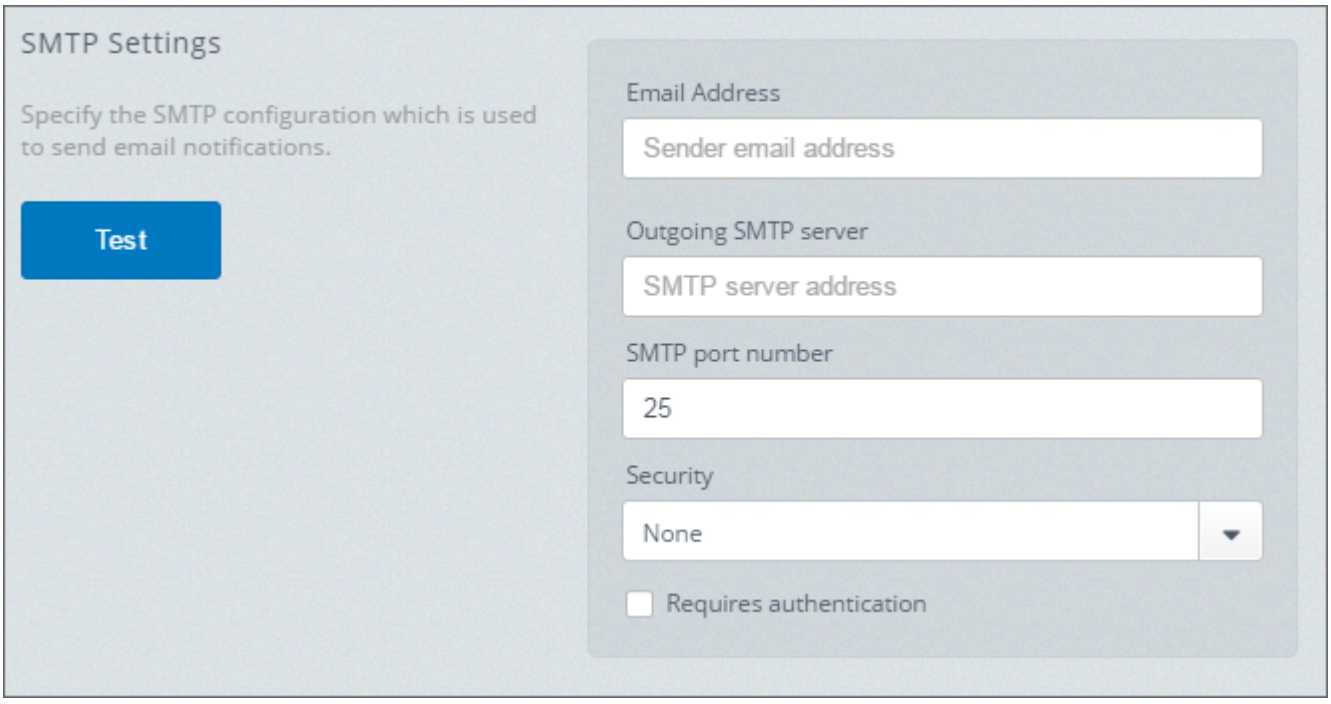
4.1.1 Mail server SMTP information

GFI OneGuard requires your mail server SMTP information to enable GFI OneGuard to send email notifications.

To configure the SMTP settings:

1. Log in to the GFI OneGuard Platform and click **Settings**.

2. From the left pane choose **SMTP Settings**.



Screenshot 61: SMTP settings options

3. Configure the following options:

Option	Description
Email Address	Enter the sender email address displayed for emails sent by GFI OneGuard.
Outgoing SMTP server	Type the IP address or hostname of the mail server.
SMTP port number	Enter the SMTP port number used by the mail server to send and receive emails.

Option	Description
Security	Select the type of security and encryption technology required by the mail server. The options available are: » None » SSL » TLS
Requires Authentication	Check this option if the mail server requires the sender to be authenticated before sending emails. If authentication is required, type the credentials to be used to authenticate with the mail server. It is recommended to use an account for which the password does not get regularly changed, as otherwise these credentials will become invalid and emails may fail until they are manually updated.

4. Click **Test** to ensure that GFI OneGuard can use the specified mail server to send emails.

5. On completion, click **Save Settings** to save and apply changes.

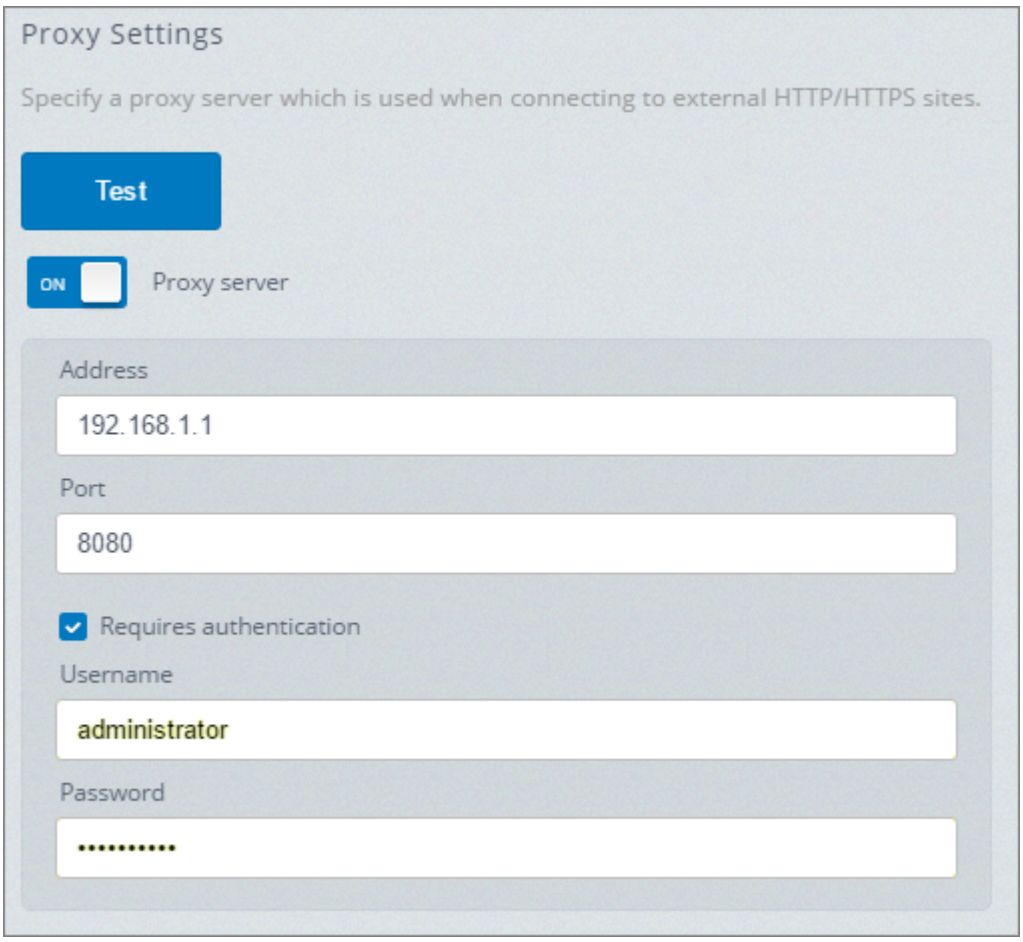
4.1.2 Proxy settings

GFI OneGuard requires internet access for various features, such as when checking for patches and antivirus definitions. If the server on which GFI OneGuard is installed, connects to the internet through a proxy server, configure its details.

To configure the Proxy settings:

1. Log in to the GFI OneGuard Platform and click **Settings**.

2. From the left pane choose **Proxy Settings**.



Screenshot 62: Proxy settings configuration

3. Change the **Proxy server** option to **ON** and configure the following options:

Option	Description
Address	Type the IP address or hostname of the proxy server.
Port	Enter the port number used to communicate with the proxy server.
Requires authentication	Check this option if the proxy server requires authentication. If required, type the credentials to be used to authenticate with the proxy server. It is recommended to use an account for which the password does not get regularly changed, as otherwise these credentials will become invalid causing internet access downtime until these credentials are updated.

4. Click **Test** to ensure that GFI OneGuard can use the specified proxy server to connect to the Internet.

5. On completion, click **Save Settings** to save and apply changes.

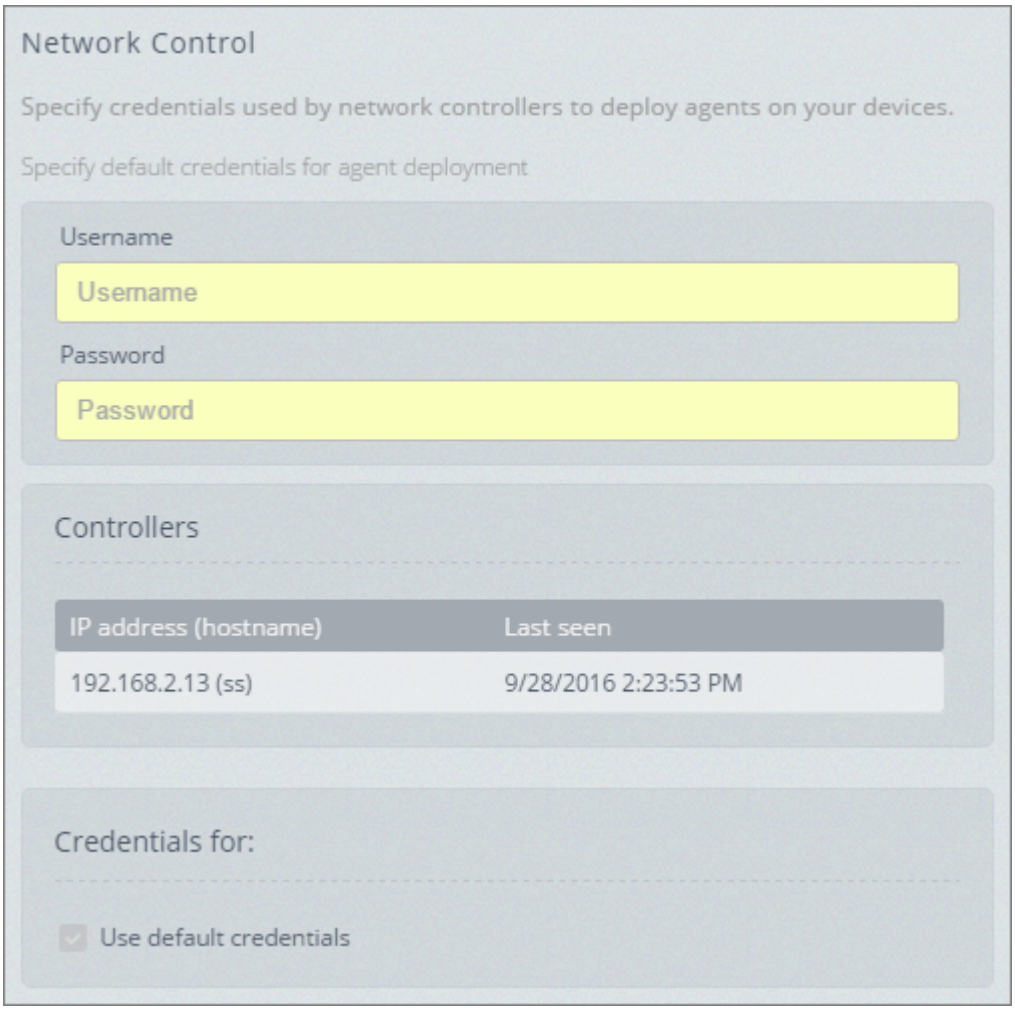
4.1.3 Network Control

Network control contains settings related to GFI OneGuard Controllers, how these communicate with the Platform and credentials used to deploy Agents on discovered devices.

To configure the Network Control:

1. Log in to the GFI OneGuard Platform and click **Settings** .

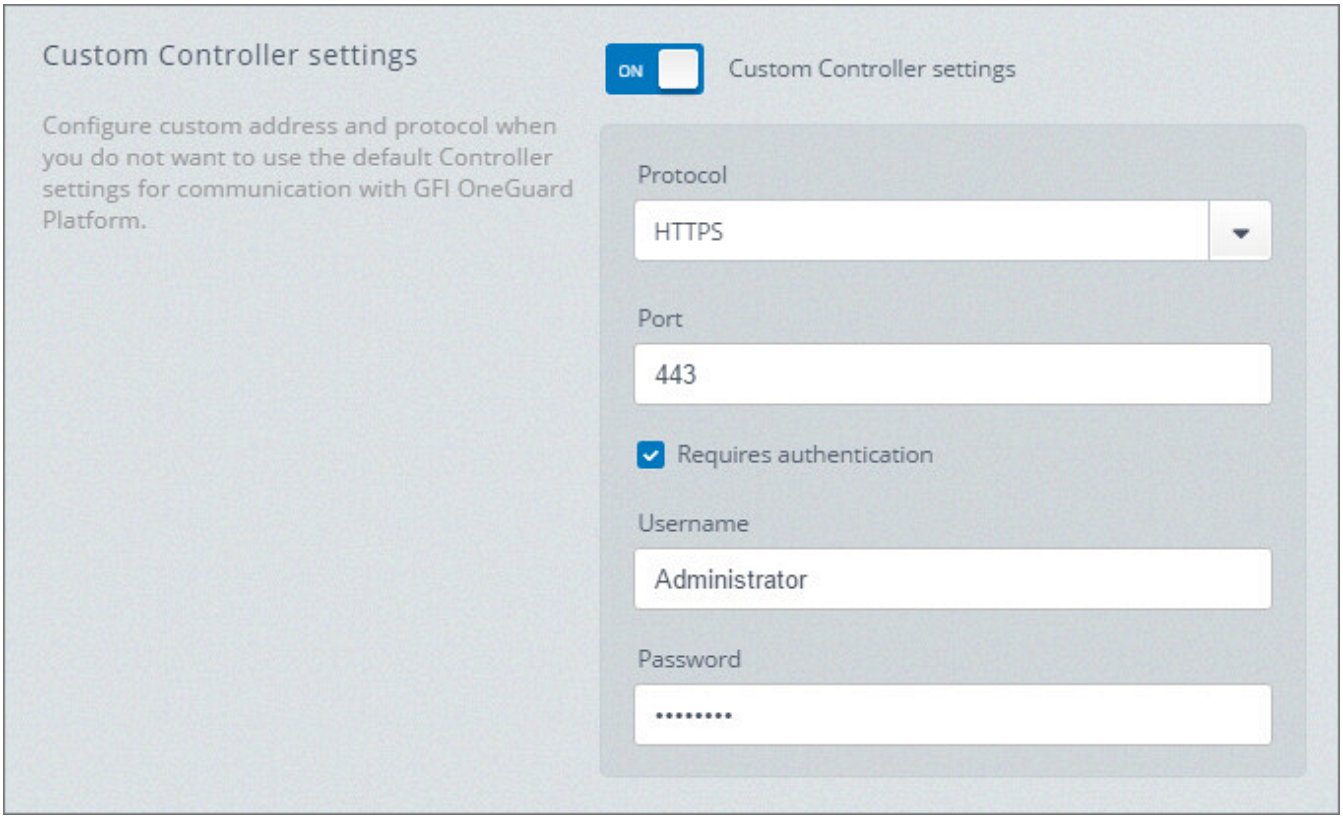
2. From the left pane choose **Network Control**.



Screenshot 63: Network control settings

3. Configure the following features in the **Network Control** area:

Feature	Description
Default Username & Password	Enter the **Username** & **Password** of an account that will be used by Controllers to scan the network, deploy agents and run GFI OneGuard services on managed machines. These credentials are used when no custom credentials are entered per Controller (read more below). The account used must have administrative rights on managed machines and sufficient permissions to deploy software. When a Controller is deployed in a domain environment, the account must also have read access to Active Directory to enable enumeration of machines on the network. Note that custom credentials can also be configured by device. For more information, refer to Customizing device login credentials (page 26).
Controllers area	The **Controllers** area shows the list of installed Controllers that have communicated at least once with the Platform. The **Last seen** column shows the last time that the Platform made contact with the Controller.
Custom Controller credentials	If the default credentials are not valid or do not have sufficient privileges in a particular environment, the Controller deployed in that environment requires a different set of credentials. To do this, in the **Credentials for:** area, uncheck **Use default credentials** and key in a new set of credentials. These credentials will be used to scan the network, deploy agents and run GFI OneGuard services on machines managed by this Controller only. The account used must have administrative rights on managed machines and sufficient permissions to deploy software. When a Controller is deployed in a domain environment, the account must also have read access to Active Directory to enable enumeration of machines on the network.



Screenshot 64: Custom Controller settings

4. In the **Custom Controller settings** area, configure how the Platform and Controllers communicate:

Option	Description
Custom Controller settings	Enable this option if you do NOT want Platform-Controllers communications to use the default settings. By default, these communications are performed via HTTP on port 80 and do not require authentication. **IMPORTANT** If changing these settings to non-default, configure the Platform communications options within each Controller to match these settings as configured below. If these settings are not manually configured similarly between on both the Platform and each Controller, communications between them will fail. For more information, refer to Communication - Platform (page 95).
Protocol	If you have a valid certificate implemented on your web server, you can change your protocol to **HTTPS** to encrypt communications.
Port	Configure the port for Platform-Controllers communications. Ensure that this port is open on both the Platform server and each Controller.
Requires authentication	To require Controllers to authenticate with the Platform, select this option and key in a custom **Username** and **Password**. These credentials can be invented for this purpose and do not have to be configured in Active Directory or any other system. When this option is selected, the Platform expects Controllers to authenticate with it using these credentials. For more information, refer to Communication - Platform (page 95).

5. On completion, click **Save Settings** to save and apply changes.

4.1.4 Notification Settings

The notifications list is a list of users and email addresses that receive email notifications when key events occur.

To configure the list of users that receive email notifications when key events occur.:

1. Log in to the GFI OneGuard Platform and click **Settings**.

2. From the left pane choose **Notification Settings**.

3. In the User or User Group field, type the first few letters of the name of the user you want to add, to automatically retrieve the list of users that match this pattern. Select the required user and click the plus **+** button on the right to add the user.

> **NOTE**
> By default, the account used to login the Platform is already added to the notification list.

4. On completion, click **Save Settings** to save and apply changes.

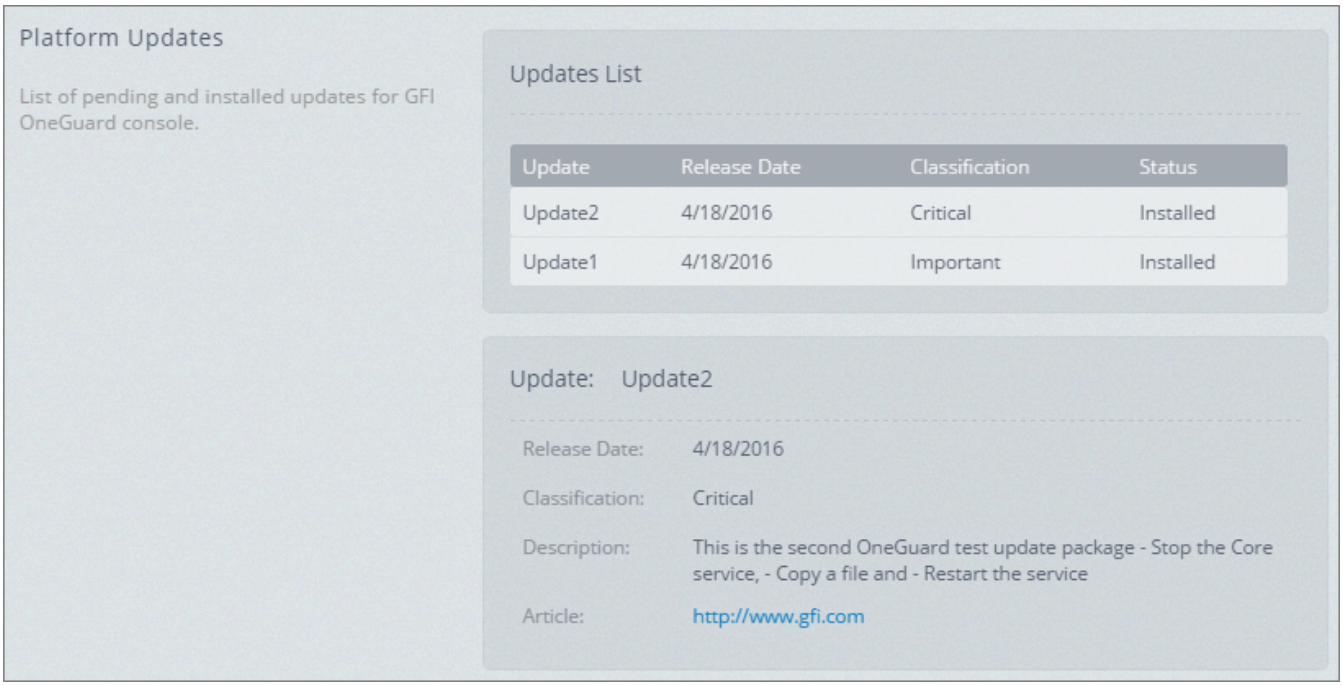
4.1.5 Platform updates

Monitor and configure how GFI OneGuard downloads and installs updates issued by GFI Software for the Platform.

To configure the Platform Updates:

1. Log in to the GFI OneGuard Platform and click **Settings**.

2. From the left pane choose **Platform updates**.



Screenshot 65: Platform updates settings - Updates list

3. Configure the following options:

Option	Description
Platform Updates	Displays a list of pending and installed updates for the Platform. Click on specific entries in the list to view additional information.
Auto updates	When this option is enabled, GFI OneGuard installs updates automatically. Specify a schedule for when to install updates. It is recommended to install updates at off-peak times. Select **Apply major platform updates immediately** to automatically install important updates as soon as these are available.
Notifications	Enable this option to receive email notifications when updates are available or installed. Select: » **New updates are available** - send email notifications whenever GFI OneGuard finds new updates. » **Platform update was successfully installed** - send email notifications whenever updates are successfully installed. Note that GFI OneGuard always sends a notification when an update fails to install. » **Administrators who have access** - if enabled, email notifications related to updates are sent to users who have access to the Platform settings (Configure Settings permission in Roles & Permissions). These users must also be added to the Notification Settings list to receive this email. If this option is disabled, you can manually enter a list of email addresses that will receive these notifications.

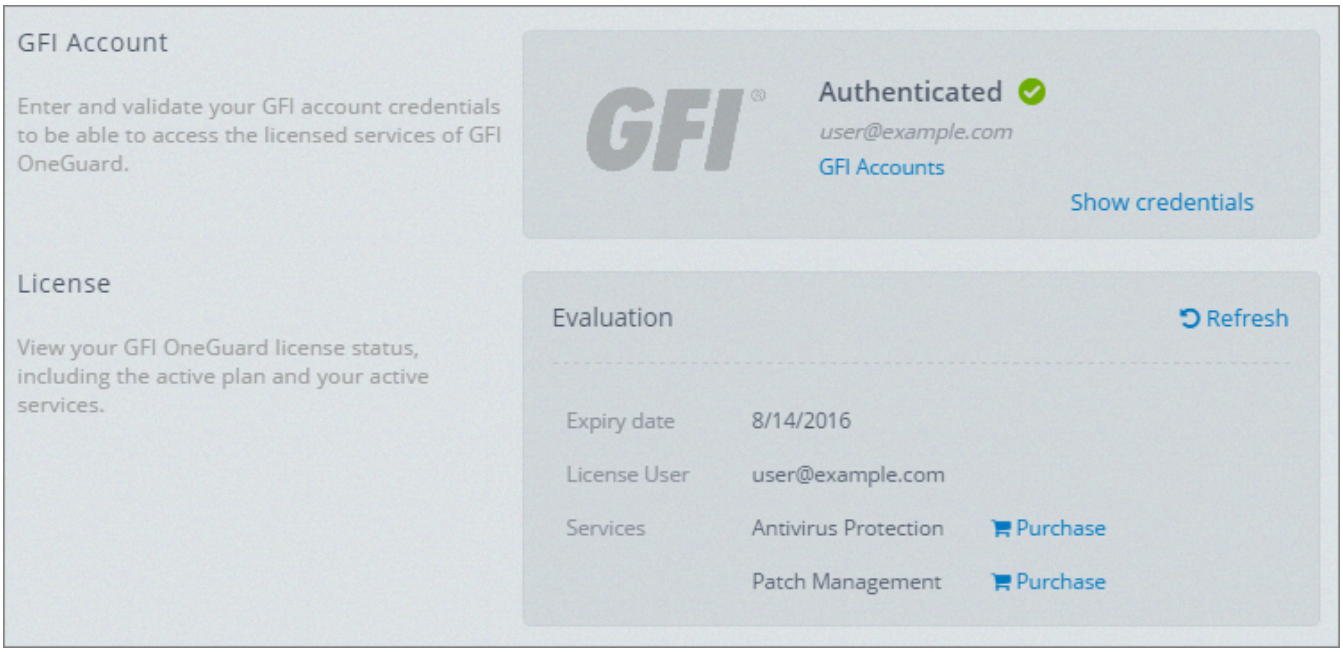
4. On completion, click **Save Settings** to save and apply changes.

4.1.6 Licensing

To review and configure information related to your GFI OneGuard license.

1. Log in to the GFI OneGuard Platform and click **Settings**.

2. From the left pane choose **Licensing**.



Screenshot 66: Licensing page during evaluation

3. Configure the following options:

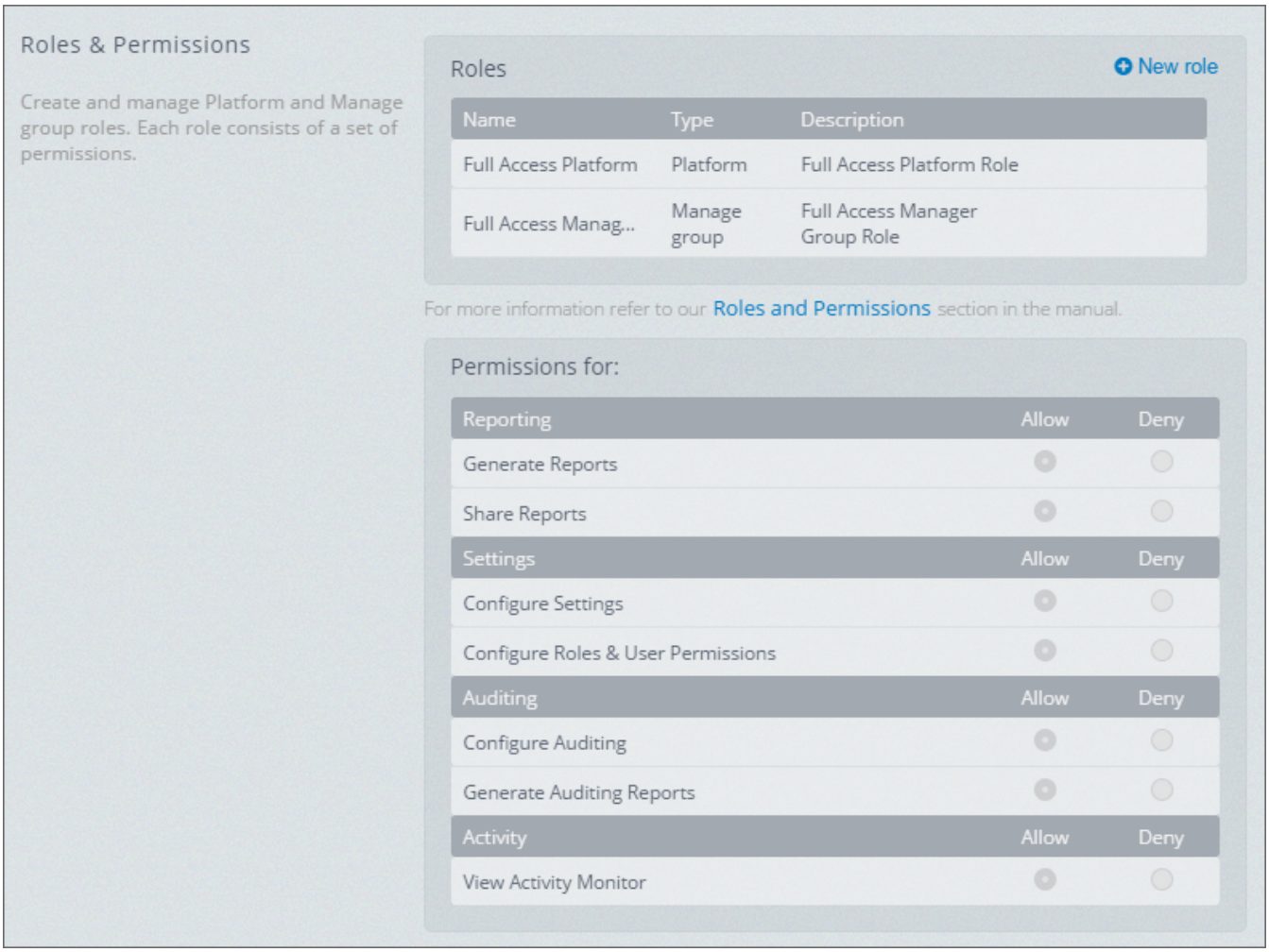
Options	Description
GFI Account	Review and edit your GFI account credentials to be able to access the licensed services of GFI OneGuard. This area shows the status of your GFI Account's GFI OneGuard subscription. Click **Show credentials** to show your account credentials. To change the account credentials, key in your new details and click **Authenticate**. GFI OneGuard verifies your new credentials and retrieves your new licensing information.
License	View your license status, including the expiry date and your active services. Click **Refresh** to request GFI OneGuard to update the license information. You may also click **Buy more seats** to launch the GFI Accounts portal where you can purchase more seats.
Services	This area shows a detailed breakdown of seat usage per service. Toggle the **ON/OFF** switch to turn on or off a particular service. When a service is on, the **Protecting** field shows the number of seats used out of the maximum number allowed by your subscription. The **Active Groups** field shows device groups that have the service enabled. Click in a group tab to turn off the service for that group. You can also enable a service from this view by clicking **Enable Group** and choosing the group from the hierarchical structure. Note that this option only allows for enabling the service. For more features it is recommended to enable services from the **Manage** menu. For more information, refer to Group settings (page 21).

4. On completion, click **Save Settings** to save and apply changes.

4.1.7 Roles and Permissions

In GFI OneGuard, roles are made up of a set of pre-configured permissions. Active Directory users and groups can then be assigned a role, inheriting the role permissions when accessing GFI OneGuard.

To access and configure roles and permissions, login to GFI OneGuard and click (Settings). Click **Roles and Permissions** from the left pane.



Screenshot 67: Configuring Roles and Permissions

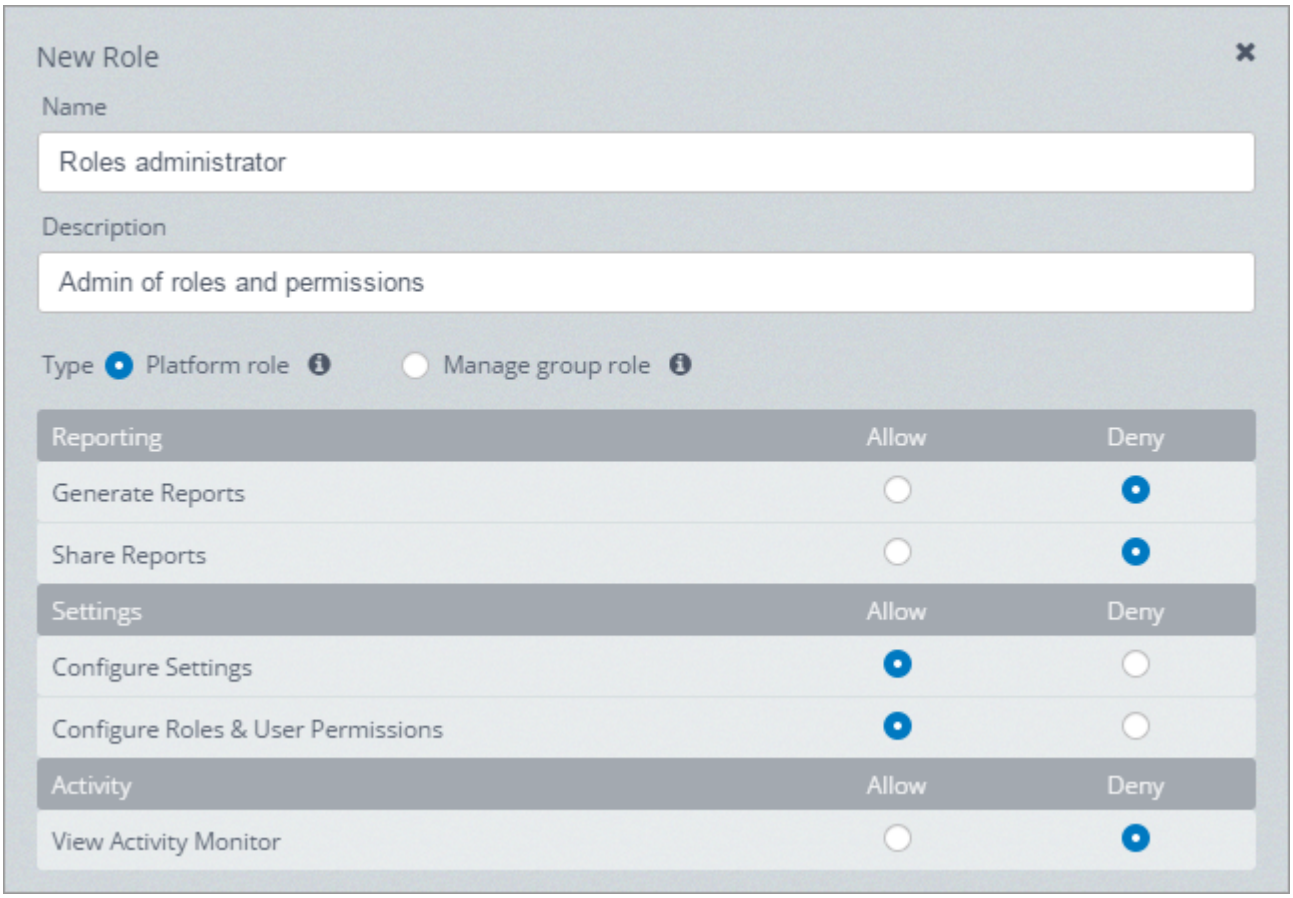
In the **Roles** area you can view existing roles or create new ones. There is no limit to the number of roles that can be created.

Click on a role to view its configured permissions.

4.1.8 Creating a new role

To create a new role:

1. Click **New role**.



Screenshot 68: Creating a new role

2. In the **Name** field, key in a friendly name for the new role.

3. In the **Description** field, type the description of the intended use of the new role.

4. Select the type of role from the following options:

Type	Description
Platform Role	A set of permissions that enable users to perform specific actions on the platform. This Platform role type can be configured to access and configure: Reporting, System settings and network Activity.
Manage group role	A role that allows users to access and configure groups, devices, policies, services and jobs.

5. Select the permissions to allow or deny according to the scope of the role being configured. Note that roles cannot be created with all permissions denied.

6. Click **Save Settings**.

After creating the role, you may now start adding users or groups to the role. For more information, refer to Role assignment (page 91).

4.1.9 Editing an existing role

To edit an existing role:

1. Click next to the role to modify.
2. In the **Name** field, change the role name as required.
3. In the **Description** field, change the role description as required.
4. Select the permissions to allow or deny according to the scope of the role being configured.
5. Click **Save Settings**.

4.1.10 Role assignment

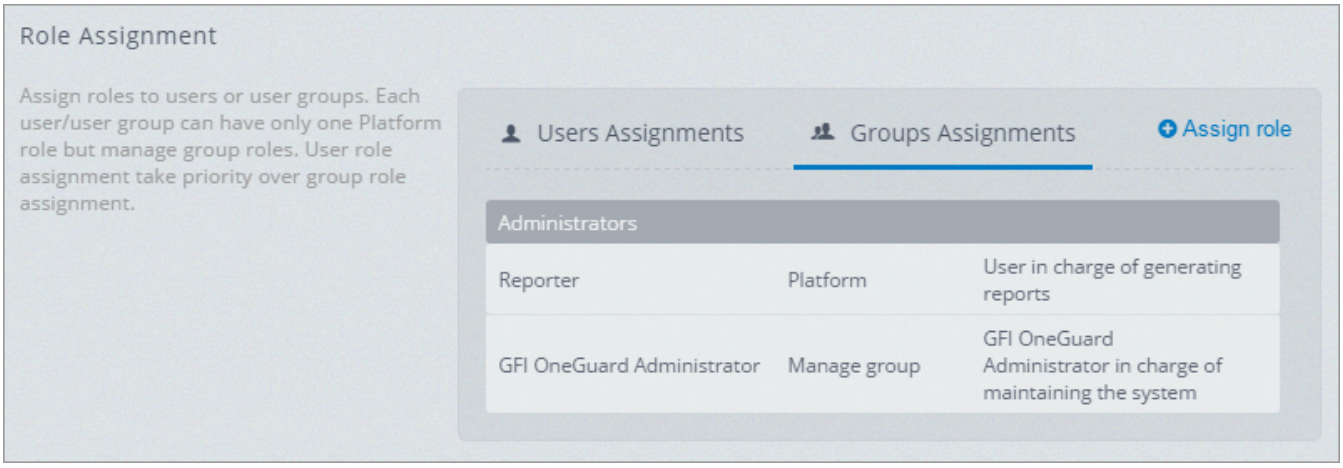
Active Directory users or groups can be assigned to roles . Users logging in to GFI OneGuard will be provided access to the features configured to their assigned role.

Each role assignment can have one Platform role but multiple Manage group roles.

Roles can be assigned to Active Directory Groups and Users on the local domain where GFI OneGuard is installed.

Note that roles assigned to individual users have higher priority than group assignments. The order of priority of group assignments is configurable, and users that are part of multiple groups inherit the role assigned to the higher priority group.

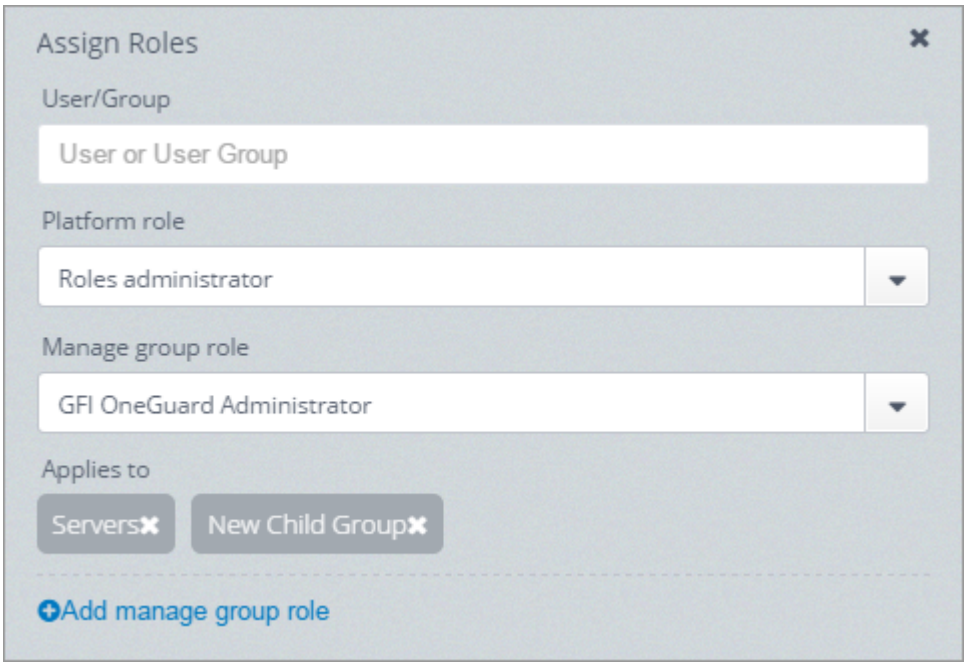
By default, the administrative group configured during the post-installation wizard (when GFI OneGuard is loaded the first time) are granted full permissions.



Screenshot 69: Assigning a role in GFI OneGuard

To assign a role to a user or group:

1. Click **Assign role**.



Screenshot 70: Configuring role assignments

2. In the **User/Group** field, start typing the name of an Active Directory user or group to assign. Names or groups that are not available in Active Directory are not recognized.

3. From the **Platform role** drop down list, select a platform role. Each user or group can only have one platform role.

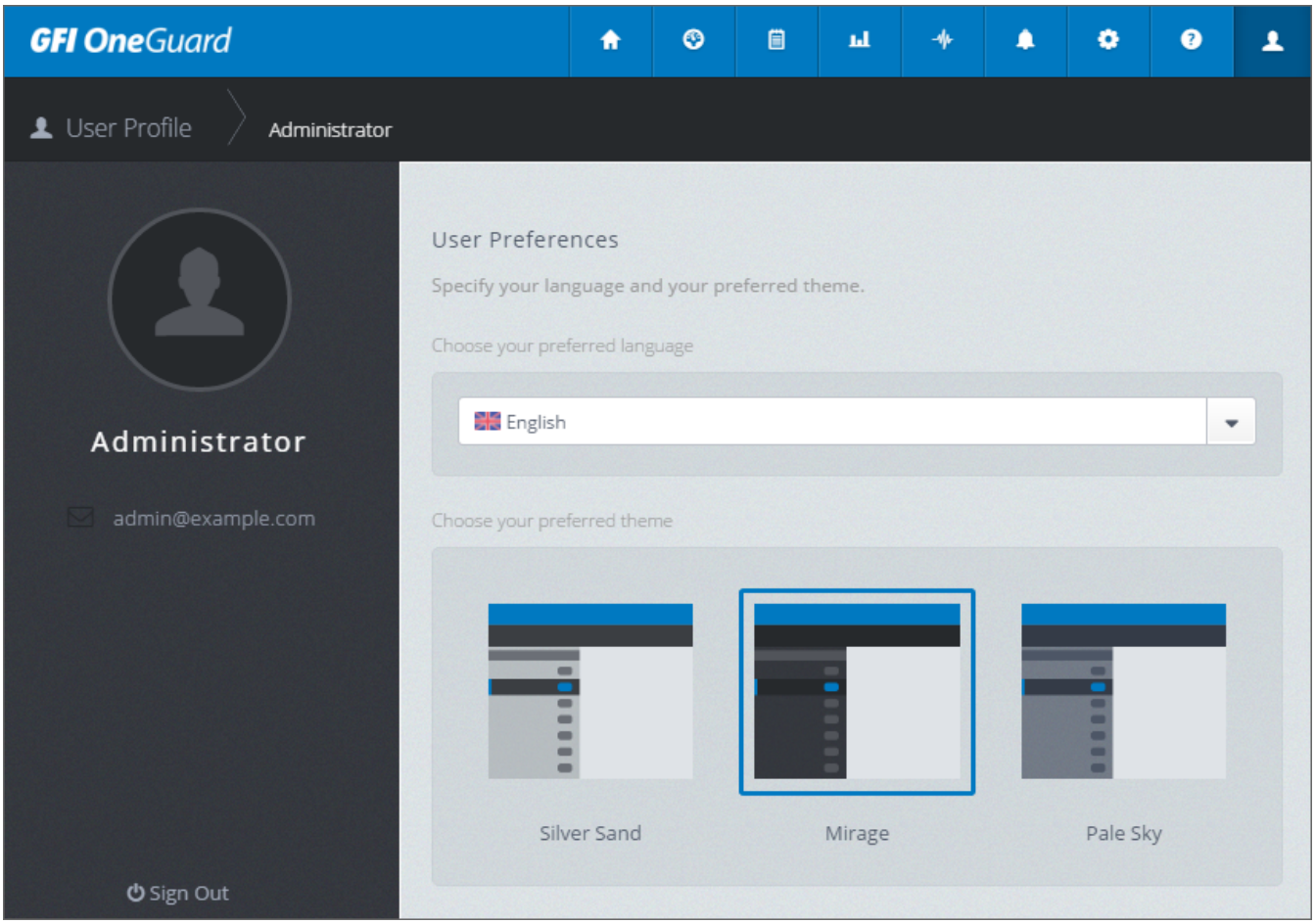
4. From the **Manage group role** drop down list, select a role, then select GFI OneGuard groups from the popup window. A user/group can be assigned multiple Manage group roles. Click **Add manage group role** to add another manage group role for the user/group being configured.

5. Click **Save Settings**.

4.2 User profile settings

The user profile area lets users customize the profile used to log in GFI OneGuard as well as the appearance of the user interface.

To view the profile of the currently logged on user, click  from the top navigation and select **Profile**.



Screenshot 71: User profile settings

Configure the following options:

Option	Description
Login Credentials	Click **Change password** to change the password of the currently logged in user.
User Preferences	Select UI language (currently only English is supported) and a preferred theme.
Sign Out	Click to sign out of GFI OneGuard.

4.3 Controller configuration

The GFI OneGuard Controller is responsible for searching the network for devices. It also installs Agents on managed devices and relays information between the Platform and the Agents.

A GFI OneGuard Controller installation consists of a background service and a system tray agent. The system tray agent is used for monitoring and configuration purposes.

> **NOTE**
> Accessing the Controller is not usually required since all operations can be done directly from the Platform. Use the Controller for special customizations or for troubleshooting purposes. It is recommended that only individuals with advanced knowledge of the network infrastructure configure the Controller since a misconfiguration may stop communications between GFI OneGuard and devices.

To open the Controller, log in to the server where the Controller is installed, right-click the GFI OneGuard Controller icon in the system tray and click **Open**.

4.3.1 Monitoring the Controller's status

The main screen of the Controller lets you monitor the status of the Controller and the list of devices connected to it.

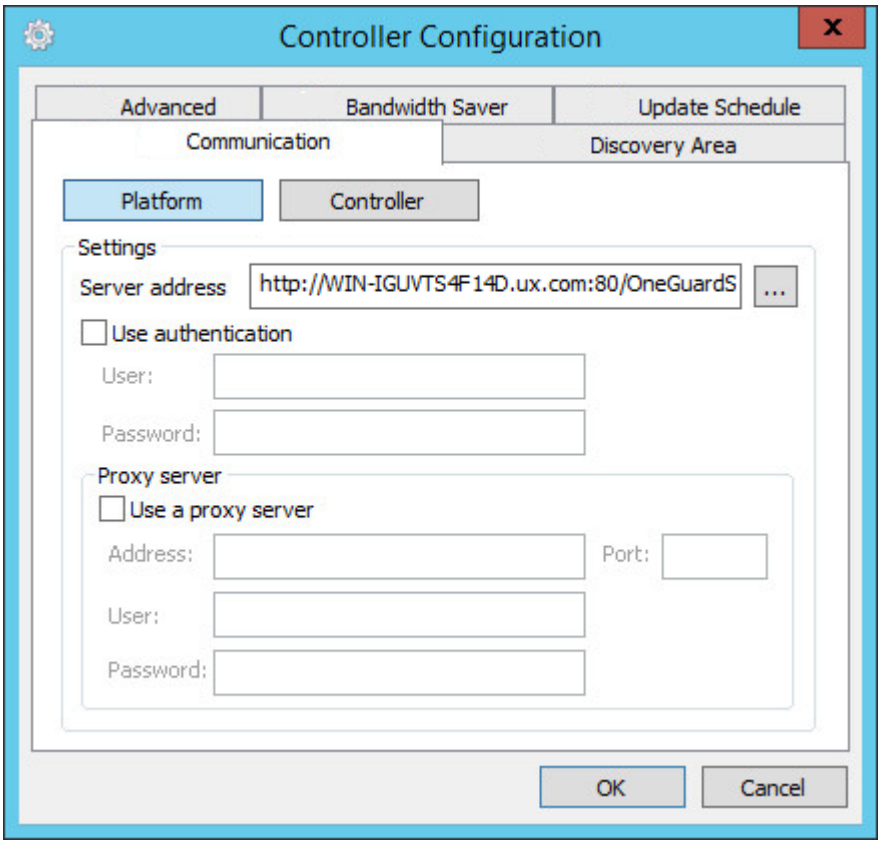
Screenshot 72: Monitoring the Controller status

The **Service Status** option shows the status of the Controller background service. If this service is not running, launch the Services applet (`services.msc`) and start **GFI OneGuard Controller Service**.

The **Agents** table shows the list of devices connected to this Controller instance and the agent version.

4.3.2 Controller settings

To configure the GFI OneGuard Controller, click **Configure...** in the Controller main window.



Screenshot 73: Controller settings

Use the different tabs to configure the following options:

Tab	Description
Communication - Platform	Configure how the Controller communicates with the GFI OneGuard Platform. 1. Go to the **Communication** tab and select **Platform**. 2. In **Server address**, specify the location of the Platform and the connection details. Click **...** and key in the following details: • **Server**: Key in the Platform server name or IP address. • **Port number**: Key in the Platform listening port. This must match the port configured in the GFI OneGuard Platform under **System Settings > Network Control**. For more information, refer to Network Control (page 84). • **Protocol**: Select the protocol accepted by the Platform. This must match the protocol configured in the GFI OneGuard Platform System Settings, under **Network Control**. For more information, refer to Network Control (page 84). 3. Click **OK**. 4. If the Platform is configured to require authentication by the Controllers, check **Use authentication** and key in the credentials as configured in the **Network Control** settings in the Platform. For more information, refer to Network Control (page 84). 5. If the communication with Platform must pass through an HTTP/HTTPS proxy, check **Use a proxy server** and key in the proxy server details. 6. Click **OK**.

Tab	Description
Communication - Agents	**IMPORTANT** Customize these settings with caution. These are meant to be configured only when installing the Controller the first time, before deploying Agents. Customizing these settings after Agents have been deployed may impact the existing connection with the deployed agents and require their re-installation. Configure how the Controller communicates with the Agents: 1. Go to the **Communication** tab and select **Controller**. 2. In **Server address**, specify the connection details. Click **...** and key in the following details: • **Port number**: Key in the listening port of the Controller. • **Protocol**: Select the protocol that the Controller accepts. 3. Click **OK**. 4. For added security, you may set agents to authenticate with the Controller. Click **Use authentication** and key in a random username and password that agents will then use when communicating with Controller. 5. If the communication between Controller and agents must pass through an HTTP/HTTPS proxy, select **Use a proxy server** and key in the proxy server details. 6. Check **Create and bind self-signed certificate** to encrypt communication with agents using a certificate. 7. Click **OK**.
Discovery Area	Configure where the Controller looks for machines to be managed in GFI OneGuard. By default, the Controller looks for other machines in the current domain or workgroup. To discover more machines: 1. Go to the **Discovery Area** tab and click **Add**. 2. Select the type of area to add, for example, **IP Range** to discover machines within a range of IP addresses. 3. Key in the area details and click **OK**.
Advanced	Configure other Agent deployment settings: » **Timeout**: The value in seconds that the Controller waits when deploying agents. If the timeout value is exceeded, agent deployment cannot be executed. » **Thread Pool Size**: The number of threads that the controller uses to install agents. Click **OK**.
Bandwidth Saver	The Controller may be configured as a bandwidth saver so that downloadable files (such as system patches) are temporarily stored on the Controller. Agents download files through the Controller rather than directly from the internet. The Controller stores a copy of files on disk for future use by other devices, reducing bandwidth use. To configure the Bandwidth Saver: 1. In the Bandwidth Saver tab, check **Enable Bandwidth Saver** to switch on the feature. 2. Key in the following: • **Address**: Key in the IP or FQDN address of the Bandwidth Saver machine. • **Port**: The port used by the proxy. Ensure that this port is open for both the Agents and the Controller. The default port is 8123. • **Name** and **Password**: Define custom credentials to be used for authentication. Deployed GFI OneGuard Agents automatically use these credentials. • **Cache Path**: The location where the Bandwidth Saver stores files for download by the agents. Ensure that there is enough disk space on this folder's drive since the cache may become quite large. 3. If the Controller connects to the internet via another proxy, fill in the **Cascading proxy** details with the details of the proxy server. 4. Click **OK**.

Tab	Description
Update schedule	Configure the frequency of GFI OneGuard Controller and Agent automatic updates. 1. Go to the **Update Schedule** tab. 2. Ensure that **Enable automatic update** is checked and configure a schedule. Select the frequency of the updates and specify that exact day and time for the update to occur. 3. Click **OK**.
Controller Enrollment	Specify the connection information used by the Controller to connect to the GFI OneGuard Platform the first time. This is used when the Controller is not yet connected to any Platform instance. Configure the following options: 1. In **Server address**, specify the connection details. Click **...** and key in the following details: • **Controller**: Key in the Platform server name or IP address. • **Port number**: Key in the listening port of the Controller. • **Protocol**: Select the protocol that the Controller accepts. 2. Click **OK**. 3. Key in connection credentials and click **Connect** 4. Click **OK**. When a connection is established, configure Platform communication options from the Communication tab.

4.4 How to backup GFI OneGuard configuration

It is always recommended to keep a backup of product configuration data, so it can be used in case of data loss. This topic describes how to backup your GFI OneGuard configuration.

These instructions apply to the latest version of GFI OneGuard only.

4.4.1 Step 1: Stop GFI OneGuard services

GFI OneGuard services must be stopped when backing up the configuration. If services are open or running, the backup may be unusable.

To stop services, use either the Services applet or create a batch file using the `net stop` command.

GFI OneGuard services to stop:

» `GFI OneGuard SEP Core`

» `GFI OneGuard SEP Store`

4.4.2 Step 2: Backup folders

While copying take note of the folders' path as they are to be placed at the same path (either on the same or on a different server) when restoring configuration.

Backup GFI OneGuard Platform configuration

To backup the GFI OneGuard Platform settings, databases and reports, copy the following folders that reside in the GFI OneGuard Platform installation directory and store them at a secure location.

Folders' Name	Path
Data, **Databases** and **Reports**	`< GFI OneGuard Platform installation directory>\Core`
Data and **Databases**	`< GFI OneGuard Platform installation directory>\Store`

Unless modified manually during installation, by default the GFI OneGuard Platform is installed at the following location: **C:\Program Files\GFI\OneGuard\Platform**

Backup GFI OneGuard Controller settings

To backup the GFI OneGuard Controller's configuration, copy the following folder that resides in the GFI OneGuard Controller installation directory and store it at a secure location.

Folder Name	Path
Data	`< GFI OneGuard Controller installation directory>`

Unless modified manually during installation, by default the GFI OneGuard Controller is installed at the following location: **C:\Program Files (x86)\GFI\OneGuard\Controller** (or at **C:\Program Files\GFI\OneGuard\Controller** on 32-bit systems)

4.4.3 Step 3: Start the GFI OneGuard services

Start the services that were stopped in Step 1.

When starting services manually, use either the Services applet or create a batch file using the `net start` command.

4.5 Securing Platform communications

You can use HTTPS certificates to secure all network communications performed by the GFI OneGuard Platform. Configure IIS to use HTTPS to provide:

- a secure connection when network users access the GFI OneGuard web interface.
- secure the communications between the Platform and Controllers.

This feature is especially recommended when the GFI OneGuard Platform is accessed from external networks, so that all communications are encrypted.

To enable HTTPS for the GFI OneGuard Platform:

Step 1: Configure an HTTPS certificate

Configure your IIS web server to use a certificate .

To create or import a certificate:

1. Open **Internet Information Services (IIS) Manager**.
2. Choose **Server**.
3. In the left pane, under **IIS** click **Server Certificates**.
4. Under **Action**, you can import an existing certificate or create a self-signed certificate.

> **NOTE**
> If a new certificate is created in IIS, the certificate needs to be distributed to the machines from where the GFI OneGuard web interface needs to be accessed.

Step 2: Configure HTTPS bindings

Ensure that HTTPS binding is enable for the web server hosting the GFI OneGuard site:

1. Open **Internet Information Services (IIS) Manager**.
2. Expand **Server > Sites**.

3. Right-click on **Default Web Site** and select **Edit Bindings**.

4. Click **Add...** and select **HTTPS**.

5. The default port is set to `443`. If another port needs to be used it can be changed here.

6. Under **SSL certificate**, select the certificate imported or created previously.

7. Click **OK** twice.

8. Click **Close** to complete the process.

Step 3: Enforce the use of SSL

Enforce the use of SSL to ensure that GFI OneGuard uses HTTPS to access the web interface:

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

2. Browse to **Server > Sites > Default Web Site**.

3. Choose the GFI OneGuard virtual directory. (default is **OneGuard**)

4. In the left pane, under **IIS** click **SSL Settings**.

5. Select **Require SSL**

6. In the **Client Certificates** options, select **Require**.

7. Click **Apply**.

Step 4: Configure the Platform

Update communication settings from the **Platform** to use HTTPS:

1. Verify that you have access to the GFI OneGuard web interfaces using the revized connection settings. Depending on the settings applied in the previous steps, the GFI OneGuard URL probably changes in the following structure:
`https://<servername/IP>:<new port>/<GFI OneGuard virtual directory>`
for example:
`https://myserver.example.com:443/OneGuard`

2. When the new URL is confirmed and the login screen is shown, log into the GFI OneGuard Platform and click **Settings**  .

3. From the left pane choose **Network Control**.

4. Turn on **Custom Controller Settings**.

5. Select **HTTPS**.

6. Key in a port number, for example, `443`. Use the same port selected inr the HTTPS binding of the IIS configuration, and make sure the port is open on the firewall.

7. To add a further layer of security, you can enforce the use of authentication by selecting **Requires authentication**. Enter a custom set of credentials in the **Username** and **Password** fields. These do not have to be a domain or system credentials, but a custom set which would also be configured in the Controller as an added measure of authentication. Take note of these credentials as they need to be specified in the next step.

8. Click **Save Settings**.

Step 5: Configure the controller communication protocol

All Controller instances need to be updated to communicate with the Platform using HTTPS:

1. Log in to the server where the Controller is installed.

2. Right-click the GFI OneGuard Controller icon in the system tray and click **Open**.

3. Click **Configure...** in the Controller main window.

4. Go to the **Communication** tab and select **Platform**.

5. Click  in the **Server address** field.

6. Type the new port number as configured in IIS (default port for HTTPS is `443`) and select **HTTPS**.

7. Click **OK**.

8. Update the other settings in the **Communication** tab as required. For more information, refer to Communication - Platform (page 95)..

Repeat this step for all Controller instances deployed in your environment.

4.6 Managing multiple domains

GFI OneGuard works with various network setups including multiple domains controlled from a single Platform.

GFI OneGuard Platform needs to communicate with the GFI OneGuard Controller instance deployed in other domains to install and manage agents on the client machines.

Follow the steps below to prepare the environment and to configure GFI OneGuard.

Step 1: Configure firewalls

Ensure that the Platform, the machine where the Controller is installed and the machines on the other domains can communicate through the following ports:

TCP Ports	Description
80	Listening port on GFI OneGuard Platform server, handling all Platform-Controller-Agents communications. This port can be customized from the Controller settings.
135	Remote WMI - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.
139	Remote Registry - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.
443	Listening Port on GFI OneGuard Platform server, accepting transfer of data from the Controller to the Platform.
445	Remote Registry - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.

Step 2: Install a GFI OneGuard Controller per domain

Install a GFI OneGuard Controller in each domain to be monitored by GFI OneGuard. For more information, refer to Installing the GFI OneGuard Controller (page 12).

After the installation ensure that the new Controller can communicate with the Platform:

1. Login to the GFI OneGuard Platform using an administrative account.

2. Go to **Settings > Network Control**.

3. Ensure that the new Controller is listed under **Controllers**. In case the Controller is not listed, check the status and configuration of the Controller. For more information, refer to Controller configuration (page 93).

Step 3: Configure discovery account

Configure the Controller to use an account with full permissions on the remote machines withing the domain to manage:

1. Login to the GFI OneGuard Platform using an administrative account.

2. Go to **Settings > Network Control**.

3. Click the  icon next to the Controller installed on the domain that you want to manage.

4. Enter the username and password of an account with administrative privilege on the domain. This account is used to install the agent and execute remote actions like scanning for missing patches, installing patches and updating anti-virus definitions.

5. Click **Save Settings**.

Next steps

After completing the steps above, wait until the Controller discovers the new machines and for it to populate them in the **Discovered Devices** node. When the devices are discovered, they are ready to be remotely managed by GFI OneGuard Platform. For more information, refer to Groups and Devices (page 18).

Ensure that the client machines meet the system requirements for the GFI OneGuard agent to be installed. For more information, refer to GFI OneGuard Agents (page 13).

4.7 Controlling workgroups

GFI OneGuard works with various network setups including workgroups controlled from the main Platform instance.

GFI OneGuard Platform needs to communicate with the GFI OneGuard Controller instance deployed in the workgroup to install and manage agents on the client machines.

> **NOTE**
> The GFI OneGuard Platform needs to be installed in a domain environment. From the GFI OneGuard Platform administrators can manage client machines in a workgroup.

Follow the steps below to prepare the environment and configure GFI OneGuard:

Step 1: Configure firewalls

Ensure that the Platform, the machine where the Controller is installed and the machines on the workgroup can communicate through the following ports:

TCP Ports	Description
80	Listening port on GFI OneGuard Platform server, handling all Platform-Controller-Agents communications. This port can be customized from the Controller settings.
135	Remote WMI - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.
139	Remote Registry - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.

TCP Ports	Description
443	Listening Port on GFI OneGuard Platform server, accepting transfer of data from the Controller to the Platform.
445	Remote Registry - Port used for Agent deployment on both server and client machines managed by GFI OneGuard.

Step 2: (Optional) Create a common administrative account

GFI OneGuard needs an account to connect to the machines on the workgroup. To facilitate the administration of multiple machines in the workgroup, it is recommended to create an administrative account with the same username and password in all machines.

If the administrator chooses to skip this step, once the device has been discovered by GFI OneGuard Platform, the administrator can enter an account in the properties of each new device discovered:

1. Go to **Manage > Devices > Managed Groups**.
2. Expand the group where the devices belong.
3. On the device click **Manage**.
4. Click **Set Credentials**.
5. Key in the username and password of an administrative account on the machine and click **Save**.
6. Repeat steps 3 to 5 for every machine.

Step 3: Install Controller in the workgroup

Install GFI OneGuard Controller on a machine within the workgroup. For more information, refer to Installing the GFI OneGuard Controller (page 12).

After the installation ensure that the new Controller can communicate with the Platform:

1. Login to the GFI OneGuard Platform using an administrative account.
2. Go to **Settings > Network Control**.
3. Ensure that the new Controller is listed under **Controllers**. In case the Controller is not listed, check the status and configuration of the Controller. For more information, refer to Controller configuration (page 93).

Step 4: (Optional) Configure discovery account

If a common administrative account is being used to manage the workgroup clients as described in step 2 above, configure GFI OneGuard to use this account:

1. Login to the GFI OneGuard Platform using an administrative account.
2. Go to **Settings > Network Control**.
3. Click the  icon next to the Controller where you already set the discovery area.
4. Enter the username and password of the account created in step 2 above.
5. Click **Save Settings**.

Next steps

After completing the steps above, wait until the Controller discovers the new machines and for it to populate them in the **Discovered Devices** node. When the devices are discovered, they are ready to be remotely managed by GFI OneGuard Platform. For more information, refer to Groups and Devices (page 18).

Ensure that the client machines meet the system requirements for the GFI OneGuard agent to be installed. For more information, refer to GFI OneGuard Agents (page 13).

5 Troubleshooting and support

For a list of common issues encountered when using GFI OneGuard, go to http://go.gfi.com/?pageid=OneGuardHelp#cshid=troubleshoot

Most issues can be solved through the information in this help system. If you cannot find a solution to your problem or if you think that our content can be improved in any way, let us know by sending an email to documentation@gfi.com

Other sources of information available to solve issues with our software are:

- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

GFI Knowledge base

GFI maintains a comprehensive repository of answers to the most common problems. GFI knowledge base always has the most up-to-date listing of technical support questions and patches. If the information in this guide does not solve your problems, refer to knowledge base.

Web Forum

User to user technical support is available via the GFI Web Forum.

Request Technical Support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: https://www.gfi.com/support/technical-support-form
- **Phone**: To obtain the correct technical support phone number for your region visit: https://www.g-fi.com/contact-us

> **NOTE**
> Before contacting Technical Support by telephone, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com

6 Glossary

A

Active Directory
A technology that provides a variety of network services, including LDAP-like directory services.

Agent
A GFI OneGuard component that runs as a background service on target devices and handles the deployment of patches, service packs and software updates.

agents
A GFI OneGuard component that runs as a background service on target devices and handles the deployment of patches, service packs and software updates.

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.

Asset Tracking
An inventory of the software and hardware installed in the network.

Auto-download
A GFI OneGuard technology that automatically downloads missing patches and service packs on connected devices.

Auto-patch management
A GFI OneGuard technology that automatically downloads missing Microsoft updates and deploys them over the network.

Auto-remediation
A GFI OneGuard technology that automatically downloads and deploy missing patches. If an application is blacklisted in GFI OneGuard, auto-remediation will uninstall the application from the target computer during scheduled operations.

Azure
Microsoft cloud provider. It allows users to host operating systems, databases and devices in the cloud.

B

Bandwidth saver
A feature available on the Controller which stores locally downloadable files such as system patches. It downloads and store the patches to be used by all the computer using the same controller.

BitLocker

An encryption feature that can be enabled on machines that are using an Windows Operating System.

C

Cache

A temporary storage of files for quick access when required.

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.

Controller

A GFI OneGuard component automatically discovers devices connected to the network, acting as a relay that channels communications between Agents and Platform.

CPU

Central Processing Unit. It handles all instructions it receives from hardware and software running on the computer.

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.

Devices

Machines connected to a network that have been discovered by GFI OneGuard.

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 Controller

A server that responds to security authentication requests within a domain, such as when logging in and checking permissions.

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

Encryption

Encryption is the conversion of standard data into ciphertext with the aim to protect the confidentiality of data stored making it unreadable to third-parties, but available for those authorized to decode it with the correct key.

EndPoint Control

Service used by GFI OneGuard to control access to devices.

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.

Exclusions

A list of files or folders excluded from antivirus scans.

F

File Transfer Protocol

A protocol used to transfer files between network computers.

FTP

A protocol used to transfer files between network computers.

Full Scan

A Full Antivirus Scan performs a check of the whole system, scanning the system memory; programs loaded at startup; system backup; email databases; hard drives, removable storage media and network drives.

G

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.

H

Hardware ID

Code created by the Operating System to identify attached devices.

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.

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.

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 Azure SQL

Microsoft AzureSQL is a cloud database service offered by Microsoft.

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.

O

OLE

Object Linking and Embedding is a Microsoft owned technology that allows embedding and linking to documents and other objects.

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.

P

Platform

The main component of GFI OneGuard that connects all the services offered by the product and the database that stores all collected information.

Proxy

A server or software application used to control and filter Internet access. The correct proxy settings need to be set in GFI OneGuard to allow Internet access when a proxy is used.

Q

Quick Scan

A Quick Antivirus Scan checks the objects loaded at the operating system startup, the system memory and boot sectors.

R

RAM

Random Access Memory. A hardware device that allows information to be stored and retrieved on a computer

Remote Desktop Protocol

A protocol developed by Microsoft® to enable clients to connect with the user interface of a remote computer.

S

Scan profiles

A collection of vulnerability checks that determine what vulnerabilities are identified and which information will be retrieved from scanned targets.

Self-signed certificate

A certificate that is signed by the person or application creating it rather than a trusted certificate authority. A certificate is used to encrypt the data during transmission.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is a technology used to monitor network devices such as, routers, hubs and switches.

SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard used by GFI OneGuard for electronic mail (email) transmission. SMTP by default uses TCP port 25.

SNMP

Acronym for Simple Network Management Protocol, a technology used to monitor network devices such as, routers, hubs and switches.

Spyware

A form of malware intended to collect information from a computer without notifying the user.

SQL Server

A Microsoft relational database management system. A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated

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.

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.

Temporary Access

Feature that allows temporary access to devices blocked by an EndPoint Control policy.

Terminal Services

A service that allows connecting to a target computer and managing its installed applications and stored data.

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

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.

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.

7 Index

A

Agents 5, 11, 13, 19, 24, 26, 82, 84, 93, 100-101

Antivirus 1-2, 5, 12, 16, 18, 22, 36-37, 39, 46-47

asset tracking 22

B

backup software 5, 12

C

Configuration 50

Controller 3-4, 6-7, 11, 13, 81, 93, 98, 100-101

D

Deleting reports 77

Deployment 6

Devices 2-3, 16, 18, 20-24, 26-29, 32, 35, 39, 46, 50, 53, 57, 59, 62, 101-102

Discovered Devices 3, 22, 24-25, 101-102

Download 7, 11, 51, 70, 74

Downloading 6

E

exclusion list 44, 46-47

F

Firewall Ports 5

G

Global exclusion 47

Group settings 21

H

hardware requirements 5, 10

home page 10, 16-17, 34

I

Installation 14, 33, 41

L

Licensing 82, 87

logging in 11, 15, 91

M

Monitoring 31, 37, 49, 94

N

network control 27

Notifications 17-18, 21, 28, 35, 45, 79, 82, 87

P

Patch Management 1-2, 16, 18, 31-32, 35-36

permissions 10, 15, 21, 53, 62, 67, 82, 85, 88, 101

Platform 3-4, 6-7, 10-11, 13-14, 16, 52, 58, 61-62, 68, 81-84, 86-87, 90, 93, 97-98, 100-101

post installation 9

protection 2, 18-19, 22, 37, 39, 46-48, 50, 55, 67

proxy 12, 81, 83, 95

R

reports 1, 16, 18, 32, 38, 49, 70-71, 73-75, 77, 97

restart 29, 34

roles 11, 82, 88

S

scheduled reports 71, 75

settings 3, 5, 9-10, 17, 19, 21-23, 26, 30, 32, 36, 39, 46, 48, 50, 62, 67, 71-72, 74, 76, 81-84, 87, 90, 92, 94, 97, 99-101

shutdown 13, 29

SMTP information 82

T

troubleshoot 17, 104

troubleshooting 93

U

upgrade 10

upgrading 10

user profile 92