Panda Endpoint Protection

Administration guide

Version: 9.00.00-00

Author: Panda Security

Date: 07/12/2021

pandasecurity.com

Legal notice.

Registered trademarks.

Contact information.

Corporate Headquarters:
Panda Security
Santiago de Compostela 12
48003 Bilbao (Bizkaia) SPAIN.
https://www.pandasecurity.com/uk/about/contact/

About the Panda Endpoint Protection Administration guide

- To get the latest version of the documentation in PDF format, go to:

http://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONoAP-guide-EN.pdf

- For more information about a specific topic, please refer to the product's online help, available at:

http://www.pandasecurity.com/enterprise/downloads/docs/product/help/endpointprotection/latest/en/index.htm

Release notes

To find out what's new in the latest version of Panda Endpoint Protection, go to the following URL:

http://info.pandasecurity.com/aether/?product=EP&lang=en

Technical Support

Panda Security provides global support services aimed at responding to specific questions regarding the operation of the company's products. The technical support team also generates documentation covering technical aspects of our products. This documentation is available in the eKnowledge Base portal.

- To access specific information about the product, please go to the following URL:

https://www.pandasecurity.com/uk/support/endpoint-protection-aether.htm

- The eKnowledge Base portal can be accessed from the following link

https://www.pandasecurity.com/en/support/#enterprise

Survey on the Administration guide

Rate this Administration guide and send us suggestions and requests for future versions of our documentation:

https://es.surveymonkey.com/r/feedbackEPGuideEN

Contents

Part 1: Panda Endpoint Protection overview

Part 2: The management console

Part 3: Deployment and getting started

Part 4: Managing devices

Part 5: Managing network security

Part 6: Viewing and managing threats

Part 7: Security incident remediation

Part 8: Additional information about Panda Endpoint Protection

Part 1

Panda Endpoint Protection overview

Chapter 1

Preface

This guide contains basic information and procedures for making the most out of Panda Endpoint Protection.

CHAPTER CONTENT

Audience

The primary audience for this guide is network administrators who are responsible for managing the security of their organization's computers, determining the extent of the security problems detected, and defining cyberthreat response and prevention plans.

What is Panda Endpoint Protection?

Panda Endpoint Protection is a managed service that delivers security without requiring active, constant intervention from the network administrator. Additionally, it provides highly detailed information about the security status of the IT network thanks to the new Aether Platform developed by Panda Security.

Panda Endpoint Protection is divided into two clearly defined functional areas:

- Panda Endpoint Protection
- Aether Platform

Panda Endpoint Protection

This is the product that implements the features aimed at ensuring the security of all workstations and servers in the organization, without the need for network administrators to intervene.

Aether Platform

Aether is the ecosystem where Panda Endpoint Protection is run. It is a scalable and efficient platform for the centralized management of Panda Security's solutions, addressing the needs of key accounts and MSPs. Aether delivers all the information generated by Panda Endpoint Protection about processes, the programs run by users and the devices installed in real time and in an organized and highly detailed manner.

Icons

The following icons are used in this Administration guide;

ⓘ Additional information, such as an alternative way of performing a certain task.

⚠ Suggestions and recommendations.

💡 Important advice regarding the use of features in Panda Endpoint Protection.

🔍 Additional information available in other section of the Administration guide.

Chapter 2

Panda Endpoint Protection overview

Panda Endpoint Protection is a comprehensive security solution for workstations and servers. Based on multiple technologies, it provides customers with a complete anti-malware security service without the need to install, manage or maintain new hardware resources in the organization's infrastructure.

CHAPTER CONTENT

Benefits of Panda Endpoint Protection

Panda Endpoint Protection is a security solution that leverages multiple protection technologies, allowing organizations to replace the on-premises or standalone antivirus solution installed on their network with a complete, cloud-based managed security service.

It combines an extremely lightweight security software installed on network computers with a single Web management console accessible at anytime, anywhere and from any device.

Panda Endpoint Protection enables administrators to manage security simply and centrally from a single Web console, without the need to install new infrastructure to control the service and thereby reducing the total cost of ownership (TCO).

It is a cloud-based, cross-platform service compatible with Windows, macOS, Linux and Android, as well as with persistent and non-persistent VDI environments. Therefore, it provides a single tool to respond to the security needs of all computers on the corporate network.

Panda Endpoint Protection features

Panda Endpoint Protection is a product that allows organizations to manage the security of all computers across the network, without negatively impacting device performance and at the lowest possible cost of ownership. It provides the following key benefits:

Lightweight product

All operations are performed in the cloud, with almost no impact on computer performance:

- **Low memory usage**: the size of the locally stored signature files has been reduced thanks to Panda Security's use of real-time queries to collective intelligence. This has allowed us to move the malware database from the user's computer to the cloud.
- **Low network usage**: the number of required downloads has been reduced to the minimum.
- **Ability to share signature files among endpoints**: signature files are downloaded once and shared across the network.
- **Low processor usage**: the detection intelligence has been moved to the cloud, thereby requiring fewer processor resources on users' computers.

Cross-platform security

Covers all infection vectors on Windows, Linux, macOS and Android devices.

- **Security for all infection vectors**: web browsing, email, file system and all external devices connected to the PC.
- **Security against unknown threats**: through heuristic technologies and contextual analysis.
- **Cross-platform security**: for Windows, Linux, macOS, Android and virtual engines (VMware, Virtual PC, MS Hyper-V, Citrix). It also transparently manages the licenses assigned to computers in

persistent and non-persistent VDI environments.

Easy to manage

Easy-to-manage solution which doesn't require maintenance or additional infrastructure on the customer's network.

- **Easy to maintain**: no specific infrastructure is required to host the solution, allowing the IT team to spend their time on more productive tasks.
- **Easy protection for remote users**: each computer with Panda Endpoint Protection installed communicates directly with the cloud; roaming users and remote offices are protected quickly and easily without specific installations or VPN configurations.
- **Easy to deploy**: provides multiple deployment methods and automatic uninstallers to remove competitor products and migrate easily from a third-party solution.
- **Soft learning curve**: simple and intuitive Web-based interface. Often-used options are one click away.

Aether Platform features

Aether is the new management, communication and data processing platform developed by Panda Security and designed to centralize the services common to all of the company's products.

Aether Platform manages communication with the agents deployed across the network. Plus, its management console presents the data gathered by Panda Endpoint Protection in the simplest and easiest to understand way for later analysis by the network administrator.

The solution's modular design eliminates the need for organizations to install new agents or products on customers' computers for any new module that is purchased. All Panda Security products that run on Aether Platform share the same agent on customers' endpoints as well as the same Web management console, facilitating product management and minimizing resource consumption.

Key benefits of Aether

The following are the main services that Aether provides for all compatible products:

Cloud management platform

Aether is a cloud-based platform with a series of significant benefits in terms of usage, functionality and accessibility.

- It does not require management servers to host the management console on the customer's premises: as it operates from the cloud, it can be accessed directly by all devices subscribed to the service, from anywhere and at any time, regardless of whether they are office-based or on-the-road.
- Network administrators can access the management console at any moment and from anywhere,

using any compatible Internet browser from a laptop, desktop or even mobile devices such as tablets or smartphones.

- It is a high-availability platform, operating 99.99% of the time. Network administrators don't need to design and deploy expensive systems with redundancy to host the management tools.

Real-time communication with the platform

The pushing out of settings and scheduled tasks to and from network devices is performed in real time, the moment that administrators apply the new settings to the selected devices. Administrators can adjust the security parameters almost immediately to resolve security breaches or to adapt the security service to the dynamic corporate IT infrastructure.

Multi-product and cross-platform

The integration of Panda Security products in a single platform offers administrators a series of benefits:

- **Minimizes the learning curve**: all products share the same platform, thereby reducing the time that administrators require to learn how to use the new tool, which in turn reduces the TCO.
- **Single deployment for multiple products**: only one software program is required on each device to deliver the functionality of all products compatible with Aether Platform. This minimizes the resource consumption on users' devices in comparison with separate products.
- **Greater synergy among products**: all products report through the same console: administrators have a single dashboard from which they can see all the generated data, reducing the time and effort invested in maintaining several independent information repositories and in consolidating the information received from different sources.
- **Compatible with multiple platforms**: it is no longer necessary to invest in a range of products to cover the whole spectrum of devices used by a company: Aether Platform supports Windows, Linux, macOS and Android, as well as persistent and non-persistent virtual and VDI environments.

Flexible, granular settings

The new configuration model speeds up the management of devices by reusing setting profiles, taking advantage of specific mechanisms such as inheritance and the assignment of settings to individual devices. Network administrators can assign more detailed and specific settings with less effort.

Complete, customized information

Aether Platform implements mechanisms that enable the configuration of the amount of data displayed across a wide range of reports, depending on the needs of the administrator or the end-user of the information.

This information is completed with data about the network devices and installed hardware and software, as well as a change log, which helps administrators to accurately determine the security status of the network.

Aether architecture

Aether architecture is designed to be scalable in order to offer a flexible and efficient service. Information is sent and received in real time to and from numerous sources and destinations simultaneously. These can be endpoints linked to the service, external consumers such as SIEM systems or mail servers, or Web instances for requests for configuration changes and the presentation of information to network administrators.

Moreover, Aether implements a backend and storage layer that implements a wide range of technologies that allow it to efficiently handle numerous types of data.

Figure 2.1 shows a high-level diagram of Aether Platform.

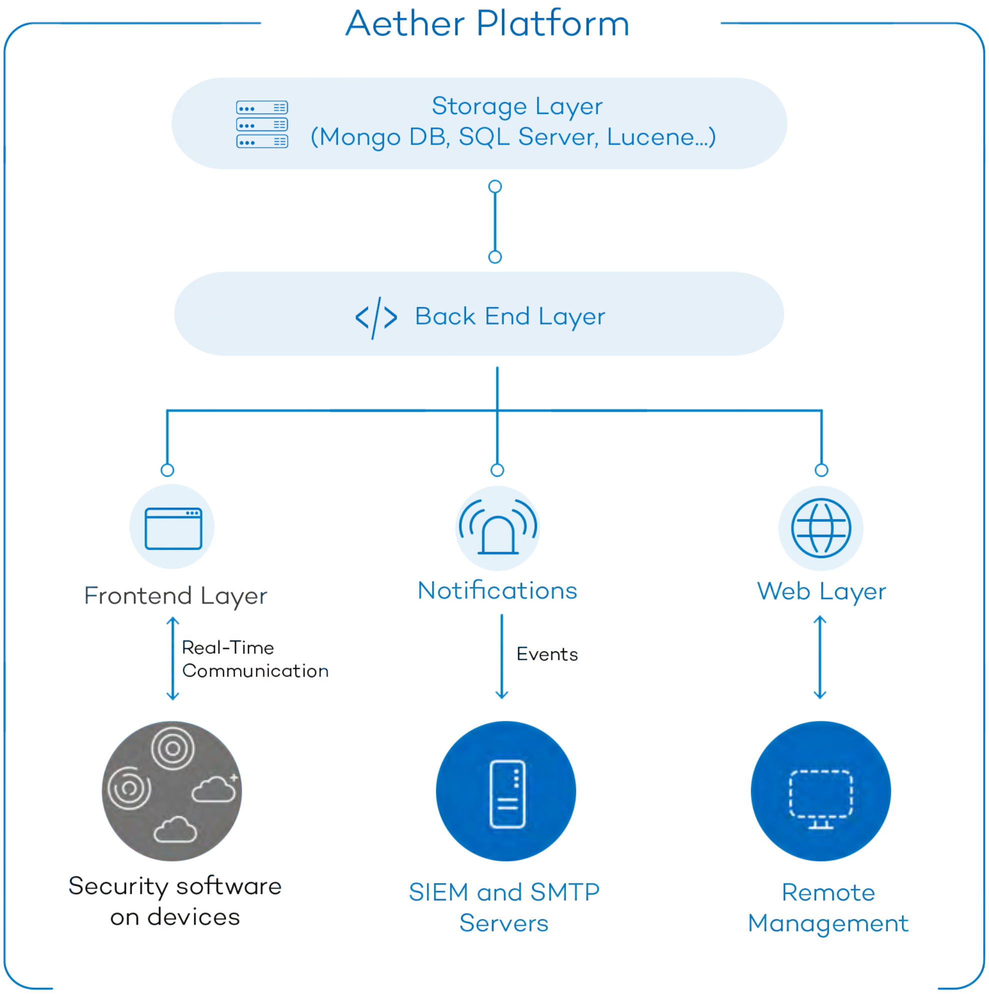


Figure 2.1: Logical structure of Aether Platform

Aether on users' computers

Network computers protected by Panda Endpoint Protection have a software program installed, made up of two independent yet related modules, which provide all the protection and management functionality.

- **Panda communications agent module (Panda agent)**: this acts as a bridge between the protection module and the cloud, managing communications, events and the security settings implemented by the administrator from the management console.
- **Panda Endpoint Protection protection module**: this is responsible for providing effective protection for the user's computer. To do this, it uses the communications agent to receive the settings profiles and send statistics and detection information and details of the items scanned.

Panda real-time communications agent

The Panda agent handles communication between managed computers and the Panda Endpoint Protection server. It also establishes a dialog among the computers that belong to the same network in the customer's infrastructure.

This module manages the security solution processes, and gathers the configuration changes made by the administrator through the Web console, applying them to the protection module.

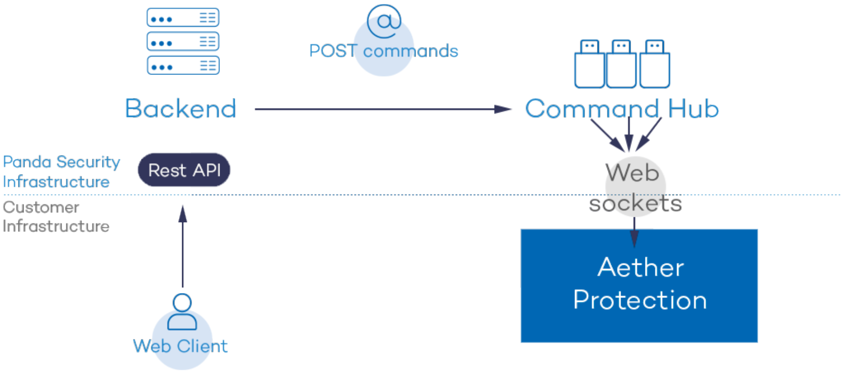


Figure 2.2: Flowchart of the commands entered via the management console

The communication between the devices and the Command Hub takes place through real-time persistent WebSocket connections. A connection is established for each computer for sending and receiving data. To prevent intermediate devices from closing the connections, a steady flow of keep-alive packets is generated.

The settings configured by the network administrator via the Panda Endpoint Protection management console are sent to the backend through a REST API. The backend in turn forwards them to the Command Hub, generating a POST command which pushes the information to all managed devices. This information is transmitted instantly provided the communication lines are not congested and every intermediate element is working properly

Panda Endpoint Protection key components

Panda Endpoint Protection is a cloud security service that moves security intelligence and most scanning tasks to the IT infrastructure deployed in Panda Security's Data Processing Centers. This results in an extremely lightweight security software with low resource usage and low requirements to run in organizations.

Figure 2.3 shows the general structure of Panda Endpoint Protection and its components:

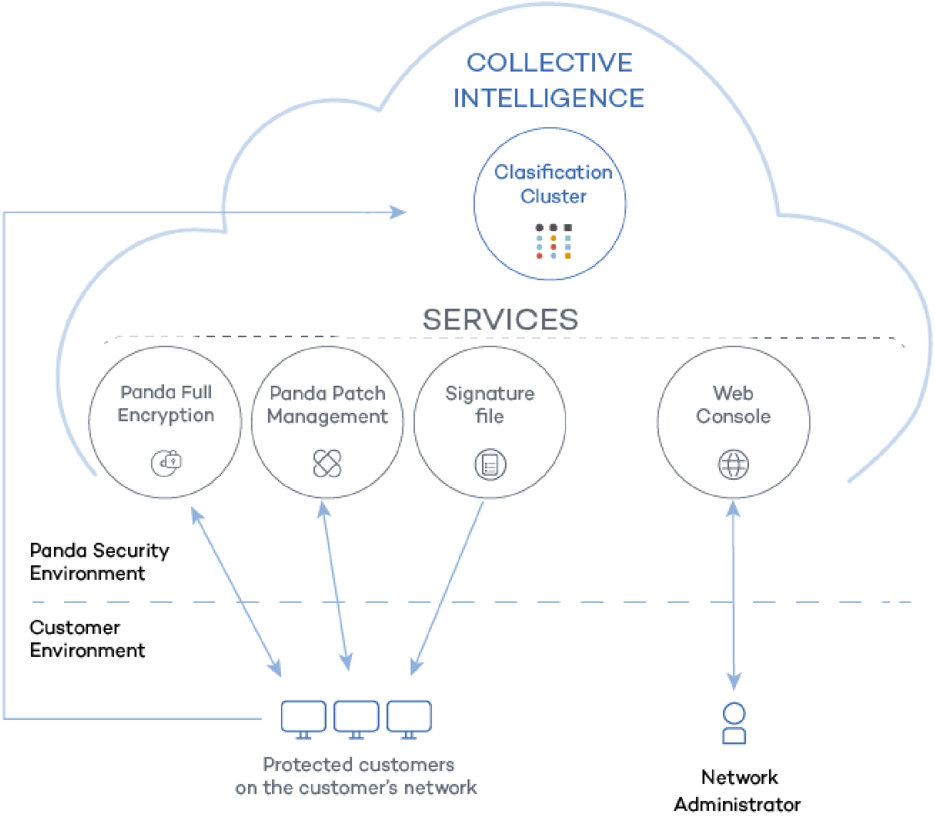


Figure 2.3: Panda Endpoint Protection general structure

- **Collective intelligence servers**: collect and classify the samples and evidence sent by Panda Security's customers. Additionally, they host a database of all detected threats, accessible in real time.
- **Signature file download servers**: host the signature file downloaded by Panda Security's products.
- **Panda Patch Management service (optional)**: a service for patching Windows operating systems and third-party applications.
- **Panda Full Encryption service (optional)**: encrypts the internal storage devices of Windows computers in order to minimize data exposure in the event of loss or theft, as well as when storage devices are removed without having deleted their content.
- **Web console**: management console server.
- Computers protected with the installed software (Panda Endpoint Protection).

- Computer of the network administrator that accesses the Web console.

Collective Intelligence servers

Collective Intelligence has servers that automatically classify and process all the data provided by the user community about the detections made on customers' systems. These servers belong to Panda Security's cloud-based infrastructure. It is worth noting that the Panda Endpoint Protection protection installed on computers queries Collective Intelligence only when required, ensuring maximum detection power without negatively affecting resource consumption.

Signature file servers

These are the cloud-based resources that Panda Security makes available to users to download the signature files required by Panda Endpoint Protection to perform detection tasks. Since signature files can be quite large and are downloaded at least once a day, signature file servers check the version of the signature files installed on the customer's computers in order to calculate the difference between those files and the published version and send only the necessary data. This way, they reduce the customer's bandwidth usage costs in relation to updating the antivirus solution installed across their network.

Web console administration

The Web console is compatible with the most popular Internet browsers, and is accessible anytime, anywhere from any device with a supported browser.

> *To check whether your Internet browser is compatible with the service, refer to "***Web console access***" on page* **380***.*

The Web console is responsive, that is, it can be used on smartphones and tablets without any problems.

Computers protected with Panda Endpoint Protection

Panda Endpoint Protection requires the installation of a small software component on all computers on the network susceptible of having security problems. This component is made up of two modules: the Panda communications agent and the Panda Endpoint Protection protection module.

> *Panda Endpoint Protection can be installed without problems on computers with competitors' security products installed.*

The protection module contains the technologies designed to protect customers' computers. Panda Endpoint Protection provides, in a single product, everything necessary to detect malware, as well as remediation tools to disinfect compromised computers.

Panda Patch Management service (optional)

This service reduces the attack surface of the Windows workstations and servers in the organization by updating the vulnerable software found (operating systems and third-party applications) with the patches released by the relevant vendors.

Additionally, it finds all programs on the network that have reached their EOL (End-Of-Life) stage. These programs pose a threat as they are no longer supported by the relevant vendor and are a primary target for hackers looking to exploit known unpatched vulnerabilities. With Panda Patch Management, administrators can easily find all EOL programs in the organization and design a strategy for the controlled removal of this type of software.

Also, in the event of compatibility conflicts or malfunction of the patched applications, Panda Patch Management allows organizations to roll back/uninstall those patches that support this feature, or exclude them from installation tasks, preventing them from being installed.

Panda Full Encryption service (optional)

The ability to encrypt the information held in the internal storage devices of the computers on your network is key to protecting the stored data in the event of loss or theft or when the organization recycles storage devices without having deleted their contents completely. Panda Security uses the Windows BitLocker technology to encrypt hard disk contents at sector level, centrally managing recovery keys in the event of loss or hardware configuration changes.

The Panda Full Encryption module lets you use the Trusted Platform Module (TPM), if available, and provides multiple authentication options, adding flexibility to computer data protection.

Product user profile

Even though Panda Endpoint Protection is a managed service that offers security without intervention by the network administrator, it also provides clear and detailed information about the activity of the processes run by all users on the organization's network. This data can be used by administrators to clearly assess the impact of security problems, and adapt the company's protocols to prevent similar situations in the future.

Supported devices and languages

*For a full description of the platforms supported by the solution, refer to "***Hardware, software and network requirements***" on page* **373**

Supported operating systems

- Windows Workstation
- Windows Server
- Persistent and non-persistent VDI systems.
- macOS
- Linux
- Android smartphones and tablets

Supported Web browsers

The management console supports the latest versions of the following Web browsers:

- Chrome
- Internet Explorer
- Microsoft Edge
- FireFox
- Opera

Languages supported in the management console

- English
- Finnish (local console only)
- French
- German
- Hungarian
- Italian
- Japanese
- Portuguese
- Russian
- Spanish
- Swedish

Chapter 3

Panda Endpoint Protection features

Companies increasingly rely on IT technologies to conduct their business operations, which exposes them to new malware types designed to threaten the integrity of their assets. In this scenario, keeping the huge number of new threats that appear every day under control demands the implementation of a new security approach that doesn't degrade the performance of the protected workstations and servers. Panda Endpoint Protection implements the necessary resources to provide customers with the comprehensive protection they need without impacting computer performance.

CHAPTER CONTENT

New security needs

In recent years, the use of the Internet and all types of mobile devices has become universal in all fields. Laptops, servers, smartphones, tablets, removable storage drives and numerous other devices are now widely used in corporate environments. The business world has benefited enormously from these changes, increasing productivity and efficiency, and also improving internal and external communication.

However, and at the same time, there have been significant changes in the malware landscape: from the exponential growth in dangerous items circulating on the Internet to the increasing sophistication with which malware operates. Today, malware aims to go completely unnoticed in order to achieve its goal, which is in almost all cases, financial.

This new scenario demands enormous resources on the computers to protect, with a huge impact on device performance.

Panda Endpoint Protection is a security product for workstations and servers based on Collective Intelligence: a huge cloud-based database which is fed with the shared knowledge on malware and disinfections collected from millions of users. Thanks to Collective Intelligence, all computers that make up the Panda community instantly share and benefit from information on the current malware landscape, without affecting performance.

Permanent antivirus protection and Collective Intelligence

The permanent antivirus protection is the traditional security module used to defend organizations against the infection vectors most commonly used by hackers. This module leverages Panda Security's locally stored signature file as well as its real-time queries to Collective Intelligence.

In the current context of ever-increasing amounts of malware, cloud-hosted services have proven much more efficient than traditional signature files to successfully combat the enormous amount of threats in circulation. That's why Panda Endpoint Protection's antivirus protection is primarily based on Collective Intelligence, a cloud-based knowledge platform that exponentially increases detection capabilities.

Collective Intelligence has servers that automatically classify and process all the information provided by the user community about the detections made on their systems. Panda Endpoint Protection queries Collective Intelligence only when required, ensuring maximum detection power without negatively affecting resource consumption.

When new malware is detected on a computer in the user community, Panda Endpoint Protection sends the information to our Collective Intelligence servers in the cloud, automatically and anonymously. This information is then processed, delivering a solution to all users in the community in real time.

In short, Panda Endpoint Protection leverages Collective Intelligence to increase its detection capabilities without negatively impacting system performance. Now, all knowledge is in the cloud, and thanks to Panda Endpoint Protection, all users can benefit from it.

*For more information about Panda Endpoint Protection's antivirus service for Windows, macOS and Linux platforms, refer to "***Security settings for workstations and servers***" on page* 207.

*For more information about Panda Endpoint Protection's antivirus service for Android platforms, refer to "***Security settings for Android devices***" on page* 223.

Protection with context-based detections

In addition to the traditional detection strategy based on comparing the payload of scanned files to the antivirus solution's signature file, Panda Endpoint Protection implements several detection engines that analyze the behavior of processes locally.

Through the integration with Windows 10's AMSI (AntiMalware Scan Interface), the solution can detect anomalous behaviors in scripts and the macros embedded in Office files.

Additionally, the solution also incorporates traditional heuristic engines and engines to detect malicious files by their static characteristics.

Email and Web protection

Panda Endpoint Protection goes beyond the traditional email and Web security approach based on plug-ins that add protection features to certain email clients and Web browsers. Instead, it works by intercepting, at low level, every communication that uses common protocols such as HTTP, HTTPS or POP3. This way, the solution is able to provide permanent, homogeneous protection for all email and Web applications past, present and future, without the need for specific configurations or updates every time an email or Web browser vendor releases a new product incompatible with the previous plug-ins.

Firewall and intrusion detection system (IDS)

Panda Endpoint Protection monitors the communications sent and received by each computer on the network, blocking all traffic that matches the rules defined by the administrator. This module is compatible with both IPv4 and IPv6, and includes multiple tools for filtering network traffic:

- **Protection using system rules**: these rules describe communication characteristics (ports, IP addresses, protocols, etc.) in order to allow or deny the data flows that match the configured rules.
- **Program protection**: rules that allow or prevent the programs installed on users' computers from communicating with other computers on the network.
- **Intrusion detection system**: detects and rejects malformed traffic patterns that can affect the security or performance of protected computers.

Device control

Popular devices such as USB flash drives, CD/DVD drives, imaging and Bluetooth devices, modems and smartphones can become a gateway for infections.

Panda Endpoint Protection allows administrators to restrict the use of those devices on protected computers, blocking access to them or allowing full or partial use only (read-only access).

Anti-exploit protection

Panda Endpoint Protection implements technologies to protect network computers against threats capable of leveraging vulnerabilities in installed software. These vulnerabilities can be exploited to cause anomalous behaviors in applications, leading to security failures on customers' networks.

These exploits leverage both known and unknown (zero-day) vulnerabilities, triggering a chain of events (CKC, Cyber Kill Chain) that they must follow to compromise systems. Panda Endpoint Protection blocks this chain of events effectively and in real time, neutralizing exploit attacks and rendering them harmless.

In order to detect the vulnerability exploit techniques used by hackers, Panda Endpoint Protection implements new hooks in the operating system, using them to locally and continually monitor all actions taken by the processes run on users' computers. This strategy goes beyond the traditional approach used by other security products and consisting of searching for patterns and statically detecting CVE-payload pairs through signature files.

Vulnerability patching (Panda Patch Management)

Panda Patch Management keeps a database of the patches and updates released by software vendors for the Windows operating systems installed on customers' networks. The service compares this database to the actual patches installed across each customer's organization and identifies computers with vulnerable software. These computers are susceptible to malicious attacks aimed at infecting the corporate network.

To tackle this threat, Panda Patch Management allows administrators to create quick and scheduled patching tasks and push them to the computers in their organization, thus reducing the attack surface of workstations and servers.

Network status visibility

Panda Endpoint Protection provides a number of resources that allow administrators to assess the security status of their corporate network at a glance, using reports and the widgets displayed in the solution's dashboard.

The Panda Endpoint Protection widgets provide key information about the detections made in the different malware infection vectors.

For more information, refer to **“Malware and network visibility”**.

Disinfection techniques

In the event of a security breach, Panda Endpoint Protection allows administrators to quickly restore the affected computers to their original state with advanced disinfection tools and a quarantine to store suspicious and deleted items.

For more information, refer to **"Remediation tools"**.

The adaptation phase

Panda Endpoint Protection can be used to strengthen endpoint security in a number of ways:

- **Changing the antivirus protection settings**

Changing the frequency of scheduled scans or enabling the protection against infection vectors such as email or the Internet will help protect those computers that get infected through those channels.

- **Partially or totally blocking access to pen drives and other external devices**

Another commonly-used infection vector is the USB drives and modems that users bring from home. Limiting or totally blocking access to these devices will block malware infections through these means.

- **Restricting communications (firewall and IDS)**

A firewall is a tool designed to minimize exposure to threats by preventing communications to and from programs that are not malicious in nature but may leave the door open to malware. If malware is detected that has infected the network via a chat or P2P application, configuring the firewall rules correctly can prevent those programs from communicating with the outside world.

Firewalls and IDS systems can also be used to prevent malware from propagating once the first computer has been infected. Examining the actions triggered by malware with the forensic analysis tool provided by Panda Endpoint Protection will help you generate new firewall rules that restrict communications from one computer to another and protect the organization against network attacks.

- **Changing the Panda Patch Management settings**

Changing the settings of patching tasks will let you minimize the time during which your programs remain vulnerable to attacks looking to exploit security holes. Also, installing more different types of patches will improve the security of the network, ensuring that all your software incorporates the latest updates released by the relevant vendors.

Additionally, uninstalling or updating the programs that have reached their EOL (End-Of-Life) stage will minimize the attack surface of your computers, as all software that does not receive updates will be removed. This software is more likely to have unpatched vulnerabilities that could be exploited by malware.

- **Encrypting the information contained on the internal storage devices of computers with Panda Full Encryption enabled.**

This will minimize the exposure of the data stored on the company's computers in the event of loss or theft, and prevent access to confidential data with recovery tools for retrieving files from removed drives. Additionally, we recommend that you use the TPM module included on computer motherboards, or update their hardware to support this tool. The TPM lets you prevent hard disks from being used on computers other than those used to encrypt them, and detect changes to a computer's boot sequence.

Part 2

The management console

Chapter 4: The management console

Chapter 5: Controlling and monitoring the management console

Chapter 4

The management console

Panda Endpoint Protection leverages the latest Web development techniques to provide a cloud-based management console that allows organizations to interact with the security service simply and centrally. Its main features are as follows:

- **It is adaptive**: its responsive design allows the console to adapt to the size of the screen or Web browser the administrator is viewing it with.
- **It is user friendly**: the console uses Ajax technologies to avoid full page reloads.
- **It is flexible**: its interface adapts easily to the administrator's needs, allowing them to save settings for future use.
- **It is homogeneous**: it follows well-defined usability patterns to minimize the administrator's learning curve.
- **It is interoperable**: the data displayed can be exported to CSV format with extended fields for later consultation.

CHAPTER CONTENT

Benefits of the Web console

The Web console is the main tool with which administrators can manage security. As it is a centralized Web service, it brings together a series of features that benefit the way the IT department operates.

- **A single tool for complete security management**

The Web console lets administrators deploy the Panda Endpoint Protection installation package to all computers on the network, configure their security settings, monitor the protection status of the network, and benefit from remediation to resolve security incidents. All these features are provided from a single Web-based console, facilitating the integration of the different tools and minimizing the complexity of using products from different vendors.

- **Centralized security management for all offices and mobile users**

The Web console is hosted in the cloud so it is not necessary to configure VPNs or change router settings to access it from outside the company network. Neither is it necessary to invest in IT infrastructures such as servers, operating system licenses or databases, nor to manage maintenance and warranties to ensure the operation of the service.

- **Security management from anywhere at anytime**

The Web console is responsive, adapting to any device used to manage security. This means administrators can manage protection in any place and at any time, using a smartphone, a notebook, a desktop PC, etc.

Web console requirements

If your security provider is Panda Security, use the following URL to access the Panda Endpoint Protection Web console:

https://www.pandacloudsecurity.com/PandaLogin/

If your security provider is WatchGuard, follow these steps to access the Panda Endpoint Protection Web console:

- Go to https://www.watchguard.com/ and click the **Log In** button in the upper-right corner of the page.
- Enter your WatchGuard credentials. The **Support Center** page opens.
- Click the **My Watchguard** menu at the top of the page. A drop-down menu appears.
- Click the **Manage Panda Products** option. The Panda Cloud page opens with all contracted services.
- Click the Panda Endpoint Protection panel. The management console opens.

The following requirements are necessary to access the Web console:

- You must have valid login credentials (user name and password).

For more information on how to create a Panda Account to access the Web console, refer to "The Panda Account" on page 383.

- A certified supported browser.
- Internet connection and communication through port 443.

IDP-based federation

Panda Endpoint Protection delegates credential management to an identity provider (IdP), a centralized application responsible for managing user identity.

This means that with a single Panda Account, the network administrator will have secure, simple access to all contracted Panda Security products.

General structure of the Web console

The Web console has resources that ensure a straightforward and smooth management experience, both with respect to security management as well as remediation tasks.

The aim is to deliver a simple yet flexible and powerful tool that allows administrators to begin to productively manage network security as soon as possible.

Below is a description of the items available in the console and how to use them.

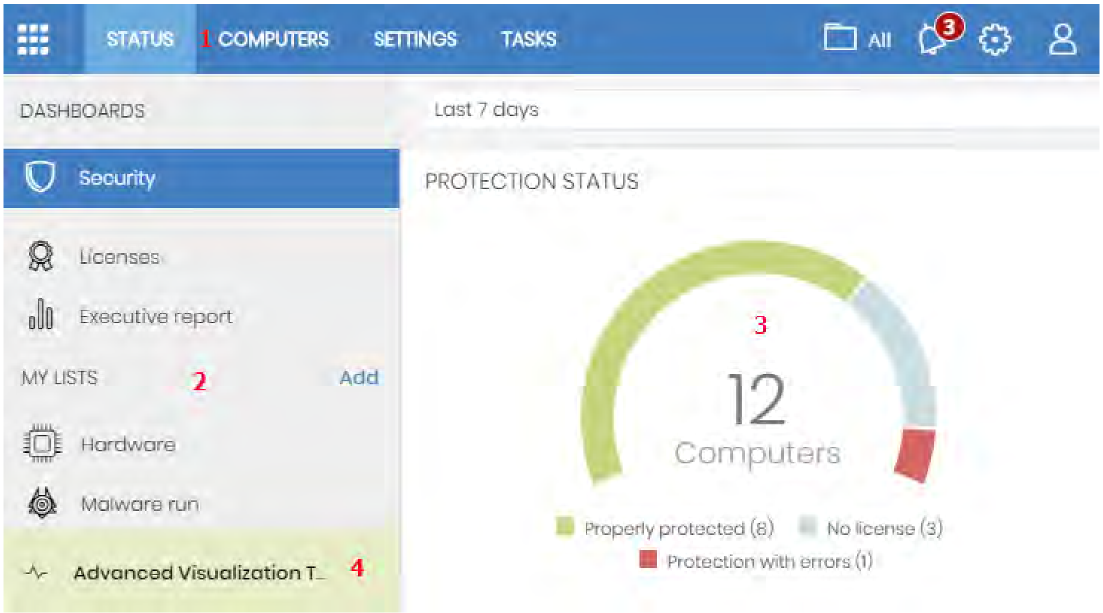


Figure 4.1: Panda Endpoint Protection management console overview

Top menu (1)

The top menu allows you to access each of the main areas that the console is divided into:

- Panda Cloud button
- Status
- Computers
- Settings
- Tasks
- Filter by group
- Web notifications
- General options
- User account

Panda Cloud button

Click the ▦ button located in the left corner of the top menu. You'll access a section from which you will be able to access every Panda Security product you have contracted, as well as editing your Panda Account settings.

Status menu

The Status menu at the top of the console displays a dashboard that provides administrators with an overview of the security status of the network through widgets and a number of lists accessible through the side menu. Refer to "**Status area overview**" for more information.

Computers menu

The **Computers** menu provides the basic tools for network administrators to define the computer structure that best adapts to the security needs of their IT network. Choosing the right device structure is essential in order to assign security settings quickly and easily. Refer to "**The Computers area**" on page 133 for more information.

Settings menu

Lets you define the behavior of Panda Endpoint Protection on the workstations and servers where it is installed. Settings can be assigned globally to all computers on the network, or to some specific computers only through templates, depending on the type of settings to apply. Settings templates are very useful for computers with similar security requirements, and help reduce the time needed to manage the security of the computers on your IT network.

> *Refer to "**Managing settings**" on page 175 for detailed information on how to create a settings profile in Panda Endpoint Protection.*

Tasks menu

Lets you schedule security tasks to be run on the day and time specified by the administrator. Refer to "**Tasks**" for more information.

Filter by group icon

Limits the information displayed in the console to that collected from the computers belonging to the selected group(s). Refer to "**Filtering results by groups**" on page 145 for more information.

Web notifications icon

Click the icon to show a drop-down menu with the general communications that Panda Security makes available to all console users, sorted by importance:

- Planned maintenance tasks
- Alerts regarding critical vulnerabilities
- Security tips
- Messages to start console upgrade processes. Refer to "**Product updates and upgrades**" on page 123.

Each communication has a priority level associated with it:

- 🔴 Important
- 🟠 Notice
- 🔵 Information

The number on the icon indicates the number of new (unread) web notifications.

To delete a web notification, click the X icon ✕. Deleted notifications are not shown again, and the number on the icon changes to show the total number of available notifications.

General options icon ⚙

Displays a drop-down menu that allows the administrator to access product documentation, change the console language and access other resources.

Option	Description
Online help	Lets you access the product's Web help.
Panda Endpoint Protection Administration guide	Lets you access the Panda Endpoint Protection administrator's guide.
Technical Support	Takes you to the Technical Support website for Panda Endpoint Protection.
Suggestion Box	Launches the mail client installed on the computer to send an email to Panda Security's technical support department.
License Agreement	Displays the product's EULA (End User License Agreement).
Data processing agreement	Displays the data processing agreement for the platform in compliance with European regulations.
Panda Endpoint Protection Release Notes	This section takes you to a support page detailing the changes and new features incorporated into the new version.
Language	Lets you select the language of the management console.
About...	Displays the version of the different elements that make up Panda Endpoint Protection. • **Version**: product version. • **Protection version**: internal version of the protection module installed on computers. • **Agent version**: internal version of the communications module installed on computers.

Table 4.1: 'General options' menu

User account icon 👤

Displays a drop-down menu with the following options:

Option	Description
Account	Name of the account used to access the console.
Customer ID	This is the number used by Panda to identify the customer. It's sent in the welcome email and requested in all communications with support.
Email address	Email address used to access the console.
Set up my profile	Lets you change the information of the product's main account. Users who access the Panda Endpoint Protection console from WGPortal won't see this option as their account is configured from the WatchGuard website.
Change account	Lists all the accounts that are accessible to the administrator and lets you select an account to work with.
Log out	Lets you log out of the management console and takes you back to the IdP screen.

Table 4.2: 'User account' menu

Side menu (2)

The side menu lets you access different subareas within the selected area. It acts as a second-level selector with respect to the top menu.

The side menu will change depending on the area you are in, adapting its contents to the information required.

To maximize the display area of the center panel, reduce the size of the side menu by clicking the panel splitter. Reducing it too much will cause the side menu to be hidden. To restore the menu to its original size, click the › icon.

Center panel (3)

Displays all relevant information for the area and subarea selected by the administrator. Figure 4.1 shows the **Status** area, **Security** subarea, with widgets that allow administrators to interpret the security information collected from the network. For more information about widgets, refer to "Security panels/widgets" on page 300.

Basic elements of the Web console

Tab menu

The most complex areas of the console provide a third-level selector in the form of tabs that present the information in an ordered manner.

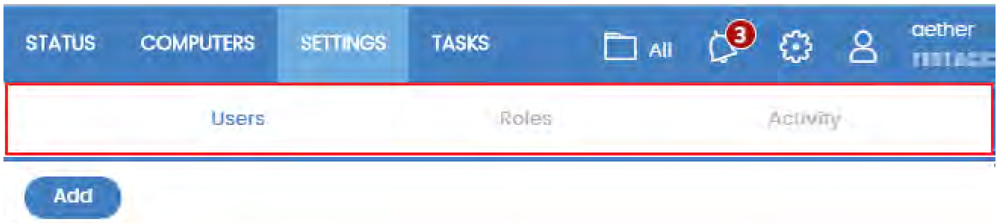


Figure 4.2: Tab menu

Action bar

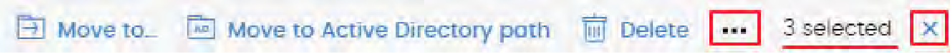


Figure 4.3: Action bar

To facilitate navigating the console and performing some common operations on your managed workstations and servers, an action bar has been added at the top of certain screens in the console. The number of buttons on the action bar adapts to the size of the window. Click the ••• icon at the right end of the action bar to view those buttons that don't fit within the allocated space.

Finally, take a look at the far right-hand corner of the action bar to see the total number of selected computers. Click the cross icon to undo your selection.

Filtering and search tools

The filtering and search tools allow administrators to filter and display information of special interest. Some filtering tools are generic and apply to the entire screen, for example, those displayed at the top of the **Status** and **Computers** screens.

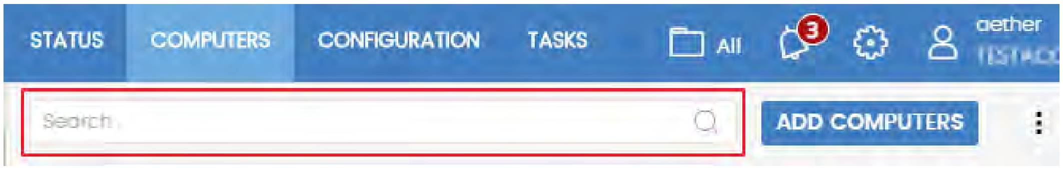
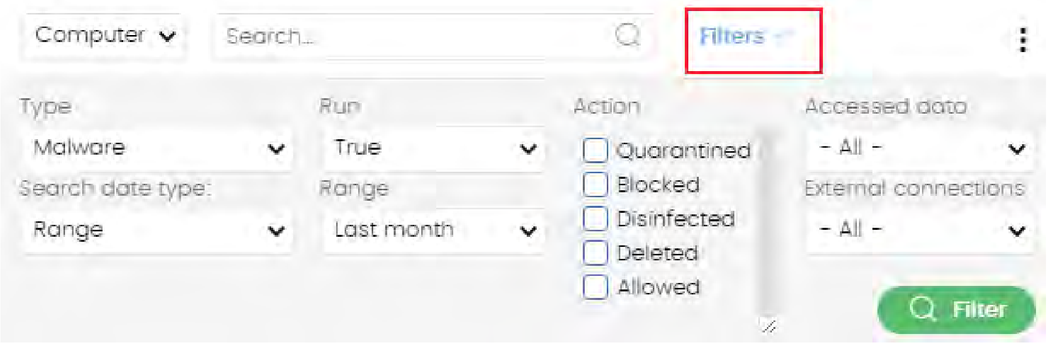


Figure 4.4: Search tool

Some filtering tools are hidden under the **Filters** button, and allow you to refine your searches according to categories, ranges and other parameters based on the information displayed.



Type
Malware

Search date type:
Range

Run
True

Range
Last month

Action
☐ Quarantined
☐ Blocked
☐ Disinfected
☐ Deleted
☐ Allowed

Accessed data
- All -

External connections
- All -

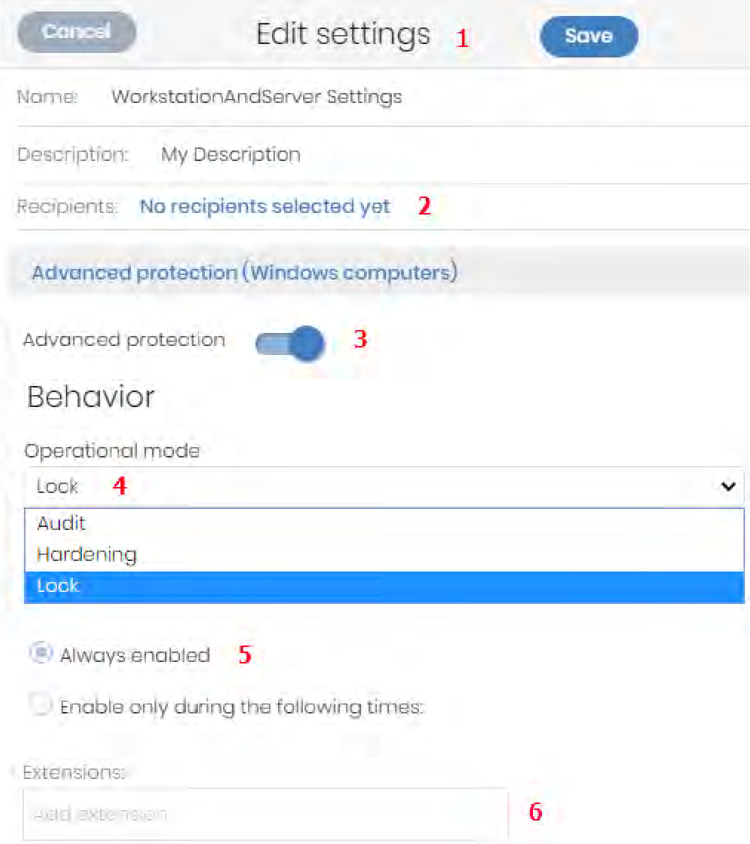
Figure 4.5: Filtering tool for data lists

Other interface elements

The Panda Endpoint Protection Web console uses standard interface elements for configuring settings, such as:

- Buttons **(1)**
- Links **(2)**
- Checkboxes **(3)**
- Drop-down menus **(4)**
- Combo boxes **(5)**

- Text fields **(6)**



Name: WorkstationAndServer Settings

Description: My Description

Recipients: No recipients selected yet

Advanced protection

Operational mode: Lock

● Always enabled

○ Enable only during the following times:

Extensions: Add extension

Figure 4.6: Controls for using the management console

Sort button

Some lists of items, such as those displayed in the **Tasks** area (top menu **Tasks**) or in the **Settings** area (top menu **Settings**), show a sort button in the top-right or bottom-right corner of the list ↓≡. This button lets you sort the items in the list according to different criteria:

- **By creation date**: items are sorted based on when they were added to the list.
- **By name**: items are sorted based on their name.
- **Ascending order**.
- **Descending order**.

Context menus

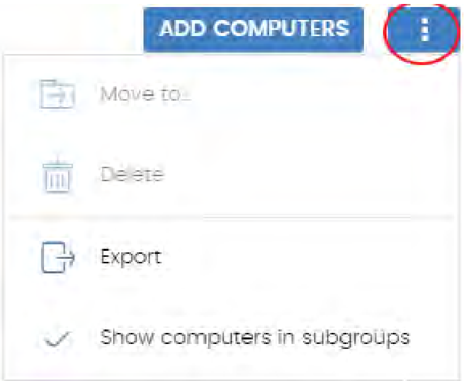


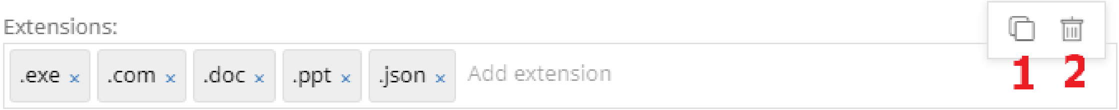
Figure 4.7: Context menu

These are drop-down menus that are displayed when you click the ⋮ icon. They show options relevant to the area they are in.

Copy contents and Delete contents buttons

If you place the mouse pointer over a text box that enables you to enter multiple values separated by spaces, two buttons will appear for copying and deleting its contents.

- **Copy button (1)**: copies the items in the text box to the clipboard, separated by carriage returns. A message appears in the console when the operation is complete.
- **Delete button (2)**: clears the contents of the text box.



Extensions: .exe × .com × .doc × .ppt × .json ×

Figure 4.8: Copy and Delete buttons

- Click on a text box and press Control+v to insert the contents of the clipboard, provided it contains text lines separated by carriage returns.

Status area overview

The **Status** menu includes the main visualization tools and is divided into several sections:

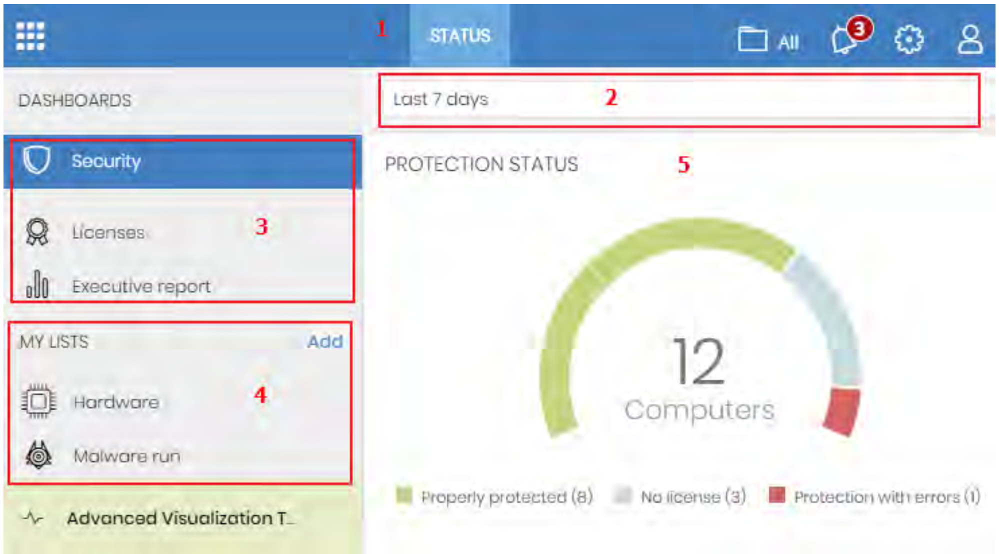


Figure 4.9: Status window (dashboard and access to lists)

- **Access to the dashboard (1)**

The **Status** menu at the top of the screen grants you access to various types of dashboards. From here you can also access different widgets, as well as lists.

The widgets represent specific aspects of the managed network, while more detailed information is available through the lists.

- **Time period selector (2)**

The dashboard displays information for the time period established by the administrator through the tool at the top of the **Status** screen. The options are:

- Last 24 hours
- Last 7 days.
- Last month.
- Last year.

Not all information panels offer information for the last year. Those that don't support this time period have a notice indicating so.

- **Dashboard selector (3)**
  - **Security:** security status of the IT network. For more information about the widgets in this section, refer to "Security panels/widgets" on page 300.

- **Patch management**: updates of the operating system and third-party software installed on computers. For more information about the widgets in this section, refer to "Panda Patch Management widgets and panels" on page 241.
- **Encryption:** encryption status of your computers' internal storage devices. For more information about the widgets in this section, refer to "Panda Full Encryption panels and widgets".
- **Licenses**: status of the Panda Endpoint Protection licenses assigned to the computers on your network. Refer to "Licenses" for more information about license management.
- **Scheduled reports**: refer to "Scheduled sending of reports and lists" for more information on how to configure and generate reports.

- **My lists (4)**

The lists are data tables with the information presented in the panels. They include highly detailed information and have search tools to locate the information you need.

- **Information panels/widgets (5)**

Each dashboard has a series of widgets related to specific aspects of network security.

The information in the panels is generated in real time and is interactive: hover the mouse pointer over the items in the panels to display tooltips with more detailed information.

All graphs have a key explaining the meaning of the data displayed, and have hotspots that can be clicked on to show lists with predefined filters.

Panda Endpoint Protection uses several types of graphs to display information in the most practical way based on the type of data displayed:

- Pie charts.
- Histograms.
- Line charts.

Managing lists

Panda Endpoint Protection structures the information collected at two levels: a first level that presents the data graphically in panels or widgets, and a second, more detailed level, where the data is presented in tables. Most of the panels have an associated list so that the administrator can quickly access the information in a graph and then get more in-depth data if required from the lists.

Panda Endpoint Protection allows administrators to schedule lists to be sent via email. This eliminates the need to access the Web console to view the details of the events that have taken place across the network. Additionally, this feature makes it easier to share information among departments and enables organizations to build an external repository containing a history of all the events that have taken place, outside the boundaries of the Web console. With this repository, the management team will be able to keep track of the generated information free from third-party interference.

Templates, settings and views

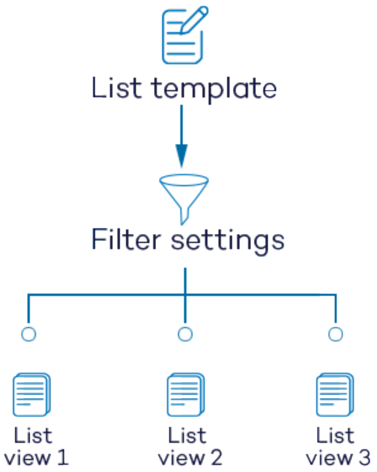


Figure 4.10: Generating three lists from a single template/data source

A list is the sum of two items: a template and a filter configuration.

A template can be thought of as a source of data about a specific area covered by Panda Endpoint Protection.

A filter is a specific configuration of the filtering tools associated with each template.

A filter applied to a template results in a 'list view' or, simply, a 'list'. Administrators can create and save new lists for later consultation by editing the filters associated with a template. This frees them from having to constantly redefine their commonly used templates, saving management time.

List templates

Go to top menu **Status**, side panel **My lists**, and click the **Add link** to display a window with all available templates grouped by type:

Group	List	Description
General	Licenses	Shows in detail the license status of the computers on your network. Refer to "**Licenses**" on page 116.
	Unmanaged computers discovered	Shows the Windows computers on your network that don't have the Panda Endpoint Protection software installed. Refer to "**Viewing discovered computers**" on page 92.
	Computers with duplicate name	Shows computers with the same name and belonging to the same domain. Refer to "**Computers with duplicate name'**" on page 157.
	Software	Shows the software installed on the computers on your network. Refer to "**'Software'**" on page 155.
	Hardware	Shows the hardware installed on the computers on your network. Refer to "**'Hardware'**" on page 153.
Security	Computer protection status	Shows in detail the protection status of the computers on your network. Refer to "**Computer protection status**" on page 307.

Table 4.3: Templates available in Panda Endpoint Protection

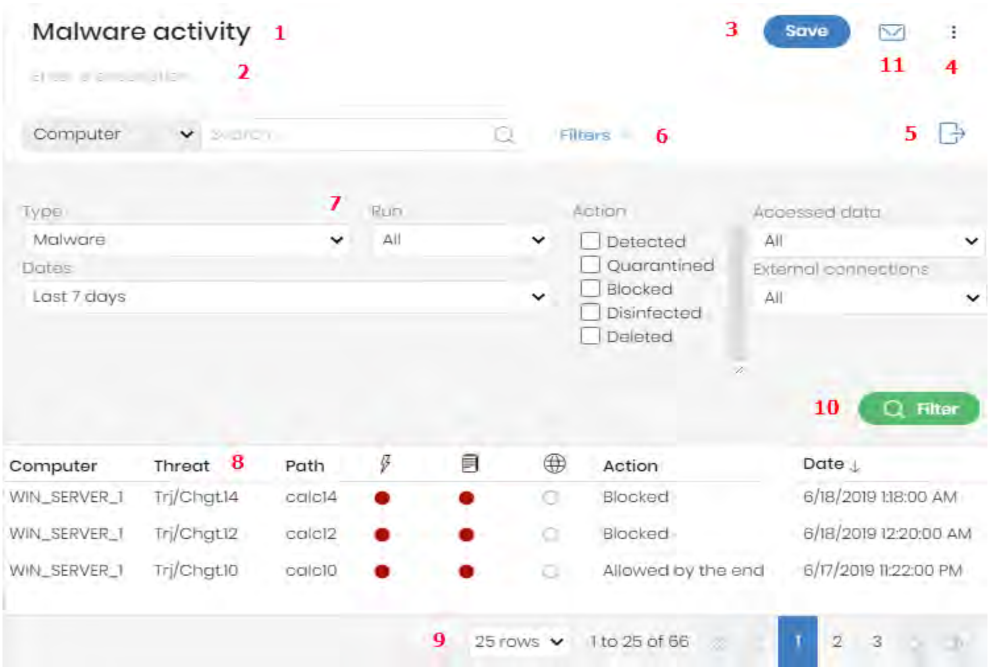
Group	List	Description
	Threats detected by the antivirus	Provides complete, consolidated information about all detections made on all supported platforms and in all the infection vectors scanned by the solution. Refer to "**Threats detected by the antivirus**" on page **312**.
	Intrusion attempts blocked	Shows the intrusion attempts blocked by the computer's firewall. Refer to "**Intrusion attempts blocked**" on page **319**.
	Blocked devices	Shows in detail all computers on your network with limitations regarding access to peripherals. Refer to "**Blocked devices**" on page **315**.
Patch management	Patch management status	Shows in detail all computers on the network compatible with Panda Patch Management. Refer to "**Patch management status**" on page **249**.
	Available patches	Shows a list of all missing patches on the computers on your network and published by Panda Security. Refer to "**Available patches**" on page **246**.
	Installation history	Shows the patches that Panda Endpoint Protection attempted to install and the computers that received them in a given time interval. Refer to "**Installation history**" on page **259**.
	End-of-Life programs	Shows information about the end of life of the programs installed on your network, grouped by the end-of-life date. Refer to "**End-of-Life programs**" on page **257**.
	Excluded patches	Shows the computer-patch pairs excluded from installation tasks. Refer to "**Excluded patches**" on page **263**.
Data protection	Encryption status	Shows information about the computers on your network compatible with the encryption feature. Refer to "**Encryption Status**" on page **289**.

Table 4.3: Templates available in Panda Endpoint Protection

Additionally, there are other templates you can directly access from the context menu of certain lists or from certain widgets on the dashboard. Refer to each widget's description for information about the lists they provide access to.

List sections

All lists have a number of tools in common to make interpretation easier. Below is a description of the main items in a sample list.



Type: Malware

Run: All

Dates: Last 7 days

Action:
- □ Detected
- □ Quarantined
- □ Blocked
- □ Disinfected
- □ Deleted

Accessed data: All

External connections: All

Computer	Threat	Path				Action	Date ↓
WIN_SERVER_1	Trj/Chgt14	calc14	●	●	○	Blocked	6/18/2019 1:18:00 AM
WIN_SERVER_1	Trj/Chgt12	calc12	●	●	○	Blocked	6/18/2019 12:20:00 AM
WIN_SERVER_1	Trj/Chgt10	calc10	●	●	○	Allowed by the end	6/17/2019 11:22:00 PM

Figure 4.11: List elements

- **List name (1)**: identifies the information on the list.
- **Description (2)**: a free text box for specifying the purpose of the list.
- **Save (3)**: a button for saving the current view and creating a new list in the My lists tree
- **Context menu (4)**: drop-down menu with the actions you can take on the list (copy and delete). Refer to "Operations with lists" for more information.
- **Context menu (5)**: drop-down menu with the list export options.
- **Link to filter and search tools (6)**: click it to display a panel with the available filter tools. Once you have configured your search parameters, click the **Filter (10)** button to apply them.
- **Filtering and search parameters (7)**: these let you filter the data displayed on the list.
- **Sorting order (8)**: change the sorting order of the list by clicking the column headers. Click the same header a second time to switch between ascending and descending order. This is indicated with arrows (an 'up' arrow ↑ or a 'down' arrow ↓). If you are accessing the management console from a small-size mobile device, click the icon in the bottom-right corner of the list to display a menu with the names of the columns included in the table.
- **Pagination (9)**: at the bottom of the table there are pagination tools to help you navigate easier

and faster.

Icon	Description
25 rows ⌄	Rows per page selector.
1 to 25 of 67	Number of rows displayed out of the total number of rows
«	First page link
‹	Previous page link
1 2 3	Numbered link to access pages directly
›	Next page link
»	Last page link

Table 4.4: Pagination tools

- **Scheduled send (11)**: Panda Endpoint Protection lets you email a .CSV file with the content of the list. Refer to "**Scheduled sending of reports and lists**" on page 339 for more information.

Operations with lists

Click the **Status** menu at the top of the console, and then click **My lists** from the side menu to view all lists created by the administrator as well as the lists that Panda Endpoint Protection includes by default. Refer to "**Default lists**".

Creating a custom list

There are various ways to create a new custom list/view:

- **From the My lists side menu**
  - Click the **Add link** from the **My lists** panel on the left to display a window showing all available templates.
  - Choose a template, configure the filter tools, edit the name and description of the list and click the **Save button (3)**.
- **From a dashboard panel**
  - Click a widget on the dashboard to open its associated template.
  - Click its context menu **(4)** and select **Copy**. A new list will be created.
  - Edit the list filters, name and description and click **Save (3)**.
- **From an existing list**
  - You can make a copy of an existing list by clicking its context menu **(4)** and then clicking **Copy**. A new list will be immediately generated with the name "Copy of...".

  - Edit the filters, name and description of the list and click the **Save** button **(3)**.

- **From the context menu of the My lists panel**

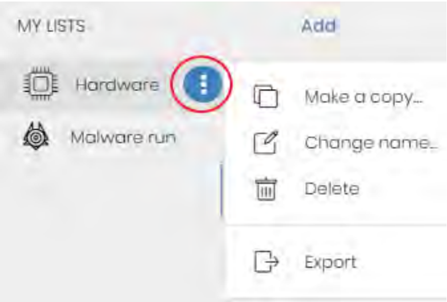


Figure 4.12: Context menu of the lists accessible from the 'My lists' panel

  - Click the context menu of the list you want to copy.
  - Click **Make a copy**. A new template view will be created which you can edit according to your preferences.
  - Edit the filters, name and description of the list and click the **Save** button **(3)**.

Deleting a list

There are various ways to delete a list:

- **From the My lists panel**
  - From the **My lists** panel, click the context menu of the relevant list.
  - Click the 🗑 icon.
- **From the list itself**
  - Click the list's context menu **(4)**.
  - Click the 🗑 icon from the drop-down menu displayed.

Copying a list

There are various ways to copy a list:

- **From the My lists panel**
  - Click the context menu of the list to copy.
  - Click the ⧉ icon.
- **From the list itself**
  - Click the list's context menu **(4).**
  - Click the ⧉ icon from the drop-down menu displayed.

Exporting a list

You can export lists to CSV format to obtain more information than is displayed in the Web console. For information about the fields in each exported file, refer to the relevant chapter in this Administration guide. There are various ways to export a list:

- From the **My lists** panel:
  - If the list does not support export of a details file, click the ⇨ icon. A .CSV file is downloaded with the list data.
  - If the list does support export of a details file, click the ⋮ icon **(5)**. A drop-down menu appears.
  - Click **Export** . A .CSV file is downloaded with the list data.
- **From the list itself:**
  - Click the list's context menu **(4).**
  - Click the ⧉ icon from the drop-down menu displayed. A .CSV file is downloaded with the list data.

Exporting a list's details

You can export a list's details to obtain more information than is displayed in the exported CSV file. For information about the fields in each exported file, refer to the relevant chapter in this Administration guide. There are various ways to export a list:

- From the **My lists panel:**
  - Click the ⋮ icon **(5)**. A drop-down menu appears.
  - Click **Export list and details**. A .CSV file is downloaded with the list details.
- From the list itself:
  - Click the list's context menu **(4)**. A drop-down menu appears.
  - Click the **Export list and details** icon ⧉ from the drop-down menu displayed. A .CSV file is downloaded with the list details.

Configuring a custom list

- Assign a new name to the list **(1)**. By default, the console creates new names for lists by adding the text "New" to the type of list, or "Copy" if the list is a copy of a previous one.
- Assign a description **(2)**: this step is optional.
- Click the **Filters** link **(6)** to display the filter options.
- Click **Filter (10)** to apply the configured filter and check if it meets your needs. The list will display the search results.
- Click **Save (3)**. The list will be added to the panel on the left under **My lists**, and will be accessible by

clicking on its name.

Scheduling a list to be sent via email

- **From the context menu of the Lists panel**
  - Click the context menu of the list to be sent and select the **Schedule send** option.
  - A window will open for you to enter the necessary information to automatically send the information.
- **From the list itself:**
  - Click the ✉ **(11) icon**. A window will open for you to enter the necessary information to automatically send the information.

*Refer to "*Scheduled sending of reports and lists*" on page* 339 *for more information*

Available actions for computers in lists

The **Licenses** and **Computer protection status** lists incorporate checkboxes to allow you to select computers. Select one or more computers to display an action bar at the top of the window which will make it easier for you to manage the selected workstations and servers.

Default lists

The management console includes various lists generated by default:

- Unprotected workstations and laptops.
- Unprotected servers.
- Hardware
- Software

Unprotected workstations and laptops

This list shows all desktop and laptop computers, regardless of the operating system installed, which may be vulnerable to threats due to a problem with the protection:

- Computers on which the Panda Endpoint Protection software is currently being installed or installation failed.
- Computers on which the protection is disabled or has errors.
- Computers without a license assigned or with an expired license.
- Refer to "Computer protection status" on page 307 for more information.

Unprotected servers

This list shows all servers, regardless of the operating system installed, which may be vulnerable to threats due to a problem with the protection:

- Servers on which the Panda Endpoint Protection software is currently being installed or installation failed.
- Servers on which the protection is disabled or has errors.
- Servers without a license assigned or with an expired license. Refer to "**Computer protection status**" on page **307** for more information.

Software

Shows a list of the programs installed across your network. Refer to "'**Software**'" on page **155** for more information.

Hardware

Shows a list of the hardware components installed across your network. Refer to "'**Hardware**'" on page **153** for more information.

Chapter 5

Controlling and monitoring the management console

Panda Endpoint Protection implements resources to control and monitor the actions taken by the network administrators that access the Web management console.

These resources are as follows:

- User account.
- Roles assigned to user accounts.
- User account activity log.

CHAPTER CONTENT

What is a user account?

A user account is a resource managed by Panda Endpoint Protection. It comprises a set of information that the system uses to regulate administrator access to the Web console and define the actions that administrators can take on users' computers.

User accounts are only used by the administrators that access the Panda Endpoint Protection console. Each administrator can have one or more personal user accounts.

In general, the term "user" is used to refer to the person who uses a computer or device. Here, however, it is associated with the user account used by the administrator to access the Web console.

User account structure

A user account comprises the following items:

- **Account login email**: this is assigned when the account is created. Its aim is to identify the administrator accessing the account.
- **Account password**: this is assigned once the account is created and is designed to control access to the account.
- **Assigned role**: this is assigned once the user account is created. It lets you determine which computers the account user will be able to manage and the actions they will be able to take.

Two-factor authentication

Panda Endpoint Protection supports the two-factor authentication (2FA) standard in order to add an additional layer of security beyond that offered by the 'user- password' basic pair. This way, when the network administrator attempts to access the Web console, they will be prompted to enter an additional authentication item: a code that only the account owner has. This is a randomly generated code that is sent to a specific device, normally the Panda Endpoint Protection administrator's personal smartphone or tablet.

Requirements for enabling 2FA

- Access to a personal smartphone or tablet with a built-in camera.
- Google Authenticator or an equivalent app must be installed on the personal device. Google Authenticator can be downloaded for free from https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl

Enabling 2FA

- In the top menu, click the user account and select the **Set up my profile** option. This will open the **Panda Account** window.

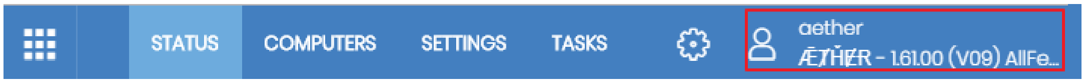


Figure 5.1: Shortcut to your Panda Account

- Click Login from the side menu and then click the **Enable** link in section **Two-step verification.** A window will open for you to configure Google Authenticator or the equivalent app installed on your mobile device.
- Scan the QR code displayed in the window using Google Authenticator or your equivalent app and enter the generated code in section **Enter the code provided by your app**. Finally, click the **Verify** button. From this moment onwards, your device will be linked to the Panda Endpoint Protection service and will generate short-lived random passcodes.

Accessing the console using an account with 2FA enabled

To access the console with a user account that has 2FA enabled, enter your login address, password, and the code generated on the device linked to the account.

Forcing all console users to use 2FA

To force all console users to enable and use 2FA, the user account from which the use of 2FA is enforced must have the **Manage users and roles** permission and access to all computers on the network. Refer to "Manage users and roles" for a description of the aforementioned permission and section "Role structure" for information on how to configure the groups the role will grant permissions on.

- Click the Settings menu at the top of the console. Then, click the **Security tab**.
- Select the option **Require users to have two-factor authentication enabled to access this account**.

- If the user account that forces all console users to have 2FA enabled does not have 2FA enabled for itself, a warning message will be displayed prompting you to access the **Panda Account** and enable the feature. Refer to "**Enabling 2FA**".

What is a role?

A role is a set of permissions for accessing the console that are applied to one or more user accounts. This way, a specific administrator is authorized to view or edit certain resources in the console, depending on the role assigned to the user account with which they access the Panda Endpoint Protection console.

A user account can only have one role assigned. However, a role can be assigned to more than one user account.

Role structure

A role is made up of the following:

- **Role name**: this is purely for identification and is assigned when the role is created.
- **Groups the role grants permissions on**: this lets you restrict the network computers accessible to the user. Select the folders in the group tree that the user account has access to.
- **Set of permissions**: this lets you determine the specific actions that the user account can take on the computers included in the accessible groups.

Why are roles necessary?

In a small IT department, all technicians will typically access the console as administrators without any type of restriction. However, in mid-sized or large departments with large networks to manage, it is highly likely that it will be necessary to organize or segment access to computers, under three criteria:

- **The number of computers to manage.**

With medium size or large networks, or those in branches of an organization, it may be necessary to assign computers to specific technicians. This way, the devices in one office managed by a particular technician will be invisible to the technicians who manage the devices of other branches.

It may also be necessary to restrict access to sensitive data by certain users. These cases will often require careful assignment of the technicians who will be able to access the devices with such data.

- **The purpose of the specific computer.**

Depending on its purpose, a computer or service within the company may be assigned to a technician specialized in the relevant field. For example, file servers are assigned to a group of specialized technicians. This way, other systems, such as user workstations, will not be visible to this group of technicians.

- **The knowledge or expertise of the technician.**

Depending on the profile of the technician or their role within the IT department, they can be assigned simply monitoring or validation access (read-only) permissions or, on the other hand, more advanced access, such as permission to edit the security settings of computers. For example, it is not uncommon in large companies to find a certain group of technicians dedicated solely to deploying software on the network.

These three criteria can overlap each other, giving rise to a combination of settings that are highly flexible and easy to set up and maintain. It also makes it easy to define the functions of the console for each technician, depending on the user account with which they access the system.

Full Control role

All Panda Endpoint Protection licenses come with the **Full Control** role assigned. The default administration account also has this role assigned. This account allows the user to take every action available in the console on the computers integrated in Panda Endpoint Protection.

The **Full Control** role cannot be deleted or edited. Nor is it possible to access its details. Any user account can be assigned this role through the Web console.

Read-only role

This role provides access to all components of the console, but doesn't let you create, edit, or delete settings, tasks, etc. That is, it provides total visibility of the environment but doesn't allow any sort of interaction. This role is especially suited to network administrators responsible for monitoring the network, but without sufficient permissions to take actions such as editing settings or launching on-demand scans.

The **Read-Only** role cannot be deleted or edited. Nor is it possible to access its details. Any user account can be assigned this role through the Web console.

What is a permission?

A permission regulates access to a particular aspect of the management console. There are different types of permissions that provide access to many aspects of the Panda Endpoint Protection console. A specific configuration of all available permissions generates a role, which can be assigned to one or more user accounts.

Understanding permissions

Below you will find a description of the permissions and their functions.

Manage users and roles

- **Enabled**: the account user can create, delete and edit user accounts and roles.
- **Disabled**: the account user cannot create, delete or edit user accounts or roles. It allows the user to view registered users and account details, but not the list of roles created.

Assign licenses

- **Enabled**: the account user can assign and withdraw licenses for the managed computers.
- **Disabled**: the account user cannot assign or withdraw licenses, but can see if the computers have licenses assigned.

Modify computer tree

- **Enabled**: the account user has complete access to the group tree, and can create and delete groups, as well as moving computers to already-created groups.
- **Enabled with permission conflict**: because of the inheritance mechanism that applies to the computer tree, any changes made to the tree structure may result in a change to the settings assigned to the affected devices. For example, in cases where the administrator does not have permission to assign settings, if they move a computer from one group to another, the web console will show a warning indicating that, because of the computer move operation and the inheritance mechanism applied, the settings assigned to the computer that was moved may have changed (even if the administrator does not have permission to assign settings). Refer to section "**Manual and automatic assignment of settings**" on page **184**.
- **Disabled:** the account user can view the group tree and the settings assigned to each group, but cannot create new groups or move computers.

Add, discover and delete computers

- **Enabled**: the account user can distribute the installer to the computers on the network and integrate them into the console. They can also delete computers from the console and configure all aspects related to the discovery of unmanaged computers: assign and revoke the discovery computer role, edit discovery settings, launch an immediate discovery task, and install the Panda agent remotely from the list of discovered computers.
- **Disabled**: the account user cannot download the installer, nor distribute it to the computers on the network. Neither can they delete computers from the console or access the computer discovery feature.

Modify network settings (proxies and cache)

- **Enabled**: the account user can create new **Network settings**, edit or delete existing ones and assign them to computers in the console.
- **Disabled**: the account user cannot create new **Network settings**, nor delete existing ones. Neither can they change the computers these settings are assigned to.

Configure per-computer settings (updates, passwords, etc.)

- **Enabled**: the account user can create new **Per-computer settings**, edit or delete existing ones and assign them to computers in the console.
- **Disabled**: the account user cannot create new **Per-computer settings**, nor edit or delete existing ones. Neither can they change the computers these settings are assigned to.

Restart and repair computers

- **Enabled**: the account user can restart workstations and servers from computer lists. They can also remotely reinstall the Panda Endpoint Protection software on Windows computers.
- **Disabled**: the account user cannot restart computers or remotely reinstall the Panda Endpoint Protectionsoftware.

Configure security for workstations and servers

- **Enabled**: the account user can create, edit, delete and assign security settings forworkstations and servers.
- **Disabled**: the account user cannot create, edit, delete or assign security settings for Windows, Linux and macOS workstations and servers.

Disabling this permission will display the **View security settings for workstations and servers** permission.

View security settings for workstations and servers

This permission is only accessible if you disable the Configure security settings for workstations and servers permission.

- **Enabled:** the account user can only see the security settings created, as well as the settings assigned to a computer or group.
- **Disabled**: the account user cannot see the security settings created nor access the settings assigned to a computer.

Configure security for Android devices

- **Enabled**: the account user can create, edit, delete and assign settings for Android devices.
- **Disabled**: the account user cannot create, edit, delete or assign settings for Android devices.

Disabling this permission will display the **View security settings for Android devices** permission, which is explained below.

View security settings for Android devices

> *This permission is only accessible if you disable the Configure security for Android devices permission.*

- **Enabled**: the account user can only see the settings created for Android devices, as well as the settings assigned to a specific Android device or group.
- **Disabled**: the account user cannot see the settings created for Android devices nor the settings assigned to a specific Android device or group.

Use the anti-theft protection for Android devices (locate, wipe, lock, etc.)

- **Enabled**: the account user can view the geolocation map and use the action panel for sending anti-theft tasks to Android devices.
- **Disabled**: the account user cannot view the geolocation map nor use the action panel for sending anti-theft tasks to Android devices.

View detections and threats

- **Enabled**: the account user can access the widgets and lists available through the **Security** section accessible from the **Status** menu at the top of the console, as well as creating new lists with custom filters.
- **Disabled**: the account user cannot see the widgets and lists available through the **Security** section accessible from the **Status** menu at the top of the console, nor create new lists with custom filters.

> *Access to the features related to the exclusion of threats is governed by the Exclude threats temporarily(Malware, PUPs and blocked items) permission.*

Launch scans and disinfect

- **Enabled**: the account user can create, edit and delete scan and disinfection tasks.
- **Disabled**: the account user cannot create new scan and disinfection tasks, nor edit or delete existing ones. They will only be able to list those tasks and view their settings.

Exclude threats temporarily (malware and PUPs)

- **Enabled**: the account user can exclude malware and PUPs from scans.
- **Disabled**: the account user cannot exclude malware and PUPs from scans, nor edit the existing

exclusions.

To allow a user to Exclude threats temporarily (Malware and PUPs), the View detections and threats permission must be enabled.

Configure patch management

- **Enabled**: the account user can create, edit, delete and assign patch management settings to Windows workstations and servers.
- **Disabled**: the account user cannot create, edit, delete or assign patch management settings to Windows workstations and servers.

Disabling this permission displays the **View patch management** settings permission.

View patch management settings

This permission is only accessible when you disable the Configure patch management permission.

- **Enabled**: the account user can only see the patch management settings created as well as the settings assigned to a computer or group.
- **Disabled**: the account user cannot see the patch management settings created.

Install, uninstall and exclude patches

- **Enabled**: the account user can create patch installation, uninstallation and exclusion tasks, and access the following lists: **Available patches**, **End-of-Life programs**, **Installation history** and **Excluded patches**.
- **Disabled**: the account user cannot create patch installation, uninstallation or exclusion tasks.

View available patches

This permission is only accessible if you disable the Install, uninstall and exclude patches permission.

- **Enabled**: the account user can access the following lists: **Patch management status**, **Available patches**, **'End-Of-Life' programs** and **Installation history**.
- **Disabled**: the account user won't be able to access the following lists: **Patch management status**, **Available patches**, **'End-Of-Life' programs** and **Installation history**.

Configure computer encryption

- **Enabled**: the account user can create, edit, delete and assign encryption settings for Windows computers.
- **Disabled**: the account user cannot create, edit, delete or assign encryption settings for Windows computers.

View computer encryption settings

> *This permission is only available if you disable the Configure computer encryption permission.*

- **Enabled**: the account user can only see the computer encryption settings created, as well as the encryption settings assigned to a computer or group.
- **Disabled**: the account user cannot see the encryption settings created, nor access the encryption settings assigned to each computer.

Access recovery keys for encrypted drives

- **Enabled**: the account user can view the recovery keys of those computers with encrypted storage devices and managed by Panda Endpoint Protection.
- **Disabled**: the account user cannot view the recovery keys of those computers with encrypted storage devices.

Accessing the user account and role settings

Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu. You'll see two sections associated with the management of roles and user accounts.

- **Users**: this lets you create new user accounts and assign a role to them.
- **Roles**: this lets you create and edit settings for accessing Panda Endpoint Protection resources.

The **Users and Roles** settings are only accessible if the user has the **Manage users and roles** permission.

Creating and configuring user accounts

Creating, editing and deleting users

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- Click the **Users** tab. There, you will be able to take all necessary actions related to the creation and editing of user accounts.

- **Add a new user account**: click **Add** to add a new user, set the email account for accessing the account, the role to which it belongs, and a description of the account. Once this is completed, the system will send an email to the account to generate the login password.
- **Edit a user account**: click the name of the user to display a window with all the account details that can be edited.
- **Delete or disable a user account**: click the 🗑 icon of a user account to delete it. Click a user account and select the button **Block this user** to temporarily block access to the Web console from this account. If the account is currently logged in, it will be logged out immediately. Also, no email alerts will continue to be sent to the email addresses configured in the account's settings.

Listing created users

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- Click the **Users** tab. A list will be displayed with all user accounts created in Panda Endpoint Protection, along with the following information:

Field	Description
Account name	User account name.
Role	Role assigned to the user account.
Email account	Email account assigned to the user.
Padlock	Indicates if the account has Two Factor Authentication (2FA) enabled.
Status	Indicates if the user account is enabled or blocked.

Table 5.1: User list

Creating and configuring roles

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- Click the **Roles** tab. There, you will be able to take all necessary actions related to the creation and editing of roles.
- **Add a new role**: click **Add** to add a new role. You will be asked for the name of the role, a description (optional), the groups the role will grant permissions on, and a specific configuration of permissions.
- **Edit a role**: click the name of the role to display a window with all the settings that can be edited.
- **Copy a role**: click the ⧉ icon to display a window with a new role with exactly the same settings as the original one.
- **Delete a role**: click the 🗑 icon of a role to delete it. If the role you are trying to delete has user accounts assigned, the process of deleting it will be canceled.

Limitations when creating users and roles

To prevent privilege escalation problems, users with the Manage users and roles permission assigned have the following limitations when it comes to creating new roles or assigning roles to existing users:

- A user account can only create new roles with the same or lower permissions than its own.
- A user account can only edit the same permissions as its own in existing roles. All other permissions will remain disabled.
- A user account can only assign roles with the same or lower permissions than its own.
- A user account can only copy roles with the same or lower permissions than its own.

User account activity log

Panda Endpoint Protection logs every action taken by network administrators in the Web management console. This makes it very easy to find out who made a certain change, when and on which object.

To access the activity log, click the **Settings** menu at the top of the console, then click **Users** from the left-side menu, and select the **Activity** tab.

Session log

The Sessions section displays a list of all accesses to the management console. It also allows you to export the information to a CSV file and filter the information.

- **Fields displayed in the 'Sessions' list**

Field	Description	Values
Date	Date and time that the access took place.	Date
User	User account that accessed the console.	Character string
Activity	Action performed by the user account.	• Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 5.2: Fields in the 'Sessions' list

- **Fields displayed in the exported file**

Field	Description	Values
Date	Date and time that the access took place.	Date
User	User account that accessed the console.	Character string
Activity	Action performed by the user account.	• Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 5.3: Fields in the 'Sessions' exported file

- **Search tool**

Field	Description	Values
From	Sets the start point of the search range.	Date
To	Sets the end point of the search range.	Date
Users	User name.	List of all user accounts created in the management console.

Table 5.4: Filters available in the 'Sessions' list

User actions log

The **User actions** section displays a list of all the actions taken by the user accounts, and allows you to export the information to a CSV file and filter the information.

- **Fields displayed in the 'Actions' list**

Field	Description	Values
Date	Date and time the action was carried out.	Date
Action	Type of action carried out.	Refer to table **Item types and actions**
Item type	Type of console object the action was performed on.	Refer to table **Item types and actions**
Item	Console object the action was performed on.	Refer to table **Item types and actions**

Table 5.5: Fields in the 'Actions' log

- **Fields displayed in the exported file**

Field	Description	Values
Date	Date and time the action was carried out.	Date
User	User account that performed the action.	Character string
Action	Type of action carried out.	Refer to table **Item types and actions**
Item type	Type of console object the action was performed on.	Refer to table **Item types and actions**
Item	Console object the action was performed on.	Refer to table **Item types and actions**

Table 5.6: Fields in the 'Action log' exported file

- **Search tool**

Field	Description	Values
From	Sets the start point of the search range. range.	Date
To	Sets the end point of the search range.	Date
Users	Users accounts found.	List of all user accounts created in the management console.

Table 5.7: Filters available in the action log

- **Item types and actions**

Item type	Action	Item
License Agreement	Accept	Version number of the accepted EULA.
Account	Update console	From Initial version to Target version.
	Cancel console update	From Initial version to Target version.
Threat	Allow	Name of the threat the action was performed on.
	Stop allowing	Name of the threat the action was performed on.
Information search	Launch	Name of the search the action was performed on.
	Delete	Name of the search the action was performed on.
	Cancel	Name of the search the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
Settings - Remote control	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Network settings	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Per-computer settings	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Workstations and servers	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Android devices	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Patch management	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Encryption	Create	Name of the settings the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Authorized software	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - VDI environments	Edit	Name of the settings the action was performed on
Device	Edit name	Name of the device the action was performed on
Scheduled send	Create	Name of the scheduled send the action was performed on.
	Edit	Name of the scheduled send the action was performed on.
	Delete	Name of the scheduled send the action was performed on.
Computer	Delete	Name of the device the action was performed on.
	Edit name	Name of the device the action was performed on.
	Edit description	Name of the device the action was performed on.
	Change group	Name of the device the action was performed on.
	Assign "Network settings"	Name of the device the action was performed on.
	Inherit "Network settings"	Name of the device the action was performed on.
	Assign 'Per-computer settings'	Name of the device the action was performed on.
	Inherit 'Per-computer settings'	Name of the device the action was performed on.
	Assign 'Workstations and servers' settings	Name of the device the action was performed on.
	Inherit 'Workstations and servers' settings	Name of the device the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Assign 'Android devices' settings	Name of the device the action was performed on.
	Inherit 'Android devices' settings	Name of the device the action was performed on.
	Assign license	Name of the device the action was performed on.
	Unassign license	Name of the device the action was performed on.
	Restart	Name of the device the action was performed on.
	Lock	Name of the device the action was performed on.
	Wipe data	Name of the device the action was performed on.
	Snap the thief	Name of the device the action was performed on.
	Remote alarm	Name of the device the action was performed on.
	Locate	Name of the device the action was performed on.
	Designate as Panda proxy	Name of the computer the action was performed on.
	Revoke Panda proxy role	Name of the computer the action was performed on.
	Designate as cache computer	Name of the computer the action was performed on.
	Configure cache computer	Name of the computer the action was performed on.
	Revoke cache computer role	Name of the computer the action was performed on.
	Designate as discovery computer	Name of the computer the action was performed on.
	Configure discovery	Name of the computer the action was performed on.
	Revoke discovery computer role	Name of the computer the action was performed on.
	Discover now	Name of the computer the action was performed on.
	Move to Active Directory path	Name of the computer the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Uninstall	Name of the device the action was performed on.
	Reinstall agent	Name of the device the action was performed on.
	Reinstall protection	Name of the device the action was performed on
Unmanaged computer	Hide	Name of the unmanaged computer the action was performed on.
	Make visible	Name of the unmanaged computer the action was performed on.
	Delete	Name of the unmanaged computer the action was performed on.
	Edit description	Name of the unmanaged computer the action was performed on.
	Install	Name of the unmanaged computer the action was performed on.
Filter	Create	Name of the filter the action was performed on.
	Edit	Name of the filter the action was performed on.
	Delete	Name of the filter the action was performed on.
Group	Create	Name of the group the action was performed on.
	Edit	Name of the group the action was performed on.
	Delete	Name of the group the action was performed on.
	Change parent group	Name of the group the action was performed on.
	Assign "Network settings"	Name of the group the action was performed on.
	Inherit "Network settings"	Name of the group the action was performed on.
	Assign 'Per-computer settings'	Name of the group the action was performed on.
	Inherit 'Per-computer settings'	Name of the group the action was performed on.
	Assign 'Workstations and servers' settings	Name of the group the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Inherit 'Workstations and servers' settings	Name of the group the action was performed on.
	Assign 'Android devices' settings	Name of the group the action was performed on.
	Inherit 'Android devices' settings	Name of the group the action was performed on.
	Sync group	Name of the group the action was performed on.
	Move computers to their Active Directory path	Name of the group the action was performed on.
Advanced reports	Access	
List	Create	Name of the list the action was performed on.
	Edit	Name of the list the action was performed on.
	Delete	Name of the list the action was performed on.
Patch	Exclude for a specific computer	Name of the patch the action was performed on.
	Exclude for all computers	Name of the patch the action was performed on.
	Stop excluding for a specific computer	Name of the patch the action was performed on.
	Stop excluding for all computers	Name of the patch the action was performed on.
	Mark as 'Manually downloaded'	Name of the patch the action was performed on.
	Mark as 'Requires manual download'	Name of the patch the action was performed on.
Action to take when a threat is reclassified	Edit	
Email sending option	Edit	
Access permission for the Panda Security team	Edit	
Access permission for resellers	Edit	
Email sending option (reseller)	Edit	

Table 5.8: Item types and actions

Item type	Action	Item
Two-factor authentication selection	Edit	
Role	Create	Name of the role the action was performed on.
	Edit	Name of the role the action was performed on.
	Delete	Name of the role the action was performed on.
Task - Security scan	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.
Task - Patch installation	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.
User	Create	Name of the user the action was performed on.
	Edit	Name of the user the action was performed on.
	Delete	Name of the user the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Block	Name of the user the action was performed on.
	Unblock	Name of the user the action was performed on.
Task - Patch uninstallation	Create	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.

Table 5.8: Item types and actions

System events

This section lists all events that occur in Panda Endpoint Protection and are not originated by a user account, but by the system itself as a response to the actions listed in table 5.12.

- **Fields displayed in the 'System events' list**

Field	Description	Values
Date	Date and time the event took place.	Date
Event	Action taken by Panda Endpoint Protection.	Refer to table 5.12.
Type	Type of object the action was performed on.	Refer to table 5.12.
Item	Console object the action was performed on.	Refer to table 5.12.

Table 5.9: Fields in the 'System events' list

- **Fields displayed in the exported file**

Field	Description	Values
Date	Date and time the event took place.	Date
Event	Action taken by Panda Endpoint Protection.	Refer to table 5.12.
Type	Type of object the action was performed on.	Refer to table 5.12.
Item	Console object the action was performed on.	Refer to table 5.12.

Table 5.10: Fields in the 'System events' exported file

- **Filter tool**

Field	Description	Values
From	Sets the start point of the search range.	Date
To	Sets the end point of the search range.	Date

Table 5.11: Filters available in the 'System events' list

- **Item types and actions**

Item type	Action	Item
Non-persistent computer	Delete automatically	Name of the computer the action was performed on.
Computer	Register on server for the first time	Name of the computer the action was performed on.
Computer	Register on server after computer deletion	Name of the computer the action was performed on.
Computer	Register on server after agent reinstallation	Name of the computer the action was performed on.
Computer	Uninstall agent	Name of the computer the action was performed on.
Scheduled report	Disable automatically	Name of the scheduled report the action was performed on.

Table 5.12: Item types and actions

Part 3

Deployment and getting started

Chapter 6: Installing the client software

Chapter 7: Licenses

Chapter 8: Product updates and upgrades

Chapter 6

Installing the client software

The installation process deploys Panda Endpoint Protection to all computers on the organization's network. The installation package contains all the software required to enable the protection service and monitor the security status of the network. There is no need to install any other program.

Panda Endpoint Protection provides several tools to make installing the protection easier. These tools are described in the next sections.

CHAPTER CONTENT

Protection deployment overview

The installation process consists of a series of steps that will vary depending on the status of the network at the time of deploying the software and the number of computers to protect. To deploy the protection successfully it is necessary to plan the process carefully, bearing the following aspects in mind:

Identify the unprotected devices on the network

Find those computers on the network without protection installed or with a third-party security product that needs replacing or complementing with Panda Endpoint Protection. Check to see if you have purchased enough licenses.

> Panda Endpoint Protection *allows you to install the solution's software even if you don't have enough licenses for all the computers that you want to protect. Computers without a license will be shown in the management console along with their characteristics (installed software, hardware, etc.), but won't be protected against malware.*

Check if the minimum requirements for the target platform are met

The minimum requirements for each operating system are described in section "**Operation system and network requirements**".

Select the installation procedure

The installation procedure will depend on the total number of Windows computers to protect, the workstations and servers with a Panda agent already installed, and the company's network architecture. Four options are available:

- Centralized distribution tool.
- Manual installation using the **Send URL by email** option.
- Placing an installer in a shared folder accessible to all users on the network.
- Remote installation from the management console.

Uninstall competitors' products and restart computers

The Panda Endpoint Protection protection services work without you having to restart your computers if you don'thave any previously-installed antivirus programs.

> *Some older versions of Citrix may require a computer restart or there may be a micro-interruption of the connection.*

To install Panda Endpoint Protection on a computer that already has a third-party security solution installed, choose between installing it without removing the other protection or uninstalling the other security solution and working exclusively with Panda Endpoint Protection. Assign your computers a **Workstations and servers** settings profile with the **Uninstall other security products** option enabled based on your needs. While looking for updates, Panda Endpoint Protection checks its assigned settings once a day. Refer to the following article **https://www.pandasecurity.com/es/support/**

card?id=50021 for a list of the third-party security products that Panda Endpoint Protection uninstalls automatically.

To finish uninstalling a third-party antivirus it may be necessary to restart the computer.

The default behavior will vary depending on the Panda Endpoint Protection version that you want to install:

- **Trial versions**

By default, trial versions of Panda Endpoint Protection can be installed without removing any other pre-existing third-party solution.

- **Commercial versions**

By default, it is not possible to install a commercial version of Panda Endpoint Protection on a computer with a solution from another vendor. If Panda Endpoint Protection has the uninstaller to uninstall the other vendor's product, it will uninstall it and then install Panda Endpoint Protection. Otherwise, the installation process will stop.

This behavior can be changed for both trial and commercial versions by assigning a **Workstation and servers** settings profile that has the **Uninstall other security products** option disabled.

*Refer to "**Uninstall other security products**" on page 210 for more information on how to define this behavior. Refer to "**Manual and automatic assignment of settings**" on page 184 for more information on how to assign settings to computers.*

- **Panda Security antivirus products**

If the target computer is already protected with Panda Endpoint Protection, Panda Endpoint Protection Plus or Panda Fusion, the solution will automatically uninstall the communications agent to install the Panda agent, and then will check to see if a protection upgrade is required. If it is required, the computer will be restarted.

Table 6.1 summarizes the necessary conditions for a computer restart.

Previous product	Panda Endpoint Protection	Restart
None	Trial or commercial version	NO
Panda Endpoint Protection Legacy, Panda Endpoint Protection Plus Legacy	Commercial version	LIKELY (only if a protection upgrade is required)

Table 6.1: Probability of a restart when installing a new security product

Previous product	Panda Endpoint Protection	Restart
Third-party antivirus	Trial	NO (by default, both products will coexist)
Third-party antivirus	Commercial version	LIKELY (a restart may be necessary to finish uninstalling the third-party product)
Citrix systems	Trial or commercial version	LIKELY (with older versions)

Table 6.1: Probability of a restart when installing a new security product

Determine the computers' default settings

In order to protect the computers on the network from the outset, Panda Endpoint Protection forces administrators to select both the target group that the computers to protect will integrate into and the network settings to apply to them. This must be selected upon generating the installer. Refer to "Local installation of the client software" for more information.

Once the software has been installed on a computer, Panda Endpoint Protection will apply to it the settings configured for the group that the computer is integrated into. If the network settings for the selected group are different from those specified when generating the installer, the installer settings will prevail.

Installation requirements

For a complete description of the necessary requirements for each platform, refer to "Hardware, software and network requirements" on page 373.

Requirements for each supported platform

- **Windows**
  - **Workstations**: Windows XP SP3 and later, Windows Vista, Windows 7, Windows 8 and later, and Windows 10.
  - **Servers**: Windows 2003 SP2 and later, Windows 2008, Windows Small Business Server 2011 and later, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server Core 2008 and later.
  - **Versions with an ARM processor**: Windows 10 Home and Pro.
  - **Free space for installation**: 650 MB.
  - **Updated root certificates** in order to use the Panda Patch Management module and establish real-time communications with the management console.

- **macOS**
  - **Operating systems**: macOS 10.10 Yosemite and later.
  - **Free space for installation**: 400 MB.
  - **Ports**: ports 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware to work.
- **Linux**
  - **64-bit operating systems**: Ubuntu 14.04 LTS and later, Fedora 23 and later, Debian 8 and later, Red Hat 6.0 and later, CentOS 6.0 and later, Linux Mint 18 and later, SUSE Linux Enterprise 11.2 and later. It does not require a graphical user interface. To manage the security software, use the `/usr/local/protection-agent/bin/pa_cmd` tool from the command line.
  - **32-bit operating systems**: Red Hat from 6.0 through 6.10 and CentOS from 6.0 through 6.10.

> *Refer to our support website* **https://www.pandasecurity.com/support/card?id=700009** *for more information about the Linux distributions and kernel versions supported by our solutions.*

  - **Free space for installation**: 100 MB.
  - **Ports**: ports 3127, 3128, 3129, and 8310 must be open for the Web malware detection feature to work. On computers with no graphical environment installed, the Web detection feature is disabled.

To install Panda Endpoint Protection on Linux platforms, the target computer must remain connected to the Internet throughout the installation process. The installation script will connect to the appropriate repositories based on the system (RPM or DEB), and the packages required to finish the installation successfully will be downloaded. Refer to section "**Installing the software on Linux platforms with no Internet connection (with no dependencies)**" for more information on how to install Panda Endpoint Protection on Linux platforms isolated from the network.

- **Android**
  - **Operating systems**: Android 5.0 and later.
  - **Free space for installation**: 10 MB (depending on the model, it is possible that the required space be larger).

Network requirements

To operate properly, Panda Endpoint Protection needs access to multiple Internet-hosted resources. Generally, it requires access to ports 80 and 443. For a complete list of all the URLs that computers with Panda Endpoint Protection installed need to access, refer to "**Access to service URLs**" on page **381**

Local installation of the client software

The process to download and install the client software on the computers on the network consists of the following steps:

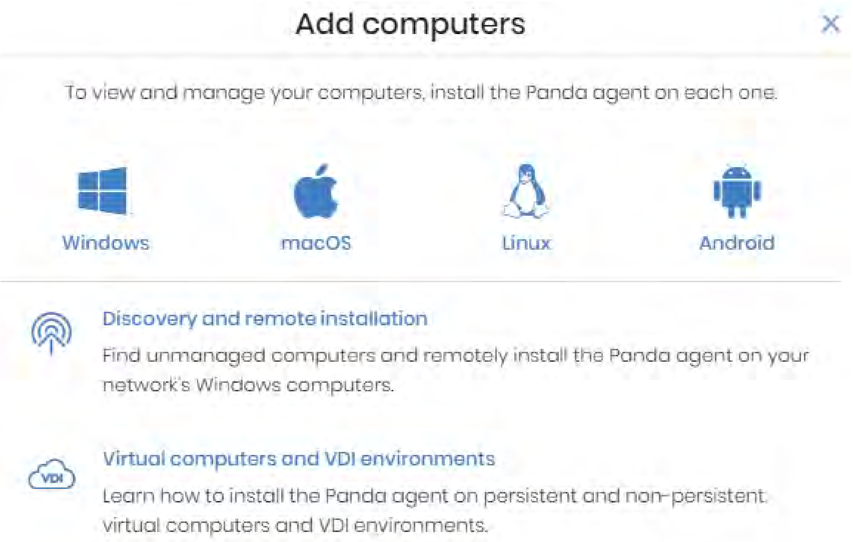
- Downloading the installation package from the Web console.
- Generating a download URL.
- Manually installing the client software.

Downloading the installation package from the Web console

*For more information on how to assign settings to computers, refer to "**Manual and automatic assignment of settings**" on page 184.*

This consists of downloading the installation package directly from the management console. To do this, follow the steps below (refer to figure 6.2 as well):

- Go to the **Computers** area, click **Add computers**, and select the platform to protect: Windows, Linux, Android or macOS. The Windows version includes the installation package for x86 and ARM processors.



Add computers

To view and manage your computers, install the Panda agent on each one.

Discovery and remote installation

Find unmanaged computers and remotely install the Panda agent on your network's Windows computers.

Virtual computers and VDI environments

Learn how to install the Panda agent on persistent and non-persistent virtual computers and VDI environments.

Figure 6.1: Window for selecting a platform compatible with Panda Endpoint Protection

- Select the group that the computer will integrate into:
  - To integrate the computer into a native group, click **Add computers to this group (1)** and select a destination in the folder tree displayed.
  - To integrate the computer into an Active Directory group, click Add computers to their Active

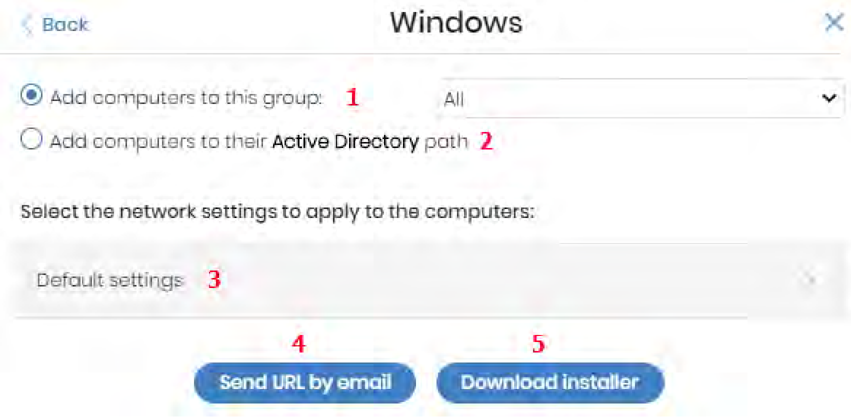
Directory path (2). For more information about the different types of groups, refer to "**Types of groups**" on page **140**.

> ⚠ *The security policies assigned to a computer depend on the group it belongs to. If the administrator of the company's Active Directory moves a computer from one organizational unit to another, that change will be replicated to the Panda Endpoint Protection console as a group change. Consequently, the security policies assigned to that computer might also change without the administrator of the Web management console noticing.*

- To integrate the computer into one group or another based on its IP address, click the option **Select the group based on the computer's IP**. Then, select the group from which a destination will be determined based on the computer's IP address. For more information, refer to "**Integrating computers based on their IP address**".

Next, select Network settings **(3)** to be applied to the computer. For more information on how to create new Network settings, refer to "**Creating and managing settings**" on page **183**.

- If the computer is to be integrated into a native group, it will automatically inherit the settings of the folder where it will reside.
- However, if you choose to integrate it into an Active Directory group, you'll have to manually select the Network settings from those displayed in the drop-down menu. If the automatic selection does not meet your needs, click the drop-down menu and select one of the available options.



● Add computers to this group: All

○ Add computers to their Active Directory path

Select the network settings to apply to the computers:

Default settings

Figure 6.2: Configuring the download package

- Finally, click **Download installer (5)** to download the appropriate installation package. The installer displays a wizard that will guide you through the steps to install the software.

Integrating computers based on their IP address

When creating a computer group, Panda Endpoint Protection lets you specify a series of individual IP addresses and IP address ranges that will determine which computers will be added to the group when installing the protection on them. Refer to "**Creating and organizing groups**" on page **141** for more information on how to create groups.

The purpose of this feature is to save time for administrators by automatically organizing newly integrated computers into groups. Panda Endpoint Protection takes the following steps to integrate a new computer into the service:

- If the option you select is **Select the group based on the computer's IP**, Panda Endpoint Protection will perform an in-depth search to retrieve the IPs associated with the group specified in the field **Select the group from which the computers will be added** and all its child groups.
- If a single matching IP address is found, the computer will be moved to the relevant group.
- However, if there are multiple IP groups that match the computer's IP address, the group that is deepest in the tree will be selected. If there are multiple groups at the same level with IP addresses that match the computer's IP address, the last one will be selected.
- If no matches are found, the computer will be moved to the group specified in the field **Select the group from which the computers will be added**. If that group does not exist at the time the computer is integrated, it will be moved to the All group.

Once a computer has been placed in a group, changing its IP address won't cause the computer to be automatically moved to another group. Similarly, changing the IP addresses assigned to a group won't cause the computers in the group to be automatically reorganized.

Generating a download URL

This option allows you to create a download URL and send it to the targeted users to launch the installation manually from their computers.

To generate a download URL, follow the steps described in "**Downloading the installation package from the Web console**" and click the **Send URL by email (4)** button.

The targeted users will automatically receive an email with the download link for their operating system. Clicking the link will download the installer.

Manually installing the client software

Admin permissions are required to install the Panda Endpoint Protection *software on users' computers.*

Installing the software on Windows x86 and ARM platforms

To run the downloaded installer, double-click its icon and follow the instructions in the installation wizard. A progress window will appear during the installation process. In the case of Windows computers, if the number of free licenses is not enough to assign a license to the target computer, a warning will be displayed to the administrator. Regardless of this, the computer will be integrated into the service despite not being protected if there aren't any free licenses.

The installer is compatible with platforms running both an x86 or ARM microprocessor. Refer to “Installation requirements”.

Once the process is complete, the product will verify that it has the latest version of the signature file and the protection engine. If not, it will update automatically.

Installing the software on Linux platforms with an Internet connection

Installing the product on the target computer requires admin permissions. Also, the downloaded package must have execute permissions. When running the installation program, it will search the target computer for the libraries it needs. If there are libraries it cannot find, it will automatically download them from the Internet.

Open a terminal in the folder where the downloaded package is located and run the following commands:

```
$ sudo chmod +x “/download path/Panda Endpoint Agent.run”
$ sudo “/download path/Panda Endpoint Agent.run”
```

To specify a list of proxies, add the following parameter: --proxy=<proxy-list>, where <proxy-list> is a list of proxy servers separated by blank spaces. Specify the user name and password of each proxy server in the following format:

```
<http|https>://<user1>:<pass1>@<host1>:<port1>
```

To verify that the AgentSvc process is running, use the following command:

```
$ ps ax | grep Agent Svc
```

Make sure the following installation directories have been created:

```
/usr/local/managemnt-agent/*
```

Installing the software on Linux platforms with no Internet connection (with no dependencies)

With workstations and servers with no Internet access (direct or through a Panda or corporate proxy), you can install the security software using the libraries included in the Panda Endpoint Protection distribution package. This installation method is only recommended when the target computer is truly isolated from the Internet, because if security failures are detected in the third-party libraries included in the installation package, they will not be automatically updated.

The installer with no dependencies is compatible with the following distributions:

- Red Hat 6, 7, 8.
- CentOS 6, 7, 8.
- SUSE Linux Enterprise from 11.2 through 15.2.

The full installer is compatible with the following Linux agent and protection versions:

- Protection version: 3.00.00.0050 and later
- Agent version: 1.10.06.0050 and later

If you try to install the solution with no dependencies on an unsupported distribution, the installation process will fail. You can only follow this installation method if you install the solution on a computer that does not have a previous version of the security software installed. Otherwise, the previous repository settings are kept.

To install the Panda Endpoint Protection agent, open a terminal in the folder where the downloaded package is located and run the following commands:

```
$ sudo chmod +x "/Ruta descarga/Panda Endpoint Agent.run"
$ sudo "/RutaDescarga/Panda Endpoint Agent.run --no-deps"
```

Installing the software on MacOS platforms

To install the product on the target computer, follow the steps below:

- Save the installer to the computer and double-click the .dmg file.
- Run the .pkg package.

To make sure the agent is installed, run the following command to verify if the AgenSvc process is running:

```
$ ps ax | grep Agent Svc
```

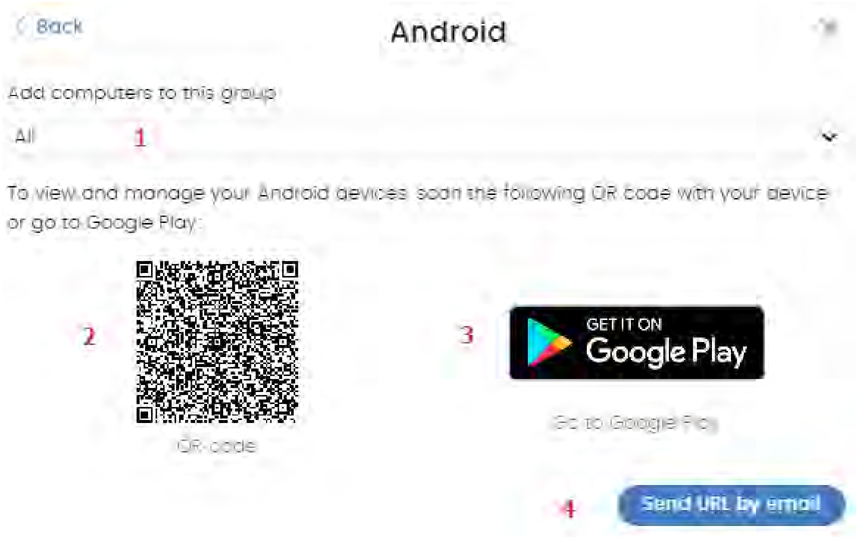
You can also check to see if the following installation directories have been created:

`/Applications/Management-gent.app/Contents` `/*/Library/ApplicationSupport/ManagementAgent/`

To install the product agent on devices with macOS Catalina installed, specific permissions need to be assigned to the protection: Refer to **https://www.pandasecurity.com/en/support/card?id=700079** *for more information.*

Installing the software on Android platforms

Click **Add computers** in the Computers menu and select the Android icon. A window will be displayed with the options below:



Add computers to this group: All

To view and manage your Android devices scan the following QR code with your device or go to Google Play:

Figure 6.3: Installation on Android devices

- **Add computers to this group (1)**: this lets you specify the group within the folder tree to which the device will be added once the Panda Endpoint Protection software is installed.
- **QR Code (2)**: the QR code that contains the link to download the software from Google Play.
- **Go to Google Play (3)**: a direct link to download the Panda Endpoint Protection software from Google Play.
- **Send URL by email (4)**: this option creates an email message with the download link ready to send to the user of the device that you want to protect with Panda Endpoint Protection.

To install the software on the user's device, follow the steps below:

- Select the group within the folder tree to which the device will be added. The QR code will be updated automatically.
- Download the Android app following one of the three methods described below:
  - **Via QR code**: click the QR code to expand it. Aim the device camera at the screen, and scan the code using a QR code reader. The device screen will display a Google Play URL to download the app. Click the URL.

> *QR Barcode Scanner and Barcode Scanner are two free QR code readers available on Google Play.*

  - **Via email**: click the **Send URL by email** link to generate an email with the link for the user. Clicking the link will allow them to download the app from Google Play.
  - **Via the management console**: if you have accessed the management console from the device,

click the **Go to Google Play** link and download the app.

- Once the app is installed, the user will be prompted to accept the granting of admin permissions for the app. Depending on the version of Android (6.0 and later), these permissions will be presented progressively as required or, on the contrary, a single window will be displayed the first time the app is run, requesting all the necessary permissions just once.

Once the process is complete, the device will appear in the group selected in the folder tree.

Remote installation of the client software

All products based on Aether Platform provide tools to find the unprotected workstations and servers on the network, and launch a remote, unattended installation from the management console.

Remote installation is only compatible with Windows platforms.

Operation system and network requirements

For you to be able to install Panda Endpoint Protection remotely, the target computers must meet the following requirements:

- UDP ports 21226 and 137 must be accessible to the System process.
- TCP port 445 must be accessible to the System process.
- NetBIOS over TCP must be enabled.
- DNS queries must be allowed.
- Access to the `Admin$` administrative share must be allowed. This feature must be explicitly enabled on Windows 'Home' editions.
- You must have domain administrator credentials or credentials for the local admin account created by default when installing the operating system.
- Windows Remote Management must be enabled.

To make sure your network computers meet these requirements without needing to manually add rules in the Windows firewall, select Turn on network discovery and Turn on file and printer sharing in Network and Sharing Center, Advanced sharing settings.

Additionally, please note that in order for a network computer with Panda Endpoint Protection installed to be able to discover unmanaged computers on the network, these must meet the following requirements:

- They must not have been hidden by the administrator.
- They must not be currently managed by Panda Endpoint Protection on Aether Platform.

- They must be located on the same subnet segment as the discovery computer.

Hidden computers

To avoid generating too long lists of discovered computers that may contain devices not eligible for Panda Endpoint Protection installation, it is possible to hide computers selectively by following the steps below:

- From the **Unmanaged computers discovered** list, click the **Discovered** button in the top right-hand corner of the screen.
- Select the checkboxes that correspond to the computers that you want to hide.
- To hide multiple computers simultaneously, click the general context menu and select **Hide and do not discover again**.
- To hide a single computer, click the computer's context menu and select **Hide and do not discover again**.

Computer discovery

Computers are discovered by means of another computer with the role of 'Discovery computer'. All computers that meet the necessary requirements will appear on the **Unmanaged computers discovered** list, regardless of whether their operating system or device type supports the installation of Panda Endpoint Protection.

The first Windows computer that is integrated into Panda Endpoint Protection will be automatically designated as discovery computer.

Assigning the role of 'Discovery computer' to a computer on your network

- Make sure the computer that you want to designate as discovery computer has Panda Endpoint Protection installed.
- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Discovery** tab.
- Click the **Add discovery computer** button, and select from the list the computer(s) that you want to perform discovery tasks across the network.

Once you have designated a computer on your network as discovery computer, it will be displayed on the list of discovery computers (top menu **Settings**, side menu **Network services**, **Discovery** tab). The following information is displayed for each discovery computer:

Field	Description
Computer name	Name of the discovery computer.
IP address	IP address of the discovery computer.

Table 6.2: Information displayed for each discovery computer

Field	Description
Discovery task settings	Settings of the automatic computer discovery task, if there is one.
Last checked	Time and date when the last discovery task was launched.
The computer is turned off or offline	Panda Endpoint Protection cannot connect to the discovery computer.
Configure	Lets you define the task scope and type (automatic or manual). If the task is automatic, it will be performed once a day.

Table 6.2: Information displayed for each discovery computer

Defining the discovery scope

> *The scope settings only affect the subnet where the discovery computer resides. To search for unmanaged devices across all subnets on the network, designate as discovery computer at least one computer per subnet.*

Follow the steps below to limit the scope of a discovery task:

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Discovery** tab. Select a discovery computer and click **Configure**.
- Select one of the following options in the **Discovery scope** section:
  - **Search across the entire network**: the discovery computer will use the network mask configured on the interface to scan its subnet for unmanaged computers.
  - **Search only in the following IP address ranges**: you can enter several IP ranges separated by commas. The IP ranges must have a "-" (dash or hyphen) in the middle. You can only specify private IP address ranges.
  - **Search for computers in the following domains**: specify the Windows domains that the discovery computer will search in, separated by commas.

Scheduling computer discovery tasks

You can schedule computer discovery tasks so that they are automatically launched by discovery computers at regular intervals.

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Discovery** tab. Select a discovery computer and click Configure.
- From the **Run** automatically drop-down menu, select **Every day**.
- Select the start time of the scheduled task.
- Select whether to use the discovery computer's local time or the Panda Endpoint Protection server time as reference.
- Click **OK**. The discovery computer will show a summary of the scheduled task in its description.

Manually running discovery tasks

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Discovery tab**. Select a discovery computer and click **Configure**.
- From the **Run** automatically drop-down menu, select **No**.
- Click **OK**. The computer will display a **Check now** link which you can use to run a discovery task on demand.

Viewing discovered computers

There are two ways to access the **Unmanaged computers discovered** list:

- From the **Protection status** widget: go to the **Status** menu at the top of the console. There you'll see the **Protection status** widget. At the bottom of the widget you'll see the following text: **XX computers have been discovered that are not being managed by** Panda Endpoint Protection.
- From **My lists**: go to the **Status** menu at the top of the console. Go to **My lists** on the left-hand side menu and click the **Add** link. From the drop-down menu, select the **Unmanaged computers discovered** list.

- **'Unmanaged computers discovered' list**

This list displays those computers discovered on the network that don't have Panda Endpoint Protection installed, and those computers where the protection is not working properly despite being correctly installed

Field	Description	Values
Computer	Name of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	• — **Unmanaged**: the computer is eligible for installation, but the installation process has not started yet. • ☁ **Installing**: the installation process is in progress. • ☁ **Installation error**: displays a message specifying the type of error. Refer to table "Computer notifications section (2)" on page 161 for a description of all possible errors. If the cause of the error is unknown, the associated error code will be displayed.
IP address	The computer's primary IP address.	Character string

Table 6.3: Fields in the 'Unmanaged computers discovered' list

Field	Description	Values
NIC manufacturer	Manufacturer of the discovery computer's network interface card.	Character string
Last discovery computer	Name of the last computer that discovered the unmanaged workstation or server.	Character string
Last seen	Date when the computer was last discovered.	Date

Table 6.3: Fields in the 'Unmanaged computers discovered' list

If the **Status** field shows the text **Installation error,** and the cause of the error is known, a text string will be added with a description of the error. Refer to "**Computer notifications section (2)**" on page 161 for a list of the installation errors reported by Panda Endpoint Protection.

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Name	Name of the discovered computer.	Character string
IP address	The computer's primary IP address.	Character string
MAC address	The computer's physical address.	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card.	Character string
Domain	Windows domain the computer belongs to.	Character string
First seen	Date when the computer was first discovered.	Character string
First seen by	Name of the discovery computer that first saw the workstation/server.	Character string
Last seen	Date when the computer was last discovered.	Date
Last seen by	Name of the discovery computer that last saw the workstation/server	Character string
Description	Description of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	• **Unmanaged**: the computer is eligible for installation, but the installation process has not started yet.

Table 6.4: Fields in the 'Unmanaged computers list' exported file

Field	Description	Values
		- **Installing**: the installation process is in progress. - **Installation error**: message specifying the type of error. Refer to table "Computer notifications section (2)" on page 161 for a description of all possible errors.
Error	Error description.	For more information, refer to table "Computer notifications section (2)" on page 161.
Installation error date	Date and time when the error took place.	Date

Table 6.4: Fields in the 'Unmanaged computers list' exported file

- **Search tool**

Field	Description	Values
Search	Search by computer name, IP address, NIC manufacturer or discovery computer.	Character string
Status	Panda Endpoint Protection installation status.	- **Unmanaged**: the computer is eligible for installation, but the installation process has not started yet. - **Installing**: the installation process is in progress. - **Installation error**: message specifying the type of error.
Last seen	Date when the computer was last discovered.	- Last 24 hours - Last 7 days - Last month

Table 6.5: Filters available in the 'Unmanaged computers discovered' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "Computer details" on page 159 for more information.

Deleted computers

Panda Endpoint Protection doesn't remove from the **Unmanaged computers discovered** list those computers that are no longer accessible because they have been withdrawn from the network due to inspection, malfunction, theft or for any other reason.

To manually remove those computers that won't be accessible again follow the steps below:

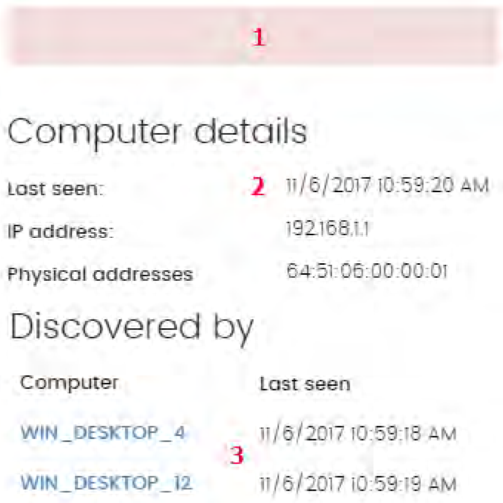
- From the **Unmanaged computers discovered** list, select **Discovered** or **Hidden** depending on the status of the computers you want to delete.
- Select the checkboxes next to the computers to delete.
  - To delete multiple computers simultaneously, click the general context menu and select **Delete**.
  - To delete a single computer, click the computer's context menu and select **Delete**.

> *Any unmanaged computer that is deleted from the console without uninstalling the* Panda Endpoint Protection *software and without being physically withdrawn from the network will appear again in the next discovery task. Delete only those computers that you are sure will never be accessible again.*

Discovered computer details

From the **Unmanaged computers discovered** list, click a computer to view its details window. This window is divided into 3 sections:

- **Computer alerts (1)**: shows installation problems.
- **Computer details (2)**: gives a summary of the computer's hardware, software, and security settings.
- **Last discovery computer (3)**: shows the discovery computer that last saw the computer.



Computer details

Last seen: 11/6/2017 10:59:20 AM

IP address: 192.168.1.1

Physical addresses 64:51:06:00:00:01

Discovered by

Computer	Last seen
WIN_DESKTOP_4	11/6/2017 10:59:18 AM
WIN_DESKTOP_12	11/6/2017 10:59:19 AM

Figure 6.4: Discovered computer details

Computer alerts

Status	Type	Solution
Error installing the Panda agent	This message specifies the reason why the agent installation failed.	
	Wrong credentials	Launch the installation again using credentials with sufficient permissions to perform the installation.
	Unable to connect to the computer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to download the agent installer	Make sure the computer is turned on and meets the remote installation requirements.

Table 6.6: 'Computer alerts' section

Status	Type	Solution
	Unable to copy the agent installer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to install the agent	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to register the agent	Make sure the computer is turned on and meets the remote installation requirements.
Error installing the Panda Endpoint Protection protection	This message indicates the reason for the protection installation failure.	
	Insufficient disk space to perform the installation	Refer to "**Hardware requirements**" on page 377 for more information about the necessary requirements to install Panda Endpoint Protection.
	Windows Installer is not operational	Make sure the Windows Installer service is running. Stop and start the service.
	Removal of the third-party protection installed was canceled by the user	Accept the removal of the third-party antivirus solution found.
	Another installation is in progress	Wait for the current installation to finish.
	Error automatically uninstalling the third-party protection installed	Refer to **Supported uninstallers** for a complete list of the third-party solutions that Panda Security can uninstall.
	There is no uninstaller available to remove the third-party protection installed	Contact tech support to obtain the relevant uninstaller.
Installing the Panda agent	Once the installation process is complete, the computer will no longer appear on the list of unmanaged computers discovered.	
Unmanaged computer	The computer doesn't have the Panda agent installed. Make sure the computer is compatible with Panda Endpoint Protection and meets the requirements specified in chapter "**Hardware, software and network requirements**" on page 373.	

Table 6.6: 'Computer alerts' section

Computer details

Field	Description
Computer name	Name of the discovered computer.
Description	Lets you assign a description to the computer, even though it is currently not managed.

Table 6.7: 'Computer details' section

Field	Description
First seen	Date/time when the computer was first discovered.
Last seen	Date/time when the computer was last discovered.
IP address	IP address of the computer's network interface card.
Physical addresses (MAC)	Physical address of the computer's network interface card.
Domain	Windows domain the computer belongs to.
NIC manufacturer	Manufacturer of the computer's network interface card.

Table 6.7: 'Computer details' section

Last discovery computer

Field	Description
Computer	Name of the discovery computer that last found the unmanaged computer.
Last seen	Date/time when the computer was last discovered.

Table 6.8: 'Last discovery computer' section

Remote installation of the software on discovered computers

To remotely install the Panda Endpoint Protection software on one or more unmanaged computers discovered follow the steps below:

From the 'Unmanaged computers discovered' list

- Go to the **Unmanaged computers discovered** list.
  - Click the **Status** menu at the top of the console and go to the **My lists** section on the left-hand side menu. Click the **Add** link. From the drop-down menu, select the **Unmanaged computers discovered** list.
  - Go to the **Status** menu at the top of the console. In the **Protection status** widget, click the link **XX computers have been discovered that are not being managed by** Panda Endpoint Protection.
  - Go to the **Computers** menu at the top of the console. Click **Add computers** and select **Discovery and remote installation**. A wizard will be displayed. Click the link **View unmanaged computers discovered**.
- From the **Unmanaged computers discovered** list, select **Discovered** or **Hidden** depending on the status of the relevant computers.
- Select the checkboxes next to the computers that you want to install the software on.
  - To install it on multiple computers simultaneously, click the general context menu and select **Install Panda agent**.
  - To install it on a single computer, click the computer's context menu and then click **Install Panda**

agent.

- Configure the installation by following the steps described in section "**Downloading the installation package from the Web console**".
- You can enter one or multiple installation credentials. Use the local administrator credentials for the target computer(s) or domain administrator credentials in order to install the software successfully.

From the Computer details window

Click a discovered computer to display its details window. At the top of the screen you'll see the button **Install Panda agent**. Follow the steps described in section "**Downloading the installation package from the Web console**".

Installation with centralized tools

On medium-sized and large networks it is advisable to install the client software for Windows computers centrally using third-party tools.

Using the command line to install the installation package

You can automate the installation and integration of the Panda agent into the management console by using the following command-line parameters:

- **GROUPPATH="group1\group2"**: path in the group tree where the computer will reside. The 'All' root node is not specified. If the group doesn't exist, the computer will be integrated into the 'All' root node.
- **PRX_SERVER**: name or IP address of the corporate proxy server.
- **PRX_PORT**: port of the corporate proxy server.
- **PRX_USER**: user of the corporate proxy server.
- **PRX_PASS**: password of the corporate proxy server.

Below is an example of how to install the agent using command-line parameters:

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="London\AccountingDept"
PRX_SERVER="ProxyCorporative" PRX_PORT="3128" PRX_USER="admin" PRX_PASS="panda"
```

Deploying the agent from Panda Patch Management

Panda Patch Management customers can deploy Panda Endpoint Protection for Windows, macOS and Linux automatically using the following components:

- Panda Endpoint Protection on Aether Installer for Windows
- Panda Endpoint Protection on Aether Installer for macOS
- Panda Endpoint Protection on Aether Installer for Linux

All three components are available for free from the Comstore for all Panda Systems Management users.

Component features and requirements

These components doesn't have any specific requirements besides those indicated for Panda Systems Management and Panda Endpoint Protection.

Component size:

- Panda Endpoint Protection Installer for Windows: 1.5 MB
- Panda Endpoint Protection on Aether Installer for macOS: 3 KB
- Panda Endpoint Protection on Aether Installer for Linux: 3 KB

Once deployed and run, the component downloads the Panda Endpoint Protection installer. Depending on the version, the installer will take up between 6 to 8 MB on each computer.

Deploying the agent with Microsoft Active Directory

Limitations of Microsoft Active Directory when deploying the security software

- This deployment method enables you to install the security software on a computer for the first time. It does not support updates of previously installed security software.
- The computer where the GPO (Group Policy Object) is defined cannot have the security software installed. Otherwise, the following error message is shown during the process: "The process of adding failed. The deployment information could not be retrieved from the package. Make sure the package is correct".

Steps to prepare an installation GPO

Below we have listed the steps to take to deploy the Panda Endpoint Protection software to Windows computers on a network with Active Directory using GPO (Group Policy Object).

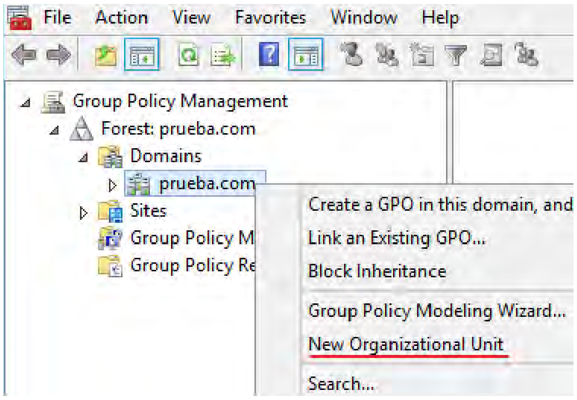


Figure 6.5: New Organizational Unit

1. Download and share the Panda Endpoint Protection installation package.

• Place the Panda Endpoint Protection installer in a shared folder accessible to all the computers that are to receive the software.

2. Create a new OU (Organizational Unit) named "Aether deployment".

• Open the mmc and add the Group Policy Management snap-in.

• Right-click the domain node, and click New and Organizational Unit to create a new Organizational Unit named "Aether deployment".

3. Create a new GPO with the installation package

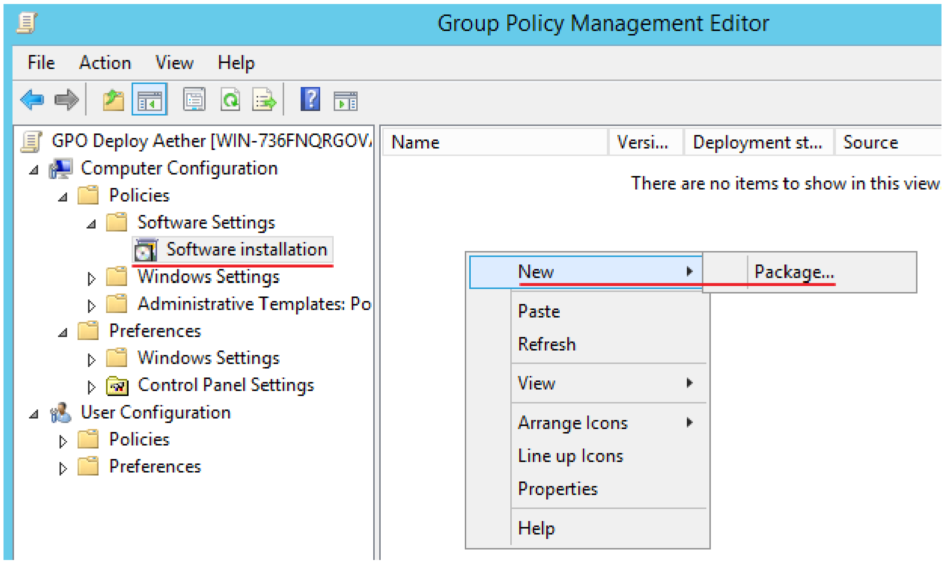


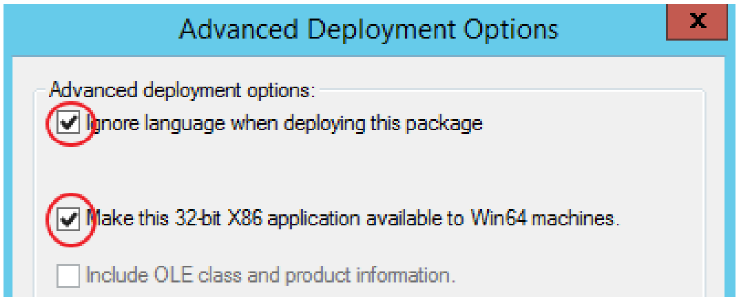
Figure 6.6: New installation package

- Right-click the newly created Organizational Unit and select the option Create a GPO in this domain. Name the GPO (in this case, "Aether deployment GPO").
- Edit the newly created GPO by adding the installation package that contains the Panda Endpoint Protection software. To do this, click Computer configuration, Policies, Software Settings, Software installation.

  • Right-click Software installation, and click New, Package.

  • Add the Panda Endpoint Protection .msi installation package.

4. Edit the package properties



Advanced deployment options:

☑ Ignore language when deploying this package

☑ Make this 32-bit X86 application available to Win64 machines.

□ Include OLE class and product information.

Figure 6.7: Configuring the deployment options

- Right-click the package you have added and select Properties, Deployment tab, Advanced. Select the following checkboxes: Ignore language when deploying this package and Make this 32-bit X86 application available to Win64 machines.
- Add all network computers that will receive the agent to the "Aether deployment" OU.

Installation using gold image generation

In large networks made up of many homogeneous computers, it is possible to automate the process of installing the operating system and the accompanying software by creating a gold image (also known as master image, base image or clone image). This image is then deployed to all computers on the network, eliminating most of the manual work involved in setting up computers from scratch.

To generate this image, install, on a computer on your network, an up-to-date operating system with all the software that users may need, including security tools.

Gold images and Panda Endpoint Protection

Every computer where Panda Endpoint Protection is installed is assigned a unique ID. This ID is used by Panda Security to identify the computer in the management console. Therefore, if a gold image is generated from a computer and then copied to other systems, every computer that receives it will inherit the same Panda Endpoint Protection ID and, consequently, the console will display only one computer. This can be avoided by using a program that deletes that ID. This program is called `Panda Aether Tool` and can be downloaded from the following URL on Panda Security's support website:

https://www.pandasecurity.com/uk/support/card?id=700050

This page will also provide you with specific instructions on how to prepare and install a gold image in persistent and non-persistent VDI environments.

Non-persistent environments and Panda Endpoint Protection

In non-persistent VDI environments, some virtual hardware parameters such as the MAC address of network interface cards may change with each restart. For this reason, these devices' hardware cannot be used for identification purposes or to assign licenses to them as the system would consider a device as new with each restart and assign a new license to it. Additionally, the storage system of non-persistent VDI computers is emptied with each restart, deleting the Panda Endpoint Protection ID assigned to it.

Creating a gold image for persistent VDI environments

In a persistent VDI environment, the information stored on a computer's hard disk persists between restarts. Therefore, creating a gold image only requires you to configure the updates of the Panda Endpoint Protection protection.

Once you have installed on one of your computers an updated version of the operating system and all programs that users may need, follow these steps:

- Install the Panda Endpoint Protection client software using the steps described in section "**Local installation of the client software**".
- Make sure the computer is connected to the Internet and assign it a settings profile with updates of the Panda Endpoint Protection protection and knowledge enabled. Refer to "**Managing settings**" on page **175** and chapter "**Product updates and upgrades**" on page **123** for more information on how to create and assign settings to computers respectively.
- Run `Panda Aether Tool` and click the **Start cache scan** button to scan the computer and preload the Panda Endpoint Protection goodware cache.
- Click the **Unregister device** button to delete the computer ID. Make sure the **Is a gold image** checkbox is cleared.
- Turn off the computer and generate the image with the virtual environment management software that you use.

Creating a gold image for non-persistent VDI environments

In the case of a non-persistent VDI environment, you'll need two Panda Endpoint Protection update settings profiles: one to update the gold image when preparing it and for maintenance purposes, and one to disable updates when running the gold image as it doesn't make sense to use bandwidth to update Panda Endpoint Protection if the computer's storage system is going to revert to its original state with each restart.

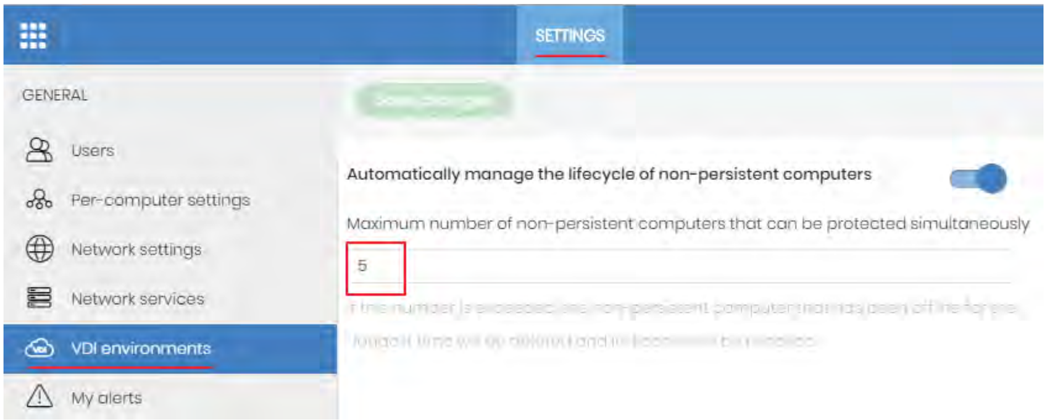
Preparing the gold image

Once you have installed on one of your computers an updated version of the operating system and all programs that users may need, follow these steps:

- Install the Panda Endpoint Protection client software using the steps described in section "**Local installation of the client software**".
- .Make sure the computer is connected to the Internet and assign it a settings profile with updates of the Panda Endpoint Protection protection and knowledge enabled. Refer to "**Managing settings**" on

page 175 and chapter “Product updates and upgrades” on page 123 for more information on how to create and assign settings to computers respectively.

- Run `Panda Aether Tool` and click the **Start cache scan** button to scan the computer and preload the Panda Endpoint Protection goodware cache.
- Click the **Unregister device** button to delete the computer ID. Make sure the **Is a gold image** checkbox is selected.
- Assign the computer a settings profile that disables updates of the Panda Endpoint Protection protection and knowledge.
- Disable the Panda Endpoint Agent service from the Windows service dashboard to prevent it from starting automatically when using the gold image on virtual instances.
- Turn off the computer and generate the image with the virtual environment management software that you use.
- Go to the **Settings** menu at the top of the console, click **VDI environments** from the left-hand side panel and configure the maximum number of computers that can be active simultaneously. This will allow automatic management of the licenses used by these computers.



Automatically manage the lifecycle of non-persistent computers

Maximum number of non-persistent computers that can be protected simultaneously

5

Figure 6.8: Configuring the number of licenses assigned to non-persistent VDI computers

Running Panda Endpoint Protection in a non-persistent VDI environment

For Panda Endpoint Protection to run properly, you need to change the startup type of the Panda agent service, which was previously disabled in the gold image. To do this, follow the steps below:

- Use the GPO management tools on a domain-connected physical computer and create a GPO to change the startup type of the Panda agent service.

For more information, refer to the following URL: https://www.microsoft.com/en-US/download/details.aspx?id=21895.

- In the GPO settings, browse to the following path: Computer Configuration, Policies, Windows Settings, Security Settings, System Services, Panda Endpoint Agent.
- The service will be disabled. Change the setting to Automatic. The service will start automatically on

next boot and will be integrated in the console.

Maintaining the gold image in a non-persistent VDI environment

Since the settings VDI computers receive have updates disabled, it is necessary to update the gold image manually at least once a month for it to receive the latest version of the protection and the signature file. To do that, follow the steps below on the computer with the gold image installed:

- Enable the Panda Endpoint Agent service.
- Make sure the computer is connected to the Internet, and assign it a settings profile with updates of the Panda Endpoint Protection protection and knowledge enabled.
- Run `Panda Aether Tool` and click the **Start cache scan** button to scan the computer and preload the Panda Endpoint Protection goodware cache.
- Click the **Unregister device** button to delete the computer ID. Make sure the **Is a gold image** checkbox is selected.
- Assign the computer a settings profile that disables updates of the Panda Endpoint Protection protection and knowledge.
- Disable the Panda Endpoint Agent service to prevent it from starting automatically when using the gold image on virtual instances.
- Turn off the computer and generate the image with the virtual environment management software that you use.
- In the VDI environment, replace the previous image with the new one.
- Repeat this maintenance process at least once a month.

Viewing non-persistent computers

Panda Endpoint Protection uses the FQDN to identify those computers whose ID has been deleted using the `Panda Aether Tool` program and are marked as gold image. To get a list of non-persistent VDI computers, follow the steps below:

- Go to the **Settings** menu at the top of the console, click **VDI environments** from the left-hand side panel and then click the **Show non-persistent computers** link.
- The **Computers** list will be displayed, with the **Non-persistent computers** filter applied.

Installation process on Windows computers

Once installed, the agent performs a series of checks automatically:

1. **Agent integration into Aether**: the agent sends information from the computer where it is installed to Panda's cloud for integration into the platform.
2. **Protection module installer download**: the agent downloads and installs the protection module.
3. **Signature file download**: the agent downloads the known malware signature file.

4. **Settings download**: the agent downloads the default and administrator-created settings to apply to the computer.

5. **Connectivity check to Panda's cloud**: if connectivity fails, the error type is reported in the following places:

   - **The agent installation console**: an error message is displayed along with the URLs that could not be accessed. Click the Retry button to perform a new check.
   - **The Windows Event Viewer (Event log)**: an error message is displayed along with the URLs that could not be accessed.
   - **The Web console**: an error message is displayed along with the URLs that could not be accessed.

Checking deployment

There are three complementary ways in which you can check the result of the Panda Endpoint Protection software deployment operation across the managed network:

- Using the **Protection status** widget. Refer to "Protection status" on page 300.
- Using the **Computer protection status** list. Refer to "Computer protection status" on page 307.
- Using the Event Viewer Application log on Windows computers.

Windows Event Viewer

The Application log in the Event Viewer provides extended information about the result of the installation of the agent on the user's computer and how it works once installed. The table below shows the information provided by Panda Endpoint Protection in each field of the Event Viewer.

Message	Level	Category	ID
The device %deviceId% was unregistered	Warning	Register (1)	101
The device %deviceId% was registered	Information	Register (1)	101
A new SiteId %SiteId% was set	Warning	Register (1)	102
Error %error%: Cannot change SiteId	Error	Register (1)	102
Error %error%: Calling %method%	Error	Register (1)	103
Error %code%: Registering device, %description%	Error	Register (1)	103
Installation success of %fullPath% with parameters %parameters%	Information	Installation (2)	201
A reboot is required after installing %fullPath% with parameters %parameters%	Warning	Installation (2)	201
Error %error%: executing %fullPath% with parameters %parameters%	Error	Installation (2)	201

Table 6.9: Agent installation result codes in the Event Viewer

Message	Level	Category	ID
Message: %Module% installer error with following data: (optional) Extended code: %code% (optional) Extended subcode: %subCode% (optional) Error description: %description% (optional) The generic uninstaller should be launched (optional) Detected AV: Name = %name%, Version = %version%	Error	Installation (2)	202
Uninstallation success of product with code %productCode% and parameters %parameters%	Information	Uninstallation (4)	401
A reboot is required after uninstalling product with code %productCode% and parameters %parameters%	Warning	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and parameters %parameters%	Error	Uninstallation (4)	401
Uninstallation of product with code %productCode% and command line %commandLine% was executed	Information	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Uninstallation (4)	401
Generic uninstaller executed: %commandLine%	Information	Uninstallation (4)	402
Error %error%: Executing generic uninstaller %commandLine%	Error	Uninstallation (4)	402
Configuration success of product with code %productCode% and command line %commandLine%	Information	Repair (3)	301
A reboot is required after configuring product with code %productCode% and command line %commandLine%	Warning	Repair (3)	301
Error %error%: Configuring product with code %productCode% and command line %commandLine%	Error	Repair (3)	301

Table 6.9: Agent installation result codes in the Event Viewer

Uninstalling the software

The Panda Endpoint Protection software can be uninstalled manually from the operating system's control panel, or remotely from the **Computers** area or from the **Computer protection status** and **Licenses** lists.

Manual uninstallation

The Panda Endpoint Protection software can be manually uninstalled by end users themselves, provided the administrator has not set an uninstallation password when configuring the security profile for the computer in question. If an uninstallation password has been set, the end user will need authorization or the necessary credentials to uninstall the protection.

Refer to "Setting up the password" on page 203 for more information on how to create or remove an agent uninstallation password.

Installing Panda Endpoint Protection actually installs multiple independent programs depending on the target platform:

- **Windows and macOS computers**: agent and protection.
- **Linux computers**: agent, protection and kernel module.
- **Android devices**: protection.

To completely uninstall Panda Endpoint Protection, all modules must be removed. If only the protection module is uninstalled, the agent will install it again after some time.

- **On Windows 8 or later:**
  - Control Panel > Programs > Uninstall a program.
  - Alternatively, type 'uninstall a program' at the Windows Start screen.
- **On Windows Vista, Windows 7, Windows Server 2003 and later:**
  - Control Panel > Programs and Features > Uninstall or change a program.
- **On Windows XP:**
  - Control Panel > Add or remove programs.
- **On macOS:**
  - Finder > Applications > Drag the icon of the protection to uninstall to the recycle bin, or run the following command `sudo sh /Applications/Protection-Agent.app/Contents/uninstall.sh`.
  - Dragging the icon to the recycle bin doesn't uninstall the agent. To remove it, you have to run the following command `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`
- **On Android devices:**
  - Go to Settings, Security > Device administrators.
  - Clear the Panda Endpoint Protection checkbox. Then, tap Disable > OK.
  - Back in the Settings window, tap Apps. Click Panda Endpoint Protection > Uninstall > OK.

- **On Linux:**

Open the command line and enter:

```
/usr/local/management-agent/repositories/pa/install -remove

/usr/local/management-agent/repositories/ma/install -remove
```

Manual uninstallation result

Once uninstalled, all data associated with the computer will disappear from the management console and its various counters (malware detected, URLs blocked, emails filtered, devices blocked, etc.). However, all that information will be retrieved as soon as you reinstall the Panda Endpoint Protection software.

Remote uninstallation

Follow these steps to remotely uninstall the Panda Endpoint Protection software from a Windows computer:

- Go the **Computers** area (or the **Licenses** or **Computer protection status** lists), and select the checkboxes of the computers whose protection you want to uninstall.
- From the action bar, click the **Delete** button. A confirmation window will be displayed.
- In the confirmation window, select the **Uninstall the Panda agent from the selected computers** checkbox to completely remove the Panda Endpoint Protection software.

Remote uninstallation is only supported on Windows platforms. On Linux and macOS platforms, the affected computer will be simply removed from the management console and all of its counters, but it will immediately reappear in the next discovery task, along with its information.

Remote reinstallation

To resolve certain situations in which the Panda Endpoint Protection software may be malfunctioning, you can reinstall it remotely from the management console, for both workstations and servers.

Software reinstallation takes place separately for the agent and for the protection module.

Remote reinstallation requirements

- The target computer must be a Windows workstation or server.
- A computer with the discovery computer role on the same network segment as the computer whose software needs reinstalling. The discovery computer must communicate with the Panda Security cloud.
- Local admin or domain admin account credentials.

Accessing the feature

This feature is accessible from any of the lists below. To access these lists, go to the Status menu at the top of the console and click the Add link from the side menu:

- "Computer protection status" on page 307.
- "Patch management status" on page 249.
- "Encryption Status" on page 289.
- "Licenses" on page 118.
- "'Hardware'" on page 153.

You can also access this feature from the Computers list accessible via the Computers top menu, by clicking any of the branches in the folder or filter tree in the side panel.

> *The Reinstall protection (requires restart) and Reinstall agent options will only show for computers supporting this feature.*

Discovering computers whose software needs reinstalling

Use the Unmanaged computers discovered list to find computers on the network whose software needs to be reinstalled. Refer to "Viewing discovered computers".

Reinstalling the software on a single computer

- Find, from the list, the computer whose software you want to reinstall.
- From the computer's context menu, click **Reinstall protection (requires restart)**⚙ or **Reinstall agent** ⚙. A window will open for you to configure the reinstallation options. Refer tos "'Reinstall protection' selection window" and "'Reinstall agent' selection window".

Reinstalling the software on multiple computers

- Use the checkboxes to select the computers whose protection or agent you want to reinstall.
- From the toolbar, click **Reinstall protection (requires restart)** ⚙ or **Reinstall agent** ⚙. A window will open for you to configure the reinstallation options. Refer tos "'Reinstall protection' selection window" and "'Reinstall agent' selection window".

'Reinstall protection' selection window

When choosing to reinstall a computer's protection, a window is displayed with the following two options:

- **Reinstall the protection immediately (requires restart)**: the computer's protection will be reinstalled in one minute. If the target computer is not available at that particular time because it is turned off or offline, the restart command will remain on the Panda Endpoint Protection server for 1 hour.

- **Delay reinstallation for a certain time**: the computer's protection will be reinstalled according to the time configured by the administrator. If the target computer is not available because it is turned off or offline, the restart command will remain on the Panda Endpoint Protection server for 7 days.

At the time the administrator starts the reinstallation process, the computer user will see a pop-up message giving them the option to restart the computer immediately or wait until the time configured by the administrator elapses. Once the waiting period expires, the protection will be uninstalled, and the computer will restart automatically in order to reinstall the protection.

If an error occurs uninstalling the protection, Panda Endpoint Protection will launch a generic uninstaller in the background in order to retry the operation and remove any traces of the previous installation. This may require an additional restart.

'Reinstall agent' selection window

- When choosing to reinstall a computer's agent, a window is displayed prompting you for the following information:
- **Discovery computer from which the agent will be reinstalled**:
  - Make sure the discovery computer is on the same network segment as the computer whose agent you want to reinstall.
  - If the discovery computer is turned off, the request will be queued until the computer becomes available again. Requests are queued for a maximum of 1 hour, after which time they are discarded.
- **Credentials for reinstalling the agent**: enter one or multiple pairs of installation credentials. Use the target computer's local or domain administrator account to complete the reinstallation successfully.

Once you have entered the aforementioned information, the discovery computer will take the following actions:

- Connect to the computer whose agent you want to reinstall.
- Uninstall the agent installed on the computer whose agent you want to reinstall.
- Download a new agent preconfigured with the customer, group, and network settings assigned to the computer. This agent will be copied to and run remotely on the computer whose agent you want to reinstall.
- If an error occurs during the process, a generic uninstaller will be launched and, if needed, a message will be displayed to the user with a countdown to an automatic restart and a button for restarting the computer immediately.

Error codes

Refer to "**Possible errors in the protection software reinstallation process**" on page **162** for a list of all possible error codes and the recommended actions to resolve them.

Chapter 7

Licenses

To protect your network computers from cyberthreats, you must purchase a number of Panda Endpoint Protection licenses equal to or greater than the number of workstations and servers to protect. Each Panda Endpoint Protection license can only be assigned to a single computer at a given time.

Next is a description of how to manage your Panda Endpoint Protection licenses: how to assign them to the computers on your network, release them, and check their status.

CHAPTER CONTENT

Definitions and basic concepts

The following is a description of terms required to understand the graphs and data provided by Panda Endpoint Protection to show the product's licensing status.

To purchase and/or renew licenses, contact your designated partner.

License contracts

The licenses purchased by a customer are grouped into license contracts. A license contract is a group of licenses with characteristics common to all of them:

- **Product type**: Panda Endpoint Protection, Panda Full Encryption, .
- **Contracted licenses**: number of licenses in the license contract.
- **License type**: NFR, Trial, Commercial, Subscription.
- **Expiration date**: date when all licenses in the license contract expire and the computers cease to be protected.

Computer status

From a licensing perspective, the computers on the network can have three statuses:

- **Computer with a license**: the computer has a valid license in use.
- **Computer without a license**: the computer doesn't have a valid license in use, but is eligible to have one.
- **Excluded**: computers for which it has been decided not to assign a license. These computers are not and won't be protected by Panda Endpoint Protection, even if there are licenses unassigned. Nevertheless, they are displayed in the console and some management features are valid for them. To exclude a computer, you have to release its license manually.

It is important to distinguish between the number of computers without a license assigned (those which could have a license if there are any available), and the number of excluded computers (those which could not have a license, even if there are licenses available).

License status and groups

There are two possible statuses for contracted licenses:

- **Assigned**: this is a license used by a network computer.
- **Unassigned**: this is a license that is not being used by any computer on the network.

Additionally, licenses are separated into two groups according to their status:

- **Used licenses**: comprising all licenses assigned to computers.
- **Unused licenses**: comprising the licenses that are not assigned.

Types of licenses

- **Commercial licenses**: these are the standard Panda Endpoint Protection licenses. A computer with an assigned commercial license benefits from the complete functionality of the product.
- **Trial licenses**: these licenses are free and valid for thirty days. A computer with an assigned trial license will benefit temporarily from the product functionality.
- **NFR licenses**: Not For Resale licenses are for Panda Security partners and personnel. It is not permitted to sell these licenses, nor for them to be used by anyone other than Panda Security partners or personnel.
- **Subscription licenses**: these are licenses that have no expiration date. This is a "pay-as-you-go" type of service.

Assigning licenses

Licenses can be assigned in two ways: manually and automatically.

Refer to "Managing computers and devices" on page 131 for more information about the search tool, the folder tree and the filter tree.

Automatic assignment of licenses

Once you install the Panda Endpoint Protection software on a computer on the network, and provided there are unused Panda Endpoint Protection licenses, the system will assign an unused license to the computer automatically.

Manual assignment of licenses

Follow the steps below to manually assign a Panda Endpoint Protection license to a network computer.

- Go to the **Computers** menu at the top of the console. Find the device to assign the license to. You can use the folder tree, the filter tree or the search tool.
- Click the computer to access its details screen.
- Go to the **Details** tab. The **Licenses** section will display the status **No licenses**. Click the ⊕ icon to assign an unused license to the computer automatically.

Releasing licenses

Just as with the license assignment process, you can release licenses in two ways: manually and automatically.

Automatic release

- When the Panda Endpoint Protection software is uninstalled from a computer on the network, the system automatically recovers a license and returns it to the group of licenses available for use.
- Similarly, when a license contract expires, licenses will automatically be released from computers in accordance with the process explained in section "“**Withdrawal of expired licenses**”

Manual release

Manual release of a license previously assigned to a computer will mean that the computer becomes 'excluded'. As such, even though there are licenses available, they will not be assigned automatically to this computer.

Follow the steps below to manually release a Panda Endpoint Protection license:

- Go to the **Computers** menu at the top of the console. Find the device whose license you want to release. You can use the folder tree, the filter tree or the search tool.
- Click the computer to access its details screen.
- Go to the **Details** tab. The **Licenses** section will display the name of the product license assigned to the computer. Click the ⊗ icon to release the license and send it back to the group of unused licenses.

Processes associated with license assignment

Case 1: Excluded computers and those with assigned licenses

By default, each new computer integrated into Aether Platform is assigned a Panda Endpoint Protection product license automatically, and as such acquires the status of a **computer with an assigned license**. This process continues until the number of unused licenses reaches zero.

Computers whose assigned licenses are released manually acquire the status of excluded, and are no longer in the queue for automatically assigned licenses if they are available.

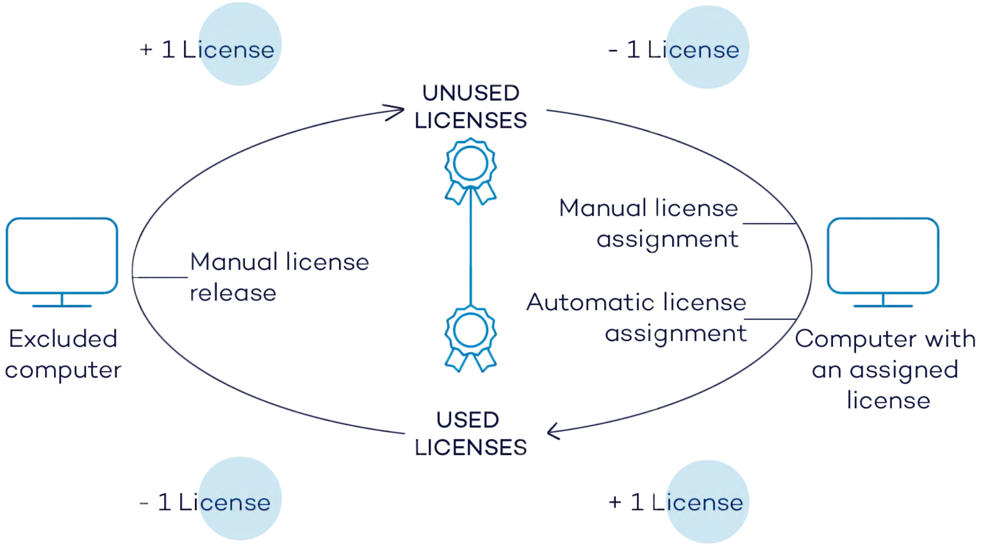


Figure 7.1: Modification of license groups with excluded computers and those with licenses assigned

Case 2: Computers without an assigned license

As new computers are integrated into Aether Platform and the pool of unused licenses reaches zero, these computers will have the status of **computers without a license**. As new licenses become available, these computers will automatically be assigned a license.

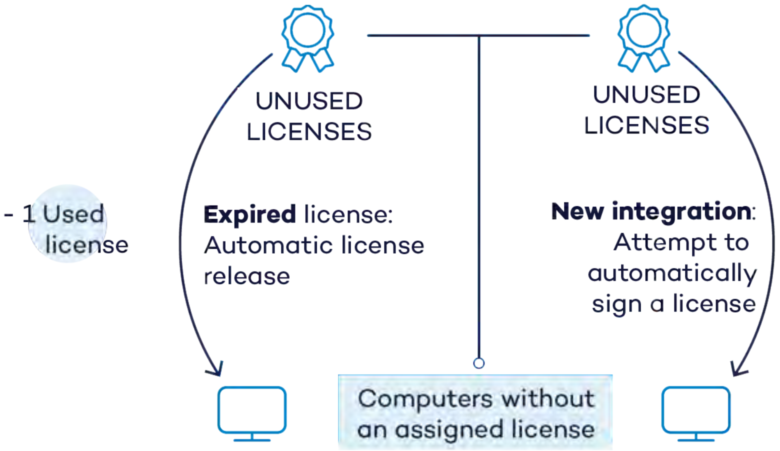

UNUSED LICENSES
UNUSED LICENSES
- 1 Used license
Expired license: Automatic license release
New integration: Attempt to automatically sign a license
Computers without an assigned license

Figure 7.2: Computers without an assigned license due to expiry of the license contract and because the group of unused licenses was empty at the time of integration

Similarly, when an assigned license expires, a computer on the network will have the **No license** status in accordance with the license expiration process explained in section "**Withdrawal of expired licenses**".

Licenses module panels/widgets

Accessing the dashboard

To access the dashboard, click the **Status** menu at the top of the console and then click **Licenses** from the side menu.

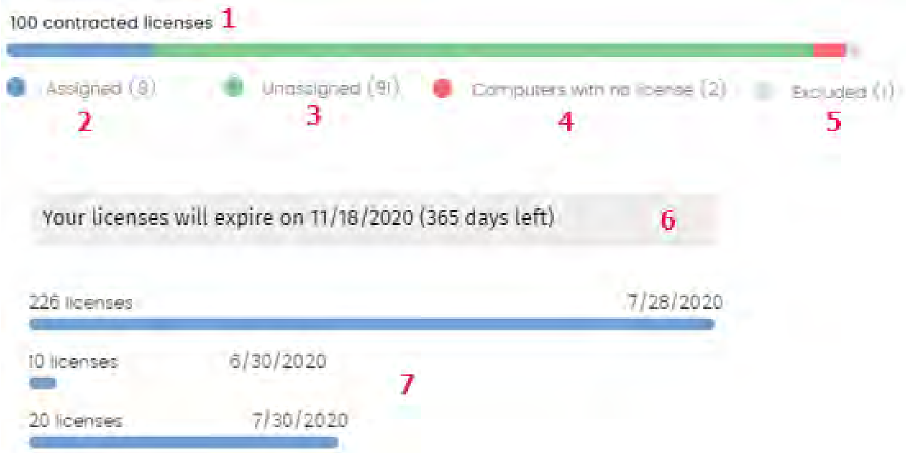
Required permissions

No additional permissions are required to access the widgets associated with the Licenses dashboard.

To see details of contracted licenses, click the **Status** menu at the top of the console and then **Licenses** from the side menu. A window with two graphs (widgets) appears: **Contracted licenses** and **License expiration**.

Licenses

The panel shows how the contracted product licenses are distributed.



100 contracted licenses

● Assigned (9) ● Unassigned (91) ● Computers with no license (2) ● Excluded (1)

Your licenses will expire on 11/18/2020 (365 days left)

226 licenses 7/28/2020

10 licenses 6/30/2020

20 licenses 7/30/2020

Figure 7.3: License panel with three license contracts

- **Meaning of the data displayed**

Hotspot	Description
Total number of contracted licenses (1)	This represents the maximum number of computers that can be protected if all the contracted licenses are assigned.
Number of assigned licenses (2)	This is the number of computers protected with an assigned license.
Number of unassigned licenses (3)	This is the number of licenses contracted that haven't been assigned to a computer and are therefore not being used.
Number of computers without a license (4)	Computers that are not protected as there are insufficient licenses. Licenses will be assigned automatically once they are bought.

Table 7.1: Fields in the 'Licenses' panel

Hotspot	Description
Number of excluded computers (5)	Computers without a license assigned and that are not eligible to have a license.
License expiration date (6)	If there is only one license contract, all licenses will expire at the same time, on the specified date.
License contract expiration dates (7)	If one product has been contracted several times over a period of time, a horizontal bar chart will be displayed with the licenses associated with each contract/license contract and their expiration date.

Table 7.1: Fields in the 'Licenses' panel

- **Lists accessible from the panel**

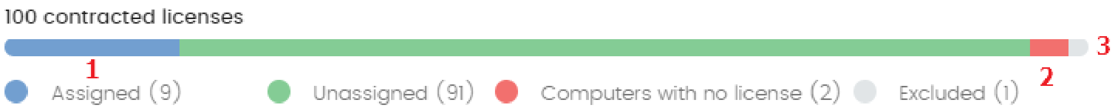


Figure 7.4: Hotspots in the 'Contracted licenses' panel

The **Licenses** list accessible from the panel will display different information based on the hotspot clicked:

List filtered by	Value
(1) License status	Assigned
(2) License status	No license
(3) License status	Excluded

Table 7.2: Filters available in the 'Contracted licenses' panel

Licenses module lists

Accessing the lists

There are two ways to access the lists:

- Click the **Status** menu at the top of the console. Then, click **Licenses** from the side menu and click the relevant widget.

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window appears with all available lists.
- Select the **Licenses** list from the **General** section to view the associated template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

No additional permissions are required to access the **Licenses** list.

Licenses

This list shows details of the licensing status of the computers on the network, with filters that help you locate desktops, laptops, servers, or mobile devices based on their licensing status.

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs.	Character string
License status	The computer's license status.	• Assigned • No license • Excluded
Last connection	Date when the computer status was last sent to Panda Security's cloud.	Date

Table 7.3: Fields in the 'Licenses' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the product belongs to.	Character string
Computer type	Purpose of the computer within the organization's network.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
Operating system	Operating system installed on the computer, internal version and patching status.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android
Active Directory	Path to the computer in the company's Active Directory.	Character string
Virtual machine	Indicates whether the computer is physical or virtual.	Boolean

Table 7.4: Fields in the 'Licenses' exported file

Field	Description	Values
Agent version	Internal version of the agent component that is part of the Panda Endpoint Protection client software.	Character string
Protection version	Internal version of the protection component that is part of the Panda Endpoint Protection client software.	Character string
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last connection date	Date when the computer status was last sent to Panda Security's cloud.	Date
License status	The computer's license status.	• Assigned • No license • Excluded
Group	Folder in the Panda Security folder tree that the computer belongs to.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string

Table 7.4: Fields in the 'Licenses' exported file

- **Filter Tool**

Field	Description	Values
Find computer	Computer name.	• Character string
Computer type	Purpose of the computer within the organization's network	• Workstation • Laptop • Mobile device • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS • Android
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago

Table 7.5: Filters available in the 'Licenses' list

Field	Description	Values
		• Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the computer status was last sent to Panda Security’s cloud.	• All • More than 72 hours ago • More than 7 days ago • More than 30 days ago
License status	The computer's license status.	• Assigned • No license • Excluded

Table 7.5: Filters available in the 'Licenses' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window.Refer to “**Computer details**” on page 159 for more information.

Expired licenses

Apart from subscription ones, all other license contracts have an expiration date assigned, after which the computers will cease to be protected.

Expiration notifications

Thirty days before a license contract expires, the **Licenses** panel will display a message showing the days remaining and the number of licenses that will be affected.

In addition to this, you will also be notified of the license contracts that have expired in the last thirty days.

> ⚠ *If all products and license contracts are expired, you will no longer have access to the management console.*

Withdrawal of expired licenses

Panda Endpoint Protection does not maintain a strict connection between license contracts and computers. Computers with licenses assigned do not belong to a particular license contract. Instead, all licenses from all license contracts are added to a single pool of available licenses, which are then distributed among the computers on the network.

Whenever a license contract expires, the number of licenses assigned to that contract is determined and the computers with licenses assigned are arranged according to the **Last connection** field, which indicates the date the computer last connected to the Panda Security cloud.

Computers whose licenses may be withdrawn will be those that have not been seen for the longest period of time. This establishes a system of priorities whereby it is more likely to withdraw a license from computers that have not been used recently.

> *This logic for withdrawing expired licenses affects all compatible devices with* Panda Endpoint Protection *and with licenses assigned*

Adding trial licenses to commercial licenses

Where a customer has commercial licenses of Panda Endpoint Protection, Panda Endpoint Protection Plus or Panda Fusion on Aether Platform and they get a trial version of Panda Endpoint Protection, there will be a series of changes, both to the management console and to the software installed on the computers on the network:

- A new trial license contract will be created for the trial period, with as many licenses as previously available plus the licenses contracted for the trial.
- The commercial license contract will be temporarily deactivated during the trial period, though its expiration and renewal cycle will be unaffected.
- The trial product's functionality will be enabled for the trial with no need to update the computers.
- Panda Endpoint Protection will, by default, be enabled on all computers in Audit mode. If you do not want to enable Panda Endpoint Protection on all computers or you want to set a different protection mode, this can be configured accordingly.

> *Refer to "***Manual and automatic assignment of settings***" for more information on how to assign settings profiles to the computers on your network.*

- Once the trial period has ended, the license contract created for the trial will be deleted, the commercial license contract will be reactivated, and the network computers will be downgraded automatically, returning to the previous settings.

Computer search based on license status

The Panda Endpoint Protection filter tree lets you search for computers based on the status of their licenses.

Refer to "Creating and organizing filters" on page 135 for more information on how to create filters in Panda Endpoint Protection.

The properties of the **License** category are as follows (these properties will allow you to create filters that generate lists of computers with specific licensing information):

Category	Property	Value	Description
License	**Status**	Lets you create filters based on the following license statuses:	
		Assigned	Lists those computers with a Panda Endpoint Protection license assigned.
		Not assigned	Lists those computers that don't have a Panda Endpoint Protection license assigned.
		Unassigned manually	Lists those computers whose Panda Endpoint Protection license was manually released by the network administrator.
		Unassigned automatically	Lists those computers whose Panda Endpoint Protection license was automatically released by the system.

Table 7.6: Fields in the 'Licenses' filter

Chapter 8

Product updates and upgrades

Panda Endpoint Protection is a cloud-based managed service that does not require network administrators to perform maintenance on the back-end infrastructure that supports it. However, administrators do need to update the client software installed on the computers on the network, and launch upgrades of the management console, when required.

CHAPTER CONTENT

Updatable modules in the client software

The components installed on users' computers are the following:

- Aether Platform communications agent.
- Panda Endpoint Protection protection engine.
- Signature file.

The update procedure and options will vary depending on the operating system of the computer to update, as indicated in table

Module	Platform			
	Windows	macOS	Linux	Android
Panda agent	On demand			
Panda Endpoint Protection protection	Configurable	Configurable	Configurable	No
Signature file	Enable /Disable	Enable /Disable	Enable /Disable	No

Table 8.1: Update procedures based on the client software component

- **On demand**: you can launch the update whenever you want, provided there is an update available, or postpone it for as long as you want.
- **Configurable**: you can establish update intervals for future and recurrent updates, and disable them as well.
- **Enable/Disable**: you can enable/disable updates. If updates are enabled, they will take place automatically whenever they are available.
- **No**: the administrator cannot influence the update process. Updates will take place as soon as they are available, and it's not possible to disable them.

Protection engine updates

To configure protection engine updates you must create and assign a **Per-computer settings** configuration profile. To do this, go to the **Settings** menu, and select **Per-computer settings** from the left-hand menu.

Updates

To enable automatic updates of the Panda Endpoint Protection protection module, move the **Automatically update** Panda Endpoint Protection **on devices** slider to the ON position. This will enable all other configuration options on the screen. If this option is disabled, the protection module will never be updated.

⚠ *It is not advisable to disable protection engine updates. A computer with out-of-date protection will be more vulnerable to malware and advanced threats over time.*

Running updates at specific time intervals

Configure the following parameters for computers to run updates at specific time intervals:

- Start time

- End time

To run updates at any time, select **Anytime.**

Running updates on specific days

Use the drop-down menu to specify the days on which updates should be run:

- **Any day**: the updates will run when they are available. This option doesn't link updates to specific days.
- **Days of the week**: use the checkboxes to select the days of the week when the Panda Endpoint Protection updates will run. If an update is available, it will run on the first day of the week that matches your selection.
- **Days of the month**: use the menus to set a range of days of the month for the Panda Endpoint Protection updates to take place. If an update is available, it will run on the first day of the month that matches your selection.
- **On the following days**: use the menus to set a specific date range for the Panda Endpoint Protection updates. This option lets you select update intervals that won't be repeated over time. After the specific date, no updates will be run. This option forces you to constantly establish a new update interval as soon as the previous one has expired.

Computer restart

Panda Endpoint Protection lets you define a logic for computer restarts, if needed, by means of the drop-down menu at the bottom of the settings window:

- **Do not restart automatically**: the user of the target computer will be presented with a restart window with increasingly shorter time intervals. They will be prompted to restart their computer to apply the update.
- **Automatically restart workstations only**
- **Automatically restart servers only**
- **Automatically restart both workstations and servers**

Communications agent updates

The Panda agent is updated on demand. Panda Endpoint Protection will display a notification in the management console every time a new agent version is available. From then on, you can launch the update whenever you want.

Updating the Panda agent does not require restarting users' computers. These updates usually contain changes and improvements to the management console to ease security administration.

Knowledge updates

To configure updates of the Panda Endpoint Protection signature file, you must edit the security settings of the device type in question.

Windows, Linux and macOS devices

Go to **Settings** at the top of the console, and select **Workstations and servers** from the left-hand side menu.

Go to **General** and here you will see the following options:

- **Automatic knowledge updates:** allows you to enable or disable signature file downloads**.** If you clear this option, the signature file will never get updated.

> ⚠ *It is not advisable to disable automatic knowledge updates. A computer with out-of-date protection will be more vulnerable to malware and advanced threats over time.*

- **Run a background scan every time there is a knowledge update**: lets you automatically run a scan every time a signature file is downloaded to the computer. These scans have minimum priority so as not to interfere with the user's work.

Android devices

Go to **Settings** at the top of the console, and select **Android devices** from the left-hand side menu.

Panda Endpoint Protection lets you restrict software updates so that they don't consume mobile data.

Select the **Only update over Wi-Fi** option to restrict updates to those occasions when there is an available Wi-Fi connection for the target smartphone or tablet.

Management console upgrades

Network administrators can choose when to start the process of upgrading the management console on the Panda Security servers. Otherwise, Panda Security will automatically upgrade the management console to the latest available version.

Considerations prior to upgrading the console version

Although this is a process that takes place entirely on the Panda Security servers, upgrading the console version can push new versions of the security software to the customer’s computers. This can result in high traffic loads and the need to restart the computers on the network in some cases. To reduce the traffic during updates, refer to “**Configuring downloads via cache computers**” on page 199.

Additionally, during console upgrades, access to the console may be interrupted for minutes or hours in the case of large corporate networks with thousands of computers, so administrators must choose the most convenient time to perform this operation based on their needs.

Starting the management console upgrade

- Click the **Web notifications** icon on the upper-right side of the top menu. The unread notifications appear.
- If there is a console upgrade available, a message entitled **New management console version** is shown, along with the **New features and improvements** link, the version to which the console will be upgraded, and the **Upgrade console now** button. This type of notification cannot be deleted, as it does not show the ✕ icon. Refer to "Web notifications icon" on page 35.

> *The **Upgrade console now** button is displayed only if the user account used to access the management console has the Full Control role assigned to it.*

- After the button is clicked, the upgrade request is queued on the server, waiting to be processed. The maximum time the request remains queued on the server is 10 minutes.
- After the request has been processed, the upgrade process starts and the notification shows the text **Upgrade in progress**. If any user account tries to log in to the console, access is denied. For the duration of the upgrade process, it is not possible to log in to the management console.
- After some time, which depends on the number of managed computers and the data stored on the console, the upgrade process will finish.

Canceling the upgrade

- After the upgrade process has started, click the **Web notifications** icon on the upper-right side of the top menu. The unread notifications appear.
- If a console upgrade exists in the request queue that has not started yet, a message entitled **New management console version** is shown, along with the **New features and improvements** link, and the **Cancel upgrade** button.
- To remove the upgrade request from the queue, click the **Cancel upgrade** button. The button disappears and the **Upgrade console now** button is shown again.

Part 4

Managing devices

Chapter 9

Managing computers and devices

The Web console lets you display managed devices in an organized and flexible way, enabling you to apply different strategies to rapidly locate and manage them.

In order for a computer on the network to be managed through Panda Endpoint Protection, the Panda agent must be installed on it. Computers without a license but with the Panda agent installed will appear in the management console, although their protection will be out of date and it won't be possible to run scans or perform other tasks associated with the protection service on them.

CHAPTER CONTENT

The Computers area

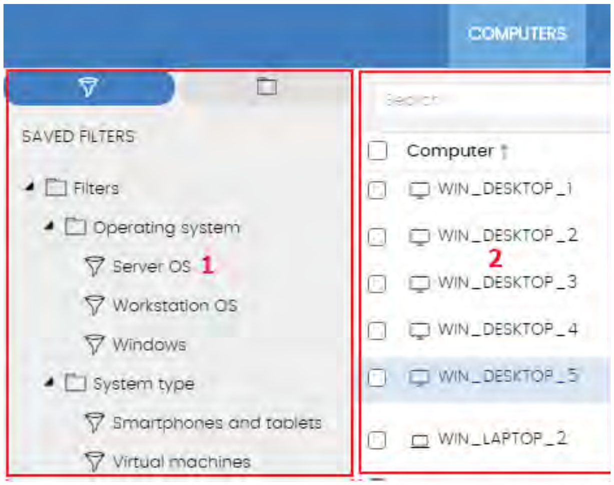


Figure 9.1: General view of the panels in the Computers area

The **Computers** area in the Web console lets you manage all devices integrated into Panda Endpoint Protection.

To access the computer management screen, click the **Computers** menu at the top of the console. Two different areas are displayed: a side panel with the **computer tree** **(1)** and a center panel with the **list of computers (2)**. Both panels work together. When you select a branch in the computer tree, the computer list is updated with the computers assigned to that branch.

Show computers in subgroups

You can restrict or expand the information displayed on the list of computers by using the **Show computers in subgroups** option accessible from the general context menu.

- If the option is selected, all computers in the selected branch and its corresponding sub-branches will be displayed.
- If the option is cleared, only those computers that belong to the selected branch of the tree will be displayed.

The Computer tree panel

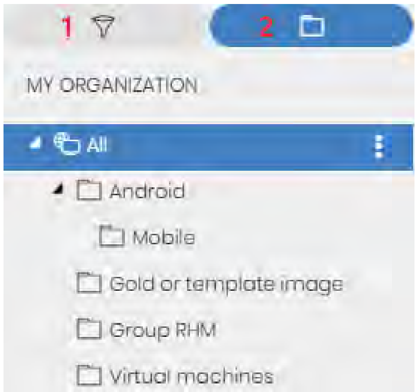


Figure 9.2: The Computers tree panel

Panda Endpoint Protection displays the computers on the network through the **Computer tree**, which provides two independent views or trees:

- **Filter tree (1):** this lets you manage the computers on your network using dynamic groups. All computers that are integrated into the console are automatically assigned to this type of group.
- **Group tree (2)**: this lets you manage the computers on your network through static groups. Computers are manually assigned to this type of group.

These two tree structures are designed to display devices in different ways, in order to facilitate different tasks such as:

- Locate computers that fulfill certain criteria in terms of hardware, software or security.
- Quickly assign security settings profiles.
- Take remediation actions on groups of computers.

*For more information on how to locate unprotected computers or those with certain security characteristics or protection status, refer to "***Malware and network visibility***" on page 299. For more information on how to assign security settings profiles, refer to "***Manual and automatic assignment of settings***" on page 184. For more information on how to take remediation actions, refer to "***Remediation tools***" on page 351.*

Hover the mouse pointer over the branches in the filter and group trees to display the context menu icon. Click it to display a pop-up menu with all available operations for the relevant branch.

Filter tree

The filter tree is one of the two computer tree views. It lets you dynamically group computers on the network using rules and conditions that describe characteristics of devices and logical operators that combine them to produce complex expressions.

The filter tree can be accessed from the left-hand panel, by clicking the filter icon ▽. Clicking different items in the tree will update the right-hand panel, presenting all the computers that meet the criteria established in the selected filter.

What is a filter?

Filters are effectively dynamic groups of computers. A computer automatically belongs to a filter when it meets the criteria established for that filter by the administrator.

A computer can belong to more than one filter.

As such, a filter comprises a series of rules or conditions that computers have to satisfy in order to belong to it. As computers meet these conditions, they join the filter. Similarly, when the status of a computer changes and ceases to fulfill those conditions, it will automatically cease to belong to the group defined by the filter.

Filters can be grouped manually in folders using whatever criteria the administrator chooses.

Predefined filters

Panda Endpoint Protection includes a series of commonly used filters that administrators can use to organize and locate network computers. These predefined filters can be edited or deleted.

⚠ *A predefined filter that has been deleted cannot be recovered.*

Name	Group	Description
Workstations and servers	Type of device	List of physical workstations and servers.
Laptops	Type of device	List of physical laptops.
Smartphones and tablets	Type of device	List of smartphones and tablets.
Virtual machines	Type of device	List of virtual machines.
Server operating system	Operating system	List of computers with a server operating system installed.
Workstation operating system	Operating system	List of computers with a workstation operating system installed.
Windows	Operating system	List of all computers with a Windows operating system installed.
macOS	Operating system	List of all computers with a macOS operating system installed.
Linux	Operating system	List of all computers with a Linux operating system installed.
Android	Operating system	List of all computers with an Android operating system installed.
Java	Software	List of all computers with the Java JRE SDK installed.
Adobe Acrobat Reader	Software	List of all computers with Acrobat Reader installed.
Adobe Flash Player	Software	List of all computers with the Flash plug-in installed.
Google Chrome	Software	List of all computers with the Chrome browser installed.
Mozilla Firefox	Software	List of all computers with the Firefox browser installed.

Table 9.1: Predefined filter list

Creating and organizing filters

To create and organize filters, click the context menu icon next to a branch of your choice in the filter tree. A pop-up menu will be displayed with the actions available for that particular branch.

Creating filters

To create a filter, follow the steps below:

- Click the context menu of the folder where the filter will be created.
    - If you want to create a hierarchical structure of filters, create folders and move your filters to them. A folder can contain other folders with filters.
- Click **Add filter**.
- Specify the name of the filter. It does not have to be a unique name. Refer to "**Configuring filters**" for more information on how to configure a filter.

Creating folders

- Click the context menu of the branch where you want to create the folder, and click **Add folder**.
- Enter the name of the folder and click **OK**.

A folder cannot be under a filter. If you select a filter before creating a folder, this will be created at the same level as the filter, under the same parent folder.

Deleting filters and folders

Click the context menu of the branch to delete, and click **Delete**. This will delete the branch and all of its children.

You cannot delete the 'Filters' root node

Moving and copying filters and folders

- Click the context menu of the branch to copy or move.
- Click **Move** or **Make a copy**. A pop-up window will appear with the target filter tree.
- Select the target folder and click **OK**.

It is not possible to copy filter folders. Only filters can be copied.

Renaming filters and folders

- Click the context menu of the branch to rename.
- Click **Rename**.

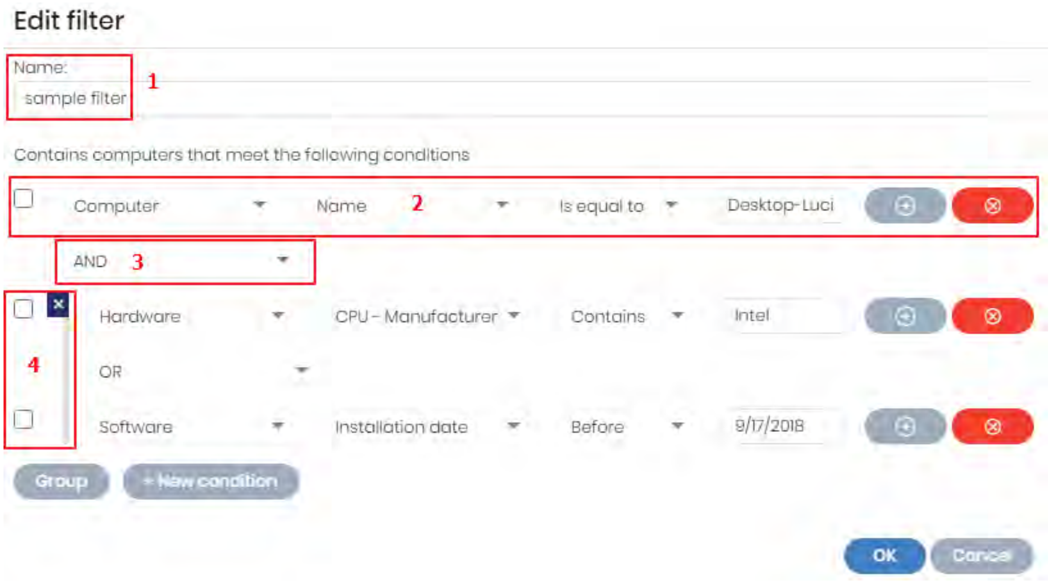
- Enter the new name.

It is not possible to rename the root folder. Additionally, to rename a filter you must edit it.

Configuring filters

To configure a filter, click its context menu and select **Edit filter** from the menu displayed. This will open the filter's settings window.

A filter comprises one or more rules, which are related to each other with the logical operators AND/ OR. A computer will be part of a filter if it meets the conditions specified in the filter rules.



Edit filter

Name: sample filter

Contains computers that meet the following conditions

□ Computer – Name – Is equal to – Desktop-Luci

AND

□ Hardware – CPU - Manufacturer – Contains – Intel

OR

□ Software – Installation date – Before – 9/17/2018

Figure 9.3: Filter settings overview

A filter has four sections

- **Filter name (1)**: this identifies the filter.
- **Filter rules (2)**: this lets you set the conditions for belonging to a filter. A filter rule only defines one characteristic of the computers on the network.
- **Logical operators (3)**: these let you combine filter rules with the values **AND** or **OR**.
- **Groups (4)**: this lets you alter the order of the filter rules related with logical operators.

Filter rules

A filter rule comprises the items described below:

- **Category**: this groups the properties in sections to make it easy to find them.
- **Property:** the characteristic of a computer that determines whether or not it belongs to the filter.
- **Operator**: this determines the way in which the computer's characteristics are compared to the

values set in the filter.

- **Value**: the content of the property. Depending on the type of property, the value field will change to reflect entries such as ‘date’, etc.

To add rules to a filter, click the ⊕ icon. To delete them, click ⊗

Logical operators

To combine two rules in the same filter, use the logical operators AND and OR. This way, you can interrelate several rules. As soon as you add a rule to a filter, the options AND/OR will automatically appear to condition the relation between the rules.

Filter rule groupings

In a logical expression, parentheses are used to alter the order in which operators (in this case, the filter rules) are evaluated.

As such, to group two or more rules in a parenthesis, you must create a grouping by selecting the corresponding rules and clicking **Group**. A thin line will appear covering the filter rules that are part of the grouping.

The use of parentheses allows you to group operands at different levels in a logical expression.

Common use cases

Here are some examples of filters commonly used by network administrators:

Windows computers according to the installed processor (x86, x64, ARM64)

Lists all computers that have a Windows operating system installed and an ARM microprocessor.

This filter is composed of two conditions linked by the AND operator:

- **Condition 1:**
  - **Category**: Computer
  - **Property**: Platform
  - **Condition**: Equals
  - **Value**: Windows
- **Condition 2:**
  - **Category**: Computer
  - **Property**: Architecture
  - **Condition**: Equals
  - **Value**: {architecture name: ARM64, x86, x64}

Computers without a specific patch installed

Lists computers that don't have a specific patch installed. Refer to "**Panda Patch Management (Updating vulnerable programs)**" on page **227** for more information about Panda Patch Management.

- **Category**: Software
- **Property**: Software name
- **Condition**: Doesn't contain
- **Value**: (patch name)

Computers that have not connected to Panda Security's cloud in X days

Lists computers that have not connected to Panda Security's cloud in the specified period.

- **Category**: Computer
- **Property**: Last connection
- **Condition**: Before
- **Value**: {Date in dd/mm/yy format}

Computers that cannot connect to the Panda Security security intelligence services

Finds all computers that have problems connecting to the Panda Security cloud:

- **Category**: Security
- **Property**: Connection for collective intelligence
- **Condition**: Equals
- **Value**: With problems
- **Rule**
  - **Category**: Security
  - **Property**: Connection for collective intelligence
  - **Condition**: Equals
  - **Value**: With problems

Integration with other management tools

Shows computers whose name matches any of the computer names specified in a list obtained by a third-party tool. Each line in the list must end with a carriage return and will be considered a computer name.

- **Category**: Computer
- **Property**: Name
- **Condition**: In

- **Value**: computer name list

Group tree

The group tree lets you statically combine the computers on the network in the groups that the administrator chooses.

To access the group tree, follow the steps below:

- Click the folder icon 🗀 from the left-hand panel.
- By clicking the different branches in the tree, the panel on the right is updated, presenting all the computers in the selected group and its subgroups.

What is a group?

A group contains the computers manually assigned by the administrator. The group tree lets you create a structure with a number of levels comprising groups, subgroups and computers.

The maximum number of levels in a group is 10.

Types of groups

Group type	Description
Root group	This is the parent group from which all other folders derive.
Native groups 🗀	These are the Panda Endpoint Protection standard groups. They support all operations (move, rename, delete, etc.) and can contain other native groups and computers.
Active Directory groups	These groups replicate the organization's Active Directory structure. Some operations are not supported by these groups. They can contain other Active Directory groups and computers.
Active Directory root group	Contains all of the Active Directory domains configured on the organization's network. It contains Active Directory domain groups.
Active Directory domain group	Active Directory branches representing domains. They contain other Active Directory domain groups, Active Directory groups and computers.

Table 9.2: Group types in Panda Endpoint Protection

Depending on the size of the network, the homogeneity of the managed computers, and the presence or absence of an Active Directory server in the organization, the group tree structure can vary from a single-level tree in the simplest cases to a complex multi-level structure for large networks comprising numerous and varied computers.

> *Unlike filters, a computer can only belong to a single group.*

Active Directory groups

For those organizations that have an Active Directory server installed on their network, Panda Endpoint Protection can automatically obtain the configured Active Directory structure and replicate it in its group tree. This works as follows: the Panda agent installed on each computer reports the Active Directory group it belongs to the Web console and, as agents are deployed, the tree is populated with the various organizational units. This way, the branch will show a computer distribution familiar to the administrator, helping you find and manage your computers faster.

To keep consistency between the Active Directory structure existing in the organization and the tree represented in the management console, the Active Directory groups cannot be modified from the Panda Endpoint Protection console. They will only change when the company's Active Directory structure is also changed. These changes will be replicated to the Panda Endpoint Protection Web console within one hour.

If the network administrator moves, in the Panda Endpoint Protection console, a computer belonging to an Active Directory group to a native group or to the root group, the synchronization relationship with the company's Active Directory will be broken. Consequently, any changes made to the company's Active Directory groups that affect that computer won't be replicated to the Panda Endpoint Protection console.

To reestablish the synchronization relationship and continue replicating the company's original Active Directory structure to the Panda Endpoint Protection console, refer to "**Returning multiple computers to their Active Directory group**".

Creating and organizing groups

The actions you can take on groups are available through the pop-up menu displayed when clicking the context menu for the relevant branch in the group tree. The menu displayed will show the actions available for that particular branch.

Creating a group

- Click the context menu of the parent group to which the new group will belong, and click **Add group**.

- Enter the name of the group in the Name text box and click the **Add** button.

You cannot create Active Directory groups from the group tree. The group tree only replicates the groups and organizational units that already exist on your organization's Active Directory server.

If you want the computers on which to install the Panda Endpoint Protection agent to be moved to a specific group based on their IP addresses. follow the steps below:

- Click the **Add IP-based automatic assignment rules** link. A text box will be displayed for you to specify the IP addresses of the computers that will be moved to the group.
- You can enter individual IP addresses separated by commas, or IP address ranges separated by a dash.

Please note that computers only move to groups at the time of installing the Panda Endpoint Protection agent on them. If, later, the computer's IP address is changed, it will remain in the group it was originally assigned to.

Deleting groups

Click the context menu of the group to delete. If the group contains subgroups or computers, the management console will return an error.

The 'All' root node cannot be deleted.

To delete the empty Active Directory groups included in another group, click the group's context menu and select **Delete empty groups**.

Moving groups

- Click the context menu of the group to move.
- Then click **Move**. A pop-up window will appear with the target group tree.
- Select the target group and click **OK**.

Neither the 'All' root node nor the Active Directory groups can be moved.

Renaming groups

- Click the context menu of the group to rename.
- Click **Change name**.

- Enter the new name.

Neither the 'All' root node nor the Active Directory groups can be renamed.

Importing IP-based assignment rules to existing groups

Follow the steps below to add IP addresses to an existing native group:

- Select the context menu of a native group other than the 'All' group and select the **Import IP-based assignment rules** option. A window will open for you to drag a file with the IP addresses to add.
- This file must contain one or more text lines and must have the following format:
    - For individual IP addresses: add a line per address:

```
.\Group\Group\Group (tab) IP
```

- For IP ranges: add a line per range:

```
.\Group\Group\Group (tab) StartIP-EndIP
```

- All specified paths will be interpreted by Panda Endpoint Protection as belonging to the tree branch selected.
- If the groups indicated in the file do not already exist, Panda Endpoint Protection will create them and assign the specified IP addresses to them.

- Click **Import**. The IP addresses will be assigned to the groups indicated in the file. Additionally, the icons in the group tree will be updated to reflect the changes in the group type.

All IP addresses previously assigned to an IP-based group will be deleted when importing a file with new group-IP pairs.

Once the process is complete, all new computers that are integrated into Panda Endpoint Protection will be moved to the relevant groups based on their IP addresses.

Exporting IP-based assignment rules

To export a file with IP-based assignment rules, follow the steps below:

- Click the context menu of an IP-based group, and select the option Export IP-based assignment rules. A .CSV file will be downloaded, containing the IP-based assignment rules defined for the group and all its child groups.
- The .CSV file format is the one specified in section "**Importing IP-based assignment rules to existing groups**".

Moving computers from one group to another

You have several options to move one or more computers to a group:

Moving groups of computers to groups

- Select the group **All** in order to list all managed computers, or use the search tool to locate the computers to move.
- From the computer list displayed, click the checkboxes next to the computers that you want to move.
- Click the ⋮ icon to the right of the search bar. A drop-down menu will appear with the option **Move to**. Click it to show the target group tree.
- Select the target group to move the computers to.

Moving a single computer to a group

There are three ways to move a single computer to a group:

- Follow the steps described above for moving groups of computers, but simply select a single computer.
- Find the computer that you want to move and click the ⋮ menu icon to its right.
- From the details screen of the computer that you want to move:
  - From the panel with the list of computers, click the computer you want to move in order to display its details.
  - Find the **Group** field and click **Change**. This will display a window with the target group tree.
  - Select the target group to move the computer to and click **OK**.

Moving computers from an Active Directory group

A computer that belongs to an Active Directory group is synchronized with the company's Active Directory and therefore cannot be moved to another Active Directory group via the Panda Endpoint Protection console. In this case, you'll have to move the computer within the organization's Active Directory and then wait a maximum of 1 hour until the Panda Endpoint Protection console synchronizes. However, computers belonging to an Active Directory group can be moved to a native group.

> ⚠ *After moving a computer from an Active Directory group to a native group, any changes made to the company's Active Directory groups that affect that computer won't be replicated to the console. Refer to "Active Directory groups".*

Moving computers to an Active Directory group

It is not possible to move a computer from a native group to a specific Active Directory group. You can only return it to the Active Directory group that it belongs to. To do this, click the computer's context menu and select **Move to Active Directory path**.

Returning multiple computers to their Active Directory group

To return multiple computers to their original Active Directory group, click the context menu of an Active Directory group and select **Retrieve all computer residing on this Active Directory branch**. All computers that belong to that group in the company's Active Directory and which have been moved by the administrator to other groups in the Panda Endpoint Protection console will be restored to their original Active Directory location.

Filtering results by groups

The feature for filtering results by groups displays in the console only the information generated by the computers on the network that belong to the groups selected by the administrator. This is a quick way to establish a filter that affects the entire console (lists, dashboards, and settings) and helps to highlight data of interest to the administrator.

Configuring the filter by groups

To configure the filtering of results by groups, follow the steps below:

- Click the relevant button from the top menu. A window with the group tree will be displayed.
- Select the groups to be displayed from the computer tree and click **OK**.

The console will only display the information generated from the computers that belong to the selected groups.

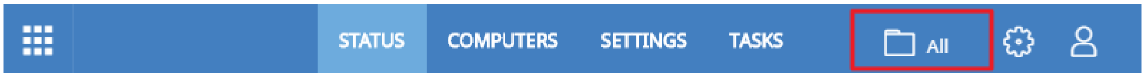


Figure 9.4: Filtering results by groups

Filtering computers will not affect task visibility or the sending of email alerts or scheduled executive reports.

Filtering groups

In very large IT infrastructures, the group tree may contain a large number of nodes distributed at multiple levels, making it difficult to find specific groups. To filter the group tree and show only those groups that match the entered characters:

- Click the 🔍 icon at the top of the group tree. A text box appears.
- Enter the letters of the name of the group to find. All groups whose name starts with, ends with, or

contains the character string entered are shown.

- After you have completed your search, select the group you are interested in and click the ✕ icon to show the full group tree again, maintaining your selection.

Scan and disinfection tasks

The group tree allows you to assign immediate or scheduled scan tasks to all computers belonging to a group and its subgroups.

> *For more information about the different types of scans, refer to "***Scan options***" on page* **355**.

Immediate scans

Click the **Scan now** option to launch an immediate scan of all computers belonging to a group or any of its subgroups. A window will be displayed for you to select the scan type to run: **The entire computer** or **Critical areas**.

Scheduled scans

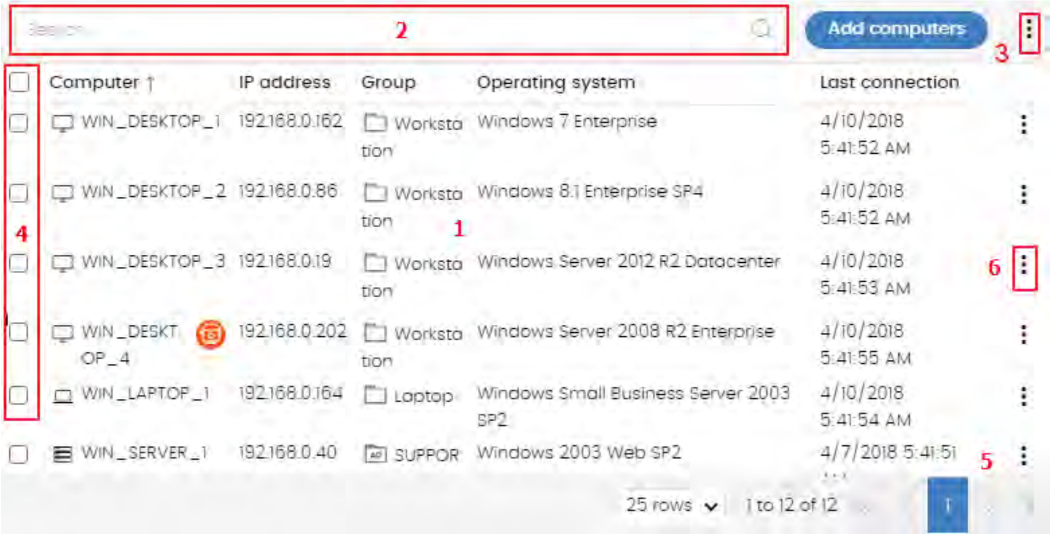
Click the Schedule scan option to create a scheduled scan task.

Available lists for managing computers

Accessing the lists

- Click the **Computers** menu at the top of the console. The panel on the left will show the computer or folder tree, whereas the panel on the right will show all managed computers on the network.

- Click an item from the group tree or filter tree on the left. The panel on the right will be updated with the content of the selected item.



Computer ↑	IP address	Group	Operating system	Last connection
WIN_DESKTOP_1	192.168.0.162	Workstation	Windows 7 Enterprise	4/10/2018 5:41:52 AM
WIN_DESKTOP_2	192.168.0.86	Workstation	Windows 8.1 Enterprise SP4	4/10/2018 5:41:52 AM
WIN_DESKTOP_3	192.168.0.19	Workstation	Windows Server 2012 R2 Datacenter	4/10/2018 5:41:53 AM
WIN_DESKTOP_4	192.168.0.202	Workstation	Windows Server 2008 R2 Enterprise	4/10/2018 5:41:55 AM
WIN_LAPTOP_1	192.168.0.164	Laptop	Windows Small Business Server 2003 SP2	4/10/2018 5:41:54 AM
WIN_SERVER_1	192.168.0.40	SUPPOR	Windows 2003 Web SP2	4/7/2018 5:41:51 ...

Figure 9.5: The Computer list panel

Required permissions

No additional permissions are required to access the **Computer list** panel.

Computers

The computer list shows the workstations and servers belonging to the group or filter selected in the computer tree. It also provides management tools you can use on individual computers or on multiple computers at the same time.

The items that make up the computer list panel are as follows:

- **(1)** List of computers belonging to the selected branch.
- **(2) Search tool**: enables you to find computers by their name, description, IP address, or last logged-in user. It supports partial matches and is not case sensitive.
- **(3)** General context menu: enables you to apply an action to multiple computers.
- **(4)** Computer selection checkboxes.
- **(5)** Pagination controls at the bottom of the panel.
- **(6)** Context menu for each computer.

The computer list can be configured to adapt the data displayed to the administrator's needs.

To add or remove columns, click the context menu in the top-right corner of the window and click the **Add or remove columns** option. A window appears with the available columns, as well as the **Default columns** link to reset the list to its default values.

The following information is displayed for each computer.

Field	Description	Values
Computer	Computer name and type.	Character string • Workstation or server. • Laptop. • Mobile device (Android smartphone or tablet).
Computer status	Agent reinstallation: • Reinstalling the agent. • Agent reinstallation error. Protection reinstallation: • Reinstalling the protection • Protection reinstallation error. • Pending restart.	Icon
IP address	The computer's primary IP address.	IP address
Description	Description assigned to the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory path	Path to the computer in the company's Active Directory.	Character string
IP address	The computer's primary IP address.	• IP address •
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs, and its type.	Character string • Group. • IP-based group • Active Directory AD or root domain. • Organizational Unit. • Group tree root.
Operating system	Name and version of the operating system installed on the computer.	Character string
Last connection	Date when the computer status was last sent to Panda Security's cloud.	Date

Table 9.3: Fields in the 'Computers' list

Field	Description	Values
Last logged-in user	Name of the user accounts currently logged-in to the console on the computer.	Character string

Table 9.3: Fields in the 'Computers' list

- **Campos mostrados en el fichero exportado**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	Comma-separated list of the IP addresses of all cards installed on the computer.	Character string
Physical addresses (MAC)	Comma-separated list of the physical addresses of all cards installed on the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory	Path to the computer in the company's Active Directory.	Character string
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
System boot date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last connection	Last time the computer connected to the cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS • Android
Operating system	Name of the operating system installed on the computer, internal version and patching status.	Character string
Virtual machine	Indicates whether the computer is physical or virtual.	Boolean

Table 9.4: Fields in the 'Computers list' exported file

Field	Description	Values
Is a non-persistent computer	Indicates if the operating system of the virtual machine resides on a storage device that persists between restarts, or reverts to its original state instead.	Boolean
Protection version	Internal version of the protection module installed on the computer.	Character string
Last update on	Date when the protection was last updated.	Date
Licenses	Licensed product.	Panda Endpoint Protection
Network settings	Name of the network settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the network settings.	Character string
Security for workstations and servers	Name of the security settings applied to the workstation or server.	Character string
Settings inherited from	Name of the folder from which the computer inherited its security settings.	Character string
Security for Android devices	Name of the security settings applied to the mobile device.	Character string
Settings inherited from	Name of the folder from which the device inherited its security settings.	Character string
Per-computer settings	Name of the settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited its settings.	Character string
Patch management	Name of the patching (Panda Patch Management) settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the patching settings.	Character string
Encryption	Name of the encryption (Panda Full Encryption) settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the encryption settings.	Character string
Description	Description assigned to the computer.	Character string
Last logged-in user	Names of the user accounts, separated by commas, that are currently logged in to the console on a Windows computer.	Character string

Table 9.4: Fields in the 'Computers list' exported file

Field	Description	Values
Requested action	Requested action that is pending execution or is in progress.	- Restart - Protection reinstallation - Agent reinstallation
Requested action failed	Type of error reported by the requested action.	- Wrong credentials - Discovery computer not available - Unable to connect to the computer - Operating system not supported - Unable to download the agent installer - Unable to copy the agent installer - Unable to uninstall the agent - Unable to install the agent - Unable to register the agent - Action requires input from the user
Last proxy used	Access method used by Panda Endpoint Protection the last time it connected to Panda Security's cloud. This data is not updated immediately, so it might take up to 1 hour for the correct value to show.	Character string

Table 9.4: Fields in the 'Computers list' exported file

- **Filter tools**

Field	Description	Values
Computer	Computer name.	Character string

Table 9.5: Filters available in the 'Computers' list

- **Management tools**

If you select one or more computers using their checkboxes **(4)**, the search tool **(2)** will be hidden and the action bar **(7)** will be displayed instead.

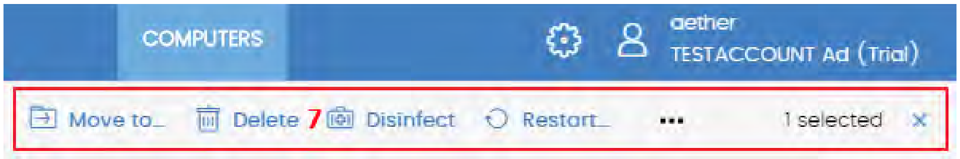


Figure 9.6: Action bar

Click the checkbox in the table header **(4)** to select all computers on the current page of the list. The **Select all xx rows in the list** option will appear, which enables you to select all computers on the list regardless of the page you are on:

Action	Description
Refresh computer information	Forces the agent installed on the computer to take the following actions: • Check for pending actions. Check for pending tasks • Check for applied settings. • Send status information. This icon is shown only for computers with the Real-time communication feature enabled. Refer to "Configuring real-time communication" on page 201.
Move to	Opens a window showing the group tree. Choose the group to move the computer to. The computer will inherit the settings assigned to the target group. Refer to "Creating and managing settings" on page 183
Move to Active Directory path	Moves the selected computer to the group that corresponds to its organizational unit in the organization's Active Directory.
Delete	Deletes the computer from the console and uninstalls the Panda Endpoint Protection client software from it. Refer to "Uninstalling the software" on page 106 for more information.
Scan now	Refer to "On-demand computer scanning and disinfection" on page 352 for a full description of scan tasks.
Schedule scan	Refer to "On-demand computer scanning and disinfection" on page 352 for a full description of scan tasks
Restart	Restarts the computer. "Computer restart" on page 358 for more information.
Schedule patch installation	Refer to "Panda Patch Management (Updating vulnerable programs)" on page 227 for more information on how to install patches on Windows computers
Reinstall protection (requires restart)	Reinstalls the protection if a malfunction occurs. Refer to "Remote reinstallation" on page 108 for more information.
× selected	Undoes the current selection.

Table 9.6: Computer management tools

My lists panel

Accessing the My lists panel

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel. A window appears with all available lists.

From the **General** group, select the **Hardware**, **Software**, or **Computers with duplicate name** list.

> *Refer to "Managing lists" on page 43 for more information about the available list types and how to work with them.*
>
> *For more information about the fields as well as the filter and search tools implemented in each list, refer to the chapter on the group the list belongs to.*

Required permissions

No additional permissions are required to access the **My lists** panel.

'Hardware'

Shows the hardware components installed on each computer on the network. Each hardware component is shown independently each time it is detected on a computer.

Field	Description	Values
Computer	Name and type of computer that contains the hardware component.	Character string • 🖥 Workstation or server • 💻 Laptop. • 📱 Mobile device (Android smartphone or tablet).
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	Character string
CPU	Make and model of the microprocessor installed on the computer. The number of installed cores is shown in brackets.	Character string
Memory	Total amount of RAM memory installed.	Character string
Disk capacity	Sum of the capacity of all the internal hard disks connected to the computer.	Character string
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Date
Context menu	Management tools. Refer to "Management tools" for more information.	

Table 9.7: Fields in the 'Hardware' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS • Android
Operating system	Name of the operating system installed on the computer, internal version and patch status.	Character string
System	Name of the computer's hardware model.	Character string
CPU-N	Model, make and characteristics of CPU number N.	Character string
CPU-N Number of cores	Number of cores in CPU number N.	Numeric value
CPU-N Number of logical processors	Number of logical cores reported to the operating system by the Hyper-Threading/SMT (simultaneous multithreading) system.	Numeric value
Memory	Sum of all the RAM memory banks installed on the computer.	Character string
Disk-N Capacity	Total space on internal storage device number N.	Character string
Disk-N Partitions	Number of partitions on internal storage device number N reported to the operating system.	Numeric value
TPM spec version	Versions of the APIs compatible with the TPM chip.	Character string

Table 9.8: Fields in the 'Hardware' exported file

Field	Description	Values
BIOS - Serial number	The computer's BIOS serial number.	Character string

Table 9.8: Fields in the 'Hardware' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Platform	Operating system make.	• Windows • Android

Table 9.9: Filters available in the 'Hardware' list

'Software'

Shows all programs installed on the computers on your network. For each package, the solution reports the number of computers that have it installed, as well as the software version and vendor.

Click any of the software packages to open the "**Computer list**" filtered by the selected package. The list will show all computers on the network that have that package installed.

Field	Description	Values
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Version	Internal version of the software package.	Character string
Computers	Number of computers with the selected package installed.	Numeric value

Table 9.10: Fields in the 'Software' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string

Table 9.11: Fields in the 'Software' exported file

Field	Description	Values
Version	Internal version of the software package.	Character string
Computers	Number of computers that have the package installed.	Numeric value

Table 9.11: Fields in the 'Software' exported file

- **Fields displayed in the detailed Excel export file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Computer that contains the package found.	Numeric value
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Installation date	Date the software was installed.	Date
Size	Installed software size.	Numeric value
Version	Internal version of the software package.	Character string
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 9.12: Fields in the detailed export file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device

Table 9.13: Filters available in the 'Software' list

Field	Description	Values
Platform	Operating system make.	• Windows • Linux • macOS • Android

Table 9.13: Filters available in the 'Software' list

- **Computers list window**

Clicking any of the rows in the list displays the list of computers filtered by the selected software.Refer to "Computers" for more information.

Computers with duplicate name'

Shows computers on the network with the same name and belonging to the same domain. Of all computers with the same name found on the network, those computers that have been offline for the longest time will be considered redundant and will be displayed in the list. The computer that has been online most recently will be considered the correct one and won't be shown in the list. This way, the administrator will be able to safely select and delete all duplicates at once.

To delete duplicate computers, select them using the relevant checkboxes and click Delete from the toolbar. A window will be shown asking you if you wish to uninstall the Panda Endpoint Protection agent.

Deleting computers from the ***Computers with duplicate name*** *list without uninstalling the Panda Endpoint Protection agent only removes them from the Panda Endpoint Protection console. Those computers will appear in the Panda Endpoint Protection console the next time they connect to the cloud. Before deleting computers in bulk without knowing which ones are true duplicates, we advise that you first check to see which computers reappear in the console before deleting the agent from any computers.*

Field	Description	Values
Computer	Computer name and type.	Character string: • 🖥 Workstation or server • 💻 Laptop computer. • 📱 Mobile device (Android smartphone or tablet).
IP address	The computer's primary IP address.	Character string
Group	Folder within the Panda Endpoint Protection folder tree the computer belongs to.	Character string

Table 9.14: Fields in the 'Computers with duplicate name' list

Field	Description	Values
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Date

Table 9.14: Fields in the 'Computers with duplicate name' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder within the Panda Endpoint Protection folder tree the computer belongs to.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Protection version	Internal version of the protection module installed on the computer.	Character string
Installation date	Date the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last connection date	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS • Android
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Active Directory	Full path to the computer in the company's Active Directory.	Character string
Last logged-in user	Names of the user accounts that are currently logged in to the console on the computer.	Character string

Table 9.15: Fields in the 'Computers with duplicate name' exported file

Field	Description	Values
Last bootup date	Date when the computer was last booted.	Date

Table 9.15: Fields in the 'Computers with duplicate name' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system make.	• All • Windows • Linux • macOS • Android
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago

Table 9.16: Filters available in the 'Computers with duplicate name' list

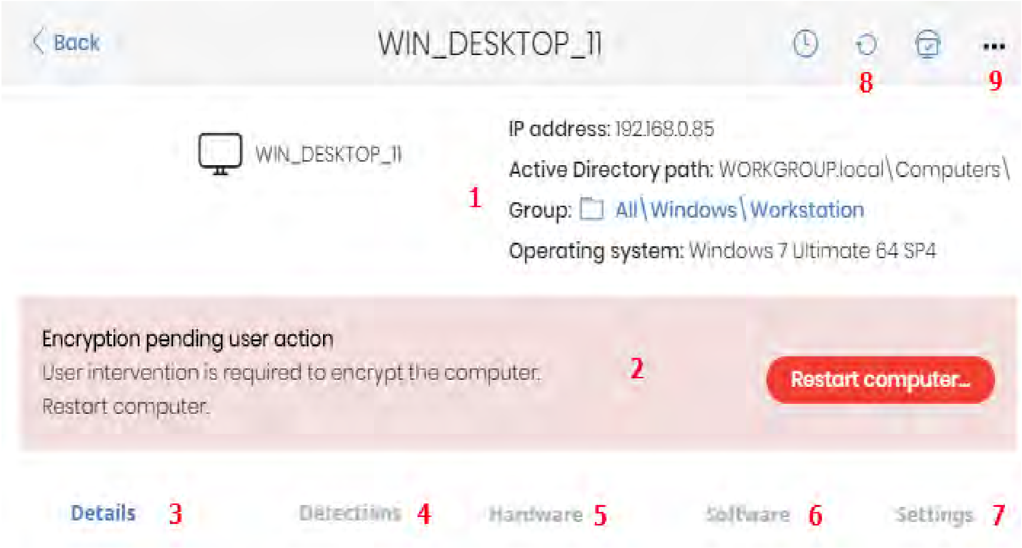
- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "**Computer details**" for more information.

Computer details

When you select a device from the list of computers, a screen is displayed with details of the hardware and software installed, as well as the security settings assigned to it.

The details screen is divided into the following sections:



WIN_DESKTOP_11

IP address: 192.168.0.85

Active Directory path: WORKGROUP.local\Computers\

Group: All\Windows\Workstation

Operating system: Windows 7 Ultimate 64 SP4

Encryption pending user action

User intervention is required to encrypt the computer.

Restart computer.

Figure 9.7: Computer details overview

- **General (1)**: this displays information to help identify the computer.
- **Notifications (2)**: details of any potential problems.
- **Details (3)**: this gives a summary of the hardware, software and security settings of the computer.
- Detections (4): computer security status. Refer to "Detections section (4)".
- **Hardware (5)**: here you can see the hardware installed on the computer, its components and peripherals, as well as consumption and use.
- **Software (6)**: here you can see the software packages installed on the computer, as well as versions and changes.
- **Settings (7)**: this shows the security settings and other settings assigned to the computer.
- **Toolbar (8)**: groups the operations available for the managed computer.
- **Hidden icons (9)**: if the window is not large enough, some tools will be hidden.

General section (1)

This contains the following information:

Field	Description
Computer name and icon indicating the type of computer	Computer name.
IP address	The computer's IP address.
Active Directory path	Full path to the computer in the company's Active Directory.

Table 9.17: Fields in the computer details' General section

Field	Description
Group	Folder in the group tree to which the computer belongs.
Operating system	Full version of the operating system installed on the computer.
Computer role	Indicates if the computer has any of the following roles assigned to it: discovery computer, cache or proxy.

Table 9.17: Fields in the computer details' General section

Computer notifications section (2)

These notifications describe any problems encountered on the computer with regard to the operation of Panda Endpoint Protection, as well as providing indications for resolving them. The following is a summary of the types of notifications generated and the recommended actions.

Computers in containment mode

Licenses

Alert	Description	Reference
Computer without a license	There are no free licenses to assign to the computer. Release an assigned license or purchase more Panda Endpoint Protection licenses.	Refer to "Releasing licenses" on page 114.
	There are free licenses but none of them have been assigned to this computer.	Refer to "Assigning licenses" on page 113.

Table 9.18: Alerts related to license assignment

Possible errors in the protection software installation process

⚠ *Panda server connection errors occurred while installing the protection software are indicated by an error code, its associated extended error code, and an extended error subcode (if available). Refer to* 16.11 *for more information.*

Alert	Description	Reference
Unprotected computer	There was an error installing the protection on the computer. With errors whose origin is known, a description of the cause will be displayed. If the origin is unknown, the associated error code will be displayed.	Refer to "Installation requirements" on page 81.

Table 9.19: Alerts related to the installation of the Panda Endpoint Protection software

Alert	Description	Reference
	A reboot is required to complete the installation due to a previous uninstallation.	Refer to "Computer restart" on page 358.
Error installing the patch manager	There was an error installing the patch management module on the computer.	Refer to "Make sure that Panda Patch Management works properly" on page 229.
Error installing the encryption module	There was an error installing the encryption module on the computer.	Refer to "Panda Full Encryption (Device encryption)" on page 271.
Error installing the Panda agent	Wrong credentials.	Refer to "Remote installation of the software on discovered computers" on page 97.
	The discovery computer is not available.	Refer to widget "Offline computers" on page 302 and section "Assigning the role of 'Discovery computer' to a computer on your network" on page 90.
	Unable to connect to the target computer because it is turned off or doesn't comply with the hardware or network requirements.	Refer to widget "Offline computers" on page 302 and section "Installation requirements" on page 81.
	The computer's operating system is not supported.	Refer to "Installation requirements" on page 81.
	Unable to download the agent installer due to a network error.	Refer to "Network requirements" on page 82.
	Unable to copy the agent installer due to low free disk space on the computer.	Refer to "Requirements for each supported platform" on page 81.
	Unable to copy the agent installer because the target computer is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Installation requirements" on page 81.
	Unable to register the agent.	Refer to widget "Offline computers" on page 302 and "Installation requirements" on page 81
Error communicating with servers	The computer cannot connect to one or more servers in the Panda cloud.	For more information, refer to "Hardware, software and network requirements" on page 373

Table 9.19: Alerts related to the installation of the Panda Endpoint Protection software

Possible errors in the protection software reinstallation process

Panda server connection errors occurred while reinstalling the protection software are indicated by an error code, its associated extended error code, and an extended error subcode (if available). Refer to 16.11 for more information.

Alert	Description	Reference
Pending protection reinstallation	The administrator requested that this computer's protection be reinstalled but the operation has not been performed yet. This may be due to the fact that the computer is turned off or offline, or the time to wait before forcing the restart hasn't elapsed yet.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
Pending agent reinstallation	The administrator requested that this computer's agent be reinstalled but the operation has not been performed yet. This may be due to the fact that the computer is turned off or offline, or the time to wait before forcing the restart hasn't elapsed yet.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
Error installing the Panda agent	Wrong credentials.	
	Discovery computer not available.	Refer to widget "Offline computers" on page 302
	Unable to connect to the computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
	Operating system not supported as it doesn't meet the remote installation requirements.	Refer to "Remote reinstallation requirements" on page 108
	Unable to download the agent installer to the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
	Unable to copy the agent installer to the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
	Unable to uninstall the agent from the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
	Unable to install the agent on the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108
	Unable to register the computer's agent because the computer is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 302 and section "Remote reinstallation requirements" on page 108

Table 9.20: Alerts related to the reinstallation of the Panda Endpoint Protection agent

Panda Endpoint Protection software malfunction errors

Alert	Description	Reference
Unprotected computer	An error was encountered in the antivirus protection. Restart the computer to fix the problem.	Refer to "Computer restart" on page 358.
Error encrypting the computer	Unable to encrypt the computer due to an error.	Refer to "Computer restart" on page 358.

Table 9.21: Alerts related to Panda Endpoint Protection software malfunction errors

Pending user or administrator action

Alert	Description	Reference
Encryption pending user action	The user must restart the computer or enter the relevant encryption credentials to complete the encryption process.	Refer to "Computer restart" on page 358. Refer to "Encryption and decryption" on page 278.
Pending restart	The administrator has requested that the computer be restarted but it hasn't restarted yet as it is offline or the time period for a forced reboot has not ended yet.	Refer to "Offline computers" on page 302.
Reinstalling protection	The administrator has requested that the computer's protection be reinstalled but the operation is not yet complete because the computer is turned off or offline, the amount of time to wait before forcing the reinstallation is not over yet, or the reinstallation is in progress	Refer to "Remote reinstallation" on page 108.
Unprotected computer	The antivirus protection is disabled. Enable the protection.	Refer to "Manual and automatic assignment of settings" on page 184, section "Creating and managing settings" on page 183 and section "Antivirus" on page 211.
Computer offline for N days	The computer is turned off or doesn't meet the network access requirements.	Refer to "Network requirements" on page 82.
Protection out-of-date	The protection requires the local user to manually restart the computer to complete the installation*.	Only on computers running the Home and Starter versions of Windows.

Table 9.22: Alerts related to lack of user or administrator action

Alert	Description	Reference
Connection problems with the Panda servers	The computer cannot successfully connect to the servers that store the security intelligence.	Refer to "Network requirements" on page 82.
The administrator has changed the protection status from the computer's local console	The administrator has changed the protection settings from the agent installed on the workstation or server. Consequently, the current settings do not match the settings defined from the Web console.	

Table 9.22: Alerts related to lack of user or administrator action

Computer with out-of-date protection

Alert	Description	Reference
Protection out-of-date	A reboot is required to complete the protection update process.	Refer to "Computer restart" on page 358.
	An error occurred while attempting to update the protection. Make sure the computer meets the hardware and network requirements.	Refer to "Installation requirements" on page 81 and the section on available hard disk space in "Hardware section (5)" on page 171
	Updates are disabled for the computer. Assign the computer a settings profile with updates enabled.	Refer to "Protection engine updates" on page 124
Malware and threat knowledge out-of-date	Knowledge updates are disabled for this computer. Assign the computer a settings profile with updates enabled.	Refer to "Knowledge updates" on page 126.

Table 9.23: Alerts related to out-of-date Panda Endpoint Protection software

General section for Android devices

For Android devices, the General **(1)** and Computer notifications **(2)** sections are replaced with the anti-theft dashboard, which allows you to launch remote actions on managed devices.

> *Refer to "Anti-theft" on page 225 for more information on how to enable the anti-theft feature for Android devices and configure the private mode.*

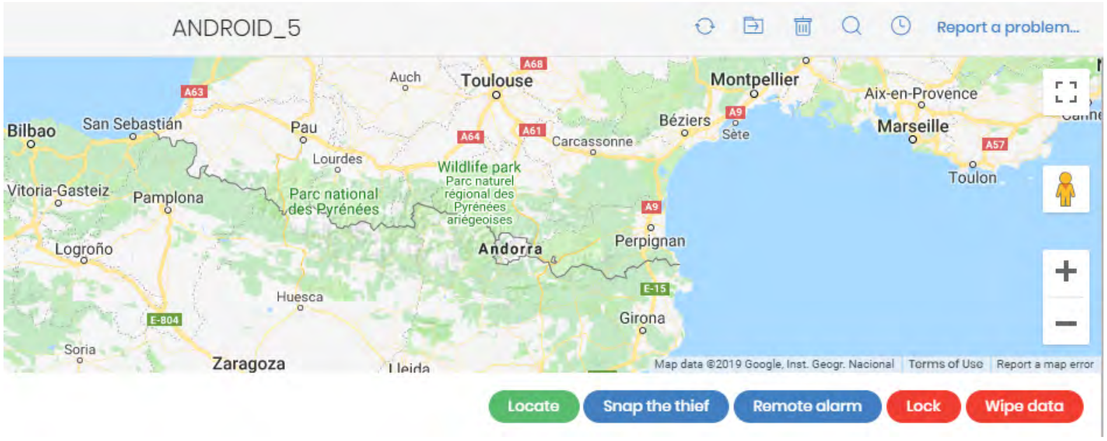


Figure 9.8: Anti-theft dashboard for Android devices

The following actions are available:

Action	Description
Locate	• **Private mode enabled**: the console will display a window for you to enter the code entered by the user of the device when enabling the private mode. If the number is correct, the Panda Endpoint Protection server will ask the device for its coordinates, showing the device's current location on the map. • **Private mode disabled**: the Panda Endpoint Protection server will directly ask the device for its coordinates, showing the device's current location on the map.
Snap the thief	Displays a window for you to enter the email address to send the photo of the potential thief to. You can also configure when the photo will be taken: • **Now**: the Panda Endpoint Protection agent will take a photo and send it to the specified address upon receiving the relevant request. • **When the screen is touched**: the Panda Endpoint Protection agent will take a photo and send it to the specified address when the user or potential thief touches the device's screen.
Remote alarm	Displays a window for you to enter a message for the user of the device and a contact number. Once received, the message will be displayed on the target device, and an alarm will be triggered at maximum volume, even if the device is locked. Click the **Don't play any sound** checkbox if you only want to display the message.
Lock	Locks the phone, preventing it from being used when it is lost or stolen. The behavior varies depending on the Android version installed on the device: • **Lower than 7**: the console asks the user to set a PIN, which is used to lock the phone. • **7 through 11 (inclusive)**: if a PIN exists that was previously set by the user, it is used to lock the phone. If a PIN has never been set previously, the console will ask the user to set one and will use it to lock the phone. • **Higher than 11**: the console never asks the user to set a PIN. If a PIN exists that was previously set by the user, it is used to lock the phone. If a PIN has never been set previously, the screen is turned off.

Table 9.24: Actions supported by the anti-theft module for Android devices

Action	Description
Wipe data	This option formats the device, deleting all its contents and applications and returning it to its factory settings.

Table 9.24: Actions supported by the anti-theft module for Android devices

Details section (3)

The information on this tab is divided into three sections: **Computer**, **Security** and **Data Protection**.

- **Computer**: information about the device settings. This information is provided by the Panda agent.
- **Security**: status of the Panda Endpoint Protection protection modules.
- **Data Protection**: status of the modules responsible for protecting the content of the data stored on computers.

Computer

Field	Description
Name	Computer name.
Description	Descriptive text provided by the administrator.
Physical addresses (MAC)	Physical addresses of the network interface cards installed.
IP addresses	List of all the IP addresses (primary addresses and aliases).
Domain	Windows domain the computer belongs to. This is empty if the computer does not belong to a domain.
Active Directory path	Path to the computer in the company's Active Directory.
Group	Group in the group tree to which the computer belongs. To change the computer's group, click **Change**.
Operating system	Operating system installed on the computer.
Virtual machine	Indicates whether the computer is physical or virtual.
Is a non-persistent desktop	Indicates if the operating system of the virtual machine resides on a storage device that persists between restarts, or reverts to its original state instead.
Licenses	Panda Security product licenses installed on the computer. Refer to “Licenses” on page 111 for more information.
Agent version	Internal version of the Panda agent installed on the computer.
Last bootup date	Date when the computer was last booted.
Installation date	Date when the computer's operating system was last installed.

Table 9.25: Fields in the Details tab's Computer section

Field	Description
Last proxy used	Access method used by Panda Endpoint Protection the last time it connected to Panda Security's cloud. This data is not updated immediately, so it might take up to 1 hour for the correct value to show.
Last connection	Date when the client software last connected to the Panda Security cloud. The communications agent connects at least every four hours.
Last settings check	Date Panda Endpoint Protection last connected to Panda Security's cloud checking for changes to the settings.
Last logged-in user	Names of the user accounts that are currently logged in to the console on the computer.

Table 9.25: Fields in the Details tab's Computer section

Security

This section indicates the status (Enabled, Disabled, Error) of the Panda Endpoint Protection technologies that protect the computer against malware.

Field	Description
File antivirus	Protection for the file system.
Antirrobo	Actions for mitigating data exposure in the event of theft of an Android mobile device.
Mail antivirus	Protection for the protocols used for sending and receiving email messages.
Web browsing antivirus	Protection against malware downloaded from web pages.
Firewall	Protection for the network traffic generated by applications.
Device control	Protection from infections stemming from external storage devices or devices that allow computers to connect to the Internet without passing through the organization's communications infrastructure (modems).
Patch management	Installation of patches and updates for Windows operating systems and third-party applications. Detection of the patch status of the computers on the network and removal of problematic patches.
Last check date	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.
Protection version	Internal version of the protection module installed on the computer.
Knowledge update date	Date when the signature file was last downloaded to the computer.

Table 9.26: Fields in the Details tab's Security section

Field	Description
Connection to knowledge servers	Status of the connection between the computer and the Panda Security servers. In case of errors, links are shown to support pages with information about the requirements that must be met.

Table 9.26: Fields in the Details tab's Security section

Data Protection

This section indicates the status of the modules that protect the data stored on the computer.

Field	Description
Hard disk encryption	Encryption module status: • **Not available**: the computer is not compatible with Panda Full Encryption. • **No information**: the computer has not yet sent any information about the encryption module. • **Enabled**: the computer has a settings profile assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: the computer has a settings profile assigned to decrypt its storage devices and no errors have occurred. • **Error**: the settings configured by the administrator don't allow an authentication method supported by Panda Full Encryption to be applied on the operating system version installed on the computer. • **Error installing**: error downloading or installing the necessary executables to manage the encryption service if they were not already installed on the computer. • **No license**: the computer doesn't have a Panda Full Encryption license assigned. **Get recovery key**: opens a window showing the IDs of the computer's encrypted storage media. Click any of them to display the relevant recovery key. Refer to "Getting the recovery key" on page 282. Encryption process status: • **Unknown**: there are drives whose status is unknown. • **Unencrypted disks**: some of the drives compatible with the encryption technology are neither encrypted nor in the process of being encrypted. • **Encrypted disks**: all drives compatible with the encryption technology are encrypted. • **Encrypting**: at least one of the computer drives is being encrypted. • **Decrypting**: at least one of the computer drives is being decrypted. • **Encrypted by the user**: all storage media are encrypted by the user. • **Encrypted by the user (partially)**: some storage media are encrypted by the user.

Table 9.27: Fields in the Data protection section

Field	Description
Authentication method	- **Unknown**: the authentication method is not compatible with those supported by Panda Full Encryption. - **Security processor (TPM)** - **Security processor (TPM) + Password** - **Password**: authentication method based on a PIN, extended PIN or passphrase. - **USB**: authentication method based on a USB drive. - **Not encrypted**: none of the drives compatible with the encryption technology is encrypted or in the process of being encrypted.
Encryption date	Date when the computer was fully encrypted for the first time.
Removable storage drive encryption	Encryption module status: - **Not available:** the computer is not compatible with Panda Full Encryption. - **No information**: the computer has not yet sent any information about the encryption module. - **Enabled**: the computer has settings assigned to encrypt its storage devices and no errors have occurred. - **Disabled**: the computer has settings assigned to decrypt its storage devices and no errors have occurred. - **Error**: the settings configured by the administrator don't allow an authentication method supported by Panda Full Encryption to be applied on the operating system version installed on the computer. - **Install error**: error downloading or installing the executables required to manage the encryption service if they were not already installed on the computer. - **No license**: the computer doesn't have a Panda Full Encryption license assigned. **View encrypted devices on this computer:** opens a window showing the IDs of the computer's encrypted external storage media. Click any of them to display the relevant recovery key. Refer to "Getting the recovery key" on page 282.

Table 9.27: Fields in the Data protection section

Detections section (4)

Shows counters associated with the computer's security and patch level through the following widgets:

Panel	Description
Threats detected by the antivirus	Refer to "Threats detected by the antivirus" on page 304.

Table 9.28: List of widgets available in the Detections section

Panel	Description
Available patches	Refer to "**Available patches**" on page **246**.
End-of-Life programs	Refer to "**End-of-Life programs**" on page **244**.

Table 9.28: List of widgets available in the Detections section

Hardware section (5)

This section contains information about the hardware resources installed on the computer:

Field	Description	Values
CPU	Information about the computer's microprocessor, along with a line chart showing CPU consumption at different time intervals based on your selection.	• 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Memory	Information about the memory chips installed, along with a line chart with memory consumption at different time intervals based on your selection.	• 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Disk	Information about the mass storage system, along with a pie chart with the current percentage of free/used space.	• Device ID • Size • Type • Partitions • Firmware revision • Serial number • Name
BIOS	Information about the BIOS installed on the computer.	• Version • Manufacture date • Serial number • Name • Manufacturer
TPM	Information about the security chip located on the computer's motherboard. To be used by Panda Endpoint Protection, the TPM must be enabled, activated and owned.	• **Manufacturer version**: internal version of the chip. • **Spec version**: supported API versions. • **Version** • **Manufacturer** • **Activated**: the TPM is ready to receive commands. This is used on systems with multiple TPMs.

Table 9.29: Fields in the computer details' Hardware section

Field	Description	Values
		• **Enabled**: the TPM is ready to work as it has been enabled in the BIOS. • **Owner**: the operating system can interact with the TPM.

Table 9.29: Fields in the computer details' Hardware section

Software section (6)

This section provides information about the software installed on the computer, the Windows operating system updates and a history of software installations and uninstallations.

Search tool

- Enter a software name or publisher in the **Search** text box and press Enter to perform a search. The following information will be displayed for each program found:

Field	Description
Name	Name of the installed program.
Publisher	The program's developer.
Installation date	Date when the program was last installed.
Size	Program size.
Version	Internal version of the program.

Table 9.30: Fields in the computer details' Software section

- To narrow your search, select the type of software you want to find from the drop-down menu:
    - Programs only
    - Updates only
    - All software

Installations and uninstallations

- Click the **Installations and uninstallations** link to show a history of all changes made to the computer:

Field	Description
Event	• 🗑 Software uninstallation. • 💾 Software installation.
Name	Name of the installed program.

Table 9.31: Fields in the Installations and uninstallations section

Field	Description
Publisher	Company that developed the program.
Date	Date the program was installed or uninstalled.
Version	Internal version of the program.

Table 9.31: Fields in the Installations and uninstallations section

Settings section (7)

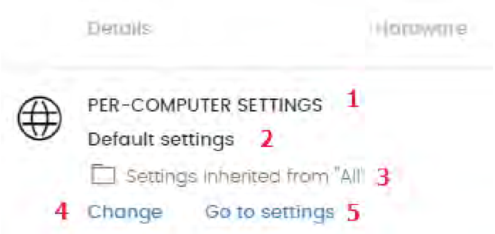


Figure 9.9: Managing and editing the assigned settings

This section displays the different types of settings assigned to the computer, and allows you to edit and manage them:

- **(1) Settings type**: indicates the type of settings assigned to the computer. Refer to "**Introduction to the various types of settings**" on page **177** for information about the different types of settings available in Panda Endpoint Protection.
- **(2) Settings name**.
- **(3) Method used to assign the settings**: directly assigned to the computer or inherited from a parent group.
- **(4) Button to change the settings profile assigned to the computer.**
- **(5) Button to edit the settings profile options**.

*Refer to "**Managing settings**" on page **175** for more information on how to create and edit settings profiles.*

Action bar (8)

This resource groups all actions that can be taken on the managed computers on your network:

Action	Description
Move to	Moves the computer to a standard group.
Move to Active Directory path	Moves the computer to its original Active Directory group.
Delete	Releases the Panda Endpoint Protection license and deletes the computer from the Web console.
Scan now	Lets you run a scan task immediately. Refer to "**On-demand computer scanning and disinfection**" on page **352** for more information.

Table 9.32: Actions available from the computer details window

Action	Description
Schedule scan	Lets you schedule a scan task. Refer to "**On-demand computer scanning and disinfection**" on page 352 for more information.
Schedule patch installation	Creates a task that installs all released patches missing from the target computer. See section "**Download and install the patches**" on page 231 for more information
Restart	Restarts the computer immediately. Refer to "**Computer restart**" on page 358 for more information.
Reinstall protection (requires restart)	Reinstalls the protection if a malfunction occurs. Refer to "**Remote reinstallation**" on page 108 for more information.
Report a problem	Opens a support ticket for Panda Security's support department. Refer to "**Reporting a problem**" on page 359 for more information.

Table 9.32: Actions available from the computer details window

Hidden icons (9)

Depending on the size of the window and the number of icons to display, some of them may be hidden under the ... icon. Click it to show all remaining icons.

Chapter 10

Managing settings

Settings, also called “settings profiles” or simply “profiles”, offer administrators a simple way of establishing security and connectivity parameters for the computers managed through Panda Endpoint Protection.

CHAPTER CONTENT

Strategies for creating settings profiles

Administrators can create as many profiles and variations of settings as they deem necessary to manage network security. A new settings profile should be created for each group of computers with similar protection needs.

- Computers used by people with different levels of IT knowledge require different levels of permissiveness with respect to the running of software, access to the Internet or to peripherals.
- Users with different tasks to perform and therefore with different needs require settings that allow access to different resources.
- Users that handle confidential or sensitive information require greater protection against threats and attempts to steal the organization's intellectual property.
- Computers in different offices require settings that allow them to connect to the Internet using a variety of communication infrastructures.
- Critical servers require specific security settings.

Overview of assigning settings to computers

In general, assigning settings to computers is a four-step process:

1. Creation of groups of similar computers or computers with identical connectivity and security requirements.
2. Assigning computers to the corresponding group.
3. Assigning settings to groups.
4. Deployment of settings to network computers.

All these operations are performed from the group tree, which can be accessed from the **Computers** menu at the top of the console. The group tree is the main tool for assigning settings quickly and to large groups of computers.

Administrators therefore have to put similar computers in the same group and create as many groups as there are different types of computers on the network.

For more information on the group tree and how to assign computers to groups, refer to "The Computer tree panel" on page 133

Immediate deployment of settings

Once a settings profile is assigned to a group, it will be applied to the computers in the group immediately and automatically, in accordance with the inheritance rules described in section "**Indirect assignment of settings: the two rules of inheritance**". Settings are applied to computers in just a few seconds.

*For more information on how to disable the immediate deployment of settings, refer to "***Configuring real-time communication***" on page* **201**

Multi-level tree

In medium-sized and large organizations, there could be a wide range of settings. To facilitate the management of large networks, Panda Endpoint Protection lets you create group trees with various levels so that you can manage all computers on the network with sufficient flexibility.

Inheritance

In large networks, it is highly likely that administrators will want to reuse existing settings already assigned to groups higher up in the group tree. The inheritance feature lets you assign settings to a group and then, in order to save time, automatically to all groups below this group in the tree.

Manual settings

To prevent settings from being applied to all inferior levels in the group tree, or to assign settings different from the inherited ones to a certain computer on a branch of the tree, it is possible to manually assign settings to groups or individual computers.

Default settings

Initially, all computers in the group tree inherit the settings established in the **All** root node. This node comes with a series of default settings created in Panda Endpoint Protection with the purpose of protecting all computers from the outset, even before the administrator accesses the console to establish a security setting profile.

Introduction to the various types of settings

Panda Endpoint Protection separates the settings to apply to managed computers into different types of profiles, each of which covers a specific aspect of security.

Below we provide you with an introduction to the different types of settings supported by Panda Endpoint Protection:

Configuration	Description
Users	Manage the user accounts that will be able to access the management console, the actions they can take (roles) and their activity. Refer to "Controlling and monitoring the management console" on page 53 for more information.
Per-computer settings	Configure settings templates to define the update frequency of the Panda Endpoint Protection security software installed on workstations and servers. This section also lets you define global settings to prevent tampering and unauthorized uninstallation of the protection. Refer to "Configuring the agent remotely" on page 193 for more information.
Network settings	Configure settings templates to define the language of the Panda Endpoint Protection software installed on workstations and servers, and the connection type used to connect to Panda Security's cloud. Refer to "Configuring the agent remotely" on page 193 for more information.
Network services	Define the behavior of the Panda Endpoint Protection software with regard to communication with neighboring computers on the customer's network. • **Proxy:** globally define the computers that will act as a proxy server to allow isolated computers with Panda Endpoint Protection installed to access the cloud. Refer to "Proxy role" on page 194 for more information. • **Cache**: globally define the computers that will act as repositories of signature files, security patches and other components used to update the Panda Endpoint Protection software installed across the network. Refer to "Cache/repository role" on page 195 for more information. • **Discovery**: globally define the computers responsible for discovering unprotected computers on the network. Refer to "Discovery computer role" on page 197 for more information.
VDI environments	Define the largest number of computers that can be simultaneously active in a non-persistent virtualization environment to facilitate license assignment.
My alerts	configure the alerts to be sent to the administrator's mailbox. Refer to "Alerts" on page 333 for more information.
Workstations and servers	Configure settings templates to define how Panda Endpoint Protection will behave to protect the computers on your network against threats and malware. Refer to "Security settings for workstations and servers" on page 207 for more information.
Android devices	Configure settings templates to define how Panda Endpoint Protection will behave to protect your Android tablets and smartphones against threats, malware and theft. Refer to "Security settings for Android devices" on page 223 for more information.

Table 10.1: Description of the types of settings available in Panda Endpoint Protection

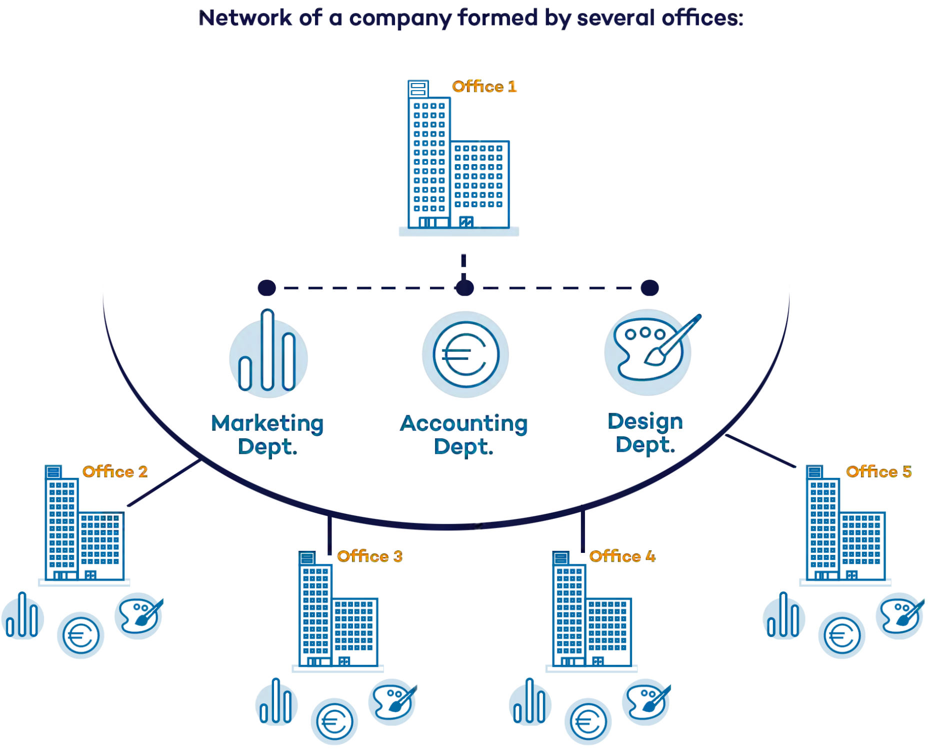
Configuration	Description
Patch management	Configure settings templates to define the discovery of the new security patches published by vendors for the Windows operating systems and third-party software installed across the network. Refer to "**Panda Patch Management (Updating vulnerable programs)**" on page 227 for more information.
Encryption	Configure settings templates to encrypt the content of your computers' internal storage devices. Refer to "**Panda Full Encryption (Device encryption)**" on page 271 for more information.

Table 10.1: Description of the types of settings available in Panda Endpoint Protection

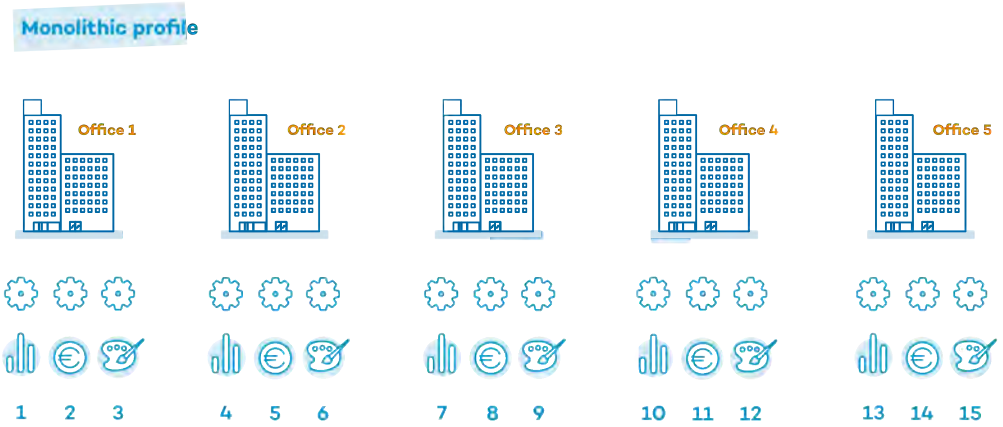
Modular vs monolithic settings profiles

By supporting different types of profiles, Panda Endpoint Protection uses a modular approach for creating and deploying the settings to apply to managed computers. The reason for using this modular approach and not just a single, monolithic profile that covers all the settings is to reduce the number of profiles created in the management console. This in turn will reduce the time that administrators have to spend managing the profiles created. The modular approach means that the settings are lighter than monolithic profiles, which result in numerous large and redundant settings profiles with little differences between each other.

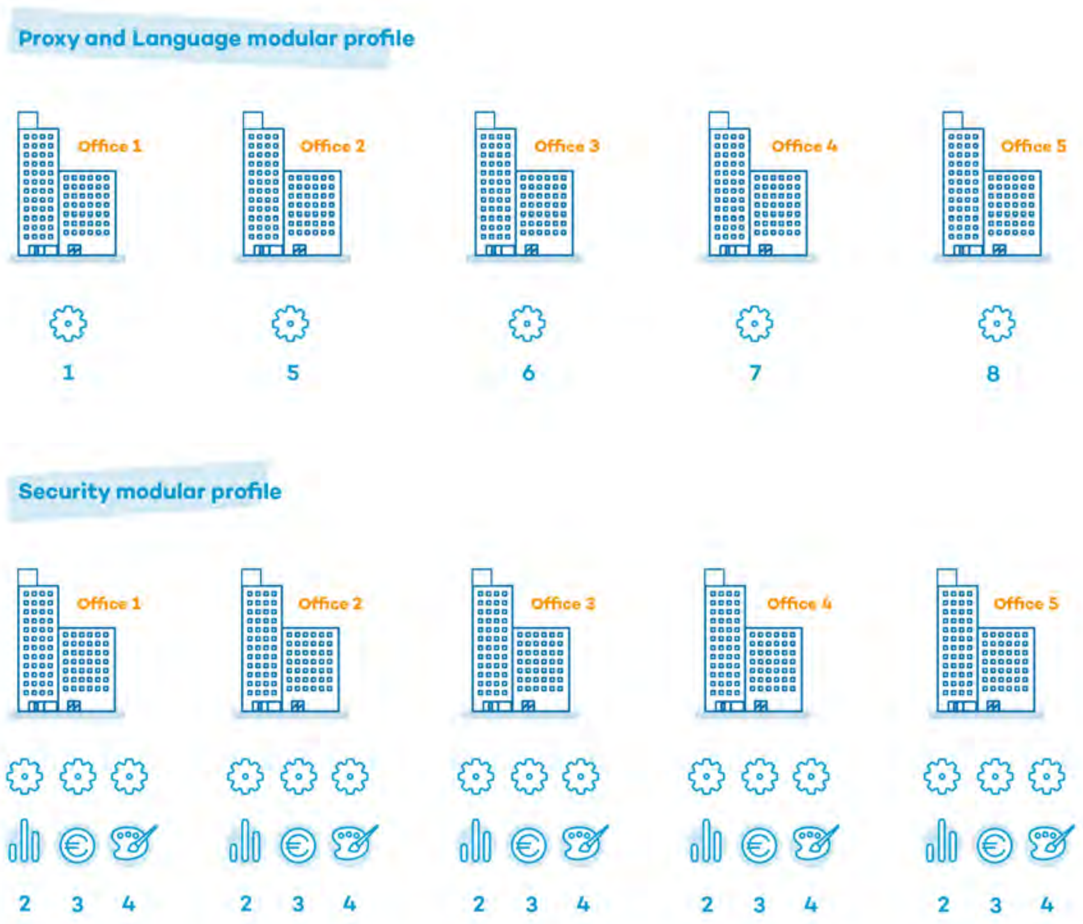
Case study: creating settings for several offices



In the following example, there is a company with five offices, each with a different communications infrastructure and therefore different proxy settings. Also, each office requires three different security settings, one for the Design department, another for the Accounts department and the other for Marketing.



If Panda Endpoint Protection implemented all configuration parameters in a single monolithic profile, the company would require 15 different settings profiles (5 x 3 =15) to adapt to the needs of all three departments in the company's offices.



However, as Panda Endpoint Protection separates the proxy settings from the security settings, the number of profiles needed is reduced (5 proxy profiles + 3 department profiles = 8) as the security profiles for each department in one of the offices can be reused and combined with the proxy profiles in other offices.

Settings management, permissions, and visibility

Permissions to manage settings

To manage settings, the user account that accesses the management console must have the permission associated with the type of settings to manage assigned to it. For more information about a specific permission, refer to "Understanding permissions" on page 57.

Settings	Permissions
Users	• Manage users and roles.
Per-computer settings	• Configure per-computer settings (updates, passwords, etc.).

Table 10.2: Permissions related to each type of settings template

Settings	Permissions
Network settings	• Modify network settings (proxies and cache).
Network services	• **Panda proxy tab**: to view the list of computers with the Panda proxy role assigned to them, no specific permission is required. To modify the computer list, the Modify network settings (proxies and cache) permission is required. • **Discovery tab**: to view the list of computers with the discovery computer role assigned to them, the Add, discover, and delete computers permission is required. To modify the computer list, the Modify network settings (proxies and cache) permission is required. • **Cache tab**: to view the list of computers with the cache role assigned to them, no specific permission is required. To modify the computer list, the Modify network settings (proxies and cache) and Add, discover, and delete computers permissions are required.
DVI environments	• To view these settings, no specific permission is required. • To modify the settings, the Add, discover, and delete computers permission is required.
My alerts	• The required permissions are related to the type of alert to be sent. Refer to "Alerts" on page 333.
Workstations and servers	• Configure security for workstations and servers. • View security settings for workstations and servers.
Android devices	• Configure security for Android devices. • View security settings for Android devices.
Patch management	• Configure patch management. • View patch management settings.
Encryption	• Configure computer encryption. • View computer encryption settings.

Table 10.2: Permissions related to each type of settings template

Computer visibility

To modify the recipients of a settings profile, the user account that modifies the settings template must have visibility into the computers to add. That is, a user account cannot add or delete computers in a settings profile if those computes are not visible to it.

Additionally, a user account can only modify an existing settings profile created by another user account if it has the right permissions for that action. The management console does not take into account the visibility of the account that modifies the settings: the changes made will be pushed to all the computers originally assigned to the settings, even if these settings were created by a user account with greater visibility than the account that modifies them.

Creating and managing settings

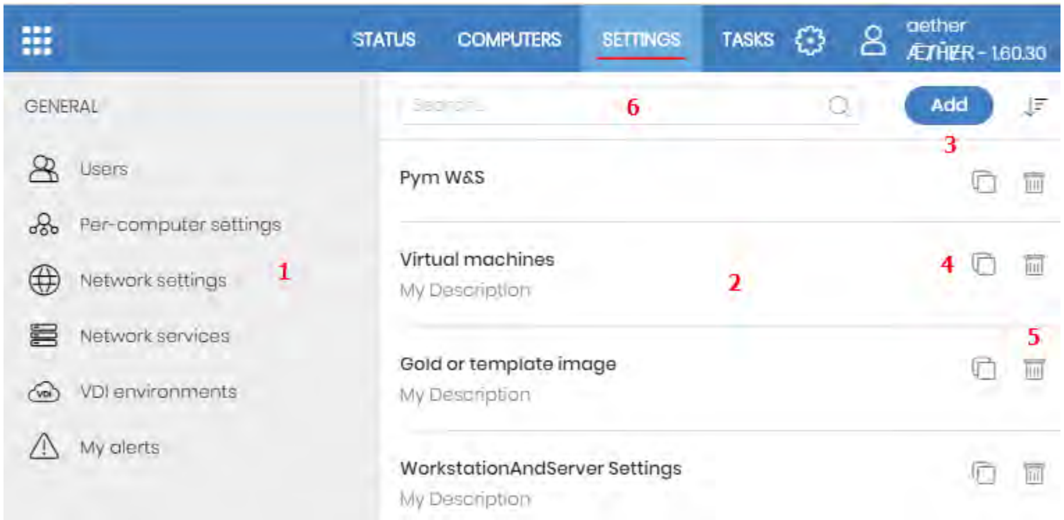


Figure 10.1: Screen for creating and managing settings profiles

Click Settings in the menu bar at the top of the screen to create, copy and delete settings. The panel on the left contains different sections corresponding to the various types of available settings profiles (1). In the right-hand panel, you can see the profiles of the selected category that have already been created (2), and the buttons for adding (3), copying (4) and deleting profiles (5). Use the search bar (6) to quickly find existing profiles.

The settings created from Panda Partner Center display the green tag Panda Partner Center. Placing the mouse pointer on the tag displays the following message: "These settings are managed from Panda Partner Center.

The settings created from Panda Partner Center are read only and only enable you to change their recipients. For more information, refer to Settings management for Panda-based products of the Panda Partner Center guide.

Creating settings

Click **Add** to display the window for creating settings**.** All profiles have a name and a description, which are displayed in the list of settings.

Sorting settings

Click the ↓☰ icon **(7)** to display a context menu with all available sort options:

- Sorted by creation date
- Sorted by name
- Ascending/Descending

Copying, deleting and editing settings

- Use the icons **(4)** and **(5)** to copy and delete a settings profile, although if it has been assigned to one or more computers, you won't be able to delete it until it has been freed up.
- Click a settings profile to edit it.

Before editing a profile, check that the new settings are correct. Please note that if the profile has already been assigned to any computers on the network, any changes you make will be applied automatically and immediately.

Manual and automatic assignment of settings

Once you have created a settings profile, it can be assigned to computers in two different ways:

- Manually (directly).
- Automatically through inheritance (indirectly).

Both procedures complement each other. It is highly advisable that administrators understand the advantages and limitations of each one in order to define the most simple and flexible computer structure possible, in order to minimize the workload of daily maintenance tasks.

Manual/direct assignment of settings

Manually assigning settings involves the administrator directly assigning profiles to computers or groups.

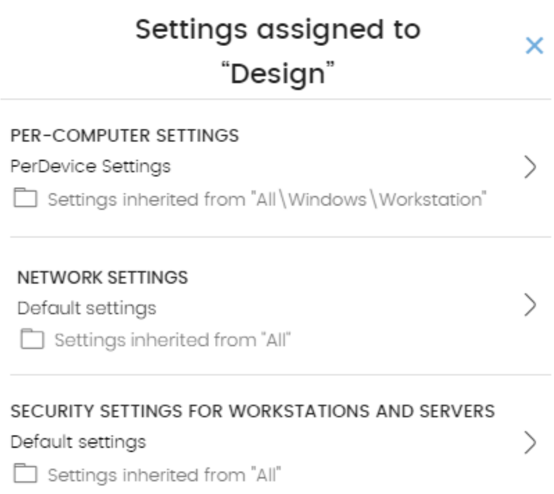
Once a settings profile has been created, there are three ways of assigning it:

- From the **Computers** menu at the top of the console (group three in the left-hand menu).
- From the target computer's details (accessible from the **Computers** list panel).
- From the profile itself when it is created or edited.

For more information about the group tree, refer to "Group tree" on page 140.

From the group tree

Follow these steps to assign a settings profile to the computers in a group:



Settings assigned to "Design"

×

PER-COMPUTER SETTINGS
PerDevice Settings
Settings inherited from "All\Windows\Workstation"

NETWORK SETTINGS
Default settings
Settings inherited from "All"

SECURITY SETTINGS FOR WORKSTATIONS AND SERVERS
Default settings
Settings inherited from "All"

Figure 10.2: Example of inherited and manually assigned settings

- Click the **Computers** menu at the top of the console, and select a group from the group tree in the left-hand menu.
- Click the group's context menu.
- Click **Settings**. A window will open with the profiles already assigned to the selected group and the type of assignment:
  - **Manual/Direct assignment**: the text **Directly assigned to this group** will be displayed.
  - **Inherited/Indirect assignment**: the text **Settings inherited from** will be displayed, followed by the name and full path of the group the settings were inherited from.
- Select a category of settings and then select the specific settings to apply. They will be deployed immediately to all members of the group and its sub-groups.

From the Computers list panel

Follow these steps to assign a settings profile to a specific computer:

- Go to the **Computers** menu at the top of the console, and click the group or filter that contains the computer to which you want to assign the settings. Click the computer in the list of computers in the right-hand panel to see its details.
- Click the **Settings** tab. This will display the various types of profiles assigned to the computer and the type of assignment:
  - **Manual/Direct assignment**: the text **Directly assigned to this group** will be displayed.
  - **Inherited/Indirect assignment**: the text **Settings inherited from** will be displayed, followed by the name and full path of the group the settings were inherited from.
- Select a category of settings and then select the specific settings to apply. They will be applied immediately to the computer.

From the settings profile itself

The quickest way to assign a settings profile to several computers belonging to different groups is via the settings profile itself.

Follow these steps to assign a settings profile to multiple computers or computer groups:

- Go to the **Settings** menu at the top of the console and select the type of settings that you want to assign from the left-hand side menu.
- Select a specific settings profile from those available, and click **Recipients**. A window will be displayed divided into two sections: **Computer groups** and **Additional computers.**
- Click the ⊕ buttons to add individual computers or computer groups to the settings profile.

- Click **Back**. The profile will be assigned to the selected computers and the new settings will be applied immediately.

Removing a computer from the list of computers that will receive a settings profile will cause it to re-inherit the settings assigned to the group it belongs to. A warning message will be displayed before the computer is removed.

Indirect assignment of settings: the two rules of inheritance

Indirect assignment of settings takes place through inheritance, which allows automatic deployment of a settings profile to all computers below the node to which the settings were initially assigned.

The rules that govern the relation between the two forms of assigning profiles (manual/direct and automatic/inheritance) are displayed below in order of priority:

- **Automatic inheritance rule**

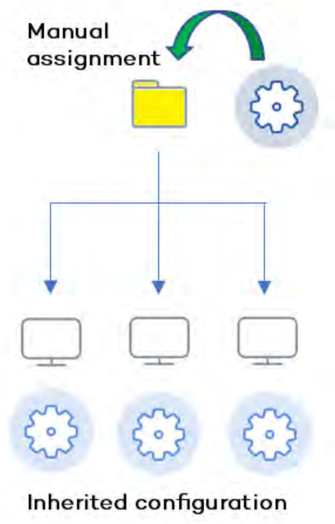


Figure 10.3: Inheritance/indirect assignment

A single compute or computer group automatically inherits the settings of the parent group (the group above it in the hierarchy).

The settings are manually assigned to the parent group, and automatically deployed to all child items (computers and computer groups with computers inside).

- **Manual priority rule**

Manually assigned profiles have priority over inherited ones.

By default, computers receive the settings inherited from a parent node. However, if at some point, you manually assign a new settings profile to a computer or computer group, all items below said computer or group will receive and apply the manually assigned settings and not the original inherited ones.

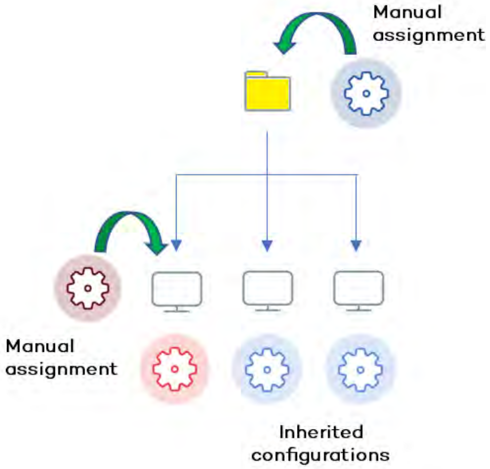


Figure 10.4: Priority of manually assigned settings over inherited ones

Inheritance limits

The settings assigned to a group (manual or inherited) are applied to all inferior branches of the tree, until manually assigned settings are found in a node.

This node and all of its child nodes will receive the manually assigned settings and not the original inherited ones.

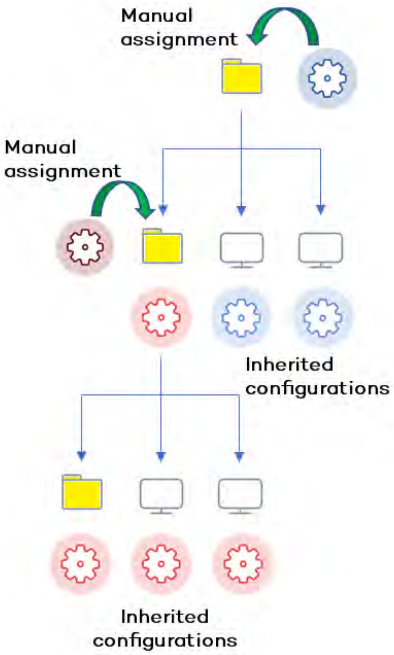


Figure 10.5: Inheritance limits

Overwriting settings

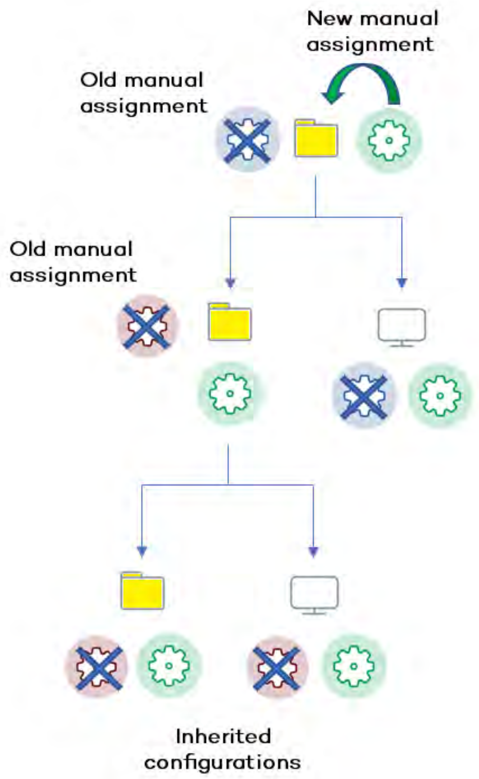


Figure 10.6: Overwriting manual settings

As illustrated in the previous point, the manual priority rule dictates that manually applied settings have preference over inherited ones.

Bearing that in mind, any change made to the settings in a higher-level node will affect the nodes below it in the following two ways:

- **If the child nodes don't have manual settings assigned**: the new settings assigned to the parent node will be applied to all its child nodes.
- **If any of the child nodes already have manual settings assigned**: the parent node will try to automatically apply the new settings it has received to all its child nodes. However, and based on the inheritance rules, those settings won't be applied to any child nodes that already have manual settings.

This way, when the system detects a change to the settings that has to be applied to subordinate nodes, and one or more of them have manually assigned settings (regardless of the level), a screen appears asking the administrator which option to apply: **Make all inherit these settings** or **Keep all settings.**

Make all inherit these settings

⚠ *Be careful when choosing this option as it is not reversible! All manually applied settings below the parent node will be lost, and the inherited settings will be applied immediately to all the computers. This could change the way* Panda Endpoint Protection *works on many computers.*

The new settings will be inherited by all nodes in the tree, overwriting any previous manual settings all the way down to the lowest level child nodes.

Keep all settings

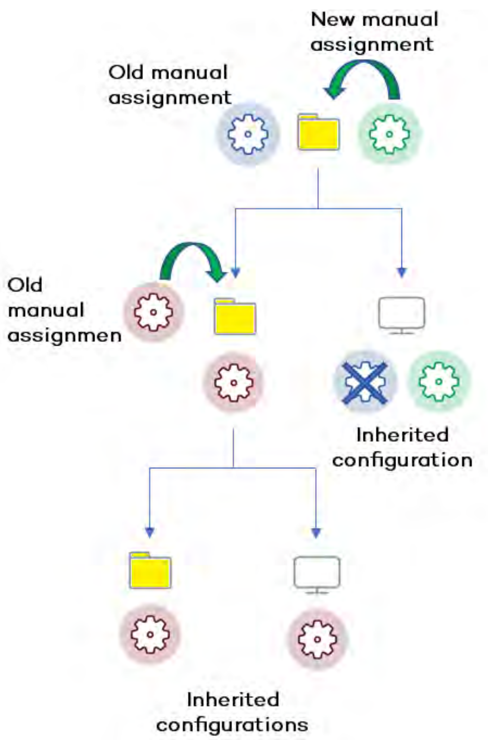


Figure 10.7: Keeping manual settings

If you choose **Keep all settings**, the new settings will be applied only to the subordinate nodes that don't have manually applied settings.

That is, if you choose to keep the existing manual settings, the propagation of the new inherited settings will stop at the first manually configured node. .

- **Deleting manually assigned settings and restoring inheritance**

Follow these steps to delete a manually assigned profile from a folder, and restore the settings inherited from a parent node:

- Go to the **Computers** menu at the top of the console. From the group tree in the panel on the left, click the group with the manually assigned settings that you want to delete.
- Click the branch's context menu icon and select **Settings**. A pop-up window will appear with the profiles assigned. Select the manually assigned profile you want to delete.
- At the bottom of the list you will see the button **Inherit from parent group** along with the settings that will be inherited if you click it, and the group from which they will be inherited.

Moving groups and computers

When moving computers from one branch in the tree to another, the way Panda Endpoint Protection operates with respect to the settings to apply will vary depending on whether the items moved are groups or individual computers.

Moving individual computers

If you move a single computer that has manual settings assigned, those settings will be kept in the new location. However, if the computer to move has inherited settings, they will be overwritten with the settings established in the new parent group.

Moving groups

If you move a group, Panda Endpoint Protection will display a window asking the following question: "**Do you want the settings inherited by this group to be replaced by those in the new parent group?**"

- If you answer **YES**, the process will be the same as with moving a single computer: the manual settings will be kept and the inherited settings overwritten with those established in the parent node.

- If the answer is **NO**, the manual settings will also be kept but the original inherited settings of the moved group will have priority and as such will become manual settings.

Exceptions to indirect inheritance

All computers that are integrated into a native group in the Web console receive from Panda Endpoint Protection the network settings assigned to the target group using the standard indirect assignment/inheritance mechanism. However, if a computer is integrated into an Active Directory or IP-based group in the Web console, the network settings must be manually assigned. This change in the way network settings are assigned will in turn result in a change in behavior when that computer is subsequently moved from one group to another: it will no longer indirectly inherit the network settings assigned to the target group, but will retain its own.

This particular behavior of the inheritance feature is due to the fact that, in mid-size and large companies, the department that manages security may not be the same as the one that manages the company's Active Directory. For this reason, a group membership change made by the technical department that maintains the Active Directory can inadvertently lead to a change of network settings within the Panda Endpoint Protection console. This situation could leave the protection agent installed on the affected computer without connectivity and therefore with less protection. By manually assigning network settings, you prevent settings changes when a computer changes groups in the Panda Endpoint Protection console due to a group change in the company's Active Directory.

Viewing assigned settings

The management console provides four methods of displaying the settings profiles assigned to a group or a single computer:

- From the group tree.
- From the **Settings** menu at the top of the console.
- From the computer's **Settings** tab.
- From the exported list of computers.

Viewing settings from the group tree

- Click the **Computers** menu at the top of the console. Then, click the ■ tab at the top of the left-side panel in order to display the group tree.
- Click the context menu of the relevant branch, and select **Settings** from the pop-up menu displayed. A window will open with the settings profiles assigned to the folder.

Below is a description of the information displayed in this window:

- **Settings type**: indicates the settings class the profile belongs to.

- **Name of the settings profile**: name given by the administrator when creating the settings.
- Inheritance type:
    - **Settings inherited from...:** 🗀 the settings were assigned to the specified parent folder and every computer on the branch has inherited them.
    - **Directly assigned to this group:** → the settings applied to the computers are those the administrator assigned manually to the folder.

Viewing settings from the Settings menu at the top of the console

- Go to the **Settings** menu at the top of the console and select a type of settings from the left-hand side menu.
- Select the relevant settings profile from those available.
- If the settings profile has been assigned to one or more computers or groups, a button called **View computers** will be displayed.
- Click the **View computers** button. You will be taken to the **Computers** screen, which will display a list of all computers with those settings assigned, regardless of whether they were assigned individually or through computer groups. At the top of the screen you'll see the filter criteria used to generate the list.

Viewing settings from a computer’s Settings tab

Go to the **Computers** menu at the top of the console. Select a computer from the panel on the right and click it to view its details. Go to the **Settings** tab to see the profiles assigned to the computer.

Viewing settings from the exported list of computers

From the computer tree (group tree or filter tree), click the general context menu and select **Export**:

*Refer to “***Fields in the 'Computers list' exported file***” on page* 149.

Chapter 11

Configuring the agent remotely

Administrators can configure various aspects of the Panda agent installed on the computers on their network from the Web console:

- Define the computer's role towards the other protected workstations and servers.
- Protect the Panda Endpoint Protection client software from unauthorized tampering by hackers and advanced threats (APTs).
- Define the visibility of the agent on the workstation or server, and its language.
- Configure the communication established between the computers on the network and the Panda Security cloud.

CHAPTER CONTENT

Configuring the Panda agent role

The Panda agent installed on the Windows computers on your network can have three roles:

- Proxy
- Discovery computer
- Cache

To assign a role to a computer with the Panda agent installed, click the **Settings** menu at the top of the console. Then, click **Network services** from the menu on the left. Three tabs will be displayed: **Panda Proxy**, **Cache**, and **Discovery**.

⚠ *Only computers with a Windows operating system can take on the Proxy, Cache, or Discovery Computer roles.*

Proxy role

Panda Endpoint Protection allows computers without direct Internet access to use the proxy installed on the organization's network. If no proxy is accessible, you can assign the proxy role to a computer with Panda Endpoint Protection installed.

⚠ *Proxy computers cannot download patches or updates via the* Panda Patch Management *module. Only computers with direct access to the Panda Security cloud or with indirect access via a corporate proxy can download patches.*

Requirements for configuring a computer as a proxy server

- The computer must be a Windows computer with Panda Endpoint Protection installed.
- Support for the 8.3 file naming format. Refer to the following MSDN article https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN for information on how to enable this feature.
- TCP port 3128 must not be in use by other applications.
- The computer's firewall must be configured to allow incoming and outgoing traffic on port 3128..
- The name of the computer with the proxy role assigned to it must be resolved from the computer that uses it.

Configuring a computer as a proxy server

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Panda proxy** tab. A list will be displayed showing all computers already configured as a proxy.
- Click **Add Panda proxy**. A window will be displayed with all computers managed by Panda Endpoint Protection that meet the necessary requirements to work as a proxy for the network.
- Use the search box to find a specific computer and click it to add it to the list of computers with the proxy role assigned.

Revoking the proxy role assigned to a computer

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Panda proxy** tab. This will display all computers configured as a proxy.
- Click the 🗑 icon of the computer whose proxy role you want to revoke.

*To configure the use of a computer with the proxy role assigned, refer to "***Configuring proxy-based Internet access lists***".*

Cache/repository role

Panda Endpoint Protection lets you assign the cache role to one or more computers on your network. These computers will automatically download and store all files required by other computers with Panda Endpoint Protection installed. This saves bandwidth as it won't be necessary for each computer to separately download the updates they need. All updates will be downloaded centrally and once for all computers that require them.

Cached items

A computer with the cache role assigned can cache the following items for different time periods based on their type:

- **Signature files**: until they are no longer valid.
- **Installation packages**: until they are no longer valid.
- **Update patches for Panda Patch Management**: 30 days.

*For a computer to be able to download patches from another computer with the cache role assigned to it, both computers must belong to the same subnet. Due to this, the cache computer must be assigned automatically. Refer to "***Configuring downloads via cache computers***".*

Cache node capacity

The capacity of a cache node is determined by the number of simultaneous connections it can accommodate in high load conditions and by the type of traffic managed (signature file downloads, installer downloads, etc.). Approximately, a computer with the cache role assigned can serve around 1,000 computers simultaneously.

Configuring a computer as a cache

- Click the **Settings** menu at the top of the console. Then, click **Network Services** from the menu on the left and select the **Cache** tab.
- Click **Add cache computer**.
- Use the search tool at the top of the screen to quickly find those computers you want to designate as cache.
- Select a computer from the list and click **OK.**

From then on, the selected computer will have the cache role and will start downloading all necessary files, keeping its repository automatically synchronized. All other computers on the same subnet will contact the cache computer for updates.

Revoking the cache role

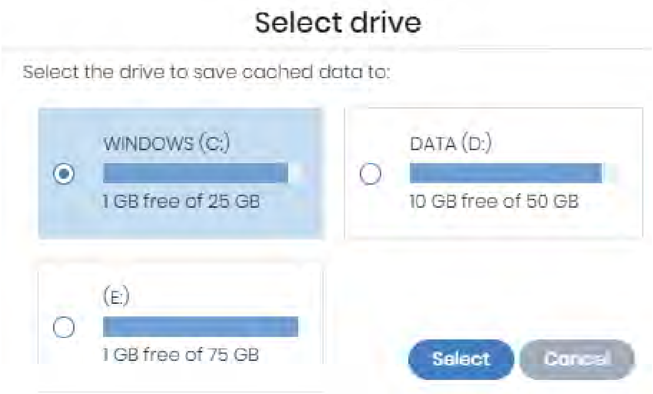
- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Cache** tab.
- Click the 🗑 icon of the computer that you want to stop acting as a cache.

Setting the storage drive

You can configure the Panda Endpoint Protection agent to store cached items on a specific volume/drive of the cache computer. Please note that the folder path on the drive will be fixed. Follow these steps to configure this option:

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the menu on the left and click the **Cache** tab.
- From a computer with the cache role assigned and which has already reported its status to the cloud, click the **Change** link. A window will appear with all available drives.
- The following information is displayed for each drive: volume name, mapped drive, free space, and

total space.



Select drive

Select the drive to save cached data to:

● WINDOWS (C:) 1 GB free of 25 GB

○ DATA (D:) 10 GB free of 50 GB

○ (E:) 1 GB free of 75 GB

Figure 11.1: Volume selection window for a computer with the cache role assigned

- To view the percentages of used and free space, hover the mouse pointer over the bars. A tooltip with the relevant information will be displayed.
- Only drives with 1 GB or more of free space will be available for selection. Select the drive where you want to store the cached items and click the **Select** button. Panda Endpoint Protection will start copying the cached items. Once the process is complete, they will be deleted from their original location.

You can only select the drive where you want to store the cached items on computers which have reported their status to the Panda Endpoint Protection server. If this condition is not met, the drive that stores the Panda Endpoint Protection installation files will be selected by default. Once the status has been reported, the ***Change*** *link for the computer with the cache role assigned will be displayed, and you will be able to select the storage drive. It may take several minutes for a computer to report its status.*

If there is not enough free space or a write error occurs when selecting the storage drive, a message will be displayed under the computer with the cache role assigned indicating the source of the problem.

Discovery computer role

Click the **Settings** menu at the top of the console and then **Network services** from the menu on the left. You'll find the **Discovery** tab, which is directly related to the installation and deployment of Panda Endpoint Protection across the customer's network.

Refer to "Computer discovery" on page 90 for more information about the Panda Endpoint Protection discovery and installation processes.

Configuring proxy-based Internet access lists

Panda Endpoint Protection lets you assign computers on the network one or more Internet connection methods, based on the resources available in the company's IT infrastructure.

Panda Endpoint Protection supports various Internet access methods which can be configured by the administrator and which it turns to when it needs to connect to Panda Security's cloud. Once selected, the access method won't change until it is no longer accessible, when Panda Endpoint Protection will move to the next method in the list until it finds one that is valid. Once it gets to the end of the list, it will go back to the beginning until all connection methods have been tried at least once.

The connection types supported by Panda Endpoint Protection are as follows:

Proxy type	Description
Do not use proxy	Direct access to the Internet. Computers access the Panda Security cloud directly to download updates and send status reports. If you select this option, the Panda Endpoint Protection software will communicate with the Internet using the computer settings.
Corporate proxy	Access to the Internet via a proxy installed on the company's network. • **Address:** the proxy server's IP address. • **Port:** the proxy server's port. • **The proxy requires authentication**: select this option if the proxy requires a user name and password. • **User name**: the user name of an existing proxy account. • **Password**: the password of the proxy account.
Automatic proxy discovery using Web Proxy Autodiscovery Protocol (WPAD)	Queries the network via DNS or DHCP to get the discovery URL that points to the PAC configuration file. Alternatively, you can directly specify the HTTP or HTTPS resource that hosts the PAC configuration file.
Panda Endpoint Protection proxy	Access via the Panda Endpoint Protection agent installed on a computer on the network. This option lets you centralize all network communications through a computer with the Panda agent installed. To configure a computer to access the Internet via a Panda Endpoint Protection proxy, click the **Select** computer link. A window will open with a list of all available computers on the network with the proxy role. Select one of the computers and click the Add button.

Table 11.1: Types of Internet access methods supported by Panda Endpoint Protection

*You can configure an access list consisting of multiple computers with the proxy role. To do that, first assign the Panda Endpoint Protection proxy role to one or more computers on the network with Panda Endpoint Protection installed, using the steps described in section "*Configuring a computer as a proxy server*".*

Configuring an access list

To configure an access list, create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the Add button or select an existing settings profile in order to edit it.
- In the Proxy section, click the ⊕ icon. A window will be displayed, listing all available connection types.
- Select one of the connection types (table 11.1) and click the **OK** button. The connection type will be added to the list.
- To modify the order of the connection methods, select an item by clicking its checkbox and use the ↑ and ↓ arrows to move the item up and down in the list.
- To delete a connection method, click the 🗑 icon.
- To change a connection method, select it by clicking its checkbox and click the ✎ icon A window will be displayed prompting you to select a new method.

Fallback mechanism

- **Direct connection**: Panda Endpoint Protection tries to connect directly to the Panda Security cloud, if this option was not previously configured in the access list.
- **Internet Explorer**: Panda Endpoint Protection tries to retrieve the computer's Internet Explorer proxy settings with the profile of the user currently logged in to the computer.
  - If the proxy requires explicit credentials, this method cannot be used.
  - If Internet Explorer is configured to use a PAC (Proxy Auto-Config) file, the Panda agent will use the URL in the configuration file, provided the resource access protocol is HTTP or HTTPS.
- **WinHTTP**: Panda Endpoint Protection reads the default proxy settings.
- **WPAD**: the solution queries the network via DNS or DHCP to retrieve the discovery URL that points to the PAC configuration file, if this option was not previously configured in the access list.

The computer will try to exit the fallback mechanism multiple times per day, checking the access list configured by the administrator. This way, it checks to see whether the connection mechanisms defined for the computer are available again.

Configuring downloads via cache computers

Access to computers with the cache role assigned to speed up updates and patch downloads is only available for Windows computers.

There are two ways to use computers with the cache role:

- **Automatic mode**: the computer that starts the download will use the cache computers found on the network that meet the requirements specified in section "**Requirements for using a cache computer in automatic mode**". If multiple cache computers are found, downloads will be balanced so as not to overload a single cache computer.
- **Manual mode**: in this mode, it is the administrator who manually sets the cache computer that will be used to download data from Panda Security's cloud. Manually selected cache nodes have the following differences from automatically selected ones:
  - The fact that a computer has multiple cache nodes assigned does not mean that downloads will be shared among them.
  - If the first computer in the list is not available, the solution will move to the next computer until it finds one that works. If it cannot find any available computers, it will try to access the Internet directly.

Requirements for using a cache computer in automatic mode

- The computer with the cache role assigned and the computer that downloads items from it must be on the same subnet. If a cache computer has multiple network cards, it will be able to act as a repository on each network segment to which it is connected.

It is advisable to designate a computer with the cache role on each network segment on the corporate network

- All other computers will automatically discover the presence of the cache node and will redirect their update requests to it.
- A protection license has to be assigned to the cache node in order for it to operate.
- The firewall must be configured to allow incoming and outgoing UPnP/SSDP traffic on UDP port 21226 and TCP port 18226.

Discovery of cache nodes

As soon as you designate a computer as cache, it will broadcast its status to the network segments to which its interfaces connect. From then on, all workstations and servers set to automatically detect cache nodes will receive that notification and will connect to the cache computer. Should there be more than one designated cache node on a network segment, all computers on the subnet will connect to the most appropriate node based on the amount of free resources it has.

Additionally, from time to time, all computers on the network set to automatically detect cache nodes will check to see if there are new nodes with the cache role.

Configuring assignment of cache nodes

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and select one of the existing settings profiles.

- Go to the **Cache** section and select one of the following two options:
    - **Automatically use the cache computers seen on the network**: the computers that receive these settings will automatically look for cache nodes on their network segment.
    - **Use the following cache computers (in order of preference)**: click the ⊕ icon to add computers with the cache role assigned and set up a list of cache nodes. The computers that receive these settings will connect to the cache nodes specified in the list in order to download files.

Configuring real-time communication

Panda Endpoint Protection communicates with Aether Platform in real time to retrieve the settings configured in the console for protected computers. Therefore, only a few seconds elapse between the time the administrator assigns a settings profile to a computer and the time it is applied.

Real-time communication between the protected computers and the Panda Endpoint Protection server requires that each computer have an open connection at all times. However, in those organizations where the number of open connections may have a negative impact on the performance of the installed proxy it may be advisable to disable real-time communication. The same applies to those organizations where the traffic generated when simultaneously pushing configuration changes to a large number of computers may impact bandwidth usage.

Requirements for real-time communication

- Real-time communications are compatible with all operating systems supported by Aether, except Windows XP and Windows 2003.
- If a computer accesses the Internet via a corporate proxy, the HTTPS connections must not manipulated. Many proxies use Man-in-the-Middle techniques to scan HTTPS connections or work as cache proxies. When that happens, real-time communications won't work.

Disabling real-time communication

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Add** button or select an existing settings profile to edit it.
- In the **Proxy** section, click **Advanced options** and clear the **Enable real-time communication** checkbox.

If you disable real-time communication, your computers will communicate with the **Panda Endpoint Protection** server every 15 minutes.

Configuring the agent language

To set up the language of the Panda agent for one or more computers, you must create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Add** button or select an existing settings profile to edit it.
- Go to the **Language** section and select a language from the list:
  - German
  - Spanish
  - Finnish
  - French
  - Hungarian
  - English
  - Italian
  - Japanese
  - Portuguese
  - Russian
  - Swedish

If the language is changed while the Panda Endpoint Protection local console is open, the system will prompt the user to restart it. This does not affect the security of the computer.

Configuring agent visibility

In those companies where the security service is 100% managed by the IT Department, there is no need for the Panda Endpoint Protection agent icon to be displayed in the notification area of managed computers. Follow the steps below to show or hide the icon:

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Open the **Preferences** section and select or clear the **Show icon in the system tray** option.

Configuring the Anti-Tamper protection and password

Anti-Tamper protection

Many advanced threats make use of techniques for disabling the security software installed on computers. The Anti-Tamper protection prevents unauthorized modification of the way the protection operates, preventing the software from being stopped, paused, or removed, by way of a password.

Panda Endpoint Protection's Anti-Tamper protection works as follows:

- The default **Per-computer settings** provided by the solution include a unique, predefined password for each customer. This password cannot be changed as all default settings are read-only.
- The **Per-computer settings** generated by users allow the Anti-Tamper protection to be enabled or disabled according to the organization's needs.

The passwords set when creating security settings must be between 6 and 15 characters long.

Enabling / disabling the Anti-Tamper protection

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Expand section **Security against unauthorized protection tampering:**
  - **Enable Anti-Tamper protection**: this prevents users and certain types of malware from stopping the protections. Enabling this option requires setting up a password which will be required if, for example, the administrator or a support team member needs to temporary disable the protection from the local computer in order to diagnose a problem. Use the switch on the right side to enable and disable this feature in the settings you create.

⚠ *Turning off the **Enable Anti-Tamper protection** or **Request password to uninstall the protection from computers** security options will cause a security warning to be displayed when saving the settings. It is not recommend to turn off these security options.*

Password-protection of the agent

Administrators can set up a password to prevent end users from changing the protection features or completely uninstalling the Panda Endpoint Protection software from their computers.

Setting up the password

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Expand section **Security against unauthorized protection tampering:**

- **Request password to uninstall the protection from computers**: this option prevents users from uninstalling the Panda Endpoint Protection software.
- **Allow the protections to be temporarily enabled/disabled from a computer's local console**: this option allows administrators to manage a computer's security parameters from its local console. Enabling this option requires setting up a password.

If a computer loses its assigned license, either because it is manually removed or because it expires or is canceled, the Anti-Tamper protection and the password-based uninstallation protection will be disabled.

Part 5

Managing network security

Chapter 12: Security settings for workstations and servers

Chapter 13: Security settings for Android devices

Chapter 14: Panda Patch Management (Updating vulnerable programs)

Chapter 15: Panda Full Encryption (Device encryption)

Chapter 12

Security settings for workstations and servers

All protection features provided by Panda Endpoint Protection can be managed through the security settings for workstations and servers. This section allows administrators to protect corporate assets against computer threats of many different types by assigning security settings profiles to them.

Next is a description of the options available for configuring the security of your workstations and servers. It also includes practical recommendations on how to protect all computers on your network, without negatively impacting users' activities.

For additional information about the 'Workstations and servers' module, refer to:

- "**Creating and managing settings**" on page 183: information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**" on page 53: managing user accounts and assigning permissions.

CHAPTER CONTENT

Accessing the security settings for workstations and servers

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Workstations and servers** from the side menu.
- Click the **Add** button to open the **Workstations and servers** settings window.

Required permissions

Permission	Access type
Configure security for workstations and servers	Create, edit, delete, copy, or assign settings for workstations and servers.
View security settings for workstations and servers	View the 'Workstations and servers' settings.

Table 12.1: Permissions required to access the 'Workstations and servers' settings

Introduction to the security settings

The parameters for configuring the security of workstations and servers are divided into various sections. Clicking each of them displays a drop-down panel with the associated options. Below we offer a brief explanation of each section:

Section	Description
General	Lets you configure updates, the removal of competitor products, and file exclusions from scans.
Antivirus	Lets you configure the parameters that control the traditional anti-malware protection against viruses and threats.
Firewall (Windows devices)	Lets you configure the parameters that control the firewall and the IDS against network attacks.
Device control (Windows devices)	Lets you configure the parameters that control user access to the peripheral devices connected to the computer.

Table 12.2: Available modules in Panda Endpoint Protection

Not all features are available for all supported platforms. Below is a summary of the Panda Endpoint Protection security features that are available for each supported platform:

Feature	Windows	macOS	Linux
Antivirus (1)	X	X	X
Firewall & IDS	X		
Email protection	X		
Web protection	X	X	X
Device control	X		

Table 12.3: Security features per platform

General settings

The general settings let you configure how Panda Endpoint Protection behaves with respect to updates, the removal of competitor products, and file and folder exclusions from scans.

Local alerts

Field	Description
Show malware, firewall, and device control alerts	Enter a descriptive message to inform users of the reason for the alert. The Panda Endpoint Protection agent will show a pop-up window with the configured text.
Show an alert every time the Web access control feature blocks a page	Shows a pop-up window on the workstation or server every time Panda Endpoint Protection blocks access to a Web page.

Table 12.4: Fields in the ‘Local alerts’ section

Updates

*Refer to “**Product updates and upgrades**” on page **123** for more information on how to update the agent, the protection, and the signature file of the client software installed on users' computers.*

Uninstall other security products

> *Refer to "Protection deployment overview" on page 78 for more information on how to configure the action to take if another security product is already installed on users' computers.*
>
> *Refer to Supported uninstallers for a full list of the competitor products that* Panda Endpoint Protection *uninstalls automatically from users' computers.*

Files and paths excluded from scans

Configure items on your computers that won't be deleted, or disinfected when scanning for malware.

> *This setting disables the antivirus protection. Because this setting can cause potential security holes, Panda recommends that you only use it to resolve performance problems.*

Disk files

Lets you select the files on the hard disk of your protected computers that won't be scanned or deleted by Panda Endpoint Protection.

Field	Description
Extensions	Lets you specify the extensions of files that won't be scanned.
Directories	Lets you specify folders whose contents won't be scanned.
Files	Lets you specify files that won't be scanned. You can use wildcard characters '*' and '?'.
Recommended exclusions for Exchange servers	Click Add to automatically load a series of Microsoft-recommended exclusions to optimize the performance of Panda Endpoint Protection on Exchange servers.

Table 12.5: Disk files that won't be scanned by Panda Endpoint Protection

Exclude the following email attachments

This option lets you specify the extensions of attachments that Panda Endpoint Protection won't scan.

Antivirus

This section lets you configure the general behavior of the signature-based antivirus engine.

Field	Description
File antivirus	Lets you enable/disable the antivirus protection for the file system.
Email antivirus	Lets you enable/disable the antivirus protection for the mail client installed on users' computers. Panda Endpoint Protection will detect threats received over the POP3 protocol and their encrypted variants.
Web browsing antivirus	Lets you enable/disable the antivirus protection for the Web client installed on users' computers. Panda Endpoint Protection will detect threats received over the HTTP protocol and their encrypted variants.

Table 12.6: Antivirus protection modules available in Panda Endpoint Protection

The action taken by Panda Endpoint Protection when finding a malware or suspicious file is defined by Panda Security's anti-malware laboratory, and is based on the following criteria:

- **Known malware files when disinfection is possible**: the original file is replaced with a harmless, disinfected copy.
- **Known malware files when disinfection is not possible**: the solution makes a backup copy of the infected file and the original file is deleted.

Threats to detect

Lets you configure the types of threats that Panda Endpoint Protection will search for and remove from the file system, mail client and Web client installed on users' computers..

Field	Description
Detect viruses	Detects files that contain patterns classified as dangerous
Detect hacking tools and PUPs de hacking y PUPs	Detects unwanted programs (programs with intrusive ads, browser toolbars, etc.) and tools used by hackers to gain access to systems.
Block malicious actions	Enables heuristic and contextual analysis technologies designed to locally monitor process behavior and detect suspicious activity.
Detect phishing	Detects fraudulent emails and websites.
Do not detect threats at the following addresses and domains	Whitelist of addresses and domains that won't be scanned for phishing attacks. All addresses and domains that start like those specified will also be whitelisted. Therefore, to whitelist an address or domain it is enough to enter a part of it. Also, the whitelist is not case-sensitive.

Table 12.7: Malware types detected by Panda Endpoint Protection's antivirus protection

File types

This section lets you specify the types of files to be scanned by Panda Endpoint Protection

Field	Description
Scan compressed files on disk	Decompresses compressed files and scans their contents for malware.
Scan compressed files in emails	Decompresses email attachments and scans their contents for malware.
Scan all files regardless of their extension when they are created or modified (Not recommended)	For efficiency and performance reasons, we recommend that you don't scan all types of files as, technically, many types of data files don't pose a threat to the security of computer networks.

Table 12.8: File types scanned by Panda Endpoint Protection's antivirus protection

Firewall (Windows computers)

Panda Endpoint Protection monitors the communications sent and received by each computer on the network, blocking all traffic that matches the rules defined by the administrator. This module is compatible with both IPv4 and IPv6, and includes multiple tools for filtering network traffic:

- **System rules**: these rules describe communication characteristics (ports, IP addresses, protocols, etc.), allowing or denying the data flows that match the configured rules.
- **Program rules**: rules that allow or prevent the programs installed on users' computers from communicating with other computers.
- **Intrusion detection system**: detects and rejects malformed traffic patterns that can affect the security or performance of protected computers.

Operating mode

This is defined through the option **Let computer users configure the firewall**:

- **Enabled (user-mode or self-managed firewall)**: this option allows end users to manage the firewall protection from the local console installed on their computers.
- **Disabled (administrator-mode firewall)**: the administrator configures the firewall protection of all computers on the network through settings profiles.

Network type

Laptops and mobile devices can connect to networks with different security levels, from public Wi-Fi networks, such as those in Internet cafés, to managed and limited-access networks, such as those found in companies. Network administrators have two options to set the default behavior of the firewall protection: manually select the type of network that the computers in the configured profile usually connect to, or let Panda Endpoint Protection select the most appropriate network type..

Network type	Description
Public network	These are the networks found in Internet cafés, airports, etc. Limitations must be established on the way protected computers are used and accessed, especially with regard to file, resource and directory sharing.
Trusted network	These are office and home networks. The computer is perfectly visible to the other computers on the network and vice versa. There are no limitations on sharing files, resources or directories.
Detect automatically	The network type (public network or trusted network) is selected automatically based on a series of requirements the user's computer must meet. Click the link **Configure rules to determine when a computer is connected to a trusted network**.

Table 12.9: Network types supported by the firewall

Panda Endpoint Protection will behave differently and will apply different predetermined rules automatically depending on the type of network selected. These predetermined rules are referred to as "Panda rules" in the Program rules and Connection rules sections.

⚠ *The network type is a concept that must be applied individually to each network interface on a computer. That is, computers with multiple network interfaces can have different network types assigned, and therefore can have different firewall rules for each network interface.*

Configuring criteria for determining the network type

Panda Endpoint Protection lets you define one or more criteria that computers protected by the firewall must meet in order to automatically select the **Trusted network** setting. If none of these conditions is met, then the network type selected for the network interface will be **Public network**.

A criterion is a rule to determine whether a computer's network interface is deemed to be connected to a trusted network. This association takes place by resolving a domain previously defined on your company's internal DNS server: if the computer is capable of connecting to the DNS server and resolving the configured domain, then it will mean that it is connected to the company's network, and the firewall will assume that the computer is connected to a trusted network.

Below is an example of how to configure these criteria:

- Add an A-type record with the following name to the primary zone of your organization's internal DNS server: "`firewallcriterion`". In this example, the organization's primary zone will be "`mycompany.com`". The IP address associated with the new record is unimportant, since it is not used to validate the criterion. "`firewallcriterion.mycompany.com`" will be the domain that the computer will attempt to resolve in order to check that it is connected to the company's network.
- Restart the DNS server if required and make sure "`firewallcriterion.mycompany.com`" is resolved

successfully from all segments of the internal network with the tools `nslookup`, dig or host.

- From the Panda Endpoint Protection console, click the link **Configure rules to determine when a computer is connected to a trusted network**. A window will be displayed for you to enter the following data:
  - **Criterion name**: descriptive name of the rule you want to configure.
  - **DNS server**: IP address of the DNS server in the organization's structure that will receive the resolution request.
  - **Domain**: request sent by the computer to the DNS server for resolution.
  - Click the **OK** button, then **Save** and then **Save** once again.
- Once the criterion has been configured and applied, the computer will attempt to resolve the "`firewallcriterion.mycompany.com`" domain on the specified DNS server every time an event occurs on the network interface (connect, disconnect, IP address change, etc.). If DNS resolution succeeds, then the settings assigned to the trusted network will be assigned to the network interface used.

Program rules

This section lets you configure which programs can communicate with the local network/Internet, and which cannot.

To build an effective protection strategy it is necessary to follow the steps below in the order listed:

1. Set the default action.

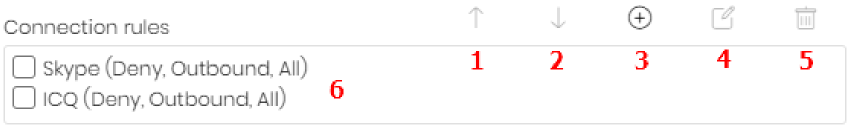
Action	Description
Allow	Implements a permissive strategy based on always accepting connections for all programs for which you haven't configured a specific rule in step 3. This is the default, basic mode.
Deny	Implements a restrictive strategy based on always denying connections for all programs for which you haven't configured a specific rule in step 3. This is an advanced mode, as it requires adding rules for every frequently used program. Otherwise, they will not be allowed to communicate, affecting their performance.

Table 12.10: Types of default actions supported by the firewall for the programs installed on computers

2. Enable Panda Security rules.

This option enables Panda Security's predefined rules for the selected network type.

3. Add rules to define the specific behavior of your applications



Connection rules

□ Skype (Deny, Outbound, All)
□ ICQ (Deny, Outbound, All)

Figure 12.1: Edit controls for program rules

You can change the order of the program rules, as well as adding, editing or removing them by using the Up **(1)**, Down **(2)**, Add **(3)**, Edit **(4)** and Delete **(5)** buttons on the right. Use the checkboxes **(6)** to select the rules to apply each action to.

The following fields are mandatory when you are creating a rule:

- **Description**: enter a description for the rule.
- **Program**: select the program whose behavior you want to control.
- **Connections allowed for this program**: define which connections will be allowed for the program::

Field	Description
Allow inbound and outbound connections	The program can connect to the Internet/local network and allows other programs or users to connect to it. There are certain types of programs that need these permissions to work correctly: file sharing programs, chat applications, Internet browsers, etc.
Allow outbound connections	The program can connect to the Internet/local network, but won't accept inbound connections from other users or applications.
Allow inbound connections	The program accepts connections from programs or users from the Internet/local network, but won't be allowed to establish outbound connections.
Deny all connections	The program cannot connect to the Internet or local network.

Table 12.11: Communication modes for allowed programs

- **Advanced permissions**: define the exact characteristics of the traffic you want to allow or deny.

Field	Description
Action	Defines the action that Panda Endpoint Protection will take if the examined traffic matches the rule. • **Allow**: allows the traffic. • **Deny**: blocks the traffic. It drops the connection.
Direction	Sets the traffic direction for connection protocols such as TCP. • **Outbound**: traffic from the user's computer to another computer on the network. • **Inbound**: traffic to the user's computer from another computer on the network.
Zone	The rule will apply only if the zone matches the zone configured in section "**Network type**". Rules whose **Zone** field is set to **All** will be applied at all times irrespective of the network type configured in the protection profile.
Protocol	Lets you establish the layer 3 protocol for the traffic generated by the program you want to control. • All • TCP • UDP

Table 12.12: Advanced communication options for allowed programs

Field	Description
IP	• **All**: the rule won't take into account the connection's source and target IP addresses. • **Custom**: lets you specify the source or target IP address of the traffic to control. You can enter multiple addresses separated by commas (,). To specify a range, use a hyphen (-). From the drop-down menu, select if the IP addresses are IPv4 or IPv6. You cannot mix different types of IP addresses in the same rule. • **Ports**: lets you specify the communication port. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).

Table 12.12: Advanced communication options for allowed programs

Connection rules

This section lets you define traditional TCP/IP traffic filtering rules. Panda Endpoint Protection extracts the value of certain fields in the headers of each packet sent and received by the protected computers, and checks it against the rules entered by the administrator. If the traffic matches any of the rules, the associated action is taken.

Connection rules affect the entire system (regardless of the process that manages them). They have priority over the aforementioned program rules that govern the connection of programs to the Internet/local network.

To build an effective strategy to protect the network against dangerous and unwanted traffic, it is necessary to follow the steps below in the order listed:

1. Specify the firewall's default action in the Program rules section.

Field	Description
Allow	Implements a permissive strategy based on always accepting all connections for which you haven't configured a specific rule in step 3. This is the default, basic configuration mode: all connections for which there is not an existing rule will be automatically accepted.
Deny	Implements a restrictive strategy based on always denying all connections for which you haven't configured a specific rule in step 3. This is an advanced mode: all connections for which there is not an existing rule will be automatically denied.

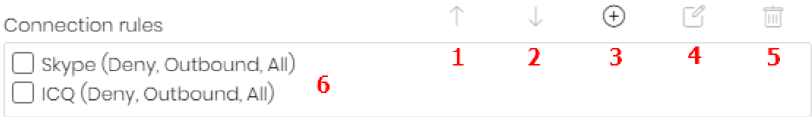
Table 12.13: Types of default actions supported by the firewall for the programs installed on users' computers

2. Enable Panda Security rules

This option enables Panda Security's predefined rules for the selected network type.

3. Add rules that describe specific connections along with the associated action

You can change the order of the firewall's connection rules, as well as adding, editing or removing them by using the Up **(1)**, Down **(2)**, Add **(3)**, Edit **(4)** and Delete **(5)** buttons to their right. Use the checkboxes **(6)** to select the rules to apply each action to.


Connection rules

□ Skype (Deny, Outbound, All)

□ ICQ (Deny, Outbound, All)

Figure 12.2: Edit controls for connection rules

The order of the rules in the list is not random. They are applied in descending order, therefore, if you change the position of a rule, you will also change its priority. Next, we describe the fields found in a connection rule:

Field	Description
Name	Enter a unique name for the rule.
Description	Describe the type of traffic filtered by the rule.
Direction	Lets you specify the direction of the traffic for connection protocols such as TCP. • **Outbound**: outbound traffic. • **Inbound**: inbound traffic.
Zone	The rule will apply only if the zone matches the zone configured in section "Network type". Rules whose **Zone** field is set to **All** will be applied at all times irrespective of the network type configured in the protection profile.
Protocol	Lets you specify the traffic protocol. The options displayed will vary depending on the option you select: • **TCP, UPD, TCP/UDP**: lets you define TCP and/or UDP rules, including local and remote ports. • **Local ports**: lets you specify the connection port used on the user's computer. Select Custom to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-). • **Remote ports**: lets you specify the connection port used on the remote computer. Select Custom to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-). • **ICMP services:** lets you create rules that describe ICMP messages, along with their type and subtype. • **ICMPv6 services**: lets you create rules that describe ICMP messages over IPv6, indicating their type and subtype. • **IP Types:** lets you create rules for the IP protocol and other higher-level protocols.

Table 12.14: Settings options for connection rules

Field	Description
IP addresses	Lets you specify the traffic's source or target IP addresses. You can enter multiple individual IP addresses separated by a comma, or IP address ranges separated by a dash. From the drop-down menu, select if the IP addresses are IPv4 or IPv6. You cannot mix different types of IP addresses in the same rule.
MAC addresses	Lets you specify the traffic's source or target MAC addresses.

Table 12.14: Settings options for connection rules

The source and destination MAC addresses included in packet headers are overwritten every time the traffic goes through a proxy, router, etc. Therefore, the data packets will reach their destination with the MAC address of the last device that handled the traffic.

Block intrusions

The intrusion detection system (IDS) allows administrators to detect and reject malformed traffic specially crafted to impact the security and performance of the computers to protect. This traffic may cause malfunction of user programs and lead to serious security issues, allowing remote execution of applications by hackers, data theft, etc.

Next is a description of the types of malformed traffic supported and the protection provided:

Field	Description
IP explicit path	Rejects IP packets that contain an explicit source route field. These packets are not routed based on their target IP address, but the routing information is defined beforehand.
Land Attack	Stops denial-of-service attacks that use TCP/IP stack loops by detecting packets with identical source and target addresses.
SYN flood	This attack type launches TCP connection attempts massively to force the targeted computer to commit resources for each connection. The protection establishes a maximum number of open TCP connections per second to prevent the computer under attack from becoming saturated.
TCP Port Scan	Detects if a host tries to connect to multiple ports on the protected computer in a specific time period. The protection filters both the requests to open ports and the replies to the malicious computer. This prevents the attacking computer from obtaining information about the status of the ports.
TCP Flags Check	Detects TCP packets with invalid flag combinations. It acts as a complement to the protection against port scanning by blocking attacks of that type such as “SYN&FIN” and “NULL FLAGS”. It also complements the protection against OS fingerprinting attacks as many of those attacks are based on replies to invalid TCP packets.

Table 12.15: Supported types of malformed traffic

Field	Description
Header lengths	• **IP**: rejects inbound packets with an IP header length that exceeds a specific limit. • **TCP**: rejects inbound packets with a TCP header length that exceeds a specific limit. • **Fragmentation overlap**: checks the status of the packet fragments to be reassembled at the destination, protecting the system against memory overflow attacks due to missing fragments, ICMP redirects masked as UDP, and computer scanning..
UDP Flood	Rejects UDP streams to a specific port if the number of UDP packets exceeds a preconfigured threshold in a particular period.
UDP Port Scan	Protects the system against UDP port scanning attacks.
Smart WINS	Rejects WINS replies that do not correspond to requests sent by the computer.
Smart DNS	Rejects DNS replies that do not correspond to requests sent by the computer.
Smart DHCP	Rejects DHCP replies that do not correspond to requests sent by the computer.
ICMP Attack	• **Small PMTU**: the protection detects invalid MTU values used to generate a denial-of-service attack or slow down outbound traffic. • **SMURF**: these attacks involve sending large amounts of ICMP (echo request) traffic to the network broadcast address with a source address spoofed to the victim's address. Most computers on the network will reply to the victim, multiplying traffic flows. The protection rejects unsolicited ICMP replies if they exceed a certain threshold in a specific time period. • **Drop unsolicited ICMP replies**: rejects all unsolicited ICMP replies and ICMP replies that have expired due to timeout.
ICMP Filter echo request	The protection rejects ICMP echo request packets.
Smart ARP	Rejects ARP replies that do not correspond to requests sent by the protected computer, avoiding ARP cache poisoning scenarios.
OS Detection	Falsifies data in replies to the sender to trick operating system detectors. It prevents attacks aimed at taking advantage of vulnerabilities associated with the operating system detected. This protection complements the TCP Flag Checker.

Table 12.15: Supported types of malformed traffic

Device control (Windows computers)

Popular devices such as USB flash drives, CD/DVD drives, imaging and Bluetooth devices, modems and smartphones can become a gateway for infections.

The device control feature lets you configure the way protected computers behave when connecting or using a removable or mass storage device. Select the device or devices you want to authorize or block, and specify their usage.

Enabling device control

- Select the **Enable device control** checkbox**.**
- Use the drop-down menus to select the authorized usage level for each type of device.
  - In the case of USB flash drives and CD/DVD drives, you can choose among **Block**, **Allow read access** or **Allow read & write access**.
  - The options available for Bluetooth and imaging devices, USB modems and smartphones are **Allow** and **Block**.

Allowed devices

This section lets you whitelist specific devices you want to allow despite belonging to a blocked device category.

- Click the ⊕ icon in the **Allowed devices** section to display the list of all devices connected to the computers on your network.
- Select those devices you want to exclude from the general blocking rules defined for each type of device.
- Use the 🗑 button to delete existing exclusions.

Exporting/importing a list of allowed devices

Use the **Export** and **Import** options available on the context menu ⋮ .

Obtaining a device's unique ID

To manage certain devices without having to wait for users to connect them to their computers, or to exclude them manually,, you need to obtain the devices' IDs:

- From the Windows Device Manager,l select the device whose ID you want to obtain. Right-click the device's name and go to **Properties**.
- Click the **Details** tab.
- From the **Property** drop-down list, select **Device instance path**. The **Value** field will display the device's unique ID.

If no value appears in **Device instance path**, you won't be able to obtain the device's ID. In that case, you can use the device's hardware ID to identify it.

From the **Property** drop-down list, select **Device Hardware ID,** The corresponding ID will be displayed..

> *A device's Hardware ID value does not identify it uniquely. It serves to identify all devices of the same hardware type.*

Enter in a text file the IDs of all the devices you want to allow, and import it as indicated in section "**Exporting/importing a list of allowed devices**".

Renaming devices

The name assigned to a computer's devices by Panda Endpoint Protection can sometimes lead to confusion or prevent the administrator from correctly identifying it. To resolve this issue, you can assign custom names to devices:

- From the **Allowed devices** section, select the device to rename.
- Click the ✎ icon. A window will appear requesting you to enter a new name for the device.
- Click **OK**. The **Allowed devices** list will be updated with the new name.

Chapter 13

Security settings for Android devices

The **Settings** menu at the top of the Panda Endpoint Protection console provides the parameters required to configure the security of the smartphones and tablets in the organization. Click the Android devices option on the left-hand menu to display a list of the security profiles already created, or to create a new one.

The following is a description of the available security and anti-theft configuration options for Android devices and recommendations to protect smartphones and tablets without interfering with user activity..

For additional information about the 'Android devices' module, refer to:

- "**Creating and managing settings**" on page 183: information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**" on page 53: managing user accounts and assigning permissions.

CHAPTER CONTENT

Security settings for Android devices

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Android devices** from the side menu.
- Click the **Add** button to open the **Android devices** settings window.

Required permissions

Permission	Access type
Configure security for Android devices	Create, edit, delete, copy, or assign settings for Android devices.
View security settings for Android devices	View the 'Android devices' settings.

Table 13.1: Permissions required to access the 'Android devices' settings

Updates

Lets you define the type of connection to be used by the device to download updates from the Panda Security cloud.

*For more information on how to configure updates, refer to "***Product updates and upgrades***" on page 123.*

Antivirus

The antivirus protection for Android devices protects smartphones and tablets against the installation of malware-infected apps and PUPs, scanning both the devices and their SD memory cards permanently and on demand.

Select the **Permanent antivirus protection** checkbox to enable malware detection.

Exclusions

This option allows you to select installed apps that you don't want to be scanned. To do that, enter the names of the packages to exclude from the scans, separated with commas (",").

To look up an app's package name, find the app in the Google Play app store using a Web browser. The package name will be listed at the end of the URL after the '`?id=`'.

Anti-theft

The anti-theft feature allows actions to be sent to target devices to prevent data loss or locate them in the event of loss or theft.

Click the Anti-theft protection switch to enable this feature.

Refer to "General section for Android devices" on page 165 for more information about the anti-theft features provided by Panda Endpoint Protection.

Behavior

Define how the anti-theft features for Android devices should work:

Field	Description
Report the device's location	The device will send its GPS coordinates to the Panda Endpoint Protection server.
Take a picture after three failed unlock attempts and email it	If the user of the device has three consecutive failed attempts to unlock it, a photo will be taken and emailed to the email addresses entered in the text box. You can enter multiple addresses separated with a comma.

Table 13.2: Anti-theft features for Android devices

Privacy

Lets users enable private mode. This mode prevents photos from being taken with the device and the device's coordinates from being captured and sent to the Panda Endpoint Protection server.

Chapter 14

Panda Patch Management (Updating vulnerable programs)

Panda Patch Management is a built-in module on Aether Platform that finds those computers on the network with known software vulnerabilities and updates them centrally and automatically. It minimizes the attack surface, preventing malware from taking advantage of the software flaws that may affect the organization's workstations and servers in order to infect them.

Panda Patch Management supports Windows operating systems. It detects both third-party applications with missing patches or in EOL (End-Of-Life) stage, as well as all patches and updates published by Microsoft for all of its products (operating systems, databases, Office applications, etc.).

⚠ *Windows XP SP3 and Windows Server 2003 SP2 computers require a computer with the cache/repository role on the same subnet in order to detect and install missing patches. Windows XP SP3 and Windows Server 2003 SP2 computers cannot download patches even if they have the cache/repository role assigned.*

Panda Patch Management is not compatible with Windows ARM systems.

For additional information about the Panda Patch Management module, refer to:

- "**Creating and managing settings**" on page 183: information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**" on page 53: managing user accounts and assigning permissions.
- "**Managing lists**" on page 43: information on how to manage lists.

CHAPTER CONTENT

Panda Patch Management features

The features provided by Panda Patch Management are accessible via the following sections in the management console:

- **To configure the discovery of missing patches**: go to the **Patch management** settings section (top menu **Settings**, side panel). Refer to "Configuring the discovery of missing patches"
- **To configure patch exclusions**: go to the **Available patches** list. Refer to "Exclude patches for all or some

computers".

- **To have visibility into the update status of the entire IT network**: go to the **Patch Management** dashboard (top menu **Status**, side panel). Refer to "Patch management status"
- **To view lists of missing patches**: check the **Patch management status, Available patches** and **End-of-Life programs** lists (top menu **Status**, side panel **My lists**, **Add**). Refer to "Panda Patch Management module lists"
- **To view a history of all installed patches**: check the **Installation history** list (top menu **Status**, side panel **My lists**, **Add**). Refer to "Installation history"
- **To patch computer:** Select one of the following options:
  - From the **Last patch installation tasks** widget, click the **View installation history** link. Refer to "Last patch installation tasks".
  - Go to the **Status** menu at the top of the console, click **Add** in the **My lists** section of the side panel and select the **Installation history** list. Refer to "Installation history".
  - Go to the **Tasks** menu at the top of the console, select the task that installed the patch to uninstall and click **View installed patches**.
  - Click the patch to uninstall. A screen will be displayed with the patch details and the **Uninstall** button if the patch supports this option. Refer to "Uninstalling a patch".

General workflow

Panda Patch Management is a comprehensive tool for patching and updating the operating systems and all programs installed on the computers on your network. To effectively reduce the attack surface of your computers, follow the steps below:

- Make sure Panda Patch Management works properly on the protected computers on your network.
- Make sure that all published patches are installed.
- Install the selected patches.
- Uninstall any patches that are causing malfunction problems (rollback).
- Exclude patches for all or certain computers
- Make sure the programs installed on your computers are not in EOL (End-Of-Life) stage.
- Regularly check the history of patch and update installations.
- Regularly check the patch status of those computers where incidents have been recorded.

Make sure that Panda Patch Management works properly

Follow the steps below:

- Make sure that all computers on your network have a Panda Patch Management license assigned and the module is installed and running. Use the "Patch management status" widget.

- Make sure that all computers with a Panda Patch Management license assigned can communicate with the Panda Security cloud. Use the "Time since last check" widget.
- Make sure the computers that will receive the patches have the Windows Update service running with automatic updates disabled.

*Select the **Disable Windows Update** on computers option in the Patch Management settings for Panda Endpoint Protection to manage the service correctly. For more information, refer to "General options".*

Make sure that all published patches are installed

As software vendors discover flaws in their products, they publish updates and patches that must be installed on the affected systems in order to fix them. These patches have a criticality level and type associated to them:

- To view missing patches by type and criticality level, use the "Patch criticality" widget.
- To view details of the patches that are missing on a computer or computer group:
  - Go to the computer tree (top menu **Computers**, **Folder** tab in the side panel), and click the context menu of a computer group containing Windows computers. Select **View available patches.** The "Available patches" will be displayed filtered by the relevant group.

Or,

  - Go to the computers screen (top menu **Computers**, right panel) and click a computer's context menu. Select **View available patches**. The "Available patches" will be displayed filtered by the relevant computer.
- To get an overview of all missing patches:
  - Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
  - Use the filter tool to narrow your search.
- To find those computers that don't have a specific patch installed:
  - Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the "Available patches".
  - Use the filter tool to narrow your search.
  - Click the context menu of the specific computer-patch and select the option **View which computers have the patch available**.

Download and install the patches

In order to install patches and updates, Panda Patch Management uses the task infrastructure implemented in Panda Endpoint Protection.

> ⚠ *The patches released by Microsoft won't be installed successfully if the Windows Update service is stopped on the target workstation or server. However, to prevent Panda Patch Management from overlapping with Windows Update, it is recommended that Windows Update be set to be inactive on the computer. Refer to "***General options***" for more information.*

Patches and updates are installed via quick tasks and scheduled tasks. Quick tasks install patches in real time but do not restart the target computer, even though this may be required in order to complete the installation process. Scheduled tasks allow you to configure all parameters related to the patch installation operation. Refer to "**Tasks**" on page **361** for more information about tasks in Panda Endpoint Protection.

- **Patch download and bandwidth savings**

Prior to installing a patch, it must be downloaded from the software vendor's servers. This download takes place in the background and separately on each computer as soon as the installation task is launched. To minimize bandwidth usage, the module leverages the cache/repository node infrastructure implemented on the customer's network.

> ⚠ *Proxy nodes cannot download patches or updates. Likewise, no patches or updates can be downloaded if the node or computer with the cache/repository role does not have direct access to the Panda Security cloud, or indirect access via a corporate proxy. Refer to "***Configuring the Panda agent role***" on page* **194** *for more information about roles in Panda Endpoint Protection.*

Nodes with the cache/repository role store patches for a maximum of 30 days; after then, the patches will be deleted. If a computer requests a patch from a cache node, but the node doesn't have the patch in its repository, the computer will wait for the cache node to download it. The wait time will depend on the size of the patch to download. If the node cannot download the patch, the computer will attempt to download it directly instead.

Once a patch has been applied to a target computer, it will be deleted from the storage media where it resides.

- **Installation task sequence**

Patch installation tasks may require downloading patches from the vendor's servers if the nodes on the network with the cache/repository role don't already have the relevant patches. In this scenario, please note that quick tasks start downloading the necessary patches as soon as they are created.

This may result in high bandwidth usage if those tasks affect many computers or there is a large amount of data to download.

In contrast, scheduled patch installation tasks start downloading the necessary patches when configured in the settings. However, if the start time of multiple tasks coincides, the module will introduce a short random delay of up to 2 minutes to prevent downloads from overlapping and minimize bandwidth usage to a certain extent.

- **Interrupting patch installation tasks**

You can interrupt patch installation tasks if the installation process has not started yet on the target computers. If the installation process has already begun, however, it is not possible to cancel the task as doing so could cause errors on computers.

- **Patch download strategies**

The management console is a very flexible tool that allows you to install patches in multiple ways. Generally speaking, you can apply the following strategies:

- To install one or multiple specific patches, use the "**Available patches**" and configure the filter tool.
- To install all patches of a certain type or with a specific criticality level, use a quick or schedule task.
- To install patches on a specific computer or computer group, use the group tree.

Next is a description of all possible combinations of patches and targets, along with the steps to take to complete the patch operation in each case.

Target / Patch	One or multiple specific patches	One, multiple or all types of patches
One or multiple computers	Case 1: from the 'Available patches' list	Case 2: from the computer tree
A group	Case 3: from the 'Available patches' list	Case 4: from the computer tree
Multiple or all groups	Case 5: from the 'Available patches' list	Case 6: from the Tasks top menu

Table 14.1: Patch installation based on the target and the patches to install

Case 1: from the 'Available patches' list

Follow these steps to install one or multiple specific patches on one or multiple computers:

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the "**Available patches**".
- Use the filter tool to narrow your search.
- Click the checkboxes besides the computers-patches you want to install, and select **Install** from the action bar to create a quick task, or **Schedule installation** to create a scheduled task.

Case 2: from the computer tree

Follow these steps to install one, multiple or all types of patches on one or multiple computers:

- Go to top menu **Computers** and click the **Folders** tab in the computer tree (left panel). Next, select the group that the target computers belong to. If the target computers belong to multiple groups, click the **All** root group.
- Click the checkboxes besides the computers that the patches will be applied to.
- From the action bar, click **Schedule patch installation**.
- Configure the task, click the **Save** button and publish it.

Case 3: from the 'Available patches' list

Follow these steps to install a specific patch on a computer group:

- Go to top menu **Computers** and click the **Folders** tab in the computer tree (left panel). Next, click the group's context menu.
- Click the **View available patches** option. The "**Available patches**" will be displayed filtered by the relevant group.
- Use the **Patch** field in the filter tool to list only the patch to install.
- Select all computers on the list by clicking the relevant checkboxes.
- Click **Install** from the action bar to create a quick task, or **Schedule installation** to create a scheduled task.

To install multiple specific patches on a group of computers, repeat these steps as many times as patches you want to install.

Case 4: from the computer tree

Follow these steps to install one, multiple or all types of patches on a computer group:

- Go to top menu **Computers** and click the **Folders** tab in the computer tree (left panel). Next, click the group's context menu.
- Click the **Schedule patch installation** option. This will take you to the task settings screen.
- Configure the task, indicating the type or types of patches that will be installed on the group. Click the **Save** button and publish it.

Case 5: from the 'Available patches' list

Follow these steps to install a specific patch on multiple computer groups:

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the "**Available patches**".
- Use the filter tool to find the patch to install.
- Click the checkbox besides the patch to install and click **Schedule installation** to create a task.

- Go to top menu **Tasks** and edit the task you have just created.
- In the **Recipients** field, add the groups that the patch will be applied to (use the **Computer groups** section to do this). Remove any additional computer that may appear in the **Additional computers** section.
- Click **Back**, finish configuring the task and click **Save**.
- Publish the task.

To install multiple specific patches on multiple computer groups, repeat these steps as many times as patches you want to install.

Case 6: from the Tasks top menu

*To manage **Install patches** tasks, the user account used to access the web console must have the **Install, uninstall, and exclude patches** permission assigned to its role. For more information about the permission system implemented in Panda Endpoint Protection, refer to "Understanding permissions" on page 57.*

Follow these steps to install one, multiple or all types of patches on multiple or all computer groups:

- Go to top menu **Tasks**, click **Add task** and select **Install patches**.
- Set the **Recipients** field, indicating the computers and groups that the patches will be applied to.
- Schedule the task. Refer to "Task schedule and frequency" for more information.
- Specify the criticality level of the patches to install.
- Specify which products will receive patches by selecting the relevant checkboxes in the product tree. Since the product tree is a 'living' resource that changes over time, please keep the following rules in mind when selecting items from the tree:
  - Selecting a node will also select all of its child nodes and all items dependent on them. For example, selecting Adobe will also select all nodes below that node.
  - If you select a node, and Panda Patch Management automatically adds a child node to that branch, that node will be selected as well. For example, as previously explained, selecting Adobe will also select all of its child nodes. In addition to this, if, later, Panda Patch Management adds a new program or family to the Adobe group, that program or family will be selected as well. In contrast to this, if you manually select a number of child nodes from the Adobe group, and later Panda Patch Management adds a new child node to the group, this won't be automatically selected.
  - The programs to patch are evaluated at the time when tasks are run, not at the time when they are created or configured. For example, if Panda Patch Management adds an entry to the tree after the administrator has created a patch task, and that entry is selected automatically in accordance with the rule in the previous point, the task will install the patches associated with that new program when being run.
- Set the restart options in case the target workstations or servers need to be restarted to finish

installing the patch.

  - **Do not restart automatically**: upon completing the patch installation task, a window will be displayed to the target computer user with the options **Restart now** and **Remind me later**. If the latter is selected, a reminder will be displayed 24 hours later.
  - **Automatically restart workstations only**: upon completing the patch installation task, a window will be displayed to the target computer user with the **Restart now** option, a **Minimize** button and a 4-hour countdown timer. This window will be maximized every 30 minutes as a reminder to the user. Less than one hour before the restart, the minimize button will be disabled. When the countdown finishes, the computer will restart automatically.
  - **Automatically restart servers only**: this option behaves in the same way as **Automatically restart workstations only**, but applies to servers only.
  - **Automatically restart both workstations and servers**: this option behaves in the same way as **Automatically restart workstations only**, but applies to both workstations and servers.
- Click **Save** and publish the task.

Download patches manually

There are cases in which Panda Patch Management cannot get a download URL to install the required patch automatically. This can happen due to many reasons: the patch requires payment or is not a publicly available patch and requires user registration prior to download, for example. The EULAs that protect certain patches may prevent Panda Security from downloading them for distribution. In those cases, it must be the administrator who manually downloads the patch and shares it across the network for those computers that require it.

Panda Patch Management provides a mechanism for administrators to add manually downloaded patches to the patch repository from the Web console.

To manually add a patch to the repository, you must have the download URL of the patch as provided by the vendor of the product to update. Once you have it, follow the steps below:

- Identify patches that must be manually downloaded.
- Get the download URL from the vendor.
- Integrate the downloaded patch into the patch repository.
- Enable the downloaded patch for installation.
- Optional: Disable a patch for installation

Identify patches that must be manually downloaded

- Go to the **Status** menu at the top of the console and click **Add** from the **My lists** side panel. A list will be shown with all available lists.
- Click the **Available patches** list and configure the following filter:
  - **Installation**: Requires manual download.

- **Show non-downloadable patches**: Yes.

- Click the **Filter** button. The list will display all patches reported by Panda Patch Management as required to update the computers on the network and which cannot be automatically downloaded.

Get the download URL

- Click one of the patches in the list obtained in step "**Identify patches that must be manually downloaded**". The patch details will be displayed.
- Click the **Download URL** field to start downloading the patch. Take note of the file name shown in the **File name** field.

Integrate the downloaded patch into the patch repository

- Find a computer on the network that has Panda Endpoint Protection installed and the cache role and copy the downloaded file to the following path:

```
c:\Programdata\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy.
```

> *If the computer's storage drive is different from the drive set by default in the Panda Endpoint Protection software installation process, go the following path:*
>
> ```
> x:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy
> ```
>
> *Where x is the drive where the computer's repository is located. Refer to "***Setting the storage drive***" on page* **196** *for more information.*

- If the **ManuallyDeploy** folder does not exist, create it with read and write admin permissions.
- If needed, rename the newly copied patch to the name displayed in the **File name** field mentioned in section "**Get the download URL**".

Enable the downloaded patch for installation

- After the patch has been copied to the repository, go back to the **Available patches** list and click the context menu of the manually downloaded patch.
- Click the Mark as '**Manually downloaded**'☁ option from the drop-down menu. From then on, the patch's status will change from **Requires manual download** to **Pending (manually downloaded)** for all computers that need to install it. Once the patch's status is **Pending (manually downloaded)**, its context menu will show all options required to install it just like an automatically downloaded patch.

Refer to "Download and install the patches".

Panda Patch Management does not check to see if there are patches with the Pending (manually downloaded) status on computers with the cache role. Nor does it check to see whether all computers on the network that require a patch actually have a cache computer assigned that has the patch in its repository. It is the administrator's responsibility to make sure that the cache computers to be used in patch downloads have all necessary manually downloaded files in their ManuallyDeploy folder.

Disable a patch for installation

To remove a patch from the patch repository, follow the steps below:

- Go to the **Available patches** list and configure a filter with the following features:
  - **Installation**: Pending (manually downloaded).
  - **Show non-downloadable patches**: Yes.
- Click the **Filter** button. The list will display all patches manually downloaded and enabled for installation.
- Click the context menu of a patch enabled for installation and select the option Mark as '**Requires manual download**' . From then on, the patch will no longer belong to the repository of installable patches, and the installation options will be removed from its context menu.

Uninstall problematic patches

Sometimes, the patches published by software vendors do not work correctly, which can lead to serious problems. This can be avoided by selecting a small number of test computers prior to deploying a patch across the entire network. In addition to this, Panda Patch Management also lets you remove (roll back) installed patches.

Requirements to uninstall an installed patch

- The administrator must have the **Install/Uninstall patches** permission enabled. Refer to "Install, uninstall and exclude patches" for more information.
- The patch must have been successfully installed.
- The patch must support the rollback feature. Not all patches support this feature.

Uninstalling a patch

- Go to the patch uninstallation screen. There are three ways to do this:
  - Go to the **Status** menu at the top of the console, click **Add** in the **My lists** section of the side panel and select the "Installation history".
  - Access the list of installed patched via the **Tasks** menu at the top of the console. Select the task

that installed the patch you want to uninstall and click the **View installed patches** link in the top-right corner of the screen.

- Access the "Last patch installation tasks" widget. Then, click the **View installation history** link.

- From the list displayed, select the patch you want to uninstall.
- If the patch can be removed, the **Uninstall the patch** button will be displayed. Click the button to access the computer selection screen.
  - Select **Uninstall from all computers** to remove the patch from all computers on the network.
  - Select **Uninstall from "{{hostName}}" only** to remove the patch from the selected computer only.
- Panda Patch Management will create an immediate execution task to uninstall the patch.
- If a restart is required to finish uninstalling the patch, the solution will wait for the user to restart it manually.

Uninstalled patches will be shown again in the lists of available patches, and will be installed again the next time a scheduled patch installation task is run, unless they are excluded. However, if a patch is withdrawn by the corresponding vendor, it will no longer be shown or installed. Refer to "Exclude patches for all or some computers".

Check the result of patch installation/uninstallation tasks

The **Tasks** menu at the top of the console lets you view those tasks in which patches have been installed or uninstalled from computers. Both provide a **View results** option that lets you view on which computers the action was taken and which patches were installed/uninstalled. For more information, refer tos "Patch installation/uninstallation task results" and "View installed/uninstalled patches".

Exclude patches for all or some computers

Network administrators have the option to prevent the installation of malfunctioning patches or patches that significantly change the characteristics of the target program. This is called excluding the patch. To exclude a patch, follow the steps below:

- Go to the Status menu at the top of the console. Then, click **Add** from the **My lists** menu on the left. Click the **Available patches** list. This list displays a line for each computer-available patch pair. An available patch is a patch that has not been installed yet on a specific computer or has been uninstalled from it.
- To exclude a single patch, click the context menu associated with the patch ⋮ and select the **Exclude** ⃠ option. A window will open for you to select the exclusion type.
  - **Exclude for X only**: excludes the patch for the selected computer only.
  - **Exclude for all computers**: excludes the patch for all computers on the network.
- To exclude several patches and/or a single patch for multiple computers, select them using the

relevant checkboxes, click the action bar and choose the **Exclude** ⃠ option. A window will open for you to select the exclusion type.

- **Exclude for the selected computers only**: excludes the patches for the selected computers only.
- **Exclude for all computers**: excludes the patches for all computers on the network.

> ⚠ *When you exclude a patch, you exclude a specific version of the patch. That is, if you exclude a patch, and later the software vendor releases a later version of that patch, this won't be automatically excluded.*

Make sure the programs installed are not in EOL (End-Of-Life) stage

Programs in EOL (End-Of-Life) stage do not receive any type of update from the relevant software vendor, therefore it is advisable to replace them with an equivalent program or a more advanced version.

Follow these steps to find those programs on the network that have reached their EOL or will reach it shortly:

- Go to the **Status** menu at the top of the console and click **Patch Management** from the side panel.
- You'll see the "End-of-Life programs" widget, which is divided into the following sections:
  - **Currently in EOL**: programs on the network that do not receive updates from the relevant vendor.
  - **In EOL (currently or in 1 year)**: programs on the network that have reached their EOL, or will reach their EOL in a year.
  - **With known EOL date**: programs on the network with a known EOL date.

Follow these steps to find all programs on your network with a known EOL date:

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel.
- Select the "End-of-Life programs" list.

The list displays a line for each computer-EOL program pair found.

Check the history of patch and update installations

Follow these steps to find out if a specific patch is installed on your network computers:

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel.
- Select the "Installation history".

The list displays a line for each computer-installed patch pair found, with information about the affected program's or operating system's name and version, and the patch criticality/type.

Check the patch status of computers with incidents

Panda Patch Management correlates those computers where incidents have been recorded with their patch status so that it is possible to determine whether an infected computer or a computer where threats have been detected has missing patches.

To check whether a computer where an incident has been detected has missing patches:

- Go to top menu **Status**, widget **Threats detected by the antivirus**, and click a computer-threat. Information about the threat detected on the computer is displayed.
- In the **Affected computer** section, click the **View available patches** button. The **Available patches** list will be displayed, filtered by the relevant computer.
- Select all of the available patches for the computer and click **Install** from the action bar in order to create a quick patch installation task.

Configuring the discovery of missing patches

Accessing the settings

- Go to the **Settings** menu at the top of the console and click **Patch management** from the side menu.
- Click the **Add** button to open the **Patch management** settings window.

Required permissions

Permission	Access type
Patch management	Create, edit, delete, copy, or assign 'Patch management' settings.
View patch management settings	View the 'Patch management' settings

Table 14.2: Permissions required to access the 'Patch management' settings

General options

- Click **Disable Windows Update on computers** for Panda Patch Management to manage updates exclusively and without interfering with the local Windows Update settings.
- Click the **Automatically search for patches** switch to enable the patch search functionality. If the switch is not on the ON position, the lists in the module won't display missing patches, although it will still be possible to apply them via the patch installation tasks.

Search frequency

Search for patches with the following frequency indicates how frequently Panda Patch Management checks for missing patches on your computers using its cloud-hosted patch database.

Patch criticality

Sets the criticality of the patches that Panda Patch Management will look for.

⚠ *The criticality level of patches is defined by the vendor of the software affected by the vulnerability. The classification criteria are not universal. We recommend that, prior to installing a patch, you check its description, especially for those patches not classified as 'critical'. This way, you can choose to install the patch or not depending on whether you are suffering the symptoms described.*

Panda Patch Management widgets and panels

Accessing the dashboard

To access the dashboard, click the **Status** menu at the top of the console and then click **Patch Management** from the side menu.

Required permissions

Permissions	Access to widgets
No permissions	• Patch management status • Time since last check
Install, uninstall, and exclude patches	• End-of-Life programs • Available patches • Last patch installation tasks
View available patches	• End-of-Life programs • Available patches • Last patch installation tasks

Table 14.3: Permissions required to access the 'Patch management' widgets

Patch management status

Shows those computers where Panda Patch Management is working properly and those where there have been errors or problems installing or running the module. The status of the module is represented with a circle with different colors and associated counters. The panel offers a graphical representation and percentage of those computers with the same status.

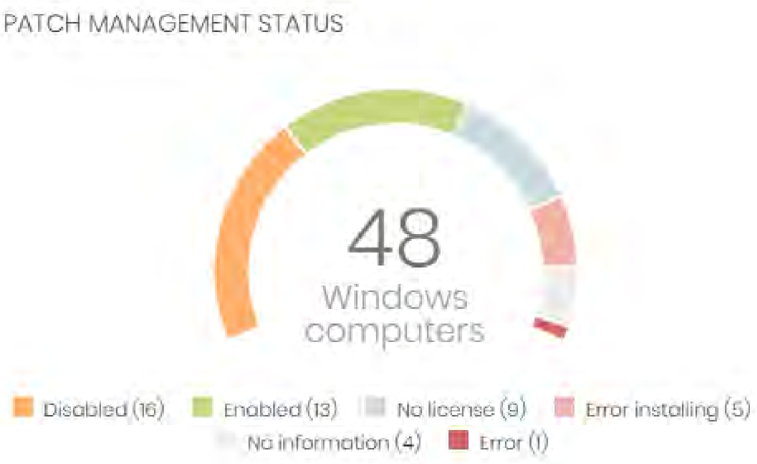


Figure 14.1: 'Patch management status' panel

- **Meaning of the data displayed**

Data	Description
Enabled	Shows the percentage of computers where Panda Patch Management was installed successfully, is running properly and the assigned settings enables the module to search for patches automatically.
Disabled	Shows the percentage of computers where Panda Patch Management was installed successfully, is running properly but the assigned settings prevent the module from searching for patches automatically.
No license	Computers where Panda Patch Management is not working because there are insufficient licenses or because an available license has not been assigned to the computer.
Installation error	Indicates the computers where the module could not be installed.
No information	Computers that have just received a license and haven't reported their status to the server yet, and computers with an outdated agent.
Error	Computers where the Panda Patch Management module does not respond to the requests sent from the server, or its settings are different from those defined in the Web console.
Central area	Shows the total number of computers compatible with the Panda Patch Management module.

Table 14.4: Description of the data displayed in the 'Patch management status'

- **Lists accessible from the panel**

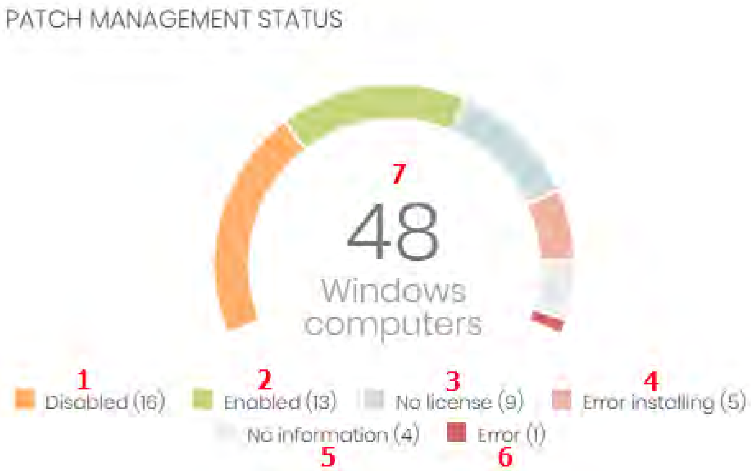


Figure 14.2: Hotspots in the 'Patch management status' panel

Click the hotspots shown in the figure 14.2 to access the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Patch management status = Disabled
(2)	Patch management status = Enabled
(3)	Patch management status = No license
(4)	Patch management status = Installation error
(5)	Patch management status = No information
(6)	Patch management status = Error
(7)	No filters

Table 14.5: Filters available in the 'Patch management status' list

Time since last check

Displays computers that have not connected to the Panda Security cloud to report their patch status for a certain amount of time. Such computers are susceptible to security problems and require special attention from the administrator.

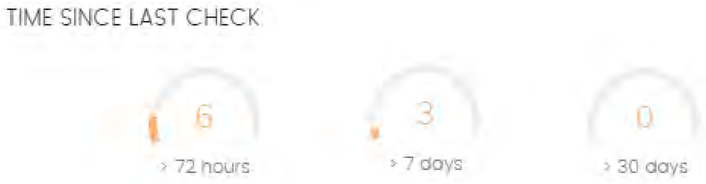


Figure 14.3: 'Time since last check' panel

- **Meaning of the data displayed**

Data	Description
72 hours	Number of computers that have not reported their patch status in the last 72 hours.
7 days	Number of computers that have not reported their patch status in the last 7 days.
30 days	Number of computers that have not reported their patch status in the last 30 days.

Table 14.6: Description of the data displayed in the ‘Time since last check’ panel

- **Lists accessible from the panel**

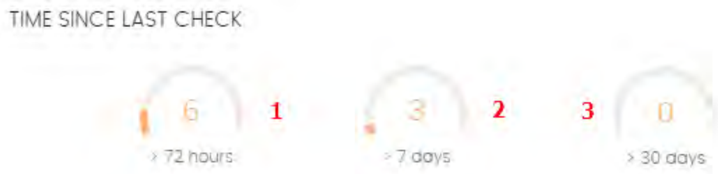


Figure 14.4: Hotspots in the 'Time since last check' panel

Click the hotspots shown in the figure 14.4 to access the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago and Patch management status = Enabled or Disabled or No information or Error.
(2)	Last connection = More than 7 days ago and Patch management status = Enabled or Disabled or No information or Error.
(3)	Last connection = More than 30 days ago and Patch management status = Enabled or Disabled or No information or Error.

Table 14.7: Filters available in the Time since last check' panel

End-of-Life programs

Shows information about the End-of-Life of the programs on the network, grouped by date.

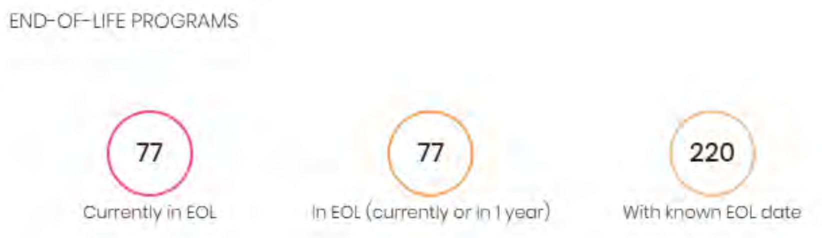


Figure 14.5: 'End-of-Life programs' panel

- **Meaning of the data displayed**

Data	Description
Currently in EOL	Programs on the network that have reached their EOL.
Currently in EOL	Programs on the network that have reached their EOL or will reach it in a year.
With known EOL date	Programs on the network with a known EOL date.

Table 14.8: Description of the data displayed in the 'End of life' panel

- **Lists accessible from the panel**

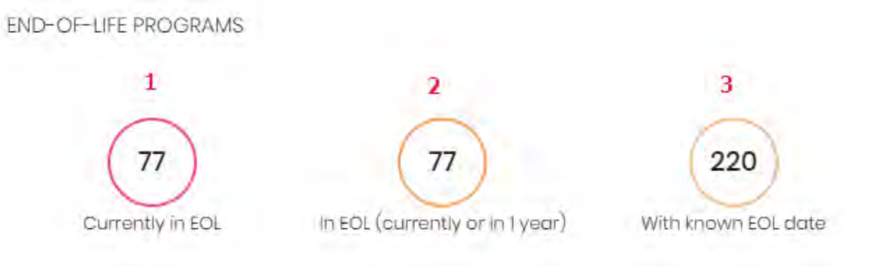


Figure 14.6: Hotspots in the 'End-of-Life programs' panel

Click the hotspots shown in the figure 14.6 to access the **End-of-Life programs** list with the following predefined filters.

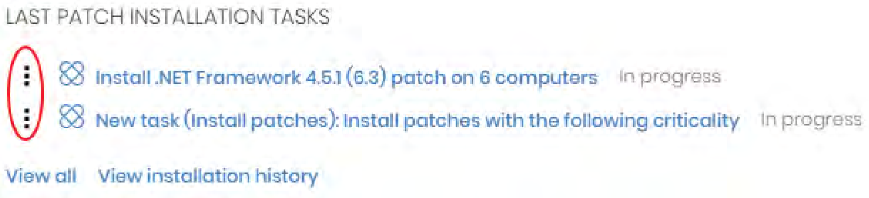
Hotspot	Filter
(1)	End-of-Life date = Currently in EOL
(2)	End-of-Life date = In EOL (currently or in 1 year)
(3)	End-of-Life date = All

Table 14.9: Filters available in the "End Of Life' list

Last patch installation tasks

Refer to "Task management" on page 367 for more information on how to edit an existing task.

Shows a list of the last patch installation tasks created. This widget displays multiple links through which you can manage the patch installation tasks:



LAST PATCH INSTALLATION TASKS

Install .NET Framework 4.5.1 (6.3) patch on 6 computers In progress

New task (Install patches): Install patches with the following criticality In progress

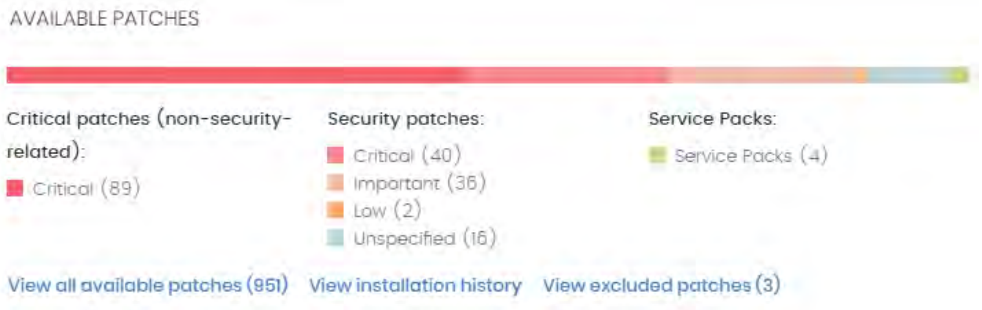
View all View installation history

Figure 14.7: 'Last patch installation tasks' panel

- Click a task to edit its settings.
- Click the **View all** link to access the top menu **Tasks**. There you'll see all the tasks that have been created.
- Click the **View installation history** link to access the **Installation history** list. There you'll see the patch installation tasks that have finished successfully or with errors.
- Click the context menu associated with a task to display a drop-down menu with the following options:
  - **Cancel**: interrupts the task before starting to install patches on the target computer.
  - **View results**: shows the task results.

Available patches

Shows the number of computer-missing patch pairs on the network, sorted by patch type. Each missing patch is counted as many times as there are computers that don't have it installed.



AVAILABLE PATCHES

Critical patches (non-security-related):

🟥 Critical (89)

Security patches:

🟥 Critical (40)

🟧 Important (36)

🟧 Low (2)

🟦 Unspecified (16)

Service Packs:

🟩 Service Packs (4)

View all available patches (951) View installation history View excluded patches (3)

Figure 14.8: 'Available patches' panel

- **Meaning of the data displayed**

Data	Description
Security patches - Critical	Number of security patches rated 'critical' and pending application
Security patches - Important	Number of security patches rated 'important' and pending application
Security patches - Low	Number of security patches rated 'low' and pending application
Security patches – Unspecified	Number of security patches that don't have a severity rating and are pending application
Other patches (non-security-related)	Number of non-security patches that are pending application
Service Packs	Number of patch and hotfix bundles that are pending application
View all available patches	Number of patches of any severity, related or not to system security and which are pending application

Table 14.10: Description of the data displayed in the 'Available patches' panel

- **Lists accessible from the panel**

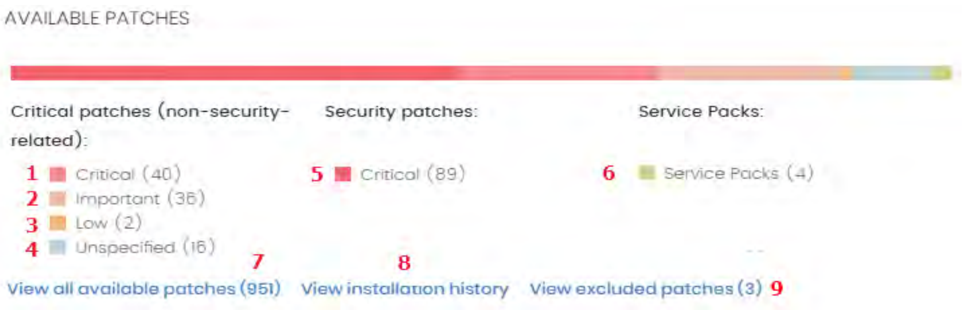


Figure 14.9: Hotspots in the 'Available patches' panel

Clicking the hotspots shown in figure 14.9 will open lists with the following predefined filters:

Hotspot	List	Filter
(1)	Available patches	Criticality = Critical (security-related)
(2)	Available patches	Criticality = Important (security-related)
(3)	Available patches	Criticality = Low (security-related)
(4)	Available patches	Criticality = Unspecified (security-related)
(5)	Available patches	Criticality = Other patches (non-security-related)
(6)	Available patches	Criticality = Service Pack

Table 14.11: Filters available in the 'Available patches' list

Hotspot	List	Filter
(7)	Available patches	No filters.
(8)	Installation history	No filters.
(9)	Excluded patches	No filters.

Table 14.11: Filters available in the ‘Available patches’ list

Panda Patch Management module lists

Accessing the lists

There are two ways to access the lists:

- Click the **Status** menu at the top of the console. Then, click **Patch Management** from the side menu and click the relevant widget.

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window will open with all available lists.
- Select a list from the **Patch management** section to view the associated template. Edit it and click **Save**. The new list will be added to the side menu.

The patch installation and uninstallation lists can be accessed from the **Last patch installation tasks** widget by clicking **View installation history**.

The **Patch installation/uninstallation task results** and **View installed/uninstalled patches** lists can be accessed from the **Task** menu at the top of the console by clicking **View results** in a patch installation or uninstallation task.

Required permissions

Permissions	Access to lists
No permissions	• Patch management status
Install, uninstall, and exclude patches	Access to lists and context menus to install and uninstall patches: • Available patches • Installation history • End-of-Life programs • Excluded patches • Patch installation/uninstallation task results • View installed/uninstalled patches

Table 14.12: Permissions required to access the ‘Patch management’ lists

Permissions	Access to lists
View available patches	Read-only access to lists: • Available patches • Installation history • End-of-Life programs • Excluded patches • Patch installation/uninstallation task results • View installed/uninstalled patches

Table 14.12: Permissions required to access the 'Patch management' lists

Patch management status

This list shows all computers on the network that are compatible with Panda Patch Management (with filters to allow administrators to identify those workstations and servers that are not using the service due to one of the reasons displayed in the associated panel).

Field	Comments	Values
Computer	Name of the computer with outdated software.	Character string
Computer status	Agent reinstallation: • ⚙ Reinstalling the agent. • ⚙ Agent reinstallation error Protection reinstallation: • ⚙ Reinstalling the protection. • ⚙ Protection reinstallation error. • ↻ Pending restart.	Icon
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Patch management	Module status.	• ✓ Enabled • ⊖ Disabled • ⊗ Installation error (failure reason) • ☒ No license • __ No information • ⊗ Error
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date

Table 14.13: Fields in the 'Patch management status' list

Field	Comments	Values
Last connection	Date when the Panda Endpoint Protection status was last reported to the Panda Security cloud.	Date

Table 14.13: Fields in the 'Patch management status' list

*To view a graphical representation of the list data, go to widget “***Patch management status***”.*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Agent version		Character string
Installation date	Date when the Panda Patch Management module was successfully installed on the computer.	Date
Last connection date	Date when the agent last connected to the Panda Security cloud.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version and patch status.	Character string
Protection updated	Indicates whether the installed protection has the latest released version.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date when the signature file was last updated.	Date

Table 14.14: Fields in the 'Patch management status' exported file

Field	Comments	Values
Patch management status	Module status.	• Enabled • Disabled • Installation error • No license • No information • Error
Requires restart	The computer requires a reboot to finish installing one or more downloaded patches.	Boolean
Last check date	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date
Installation error date	Date when the administrator attempted to install the Panda Patch Management module and the operation failed.	Date
Installation error	Failure reason	• Download error • Execution error

Table 14.14: Fields in the 'Patch management status' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	• All • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the agent last connected to the Panda Security cloud	Date
Pending restart to complete patch installation	The computer requires a reboot to finish installing one or more downloaded patches.	Boolean
Patch management status	Module status.	• Enabled • Disabled • Installation error • No license • No information • Error

Table 14.15: Filters available in the 'Patch management status' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "Computer details" on page 159 for more information.

Available patches

Shows a list of all missing patches on the network computers and published by Panda Security. Each line in the list corresponds to a patch-computer pair.

Field	Comments	Values
Computer	Name of the computer with outdated software.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Indicates the patch installation status: • **Pending**: the patch is available for the computer but hasn't been installed yet. • **Requires manual download**: the patch must be manually downloaded and copied to a cache computer by the administrator. Refer to "Download patches manually". • **Pending (manually downloaded)**: the patch has been manually downloaded and is already included in the patch repository. Refer to "Download patches manually". • **Pending restart:** the patch has been installed but the computer has not been restarted. Some patches may not be applied until the computer is restarted.	

Table 14.16: Fields in the 'Available patches' list

Field	Comments	Values
Context menu	Displays an actions menu: • **Install**: lets you create a quick task to immediately install the patch on the computer. • **Schedule installation**: lets you create a scheduled task to install the patch on the computer. • **View all available patches for the computer**: displays all available patches for the computer that have not been installed yet. • **View which computers have the patch available**: displays all computers that have the patch available for installation.	

Table 14.16: Fields in the 'Available patches' list

*To view a graphical representation of the list data, go to widget "**Available patches**".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value

Table 14.17: Fields in the 'Available patches' exported file

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Last seen	Date when the computer was last discovered.	Date
Is downloadable	Indicates if the patch is available for download or requires an additional support contract with the software vendor in order to have access to it.	Boolean
Download size (KB)	Patch size in compressed format. Applying the patch may require more space on the target computer's storage media than indicated in this field.	Numeric value

Table 14.17: Fields in the 'Available patches' exported file

Field	Comments	Values
Status	Indicates the patch installation status: • **Pending**: the patch is available for the computer but hasn't been installed yet. • **Requires manual download**: the patch must be manually downloaded and copied to a cache computer by the administrator.Refer to "**Download patches manually**". • **Pending (manually downloaded)**: the patch has been manually downloaded and is already included in the patch repository.Refer to "**Download patches manually**".	Character string
File name	Name of the file that contains the patch.	Character string
Download URL	HTTP resource for downloading the patch in the software vendor's infrastructure.	Character string

Table 14.17: Fields in the 'Available patches' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Find computer	Computer name.	Character string
Computer	Name of the computer with outdated software.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related)

Table 14.18: Filters available in the 'Available patches' list

Field	Comments	Values
		Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack
Installation	Displays patches that are in the process of installation, filtering them by the installation stage they are in.	Pending Requires manual download Pending (manually downloaded) Pending restart
Show non-downloadable patches	Shows those patches that cannot be directly downloaded by Panda Patch Management as there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.)	Boolean

Table 14.18: Filters available in the 'Available patches' list

- **'Patch detected' window**

Click any of the rows in the list to open the **Patch detected** window. This window can provide the following content:

- Information about the available patch and the **Install patch** button.
- Information about the patch in the process of installation. The text **Pending restart** appears next to the **Install patch** button.

Click the **Install patch** button. A pop-up window appears for you to select the recipients of the patch installation task:

- **The current computer:** the task will have the computer selected in the list as recipient.
- **Install on all computers in the selected filter**: select a filter from the filter tree displayed. The patch will be installed on all computers in the selected filter.
- **Install on all computers:** the patch will be installed on all computers on the network.

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string

Table 14.19: Fields in the 'Patch detected' window

Field	Comments	Values
Criticality	Indicates the update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer	Name of the computer with outdated software.	Character string
Installation status	Indicates if the patch is already included in the repository that contains the patches to be applied to computers or if it must be manually downloaded and added to the patch repository by the administrator.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update may require more space on the target computer's storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its installation requirements (if any).	Character string
Download URL	URL for downloading the patch individually.	Character string
File name	Name of the file that contains the patch.	Character string

Table 14.19: Fields in the 'Patch detected' window

End-of-Life programs

Shows programs that are no longer supported by the relevant vendor. These programs are particularly vulnerable to malware and cyberthreats.

Field	Comments	Values
Computer	Name of the computer with EOL software.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to	Character string

Table 14.20: Fields in the 'End-of-Life programs' list

Field	Comments	Values
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program entered its EOL stage.	Date (in red if the program has reached its EOL).

Table 14.20: Fields in the 'End-of-Life programs' list

*To view a graphical representation of the list data, go to widget "**End-of-Life programs**".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program entered its EOL stage.	Date
Last seen	Date when the computer was last discovered.	Date

Table 14.21: Fields in the 'End-of-Life programs' exported file

- **Filter tool**

Field	Comments	Values
Find computer	Computer name.	Character string
End-of-Life date	Date when the program will reach its EOL.	• All • Currently in End of Life • In End of Life (currently or in 1 year)

Table 14.22: Filters available in the 'End-of-Life programs' list

- **'Program details' window**

Clicking any of the programs in the list opens the **Program details** window.

Field	Comments	Values
Program	Name of the program or Windows operating system that reached its end of life.	Character string
Family	Bundle, suite, or program group the software belongs to.	Character string
Publisher/ Company	Company that designed or published the program.	Character string
Version	Program version.	Character string
EOL	Date when the program reached its end of life.	Date

Table 14.23: Fields in the 'Program details' window

Installation history

Shows the patches that Panda Patch Management attempted to install and the computers that received them in a given time interval.

Field	Comments	Values
Date	Date when the patch or update was installed.	Date
Computer	Name of the computer that received the patch or update.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the program or Windows operating system that received the patch or update.	Character string
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the installed patch.	• Other patches • Critical • Important • Moderate • Low • Unspecified • Service Pack

Table 14.24: Fields in the 'Installation history' list

Field	Comments	Values
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • Uninstalled • The patch is no longer required
Context menu	Displays a drop-down menu with options.	• **View task**: shows the settings of the patch installation or uninstallation task.

Table 14.24: Fields in the 'Installation history' list

*To view a graphical representation of the list data, go to widget "***Last patch installation tasks***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Date	Date of the installation attempt.	Date
Program	Name of the program or Windows operating system that received the patch or update.	Character string
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	Character string

Table 14.25: Fields in the 'Installation history' exported file

Field	Comments	Values
Criticality	Severity rating of the installed patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Installation error	The Panda Patch Management module didn't install correctly	• **Unable to download**: Installer not available • **Unable to download**: The file is corrupted • **Not enough disk space**
Download URL	URL for downloading the patch individually.	Character string
Result code	Code indicating the result of the patch installation task. Success or reason for failure. Refer to the vendor's documentation for more information on how to interpret the result code	Numeric value

Table 14.25: Fields in the 'Installation history' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Find computer	Computer name.	Character string
From	Start date for the search range.	Date
To	End date for the search range.	Date
Criticality	Severity rating of the installed patch.	• Critical (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string

Table 14.26: Filters available in the 'Installation history' list

- **'Patch installed' window**

Clicking any of the rows in the list opens the Patch installed window. This window provides detailed information about the patch.

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Table 14.27: Fields in the 'Patch installed' window

Field	Comments	Values
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Installation date	Date the patch was successfully installed on the computer.	Date
Result	Installation status of the patch or update.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update may require more space on the target computer's storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its installation requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 14.27: Fields in the 'Patch installed' window

Excluded patches

This list shows those patches that the administrator has excluded, preventing them from being installed on the computers on the organization's network. The list displays a line for each computer-excluded patch pair, except in the case of those patches excluded for all computers on the network, for which a single line is displayed.

Field	Comments	Values
Computer	The content of this field will vary depending on the target of the exclusion: • 🖥 If the patch was excluded for a single computer, the field will display the computer name. • 🌐 If the patch was excluded for all computers in the account, the text "(All)" will be displayed.	Character string
Group	Folder in the Panda Endpoint Protection group tree to which the computer belongs.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the excluded patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Excluded by	Management console user account who excluded the patch	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.28: Fields in the 'Excluded patches' list

*To view a graphical representation of the list data, go to widget "***Available patches***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	The content of this field will vary depending on the target of the exclusion: • If the patch was excluded for a single computer, the field will display the computer name. • If the patch was excluded for all computers in the account, the text "(All)" will be displayed.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	The computer's description entered by the network administrator.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the excluded patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string

Table 14.29: Fields in the 'Excluded patches' exported file

Field	Comments	Values
Release date	Date when the patch was released for download and application.	Date
Download size (KB)	Patch size in compressed format. Applying the patch may require more space on the target computer's storage media than indicated in this field.	Numeric value
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.29: Fields in the 'Excluded patches' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer for which patches have been excluded.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Show non-downloadable patches	Shows those patches that cannot be directly downloaded by Panda Patch Management as there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.)	Boolean
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Criticality	Severity rating of the excluded patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related)

Table 14.30: Filters available in the 'Excluded patches' list

Field	Comments	Values
		• Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.30: Filters available in the 'Excluded patches' list

- **'Excluded patch' window**

Clicking any of the rows in the list opens the **Excluded patch** window. This window provides detailed information about the patch excluded from installation tasks.

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related)
		• Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update may require more space on the target computer's storage media than indicated in this field.	Numeric value

Table 14.31: Fields in the 'Excluded patch' window

Field	Comments	Values
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its installation requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 14.31: Fields in the 'Excluded patch' window

Patch installation/uninstallation task results

This list shows the results of the patch installation or uninstallation tasks performed on the computers on your network.

Field	Description	Values
Name	Name of the computer the patch was installed/ uninstalled from.	Character string
Group	Panda Endpoint Protection group to which the computer belongs.	Character string
Status	Task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Patches installed/ uninstalled	Number of patches installed/uninstalled.	Character string.
Start date	Date the installation task started.	Date
End date	Date the installation task ended.	Date

Table 14.32: Fields in the 'Installation/uninstallation task results' list

*To view a graphical representation of the list data, go to widget "**Last patch installation tasks**".*

- **Filter tools**

Field	Description	Values
Status	Installation/uninstallation task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Applied/ Uninstalled patches	Computers on which patches have been installed/uninstalled.	• All • No patches installed/uninstalled • With patches installed/uninstalled

Table 14.33: Filters available in the 'Patch installation/uninstallation task results' list

View installed/uninstalled patches

This list shows the patches installed on computers and other additional information.

Field	Description	Values
Computer	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Panda Endpoint Protection group to which the computer belongs.	Character string
Program	Patched program.	Character string
Version	Program version.	Character string
Patch	Installed/uninstalled patch.	Character string
Criticality	Relevance of the installed/uninstalled patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.34: Fields in the 'View installed/uninstalled patches' list

Field	Description	Values
Result	Indicates if the task was completed successfully or failed.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Date	Date the task was run.	Date

Table 14.34: Fields in the 'View installed/uninstalled patches' list

*To view a graphical representation of the list data, go to widget "***Last patch installation tasks***".*

Chapter 15

Panda Full Encryption (Device encryption)

Panda Full Encryption is a built-in module on Aether Platform that encrypts the content of the data storage media connected to the computers managed by Panda Endpoint Protection. By doing this, it minimizes the exposure of corporate data in the event of data loss or theft as well as when storage devices are removed without having deleted the data.

Panda Full Encryption is compatible with Windows 7 and later versions of the OS (see section "**Supported operating system versions**") and enables you to monitor the encryption status of network computers and centrally manage the corresponding recovery keys. It also takes advantage of hardware resources such as TPM, delivering great flexibility when it comes to choosing the optimum authentication system for each computer.

For more information about the different features of the Panda Full Encryption module, see the following sections:

- "**Creating and managing settings**": information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**": managing user accounts and assigning permissions.
- "**The management console**": information on how to manage lists.

CHAPTER CONTENT

Introduction to encryption concepts

Panda Full Encryption uses the tools integrated in Windows operating systems to manage encryption on network computers protected with Panda Endpoint Protection.

In order to understand the processes involved in the encryption and decryption of information, we will first present some concepts related to the encryption technology used.

TPM

TPM (Trusted Platform Module) is a chip included in the motherboards of some desktops, laptops and servers. Its main aim is to protect users' sensitive data, stored passwords and other information used in login processes.

The TPM is also responsible for detecting changes in the chain of startup events on a computer, for example preventing access to a hard drive from a computer other than the one used for its encryption.

The minimum version of TPM supported by Panda Full Encryption is 1.2. and Panda Security recommends it is used along with other supported authentication systems. The TPM may be disabled in the computer BIOS in some scenarios and it may be necessary to enable it manually.

Supported password types

- **PIN**

The PIN (Personal Identification Number) is a sequence of numbers that serves as a simple password and is necessary to start a computer with an encrypted drive. Without the PIN, the boot sequence is not completed and it is impossible to access the computer.

- **Extended PIN**

If the hardware is compatible, Panda Full Encryption uses an extended or enhanced PIN combining letters and numbers to increase the complexity of the password.

Given that the extended PIN is required in the process of starting up the computer, before the operating system is loaded, the limitations of the BIOS may restrict access from the keyboard to the 7-bit ASCII table. Moreover, keyboards other than EN-US, such as QWERTZ or AZERTY keyboards, may lead to errors when entering the extended PIN. For this reason, Panda Full Encryption checks that the characters entered by users belong to the EN-US charset before setting the extended PIN in the process of encrypting the computer.

- **Passphrase**

A passphrase is similar to a password, but is typically longer. It consists of alphanumeric characters and is equivalent to the extended PIN.

Panda Full Encryption prompts users for a different type of password based on the following circumstances:

- **Passphrase**: if the computer has a TPM installed.
- **Extended PIN**: if the computer operating system and hardware support it.
- **PIN**: if the other options are not valid.

USB key

This allows you to store the encryption key on a USB device formatted with NTFS, FAT or FAT32. This means that you don't have to enter any password to start up the computer, but you do need to connect the USB device.

> *Some older PCs cannot access USB devices during the startup process. Check whether the computers in your organization have access to USB devices from the BIOS.*

Recovery key

When an irregular situation is detected on a computer protected by Panda Full Encryption, or if you forget the password, the computer will ask you for a 48-digit recovery key. This password is managed from the management console and must be entered in order to complete the startup process in these circumstances. Each encrypted drive will have its own specific recovery key.

> Panda Full Encryption *only stores the recovery keys for the computers it manages. The management console will not display the passwords for computers encrypted by users or those not managed by Panda Security.*

The recovery key will be requested in the following circumstances:

- When the PIN or passphrase is entered incorrectly repeatedly in the startup process.
- When a computer protected with TPM detects a change to the startup sequence (hard disk protected with TPM and connected to another computer).
- When the motherboard has been changed and consequently the TPM.
- On disabling or deleting the TPM content.
- On changing the startup settings.
- When the startup process is changed:
    - BIOS update.
    - Firmware update.
    - UEFI update.
    - Changes to the boot sector.
    - Changes to the master boot record.
    - Changes to the boot manager.
    - Changes to the firmware in certain components that take part in the boot process (video cards, disk controllers, etc), known as the Option ROM.
    - Changes to other components that take part in the initial startup phases.

BitLocker

This is the software installed on some versions of Windows 7 and later and which is responsible for encrypting and decrypting the data stored on the computer drives. Panda Full Encryption installs BitLocker automatically on those server versions that do not have it but are compatible.

System partition

This is a small area of the hard disk -approximately 1.5 gigabytes- which is unencrypted and is required for the computer to correctly complete the startup process. Panda Full Encryption automatically creates this system partition if it does not already exist.

Encryption algorithm

The encryption algorithm in Panda Full Encryption is AES-256, though computers with drives encrypted by users with other algorithms are also compatible.

Panda Full Encryption service overview

The general encryption process covers several areas that administrators should be aware of in order to adequately manage network resources that could contain sensitive information or compromising data if the drive were to be lost or stolen:

- **Meeting minimum hardware and software requirements:** See section "**Panda Full Encryption minimum requirements**" to see the limitations and specific conditions of each supported platform.
- **Previous encryption status of the user's computer**: Depending on whether BitLocker was used before on the user's computer, the process of integration in Panda Endpoint Protection may vary slightly.
- **Assigning encryption settings**: Determine the encryption status (encrypted or not) of network computers and the authentication methods.
- **Interaction of the user with the encryption process:** The initial encryption process requires user interaction. See section "**Encryption of previously unencrypted drives**".
- **Viewing the network encryption status** with the widgets/panels in the **Status** menu, **Full Encryption** side panel. See section "**Panda Full Encryption panels and widgets**" for a complete description of the widgets included in Panda Full Encryption. Filters are also supported to locate computers in the lists according to their status. See section "**Available filters**".
- **Restriction of encryption permissions to security administrators**: The roles system described in "**Understanding permissions**" on page **57** covers the functionality of the encryption module and viewing of the status of network computers.
- **Access to the recovery key**: Where users forget the PIN/passphrase or when the TPM has detected an irregular situation, the network administrator can centrally obtain the recovery key and send it to the user. See section "**Getting the recovery key**"

General features of Panda Full Encryption

Supported authentication types

Depending on whether there is a TPM and on the OS version, Panda Full Encryption allows different combinations of authentication methods. These are as follows, and in the order that they are recommended by Panda Security:

- **TPM + PIN**: compatible with all supported versions of Windows. The TPM chip must be enabled in the BIOS and a PIN must be established.
- **Only TPM**: compatible with all supported versions of Windows. The TPM chip must be enabled in the BIOS except in Windows 10, where it is automatically enabled.
- **USB key**: requires a USB device and that the computer can access USB drives during startup. Required on Windows 7 computers without TPM.
- **Passphrase**: only available on Windows 8 and later without TPM.

By default, Panda Full Encryption uses an encryption method that includes the use of the TPM if available. If you choose an authentication routine not included in the above list, the management console will display a warning indicating that the computer will not be encrypted.

Supported storage devices

Panda Full Encryption encrypts all internal mass storage devices:

- Fixed storage drives on the computer (system and data)
- Virtual hard drives (VHD), though only used space, regardless of what appears in the management console.
- Removable hard drives.
- USB drives.

The following are not encrypted:

- Dynamic hard disks.
- Very small partitions.
- Other external storage devices.

Panda Full Encryption minimum requirements

The minimum requirements are split into:

- Versions of the Windows operating system and compatible families.
- Hardware requirements.

Supported operating system versions

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows Server 2008 R2 and later (including Server Core editions)

Hardware requirements

- TPM 1.2 and later if this method of authentication is used.
- USB key and computer that supports reading USB devices from the BIOS in Windows 7.

Management of computers according to their prior encryption status

Management of computers by Panda Full Encryption

For a computer to be managed by Panda Full Encryption, it must meet the following conditions:

- It must meet the minimum requirements described in section "**Panda Full Encryption minimum requirements**".
- The computer must have successfully received, at least once, settings from the management console that establish the encryption of the drives.

Computers that previously had some drives encrypted and have not received settings to encrypt their drives will not be managed by Panda Full Encryption and, therefore, the administrator will not have access to the recovery key or the status of the computer.

However, computers that have received settings to encrypt drives, regardless of their previous status (encrypted or not) will be managed by Panda Full Encryption.

Uninstallation of the Panda Endpoint Protection agent

Regardless of whether the computer was managed by Panda Full Encryption or not, if the drives were encrypted, when uninstalling Panda Endpoint Protection they will be left as they are. However, centralized access to the recovery key will be lost.

If the computer is subsequently reinstated in Panda Endpoint Protection, the last stored recovery key will be displayed.

Encryption and decryption

Encryption of previously unencrypted drives

The encryption process starts when the Panda Endpoint Protection agent installed on the user's computer downloads Encryption settings. At that moment, the user will see a window that will guide them through the process.

The total number of steps involved varies depending on the type of authentication chosen by the administrator and the previous status of the computer. If any of the steps ends in an error, the agent will report it to the management console and the process will stop.

> ⚠ *It is not permitted to encrypt computers from a remote desktop session as it is necessary to restart the computer and enter a password before loading the operating system, actions that are not possible with a standard remote desktop tool.*
>
> *The encryption process will begin when installation or uninstallation of patches run by Panda Full Encryption has finished.*

Below we describe the complete encryption process and whether feedback is displayed to the computer user and if a restart is required:

Step	Process on the computer	User interaction
1	The agent receives the settings from the encryption module, which asks for the content of the storage drives installed to be encrypted.	None.
2	If the computer is a server and does not have BitLocker tools installed, they are downloaded and installed.	A window is displayed requesting permission to restart the computer and complete installation of BitLocker or to postpone the process. If 'postpone' is selected, the request will be made again during the next login. **Requires restart.**
3	If the computer wasn't previously encrypted, the system partition is created.	A window appears asking for permission to restart the computer and complete the creation of the system partition or postpone it. If 'postpone' is selected, the process will be stopped and the user will be asked again during the next login. **Requires restart.**

Table 15.1: Steps for encrypting previously unencrypted drives

Step	Process on the computer	User interaction
4	If there is a group policy previously established by the administrator and which conflicts with those set by Panda Full Encryption, an error message will appear and the process will stop. The group policies configured by Panda Full Encryption are: In the local group policy editor, follow this path: Local computer policy > Computer configuration > Administrative templates > Windows components > BitLocker drive encryption > Operating system drives. Select Not set for the specified policies to avoid this error.	If the administrator has not defined global group policies that conflict with the local ones defined by Panda Full Encryption, no message will appear.
5	Preparing the TPM if it exists, and whether the authentication method selected requires this component and whether it was previously enabled from the BIOS.	This requires confirming a restart so that the user can enter the BIOS on the computer to enable the TPM. In Windows 10 there is no need to alter the BIOS but restart is required. The restart in step 3, if required, will combine with this one.
6	Preparing the USB device if the authentication method selected requires this component.	This requires users to plug in a USB device to store the password for starting the computer.
7	Storing the PIN if the authentication method selected requires this component.	The user is required to enter the PIN. If alphanumeric characters are used and the hardware is not compatible with those characters, error "-2144272180" will be displayed. In that case, a numerical PIN must be entered.
8	Storing the passphrase if the authentication method selected requires this component.	The user is required to enter the passphrase.
9	The recovery key is generated and sent to the Panda Security cloud. Once it has been received, the process continues on the user's computer.	None.
10	Checking that the hardware on the computer is compatible with the encryption technology. The encryption process begins.	Confirmation of restart is required in order to check the hardware used in the various authentication methods. **Requires restart.**
11	Encryption of drives.	The encryption process begins and runs in the background, without interfering with the user. The length of the process will depend on the drive being encrypted. On average, the encryption time will be about 2-3 hours.

Table 15.1: Steps for encrypting previously unencrypted drives

Step	Process on the computer	User interaction
		Users can use and switch off computers. In the latter case, the process will continue whenever the computer is restarted.
12	The encryption process takes place silently and from then on is completely invisible to the user.	Depending on the authentication method selected, the user may need to enter a USB key, a PIN, a passphrase or nothing at all when the computer restarts.

Table 15.1: Steps for encrypting previously unencrypted drives

Encryption of previously encrypted drives

If any drive on the computer is already encrypted, Panda Full Encryption will alter certain parameters so that it can be centrally managed. The action taken is as follows:

- If the authentication method chosen by the user does not coincide with the one specified in the settings, the latter will change, and the user will be asked for the necessary passwords or hardware resources. If it is not possible to assign an authentication method compatible with the platform and specified by the administrator, the computer will continue using the user's encryption and will not be managed by Panda Full Encryption.
- If the encryption algorithm used is not supported (not AES-256), no change will take place to avoid complete decryption and encryption of the drive but the computer will be managed by Panda Full Encryption.
- If there are both encrypted and unencrypted drives, all drives will be encrypted with the same authentication method.
- If the previous authentication method required a password to be entered, and is compatible with the methods supported by Panda Full Encryption, the user will be asked for the password in order to unify the authentication method in all drives.
- If the user chose encryption settings different from those set by the administrator (encryption solely of the occupied sectors not the whole drive), no changes will be made in order to minimize the encryption process.
- At the end of the process, the device will be managed by Panda Full Encryption. A recovery key will be generated and sent to Panda Security's cloud.

Encryption of new drives

If a user creates a new drive after the encryption process is complete, Panda Full Encryption will encrypt it immediately, respecting the encryption settings assigned by the network administrator.

Decrypting drives

There are three scenarios:

- If Panda Full Encryption encrypts a computer, from that moment the administrator can assign settings to decrypt it.

- If a computer was encrypted by the user prior to the installation of Panda Full Encryption and is assigned encryption settings, it will be considered encrypted by Panda Full Encryption and can be decrypted by assigning settings from the management console.
- If a computer was already encrypted by the user prior to installing Panda Full Encryption and has never been assigned encryption settings, it will not be considered encrypted by Panda Full Encryption and cannot be decrypted by assigning settings from the management console.

Local editing of BitLocker settings

The computer user has access to the local BitLocker settings from the Windows tools, but the changes made will immediately revert to the settings established by the network administrator through the management console. The way that Panda Full Encryption responds to a change of this type is described below:

- **Disable automatic locking of a drive**: It reverts to automatic locking.
- **Eliminate the password of a drive**: A new password will be requested.
- **Decrypt a drive previously encrypted by** Panda Full Encryption: The drive will automatically be encrypted.
- **Encrypt a decrypted drive**: If the Panda Full Encryption settings imply decrypting drives, the user action takes preference and the drive won’t be decrypted.

Encrypting and decrypting external hard drives and USB keys

As users can connect and disconnect external storage devices from their computers at any time, the way Panda Full Encryption works with these devices is as follows:

- If the workstation or server does not have BitLocker installed and running, the agent will not download the required packages and the device will not be encrypted. Nor will any messages be displayed to the user.
- If the computer has BitLocker installed and running, a pop-up message will be displayed to the user prompting them to encrypt the device in the following situations:
  - Every time they connect an unencrypted USB storage device.
  - If there is an unencrypted device connected to the computer at the time the administrator enables the encryption settings from the Web console.
- The encryption message will be displayed to the user for 5 minutes, after which it will disappear. Regardless of whether the user agrees to encrypt the device or not, they will be able to use the device normally, unless settings have been configured that prevent the use of unencrypted devices. Refer to “**Write to removable storage drives**” on page **253**.
- Encrypting a USB device does not require creating a system partition.
- If the external storage device is already encrypted by a solution other than Panda Full Encryption, and the user connects it to their computer, the encryption message will not be displayed and the device can be used normally. Panda Full Encryption will not send the recovery keys to the Web

console.

- Writing to the USB device won't be allowed if the option **Write to removable storage drives** in Panda Data Control is set to ON and the device has not bee encrypted by BitLocker or by Panda Full Encryption. Refer to "Write to removable storage drives".
- To decrypt a device encrypted by Panda Full Encryption, the user can use BitLocker manually.
- Only the space used is encrypted.
- All partitions on the device are encrypted with the same key.

⚠ *Removing a USB device when the encryption process is not complete might corrupt its contents*

Panda Full Encryption response to errors

- **Errors in the hardware test**: The hardware test runs every time the computer is started up until it is passed, at which time the computer will automatically begin encryption.
- **Error creating the system partition**: Many of the errors that occur when creating the system partition can be rectified by the user (e.g. lack of space). Periodically, Panda Full Encryption will automatically attempt to create the partition.
- **User refusal to activate the TPM chip**: The computer will display a message on startup asking the user to activate the TPM chip. Until this condition is resolved, the encryption process will not commence.

Getting the recovery key

In cases where the user has lost the PIN/passphrase/USB device or where the TPM chip has detected a change to the series of events for starting the device, it will be necessary to enter the recovery key. Panda Full Encryption keeps all the recovery keys for the encrypted network computers that it manages.

To get the recovery key for a computer, follow the steps below:

- In the **Computers** menu, click the computer for which you want to obtain the key.
- In the **Details** tab, in **Data protection**, click the **Get recovery key** link. You will see a link with the identifiers of the encrypted drives.
- Click a drive identifier to display the recovery key.

Panda Full Encryption panels and widgets

Accessing the dashboard

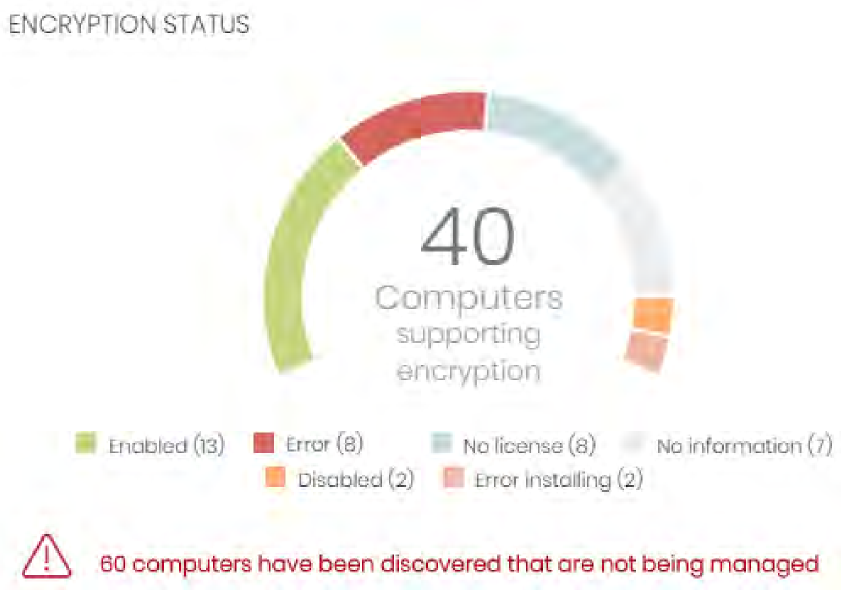
To access the dashboard, click the **Status** menu at the top of the console and then click **Full Encryption** from the side menu.

Required permissions

No additional permissions are required to access the widgets associated with Panda Full Encryption.

Encryption Status

This shows all the computers that support Panda Full Encryption as well as their encryption status.



⚠ 60 computers have been discovered that are not being managed

Figure 15.1: Encryption status pane

- **Meaning of the data**

Status	Description
Enabled	Computers with Panda Full Encryption installed, settings assigned to encrypt the computer and which haven't reported encryption or installation errors.
Disabled	Computers with Panda Full Encryption installed, settings assigned to not encrypt the computer and which haven't reported encryption or installation errors.
Error	It hasn't been possible to carry out the action that the administrator specified in the encryption or decryption settings.
Error installing	It hasn't been possible to install and download BitLocker if it were required.

Table 15.2: Meaning of the Encryption Status panel

Status	Description
No license	The computer is compatible with Panda Full Encryption but no license is assigned.
No information	Computers with a recently assigned license and which haven't yet reported their status to the server, or a computer with an out-of-date agent.

Table 15.2: Meaning of the Encryption Status panel

- **Lists accessible from the panel**

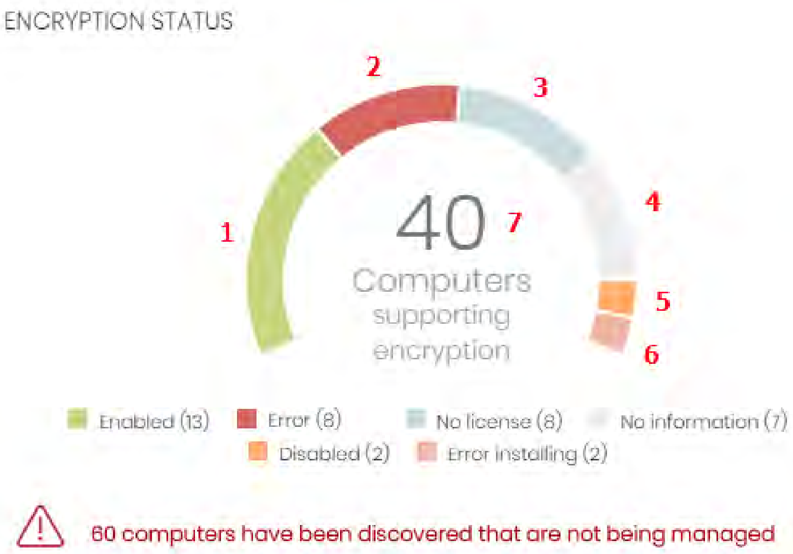


Figure 15.2: Hotspots in the Encryption Status panel

Click the hotspots shown in figure 16.2 to access the **Encryption Status** list with the following predefined filters:

Hotspot	Filter
(1)	Encryption status = Enabled
(2)	Encryption status = Error
(3)	Encryption status = No license
(4)	Encryption status = No information
(5)	Encryption status = Disabled
(6)	Encryption status = Error installing
(7)	No filter

Table 15.3: Filters available in the Encryption Status list

Computers Supporting Encryption

This shows the computers that are compatible (or not) with the encryption technology, grouped by type.

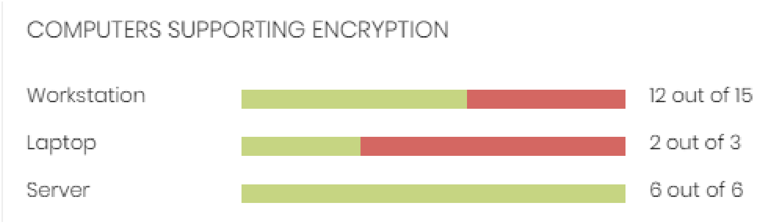


Figure 15.3: Computers Supporting Encryption panel

- **Meaning of the data displayed**

Data	Description
Workstation - green	Workstations that support encryption.
Workstation - red	Workstations that don't support encryption.
Laptop - green	Laptops that support encryption.
Laptop - red	Laptops that don't support encryption.
Server - green	Servers that support encryption.
Server - red	Servers that don't support encryption.

Table 15.4: Description of the Computers Supporting Encryption panel

- **Lists accessible from the panel**

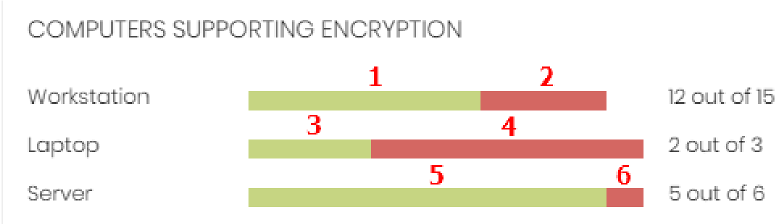


Figure 15.4: Hotspots in the Computers Supporting Encryption panel

By clicking the areas in the panel, the **Encryption Status** list opens displaying the following filters:

Hotspot	Filter
(1)	Computer type = Workstation
(2)	List of computers filtered by **Encryption not supported.**
(3)	Type of computer = Laptop
(4)	List of computers filtered by **Encryption not supported.**

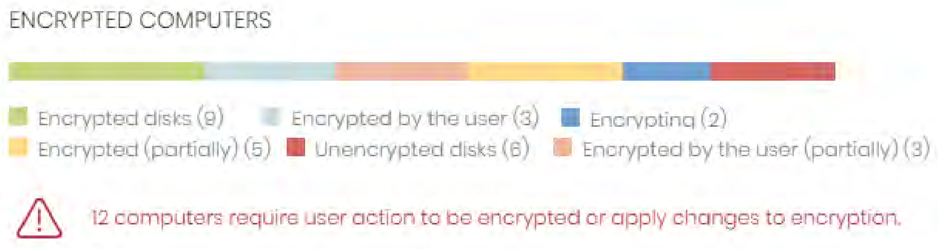
Table 15.5: Lists accessible from the Encryption Status panel

Hotspot	Filter
(5)	Type of computer = Server
(6)	List of computers filtered by **Encryption not supported.**

Table 15.5: Lists accessible from the Encryption Status panel

Encrypted Computers

This shows the encryption status of the network computers that support Panda Full Encryption.



ENCRYPTED COMPUTERS

🟩 Encrypted disks (9) ⬜ Encrypted by the user (3) 🟦 Encrypting (2)
🟨 Encrypted (partially) (5) 🟥 Unencrypted disks (6) 🟧 Encrypted by the user (partially) (3)

⚠ 12 computers require user action to be encrypted or apply changes to encryption.

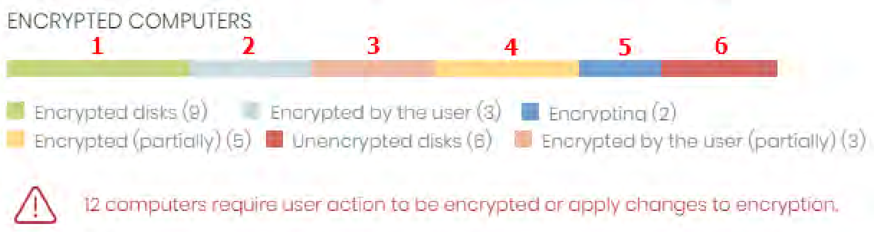
Figure 15.5: Encrypted Computers panel

- **Meaning of the data displayed**

Data	Description
Unknown	Disks encrypted with an authentication method not supported by Panda Full Encryption.
Unencrypted disks	None of the disks on the computer are encrypted by the user nor by Panda Full Encryption.
Encrypted disks	All the disks on the computer are encrypted by Panda Full Encryption.
Encrypting	At least one of the disks on the computer is in the process of being encrypted.
Decrypting	At least one of the disks on the computer is in the process of being decrypted.
Encrypted by the user	All the disks on the computer are encrypted, but some or all of them were encrypted by the user.
Encrypted by the user (partially)	One or more disks on the computer are encrypted by the user and the rest are either unencrypted or are encrypted by Panda Full Encryption.
Encrypted (partially)	At least one of the disks on the computer is encrypted by Panda Full Encryption but the rest are unencrypted.

Table 15.6: Description of the Encrypted Computers panel

- **Lists accessible from the panel**


ENCRYPTED COMPUTERS
1
2
3
4
5
6
Encrypted disks (9)
Encrypted by the user (3)
Encrypting (2)
Encrypted (partially) (5)
Unencrypted disks (6)
Encrypted by the user (partially) (3)

12 computers require user action to be encrypted or apply changes to encryption.

Figure 15.6: Hotspots in the Encrypted Computers panel

Click the hotspots shown in figure 15.6 to access the **Encryption Status** list with the following predefined filters:

Hotspot	Filter
(1)	Disk encryption = Encrypted disks
(2)	Disk encryption = Encrypted by the user
(3)	Disk encryption = Encrypted by the user (partially)
(4)	Disk encryption = Encrypted (partially)
(5)	Disk encryption = Encrypting
(6)	Disk encryption = Unencrypted disks
(7)	Disk encryption = Decrypting
(8)	Disk encryption = Unknown

Table 15.7: Lists accessible from the Encryption Status panel

Authentication Method Applied

This displays the network computers with encryption according to the type of encryption used.

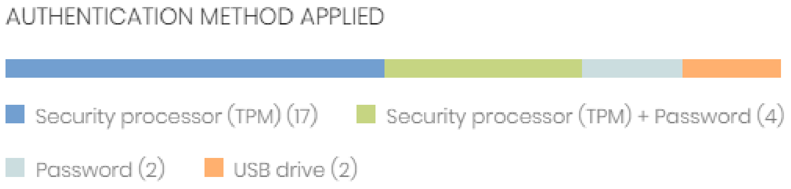

AUTHENTICATION METHOD APPLIED
Security processor (TPM) (17)
Security processor (TPM) + Password (4)
Password (2)
USB drive (2)

Figure 15.7: Authentication Method panel

- **Meaning of the data displayed**

Data	Description
Unknown	The authentication method selected by the user is not supported by Panda Full Encryption.

Table 15.8: Description of the Authentication Method Applied panel

Data	Description
Security processor (TPM)	The authentication method used is TPM.
Security processor (TPM) + Password	The authentication method used is TPM and PIN or passphrase requested on startup.
Password	The authentication method is PIN or passphrase requested on startup.
USB drive	The authentication method is a USB key connected during startup.
Unencrypted	None of the disks on the computer are encrypted.

Table 15.8: Description of the Authentication Method Applied panel

- **Lists accessible from the panel**

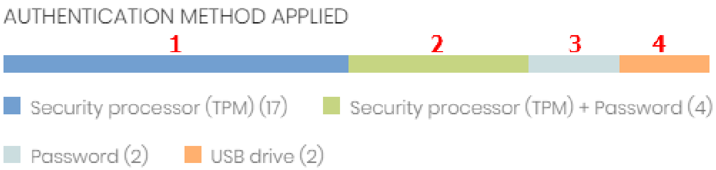


Figure 15.8: Hotspots in the Authentication Method Applied panel

Click the hotspots shown in figure 15.8 to access the **Encryption Status** list with the following predefined filters:

Hotspot	Filter
(1)	Authentication method = Security processor (TPM)
(2)	Authentication method = Security processor (TPM) + Password
(3)	Authentication method = Password
(4)	Authentication method = USB drive
(5)	Authentication method = Unknown
(6)	Authentication method = Unencrypted

Table 15.9: Lists accessible from the Authentication Method Applied panel

Panda Full Encryption lists

Accessing the lists

There are two ways to access the lists:

- Click the **Status** menu at the top of the console. Then, click **Full Encryption** from the side menu and click the relevant widget.

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window will open with all available lists.
- Select a list from the **Data protection** section to view the associated template. Edit it and click **Save**. The new list will be added to the side menu.

Required permissions

Administrators don't need additional permissions to access the Encryption status list.

Encryption Status

This list shows all the computers on the network managed by Panda Endpoint Protection and that support Panda Full Encryption. It includes filters related to the module to see the encryption status of the network.

Field	Comment	Values
Computer	Name of the computer that supports the encryption technology.	Character string
Computer status	Agent reinstallation: • ⚙ Reinstalling the agent. • ⚙ Agent reinstallation error. Protection reinstallation: • ⚙ Reinstalling the protection. • ⚙ Protection reinstallation error. • ↻ Pending restart.	Icon
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	Character string
Operating system	Operating system and version installed on the workstation or server.	Character string
Encryption status	Status of the Panda Full Encryption module.	• No information • Enabled • Disabled • Error • Error installing • No license
Disk encryption	Encryption status of the disks on the computer.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting

Table 15.10: List fields

Field	Comment	Values
		• Decrypting • Encrypted by the user • Encrypted by the user (partially) • Encrypted (partially)
Authentication method	Authentication method selected for the encrypted disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted
Last connection	The last time the agent connected to the Panda Security cloud.	Date

Table 15.10: List fields

To view a graphical representation of the list data, go to widget **"Encrypted Computers"**.

- **Fields displayed in the exported file**

Field	Comment	Values
Client	Client account to which the service belongs.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer that supports the encryption technology.	Character string
IP address	Primary IP address of the computer.	Character string
Domain	Windows domain to which the computer belongs.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	Character string

Table 15.11: Fields in the exported file

Field	Comment	Values
Agent version	Internal version of the Panda module agent.	Character string
Installation date	Date that Panda Endpoint Protection was installed on the computer.	Date
Last connection		Date
Platform	Operating system installed on the computer.	Character string
Operating system	Internal version and patches of the operating system installed.	Character string
Updated protection	The protection module installed on the computer is the latest version released.	Boolean value
Protection version	Internal version of the protection module.	Character string
Updated knowledge	The signature file on the computer is the latest version.	Boolean value
Last update	Date the signature file was downloaded.	Date
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Disk status	Status of the computer's internal storage media with regard to encryption.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Encryption pending user action	User actions (entering data or restarting) are pending to complete the encryption process.	Boolean value
Authentication method	Authentication method chosen for the encryption.	• All • Unknown • Security processor (TPM)

Table 15.11: Fields in the exported file

Field	Comment	Values
		• Security processor (TPM) + Password • Password • USB drive • Not encrypted
Encryption date	Date when the first drive was encrypted and the computer was considered completely encrypted (all supported drives were encrypted).	Date
TPM spec version	Version of the TPM specifications supported by the chip on the computer.	Character string
Encryption installation error date	Date of the last reported installation error.	Date
Encryption installation error	An error occurred installing Panda Full Encryption on the computer.	Character string
Encryption error date	Last date that an encryption error was reported on the computer.	Date
Encryption error	The encryption process returned an error.	Character string

Table 15.11: Fields in the exported file

- **Filter tool**

Field	Comment	Values
Encryption date from	Date from which the computer was considered completely encrypted.	Date
Encryption date to	Date until which the computer was considered completely encrypted.	Date
Computer type	Type of device.	• Workstation • Laptop • Server
Disk status	Status of the computer's internal storage media with regard to encryption.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)

Table 15.12: List filters

Field	Comment	Values
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Authentication method	Authentication method selected.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted
Last connection	The last time the Panda Endpoint Protection status was sent to the Panda Security cloud.	Date

Table 15.12: List filters

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "**Details section (3)**" on page 167 for more information.

Encryption settings

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Encryption** from the side menu.
- Click the **Add** button to open the settings window.

Required permissions

Permission	Access type
Configure computer encryption	Create, edit, delete, copy, or assign Encryption settings.
View computer encryption settings	View the Encryption settings.

Table 15.13: Permissions required to access the Encryption settings

Panda Full Encryption settings

Encrypt all hard disks on computers

This indicates whether the computers will be encrypted or not. Depending on the previous status of the computers, the way that Panda Full Encryption acts will vary:

- If the computer is encrypted with Panda Full Encryption and **Encrypt all hard disks on computers** is disabled, all encrypted drives will be decrypted.
- If the computer is encrypted but not with Panda Full Encryption, and **Encrypt all hard disks on computers** is disabled, there will be no change.
- If the computer is encrypted but not with Panda Full Encryption, and **Encrypt all hard disks on computers** is enabled, the internal encryption settings will be adjusted to coincide with the encryption methods supported by Panda Full Encryption, thereby avoiding re-encrypting the drive. See section "**Encryption of previously encrypted drives**".
- If the computer is not encrypted and **Encrypt all hard disks on computers** is enabled, all the drives will be encrypted as described in section "**Encryption of previously unencrypted drives**"

Ask for password to access the computer

This enables password authentication on starting up the computer. Depending on the platform and whether there is TPM hardware, two types of passwords are permitted:

- **Computers with TPM**: a PIN type password will be requested.
- **Computers without TPM**: a passphrase will be requested.

⚠ *If this option is set to 'No' and the computer doesn't have access to a compatible TPM security processor, the disks will not be encrypted.*

Do not encrypt computers that require a USB drive for authentication

To prevent the use of USB devices supported by Panda Full Encryption in authentication, administrators can disable their use.

⚠ *Only Windows 7 without TPM can use USB authentication. If administrators disable USB devices, these computers will not be encrypted.*

Encrypt used disk space only

The administrator can minimize the encryption time by restricting the feature to the sectors of the hard disk that are actually being used. The sectors released after deleting a file will remain encrypted, but the space that was free prior to the encryption of the hard disk will remain unencrypted, and will be accessible to third parties using tools for recovering deleted files.

Prompt for removable storage drive encryption

Displays a window prompting the user to encrypt the external mass storage devices and USB keys connected to the computer. Refer to "**Encrypting and decrypting external hard drives and USB keys**" for more information about the behavior and requirements for this setting.

Available filters

To locate network computers with any of the encryption statuses defined in Panda Endpoint Protection, use the filter tree resources shown in section "**Filter tree**" on page 134. The available filters are as follows:

- Encryption
  - Encryption pending user action
  - Disk encryption
  - Encryption date
  - Authentication method
  - Is waiting for the user to perform encryption actions
- Settings
  - Encryption
- Computer
  - Has a TPM
- Hardware
  - TPM - Activated
  - TPM - Manufacturer
  - TPM - Owner
  - TPM - Version
  - TPM – Spec version
- Modules
  - Encryption

Part 6

Viewing and managing threats

Chapter 16

Malware and network visibility

Panda Endpoint Protection offers administrators three large groups of tools for viewing the health and safety of the IT network they manage:

- The dashboard, with real-time, up-to-date information.
- Custom lists of incidents, detected malware and managed devices along with their status.
- Networks status reports with information collected and consolidated over time.

*For more information about consolidated reports, refer to "***Scheduled sending of reports and lists***" on page* **339**.

The visualization and monitoring tools determine in real time the network security status as well as the impact of any possible security breaches in order to facilitate the implementation of appropriate security measures.

CHAPTER CONTENT

Security panels/widgets

Panda Endpoint Protection shows the security status of the entire IT network or specific devices through widgets:

- **IT network**: click **Status** in the menu at the top of the console then **Security** 🛡 from the side menu, You will see counters showing the security status of the computers that are visible to the administrator. Refer to "**Role structure**" on page **56** for information about how to set the computer groups that are visible to the account used to access the management console, and "**Filter by group icon**" on page **35** to restrict the visibility of the groups defined in the role.
- **Computer**: click **Computers** in the menu at the top of the console, choose a computer from the network and click the **Detections** tab. You will see counters showing the security status of the selected computer. Refer to "**Detections section (4)**" on page **170**.

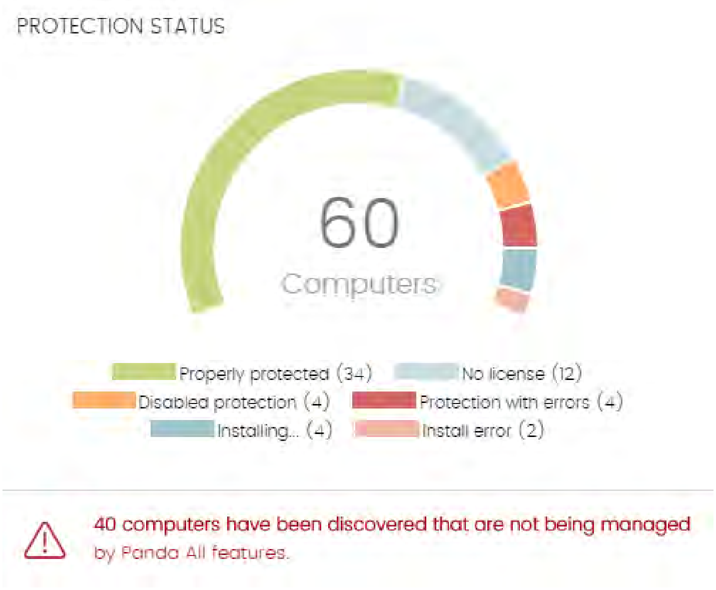
Below is a description of the different widgets displayed on the Panda Endpoint Protection dashboard, their areas and hotspots, as well as their tooltips and their meaning.

Protection status

Shows those computers where Panda Endpoint Protection is working properly and those where there have been errors or problems installing or running the protection module. The status of the network computers is represented with a circle with different colors and associated counters.

The panel offers a graphical representation and percentage of those computers with the same status.

> *The sum of all percentages can be greater than 100% as the status types are not mutually exclusive. A computer can have different statuses at the same time.*



40 computers have been discovered that are not being managed by Panda All features.

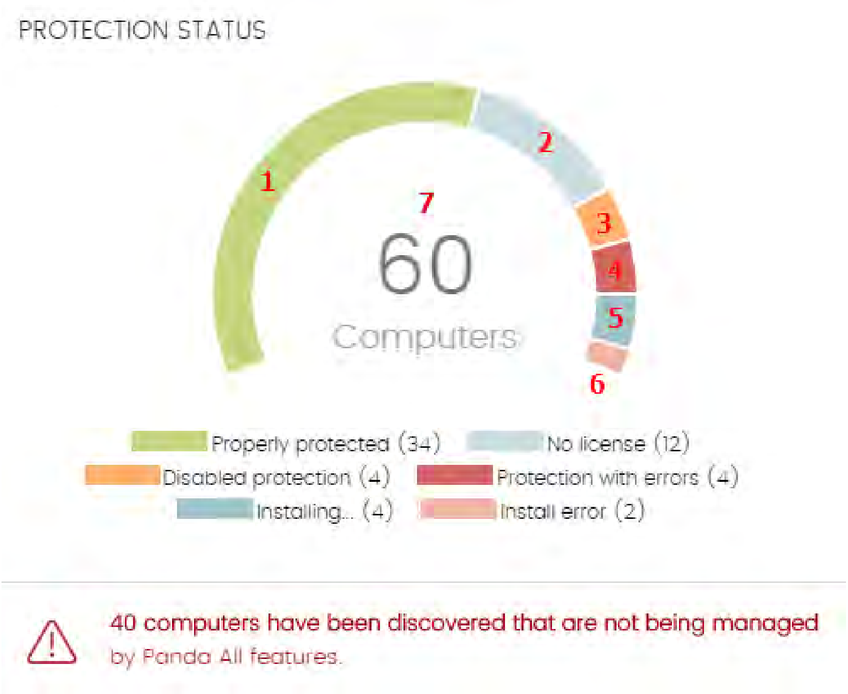
Figure 16.1: 'Protection status' panel

- **Meaning of the data displayed**

Data	Description
Properly protected	Percentage of computers where Panda Endpoint Protection installed without errors and is working properly.
Installing...	Percentage of computers on which Panda Endpoint Protection is currently being installed.
No license	Computers that are unprotected because there are insufficient licenses or because an available license has not been assigned to the computer.
Disabled protection	Computers where the antivirus protection is not enabled.
Protection with errors	Computers with Panda Endpoint Protection installed, but whose protection module does not respond to the requests sent from the Panda Security servers.
Installation error	Computers on which the installation process could not be completed.
Central area	Number of computers on the network with a Panda agent installed.

Table 16.1: Description of the data displayed in the 'Protection status' panel

- **Lists accessible from the panel**



40 computers have been discovered that are not being managed by Panda All features.

Figure 16.2: Hotspots in the 'Protection status' panel

Click the hotspots shown in figure 16.2 to access the **Computer protection status** list with the following predefined filters:

Hotspot	Filter
(1)	Protection status = Properly protected.
(2)	Protection status = Installing...
(3)	Protection status = Disabled protection.
(4)	Protection status = Protection with errors.
(5)	Protection status = No license.
(6)	Protection status = Installation error.
(7)	No filter.

Table 16.2: Filters available in the 'Computer protection status' list

Offline computers

Displays the computers that have not connected to the Panda Security cloud for a certain amount of time. These computers are susceptible to security problems and require special attention from the administrator.

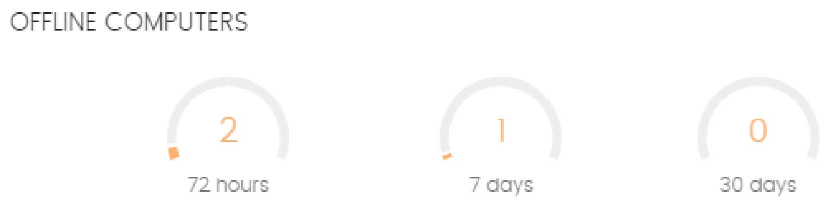


Figure 16.3: 'Offline computers' panel

- **Meaning of the data displayed**

Data	Description
72 hours	Number of computers that have not reported their status in the last 72 hours.
7 days	Number of computers that have not reported their status in the last 7 days.
30 days	Number of computers that have not reported their status in the last 30 days.

Table 16.3: Description of the data displayed in the ‘Offline computers’ panel

- **Lists accessible from the panel**

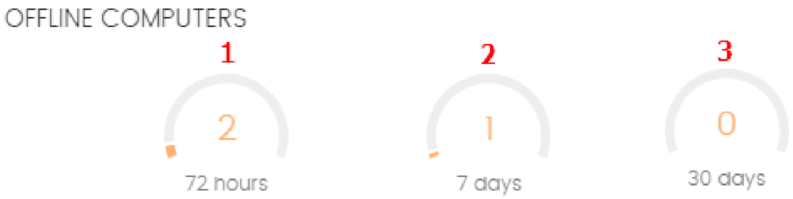


Figure 16.4: Hotspots in the 'Offline computers' panel

Click the hotspots shown in the figure 16.4 to access the **Offline computers** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 16.4: Filters available in the 'Offline computers' list

Outdated protection

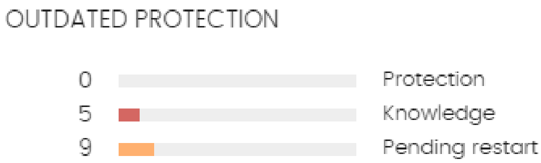


Figure 16.5: 'Outdated protection' panel

Displays the computers whose signature file is more than three days older than the latest one released by Panda Security. It also displays the computers whose antivirus engine is more than seven days older than the latest one released by Panda Security. Such computers are therefore vulnerable to attacks from threats.

- **Meaning of the data displayed**

The panel shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts:

Data	Description
Protection	For at least seven days, the computer has had a version of the antivirus engine older than the latest one released by Panda Security.
Knowledge	It has been at least three days since the computer has updated its signature file.
Pending restart	The computer requires a restart to complete the update.

Table 16.5: Description of the data displayed in the 'Outdated protection' panel

- **Lists accessible from the panel**

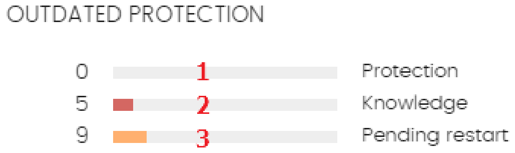


Figure 16.6: Hotspots in the ‘Outdated protection’ panel

Click the hotspots shown in the figure 16.6 to access the **Computers with out-of-date** protection list with the following predefined filters:

Hotspot	Filter
(1)	Updated protection = No.
(2)	Updated knowledge = No.
(3)	Updated protection = Pending restart.

Table 16.6: Filters available in the 'Computers with out-of-date protection' list

Threats detected by the antivirus

Consolidates all the intrusion attempts that Panda Endpoint Protection has dealt with in the selected time period.

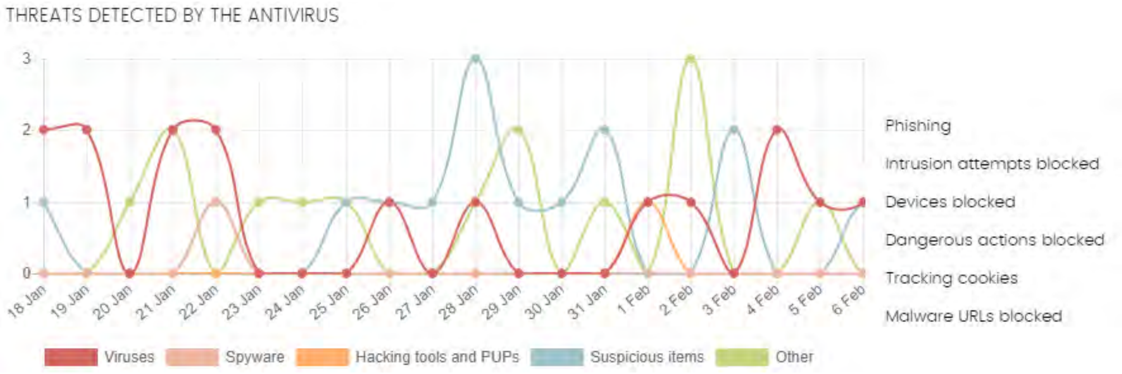


Figure 16.7: Threats detected by the antivirus' panel

The data covers all infection vectors and all supported platforms, so administrators are able to get specific data (volume, type, form of attack) related to the malware that reached the network during a selected period of time.

- **Meaning of the data displayed**

This panel comprises two sections: a line chart and a summarized list.

The line chart represents detections on the network over time, split into malware categories:

Data	Description
Viruses and spyware	Programs that can enter computers and IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.
Hacking tools and PUPs	Programs used by hackers to carry out actions that cause problems for the user of the affected computer (control the computer, steal confidential information, scan communication ports, etc.).
Hacking tools and PUPs	Programs used by hackers to carry out actions that cause problems for the user of the affected computer (control the computer, steal confidential information, scan communication ports, etc.).
Suspicious items	Files with a high probability of being malware after having been analyzed by our heuristic technologies. This type of technology is only used in the on-demand scans performed from scheduled tasks. In this type of scan, the investigated file is not executed. Therefore, the security software has far less information to evaluate the file's behavior, which reduces the classification accuracy. To compensate for the reduced accuracy of the static scan, the heuristic technologies are used.
Phishing	A technique for obtaining confidential information from users fraudulently. The targeted information includes passwords, credit card numbers and bank account details.
Other	Hoaxes, worms, Trojans and other types of viruses.

Table 16.7: Description of the data displayed in the 'Classification of all programs run and scanned' panel

The list to the right of the chart shows events that the administrator may want to monitor in order to look for symptoms of potentially dangerous situations.

Data	Description
Dangerous actions blocked	Detections made by analyzing local behavior.
Intrusion attempts blocked	Detections of malformed network traffic specially crafted to cause an execution error in one of the components on the targeted computer. This traffic can lead to unwanted system behavior.
Devices blocked	Detection of a user's attempt to use a restricted device according to the settings established by the network administrator in the Device Control module.
Tracking cookies	Detection of cookies used to track users' Web activity.
Malware URLs	Web addresses that point to pages containing malware.

Table 16.8: Description of the data displayed in the 'Threats detected by the antivirus' panel

- **Lists accessible from the panel**

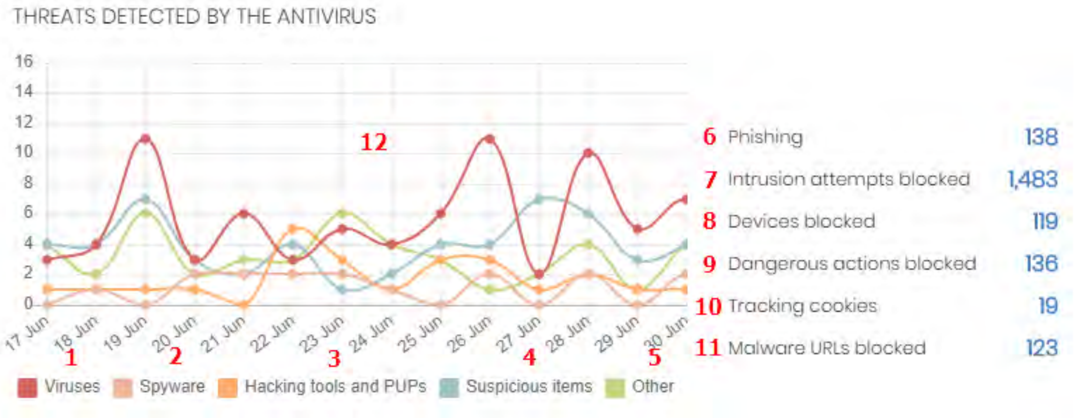


Figure 16.8: Hotspots in the 'Threats detected by the antivirus' panel

Click the hotspots shown in the figure 16.8 to access the **Threats detected by the antivirus** list with the following predefined filters.

Hotspot	List	Filter
(1)	Threats detected by the antivirus	Threat type = Virus
(2)	Threats detected by the antivirus	Threat type = Spyware
(3)	Threats detected by the antivirus	Threat type = Hacking tools and PUPs
(4)	Threats detected by the antivirus	Threat type = Suspicious items
(5)	Threats detected by the antivirus	Threat type = Other
(6)	Threats detected by the antivirus	Threat type = Phishing
(7)	Intrusion attempts blocked	No filter
(8)	Devices blocked	No filter
(9)	Threats detected by the antivirus	Threat type = Dangerous actions blocked
(10)	Threats detected by the antivirus	Threat type = Tracking cookies
(11)	Threats detected by the antivirus	Threat type = Malware URLs
(12)	Threats detected by the antivirus	No filter

Table 16.9: Filters available in the 'Threats detected by the antivirus' list

Security module lists

The security lists display the information collected by Panda Endpoint Protection in connection with computer protection activities. They provide highly detailed information as they contain the raw data used to generate the widgets.

There are two ways to access the security lists:

- Go to the **Status** menu at the top of the console and click **Security** from the side panel. Click any of the available widgets to access its associated list. Depending on the item you click on the widget, you'll access different lists with predefined filters.

Alternatively,

- Go to the **Status** menu at the top of the console and click **Add** from the **My lists** side panel. A window will be displayed showing all lists available in Panda Endpoint Protection.
- Click any of the lists in the Security section. The list will open with no filters applied.

Click any of the entries on the list to open a new window with more details about that particular item.

Computer protection status

This list shows all computers on the network, with filters to allow you to search for those computers and mobile devices that are unprotected for some specific reason.

To ensure correct operation of the protection, the computers on the network must communicate with the Panda Security cloud. See the list of URLs that must be accessible from computers in section "**Access to service URLs**" on page 381

Field	Description	Values
Computer	Computer name.	Character string
Computer status	Agent reinstallation: • Reinstalling the agent. • Agent reinstallation error. Protection reinstallation: • Reinstalling the protection. • Protection reinstallation error. • Pending restart.	Icon
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	• Character string • 'All' group • Native group • Active Directory group
Antivirus	Antivirus protection status	• Installing • Error. If it is a known error, the cause of the error will be displayed. If it is an unknown error, the error code will be displayed instead

Table 16.10: Fields in the 'Computer protection status' list

Field	Description	Values
		- ☒ Error - ✓ Enabled - ! Disabled - ∅ No license
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released. Hover the mouse pointer over the field to see the version of the installed protection.	- ✓ Updated. - ☒ Not updated (7 days without updating since last release). - ↻ Pending restart.
Knowledge	Indicates whether or not the signature file found on the computer is updated to the latest version. Hover the mouse pointer over the field to see the date that the file was last updated.	- ✓ Updated. - ☒ Not updated (3 days without updating since last release).
Connection to knowledge	Indicates whether the computer can communicate with the Panda Security cloud to send monitored events and download security intelligence.	- ✓ Connection OK - ☒ One or more services are not accessible - — Information not available
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Date

Table 16.10: Fields in the 'Computer protection status' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	- Workstation - Laptop - Server - Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string

Table 16.11: Fields in the 'Computer protection status' exported file

Field	Description	Values
Description	Description assigned to the computer.	Character string
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	Character string
Agent version	Internal version of the Panda agent module.	Character string
Installation date	Date when the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last update on	Date the agent was last updated.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version and patch status.	Character string
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released.	Binary value
Protection version	Internal version of the protection module.	Character string
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Last update on	Date when the signature file was last updated.	Date
File antivirus **Mail antivirus** **Web browsing antivirus** **Firewall** **Device control** **Anti-Theft**	Status of the associated protection.	• Not installed • Error: if it is a known error, the cause of the error will be displayed. If it is an unknown error, the error code will be displayed instead • Error • Enabled • Disabled • No license

Table 16.11: Fields in the 'Computer protection status' exported file

Field	Description	Values
Error date	If an error took place installing Panda Endpoint Protection, date and time of the error.	Date
Installation error	If an error took place installing Panda Endpoint Protection, error description.	Character string
Instalation error code	Displays codes that identify the installation error occurred.	Codes are separated by ";": • Error code • Extended error code • Extended error subcode
Connection for collective intelligence	Shows the status of the connection between the computer and the servers that store signature files and security intelligence.	• OK • With problems
Other security products	Name of any third-party antivirus product found on the computer at the time of installing Panda Endpoint Protection.	Character string

Table 16.11: Fields in the 'Computer protection status' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Find computer	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Character string
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago

Table 16.12: Filters available in the 'Computer protection status' list

Field	Description	Values
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	• All • More than 72 hours ago • More than 7 days ago • More than 30 days ago
Updated protection	Indicates whether or not the installed protection is updated to the latest version released.	• All • Yes • No • Pending restart
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS • Android
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Connection to knowledge servers	Indicates whether the computer can communicate with the Panda Security cloud to send monitored events and download security intelligence.	• All • OK • **With problems**: one or more services are not accessible
Protection status	Status of the protection module installed on the computer.	• Installing... • Properly protected • Protection with errors • Disabled protection • No license • Installation error

Table 16.12: Filters available in the 'Computer protection status' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "**Details section (3)**" on page 167 for more information.

Threats detected by the antivirus

This list provides complete and consolidated information about all the detections made on all supported platforms and for all the infection vectors used by hackers to infect computers on the network.

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
IP address	The computer's primary IP address.	Character string
Group	Group within the Panda Endpoint Protection group tree that the computer belongs to.	• Character string • 'All' group • Native group • Active Directory group
Threat type	Type of detected threat.	• Virus. • Spyware. • Hacking tools and PUPs. • Phishing. • Suspicious items. • Dangerous actions blocked. • Tracking cookies. • Malware URLs. • Other.
Path	Location of the threat on the file system.	Character string
Action	Action taken by Panda Endpoint Protection.	• Deleted • Disinfected • Quarantined • Blocked • Process ended
Date	Date when the item was detected.	Date

Table 16.13: Fields in the 'Threats detected by the antivirus' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string

Table 16.14: Fields in the 'Threats detected by the antivirus' exported file

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Name of the computer where the threat was detected.	Character string
Malware name	Name of the detected threat.	Character string
Threat type	Type of detected threat.	• Virus. • Spyware. • Hacking tools and PUPs. • Phishing. • Suspicious items. • Dangerous actions blocked. • Tracking cookies. • Malware URLs. • Other.
Malware type	Threat subclass.	Character string
Number of detections	Number of times that Panda Endpoint Protection detected the threat on the computer on the specified date.	Numeric value
Action	Action taken by Panda Endpoint Protection.	• Quarantined • Deleted • Blocked • Process ended
Detected	Engine that detected the threat.	• Device control. • File protection. • Firewall. • Mail protection. • On-demand scan. • Web protection.
Detection path	Location of the threat on the file system.	Character string
Excluded	The threat was excluded from the scans by the administrator so it can be run.	Binary value
Date	Date when the item was detected.	Date
Group	Group within the Panda Endpoint Protection group tree that the computer belongs to.	Character string

Table 16.14: Fields in the 'Threats detected by the antivirus' exported file

Field	Description	Values
IP address	Primary IP address of the computer where the detection was made.	Character string
Domain	Windows domain that the computer belongs to.	Character string
Description	Description assigned to the computer by the network administrator.	Character string

Table 16.14: Fields in the 'Threats detected by the antivirus' exported file

- **Filter tool**

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
Dates	• **Range**: lets you set the time period, from the current moment back. • **Custom range**: lets you choose a specific date from a calendar.	• Last 24 hours • Last 7 days • Last month • Last year
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Threat type	Type of threat.	• Virus. • Spyware. • Hacking tools and PUPs. • Phishing.
		• Suspicious items. • Dangerous actions blocked. • Tracking cookies. • Malware URLs. • Other.

Table 16.15: Filters available in the 'Threats detected by the antivirus' list

- **Details window**

Shows detailed information about the detected virus.

Field	Description	Values
Threat	Threat name.	Character string

Table 16.16: Details accessible from the 'Threats detected by the antivirus' list

Field	Description	Values
Action	Action taken by Panda Endpoint Protection.	• Quarantined • Deleted • Blocked • Process ended
Computer	Name of the computer where the threat was detected. It includes a link to the Computer details window.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
IP address	The computer's primary IP address.	Character string
Logged-in user	Operating system user under which the threat was loaded and run.	Character string
Detection path	File system path of the threat.	Character string
Name	Threat name.	Character string
Threat type	Type of threat.	Character string
Malware type	Type of malware.	• Virus. • Spyware. • Hacking tools and PUPs. • Phishing. • Suspicious items. • Dangerous actions blocked. • Tracking cookies. • Malware URLs. • Other.
Detected by	Module that detected the item	Character string
Date	Date when the item was detected	Date

Table 16.16: Details accessible from the 'Threats detected by the antivirus' list

Blocked devices

This list provides details of the network computers that have restricted access to peripherals.

Field	Description	Values
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string

Table 16.17: Fields in the 'Blocked devices' list

Field	Description	Values
Group	Folder within the Panda Endpoint Protection folder tree that the computer belongs to.	• Character string • 'All' group • Native group • Active Directory group
Name	Name assigned to the device by the administrator.	Character string
Type	Type of blocked device.	• Removable storage drives. • Imaging devices. • CD/DVD drives. • Bluetooth devices. • Modems. • Mobile devices.
Action	Action taken on the device.	• Block • Allow read access • Allow read & write access
Date	Date and time when the action was taken.	Date

Table 16.17: Fields in the 'Blocked devices' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by the administrator.	Character string

Table 16.18: Fields in the 'Blocked devices' exported file

Field	Description	Values
Type	Type of device.	• Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices • Modems • Mobile devices
Instance ID	ID of the affected device.	Character string
Number of detections	Number of times the disallowed action was detected on the device.	Numeric value
Action	Action taken on the device.	• Block • Allow read access • Allow read & write access
Detected by	Module that detected the disallowed operation.	Device control
Date	Date when the disallowed operation was detected.	Date
Group	Folder within the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain that the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 16.18: Fields in the 'Blocked devices' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Find computer	Computer name.	Character string
Dates	• **Range**: lets you set the time period, from the current moment back. • **Custom range**: lets you choose a specific date from a calendar.	• Last 24 hours • Last 7 days • Last month

Table 16.19: Filters available in the 'Blocked devices' list

Field	Description	Values
Device type	Type of device affected by the security settings.	• Removable storage drives. • Imaging devices • CD/DVD drives. • Bluetooth devices. • Modems. • Mobile devices.
Name	Device name	Character string

Table 16.19: Filters available in the 'Blocked devices' list

- **Details window**

Shows detailed information about the blocked device.

Field	Description	Values
Device	Name of the blocked device.	Character string
Action	Action taken by Panda Endpoint Protection.	• Quarantined • Deleted • Blocked • Process ended
Computer	Name of the computer where the device was blocked.	Character string
Computer type	Type of computer.	• Workstation • Laptop • Mobile device • Server
IP address	The computer's primary IP address	Character string
Name	Name of the blocked device	Character string
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by the administrator. It can be edited by clicking the ✎ icon.	Character string
Device type	Type of device	• Removable storage drives. • Imaging devices. • CD/DVD drives. • Bluetooth devices. • Modems. • Mobile devices.

Table 16.20: Details accessible from the 'Blocked devices' list

Field	Description	Values
Instance ID	ID of the affected device	Character string
Blocked	Module that detected the item	Character string
Number of detections	Number of detected blocks.	Numeric value
Date	Date when the item was detected.	Date

Table 16.20: Details accessible from the 'Blocked devices' list

Intrusion attempts blocked

This list shows the network attacks received by the computers on the network and blocked by the firewall.

Field	Description	Values
Computer	Name of the computer that received the network attack.	Character string
IP address	IP address of the primary network interface of the computer that received the network attack.	Character string
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs.	Character string
Intrusion type	Indicates the type of intrusion detected. Refer to "**Block intrusions**" for more information on each type of network attack.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Date	Date and time Panda Endpoint Protection logged the attack on the computer.	Date

Table 16.21: Fields in the 'Intrusion attempts blocked' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Name of the computer that received the network attack.	Character string
Intrusion type	Indicates the type of intrusion detected. Refer to "Block intrusions" on page 218 for more information on each type of network attack.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Local IP address	IP address of the computer that received the network attack.	Character string
Remote IP address	IP address of the computer that started the network attack.	Character string
Remote MAC address	Physical address of the computer that started the network attack, provided it is on the same subnet as the computer that received the attack.	Character string
Local port	In TCP and UDP attacks, this column indicates the port where the intrusion attempt was received.	Numeric value
Remote port	In TCP and UDP attacks, this column indicates the port from which the intrusion attempt was launched.	Numeric value
Number of detections	Number of intrusion attempts of the same type received.	Numeric value

Table 16.22: Fields in the 'Intrusion attempts blocked' exported file

Field	Description	Values
Action	Action taken by the firewall according to its settings. Refer to "Firewall (Windows computers)" on page 212 for more information.	Block
Detected by	Detection engine that detected the network attack.	Firewall
Date	Date the network attack was logged.	Date
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 16.22: Fields in the 'Intrusion attempts blocked' exported file

- **Filter tool**

Field	Description	Values
Dates	• **Range**: lets you set the time period, from the current moment back. • **Custom range**: lets you choose a specific date from a calendar.	• Last 24 hours • Last 7 days • Last month
Intrusion type	Indicates the type of intrusion detected. Refer to "Block intrusions" on page 218 for more information on each type of network attack.	• All intrusion attempts • ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan

Table 16.23: Filters available in the 'Intrusion attempts blocked' list

Field	Description	Values
Computer type	Type of device.	• All computer types • Workstation • Laptop • Mobile device • Server

Table 16.23: Filters available in the 'Intrusion attempts blocked' list

- **Details window**

Shows detailed information about the network attack detected.

Field	Description	Values
Intrusion type	Indicates the type of intrusion detected. Refer to "**Block intrusions**" on page 218 for more information about each type of network attack.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Action	Action taken by Panda Endpoint Protection	Blocked
Computer	Name of the computer where the threat was detected.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
IP address	The computer's primary IP address.	Character string
Local IP address	IP address of the computer that received the network attack.	Character string
Remote IP address	IP address of the computer that started the network attack.	Character string

Table 16.24: Details accessible from the 'Intrusion attempts blocked' list

Field	Description	Values
Remote MAC address	Physical address of the computer that started the network attack, provided it is on the same subnet as the computer that received the attack.	Character string
Local port	In TCP and UDP attacks, this section indicates the port where the intrusion attempt was received.	Numeric value
Remote port	In TCP and UDP attacks, this section indicates the port from which the intrusion attempt was launched.	Numeric value
Detected by	Module that detected the attack.	Firewall
Number of detections	Number of successive times the same type of attack occurred between the same source and target computers.	Numeric value
Date	Date when the attack was detected.	Date

Table 16.24: Details accessible from the 'Intrusion attempts blocked' list

Chapter 17

Managing threats, items in the process of classification, and quarantine

Panda Endpoint Protection provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This balance is achieved through tools that enable you to manage the detection of found threats.

CHAPTER CONTENTS

Introduction to threat management tools

Network administrators can change the behavior of Panda Endpoint Protection with regard to found threats using the following tools:

- Allow/stop allowing the execution of programs classified as viruses.
- Detect/stop detecting programs classified as viruses.
- Manage the backup/quarantine area.

Detect/stop detecting programs classified as viruses

Administrators can allow the execution of software that implements features valued by users but which has been classified as a threat. That is the case of PUPs, for example. These are often toolbars which provide search capabilities but also collect users' private data and confidential corporate information for advertising purposes. Refer to "Allowing and preventing items to run".

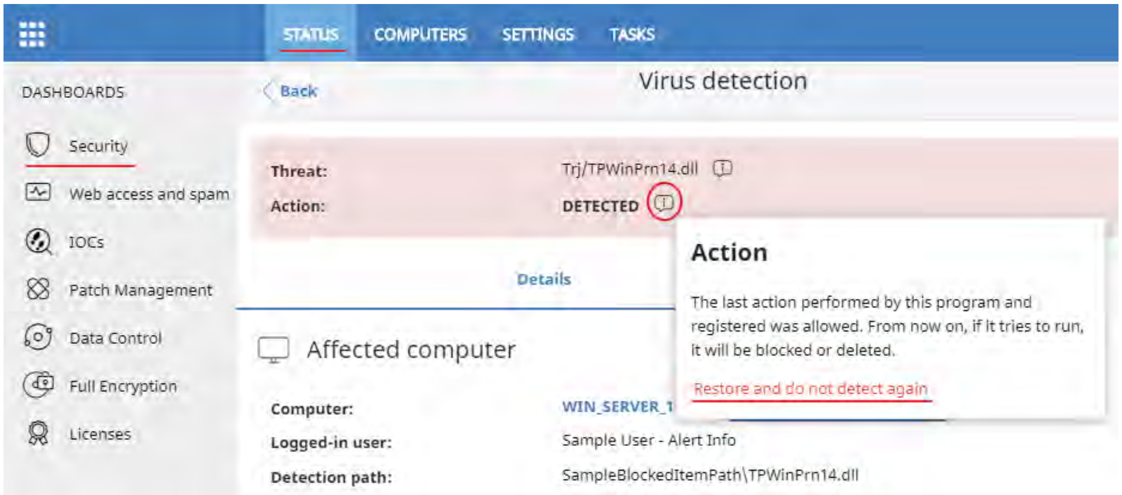
Manage the backup/quarantine area

Administrators can retrieve items considered threats and therefore deleted from users' computers.

Allowing and preventing items to run

Restoring/Stopping detecting programs classified as viruses

If users need to use certain features provided by a program classified as a threat by the signature file, and the administrator considers that the danger posed to the integrity of the managed IT network is low, the administrator can allow the program to run.



Virus detection

Threat: Trj/TPWinPrn14.dll

Action: DETECTED

Action

The last action performed by this program and registered was allowed. From now on, if it tries to run, it will be blocked or deleted.

Restore and do not detect again

Affected computer

Computer: WIN_SERVER_1

Logged-in user: Sample User - Alert Info

Detection path: SampleBlockedItemPath\TPWinPrn14.dll

Figure 17.1: Restore and do not detect a threat again

To restore deleted programs from the quarantine/backup area and not detect them again:

- Click the **Status** menu at the top of the console. Then, click **Security** from the side panel.
- Click on the **Threats detected by the antivirus** panel and select the item that you want to allow to run.
- Click the ⓘ icon in the **Action** field. A window opens explaining the action taken by Panda Endpoint Protection.
- Click the **Restore and do not detect again** link. Panda Endpoint Protection will perform the following actions:
  - The item will be copied from the quarantine/backup area to its original location on the computers

on the IT network.

- The item will be allowed to run and won’t generate any detections.
- The program will be added to the **Programs allowed by the administrator** list.

Stopping allowing the execution of previously allowed items

To block again an item previously allowed by the administrator:

- Click the **Status** menu at the top of the console. Then, click **Security** from the side panel.
- In the **Programs allowed by the administrator** panel, click the type of item that you want to stop allowing to run: **Malware** or **PUP**.
- In the **Programs allowed by the administrator** list, click the 🗑 icon to the right of the item that you want to stop allowing to run:

After you click the 🗑 icon, Panda Endpoint Protection will perform the following actions:

- The item will be removed from the **Programs allowed by the administrator** list.
- An entry will be added to the **History of programs allowed by the administrator** list, with the **Action** column showing the value **Exclusion removed by the user**.
- If the item is classified as a virus, it will reappear in the **Threats detected by the antivirus** list
- If the item is classified as a virus, it will generate incidents again.

Information about detected threats

Network administrators can get information about the programs classified as threats by the signature file in the **Threats detected by the antivirus** panel and the **Threats detected by the antivirus** list. Refer to “Threats detected by the antivirus” on page 304.

List of allowed threats

Network administrators have multiple panels and lists available to get information about programs that were initially blocked by Panda Endpoint Protection and then allowed to run:

- The **Programs allowed by the administrator** panel.
- The **Programs allowed by the administrator** list
- The **History of programs allowed by the administrator** list.

Programs allowed by the administrator

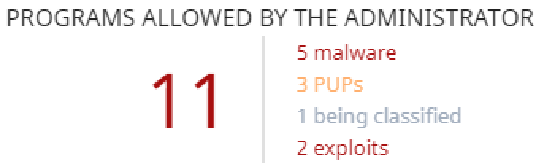


Figure 17.2: 'Programs allowed by the administrator' panel

Shows programs allowed by the administrator which initially were prevented from running by Panda Endpoint Protection because they were classified as a threat.

- **Meaning of the data displayed**

The panel shows the total number of items excluded from blocking by the administrator, broken down by type:

- Malware
- PUP

- **Lists accessible from the panel**

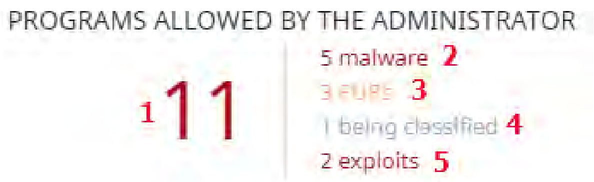


Figure 17.3: Hotspots in the 'Programs allowed by the administrator' panel

Click the hotspots shown in figure 17.3 to access the **Programs allowed by the administrator** list with the following predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Classification = Malware.
(3)	Classification = PUP.

Table 17.1: Filters available in the 'Programs allowed by the administrator' list

'History of programs allowed by the administrator' list

This list shows a history of all events that have occurred over time regarding threats and unknown files in the process of classification which the administrator allowed to run. This list shows all the classifications that a file has gone through, from the time it entered the **Programs allowed by the administrator** list until it left it, as well as all other classifications caused by Panda Endpoint Protection or the administrator.

This list doesn't have a corresponding panel. To access the list, click the **History** link in the top right corner of the **Software allowed by the administrator** list.

Field	Description	Values
Program	Name of the file with malicious code and that is allowed to run.	Character string
Classification	Type of threat that was allowed to run.	• Malware • PUP • Goodware
Threat	Name of the malware or PUP that is allowed to run. If it has not been identified, the column will display the file's name instead. If it is an exploit, the exploit technique used will be indicated.	Character string
Hash	String identifying the file. This is empty if it is an exploit.	Character string
Action	Action taken on the allowed item. • **Exclusion removed by the user**: The administrator allowed the item to be quarantined again**.** • **Exclusion added by the user**: The administrator allowed the item to be removed from quarantine.	Enumeration
User	User account under which the file was allowed.	Character string
Date	Date the event took place.	Date

Table 17.2: Fields in the 'History of programs allowed by the administrator' list

- **Fields displayed in the exported file**

Field	Description	Values
Program	Name and path of the file with malicious code that was allowed to run.	Character string
Current type	Last classification of the threat allowed to run.	• Malware • PUP
Original type	Original classification of the file when it was allowed to run.	• Malware • PUP
Threat	Name of the malware or PUP that is allowed to run. If it has not been identified, the column will display the file's name instead. If it is an exploit, the exploit technique used will be indicated.	Character string
Hash	String identifying the file. This is empty if it is an exploit.	Character string

Table 17.3: Fields in the 'History of programs allowed by the administrator' exported file

Field	Description	Values
Action	Action taken on the allowed item. • **Exclusion removed by the user**: The administrator allowed the item to be quarantined again. • **Exclusion added by the user**: The administrator allowed the item to be removed from quarantine.	Enumeration
User	User account which triggered the change to the allowed file.	Character string
Date	Date the event took place.	Date

Table 17.3: Fields in the 'History of programs allowed by the administrator' exported file

- **Filter tool**

Field	Description	Values
Search	• **User**: User account which triggered the change to the allowed file. • **Program**: Name of the file containing the threat. • **Hash**: String identifying the file.	Enumeration
Classification	Type of file the last time it was classified.	• All • Malware • PUP • Goodware • Item being classified (suspicious items)
Original classification	Original classification of the file when it was allowed to run.	• All • Malware • PUP • Being classified (Suspicious item)
Action	Action taken on the allowed item. • **Exclusion removed by the user**: The administrator allowed the item to be quarantined again. • **Exclusion added by the user**: The administrator allowed the item to be removed from quarantine.	Enumeration

Table 17.4: Filters available in the 'History of programs allowed by the administrator' list

Managing the backup/quarantine area

Panda Endpoint Protection's quarantine is a backup area that stores items that have been deleted after being classified as a threat.

Quarantined items are stored on each user's computer, in the `Quarantine` folder located in the software installation directory. This folder is encrypted and cannot be accessed by any other process. It is therefore not possible to directly access or run the programs there, unless it is through the Web console.

The quarantine feature supports Windows, macOS, and Linux platforms.

The Panda Labs department at Panda Security determines the action to take in accordance with the classification and type of item detected. As such, the following situations can occur:

- **Malicious items for which disinfection is possible**: These are disinfected and restored to their original location.
- **Malicious items for which disinfection is not possible**: These are moved to quarantine and remain there for seven days.
- **Non-malicious items**: If goodware is incorrectly classified (false positive), it is automatically restored from quarantine to its original location.
- **Suspicious items**: These are stored in quarantine for 30 days. If it finally turns out to be goodware, it will be automatically restored to its original location.

Panda Endpoint Protection doesn't delete files from users' computers. All deleted files are sent to the backup area.

Viewing quarantined items

To get a list of the items sent to quarantine:

- Click **Status** in the menu at the top of the console then **Security** in the side panel.
- Click in the **Threats detected by the antivirus** panel.
- Select the **Moved to quarantine** checkbox and **Deleted** in the **Action** field. Then click **Filter**.

Restoring items from quarantine

- Click **Status** in the menu at the top of the console then **Security** in the side panel.
- Click in the **Threats detected by the antivirus** panel.
- Select the threat from the list where the **Action** field is **Moved to quarantine** or **Disinfected**.

- Click the ⓘ icon in the **Action** field. A window opens explaining the reason the item was moved to quarantine.
- Click the **Restore and do not detect again** link. The item will be moved to its original location. The permissions, owner, and registry entries regarding the file will also be restored.

Chapter 18

Alerts

The alert system is a resource provided by Panda Endpoint Protection to quickly notify administrators of situations that might affect the correct operation of the security service.

Namely, an alert is sent to the administrator every time one of the following events occur:

- A malware specimen is detected.
- A network attack is detected.
- There is an attempt to use an unauthorized external device.
- An unknown item (malware or PUP) is reclassified.
- There is a license status change.
- There are installation errors or a computer is unprotected.

CHAPTER CONTENT

Email alerts

Email alerts are messages generated and sent by Panda Endpoint Protection to the configured recipients (typically the network administrator) when certain events occur.

Accessing the alert settings

Click the **Settings** menu at the top of the console. Then, click **My alerts** from the side menu. You'll access the **Email alerts** window, where you can configure the email alert settings.

Alert settings

The alert settings window is divided into three sections:

- **Send alerts in the following cases**: select which events will trigger an alert. Refer to 18.1 for more information.
- **Send the alerts to the following address**: enter the email addresses of the alert recipients.
- **Send the alerts in the following language**: choose the alert message language from those supported in the console:
  - German
  - Spanish
  - French
  - English
  - Italian
  - Japanese
  - Hungarian
  - Portuguese
  - Russian
  - Swedish

Access permissions and alerts

Alerts are defined independently for each user of the Web console. The contents displayed in an alert will vary depending on the managed computers that are visible to the recipient's role.

Alert types

Type	Frequency	Condition	Information displayed
Malware detections	Every 15 minutes	• Malware is detected in real time by an on-demand or scheduled scan.	• Number of threats detected within the time range. • Number of affected computers.
Hacking tool & PUP detections	Every 15 minutes	• A PUP or hacking tool is detected in real time by an on-demand or scheduled scan.	• Number of threats detected within the time range. • Number of affected computers.
Malware URL blocked	Every 15 minutes	• A URL pointing to malware is detected.	• Number of malware URLs detected within the time range. • Number of affected computers.

Table 18.1: Alert table

Type	Frequency	Condition	Information displayed
Phishing detections	Every 15 minutes	• A phishing attack is detected.	• Number of phishing attacks detected within the time range. • Number of affected computers.
Intrusion attempt blocked	Every 15 minutes	• An intrusion attempt is blocked by the IDS module. • Compatible with Windows computers.	• Number of intrusion attempts blocked within the time range. • Number of affected computers.
Device blocked	Every 15 minutes	• A user tries to access a device or peripheral blocked by the administrator. • Compatible with Windows, Linux, macOS and Android devices.	• Number of device access attempts blocked. • Number of affected computers.
Protection errors	Every time the relevant event is detected.	• An unprotected computer is found on the network. • A computer with a protection or installation error is found.	• Computer name. • Group. • Description. • Operating system. • IP address. • Active Directory path. • Domain. • Date and time (UTC). • Failure reason: Protection with errors or Installation error.
Computer without a license	Every time the relevant event is detected.	The solution fails to assign a license to a computer due to lack of sufficient free licenses.	• Computer name. • Description. • Operating system. • IP address. • Group. • Active Directory path. • Domain. • Date and time (UTC). • Failure reason: Computer without a license.

Table 18.1: Alert table

Type	Frequency	Condition	Information displayed
Installation error	Every time the relevant event is detected.	• An event occurs that causes a computer's status to change **(1)** from protected to unprotected. • If several circumstances are detected at the same time that may cause a computer's status to change from protected to unprotected, only one alert will be generated with a summary of all those circumstances.	• Computer name. • Protection status. • Reason for the status change.
Unmanaged computer detected	Every time the relevant event is detected.	• A discovery computer finishes a discovery task. • A discovery task finds a never-seen-before computer on the network.	• Name of the discovery computer. • Number of discovered computers. • Link to the list of unmanaged computers discovered.

Table 18.1: Alert table

Status changes (1)

The following computer statuses will trigger an alert:

- **Protection with errors**: if the status of the antivirus protection installed on a computer shows an error, an alert is generated.
- **Installation error**: if an installation error occurs that requires user intervention (e.g. insufficient disk space), an alert is generated. Transient errors that can be resolved autonomously after a number of retries won't generate an alert.
- **No license**: if a computer doesn't receive a license after registration because there aren't any free licenses, an alert is generated.

Finally, the following computer statuses will not trigger an alert:

- **No license**: no alert is generated if the administrator manually removes a computer's license or if Panda Endpoint Protection automatically removes a computer's license because the number of purchased licenses has been reduced.
- **Installing**: it doesn't make sense to generate an alert every time the protection is installed on a computer on the network.
- **Disabled protection**: this status is the consequence of a voluntary change of settings, so no alert is

generated.

- **Outdated protection**: this status doesn't necessarily mean the computer is unprotected, despite its protection is out of date.
- **Pending restart:** this status doesn't necessarily mean the computer is unprotected.
- **Outdated knowledge:** this status doesn't necessarily mean the computer is unprotected.

Opting out of email alerts

In cases where the email alert recipient wants to opt out of the notifications but cannot access the Panda Endpoint Protection console or doesn't have enough permissions to modify the settings, the steps below must be taken:

- Click the link at the bottom of the message: "If you don't want to receive any more messages of this kind, click here.". A window appears prompting for the email address at which the notifications are being received. The link is valid for 15 days.
- If an email address is entered that is included in any of the Panda Endpoint Protection settings, an email will be sent to that address for the user to confirm that they want to opt of the notifications sent for that account.
- Click the link in the email received to delete the email account from all settings in which it appears. The link is valid for 24 hours.

Chapter 19

Scheduled sending of reports and lists

The reports module sends via email up-to-date information about the security status of a company's IT infrastructure. This method of delivering reports enables you to:

- Share information across departments in a company.
- Keep a history of all the events on the platform, even beyond the capacity limits of the web console.
- Closely monitor the security status of the network without having to access the web console, thereby saving management time.

Automate email reports, enabling stakeholders to stay up-to-speed on all security events, thanks to a tamper-proof system that enables them to accurately assess the network security status.

CHAPTER CONTENTS

Types of reports available

Report features

Report period

- **Consolidated reports**: These include, in a single document, all the information generated over a given period of time.
- **Instant reports**: These reflect the security status of the network at a specific moment in time.

Method of sending

Panda Endpoint Protection enables you to generate and send reports automatically based on the settings established in the task scheduler or manually on demand.

Format

Depending on the type, reports can be sent in PDF and/or CSV format.

Content

Depending on the type of report, its content may be configurable, including any number of modules or restricting results to computers that meet certain criteria.

Report types

Panda Endpoint Protection enables you to generate three types of reports, each with its own features:

- List views
- Executive reports
- Lists of devices

Next is a summary of the features of each type of report:

Type	Period	Sent	Contents	Format
List views	Instant	Automatically	Configurable using searches	CSV
Executive reports	Consolidated	Automatically and on demand	Configurable by categories and groups	PDF, CSV, Excel, Word
Lists of devices	Instant	Automatically	Configurable using filters	CSV

Table 19.1: Summary of report types and their features

Tasks required to generate reports

Users with the read-only role can preview executive reports but cannot schedule the sending of new reports.

Next is a description of the tasks administrators have to perform to use the feature for sending scheduled reports.

List views

Administrators can use a default view or create a new one and set up the search tools so the list shows the required information. After this is done, it is possible to create a scheduled report. Refer to "**Creating a custom list**" on page **47** for more information on how to create list views with the corresponding searches.

Executive reports

The content is determined when configuring the scheduled report.

List of filtered devices

Administrators have to create a filter or use one of the previously created filters. Refer to "**Filter tree**" on page **134** for more information on how to configure the filters.

Accessing the sending of reports and lists

From the Scheduled reports section

Click **Status** in the menu at the top of the console. Click **Scheduled reports** in the side panel. A page opens with the tools required for searching for previously created send tasks, editing them, deleting them, or creating new ones.

From a list view

Select the **Status** menu. The left-side panel contains the default views and those created by the administrator.

To schedule the sending of a view:

- **From the context menu**: Click the context menu of the list view and then the option **Schedule report** ✉. A window opens with the information required, which is explained in section "**Configuring reports and lists**".
- **From the list view**: Click the ✉ icon in the upper-right corner of the window. A window opens with the information required, which is explained in section "**Configuring reports and lists**".

After the scheduled report has been created, a pop-up message appears in the upper-right corner of the page confirming the creation of the task.

From a filter

- Click the **Computers** menu at the top of the console. Click the ▽ tab to display the filter tree.
- On clicking a filter, the list of devices is refreshed to show the devices whose characteristics meet the conditions of the selected filter.
- Click the context menu icon ⋮ corresponding to the filter and click **Schedule report**. A window opens with the information required, which is explained in section "**Configuring reports and lists**".

After the scheduled report has been created, a pop-up message appears in the upper-right or bottom-right corner of the page confirming the creation of the task. This message also includes a link to the list of scheduled reports. Refer to "**List of scheduled reports**".

Managing reports

To create, delete, edit, and list scheduled reports, click the **Status** menu at the top of the console. Click **Scheduled reports** from the side menu.

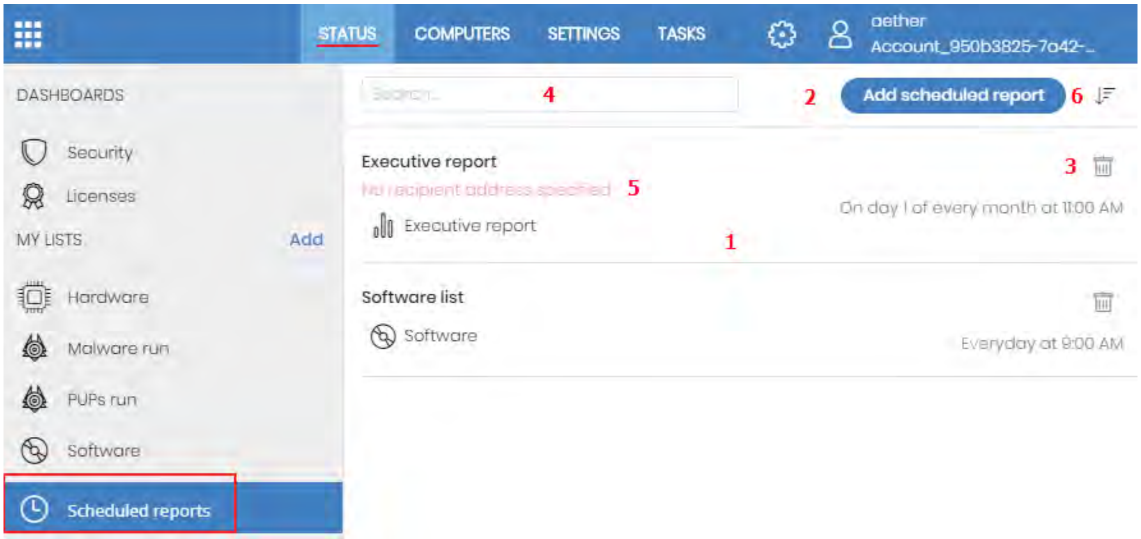


Figure 19.1: Page for managing scheduled sending of lists and reports

List of scheduled reports

In the right-side panel, you can see the list of previously created scheduled reports (Figure 19.1 **1)**.

All the tasks include a name and status. (Figure 19.1 **5**).

Creating scheduled reports

Click the button **Add scheduled report** to display the settings window (Figure 19.1 **2**).

Refer to "**Configuring reports and lists**" for more information about the data administrators need to provide to create a scheduled report.

Sorting scheduled reports

Click the ⇣ icon **(6)** to expand a context menu with the options for ordering the list.

Deleting and editing scheduled reports

- To delete a scheduled report, use the 🗑 icon to the right. (Figure 19.1 **3**).

- To edit a scheduled report, click its name.

> ⚠ *A list view or filtered list with a scheduled report configured cannot be deleted until the corresponding report has been deleted.*
>
> *The lists sent by a scheduled report correspond to a specific list view or filtered list. If these are edited, the scheduled report will be updated accordingly.*

Automatic disabling of scheduled reports

A scheduled report ceases to be sent automatically when any of the following conditions are met:

- If all of the customer's licenses expire.
- If the licenses have expired for the module to which the report corresponds.
- If the administrator account that last modified the scheduled report no longer exists in the console.

Configuring reports and lists

Field	Description
Name	Name of the entry shown in the list of scheduled reports.
Send automatically	Frequency with which the report or list will be sent: • **Every day**: It will be sent every day at the scheduled time. • **Every week**: It will be sent every week on the scheduled day and at the scheduled time • **Every month**: It will be sent every month at the scheduled time on the scheduled date.
Report type	Type of report to send: • Executive report • List • Filter Refer to "**Contents of the reports and lists**".
Preview report	This link is only displayed when the report type chosen is Executive Report. Click here to open a new tab in the browser containing the contents of the report so it can be reviewed before scheduling the report, downloading it, or printing it from the top bar. For lists, the format is CSV and the preview option is therefore not available.

Table 19.2: Information for generating on-demand reports

Field	Description
Dates	Time period covered by the report. • Last month • Last 7 hours • Last 24 hours This field is only displayed for executive reports. The lists contain data relevant to the moment they are created.
Computers	The computers from which data will be extracted to generate the executive report: • **All computers.** • **Selected groups**: Shows the group tree from which individual groups can be selected using the checkboxes. This field is only displayed for executive reports.
To	Target email addresses separated with commas.
CC	Target email addresses (carbon copy recipients) separated with commas.
CCO	Target email addresses (blind copy recipients) separated with commas.
Subject	Summary description of the email.
Format	• **For list views**: A .CSV file is attached to the email. • **For executive reports**: A PDF, Excel, or Word file containing the report is attached to the email.
Language	Language of the report.
Contents	Type of information included in the report: • **Table of contents:** List of the sections in the report. • **License status**: This shows information about the licenses contracted and used as well as their expiration dates. Refer to "Licenses" on page 111. • **Security status**: The status of the Panda Endpoint Protection software on the network computers on which it is installed. • **Detections**: This shows the threats detected on the network. • **Patch management**: This shows the status of computers regarding patches. Refer to "Panda Patch Management widgets and panels" on page 241. • **Encryption**: This shows the encryption status of the computers on the network. Refer to "Panda Full Encryption panels and widgets" on page 283. Refer to "Contents of the reports and lists".

Table 19.2: Information for generating on-demand reports

Contents of the reports and lists

Lists

The content of the lists sent is similar to that generated by the **Export** or **Detailed export** button of a list view. If the list view supports detailed exports, when configuring the send task there are two options:

- **Summary report**: This corresponds to the **Export** option in the list.
- **Full report**: This corresponds to the **Detailed export** option in the list.

The lists that support detailed exports are:

- Software

Refer to “Managing lists” on page 43 for more information about the types of lists available in Panda Endpoint Protection and their content.

The list includes the computers visible to the user account that last edited the scheduled report. For this reason, a list edited by an account with less visibility than the account that initially created it contains information for a smaller number of computers than those displayed when it was first created.

Lists of devices

The content of the report sent corresponds to the basic exported list of devices filtered by certain criteria. Refer to “The Computers area” on page 133 for more information about the contents of the .CSV file sent, and “Filter tree” on page 134 for information on how to manage and configure filters.

Executive report

Depending on the settings defined in the **Contents** field, the executive report can have the following data:

Overview

- **Created on**: Date the report was created.
- **Period**: Time period covered by the report.
- **Included information:** Computers included in the report.

Table of contents

Shows a list with links to different sections included in the executive report.

License status

- **Contracted licenses**: Number of licenses contracted.
- **Used licenses**: Number of licenses assigned to the network computers.
- **Expiration date**: Date the license contract expires.

Refer to “Licenses” on page 111.

Network security status

Operation of the protection module on the network computers on which it is installed.

- **Protection status**: Refer to "Protection status" on page 300
- **Online computers**: Refer to "Offline computers" on page 302
- **Up-to-date protection**: Refer to "Outdated protection" on page 303
- **Up-to-date knowledge**: Refer to "Outdated protection" on page 303

Detections

The threats detected on the network

- **Top 10 computers with most detections**: The top 10 computers with most detections by the antivirus module during the specified period:
  - **Computer**: Name of the computer.
  - **Group**: Group to which the computer belongs.
  - **Detections**: Number of detections during the specified period.
  - **First detection**: Date of first detection.
  - **Last detection**: Date of last detection.
- **Threats detected by the antivirus**: Refer to "Threats detected by the antivirus" on page 304.

Patch management

Status of computers regarding patches.

- **Patch management status**: Refer to "Patch management status" on page 241.
- **Top 10 computers with most available patches**: List of the ten computers with most patches available but not installed, grouped by type: security patches, non-security patches, and Service Packs. Refer to "Available patches" on page 246.
- **Top 10 most critical patches**: List of the ten most critical patches ordered by the number of computers affected. Refer to "Available patches" on page 246.

Encryption

Encryption status of computers. It includes information collected from the following widgets and lists:

- **Encryption status**: Refer to "Encryption Status" on page 283.
- **Computers supporting encryption**: Refer to "Computers Supporting Encryption" on page 285
- **Encrypted computers**: Refer to "Encrypted Computers" on page 286.
- **Authentication method applied:** Refer to "Authentication Method Applied" on page 287.
- **Last encrypted computers**: Lists the ten computers that have been encrypted most recently by Panda Full Encryption, sorted by encryption date. Each line in the list contains the computer name, group, operating system, authentication method, and encryption date.

Part 7

Security incident remediation

Chapter 20: Remediation tools

Chapter 21: Tasks

Chapter 20

Remediation tools

Panda Endpoint Protection provides several remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle. Some of these tools are automatic and don't require administrator intervention, whereas other tools require the execution of certain actions through the Web console.

Table 20.1 shows the tools available for each platform and their type (manual or automatic):

Remediation tool	Platform	Type	Purpose
Automatic computer scanning and disinfection	Windows, macOS, Linux, Android	Automatic	Detects and disinfects malware upon detecting movement in the file system (copy, move, run) or in a supported infection vector.
On-demand computer scanning and disinfection	Windows, macOS, Linux, Android	Automatic (scheduled)/ Manual	Detects and disinfects malware in the file system when required by the administrator: at specific time intervals or after creating a remediation task.
On-demand restart	Windows	Manual	Forces a computer restart to apply updates, finish manual disinfection tasks and fix protection errors.

Table 20.1: Panda Endpoint Protection remediation tools

CHAPTER CONTENT

Automatic computer scanning and disinfection

Panda Endpoint Protection's protection modules automatically detect and disinfect the threats found on protected computers and in the following infection vectors:

> *Automatic disinfection does not require administrator intervention. However, the **File protection** checkbox must be selected in the security settings assigned to the computers to protect. Refer to "Security settings for workstations and servers" on page 207 for more information about the blocking modes and configuration options available in the antivirus module included in Panda Endpoint Protection.*

- **Web**: malware downloaded onto targeted computers via the Web browser.
- **Email**: malware that reaches email clients as a message attachment.
- **File system**: malware detected when a file containing a known or unknown threat and located in the computer's storage system is run, moved or copied.
- **Network**: intrusion attempts from a host on the network/Internet and blocked by the firewall.

Upon detecting a known threat, Panda Endpoint Protection automatically cleans the affected items provided there is a disinfection method available. Otherwise, the items are quarantined.

On-demand computer scanning and disinfection

Permissions required to manage Scheduled scan tasks

To manage **Scheduled scan** tasks, the user account used to access the web console must have the **Launch scans and disinfect** permission assigned to its role.

> *For more information about the permission system implemented in Panda Endpoint Protection, refer to "Understanding permissions" on page 57.For more information about how to manage the tasks run on workstations and servers, view their results, and edit their settings, refer to "Tasks" on page 361*

There are two ways to scan and disinfect computers on demand:

- Creating a scheduled scan task.
- Running an immediate scan.

Creating a task from the computer tree

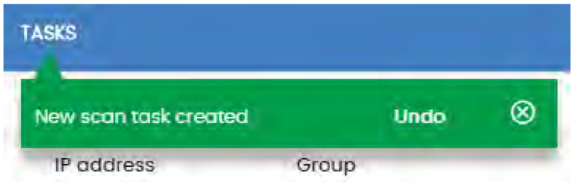
The computer tree lets you define scan tasks for all computers in a computer group very quickly.

- Go to the **Computers** menu at the top of the console. From the panel on the side, click the 🗀 icon to display the computer tree's folder view.
- From the computer tree, click the context menu icon of the group whose computers you want to scan and disinfect. The context menu of the relevant branch will open.
- Click one of the following two options:
  - **Scan now**: lets you create a scan task which will be run immediately on all computers in the group.
  - **Schedule scan**: takes you to the **Tasks** area where you can create a recurring and/or scheduled task. The task template will be partially populated: the **Recipients** field will show the group selected in the computer tree. Fill in the remaining options, as explained in section "Creating a task from the Tasks area" on page 363.

Immediate tasks

Immediate tasks (launched through the **Scan now** option in the context menu) have the following characteristics:

- You can select the scan type (**The entire computer** or **Critical areas**). Refer to "Task schedule and frequency" on page 364 for more information.
- They scan the computer's local file system; network drives are ignored.
- **You don't need to specify an execution time or repetition interval**: they are one-time tasks which start right after being configured.
- **You don't need to publish them**: they are automatically published by Panda Endpoint Protection.
- The management console displays a pop-up message informing of the success or failure of the task creation operation.



New scan task created

Figure 20.1: Scan task created' message

Scheduled tasks

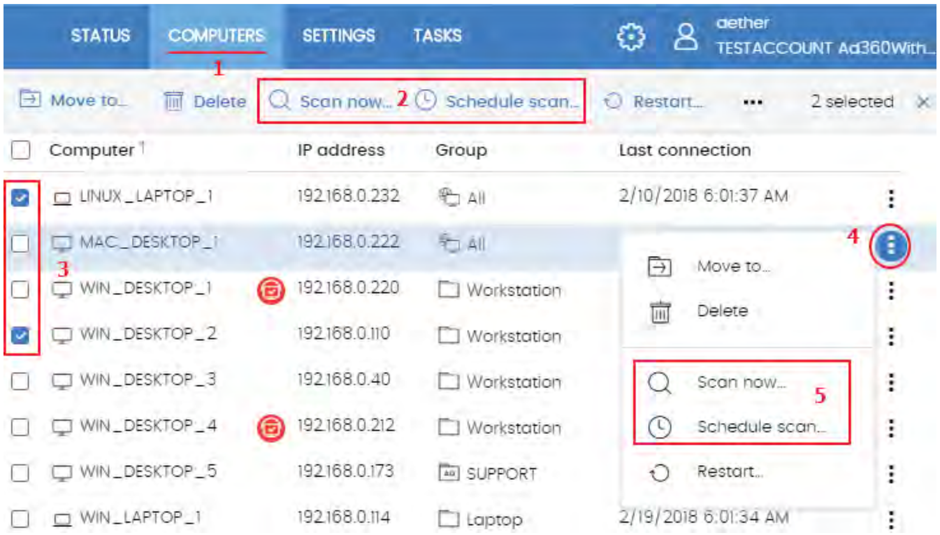
Scheduled tasks (launched through the **Schedule scan** option in the context menu) are identical to the tasks created from the **Tasks** area and discussed in section "Creating a task from the Tasks area" on page 363. The only difference is that the **Recipients** field will be populated with the group selected in the **computer tree**. When creating a scheduled task, you'll have to specify the task's execution time and repetition interval, and publish it for activation.

Creating a task from the Computers list

The **Computers** area lets you create tasks in a similar way to the computer tree or the **Tasks** area. However, in this case you can individually select computers belonging to the same group or subgroup.

Use one of the following resources depending on the number of computers that will receive the task:

- **Context menu**: if the task is to be applied to one computer only.
- **Checkboxes and action bar**: if the task is to be applied to one or more computers belonging to a group or subgroups.



	Computer	IP address	Group	Last connection
☑	LINUX_LAPTOP_1	192.168.0.232	All	2/10/2018 6:01:37 AM
□	MAC_DESKTOP_1	192.168.0.222	All	
□	WIN_DESKTOP_1	192.168.0.220	Workstation	
☑	WIN_DESKTOP_2	192.168.0.110	Workstation	
□	WIN_DESKTOP_3	192.168.0.40	Workstation	
□	WIN_DESKTOP_4	192.168.0.212	Workstation	
□	WIN_DESKTOP_5	192.168.0.173	SUPPORT	
□	WIN_LAPTOP_1	192.168.0.114	Laptop	2/19/2018 6:01:34 AM

Figure 20.2: Context menus and action bar for quick task creation

Context menu associated with a single computer

- Click the Computers **(1)** menu at the top of the console, and select the group in the computer tree that the computer to scan belongs to.
- From the computer list, click the context menu icon of the computer to scan. **(4)**
- From the context menu displayed **(5)**, click one of the following two options:
  - **Scan now:** lets you create a scan task which will be run immediately on the selected computer.
  - **Schedule scan**: takes you to the **Tasks** area. The task template will be partially populated: the Recipients field will show the selected computer. Fill in the remaining options as explained in section "Creating a task from the Tasks area" on page 363.

Checkboxes and action bar

- Click the **Computers (1)** menu at the top of the console and select the group in the computer tree that the computer(s) to scan belong to.
- Use the checkboxes **(3)** to select the computers that will receive the task. An action bar **(2)** will be immediately displayed at the top of the window.

- Click one of the following icons:

  - **Scan now** 🔍 : Lets you create a scan task which will be run immediately on the selected computers.

  - **Schedule scan** 🕒 : takes you to the **Tasks** area. The task template will be partially populated: the Recipients field will display the computers selected in the **computer tree**. Fill in the remaining options as explained in section "Creating a task from the Tasks area" on page 363.

Scan options

The scan options let you configure the scan engine parameters in order to scan your computers' file systems.

Value	Description
Scan type	• **The entire computer**: runs an in-depth scan of the computer, including all connected storage devices. • **Critical areas**: quick scan of the following areas: • `%WinDir%\system32` • `%WinDir%\SysWow64` • Memory • Boot system • Cookies • **Specific items**: lets you enter the path of the mass storage devices you want to scan. This option supports environment variables. The solution will scan the specified path and every folder and file it may contain.
Detect viruses	Detects programs that enter computers with malicious purposes. This option is always selected.
Detect hacking tools and PUPs	Detects potentially unwanted programs, as well as programs that can be used by hackers to carry out actions that cause problems for the user of the affected computer.
Detect suspicious files	In scheduled scans, the security software scans the programs installed on users' computers statically (without running them). This reduces the chance of detecting certain types of threats. To compensate for this and increase the detection rate, Panda Endpoint Protection can use heuristic algorithms. Only if a program is detected by the heuristic protection will the security software treat it as a suspicious program.
Scan compressed files	This option decompresses compressed files and scans their contents.

Table 20.2: Scan options

Value	Description
Exclude the following files from scans	- **Do not scan files excluded from the permanent protections**: files whose execution was allowed by the administrator won't be scanned, along with any file globally excluded in the console. - **Extensions**: enter the extensions of the files that you don't want scanned. You can enter multiple extensions separated by commas. - **Files:** enter the names of the files that you don't want scanned. You can enter multiple names separated by commas. - **Directories**: enter the names of the folders that you don't want scanned. You can enter multiple names separated by commas.

Table 20.2: Scan options

Lists generated by scan tasks

Scan tasks generate lists with results.

Accessing the lists

Follow the steps below to access these lists:

- Go to the **Tasks** menu at the top of the console. Then, click **View results** in the scan task whose results you want to view. You'll access the **Task results** list.
- From the **Task results** list, click **View detections** to access the list of detected items.

Required permissions

Permissions	Access to lists
No permissions	**Scan task results** list.
View detections and threats	Access to a task's **View detections** list.

Table 20.3: Permissions required to access the scan task lists

'Scan task results' list

This list shows the items detected on the computers on your network:

Field	Description	Values
Computer	Name of the scanned computer.	Character string
Group	Folder within the Panda Endpoint Protection folder tree the computer belongs to.	Character string
Detections	Number of items found on the computer.	Numeric value

Table 20.4: Fields in the 'Scan task results' list

Field	Description	Values
Status	Computer scan task status.	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Start date	Date when the computer scan started.	Date
End date	Date when the computer scan ended.	Date

Table 20.4: Fields in the 'Scan task results' list

- **Filter tools**

Field	Comments	Values
Status	The task status	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Detections	Computers where malware was or wasn't detected	• All • With detections • No detections

Table 20.5: Filters available in the 'Scan task results' list

'View detections' list

This list shows details of each malware detection made by the scan task.

Field	Description	Values
Computer	Computer name.	Character string

Table 20.6: Fields in the 'View detections' list

Field	Description	Values
Group	Folder within the Panda Endpoint Protection folder tree the computer belongs to.	Character string
Threat type	Malware category based on the actions the threat is designed to perform.	• Virus • Spyware • Tracking cookies • Hacking tools and PUPs • Phishing • Dangerous actions blocked • Malware URLs • Other
Path	Threat location on the computer.	Character string
Action	Action performed on the computer.	• Quarantined • Deleted • Disinfected • Blocked • Process ended
Date	Date the action was taken.	Date

Table 20.6: Fields in the 'View detections' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "Computer details" on page 159 for more information.

Computer restart

The Web console lets administrators restart computers remotely. This is particularly useful if you have computers that need a restart to finish updating or to fix a protection problem:

- Go to the **Computers** menu at the top of the console and select the computer(s) to restart from the right-hand panel.
  - **To restart a single computer**: click the computer's context menu on the computer list. Select **Restart** from the menu displayed**.**
  - **To restart multiple computers**: use the checkboxes to select the computers to restart. Select **Restart** from the action bar displayed at the top of the screen.

With computers that are turned off, Panda Endpoint Protection will retain the restart command for up to 7 days, after which, if the computer has not been started, the command will be discarded.

Reporting a problem

As with any technology, the Panda Endpoint Protection software installed on your network computers may occasionally function incorrectly. Some symptoms could include:

- Errors reporting a computer's status.
- Errors downloading knowledge or engine updates.
- Protection engine errors.

If Panda Endpoint Protection functions incorrectly on a computer on the network, you can contact Panda Security's support department through the console and automatically send all the information required for diagnosis. To do this, click the **Computers** menu at the top of the console, select the computer with errors, and click its context menu. Select **Report a problem** from the menu displayed.

Allowing external access to the Web console

If you find problems you can't resolve, you can grant Panda Security's support team access to your console. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- On the **Users** tab, click **Allow the Panda Security S.L. team to access my console**.

Chapter 21

Tasks

A task is a resource implemented in Panda Endpoint Protection that allows administrators to associate a process with two variables: repetition interval and execution time.

- **Repetition interval**: tasks can be configured to be performed only once, or repeatedly through specified time intervals.
- **Execution time**: tasks can be configured to be run immediately after being set (immediate task), or at a later time (scheduled task).

CHAPTER CONTENT

Introduction to the task system

Accessing the task system

Depending on your need to configure all parameters of a task, these can be set up from different areas of the management console:

- Top menu **Tasks**
- Computer tree (accessible from the top menu **Computers**)
- Lists associated with the different supported modules.

The computer tree and the lists let you schedule and launch tasks easily and quickly, without having to go through the entire configuration and publishing process described in section "**Steps to launch a task**". However, they provide less configuration flexibility.

Steps to launch a task

The primary resource for creating a task is the **Tasks** area accessible from the menu at the top of the console. This area lets you create tasks from scratch, configuring every aspect of the process.

The process of launching a task consists of three steps:

- **Task creation and configuration**: select the affected computers, the characteristics of the task, the time/date the task will be launched, the task frequency, and the way it will behave in the event of an error.
- **Task publication**: the tasks you create must be entered in the Panda Endpoint Protection task scheduler in order to be run on the scheduled day/time.
- **Task execution**: the task is run when the configured conditions are met.

Task types

Panda Endpoint Protection performs the following tasks:

- Scans and disinfects files. Refer to "**On-demand computer scanning and disinfection**" on page 352.
- Installs patches and updates for the operating system and other programs installed on users' computers. Refer to "**Panda Patch Management (Updating vulnerable programs)**" on page 227.

Permissions associated with task management

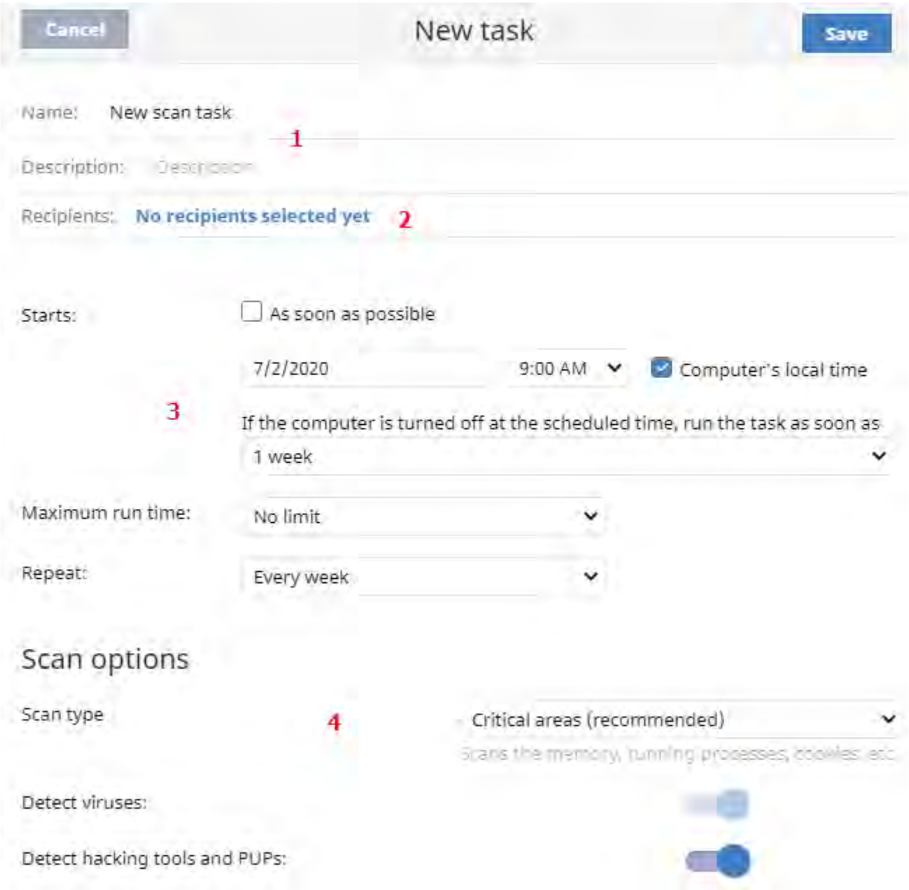
*For more information about the permission system implemented in Panda Endpoint Protection, refer to "**Understanding permissions**" on page 57.*

To create, edit, delete, or view tasks, you must use a user account that has the appropriate permission assigned to its role. Depending on the task, the required permissions are:

- **Launch scans and disinfect**: to create, delete, and edit **Scheduled scans** tasks.
- **Install, uninstall, and exclude patches**: to create, delete, and edit **Install patches** tasks.
- **View detections**: to view the results of **Scheduled scans** tasks.

Creating a task from the Tasks area

- Click **Tasks** in the top menu. A list of all created tasks will be displayed, along with their status.
- Click the **Add task** button and select a task type from the drop-down menu. A window will be displayed with the task details, divided into multiple areas:
  - **Overview (1)**: task name and description.
  - **Recipients (2)**: computers that will receive the task.
  - **Schedule (3)**: task schedule (day and time the task will be launched).
  - **Settings (4)**: specify the actions to be taken by the task. This section varies based on the task type and is described in the documentation associated with the related module.



Name: New scan task

Description: Description

Recipients: No recipients selected yet

Starts: ☐ As soon as possible

7/2/2020 9:00 AM ☑ Computer's local time

If the computer is turned off at the scheduled time, run the task as soon as: 1 week

Maximum run time: No limit

Repeat: Every week

Scan options

Scan type: Critical areas (recommended)

Scans the memory, running processes, cookies, etc.

Detect viruses:

Detect hacking tools and PUPs:

Figure 21.1: Overview of the 'New task' window for a scan-type task

Task recipients (2)

- Click the **No recipients selected yet** link in the **Recipients** section. This will open a window where you will be able to select the computers that will receive the configured task.
- Click the ⊕ button to add individual computers or computer groups, and the 🗑 button to remove

them.

To access the computer selection window, you must first save the task. If you haven't saved the task, a warning message will be displayed.

- Click the **View computers** button to view the computers that will receive the task.

Task schedule and frequency

You can configure the following three parameters:

- **Starts:** indicates the task start time/date.

Value	Description
As soon as possible (selected)	The task will be launched immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified **if the computer is turned off**.
As soon as possible (cleared)	The task will be launched on the date selected in the calendar. Specify whether to take into account the computer's local time or the Panda Endpoint Protection server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task won't run. The task scheduler lets you establish the task's expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** the task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** lets you define the time interval during which the task will be run if the computer becomes available. • **Run when the computer is turned on:** there is no time limit. The system waits indefinitely for the computer to be available to launch the task.

Table 21.1: Task launch parameters

- **Maximum run time**: indicates the maximum time that the task can take to complete. After that time, the task will be canceled returning an error.

Value	Description
No limit	There is no time limit for the task to complete.
1, 2, 8, or 24 hours	There is a time limit for the task to complete. After that time, if the task has not finished, it is canceled returning an error.

Table 21.2: Task duration parameters

- **Frequency**: set a repeat interval (every day, week, month, or year) from the date specified in the

Starts: field.

Value	Description
One time	The task is run only once at the time specified in the **Starts:** field.
Daily	The task is run every day at the time specified in the **Starts:** field.
Weekly	Use the checkboxes to select the days of the week on which the task must be run, at the time specified in the **Starts:** field.
Monthly	Choose an option: Run the task on a specific day of every month. If you select the, 29th, 30th, or 31st of the month, and the month does not have that day, the task will be run on the last day of the month. Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 21.3: Configuring the frequency of a task

Automatic conversion of the execution frequency

If any of the computers on the network has an older version of the security software installed, it may not be able to correctly interpret the frequency set by the administrator in the web console. In that case, the computer will establish the following correspondence with regard to the frequency of the tasks to be run:

- **Daily tasks**: no change.
- **Weekly tasks**: the days selected by the administrator are ignored. The first execution occurs on the date specified in the **Starts:** field. Then, the task is rerun every 7 days.
- **Monthly tasks**: the days selected by the administrator are ignored. The first execution occurs on the date specified in the **Starts:** field. Then, the task is rerun every 30 days.

Task publication

Once you have created and configured a task, it will be added to the list of configured tasks. However, it will display the **Unpublished** tag, meaning that it is not yet active.

To publish a task, click the **Publish** button. It will be added to the Panda Endpoint Protection task scheduler, which will launch the task based on its settings.

Task list

Click **Tasks** in the top menu to view a list of all created tasks, their type, status, and other relevant information.

Field	Comments	Values
Icon	The task type	• 🩹 Patch installation or uninstallation task • 🔍 On-demand scan task • 🧰 Disinfection task
Name	The task name	Character string
Schedule	Date the task is set to run.	Character string
Status	• **No recipients:** the task won't run because there are no recipients assigned to it. Assign one or more computers to the task. • **Unpublished:** the task won't run because it hasn't been added to the scheduler queue. Publish the task so that it can be launched by the scheduler based on its settings. • **In progress:** the task is running. • **Canceled**: the task was manually canceled. This does not mean that all processes that were running on the target computers have stopped. • **Finished**: the task finished running on all affected computers, regardless of whether it failed or was performed successfully. This status only applies to one-time tasks.	Character string

Table 21.4: Fields in the 'Tasks' list

- **Filter tool**

Field	Comments	Values
Type	The task type	• Scan • Disinfection • Patch installation • Patch uninstallation • All
Search task	Enter the task name	Character string
Schedule	The task's repeat frequency	• All • Immediate • Once • Scheduled
Sort list ⇣	Task list sort order.	• Sort by creation date • Sort by name • Ascending • Descending

Table 21.5: Filters available in the 'Tasks' list

Task management

Click **Tasks** in the top menu to delete, copy, cancel, or view the results of created tasks.

Modifying a published task

Click a task's name to display its settings window. There you will be able to modify any of the task's parameters.

> *Published tasks only allow you to change their name and description. To be able to modify other parameters of a published task, you must copy it.*

Canceling a published task

Select the checkboxes to the left of the tasks to cancel. Click the **Cancel** ⊗ icon from the toolbar. The tasks are canceled, but they do not disappear from the Tasks page so you can still view their results. Only tasks whose status is **In progress** can be canceled.

Deleting a task

Executed tasks are not automatically deleted. To delete a task, select it using the checkboxes and click the 🗑 icon. A published task can only be deleted if it is previously canceled.

Deleting a task also deletes its results.

Copying a task

To copy a task, click its ⧉ icon.

Task results

Click the **View results** link of a published task to view its results so far and access a filter tool for finding specific computers among those that received the task.

Some of the fields in the results list are specific to certain tasks. Those fields are described in the documentation associated with the relevant module. Below is a description of the fields that are common to all results lists.

Field	Description	Values
Computer	Name of the computer where the task took place.	Character string
Group	Folder within the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Status	Status of the task process on the affected computer: • **Pending**: the task was published successfully, but the target computer has not yet received it or has received it but the task has not yet run because it is scheduled to run at a later time. • **In progress**: the task is running on the computer. • **Finished**: the task finished successfully. • **Failed**: the task failed and returned an error. • **Canceled (the task could not start at the scheduled time):** the task could not start at the scheduled time because the target computer was turned off or in a state that prevented the task from running. • **Canceled**: the process was canceled on the computer.	Character string

Table 21.6: Common fields in task results lists

Field	Description	Values
	• **Canceling:** the task was canceled, but the target computer has not finished canceling the task process. • **Canceled (maximum run time exceeded:** the task was automatically canceled because it exceeded its maximum configured run time.	
Start date	The task start date.	Date
End date	The task end date.	Date

Table 21.6: Common fields in task results lists

- **Task filter tool**

Field	Description	Values
Date	Drop-down menu with the date the task became active based on the configured schedule. An active task will launch immediately or wait until the target machine is available. This date is shown in the Date column.	Date
Status	• **Pending**: the task has not yet started as the execution window has not been reached. • **In progress**: the task is currently running. • **Finished**: the task finished successfully. • **Failed**: the task failed and returned an error. • **Canceled (the task could not start at the scheduled time)**: the target computer was not accessible at the time the task was set to start or during the defined window. • **Canceled**: the task was manually canceled. • **Canceled (maximum run time exceeded)**: the task was automatically canceled because it exceeded its maximum configured run time.	Enumeration

Table 21.7: Search filters in task results

Automatic adjustment of task recipients

If the administrator selects a computer group as the recipient of a task, the computers that finally run the task may vary from those initially selected. This is because groups are dynamic entities that change over time.

That is, you can define a task at a specific time (T1) to be run on a specific group containing a series of computers. However, at the time the task is run (T2), the computers in that group may have changed.

When it comes to determining which computers will receive a configured task, there are three cases depending on the task:

- Immediate tasks.
- One-time scheduled tasks.
- Recurring scheduled tasks.

Immediate tasks

These tasks are created, published, and launched almost simultaneously and only once. The target group is evaluated at the time the administrator creates the task. The task status for the affected computers will be **Pending**.

- **Adding computers to the target group**

It is not possible to add new computers to the target group. Even if you add new computers to the target group, they won't receive the task.

- **Removing computers from the target group**

You can remove computers from the target group. Move a computer to another group to cancel the task on that computer.

One-time scheduled tasks

There are two possible scenarios for changing the computers included in the target group:

- **Tasks which started running less than 24 hours ago**

Within the first 24 hours after a task started running, it is still possible to add or remove computers from its target groups. This 24-hour period is established to cover all time zones for multinational companies with a presence in several countries.

- **Tasks which started running more than 24 hours ago**

24 hours after a task starts running, it is not possible to add new computers to it. Even if you add new computers to the target group, they won't receive the task. To cancel the task on a computer, move it outside the target group.

Recurring scheduled tasks

These tasks allow the addition and removal of target computers at any time before they are canceled or completed.

Unlike immediate tasks, the status of the task on each computer will not be automatically set to **Pending**. The status of the task on each computer will be shown gradually in the console as the Aether platform receives the relevant information from each machine.

Part 8

Additional information about Panda Endpoint Protection

Chapter 22

Hardware, software and network requirements

Most of the security intelligence that Panda Endpoint Protection generates and uses is generated in the cloud. This intelligence is downloaded and leveraged by the security software installed on users' computers. To make sure the security software works correctly, the customer's IT infrastructure must meet the requirements specified in the next sections.

CHAPTER CONTENT

Features by platform

Available features		Windows (Intel & ARM)	Linux	MacOS	Android
General	Web console	X	X	X	X
	Dashboards	X	X	X	X
	Filter-based computer organization	X	X	X	X
	Group-based computer organization	X	X	X	X
	Languages supported by the agent	11	11	11	16
Lists and reports	Frequency of sending malware, PUP, and exploit activity data and blocked programs to the server	1 min	10 mins	10 mins	Immediately after a scan is completed
	Frequency of sending detections to the server	15 mins	15 mins	15 mins	Right after a scan is complete
	List of detections	X	X	X	X
	Executive report	X	X	X	X
	Scheduled executive report	X	X	X	X
Protections	Anti-Tamper protection	X			X
	Real-time permanent antivirus protection	X	X	X	X
	Contextual detections	X	X		
	Firewall	X			
	Device control	X			
Hardware and software information	Hardware information and list	X	X		X
	Software information and list	X	X	X	X
	Software change log	X	X	X	X

Table 22.1: Features by platform

Available features		Windows (Intel & ARM)	Linux	MacOS	Android
	Information about the OS patches installed	X			
Settings	Security for workstations and servers	X	X	X	N/A
	Password for uninstalling the protection and taking actions locally	X			
	Ability to assign multiples proxies	X			N/A
	Ability to act as Panda proxy	X			N/A
	Ability to use Panda proxy	X	X	X	N/A
	Ability to act as a repository/cache	X			N/A
	Ability to use a repository/cache	X			N/A
	Ability to discover unprotected computers	X			
	Email alerts in the event of an infection	X	X	X	X
	Email alerts when finding unprotected computers	X	X	X	X
Remote actions from the Web console	Real-time actions	X	X	X	X
	On-demand scans	X	X	X	X
	Scheduled scans	X	X	X	X
	Remote installation of the Panda agent	X			
	Ability to reinstall the protection agent	X			
	Ability to restart computers	X	X	X	

Table 22.1: Features by platform

Available features		Windows (Intel & ARM)	Linux	MacOS	Android
	Ability to report incidents (PSInfo)	X			X
Updates	Signature updates	X	X	X	X
	Protection upgrades	X	X	X	X
	Ability to schedule protection upgrades	X	X	X	Google Play
Modules	Panda Patch Management (*)	X			
	Panda Full Encryption	X			

Table 22.1: Features by platform

(*) Only available for Intel microprocessors.

Requirements for Windows platforms

Supported operating systems

Workstations with an x86 or x64 microprocessor

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)

Computers with an ARM microprocessor

- Windows 10 Pro
- Windows 10 Home

Servers with an x86 or x64 microprocessor

- Windows 2003 (32-bit, 64-bit and R2) SP2 and later
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2

- Windows Server 2016 and 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 and 2019

IoT and Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits)

Hardware requirements

- **Processor:** x86 or x64-compatible CPU with SSE2 support
- **RAM:** 1 GB
- **Available hard disk space for installation**: 650 MB

Other requirements

For the product to work correctly it is necessary to keep the root certificates of workstations and servers fully up to date. If this requirement is not met, some features such as the ability for agents to establish real-time communications with the management console or the Panda Patch Management module might stop working.

Requirements for macOS platforms

Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.0 Big Sur

Hardware requirements

- **Processor**: Intel® Core 2 Duo
- **RAM**: 2 GB
- **Available hard disk space for installation**: 400 MB
- **Ports**: ports 3127, 3128, 3129 and 8310 must be accessible for the malware detection to work.

Requirements for Linux platforms

Panda Endpoint Protection can be installed on both Linux workstations and servers. If there is no graphical environment installed at the time of installing the solution, the Web filter protection will be disabled. On computers with no graphical environment installed, use the `/usr/local/protection-agent/pa_cmd` tool to manage the protection.

To complete the installation of Panda Endpoint Protection on Linux platforms, the target computer must remain connected to the Internet throughout the installation process.

Supported 64-bit distributions

- **Ubuntu**: 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS, 16.10, 17.04, 17.10, 18,04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04
- **Fedora:** 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, and 34
- **Debian:** 8, 9, 10
- **Red Hat:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, and 8.4
- **CentOS:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, and 8.4
- **Linux Mint:** 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2, 19.3, 20, 20.1
- **SUSE Linux Enterprise**: 11.2, 11.3, 11.4, 12, 12.1, 12.2, 12.3, 12.4, 12.5, 15, 15.1, 15.2

Supported 32-bit distributions

- RedHat 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10
- CentOS 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10

Supported kernel versions

For more information about the supported Linux distributions and kernels, refer to https://www.pandasecurity.com/en/support/card?id=700009#show2.

Panda Endpoint Protection is not supported on special or modified versions of the Linux kernel.

Supported file managers

- Nautilus
- PCManFM
- Dolphin

Hardware requirements

- **Processor:** x86 or x64-compatible CPU with SSE2 support
- **RAM:** 1.5 GB
- **Available hard disk space for installation:** 100 MB.
- **Ports:** ports 3127, 3128, 3129 and 8310 must be accessible for the malware detection to work.
- **Installation package dependencies:**

During the installation process, the Linux agent will download all packages required to satisfy dependencies. Generally speaking, the packages required by the system to work are as follows:

- Libcurl
- OpenSSL
- GCC and Fedora's compilation utilities (make, makeconfig, etc.)

> *The installation process on Fedora includes compilation of the modules required by the Panda Endpoint Protection agent to work properly.*

To display the agent dependencies, run the following commands on a terminal based on the target distribution:

- For Debian-based distributions: `dpkg --info package.deb`
- For Fedora-based distributions: `rpm --qRp package.rpm`

Requirements for Android platforms

Supported operating systems

- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0
- Pie 9.0

- Android 10
- Android 11

Hardware requirements

A minimum of 10 MB of internal memory is required on the target device. Depending on the model, it is possible that the required space be larger.

Network requirements

For push notifications to work properly, it is necessary to open ports 5228, 5229 and 5230 to all IP addresses contained in the IP blocks listed in Google's ASN of 15169.

Web console access

The management console supports the latest versions of the following Web browsers:

- Chrome
- Internet Explorer
- Microsoft Edge
- FireFox
- Opera

Access to service URLs

For Panda Endpoint Protection to operate properly, the protected computers must be able to access the following URLs.

Product name	URLs
Panda Endpoint Protection	• https://*.pandasecurity.com • Downloading of installers, the generic uninstaller, and policies. • Agent communications (registration, configuration, tasks, actions, status, real-time communications). • Communications between the protection and Collective Intelligence. • Downloading of signature files on Android systems. • http://*.pandasecurity.com • Downloading of signature files (on all systems except Android). • https://*.windows.net • Performance counters (CPU, memory, disk, etc.) • Notifications every 15 minutes if there is no real-time communication.
Root Certificates	• http://*.globalsign.com • http://*.digicert.com • http://*.sectigo.com
Panda Patch Management	• All URLs in the following resource: https://forums.ivanti.com/s/article/URL-Exception-List-for-Ivanti-Patch-for-SCCM • https://content.ivanti.com
Activity testing	• http://proinfo.pandasoftware.com/connectiontest.html In the case of Windows protection versions prior to 8.00.16. • http://*.pandasoftware.com For connectivity tests.

Table 22.2: Access to service URLs

Ports

- Port 80 (HTTP)
- Port 443 (HTTPS, WebSocket)
- Port 8080 (access from Orion)

Patch and update download (Panda Patch Management)

Refer to the following support article **https://www.pandasecurity.com/uk/support/card?id=700044** for a full list of the URLs that must be accessible by the network computers that will receive patches, or by the network computers with the cache/ repository role.

Chapter 23

The Panda Account

The Panda Account provides administrators with a safer mechanism to self-manage login credentials and access the Panda Security services purchased by their organization than the standard method of receiving credentials by email.

With a Panda Account, it is the administrator who creates and activates the access method to Panda Endpoint Protection's Web console.

> *Users with access to the Panda Account are those who were initially registered in Panda Security, regardless of whether they have been migrated to the WatchGuard provider. Users belonging to the WatchGuard security provider from the start don't have access to the Panda Account.*

CHAPTER CONTENTS

Creating a Panda Account for Panda Security users

Follow the steps below to create a new Panda Account.

Receive the email

- When purchasing Panda Endpoint Protection, you will receive an email from Panda Security.
- Click the link in the message to access a website from which you will be able to create your Panda Account.

Fill out the form

- Enter your information in the form shown.
- Use the drop-down menu located in the bottom-right corner if you want to display the page in a different language.
- Access the License Agreement and the Privacy Policy by clicking the relevant links.
- Click **Create** to finish and receive an email at the address indicated in the form. Use that message to activate your account.

Activating the Panda Account

After it is created, you need to activate your Panda Account. To do this, you must use the message received at the email address you specified when creating your Panda Account.

- Find the message in your inbox.
- Click the activation button. By doing this, the address provided when creating your Panda Account will be confirmed as valid. If the button doesn't work, copy and paste the URL included in the message into your browser.
- The first time you access your Panda Account, you will be asked to confirm your password. Do it and click the **Activate account** button.
- Enter the required information and click **Save data**. If you prefer to provide your data at another time, use the **Not now** option.
- Accept the License Agreement and click **OK**.

Once your Panda Account has been successfully activated, you will be taken to the Cytomic Central site home page. From there, you will be able to access the Panda Endpoint Protection Web console. To do this, click the solution's icon you will find in the **My Services** section.

Editing the Panda Account

If your associated security provider is Panda Security, click the **Edit account** option in Cytomic Central.

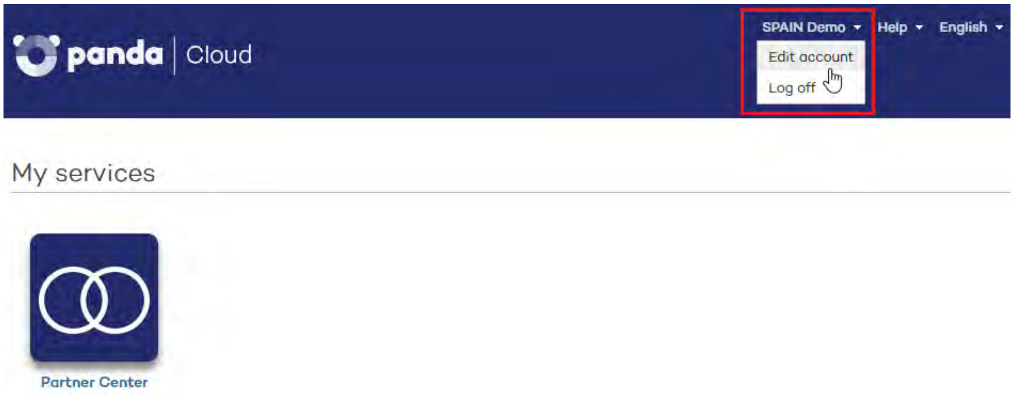


Figure 23.1: Editing the user account

If your associated security provider is WatchGuard, go to https://watchguard.com/

Creating and linking a Panda Account to WatchGuard

For more information on how to activate and link a Panda Account when activating a commercial license, refer to https://www.pandasecurity.com/en/support/card?id=300003.

To manage products from Aether, WatchGuard users must meet the following requirements:

- They must have a WatchGuard user account.
- They must have a Panda Endpoint Protection user account.
- They must link both accounts.

Users belonging to the WatchGuard security provider from the start automatically create a Panda Account when activating a commercial license for a Panda Security product for the fist time.

Users belonging to the WatchGuard security provider but who initially belonged to Panda Security already have a Panda Account. All they have to do is link that account to their WatchGuard Account.

Creating a Panda Account automatically when assigning a commercial license for a Panda Security product

- Go to https://watchguard.com/activate and enter the license key for the Panda Security product.
- Click **I need a Panda account**. A page opens with the account name and ID. We recommend that you save this information. You need this information if you contact Support.
- Click **Submit** and **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.
- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Panda Endpoint Protection.
- To access Panda Endpoint Protection, click **Manage Your Panda Product**. Next, click **Accept and continue** to accept the End User License Agreement.

Linking a Panda Account to a WatchGuard Account when assigning a commercial license for a Panda Security product

- Go to https://watchguard.com/activate and enter the license key for the Panda Security product.
- Click **Link my Panda account**. The Cytomic Central page opens. Enter your Panda Endpoint Protection login credentials. These were sent to you in the welcome email.
- Click the **Log in** button. A page opens indicating that both accounts are linked.
- Click **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.
- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Panda Endpoint Protection.
- To access Panda Endpoint Protection, click **Manage Your Panda Product**. Next, click **Accept and continue** to accept the End User License Agreement.

Chapter 24

Key concepts

Active Directory

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed directory service for finding a range of information on network environments.

Adware

Program that automatically runs, displays or downloads advertising to the computer.

Anti-Tamper protection

A set of technologies aimed at preventing tampering of the Panda Endpoint Protection processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

Anti-theft

Set of technologies incorporated into Panda Endpoint Protection and designed to locate lost or stolen mobile devices and minimize data exposure in the case of theft.

Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, contextual analysis, etc.), to detect and remove computer viruses and other threats.

ARP (Address Resolution Protocol)

A telecommunication protocol used for resolution of Internet layer addresses into link layer addresses. On IP networks, this protocol translates IP addresses into physical MAC addresses.

Automatic assignment of settings

See “**Inheritance**”.

Backup

Storage area for non-disinfectable malicious files, as well as the spyware items and hacking tools detected on your network. All programs classified as threats and removed from the system are temporarily moved to the backup/quarantine area for a period of 7/30 days based on their type.

BitLocker

Software installed on certain versions of Windows 7 and above computers and designed to encrypt and decrypt the data stored on computer volumes. This software is used by Panda Full Encryption.

Broadcasting

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network simultaneously, without the need to send it individually to each device. Broadcast packets don't go through routers and use different addressing methodology to differentiate them from unicast packets.

Buffer overflow

Anomaly affecting the management of a process' input buffers. In a buffer overflow, if the size of the data received is greater than the allocated buffer, the redundant data is not discarded, but is written to adjacent memory locations. This may allow attackers to insert arbitrary executable code into the memory of a program on systems prior to Microsoft's implementation of the DEP (Data Execution Prevention) technology.

Cache/Repository (role)

Computers that automatically download and store all files required so that other computers with Panda Endpoint Protection installed can update their signature file, agent and protection engine without having to access the Internet. This saves bandwidth as it won't be necessary for each computer to separately download the updates they need. All updates are downloaded centrally for all computers on the network.

Cloud (Cloud computing)

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

Computers without a license

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers are not protected, but are displayed in the Web management console.

CVE (Common Vulnerabilities and Exposures)

List of publicly known cyber-security vulnerabilities defined and maintained by The MITRE Corporation. Each entry on the list has a unique identifier, allowing CVE to offer a common naming scheme that security tools and human operators can use to exchange information about vulnerabilities with each other.

Device control

Module that allows organizations to define the way protected computers must behave when connecting a removable or mass storage device to them.

DEP (Data Execution Prevention)

A feature implemented in operating systems to prevent the execution of code in memory pages marked as non-executable. This feature was developed to prevent buffer-overflow exploits.

DHCP

Service that assigns an IP address to each computer on a network

Dialer

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

Discovery computer (role)

Computers capable of finding unmanaged workstations and servers on the network in order to remotely install the Panda Endpoint Protection agent on them.

Disinfectable file

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

Domain

Windows network architecture where the management of shared resources, permissions and users is centralized in a server called a Primary Domain Controller (PDC) or Active Directory (AD).

Domain Name System (DNS)

Service that translates domain names into different types of information, generally IP addresses.

End-of-Life (EOL)

A term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life. Once a product reaches its EOL stage, it stops receiving updates or fixes from the relevant vendor, leaving it vulnerable to hacking attacks.

Environment variable

A string consisting of environment information such as a drive, path or file name, which is associated with a symbolic name that Windows can use. You can use the System applet in the Control Panel or the 'set' command at the command prompt to set environment variables.

Exchange server

Mail server developed by Microsoft. Exchange servers store inbound and/or outbound emails and distribute them to users' email inboxes.

Excluded program

Programs that were initially blocked as they were classified as malware or PUP, but have been selectively and temporarily allowed by the administrator, who excluded them from the scans performed by the solution.

Filter tree

Collection of filters grouped into folders, used to organize all computers on the network and facilitate the assignment of settings.

Firewall

Technology that blocks the network traffic that coincides with certain patterns defined in rules established by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

Folder tree

Hierarchical structure consisting of static groups, used to organize all computers on the network and facilitate the assignment of settings.

FQDN

A fully qualified domain name (FQDN) is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone. A fully qualified domain name is distinguished by its lack of ambiguity: it can be interpreted only in one way.

Fragmentation

On data transmission networks, when the MTU of the underlying protocol is not sufficient to accommodate the size of the transmitted packet, routers divide the packet into smaller segments (fragments) which are routed independently and assembled in the right order at the destination.

Geolocation

Geographical positioning of a device on a map from its coordinates.

Goodware

A file which, after analysis, has been classified as legitimate and safe.

Group

Static container that groups one or more computers on the network. Computers are assigned to groups manually. Groups simplify the assignment of security settings, and facilitate management of all computers on the network.

Hacking tool

Programs used by hackers to carry out actions that cause problems for the user of the affected computer (allowing the hacker to control the computer, steal confidential information, scan communication ports, etc.).

Heap Spraying

Heap Spraying is a technique used to facilitate the exploitation of software vulnerabilities by malicious processes.

As operating systems improve, the success of vulnerability exploit attacks has become increasingly random. In this context, heap sprays take advantage of the fact that on most architectures and operating systems, the start location of large heap allocations is predictable and consecutive allocations are roughly sequential. This allows attackers to insert and later run arbitrary code in the target system's heap memory space.

This technique is widely used to exploit vulnerabilities in Web browsers and Web browser plug-ins.

Heuristic scanning

Static scanning that employs a set of techniques to statically inspect potentially dangerous files. It examines hundreds of characteristics of a file to determine the likelihood that it may take malicious or harmful actions when run on a user's computer.

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

ICMP (Internet Control Message Protocol)

Error notification and monitoring protocol used by the IP protocol on the Internet.

IDP (Identity Provider)

Centralized service for managing user identity verification.

Indirect assignment of settings

See "**Inheritance**".

Infection vector

The means used by malware to infect users' computers. The most common infection vectors are Web browsing, email and pen drives.

Inheritance

A method for automatically assigning settings to all subsets of a larger, parent group, saving management time. Also referred to as 'automatic assignment of settings' or 'indirect assignment of settings'.

IP address

Number that identifies a device interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

IP (Internet Protocol)

Principal Internet communications protocol for sending and receiving datagrams generated on the underlying link level.

Joke

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

Linux distribution

Set of software packets and libraries that comprise an operating system based on the Linux kernel.

MAC address

48-bit hexadecimal number that uniquely identifies a network card or interface.

Malware

This term is used to refer to all programs that contain malicious code (MALicious softWARE), whether it is a virus, Trojan, worm or any other threat to the security of IT systems. Malware tries to infiltrate or damage computers, often without users knowing, for a variety of reasons.

Malware Freezer

A feature of the quarantine/backup module whose goal is to prevent data loss due to false positives. All files classified as malware or suspicious are sent to the quarantine/backup area, thereby avoiding deleting and losing data if the classification is wrong.

Manual assignment of settings

Direct assignment of a set of settings to a group, as opposed to the automatic or indirect assignment of settings, which uses the inheritance feature to assign settings without administrator intervention.

MD5 (Message-Digest Algorithm 5)

A cryptographic hash function producing a 128-bit value that represents data input. The MD5 hash value calculated for a file is used to identify it unequivocally or check that it has not been tampered with.

MTU (Maximum Transmission Unit)

Maximum packet size (in bytes) that the transport will transmit over the underlying network.

Network adapter

Hardware that allows communication among different computers connected through a data network. A computer can have more than one network adapter installed, and is identified in the system through a unique identifier.

Network topology

Physical or logical map of network nodes.

OU (Organizational Unit)

Hierarchical method for classifying and grouping objects stored in directories.

Panda Endpoint Protection software

Program installed on the computers to protect. It consists of two modules: the Panda agent and the protection.

Panda agent

One of the modules included in the Panda Endpoint Protection software. It manages communications between computers on the network and Panda Security's cloud-based servers, in addition to managing local processes.

Panda Full Encryption

A module compatible with Panda Endpoint Protection and designed to encrypt the content of computers' internal storage devices. It aims to minimize the exposure of the data stored by organizations in the event of loss or theft, or when unformatted storage devices are replaced or withdrawn.

Panda Patch Management

A module compatible with Panda Endpoint Protection that updates and patches the programs installed on an organization's workstations and servers in order to remove the software vulnerabilities stemming from programming bugs and reduce the attack surface.

Partner

A company that offers Panda Security products and services.

Passphrase

Also known as enhanced PIN or extended PIN, a passphrase is a PIN that incorporates alphanumeric and non-alphanumeric characters. A passphrase supports lowercase and uppercase letters, numbers, spaces and symbols.

Patch

Small programs published by software vendors to fix their software and add new features.

Payload

In the IT and telecommunications sectors, a message payload is the set of useful transmitted data (as opposed to other data that is also sent to facilitate message delivery: header, metadata, control information, etc.).

In IT security circles, however, an exploit's payload is the part of the malware code that controls the malicious actions taken on the system, such as deleting files, stealing data, etc. (as opposed to the part responsible for leveraging the software vulnerability -the exploit- in order to run the payload).

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Phishing

A technique for obtaining confidential information from a user fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

Port

Unique ID number assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

Potentially Unwanted Program (PUP)

A program that may be unwanted, despite the possibility that users consented to download it. Potentially unwanted programs are often downloaded inadvertently along with other programs.

Protection (module)

One of the two components of the Panda Endpoint Protection software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the Panda Endpoint Protection cloud.

Public network

Networks in public places such as airports, coffee shops, etc. These networks require that you establish some limitations regarding computer visibility and usage, especially with regard to file, directory and resource sharing.

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Quarantine

See "**Backup**".

Recovery key

If an anomalous situation is detected on a computer protected with Panda Full Encryption, or if you forget the unlock key, the system will request a 48-digit recovery key. This key is managed from the management console and must be entered to start the computer. Each encrypted volume has its own unique recovery key.

RIR (Regional Internet Registry)

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

Role

Specific permission configuration applied to one or more user accounts, and which authorizes users to view and edit certain resources of the console.

Rootkit

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is used by attackers to hide evidence and utilities on previously compromised systems.

RWD (Responsive Web Design)

A set of techniques that enable the development of Web pages that automatically adapt to the size and resolution of the device being used to view them.

Settings

See "**Settings profile**".

Settings profile

Specific settings governing the protection or any other aspect of the managed computer. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

Signature file

File that contains the patterns used by the antivirus to detect threats.

SMTP server

Server that uses SMTP (Simple Mail Transfer Protocol) to exchange email messages between computers.

Spyware

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and collects personal data.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

Suspicious item

A program with a high probability of being malware and classified by our heuristic scanner. This type of technology is only used in the scheduled and on-demand scans launched from the Tasks module, never in real-time scans. Heuristic scanning is used to compensate for the lower detection capability of scheduled scan tasks, in which program code is scanned statically, without running the program.

Refer to "**Heuristic scanning**".

SYN

Flag in the TOS (Type Of Service) field of TCP packets that identifies them as connection start packets.

System partition

Area of the hard disk that remains unencrypted and which is necessary for computers with Panda Full Encryption enabled to start up properly.

Task

Set of actions scheduled for execution at a configured frequency during a specific period of time.

TCO (Total Cost of Ownership)

Financial estimate of the total direct and indirect costs of owning a product or system.

TCP (Transmission Control Protocol)

The main transport-layer Internet protocol, aimed at connections for exchanging IP packets.

TLS (Transport Layer Security)

New version of protocol SSL 3.0.

TPM (Trusted Platform Module)

The TPM is a chip that's part of the motherboard of desktops, laptops and servers. It aims to protect users' sensitive information by storing passwords and other information used in authentication processes.

Additionally, the TPM is responsible for detecting changes to a computer's boot chain, preventing, for example, access to a hard disk from a computer other than the one used to encrypt it.

Trojans

Programs that reach computers disguised as harmless software to install themselves on computers and carry out actions that compromise user confidentiality.

Trusted network

Networks in private places such as offices and households. Connected computers are generally visible to the other computers on the network, and there is no need to establish limitations on file, directory and resource sharing.

UDP (User Datagram Protocol)

A transport-layer protocol which is unreliable and unsuited for connections for exchanging IP packets.

Unblocked program

Program blocked during the classification process but temporarily and selectively allowed by the administrator to avoid disrupting user activity.

USB key

A device used on computers with encrypted volumes and which allows the recovery key to be stored on a portable USB drive. With a USB key it is not necessary to enter a password to start up the computer. However, the USB device with the startup password must be plugged into the computer's USB port.

User (console)

Information set used by Panda Endpoint Protection to regulate administrator access to the Web console and establish the actions that administrators can take on the network's computers.

User (network)

A company's workers using computing devices to do their job.

User account

See “**User (console)**”.

VDI (Virtual Desktop Infrastructure)

Desktop virtualization solution that hosts virtual machines in a data center accessed by users from a remote terminal with the aim to centralize and simplify management and reduce maintenance costs. There are two types of VDI environments:

- **Persistent VDIs**: the storage space assigned to each user persists between restarts, including the installed software, data, and operating system updates.
- **Non-persistent VDIs**: the storage space assigned to each user is deleted when the VDI instance is restarted, returning to its initial state and undoing all changes made.

Virus

Programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

VPN (Virtual Private Network)

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

Web console

Tool to manage the advanced security service Panda Endpoint Protection, accessible anywhere, anytime through a supported Internet browser. The Web console allows administrators to deploy the security software, push security settings, and view the protection status. It also provides access to a set of forensic analysis tools to assess the scope of security problems.

Widget (Panel)

Panel containing a configurable graph representing a particular aspect of network security. Panda Endpoint Protection's dashboard is made up of different widgets.

Window of opportunity

The time it takes between when the first computer in the world is infected with a new malware specimen and its analysis and inclusion by antivirus companies in their signature files to protect computers from infections. This is the period when malware can infect computers without antivirus software being aware of its existence.

Workgroup

Architecture in Windows networks where shared resources, permissions and users are managed independently on each computer.