Panda Endpoint Protection on Aether

Administration guide

Version: 8.42.00-00

Author: Panda Security

Date: 31/3/2019

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 on Aether Administration Guide

- You can find the most recent version of this guide at:

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 on Aether, 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/uk/support/endpoint-protection-aether.htm

Survey on the Administration Guide

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

https://en.surveymonkey.com/r/feedbackSIEMFeederEvManEN

Contents

Part 1: Panda Endpoint Protection overview

Part 2: The administration console

Part 3: Deployment and getting started

Part 4: Managing network security and devices

Part 5: Viewing and managing threats

Parte 6: Security incident and remediation

Part 7: Additional information about Panda Endpoint Protection

Part 1

Panda Endpoint Protection overview

Chapter 1: Preface

Chapter 2: Panda Endpoint Protection overview

Chapter 3: Panda Endpoint Protection features

Chapter 1

Preface

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

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 on Aether?

Panda Endpoint Protection on Aether 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 on Aether 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 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 on Aether.
🔍	Additional information available in other chapters or sections of the 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 on Aether

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**: anti-exploit technology to prevent malware from leveraging unknown security flaws in software in order to infect computers.
- **Behavior-based protection**: to detect unknown malware.

- **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 Panda Security products:

Cloud management platform

Aether is a cloud-based platform from Panda Security, 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-theroad.

- 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's 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.

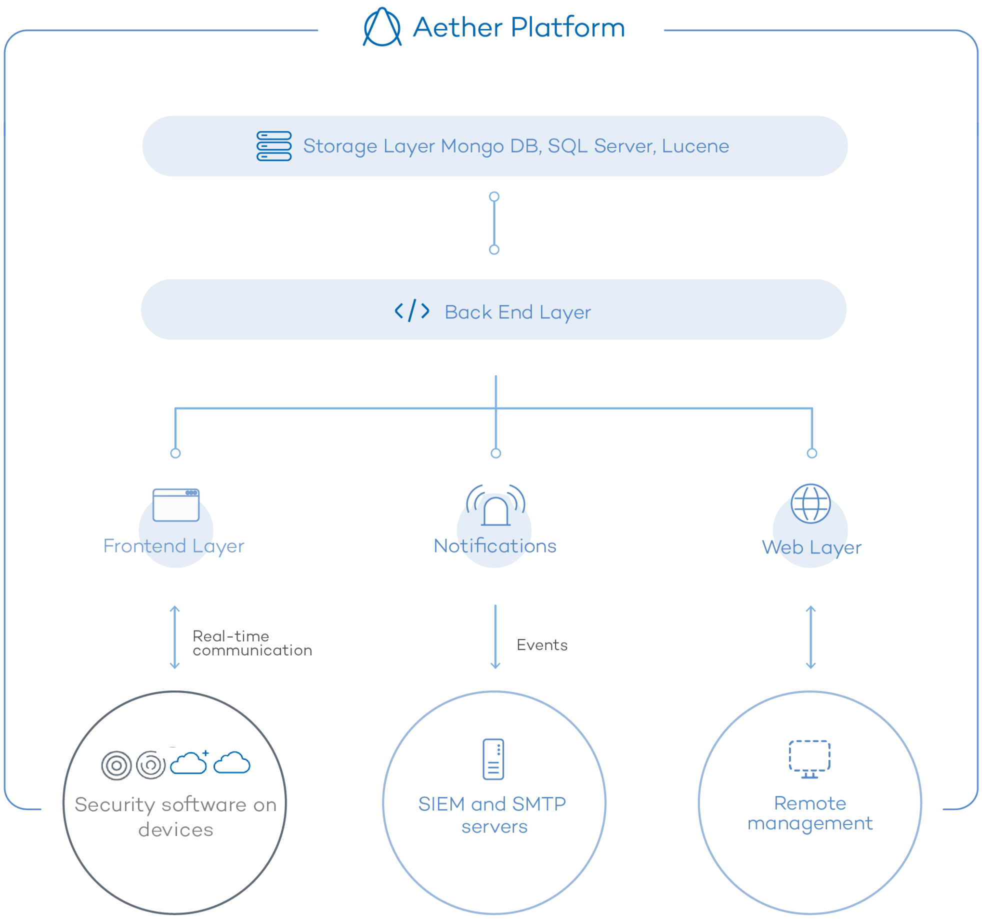


Figure 2.1: logical structure of Aether Platform

Aether on users' computers

Network computers protected by Panda Endpoint Protection on Aether 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.

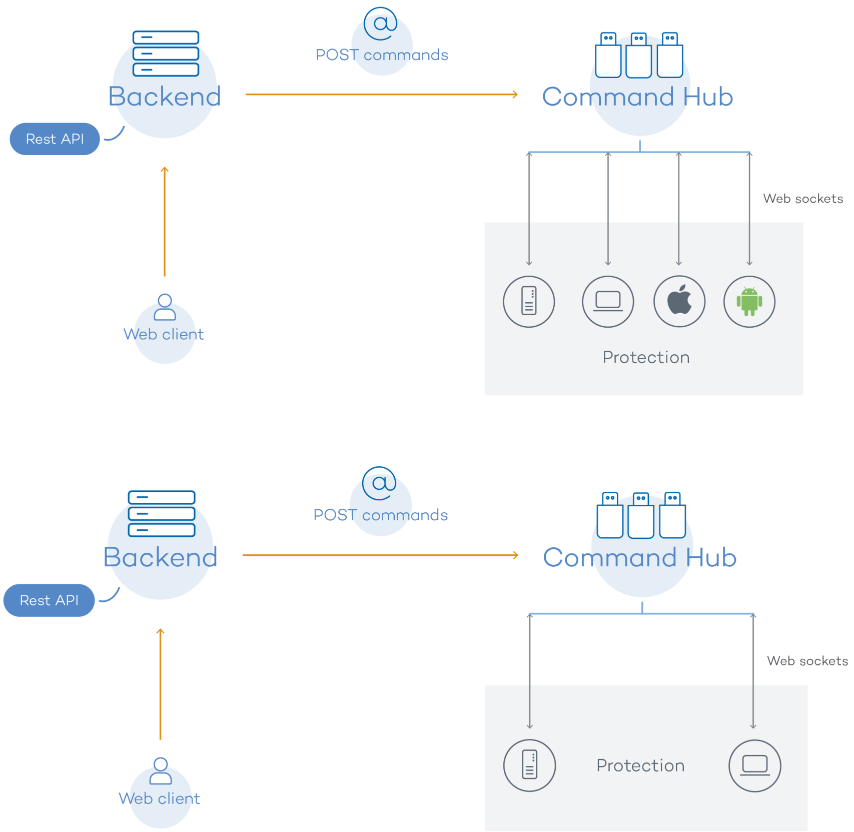


Figure 2.2: flowchart of the commands entered via the management console

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:

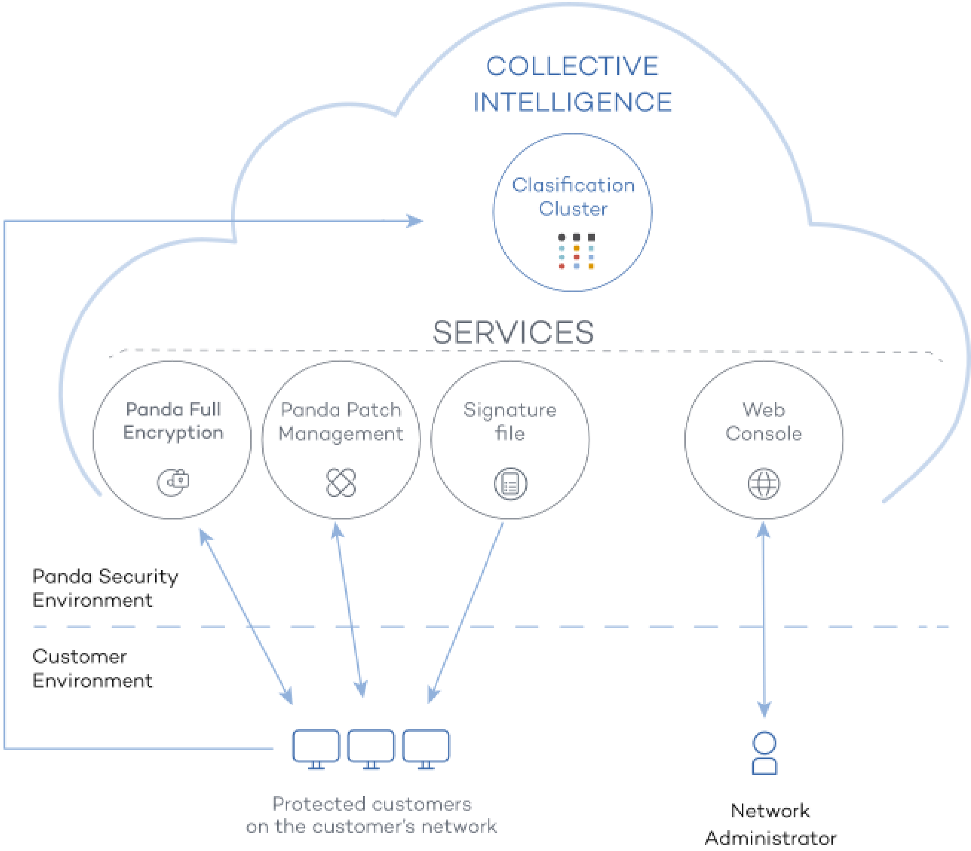


Figure 2.3: Panda Endpoint Protection general structure

- **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

Panda Endpoint Protection is managed entirely through the Web console accessible to administrators from **https://www.pandacloudsecurity.com/PandaLogin/**

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 section "***Web console access***" on page* **310**.

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.

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 leverages the 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 chapter "**Hardware, software and network requirements**" on page **307***

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

- Spanish
- English
- Swedish
- French
- Italian
- German
- Portuguese
- Hungarian
- Russian

- Japanese
- Finnish (local console only)

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 platforms, refer to chapter "***Security settings for workstations and servers***" on page* **181**.

*For more information about Panda Endpoint Protection's antivirus service for Android platforms, refer to chapter "***Security settings for Android devices***" on page* **195**.

Protection against advanced stealth techniques and macro viruses

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 scan the behavior of processes locally.

This allows the solution to detect strange behaviors in the main scripting engines (Visual Basic Script, JavaScript and PowerShell) incorporated into all current Windows systems, and in the malicious macros embedded in Office files (Word, Excel, PowerPoint, etc.).

Finally, 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 provides three basic tools to filter the network traffic that protected computers send and receive:

- **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).

Spam, virus and content filtering for Exchange servers

Panda Endpoint Protection scans Exchange servers for viruses, hacking tools and suspicious/potentially unwanted programs directed to users' mailboxes.

Eliminating junk mail (spam) is a time-consuming task. And not only that, spam is also a frequent source of scams. To tackle this problem, Panda Endpoint Protection provides anti-spam protection for Exchange servers. This feature helps companies improve user productivity and increase the security of the computers on their network.

Panda Endpoint Protection protects Exchange email servers by using two different technologies:

- Mailbox protection.
- Transport protection.

Mailbox protection

This protection is used on Exchange servers with the Mailbox role, and scans folders/mailboxes in the background or when messages are received and stored in users' folders.

The mailbox protection allows manipulation of the items contained in the body of scanned messages. Thus, the protection can replace any dangerous item found with a clean one, move dangerous items to quarantine, etc.

Additionally, the mailbox protection scans the Exchange server user folders in the background, making the most of server idle times. This protection uses smart scans to avoid re-scanning already scanned items. Finally, every time a new signature file is published, the protection scans all mailboxes and the quarantine folder in the background.

Transport protection

This protection is used on Exchange servers with the Client Access, Edge Transport and Mailbox roles, and scans the traffic that goes through the Exchange server.

This protection does not allow manipulation of the items contained in the body of scanned messages. That is, the body of dangerous messages is treated as a single component, and every action taken by Panda Endpoint Protection affects the entire message: delete the message, quarantine it, let it through without taking any action, etc.

Web access control

Panda Endpoint Protection divides websites into 64 categories, enabling administrators to restrict access to them and to any manually entered URL. This protection helps organizations optimize network bandwidth usage and employee productivity, restricting access to non-business related Web content.

Additionally, Panda Endpoint Protection allows administrators to set time restrictions to limit access to certain website categories and blacklisted sites during workhours, or authorize it during non-business hours or weekends.

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.

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 chapter "**Malware and network visibility**" on page **249**.*

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 chapter "**Remediation tools**" on page **289**.*

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 administration 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

The Web console can be accessed from the following link:

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

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 section "***Creating a Panda Account***" on page* **313***.*

- 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 and forensic analysis 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
- 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 section "**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 section "**The Computers area**" on page **124** 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 chapter "**Managing settings**" on page **157** for detailed information on how to create a settings profile in Panda Endpoint Protection.*

Panda Endpoint Protection lets you configure the following aspects of the service:

- **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 chapter "**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 chapter "**Configuring the agent remotely**" on page **173** 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 chapter "**Configuring the agent remotely**" on page **173** 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 section "**Proxy role**" on page **174** 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 section "**Cache/repository role**" on page **175** for more information.
- **Discovery**: globally define the computers responsible for discovering unprotected computers on the network. Refer to section "**Discovery computer role**" on page **176** 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 chapter "**Alerts**" on page **279** for more information.
- **Workstations and servers**: configure settings templates to define how Panda Endpoint Protection will behave to protect the Windows, Linux and macOS computers on your network against threats and malware. Refer to chapter "**Security settings for workstations and servers**" on page **181** 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 chapter "**Security settings for Android devices**" on page **195** for more information.
- **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 chapter "**Panda Patch Management (Updating vulnerable programs)**" on page **197** for more information.
- **Encryption**: configure settings templates to encrypt the content of your computers' internal storage devices. Refer to chapter "**Panda Full Encryption (device encryption)**" on page **225** for more information.

Tasks menu

Lets you schedule security tasks to be run on the day and time specified by the administrator. Refer to chapter "**Tasks**" on page **297** for more information.

General options menu ⚙

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.

Table 4.1: 'General options' menu

Option	Description
Technical Support	Takes you to the Technical Support website for Panda Endpoint Protection on Aether.
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).
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 menu

Displays a drop-down menu with the following options:

Option	Description
Set up my profile	Lets you change the information of the product's main account.
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.

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 section "**Security panels/widgets**" on page **250**.

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.

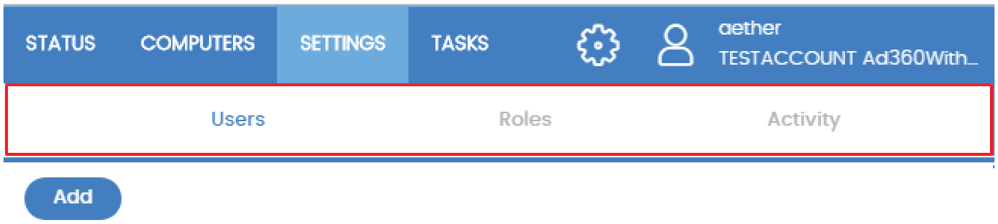


Figure 4.2: tab menu

Action bar

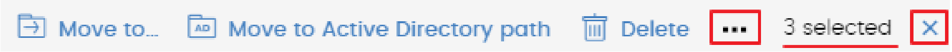


Figure 4.3: Action bar

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.

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.

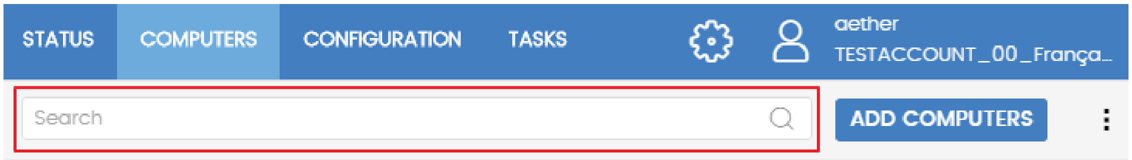
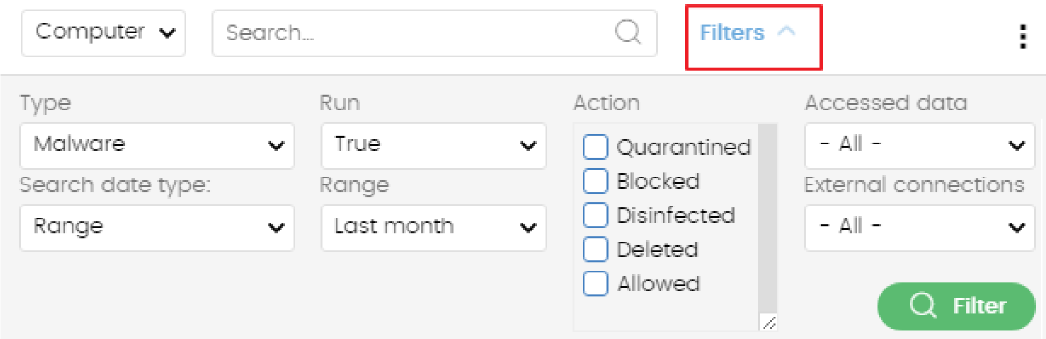


Figure 4.4: search tool

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
Run: True
Search date type: Range
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)**

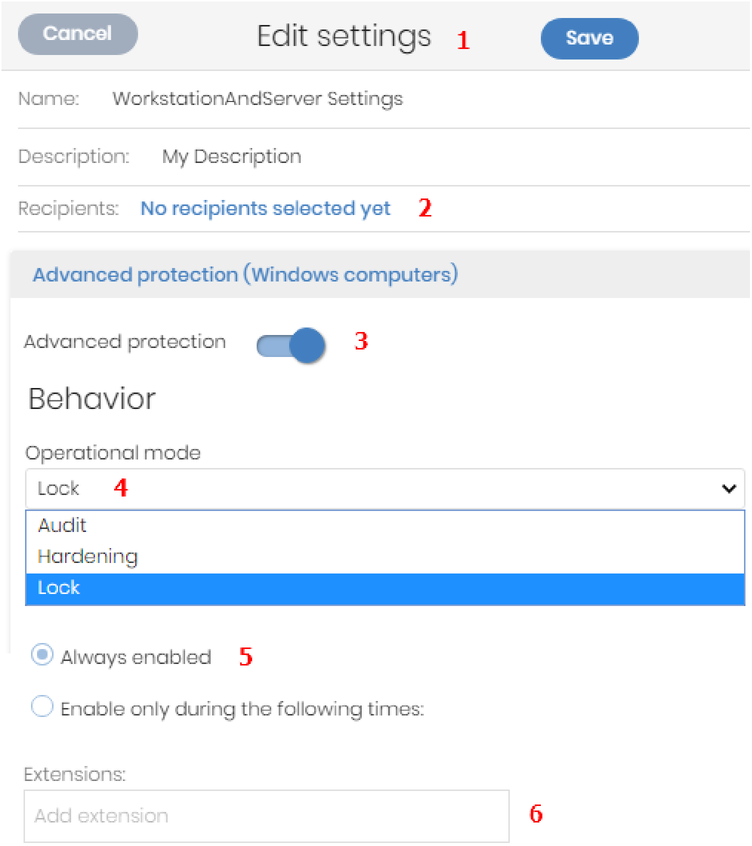

Cancel
Edit settings
1
Save
Name: WorkstationAndServer Settings
Description: My Description
Recipients: No recipients selected yet
2
Advanced protection (Windows computers)
Advanced protection
3
Behavior
Operational mode
Lock
4
Audit
Hardening
Lock
Always enabled
5
Enable only during the following times:
Extensions:
Add extension
6

Figure 4.6: controls for using the management console

Context menus

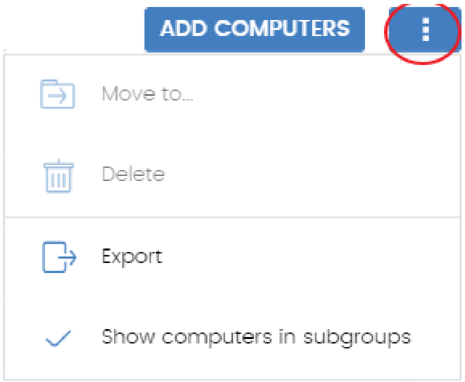
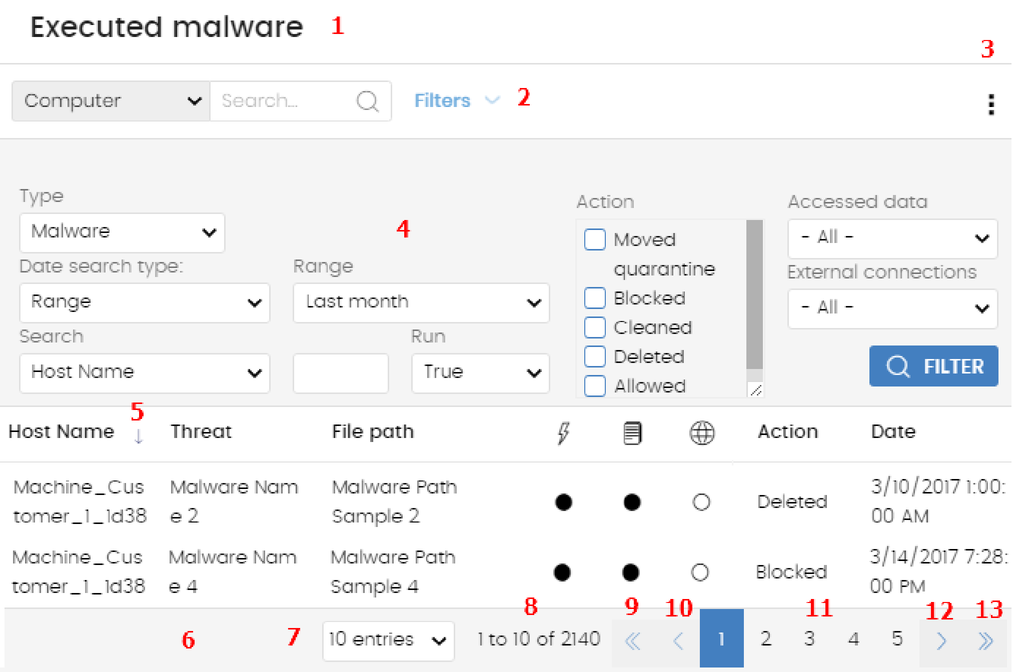


Figure 4.7: context menu

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

Lists

The lists display information in tables along with tools to help with navigation. To view and create lists, click the Status menu at the top of the console. Go the **My lists** section in the side panel and click **Add** to add a new list.



Executed malware

Computer | Search... | Filters

Type: Malware
Date search type: Range
Range: Last month
Search: Host Name
Run: True
Action: □ Moved quarantine □ Blocked □ Cleaned □ Deleted □ Allowed
Accessed data: - All -
External connections: - All -
FILTER

Host Name ↓	Threat	File path	⚡	🗎	🌐	Action	Date
Machine_Customer_1_1d38	Malware Name 2	Malware Path Sample 2	●	●	○	Deleted	3/10/2017 1:00:00 AM
Machine_Customer_1_1d38	Malware Name 4	Malware Path Sample 4	●	●	○	Blocked	3/14/2017 7:28:00 PM

10 entries | 1 to 10 of 2140 | « ‹ 1 2 3 4 5 › »

Figure 4.8: list elements

- **List name (1)**: lets you identify the information on the list.
- **Filtering and search tool link (2)**: click it to display a panel with search and filtering controls.
- **Context menu (3)**: displays a drop-down menu with export options.
- **Filtering and search parameters (4)**: let you refine which data is displayed on the list.
- **Sort order (5)**: change the sort 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 (↑ for ascending and ↓ for descending). If you are accessing the management console from a small-size mobile device, click the icon in the bottom-right corner of the screen to display a menu with the names of the columns included in the table.
- **Pagination (6)**: at the bottom of the table there are pagination tools to help you navigate easier and faster.
  - Rows per page selector **(7)**
  - Number of rows displayed out of the total number of rows **(8)**
  - First page link **(9)**
  - Previous page link **(10)**
  - Links to the next 5 pages **(11)**

- Next page link **(12)**
- Last page link **(13)**

Status area overview

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

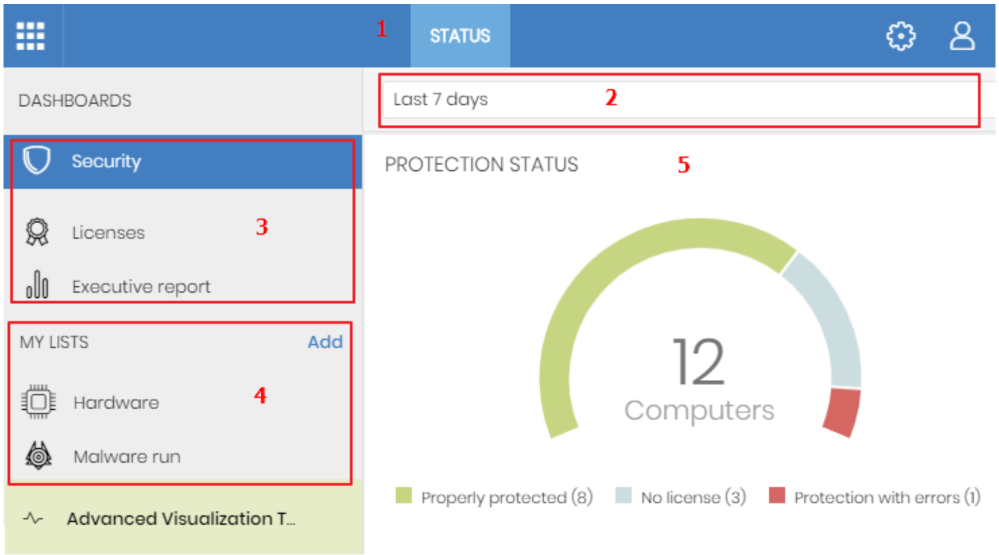


Figure 4.9: Status window (dashboard and access to lists)

- **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 section "**Security panels/widgets**" on page **250**
  - **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 section "**Panda Patch Management widgets and panels**" on page **205**.
  - **Encryption:** encryption status of your computers' internal storage devices. For more information about the widgets in this section, refer to section "**Panda Full Encryption panels and widgets**" on page **235**.
  - **Licenses**: status of the Panda Endpoint Protection licenses assigned to the computers on your network. Refer to chapter **"Licenses**" on page **105** for more information about license management.
  - **Executive report**: refer to chapter **"Reports**" on page **283** 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.

Templates, settings and views

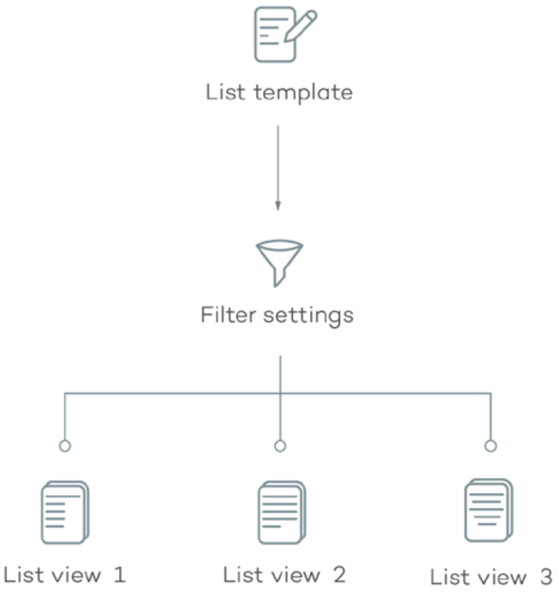


Figure 4.10: generating three lists from a single template/data sour

A list is the sum of two items: a template and a saved search.

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

A search is the specific assignment of values to the filter tools associated with each template.

A search on a template results in a 'list view' or, simply, a 'list'. Administrators can save new lists for later consultation by changing the search associated with a specific template. This avoids having to constantly redefine frequently performed searches, which reduces the time spent by administrators managing security tools.

List templates

Below is a list of the templates available in the solution, grouped by type:

Group	List	Description
General	Licenses	Shows in detail the license status of the computers on your network. Refer to "**'Licenses' list**" on page **111**.
	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 **89**.
	Software	Shows the software installed on the computers on your network. Refer to "**'Software' list**" on page **141**.
	Hardware	Shows the hardware installed on the computers on your network. Refer to "**'Hardware' list**" on page **139**.

Table 4.3: templates available in Panda Endpoint Protection

Group	List	Description
Security	Computer protection status	Shows in detail the protection status of the computers on your network. Refer to “'**Computer protection status' list**” on page **257**.
	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' list**” on page **265**.
	Intrusion attempts blocked	Shows the intrusion attempts blocked by the computer's firewall. Refer to “'**Intrusion attempts blocked' list**” on page **270**.
	Blocked devices	Shows in detail all computers on your network with limitations regarding access to peripherals. Refer to “'**Blocked devices' list**” on page **268**.
Patch management	Patch management status	Shows in detail all computers on the network compatible with Panda Patch Management. Refer to “'**Patch management status' list**” on page **211**.
	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 **210**.
	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' list**” on page **218**.
	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' list**” on page **217**
Data protection	Encryption status	Shows information about the computers on your network compatible with the encryption feature. Refer to “**Encryption Status list**” on page **241**.

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.

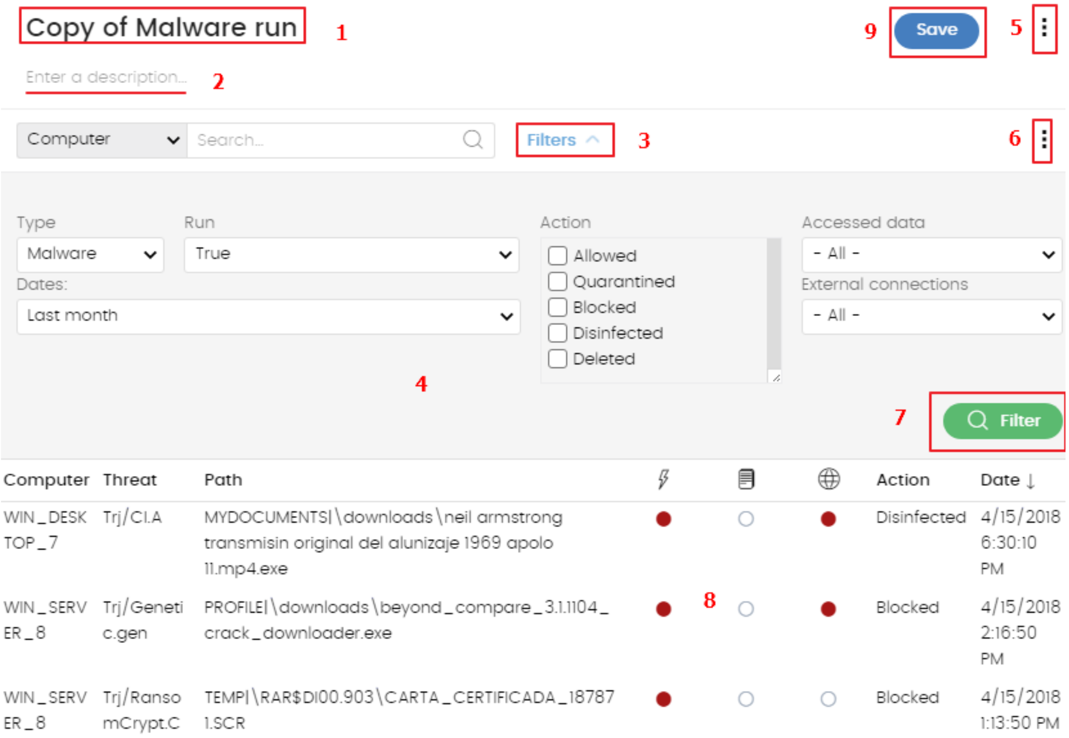
Settings

In the context of lists, the settings represent a data filter specified by the administrator and associated with a template. Each template has different filters according to the type of data displayed.

Administrators can establish as many filter settings for a template as they wish, in order to enable different views pertaining to the same source of data.

List views/Lists

The combination of a template and its settings results in a specific view of the list. A template can have several associated views if the administrator has created various settings for the same template.



Copy of Malware run

Enter a description...

Computer | Search...

Type: Malware

Run: True

Dates: Last month

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

Accessed data: - All -

External connections: - All -

Computer	Threat	Path				Action	Date ↓
WIN_DESKTOP_7	Trj/CI.A	MYDOCUMENTS|\downloads\neil armstrong transmisin original del alunizaje 1969 apolo 11.mp4.exe	●	○	●	Disinfected	4/15/2018 6:30:10 PM
WIN_SERVER_8	Trj/Genetic.gen	PROFILE|\downloads\beyond_compare_3.1.1104_crack_downloader.exe	●	○	●	Blocked	4/15/2018 2:16:50 PM
WIN_SERVER_8	Trj/RansomCrypt.C	TEMP|\RAR$DI00.903\CARTA_CERTIFICADA_18787 1.SCR	●	○	○	Blocked	4/15/2018 1:13:50 PM

Figure 4.11: overview of a list

My lists panel

All created lists are displayed on the left-hand side panel **My lists** of the **Status** main screen.

Creating a custom list

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

- **From the My lists side menu**

Click **Add** from the panel on the left to display a window showing all available templates.

- **From a dashboard panel**

  - Click a widget on the dashboard to open its associated template.
  - Click its context menu **(6)** and select **Copy**. A new list will be created.
  - Edit the list filters, name and description and click **Save (9)**.

- **From an existing list**

  - You can copy an existing list by clicking its context menu **(6)** and then clicking **Copy**.

- **From the context menu of 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.

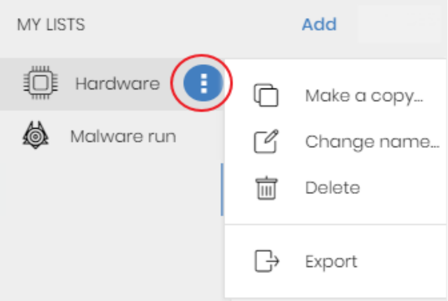


Figure 4.12: context menu of the lists accessible from the 'My lists' panel

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 **(6)**.
  - 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 **(6).**
  - Click the ⧉ icon from the drop-down menu displayed.

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 **(3)** to display the filter options.
- Configure the filter **(4)** according to your needs.
- Click **Filter (7)** to apply the configured filter and check if it meets your needs. The list **(8)** will display the search results.
- Click **Save (9)**. The list will be added to the panel on the left under **My lists**, and will be accessible by clicking on its name.

Additionally, the context menu button **(6)** provides the option to export the list to CSV format and to make a copy of the list.

> *The file generated when exporting a list to CSV format adds additional fields with respect to the list displayed in the Web console. These fields are documented later in this guide for each list.*

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 section "**'Computer protection status' list**" on page **257** 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 section "**'Computer protection status' list**" on page **257** for more information.

Software

Shows a list of the programs installed across your network. Refer to section "**'Software' list**" on page **141** for more information.

Hardware

Shows a list of the hardware components installed across your network. Refer to section "**'Hardware' list**" on page **139** for more information.

Chapter 5

Controlling and monitoring the management console

This chapter describes the resources implemented in Panda Endpoint Protection 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.

> *Unlike the rest of this guide, where the word "user" refers to the person that uses a computer or device, in this chapter "user" refers to the 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.

Main user

The main user is the user account provided by Panda Security to the customer when provisioning the Panda Endpoint Protection service. It has the **Full Control** role, which is explained in section "**Full Control role**".

The settings of the main user cannot be edited or deleted.

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 may be assigned to a technician specialized in the relevant field. For example, file servers may be assigned to a group of specialized technicians, and other systems, such as Android devices, may 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 predefined. The default administration account belongs to this role, and with this it is possible to take almost all actions that are available in the console.

The **Full Control** role cannot be deleted, edited or viewed, and any user account can belong to this role if it is assigned through the console.

Read-only role

The Read-only role is especially designed for network administrators responsible for monitoring networks, but without sufficient permissions to take actions such as editing settings or launching on-demand scans.

The permissions enabled in the Read-only role are as follows:

- View security settings for workstations and servers.
- View security settings for Android devices.
- View computer encryption settings.
- View patch management settings.
- View detections and threats.
- Access to reports.

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.

The Panda Endpoint Protection permissions are as follows:

- **Users**
  - Manage users and roles.
- **Licenses**

  - Assign licenses.
- **Computers**
  - Modify computer tree.
  - Add, discover and delete computers.
  - Modify network settings (proxies and cache).
  - Configure per-computer settings (updates, passwords, etc.).
  - Restart computers.
- **Security**
  - Configure security for workstations and servers.
  - View security settings for workstations and servers.
  - Configure security for Android devices.
  - View security settings for Android devices.
  - Use the anti-theft protection for Android devices (locate, wipe, lock, etc.)
  - View detections and threats.
  - Launch scans and disinfect.
  - Exclude threats temporarily (malware, PUPs and blocked items).
  - Configure patch management.
  - Install and uninstall patches.
  - View available patches.
- **Data protection**
  - Configure computer encryption.
  - Access recovery keys for encrypted drives.

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**: due to the inheritance rules, making changes to the computer tree may modify the affected computers' settings. If any of the permissions that allow administrators to change settings is disabled, they will only be permitted to create groups, delete empty groups and rename groups. The permissions that allow administrators to change settings are:
  - Modify network settings (proxies and cache).
  - Configure per-computer settings (updates, passwords, etc.).
  - Configure security for workstations and servers.
  - Configure security for Android devices.
  - Launch scan and disinfect
  - Configure patch management
  - Install and uninstall patches
- **Disabled:** the account user can view the group tree and the settings assigned to each group, but cannot create new groups or move computers. They will still be able to change the settings assigned to a group, as this action is governed by the following permissions: **Configure security for workstations and servers**, **Configure security for Android devices**, **Configure patch management**, **Configure computer encryption**.

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 **Proxy and language** settings, edit or delete existing ones and assign them to computers in the console.
- **Disabled**: the account user cannot create new **Proxy and language** settings, nor delete existing

ones. Neither can they change the computers these settings are assigned to..

> *Since moving a computer in the group tree can change the Proxy and language settings assigned to it, if you want to disable the Configure proxies and language permission you will also have to disable the Modify computer tree permission.*

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.

> *Since moving a computer in the group tree can change the Per-computer settings assigned to it, if you want to disable the Modify per-computer settings permission you will also have to disable the Modify computer tree permission.*

Restart computers

- **Enabled**: the account user can restart computers by going to the **Computers** menu at the top of the console and selecting **Restart** from the context menu (for Windows, Linux and macOS workstations and servers).
- **Disabled**: the account user cannot restart computers.

Configure security for workstations and servers

> *Since moving a computer in the group tree can change the Workstation and server settings assigned to it, if you want to disable the Configure security for workstations and servers permission you will also have to disable the Modify computer tree permission.*

- **Enabled**: the account user can create, edit, delete and assign security settings for Windows, Linux and macOS workstations 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.

> *Since moving a computer in the group tree can change the Android device settings assigned to it, if you want to disable the Configure security for Android devices permission you will also have to disable the Modify computer tree permission.*

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 taskt

- **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.

Since moving a computer in the Groups tree can change the Patch management settings assigned to it, if you want to disable the Configure patch management permission you will also have to disable the Modify computer tree permission.

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 patches

Since moving a computer in the Groups tree can change the Patch installation/ uninstallation settings assigned to it, if you want to disable the Install/uninstall patches permission you will also have to disable the Modify computer tree permission.

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

View available patches

This permission is only accessible when you disable the Install 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.

Since moving a computer in the group tree can change the encryption settings assigned to it, if you want to disable the Configure computer encryption permission you will also have to disable the Modify computer tree permission.

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

- 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.

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.

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 **5.4**
Item type	Type of console object the action was performed on.	Refer to table **5.4**
Item	Console object the action was performed on.	Refer to table **5.4**

Table 5.1: 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
Actions	Type of action carried out.	Refer to table **5.4**
Item type	Type of console object the action was performed on.	Refer to table **5.4**
Item	Console object the action was performed on.	Refer to table **5.4**

Table 5.2: 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 5.3: 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.
Settings - Proxy and language	Create	Name of the settings the action was performed on.

Table 5.4: 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 - 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.
	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
Computer	Delete	Name of the device the action was performed on.
	Edit name	Name of the device the action was performed on.

Table 5.4: item types and actions

Item type	Action	Item
	Edit description	Name of the device the action was performed on.
	Change group	Name of the device the action was performed on.
	Assign 'Proxy and language' settings	Name of the device the action was performed on.
	Inherit 'Proxy and language' 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.
	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.

Table 5.4: item types and actions

Item type	Action	Item
	Designate as 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.
	Uninstall	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.

Table 5.4: item types and actions

Item type	Action	Item
	Assign 'Proxy and language' settings	Name of the group the action was performed on.
	Inherit 'Proxy and language' 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.
	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	
Executive report	Add scheduled report	Name of the scheduled report the action was performed on.
	Edit scheduled report	Name of the scheduled report the action was performed on.
	Delete scheduled report	Name of the scheduled report the action was performed on.
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.

Table 5.4: item types and actions

Item type	Action	Item
	Stop excluding for all computers	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 S.L. team	Edit	
Access permission for resellers	Edit	
Email sending option (reseller)	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.

Table 5.4: item types and actions

Item type	Action	Item
	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.
	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 5.4: item types and actions

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

Table 5.5: fields in the 'Sessions' list

Field	Description	Values
IP address	IP address from which the console was accessed.	Character string

Table 5.5: 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 5.6: 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 5.7: filters available in the 'Sessions' list

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 **5.11**

- **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 **5.11**
Type	Type of object the action was performed on.	Refer to table **5.11**
Item	Console object the action was performed on.	Refer to table **5.11**

Table 5.8: 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 **5.11**
Type	Type of object the action was performed on.	Refer to table **5.11**
Item	Console object the action was performed on.	Refer to table **5.11**

Table 5.9: 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 5.10: 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.

Table 5.11: item types and actions

Part 3

Deployment and getting started

Chapter 6: Installing the client software

Chapter 7: Licenses

Chapter 8: Updating the client software

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 help administrators install the protection. These tools are discussed later in this chapter.

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**" on page **86**.

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.

Determine whether a restart will be necessary to finish the installation process

Computers with no protection installed won't need to be restarted to install the protection services provided by Panda Endpoint Protection.

> *With older versions of Citrix it may be necessary to restart the computer or there may be a micro-interruption of the connection.*

If you want to install Panda Endpoint Protection on a computer that already has an antivirus solution from another vendor, you can choose between installing our product without uninstalling the current protection so that both products coexist on the computer, or uninstalling the other solution and working exclusively with Panda Endpoint Protection.

> *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.

> *For a list of the antivirus solutions that* Panda Endpoint Protection *can automatically uninstall, refer to chapter "***Supported uninstallers***" on page* **315***. If the solution that needs to be needs to be uninstalled is not on the list, it will have to be removed manually.*

This behavior can be changed both for trial and commercial versions. Go to **Settings**, and define a configuration for workstation and servers that has the **Uninstall other security products** option enabled.

*Refer to section "**Uninstall other security products**" on page **183** for more information on how to define this behavior. Refer to section "**Manual and automatic assignment of settings**" on page **165** 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 on Aether	Restart
None	Trial or commercial	NO
Panda Endpoint Protection Legacy, Panda Endpoint Protection Plus Legacy	Commercial version	LIKELY (only if a protection upgrade is required)
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 whether it will be necessary to install the protection during non-working hours

In addition to the restart considerations covered before, installing Panda Endpoint Protection causes a micro-interruption (less than 4 seconds) in the connections established by the programs running on the target computer. All applications that do not incorporate security mechanisms to detect connection interruptions will need a restart. If a restart is not possible and there is the possibility that some applications may not work properly after the micro-interruption, it is advisable to install the Panda Endpoint Protection software outside office hours.

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 appropriate proxy and language settings. This must be selected upon generating the installer. Refer to section “**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 proxy and language 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 chapter “**Hardware, software and network requirements**” on page* **307***.*

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.
  - **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.
  - **Supported kernel**: up to version 4.10 (64-bit). Refer to our support website (**https://www.pandasecurity.com/uk/support/card?id=700009**) for more information about the last Linux kernel version supported by Panda Endpoint Protection. Any later versions won't be supported.
  - **Free space for installation**: 100 MB.
  - **Ports**: ports 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware to work.

- **Android**
  - **Operating systems**: Android 4.0 or 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 section "**Access to service URLs**" on page **311**

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:

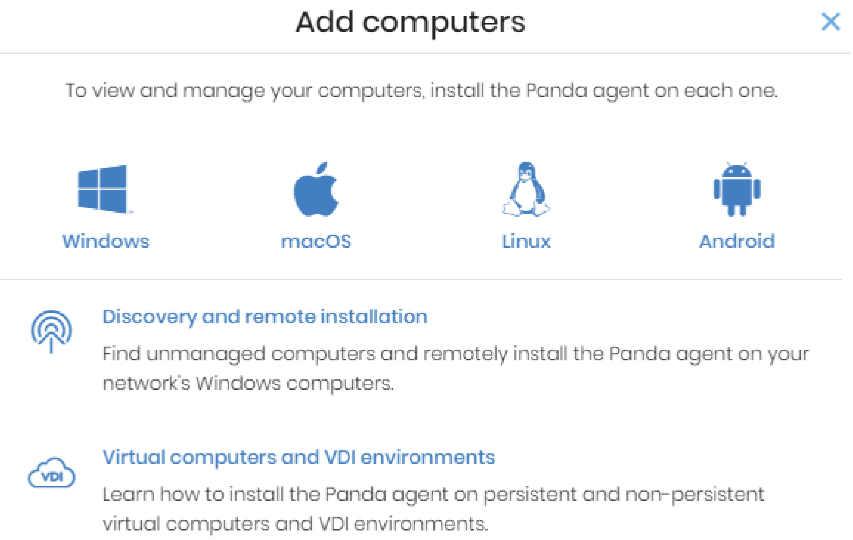
- Downloading the installation package from the Web console.
- Generating a download URL.
- Manually installing the client software.

Downloading the installation package from the Web console

*For more information on how to assign settings to computers, refer to section "**Manual and automatic assignment of settings**" on page **165**.*

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.



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.

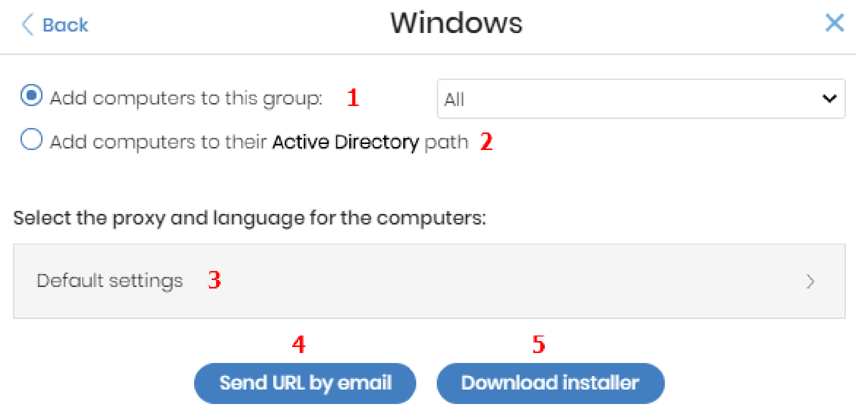
Figure 6.1: window for selecting a platform compatible with Panda Endpoint Protection

- 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 section "**Group types**" on page **130**.

Next, select the proxy and language settings **(3)** to be applied to the computer. For more information on how to create new proxy and language settings, refer to section "**Configuring Internet access via a proxy server**" on page **176** and section "**Configuring the agent language**" on page **178**.

- 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 proxy and language 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 proxy and language for 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.

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 section “**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 and macOS platforms

To run the downloaded installer, double-click its icon and follow the instructions in the installation wizard. The product will then verify that it has the latest version of the signature file and the protection engine. If it does not have it, it will update automatically.

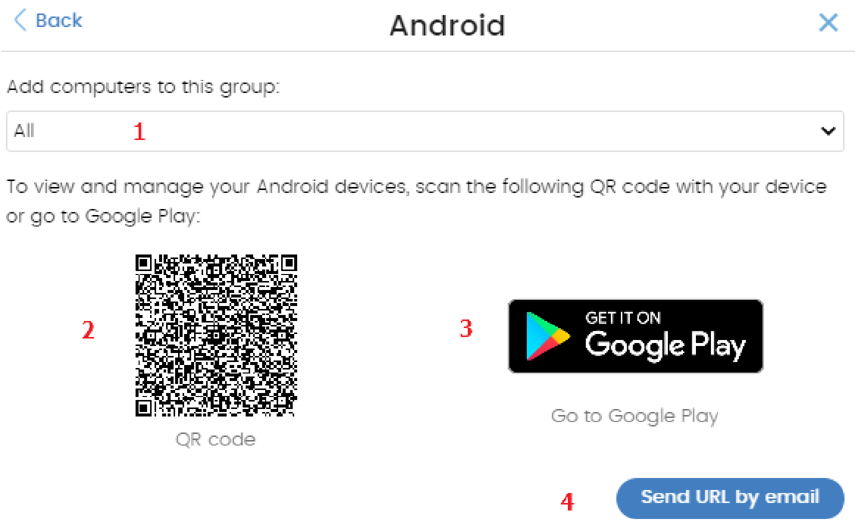
Installing the software on Linux platforms

To run the downloaded script, open a terminal session in the folder with the installation package and run the following command:

```
sudo sh "package_name"
```

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 settings** 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 settings**, **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.
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 settings** 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.
  - **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 settings** 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 settings** 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**

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 6.4 for a description of all possible errors.
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 indicates **Installation error**, a text string will be shown with a brief explanation of the error.

Error message in the Status field	Cause/Solution
Wrong credentials	Enter credentials with sufficient permissions to install the agent.
Unable to connect to the computer	• The computer is turned off. • The firewall is preventing the connection. • The computer's operating system is not supported.
Unable to download the agent installer	• The downloaded package is corrupted. • There is no installation package for the operating system of the workstation/server. • There is not enough free space on the computer to download the agent package. • The agent package download was very slow and has been canceled.
Unable to copy the agent	There is not enough free space on the computer to copy the agent package.
Unable to install the agent	• There is not enough free space on the computer to install the agent. • An agent is already installed on the computer. If both agents are the same version, the installation will be launched in repair mode.
Unable to register the agent	• The computer must be restarted before the agent can be uninstalled. • Another Aether-based product is already installed on the remote computer.

Table 6.4: installation process error messages

- **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. • **Installing**: the installation process is in progress. • **Installation error**: message specifying the type of error. Refer to table 6.4 for a description of all possible errors.
Error	Error description.	For more information, refer to table 6.4
Installation error date	Date and time when the error took place.	Date

Table 6.5: 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 6.6: filters available in the 'Unmanaged computers discovered' list

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:

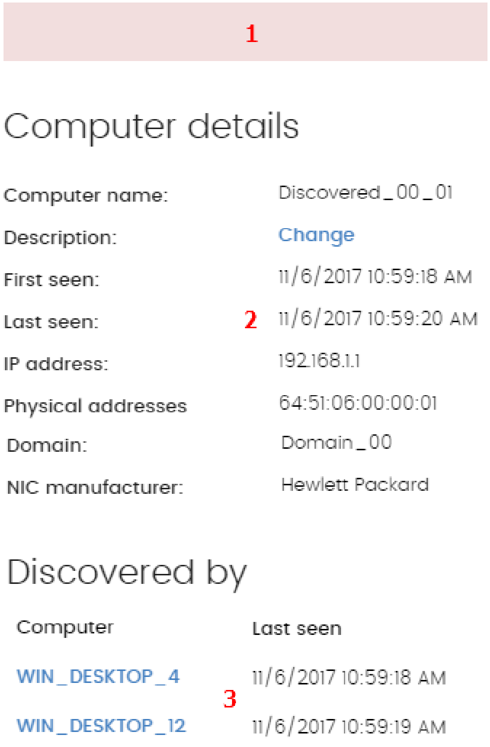
- From the **Unmanaged computers discovered** list, select **Discovered** or **Hidden** depending on the status of the computers you want to delete.
- Select the checkboxes next to the computers to delete.
  - To delete multiple computers simultaneously, click the general context menu and select **Delete**.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

Computer name:	Discovered_00_01
Description:	Change
First seen:	11/6/2017 10:59:18 AM
Last seen:	11/6/2017 10:59:20 AM
IP address:	192.168.1.1
Physical addresses	64:51:06:00:00:01
Domain:	Domain_00
NIC manufacturer:	Hewlett Packard

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.
	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.

Table 6.7: 'Computer alerts' section

Status	Type	Solution
	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 section "**Hardware requirements**" on page **308** 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 chapter "**Supported uninstallers**" on page **315** 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 **307**.	

Table 6.7: '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.
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 6.8: '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 6.9: '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:

- **IGNORE_LEGACY_AGENT=[TRUE|FALSE]**: keeps the Panda Endpoint Protection agent of the traditional platform (legacy) product if already installed. The default value is FALSE; if the legacy product's agent is already installed on the computer the installation process is interrupted.
- **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"
IGNORE_LEGACY_AGENT=TRUE
```

Deploying the agent from Panda Systems Management

Panda Systems 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 don't have any specific requirements besides those indicated for Panda Systems Management and Panda Endpoint Protection on Aether.

Component size:

- Panda Endpoint Protection on Aether 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 on Aether 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

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).

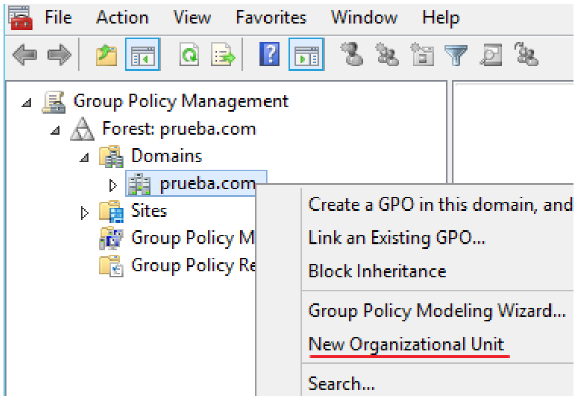


Figure 6.5: new Organizational Unit

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".

• Right-click the newly created Organizational Unit and select Block Inheritance.

3. Create a new GPO with the installation package

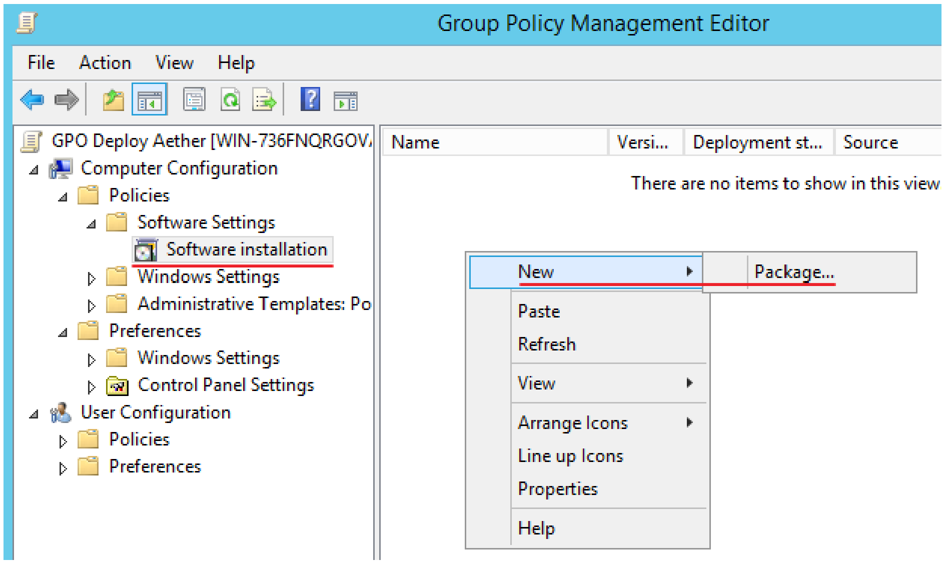


Figure 6.6: new installation package

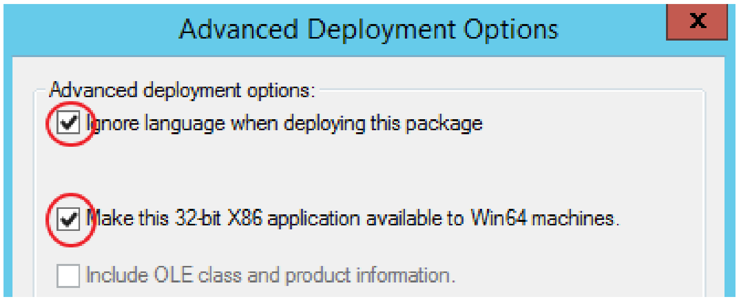
- Right-click the newly created Organizational Unit and select the option Create a GPO in this domain. Name the GPO (in this case, "Aether deployment GPO").

- 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

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 chapter "**Managing settings**" on page **157** and chapter "**Updating the client software**" on page **117** 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.

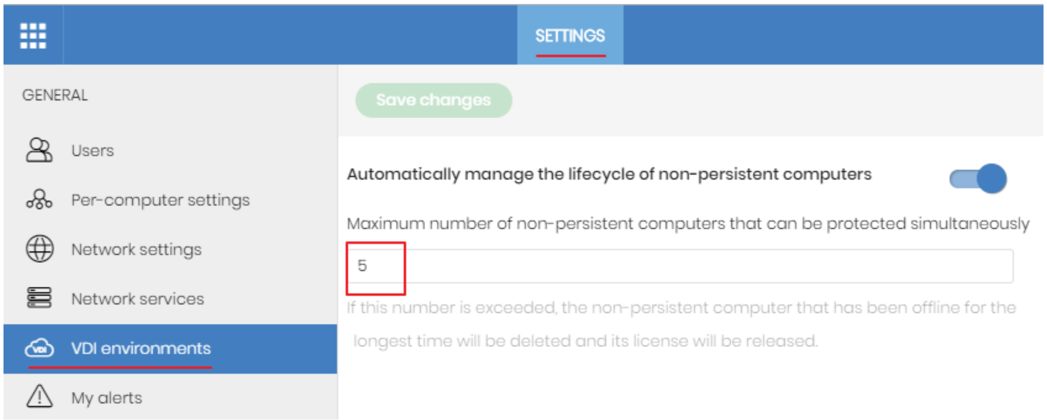
Preparing the gold image

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**" on page **82.**
- .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 chapter "**Managing**

settings" on page **157** and chapter "**Updating the client software**" on page **117** 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

If this number is exceeded, the non-persistent computer that has been offline for the longest time will be deleted and its license will be released.

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.

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 section "**Setting up the password**" on page **179** 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:**

On Linux, use the desktop environment to manage the packages included in the distribution.

- Fedora: Activities > Software > Installed
- Ubuntu: Ubuntu software> Installed

We recommend using the command line to uninstall the product:

- **Ubuntu**
  - Agent: `sudo dpkg -r management-agent`
  - Kernel: `sudo dpkg -r protection-agent-dkms`
  - Protection: `sudo dpkg -r protection-agent-corporate`
- **Fedora** (replace "version" with the package build by pressing the TAB key)
  - Agent: `sudo dnf remove management-agent-"version"`
  - Kernel: `sudo dnf remove protection-agent-dkms-"version"`
  - Protection: `sudo dnf remove protection-agent-corporate-"version"`

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

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

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.

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 (workstation, mobile device or server).

This chapter explains how to manage your Panda Endpoint Protection licenses: 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, Patch Management.
- **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 chapter “**Managing computers and devices**” on page **123** 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.

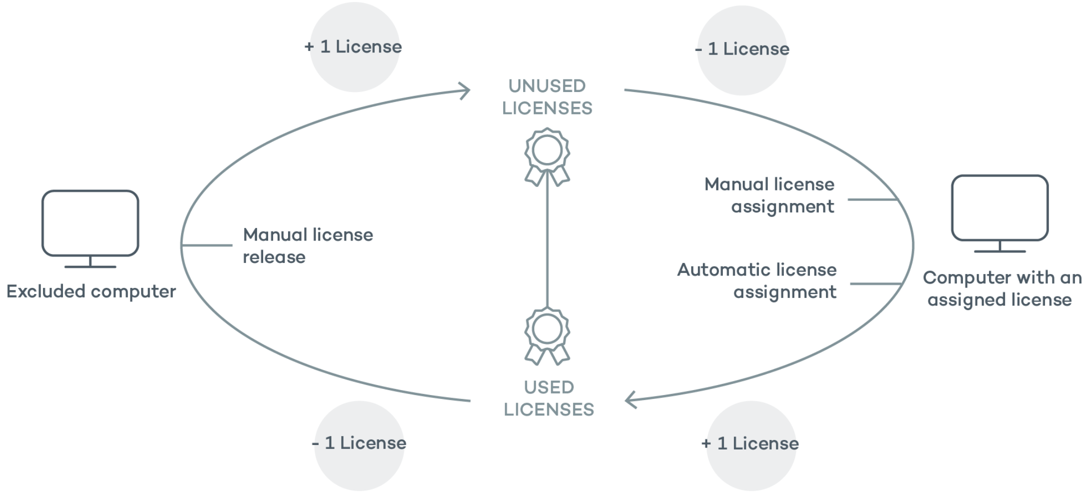


Table 7.1: modification of license groups with excluded computers and those with licenses assigned

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.

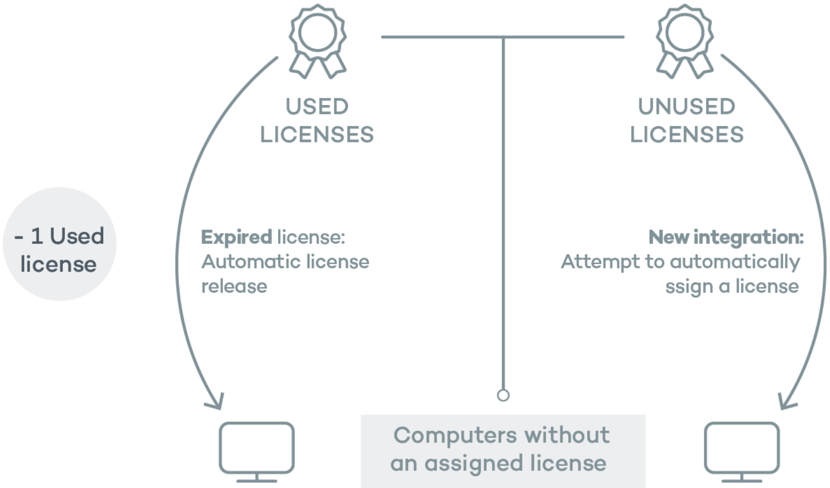

USED LICENSES
UNUSED LICENSES
- 1 Used license
Expired license: Automatic license release
New integration: Attempt to automatically ssign a license
Computers without an assigned license

Figure 7.1: 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

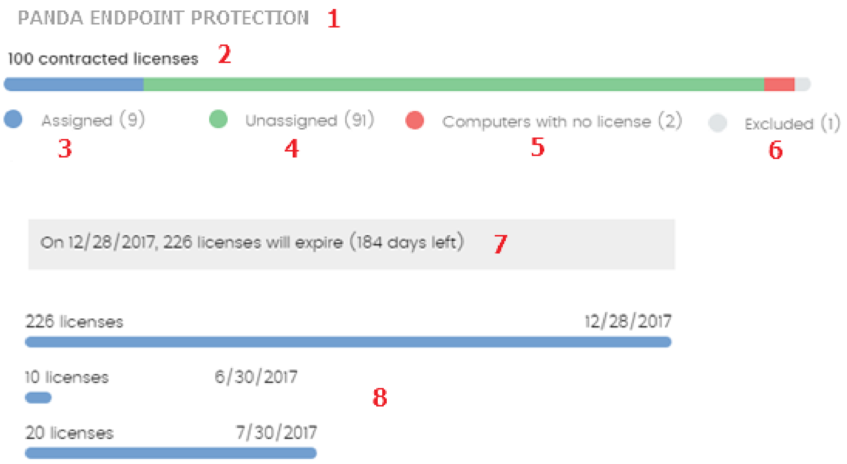
Similarly, when an assigned license expires, a computer on the network will have the **No license** status in accordance with the license expiration process explained in section "**Withdrawal of expired licenses**".

Viewing contracted licenses

To view details of contracted licenses, click the **Status** tab at the top of the console and then Licenses in the side menu. You will see a window with two graphs (widgets): **Contracted licenses** and **License expiration**.

Widget

The panel shows how the contracted product licenses are distributed.



On 12/28/2017, 226 licenses will expire (184 days left)

Figure 7.2: : license panel with three license contracts

Hotspot	Description
Name of the contracted product (1)	Specifies the products and services contracted. Each product is shown separately. If the same product has been contracted several times (several license contracts of one product) they will be shown together, indicating the different expiration dates of the licenses in a horizontal bar chart.
Total number of contracted licenses (2)	This represents the maximum number of computers that can be protected if all the contracted licenses are assigned.
Number of assigned licenses (3)	This is the number of computers protected with an assigned license.
Number of unassigned licenses (4)	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 (5)	Computers that are not protected as there are insufficient licenses. Licenses will be assigned automatically once they are bought.

Table 7.2: fields in the 'Licenses' panel

Hotspot	Description
Number of excluded computers (6)	Computers without a license assigned and that are not eligible to have a license.
License expiration date (7)	If there is only one license contract, all licenses will expire at the same time, on the specified date.
License contract expiration dates (8)	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 7.2: fields in the 'Licenses' panel

'Licenses' list

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

To access the **Licenses** list, click the **Status** tab. Then click **Add** from the **My lists** menu on the left, or click the widget accessible from the **Licenses** section**.**

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 • Mobile device • Server
Computer	Computer name.	Character string

Table 7.4: fields in the 'Licenses' exported file

Field	Description	Values
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
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

Table 7.5: filters available in the 'Licenses' list

Field	Description	Values
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 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

- **Lists accessible from the panel**

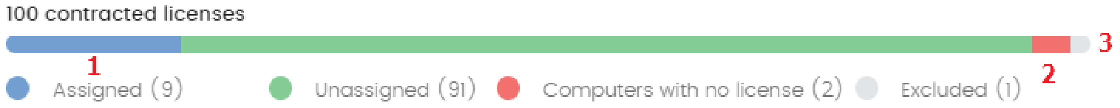


Figure 7.3: hotspots in the 'Contracted licenses' panel

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 7.6: filters available in the 'Contracted licenses' panel

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 section "***Manual and automatic assignment of settings***" on page* **165** *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 section "***Creating and organizing filters***" on page* **127** *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 7.7: fields in the 'Licenses' filter

Chapter 8

Updating the client software

Panda Endpoint Protection is a cloud-based managed service that doesn't require customers to update the back-end infrastructure that supports the protection service. However, it is necessary to update the client software installed on the computers on the network.

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 for the traditional antivirus protection.

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 Protectionprotec-tion	Configurable	Configurable	Configurable	No

Table 8.1: update procedures based on the client software component

Module	Platform			
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 (workstation, server, or Android device).

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.

Part 4

Managing network security and devices

Chapter 9: Managing computers and devices

Chapter 10: Managing settings

Chapter 11: Configuring the agent remotely

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 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.

CONTENIDO DEL CAPÍTULO

The Computers area

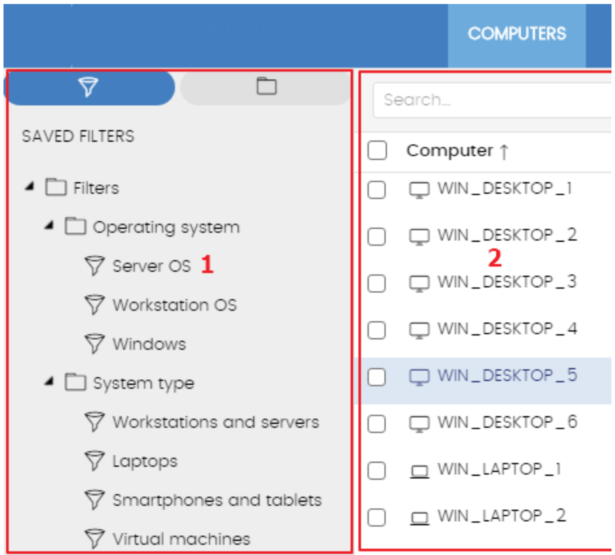


Figure 9.1: general view of the panels in the Computers area

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

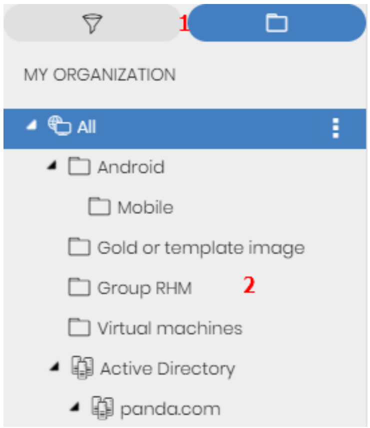


Figure 9.2: the Computers tree panel

Panda Endpoint Protection displays the computers on the network through the **Computer tree (1)**, which provides two independent views or trees **(2)**:

- **Filter tree** ▽: 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** □: 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 computers and Android 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 chapter "**Malware and network visibility**" on page **249**. For more information on how to assign security settings profiles, refer to section "**Manual and automatic assignment of settings**" on page **165**. For more information on how to take remediation actions, refer to chapter "**Remediation tools**" on page **289**.*

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.

Table 9.1: predefined filter list

Name	Group	Description
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 section "**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

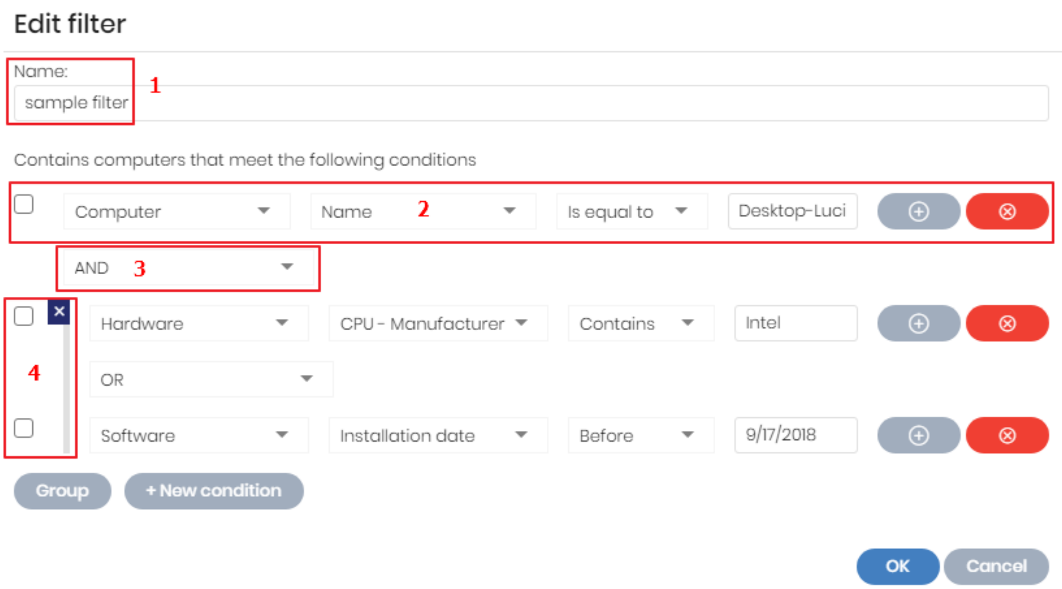
- Click the context menu of the branch to rename.
- Click **Rename**.
- Enter the new name.

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.

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.*

Group types

Group type	Description
Root group	This is the parent group from which all other folders derive.

Table 9.2: group types in Panda Endpoint Protection

Group type	Description
Native groups	These are the Panda Endpoint Protection standard groups. They support all operations (move, rename, delete, etc.) and 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 underlying Active Directory structure is also changed. These changes will be replicated in the Panda Endpoint Protection Web console within 15 minutes.

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 groups

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

It is not possible to create Active Directory groups in the group tree. The solution only replicates the groups and organizational units that already exist on your organization's Active Directory server.

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.

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

Any computer found in an Active Directory group can be moved to a standard group, but not to another Active Directory group.

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.

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 section "**Scan options**" on page **293**.*

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

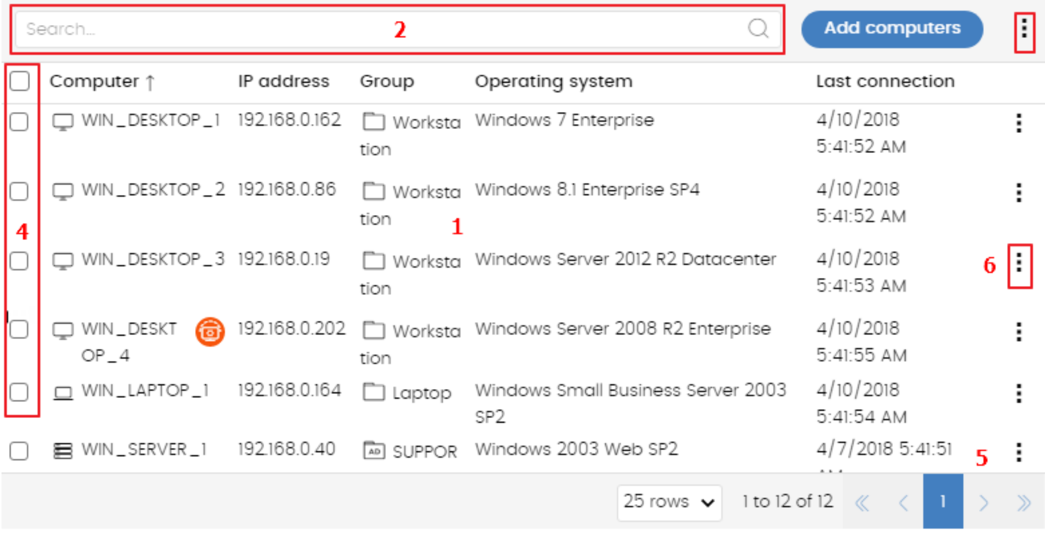
The Computer list panel

The Computer list panel 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.

Follow the steps below to display the Computer list panel:

- 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 panel on the left (group tree or filter tree). The panel on the right will show 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 9.4: the Computer list panel

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

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

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.

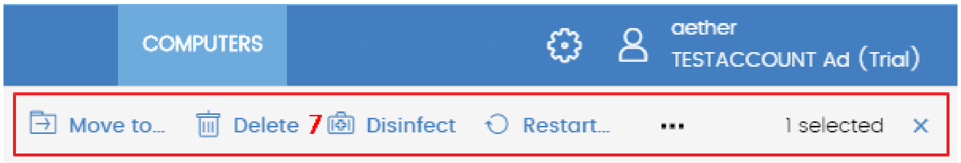


Figure 9.5: action bar

Click the checkbox in the header row **(4)** to select all computers on the current page of the list. The **Select all xx rows in the list** option will be displayed, which allows you select all computers on the list regardless of the page you are on.

‘Computers’ list

You will see the following details for each computer:

Field	Description	Values
Computer	Computer name and type.	Character string • Desktop computer (Windows, Linux or macOS workstation or server). • Laptop. • Mobile device (Android smartphone or tablet).
IP address	The computer's primary IP address.	Character string • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated.
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs, and its type.	Character string • 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

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string

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

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Computer name.	Character string
IP addresses	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
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

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

Field	Description	Values
Proxy and language	Name of the proxy and language settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the proxy and language 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
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

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

Select the checkbox next to a computer **(4)** to display an action bar showing the management actions you can take on that device:

Action	Description
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 section “**Creating and managing settings**” on page **164**
Move to Active Directory path	Moves the selected computer to the group that corresponds to its organizational unit in the organization's Active Directory.

Table 9.6: computer management tools

Action	Description
Delete	Deletes the computer from the console and uninstalls the Panda Endpoint Protection client software from it. Refer to section "**Uninstalling the software**" on page **102** for more information.
Scan now	Refer to section "**On-demand computer scanning and disinfection**" on page **290** for a full description of scan tasks.
Schedule scan	Refer to section "**On-demand computer scanning and disinfection**" on page **290** for a full description of scan tasks
Restart	Restarts the computer. "**Computer restart**" on page **294** for more information.
Schedule patch installation	Refer to chapter "**Panda Patch Management (Updating vulnerable programs)**" on page **197** for more information on how to install patches on Windows computers
✕ selected	Undoes the current selection.

Table 9.6: computer management tools

My lists panel

Go to the **Status** menu at the top of the console, and click **My lists** from the side panel. This will display a window with all available lists. Refer to section "**Managing lists**" on page **46** for more information about the different types of lists and how to work with them.

'Hardware' list

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 • Desktop computer (Windows, Linux or macOS 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

Table 9.7: fields in the 'Hardware' list

Field	Description	Values
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 section "**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 • Mobile device • 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	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

Table 9.8: fields in the 'Hardware' exported file

Field	Description	Values
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

- **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' list

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

Table 9.10: fields in the 'Software' list

Field	Description	Values
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
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

- **Filter tool**

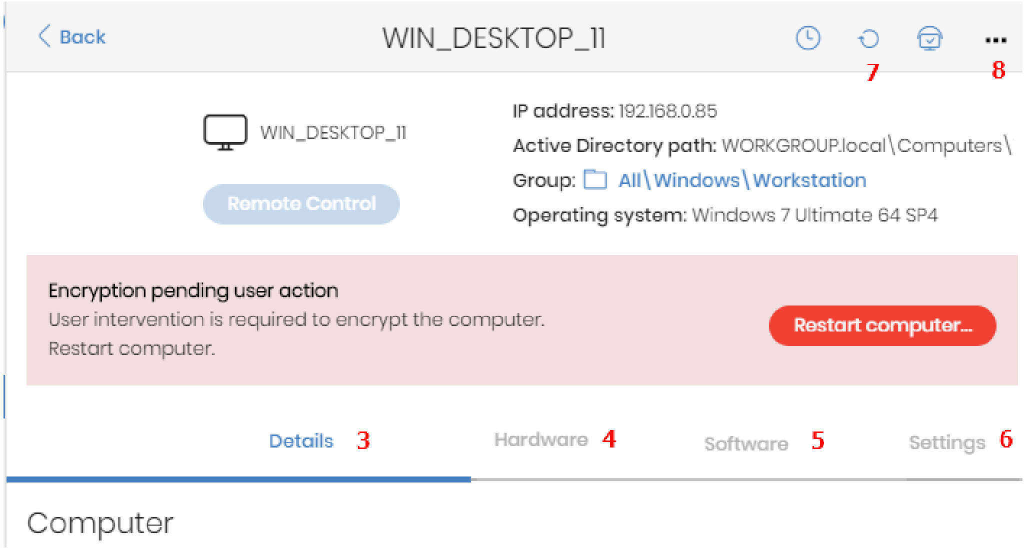
Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Platform	Operating system make.	• Windows • Linux • macOS • Android

Table 9.12: filters available in the 'Software' list

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:



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.

Computer

Figure 9.6: 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.
- **Hardware (4)**: here you can see the hardware installed on the computer, its components and peripherals, as well as consumption and use.
- **Software (5)**: here you can see the software packages installed on the computer, as well as versions and changes.
- **Settings (6)**: this shows the security settings and other settings assigned to the computer.

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.
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 9.13: 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.

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 section "**Releasing licenses**" on page **107**.
	There are free licenses but none of them have been assigned to this computer.	Refer to section "**Assigning licenses**" on page **107**.

Table 9.14: alerts related to license assignment

Installation errors

Alert	Description	Reference
Unprotected computer	There was an error installing the protection on the computer.	Refer to section "**Installation requirements**" on page **81**.
	A reboot is required to complete the installation due to a previous uninstallation.	Refer to section "**Computer restart**" on page **294**.
Error installing the patch manager	There was an error installing the patch management module on the computer.	Refer to section "**Make sure that Panda Patch Management works properly**" on page **199**.
Error installing the encryption module	There was an error installing the encryption module on the computer.	Refer to section "**Panda Full Encryption minimum requirements**" on page **230**.
Error installing the Panda agent	Wrong credentials.	Refer to section "**Remote installation of the software on discovered computers**" on page **95**.
	The discovery computer is not available.	Refer to widget "**Offline computers**" on page **252** and section "**Assigning the role of 'Discovery computer' to a computer on your network**" on page **87** on page **97**.

Table 9.15: alerts related to the installation of the Panda Endpoint Protection software

Alert	Description	Reference
	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 **252** and section “**Installation requirements**” on page **81**.
	The computer's operating system is not supported.	Refer to section “**Installation requirements**” on page **81**.
	Unable to download the agent installer due to a network error.	Refer to section “**Network requirements**” on page **82**.
	Unable to copy the agent installer due to low free disk space on the computer.	Refer to section “**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 **252** on page **292** and section “**Installation requirements**” on page **81**.

Table 9.15: alerts related to the installation of the Panda Endpoint Protection software

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 section “**Computer restart**” on page **294**.
Error encrypting the computer	Unable to encrypt the computer due to an error.	Refer to section “**Computer restart**” on page **294**.

Table 9.16: 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 section “**Computer restart**” on page **294**. Refer to section “**Encryption and decryption**” on page **231**.
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 section “**Offline computers**” on page **252**.

Table 9.17: alerts related to lack of user or administrator action

Alert	Description	Reference
Unprotected computer	The antivirus protection is disabled. Enable the protection.	Refer to section "**Manual and automatic assignment of settings**" on page **165**, section "**Creating and managing settings**" on page **164** and section "**Antivirus**" on page **184**.
Computer offline for N days	The computer is turned off or doesn't meet the network access requirements.	Refer to section "**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 9.17: 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 section "**Computer restart**" on page **294**.
	An error occurred while attempting to update the protection. Make sure the computer meets the hardware and network requirements.	Refer to section "**Installation requirements**" on page **81** and the section on available hard disk space in "**Hardware section (4)**"
	Updates are disabled for the computer. Assign the computer a settings profile with updates enabled.	Refer to section "**Protection engine updates**" on page **118**
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 section "**Knowledge updates**" on page **119**.

Table 9.18: 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 section "**Anti-theft**" on page **196** for more information on how to enable the anti-theft feature for Android devices and configure the private mode.*

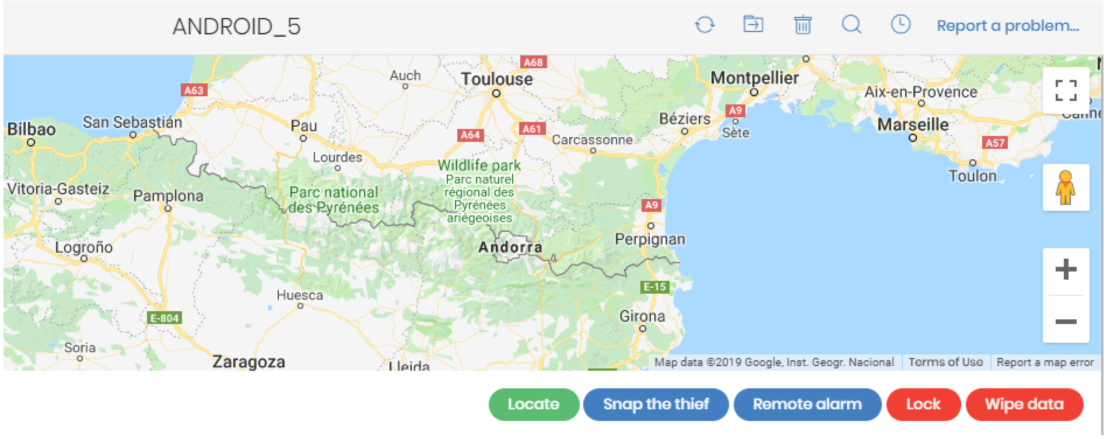


Figure 9.7: anti-theft dashboard for Android devices

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.

Table 9.19: actions supported by the anti-theft module for Android devices

Action	Description
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	The console will ask you for a 4-digit code and then lock the device. To unlock it, the user will have to enter the 4-digit code set by you.
Wipe data	This option formats the device, deleting all its contents and applications and returning it to its factory settings.

Table 9.19: 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 Control**.

- **Computer**: information about the device settings. This information is provided by the Panda agent.
- **Security**: status of the Panda Endpoint Protection protection modules.

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 chapter "**Licenses**" on page **105** for more information.
Agent version	Internal version of the Panda agent installed on the computer.

Table 9.20: fields in the Details tab's Computer section

Field	Description
Last bootup date	Date when the computer was last booted.
Installation date	Date when the computer's operating system was last installed.
Last connection	Date when the client software last connected to the Panda Security cloud. The communications agent connects at least every four hours.

Table 9.20: 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.
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. Patch status detection and problematic patch rollback.
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 9.21: fields in the Details tab's Security section

Data Control

This section indicates the status of the modules that protect the data stored on the computer.

Field	Description
Encryption status	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.
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.
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.

Table 9.22: fields in the Data protection section

Field	Description
Encryption date	Date when the computer was fully encrypted for the first time.

Table 9.22: fields in the Data protection section

Hardware section (4)

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
Optical disk	Information about the optical drives installed on the computer (CD- ROM, DVD, etc.).	• **Drive**: letter assigned by the operating system. • **Type:** characteristics of the drive. • **Name**: make and model.
Mother-board	Information about the computer's motherboard.	• Product • Serial number • Manufacturer
BIOS	Information about the BIOS installed on the computer.	• Version • Manufacture date • Serial number • Name • Manufacturer
System	Information about the computer manufacturer, make, model and serial number.	• **Architecture**: 32-bit or 64-bit • **Name**: computer model. • **Manufacturer**: company that assembled the computer.

Table 9.23: fields in the computer details' Hardware section

Field	Description	Values
		• **Hostname**: computer name assigned on the operating system. • **Domain**: Windows domain the computer is on. • Serial number
Battery	Information about the device's battery.	• Device ID • Location • Capacity • Capacity multiplier • Voltage • Chemistry • Name • Manufacturer
Audio device	Sound card make and manufacturer.	• Name • Manufacturer
Network adapter	Information about the model, manufacturer, and IP addresses of the network interface cards.	• Device ID • **Type**: layer 2 protocol. • Speed • **IP addresses**: primary address assigned to the adapter and alias. • Subnet masks • **DHCP servers**: assigned server for allocating IP addresses. • DNS servers: assigned name server. • Gateways • **MAC address**: physical address assigned to the adapter. • Name • Manufacturer
Monitor	Information about the monitor make and model.	• Device ID • Type • Manufacturer
Video controller	Information about the video card make and model and assigned drivers.	• Device ID • **RAM**: memory installed on the video controller. • DAC type • Horizontal resolution

Table 9.23: fields in the computer details' Hardware section

Field	Description	Values
		• Vertical resolution • Refresh rate • Driver version • **Name**: make and model of the video controller
Other hardware	Information about hardware that doesn't fall under any of the aforementioned categories.	• Category • 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. • **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 9.23: fields in the computer details' Hardware section

Software section (5)

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 9.24: 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

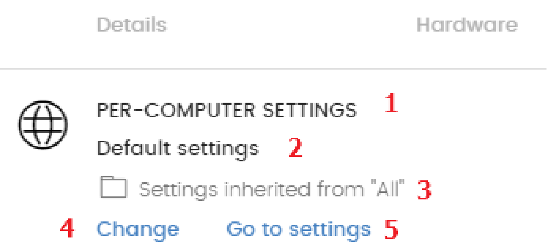
Installations and uninstallations

- 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.
Publisher	Company that developed the program.
Date	Date the program was installed or uninstalled.
Version	Internal version of the program.

Table 9.25: fields in the Installations and uninstallations section

Settings section (6)



Details Hardware

PER-COMPUTER SETTINGS 1

Default settings 2

Settings inherited from "All" 3

4 Change Go to settings 5

Figure 9.8: 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**: Per-computer settings, Proxy and language settings, Settings for workstations and servers, Settings for Android devices.
- **(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 chapter "**Managing settings**" on page **157** for more information on how to create and edit settings profiles.*

Action bar (7)

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 section "**On-demand computer scanning and disinfection**" on page **290** for more information.
Schedule scan	Lets you schedule a scan task. Refer to section "**On-demand computer scanning and disinfection**" on page **290** for more information.
Schedule patch installation	Creates a task that installs all released patches missing from the target computer. See section "**Downloading and installing patches**" on page **221** for more information
Restart	Restarts the computer immediately. Refer to section "**Computer restart**" on page **294** for more information.
Report a problem	Opens a support ticket for Panda Security's support department. Refer to section "**Reporting a problem**" on page **294** for more information.

Table 9.26: actions available from the computer details window

Hidden icons (8)

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 section "**The Computer tree panel**" on page **125***

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 section "**Configuring real-time communication**" on page* **178**

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:

- Per-computer settings.
- Proxy and language.

- Workstations and servers.
- Android devices.
- Patch management.
- Encryption.

Proxy and language

These settings let you define the language of the agent installed on end users' computers and the parameters required to connect to the Internet. Refer to chapter "**Configuring the agent remotely**" on page **173** for more information.

Per-computer settings

These settings let you define various parameters pertaining to the Panda agent:

- Update frequency of the Panda Endpoint Protection software installed on computers.
- Password required to install the software on end users' computers.
- Anti-Tamper protection.

*Refer to chapter "**Updating the client software**" on page **117** for more information.*

Workstations and servers

This section lets you define the security settings of the Windows, macOS and Linux computers on your network, both workstations and servers.

*Refer to chapter "**Security settings for workstations and servers**" on page **181**.*

Android devices

This section lets you define the security and anti-theft settings of your Android devices (tablets and smartphones).

*Refer to chapter "**Security settings for Android devices**" on page **195** for more information.*

Patch management

These settings let you define the discovery of the patches published by the vendors of the applications installed across the network.

*Refer to chapter "**Panda Patch Management (Updating vulnerable programs)**" on page **197** for more information.*

Encryption

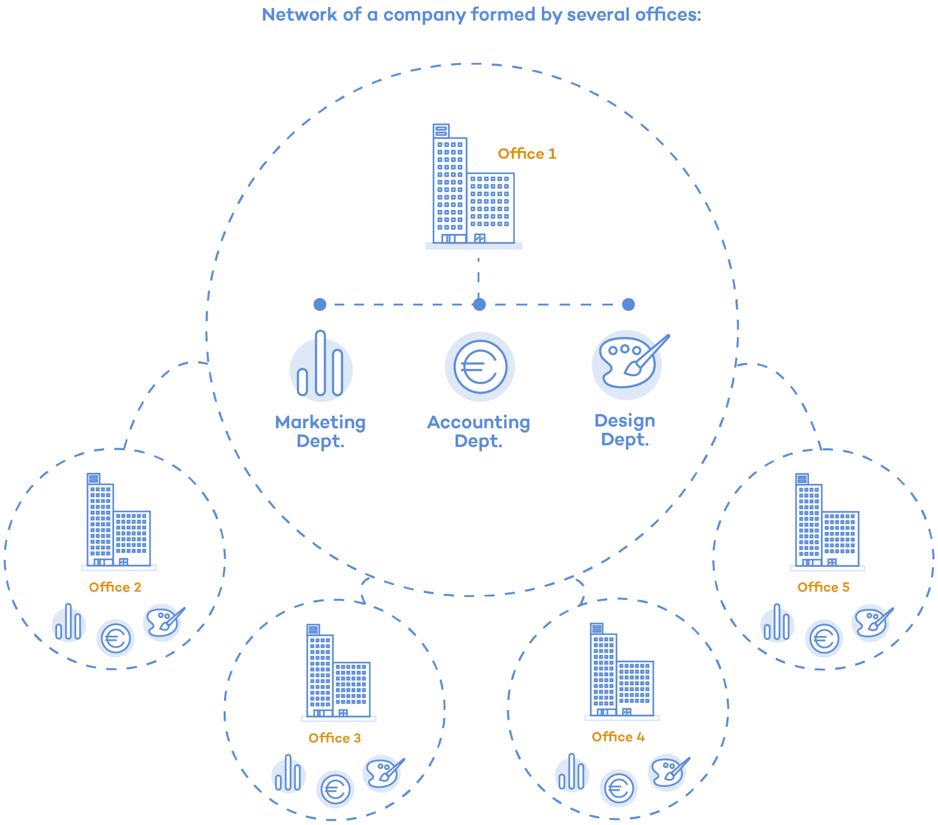
These settings let you define the status and encryption parameters of the mass storage volumes connected to your computers.

*Refer to chapter "**Panda Full Encryption (device encryption)**" on page **225** for more information.*

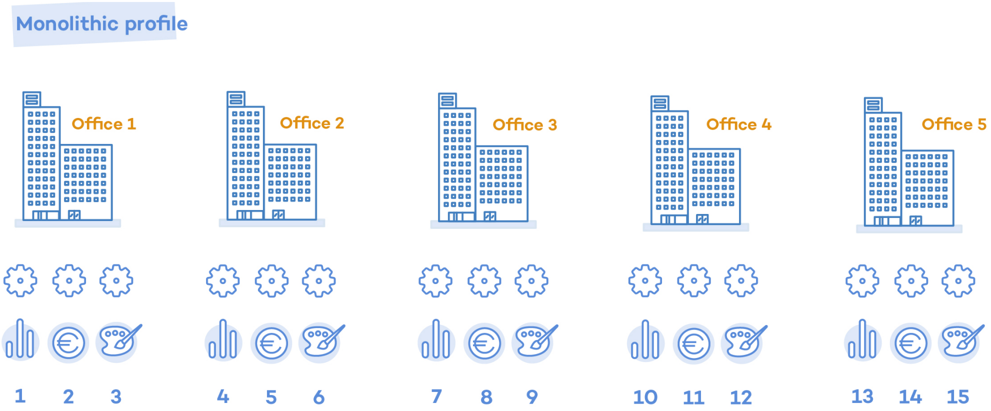
Modular vs monolithic settings profiles

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.

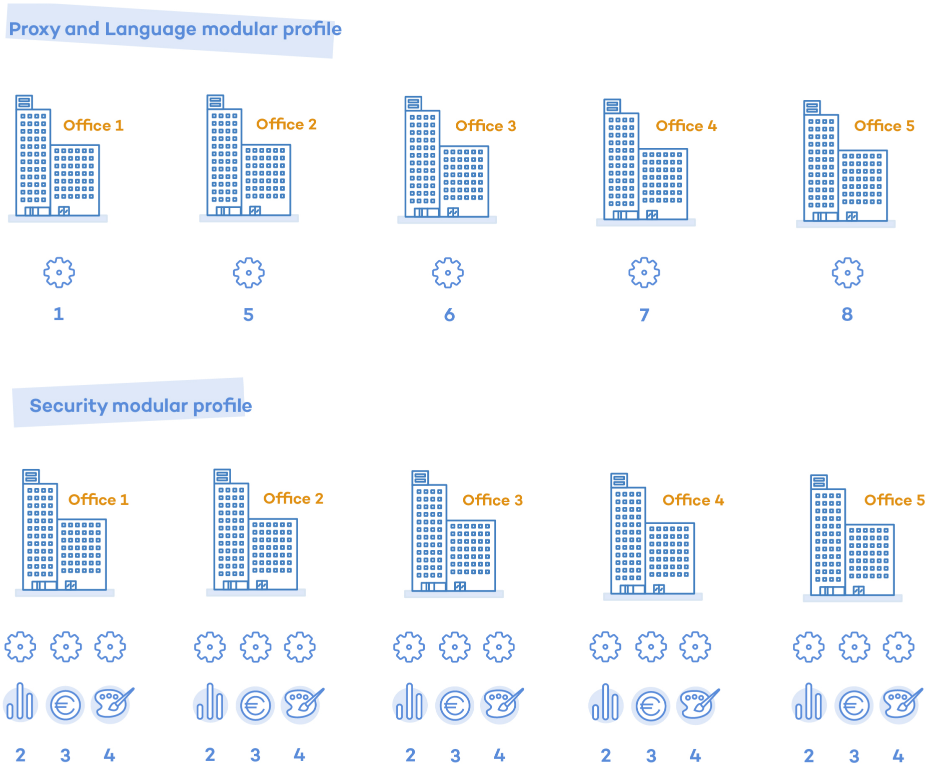
Case study: creating settings for several offices



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.

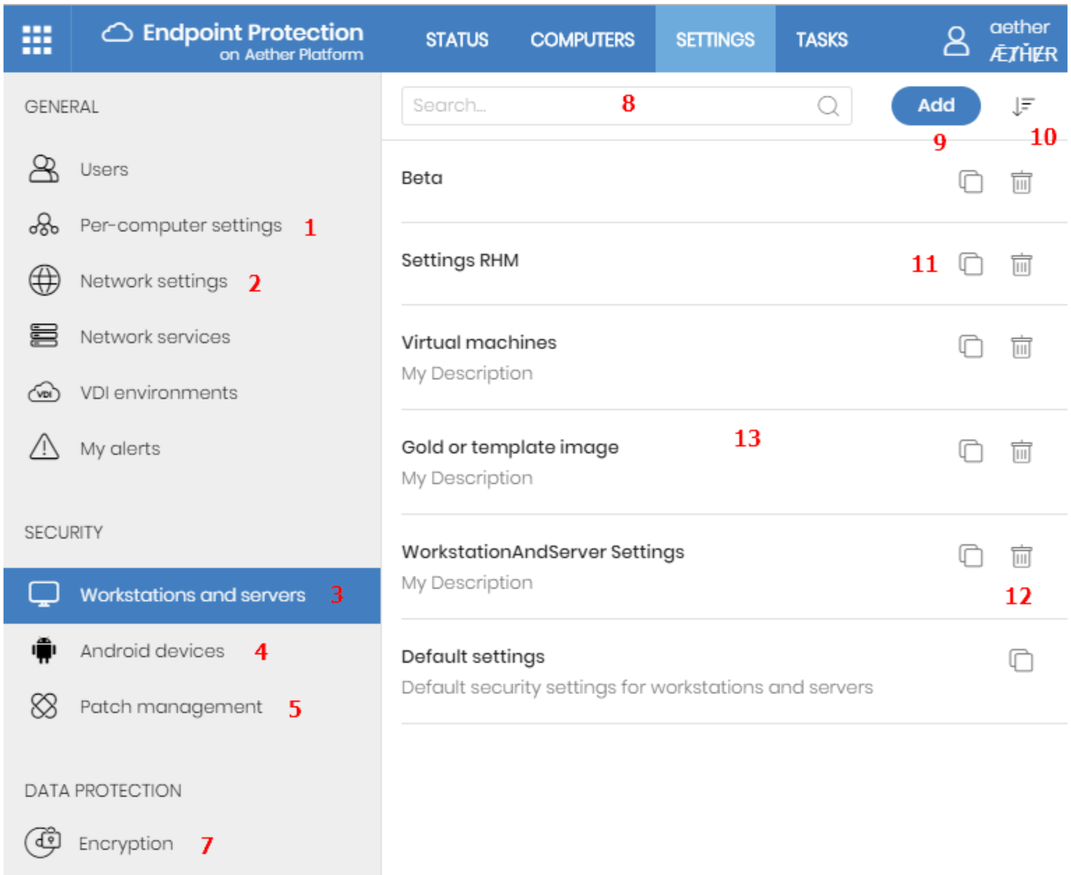


If Panda Endpoint Protection implemented all configuration parameters in a single monolithic profile, the company would require 15 different settings profiles (5 x 3 =15) to adapt to the needs of all three departments in the company's offices.



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.

Creating and managing settings



Beta

Settings RHM

Virtual machines
My Description

Gold or template image
My Description

WorkstationAndServer Settings
My Description

Default settings
Default security settings for workstations and servers

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)**, **(2)**, **(3)**, **(4)**, **(5)** and **(7)**. In the right-hand panel, you can see the profiles of the selected category that have already been created **(13)**, and the buttons for adding **(9)**, copying **(11)** and deleting profiles **(12)**. Use the search bar **(8)** to quickly find existing profiles.

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 **(11)** 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 **(11)** and **(12)** 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.

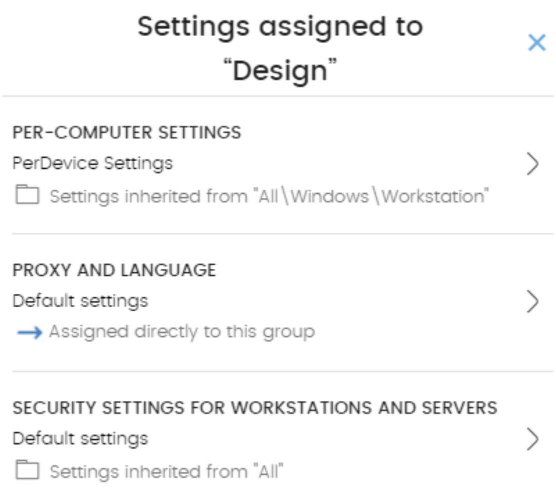
Once a settings profile has been created, there are three ways of assigning it:

- 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 section "**Group tree**" on page **130**.*

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"

PROXY AND LANGUAGE
Default settings
→ Assigned directly to this group

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**

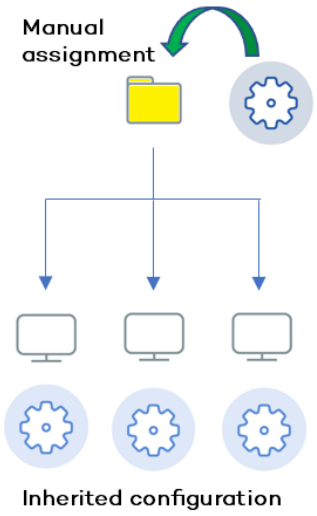


Figure 10.3: inheritance/indirect assignment

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.

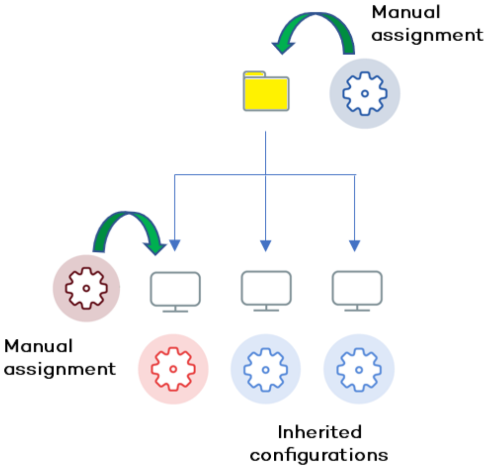


Figure 10.4: priority of manually assigned settings over inherited ones

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.

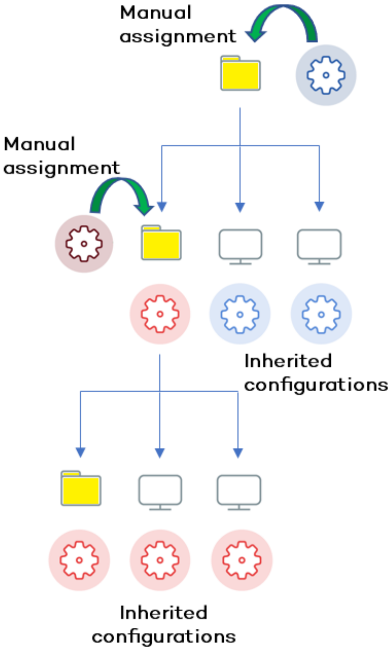


Figure 10.5: Inheritance limits

Overwriting settings

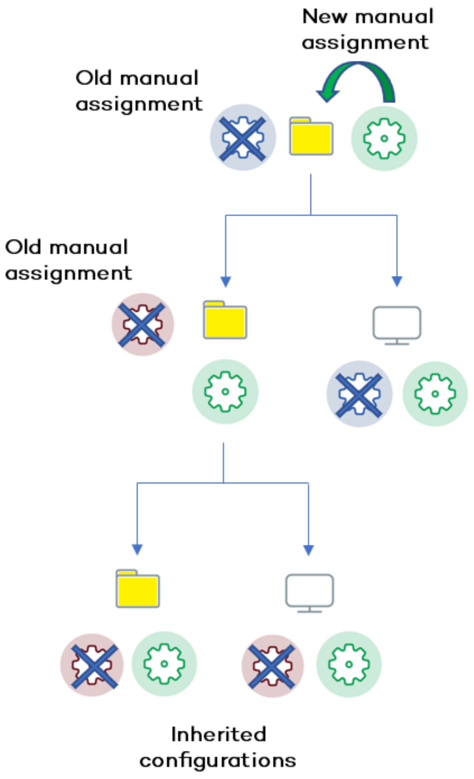


Figure 10.6: overwriting manual settings

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

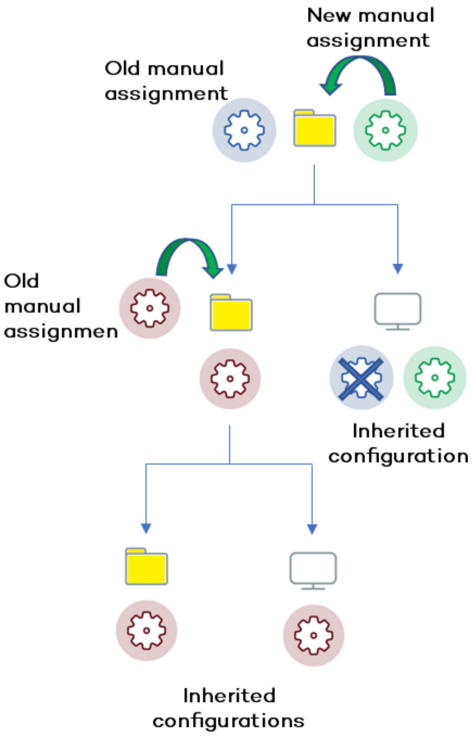


Figure 10.7: keeping manual settings

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.

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

To view the settings assigned to a group, click the context menu of the relevant branch in the group tree and select **Settings** in the pop-up menu displayed. Below is a description of the information displayed in this window:

- **Type of settings:**
  - Proxy and language settings.
  - Per-computer settings.
  - Security settings for workstations and servers.
  - Security settings for Android devices.
- **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 section “***Fields displayed in the exported file***” on page* **136**

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).
- 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.*

Configuring a computer as a proxy server

UDP port 21226 and TCP port 3128 on those computers designated as Panda Endpoint Protection *proxies cannot be used by other applications. Additionally, the computers' firewall must be configured to allow incoming and outgoing traffic on both ports.*

- 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.

Cache/repository role

Panda Endpoint Protection lets you assign the cache role to one or more computers on your network. These computers 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 will be downloaded centrally and once for all computers on the network.

Requirements and limitations of computers with the cache role

- The scope of the computer with the cache role is restricted to the network segment to which its network interface is connected. If a cache computer has several network interface cards, it can serve as a repository for each network segment to which it is connected.

> *It is advisable to designate a computer with the cache role in 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 3128.

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.

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. Then, all other workstations and servers in those segments will receive that notification and connect to the cache computer. Should there be more than one designated cache node on a network segment, all other computers on the subnet will connect to the most appropriate node based on the amount of free resources.

Additionally, from time to time, all computers on the network check to see if there are new nodes with the cache role.

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.

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 section "***Computer discovery***" on page* **87** *for more information about the* Panda Endpoint Protection *discovery and installation processes.*

Configuring Internet access via a proxy server

Configuring proxy usage

To configure the way one or more computers connect to the Internet via a proxy server, you must create a Proxy and language 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.
- Select an existing **Proxy and language** settings profile or create a new one.

- In the **Proxy** section, choose the type of proxy to use.

Proxy type	Description
Do not use proxy	Direct access to the Internet. Computers without a proxy configured 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.
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. Only Windows computers can use a Panda Endpoint Protection proxy..

Tabla 11.1: types of Internet access supported by Panda Endpoint Protection

To configure the sending of data via a Panda Endpoint Protection proxy, click the **Select computer** link to display a list of the available computers on the network that have the proxy role.

Fallback mechanisms

If a Panda agent cannot connect to Aether Platform, the following fallback mechanism are used to restore the connection via other means:

- **Corporate proxy**: if the Internet connection is configured to take place via a corporate proxy or a Panda Endpoint Protection proxy and there is no response, an attempt is made to connect directly.
- **Internet Explorer**: the Panda agent tries to use 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 can't be used.
  - If Internet Explorer is configured to use a PAC (Proxy Auto-Config) file, the Panda agent will use the URL in the config file, provided the access protocol is HTTP or HTTPS.
- **WinHTTP/WinINet**: the default proxy settings are read.
- **WPAD** (Web Proxy Auto-Discovery Protocol): a request is sent to the network via DNS or DHCP to get the discovery URL that points to the PAC config file.

Configuring real-time communication

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.

> ⚠ *Isolated workstations and servers cannot communicate in real time with the* Panda Security *cloud via a computer with the Panda Endpoint Protection proxy role assigned. These communications will be established through the ordinary procedure. This limitation doesn't affect computers using a corporate proxy to access the Internet*

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, create a **Proxy and language** 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:
  - English
  - Spanish
  - Swedish
  - French
  - Italian
  - German
  - Portuguese
  - Hungarian

- Russian
- Japanese
- Finnish

> *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 the Anti-Tamper protection and password

Anti-Tamper protection

Many advanced threats and hackers take advantage of sophisticated techniques to disable the security software installed on computers and bypass protection features. To tackle this threat, Panda Endpoint Protection incorporates anti-tamper technologies that prevent unauthourized tampering of the protection.

Enabling 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.

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.

Chapter 12

Security settings for workstations and servers

The **Settings** menu at the top of the Panda Endpoint Protection console provides access to the parameters required to configure the security settings for the workstations and servers in your organization. Click the **Workstations and servers** section from the left-hand menu to display a list of the security settings already created.

This chapter describes 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.

CHAPTER CONTENT

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 12.1: 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	X	X	X
Firewall & IDS	X		
Email protection	X		
Web protection	X	X	X
Device control	X		

Table 12.2: 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.

Updates

Refer to chapter "**Updating the client software**" *on page* **117** *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 section "**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 chapter "**Supported uninstallers**" *on page* **315** *for a full list of the competitor products that* Panda Endpoint Protection *uninstalls automatically from users' computers.*

Exclusions

The **Exclusions** section lets you select items that won't be deleted or disinfected.

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 indicate specific files that won't be scanned.
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 12.3: 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 12.4: 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 anti-exploit and heuristic technologies designed to analyze process behavior locally and detect suspicious activity.
Detect phishing	Detects fraudulent emails and websites.

Table 12.5: 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 12.6: file types scanned by Panda Endpoint Protection's antivirus protection

Firewall (Windows computers)

Panda Endpoint Protection provides three tools to filter the network traffic that protected computers send and receive:

- **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. To set the firewall's default behavior, the network administrator must select the type of network that the computers in the configured profile usually connect to.

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.

Table 12.7: 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.

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.

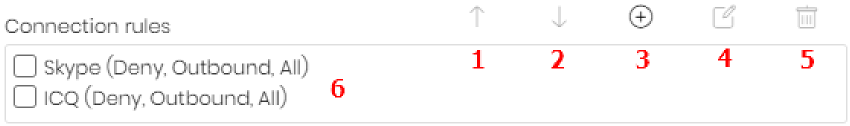
Action	Description
Allow	Implements a permissive strategy based on always accepting connections for all programs for which you haven't configured a specific rule in step 3. This is the default, basic mode.
Deny	Implements a restrictive strategy based on always denying connections for all programs for 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 12.8: 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 12.9: 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.

Table 12.10: advanced communication options for allowed programs

Field	Description
Protocol	Lets you establish the layer 3 protocol for the traffic generated by the program you want to control. • All • TCP • UDP
IP	• **All**: the rule won't take into account the connection's source and target IP addresses. • **Custom**: lets you specify the source and target IP addresses of the traffic to control. You can enter multiple addresses separated by commas (,). To specify a range, use a hyphen (-). • **Ports**: lets you specify the communication port. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).

Table 12.10: 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.

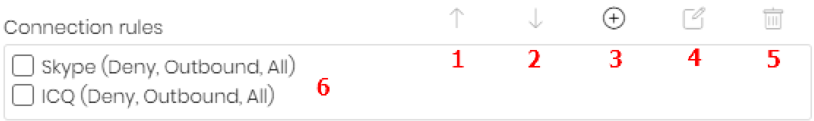
Table 12.11: types of default actions supported by the firewall for the programs installed on users' computers

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**: lets you create rules that describe ICMP messages, along with their type and subtype. **IP Types**: lets you create rules for the IP protocol and other higher-level protocols.
IP addresses	Lets you specify the traffic's source and target IP addresses.

Table 12.12: settings options for connection rules

Field	Description
MAC addresses	Lets you specify the traffic's source and target MAC addresses.

Table 12.12: 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.
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.

Table 12.13: supported types of malformed traffic

Field	Description
	• **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 12.13: 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

If you want to exclude a device from the device control feature without having to wait for the user to connect it and then exclude it manually, obtain the device's ID:

- Open Windows Device Manager, and access the properties of the USB device that you want to identify in order to exclude it.
- Click the Details tab and select Resources from the Property drop-down list. A value called CM_DEVCAP_UNIQUEID should be displayed.
- Next, select Device Instance Path from the Property drop-down list to get the device's unique ID.

If the CM_DEVCAP_UNIQUEID value is not present, it won't be possible to get the device’s ID. In that case you can use the device's hardware ID to identify it. To get that value, select **Hardware IDs** from the **Property** drop-down list.

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**".

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.

This chapter explains the available security and anti-theft configuration options for Android devices, and gives recommendations to protect smartphones and tablets without interfering with user activity.

CHAPTER CONTENT

Introduction to the security settings for Android devices

The settings options for Android devices are divided into various sections. Click each of them to display a drop-down menu with the associated options. Below we provide a brief explanation of each section:

- **Updates**: lets you define the type of connection to be used by the device to download updates from Panda Security's cloud.

*For more information on how to configure updates, refer to chapter ““**Updating the client software**” on page **117**.*

- **Antivirus**: lets you configure the antivirus protection.

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 section “**General section for Android devices**” on page* **147** *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 13.1: 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.*

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 section "**Configuring the discovery of missing patches**"
- **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 section "**'Patch management status' list**"
- **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 section "**Panda Patch Management lists**"
- **To view a history of all installed patches**: check the **Installation history** list (top menu **Status**, side panel **My lists**, **Add).** Refer to section "**Installation history' list**"
- **To patch computers**: go to top menu **Tasks**, and create an **Install patches** scheduled task. You can also patch computers via the context menus available in the group tree (top menu **Computers**), on the lists, and on the **Computer details** screen. Refer to section "**Patch installation**"
- **To uninstall patches**: select one of the following options:
  - From the **Last patch installation tasks** widget, click the **View installation history** link. Refer to section "**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 section "**Installation history' list**".
- 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**. Refer to section "**Tasks top menu**".
- 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 section "**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).
- 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 section "**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' list**" 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' list**" 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' list**".
  - 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**.

Install the patches

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 chapter "**Tasks**" for more information about tasks in Panda Endpoint Protection**.**

Despite 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' list**" 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.

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' list**".
- 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' list**" 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' list**".
- 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

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.
- Select the types of patches to install.
- Click **Save** and publish the task.

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 Endpoint Protection 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 chapter "**Install/uninstall patches**" on page **62** 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' list**".
    - 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 Endpoint Protection 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. If a patch is withdrawn by the corresponding vendor, it will no longer be shown or installed.

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**" 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' list**".

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 Endpoint Protection 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.

Follow these steps to check whether a computer where an incident has been detected has missing patches:

- Go to top menu **Status**, click on the **Malware activity**, **PUP activity**, **Currently blocked programs being classified**, or **Threats detected by the antivirus** widgets and click a computer-threat. Information about the threat detected on the computer will be 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

Panda Patch Management keeps an inventory of missing patches and updates for all computers on your network that have an active Panda Patch Management license.

Follow these steps to configure the discovery of missing patches:

- Go to top menu **Settings** and click **Patch management** from the side panel.
- Click the **Add** button and configure the options described in the following sections.
- Assign the new settings to those computers on your network with an active Panda Patch Management license.

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 in its cloud-hosted database.

> ⚠ *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

Next is a description of the widgets implemented in the **Patch Management** dashboard, their areas and hotspots, as well as the tooltips and what they mean.

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.

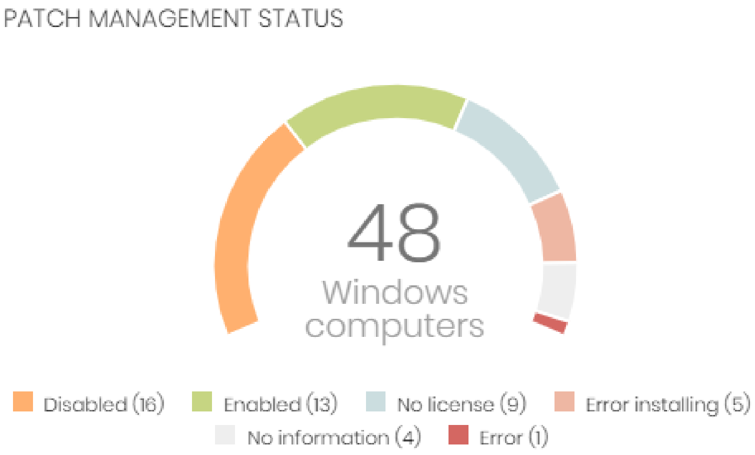


Figure 14.1: 'Patch management status' panel

- **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 14.2: description of the data displayed in the 'Patch management status'

- **Lists accessible from the pane**

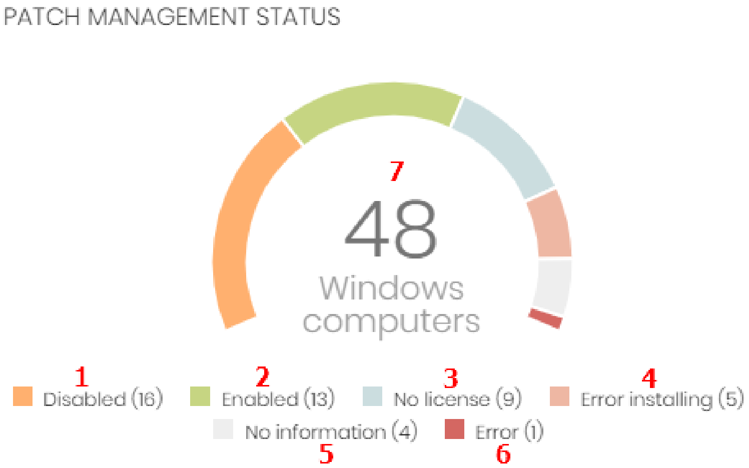


Figure 14.2: hotspots in the 'Patch management status' panel

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 14.3: 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.

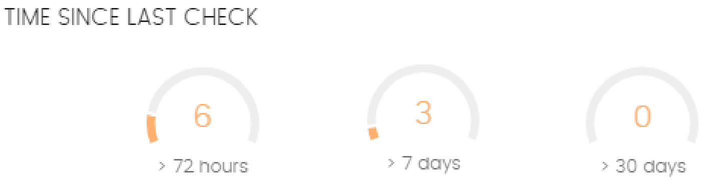


Figure 14.3: 'Time since last check' panel

- **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 14.4: description of the data displayed in the 'Time since last check' panel

- **Lists accessible from the panel**

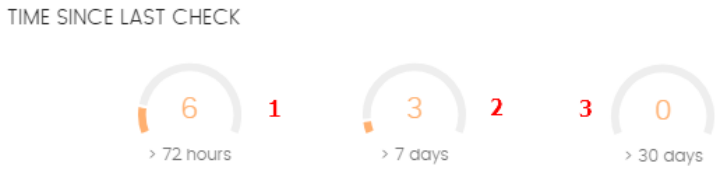


Figure 14.4: hotspots in the 'Time since last check' panel

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 checked = More than 3 days ago and Patch management status = Enabled and Disabled
(2)	Last checked = More than 7 days ago and Patch management status = Enabled and Disabled
(3)	Last checked = More than 30 days ago and Patch management status = Enabled and Disabled

Table 14.5: filters available in the 'Patch management status' list

End-of-Life programs

Shows information about the End-of-Life of the programs on the network, grouped by date.

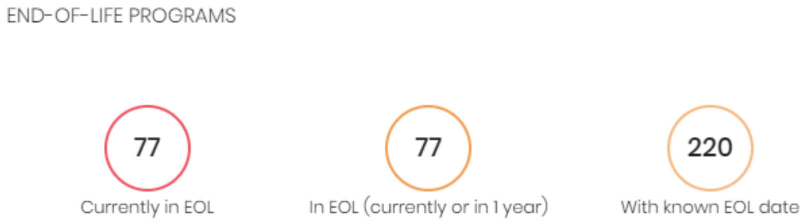


Figure 14.5: 'End-of-Life programs' panel

- **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 14.6: description of the data displayed in the ‘End of life’ panel

- **Lists accessible from the panel**

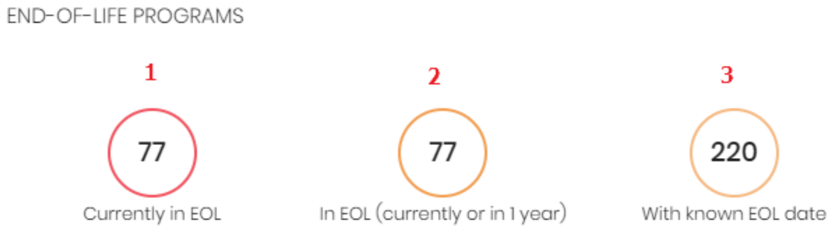


Figure 14.6: hotspots in the 'End-of-Life programs' panel

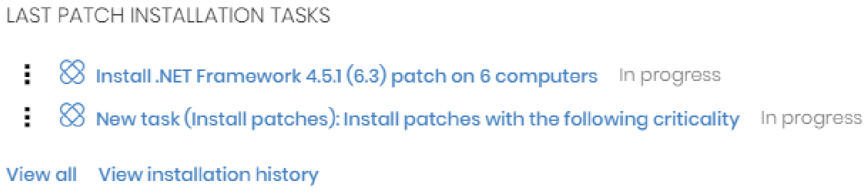
Click the hotspots shown in the figure 14.6 to access the **End-of-Life programs** list with the following predefined filters.

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 14.7: filters available in the "End Of Life’ list

Last patch installation tasks

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

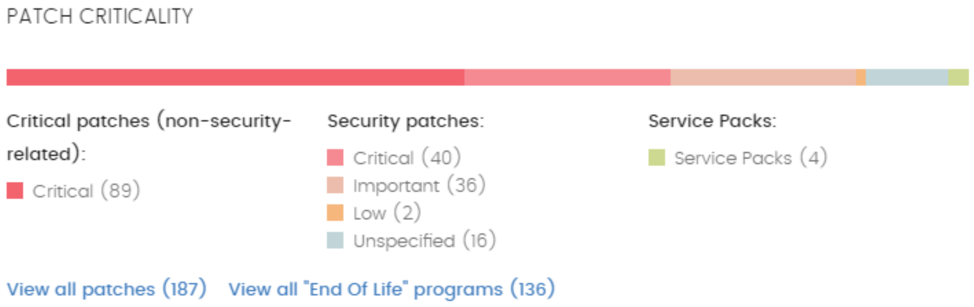
Figure 14.7: 'Last patch installation tasks' panel

- 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.

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.



PATCH CRITICALITY

Critical patches (non-security-related):

🟥 Critical (89)

Security patches:

🟥 Critical (40)
🟫 Important (36)
🟧 Low (2)
⬜ Unspecified (16)

Service Packs:

🟩 Service Packs (4)

View all patches (187) View all "End Of Life" programs (136)

Figure 14.8: Path criticality' 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	Number of non-security patches that are pending application
Service Packs – 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 14.8: description of the data displayed in the 'Patch criticality' panel

- **Lists accessible from the panel**

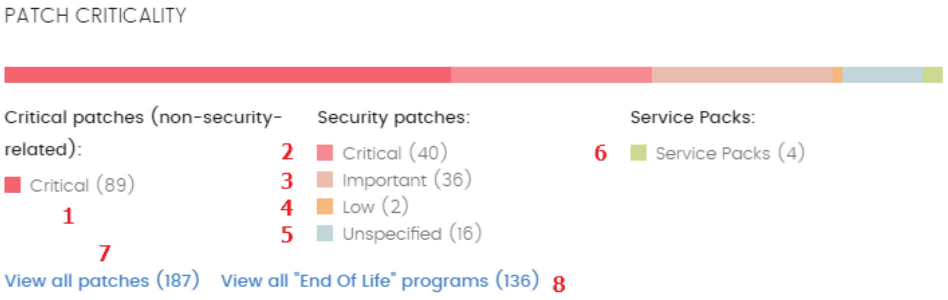


Figure 14.9: hotspots in the 'Path criticality' panel

Click the hotspots shown in the figure 14.9 to access the **Available patches** list with the following predefined filters.

Hotspot	Filter
(1)	Criticality = Critical (security-related)
(2)	Criticality = Important (security-related)
(3)	Criticality = Low (security-related)
(4)	Criticality = Unspecified (security-related)
(5)	Criticality = Other patches (non-security-related)
(6)	Criticality = Service Pack
(7)	No filters

Table 14.9: filters available in the 'Available patches' list

Panda Patch Management lists

'Patch management status' list

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
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string

Table 14.10: fields in the 'Patch management status' list

Field	Comments	Values
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
Last connection	Date when the Panda Endpoint Protection status was last reported to the Panda Security cloud.	Date

Table 14.10: fields in the 'Patch management status' list

- **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
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

Table 14.11: fields in the 'Patch management status' exported file

Field	Comments	Values
Operating system	Operating system installed on the computer, internal version and patch status.	Character string
Exchange Server	Version of the mail server installed.	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
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
Isolation status	Indicates if the computer has been isolated or can communicate normally with all other computers on the network.	• Isolated • Not isolated
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 14.11: 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

Table 14.12: filters available in the 'Patch management status' list

Field	Comments	Values
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 14.12: filters available in the 'Patch management status' list

'Available patches' list

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
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

Table 14.13: 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. • **Isolate computer**: lets you isolate the computer from the network. • **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 14.13: fields in the 'Available patches' list

- **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
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

Table 14.14: fields in the 'Available patches' exported file

Field	Comments	Values
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 14.14: 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

Table 14.15: filters available in the 'Available patches' list

Field	Comments	Values
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) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
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 14.15: filters available in the 'Available patches' list

'End-of-Life programs' list

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
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 14.16: fields in the 'End-of-Life programs' list

- **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 14.17: 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 14.18: filters available in the 'End-of-Life programs' list

Installation history' list

Shows the patches that Panda Endpoint Protection 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

Table 14.19: fields in the 'Installation history' list

Field	Comments	Values
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
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • Uninstalled • The patch is no longer required

Table 14.19: fields in the 'Installation history' list

- **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

Table 14.20: fields in the 'Installation history' exported file

Field	Comments	Values
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 (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 14.20: 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 14.21: filters available in the 'Installation history' list

Downloading and installing patches

In order to install patches and updates, Panda Patch Management uses the task infrastructure implemented in Panda Endpoint Protection.

> ⚠ *It is not possible to install the patches released by Microsoft if the Windows Update service is disabled on the target workstation or server.*

Patch installation

To speed up the configuration process when patching computers, Panda Endpoint Protection lets you create patching tasks by leveraging preconfigured parameters. The number of preconfigured parameters will differ (all, some or none) depending on where in the management console you create the task from:

- From the **Tasks** menu at the top of the console.
- From the **Available patches** list.
- From the folder tree.
- From the **Computers** screen.

The preconfigured parameters can be as follows:

- **Recipients**: the computers that will receive the patch or patch group. These can be groups as well as individual workstations or servers.
- **Patches**: the specific updates to be installed.
- **Task type**: quick or scheduled.

Tasks top menu

Lets you create tasks from scratch. Neither the patches to be installed nor the target computers are preconfigured.

Follow the steps below to create a patch installation task:

- Go to top menu **Tasks**, click **Add task** and select **Install patches**.
- In the **Recipients** field, select the groups and computers that will receive the task.
- Schedule the task. See chapter "**Scheduled recurring tasks**" on page **304** for more information.

Select the type of patches to install. When creating a new task from scratch you cannot specify individual patches.

Set the restart options in case the target workstation or server needs to be restarted to finish installing the patch.

- **Do not restart automatically**: upon completing the patch installation task, a window is 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 is 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 be restarted.
- **Automatically restart servers only**: this option behaves in the same way as **Automatically restart workstations only**.

- **Automatically restart both workstations and servers**: this option behaves in the same way as **Automatically restart workstations only.**
- Click **Save** and publish the task.

'Available patches' list

Lets you create tasks using preconfigured computer-patch pairs.

Follow these steps to create a patch installation task from the **Available patches** list:

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
- Select the computer-patch pairs that suit your needs.
- If you select multiple patches, click **Install** (quick task) or **Schedule installation** (scheduled task) from the action bar in order to install them.
  - Quick tasks are automatically published.
  - Scheduled tasks are not published immediately and may require configuration changes. Go to the **Tasks** menu at the top of the console to edit and publish a scheduled task.
- If you select a single computer-patch pair, you can use the computer's context menu to select **Install** or **Schedule installation**.

Folder tree

Lets you create tasks using preconfigured computer groups. These tasks are always scheduled tasks.

Follow these steps to create a scheduled patch installation task from the folder tree:

- Go to top menu **Computers**, and click the context menu of the computer group that will receive the scheduled patch installation task.
- Select **Schedule patch installation**.
- Go to top menu **Tasks**, and edit the task to configure the type of patches to install.
- Click **Save** and publish the task.

The Computers screen

Lets you create tasks for specific computers. These tasks are always scheduled tasks.

Follow these steps to create a scheduled patch installation task from the **Computers** screen:

- Go to top menu **Computers**, and click the group that contains the computers that will receive the scheduled patch installation task.
- From the right panel, click the checkboxes besides the computers that will receive the patch installation task.
- Select **Schedule patch installation** from the action bar. If the patches are to be applied to a single workstation or server, you can use the computer's context menu.
- Go to top menu **Tasks**, and edit the task to configure the type of patches to install.

- Click **Save** and publish the task.

Patch download and bandwidth savings

Prior to installing a patch, it must be downloaded from the Panda Security cloud. 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 are 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 chapter "***Configuring the Panda agent role***" on page* **174** *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 are 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 computer's storage media.

Installation task sequence

Patch installation tasks may require downloading patches from the Panda Security cloud if the nodes on the network with the cache/repository role don't already have the relevant patches. In this scenario, bear in mind that quick tasks start downloading the necessary patches as soon as they are created. This may result in high bandwidth usage if these tasks affect many computers or there is a huge amount of data downloaded.

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.

Chapter 15

Panda Full Encryption (device encryption)

Panda Full Encryption is a module in the Aether platform that encrypts the content of data storage devices. 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**" on page **230**) 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.

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.

PIN and extended/improved PIN

The PIN (Personal Identification Number) is a sequence of 4 to 20 numbers (6 to 20 on Windows 10 version 1709 and later) 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.

If the hardware is compatible, Panda Endpoint Protection 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 Endpoint Protection 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

This is an 8 to 255 alphanumeric character password equivalent to the extended PIN.

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.

Overview of the encryption service

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, **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.

The following are not encrypted:

- Dynamic hard disks.
- Removable hard drives.
- USB drives.

- 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 (excluding 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 Patch Management 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.**

Table 15.1: Steps for encrypting previously unencrypted drives

Step	Process on the computer	User interaction
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.**
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.
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.

Table 15.1: Steps for encrypting previously unencrypted drives

Step	Process on the computer	User interaction
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. 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.

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 Endpoint Protection 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 Endpoint Protection 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.

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:

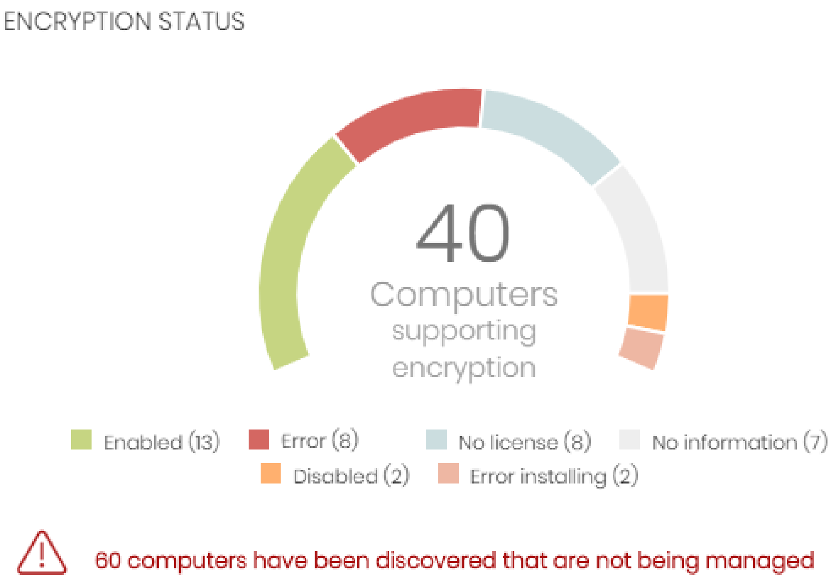
- In the **Computers** menu, click the computer for which you want to obtain the key.
- In the **Details** tab, in **Data protection**, click the **Get recovery key** link. You will see a link with the identifiers of the encrypted drives.
- Click a drive identifier to display the recovery key.

Panda Full Encryption panels and widgets

Below there is an explanation of the different widgets in the **Encryption** dashboard, describing the different areas and hotspots included and the tooltips and their meanings. To access these, click **Status** in the top menu, then **Encryption** in the side panel.

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

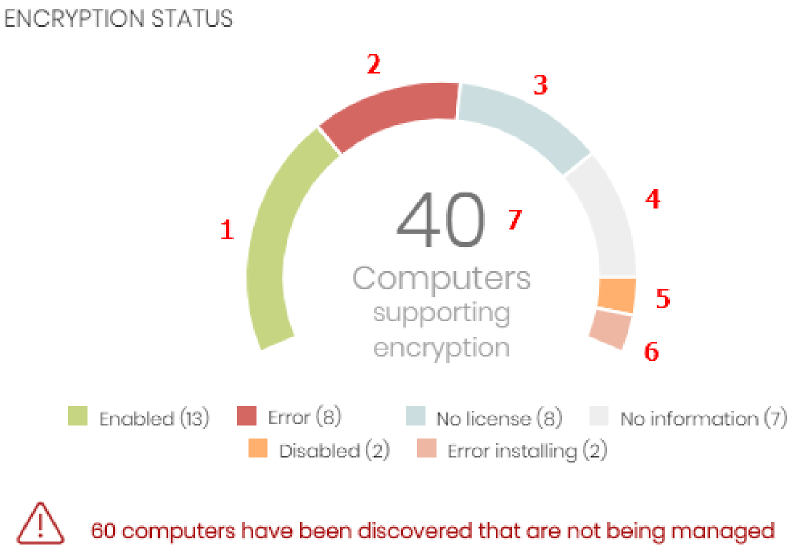
Figure 15.1: Encryption status pane

- **Meaning of the data**

Status	Description
Enabled	Computers with Panda Full Encryption installed, with encryption settings assigned and without having reported encryption errors.
Disabled	Computers with Panda Full Encryption installed, with decryption settings assigned and without having reported decryption 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.
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**


ENCRYPTION STATUS

⚠ 60 computers have been discovered that are not being managed

Figure 15.2: Hotspots in the Encryption Status panel

By clicking the areas indicated in figure 16.2, the **Encryption Status** list opens with the following filters:

Hotspot	Filter
(1)	Encryption status = Enabled
(2)	Encryption status = Error

Table 15.3: Filters available in the Encryption Status list

Hotspot	Filter
(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.

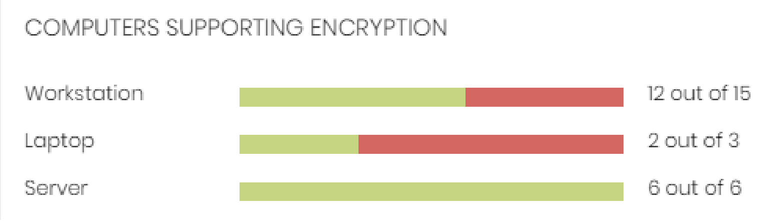


Figure 15.3: Computers Supporting Encryption panel

- **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**

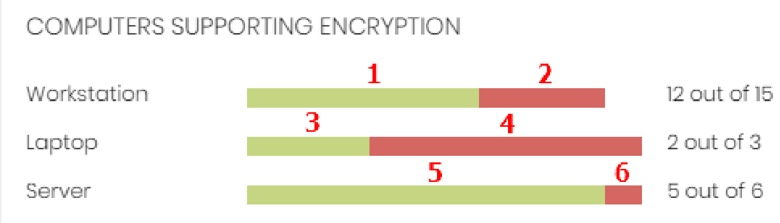


Figure 15.4: Hotspots in the Computers Supporting Encryption panel

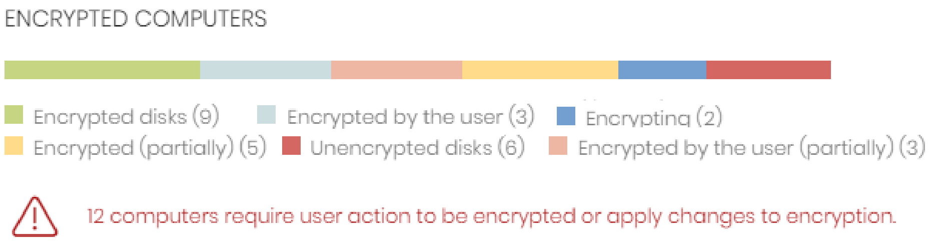
By clicking the areas in the panel, the **Encryption Status** list opens displaying the following filters:

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.**
(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.

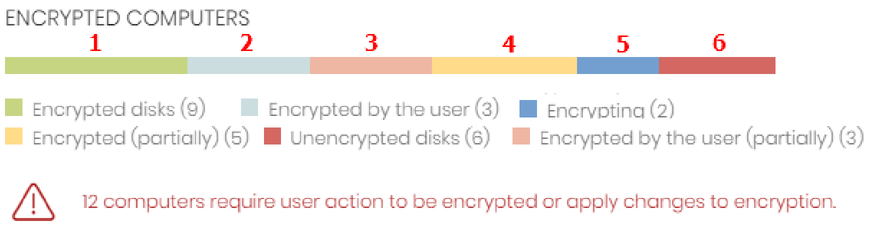
Figure 15.5: Encrypted Computers panel

- **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	The encryption process is in progress.
Decrypting	The decryption process is in progress.
Encrypted by the user	All disks have been encrypted by the user.
Encrypted by the user (partially)	Some disks have been encrypted by the user.

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

By clicking the areas indicated in 15.6, the **Encryption Status** list opens displaying the following 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.

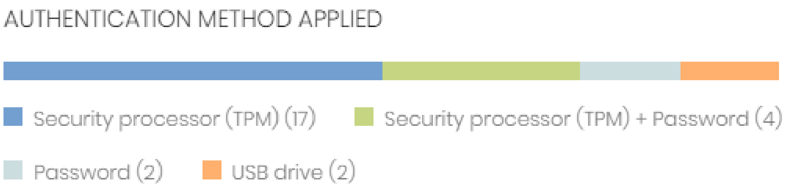

AUTHENTICATION METHOD APPLIED
Security processor (TPM) (17)
Security processor (TPM) + Password (4)
Password (2)
USB drive (2)

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**

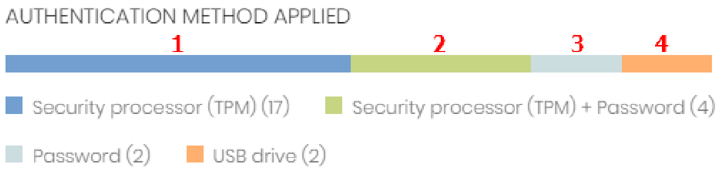


Figure 15.8: Hotspots in the Authentication Method Applied panel

By clicking the areas indicated in figure 15.8, the **Encryption Status** list opens displaying the following 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

To access the lists in Panda Full Encryption, follow the steps below:

- **To show lists using preset filters**: In the **Status** menu, go to **Encryption** in the side panel and click on the items in the widgets shown. The list associated with the widget will open with the filtering tool configured to show the selected information.

- **To show lists without using preset filters**: In the **Status** menu, go to the **My lists** panel and click **Add**. Then select a list.

> *See section "**Managing lists**" on page **46** for more details on managing lists in Panda Endpoint Protection.*

Encryption Status list

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
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 • Decrypting • Encrypted by the user • Encrypted by the user (partially)
Authentication method	Authentication method selected for the encrypted disks.	• All • Unknown • Security processor (TPM)

Table 15.10: List fields

Field	Comment	Values
		• 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

- **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
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

Table 15.11: Fields in the exported file

Field	Comment	Values
Last update	Date the signature file was downloaded.	Date
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 • Decrypting • Encrypted by the user • 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) • 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.	
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 encryption	Encryption status of the disks.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted by the user (partially)
Encryption status	Status of the Panda Full Encryption module.	• No information • Enabled • Disabled • Error • Error installing • 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

Encryption settings

Panda Full Encryption lets you centrally set the encryption settings for your network computers.

To configure the encryption on computers:

- Click **Settings** in the top menu, then **Encryption** in the side panel**.**
- Click **Add** and configure the options described in section "**Panda Full 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 Endpoint Protection, 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.

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 **126.** 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 5

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 chapter "**Reports**" on page **283**.*

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

To access panels and lists covering the security status of your network, click the **Status** menu at the top of the console and then click **Security** from the menu on the side.

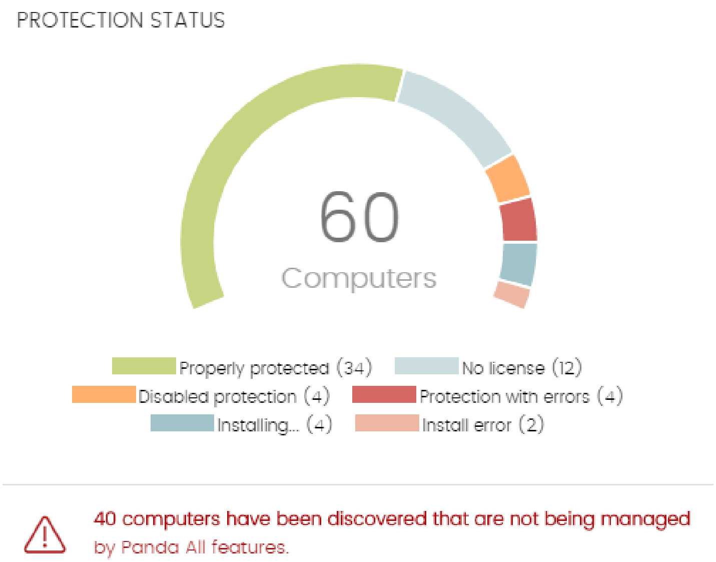
Below is a description of the different widgets displayed on the Panda Endpoint Protection dashboard, their areas and hotspots, as well as their tooltips and their meaning.

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**

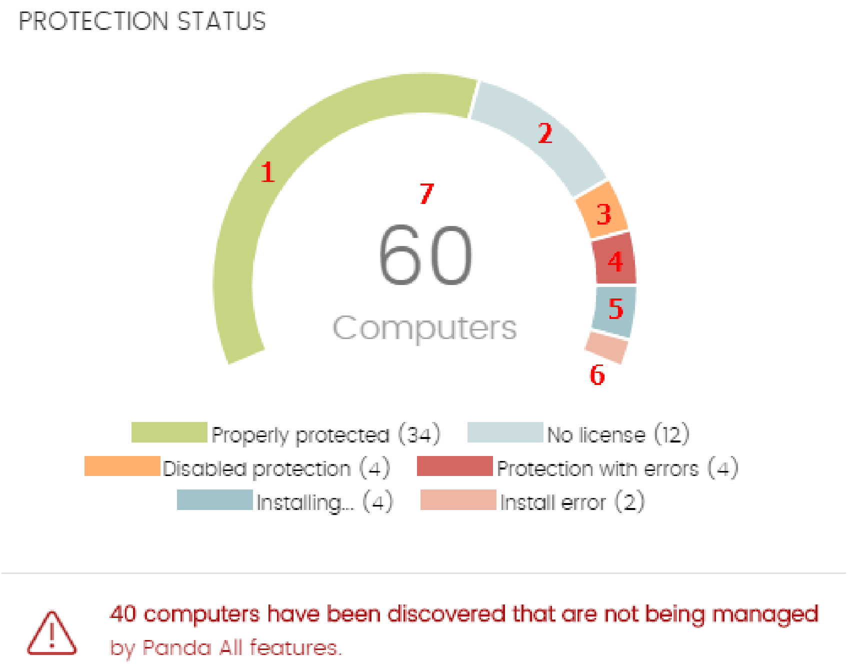
Data	Description
Properly protected	Percentage of computers where Panda Endpoint Protection installed without errors and is working properly.

Table 16.1: description of the data displayed in the ‘Protection status’ panel

Data	Description
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...

Table 16.2: filters available in the 'Computer protection status' list

Hotspot	Filter
(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.

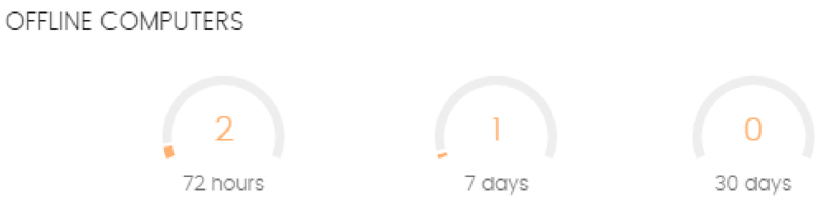


Figure 16.3: 'Offline computers' panel

- **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**

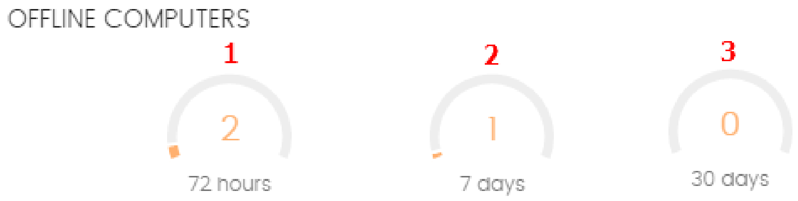


Figure 16.4: hotspots in the 'Offline computers' panel

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

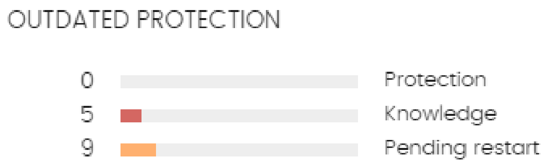


Figure 16.5: 'Outdated protection' panel

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**

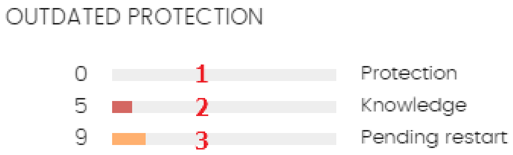


Figure 16.6: hotspots in the 'Outdated protection' panel

Click the hotspots shown in the figure 16.6 to access the **Computers with out-of-date** protection list with the following predefined filters:

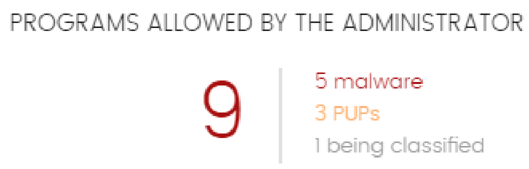
Hotspot	Filter
(1)	Updated protection = No.
(2)	Updated knowledge = No.
(3)	Updated protection = Pending restart.

Table 16.6: filters available in the 'Computers with out-of-date protection' list

Programs allowed by the administrator

> Panda Endpoint Protection *will allow the execution of all libraries and binaries used by the programs allowed by the administrator, except for those that are known threats.*

Panda Endpoint Protection prevents all programs classified as malware from running. If the administrator wants to allow an item classified as a threat to run, Panda Endpoint Protection implements tools to create an exclusion.



PROGRAMS ALLOWED BY THE ADMINISTRATOR

9

5 malware

3 PUPs

1 being classified

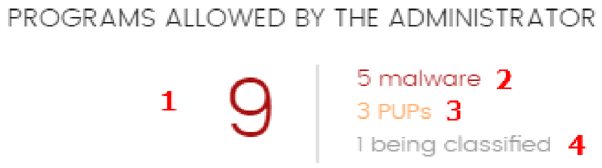
Figure 16.7: 'Programs allowed by the administrator' panel

- **Meaning of the data displayed**

The panel shows the total number of items excluded from blocking, broken down into three categories:

- Malware
- PUPs
- Being classified

- **Lists accessible from the panel**



PROGRAMS ALLOWED BY THE ADMINISTRATOR

1 9

5 malware 2

3 PUPs 3

1 being classified 4

Figure 16.8: hotspots in the ‘Programs allowed by the administrator’ panel

Click the hotspots shown in the figure 16.8 to access the **Programs allowed by the administrator** list with the following predefined filters:

Hotspot	Filter
(1)	No filter.
(2)	Current classification = Malware.
(3)	Current classification = PUP.
(4)	Current classification = Being classified (blocked and suspicious items).

Table 16.7: filters available in the 'Programs allowed by the administrator' list

Threats detected by the antivirus

Consolidates all the intrusion attempts that Panda Endpoint Protection has dealt with in the selected time period.

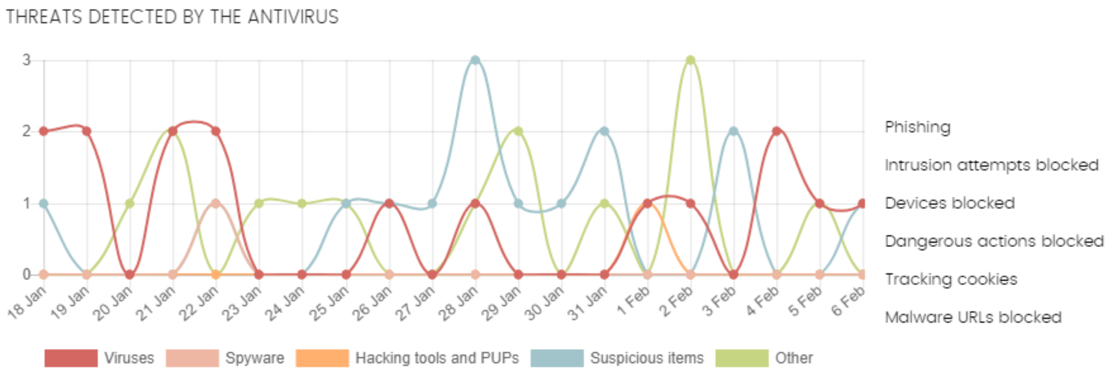


Figure 16.9: 'Threats detected by the antivirus' panel

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	Programs whose behavior leads Panda Endpoint Protection to conclude that they have a high probability of being malware.
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 16.8: 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
Intrusion	Attacks blocked by the firewall and the intrusion prevention system.
Devices	Peripheral devices blocked by the device control feature.
Dangerous operations	Detections made by analyzing local behavior.
Tracking cookies	Detection of cookies used to track users' Web activity.
Malware URLs	Web addresses that point to pages containing malware.

Table 16.9: description of the data displayed in the 'Threats detected by the antivirus' panel

- **Lists accessible from the panel**

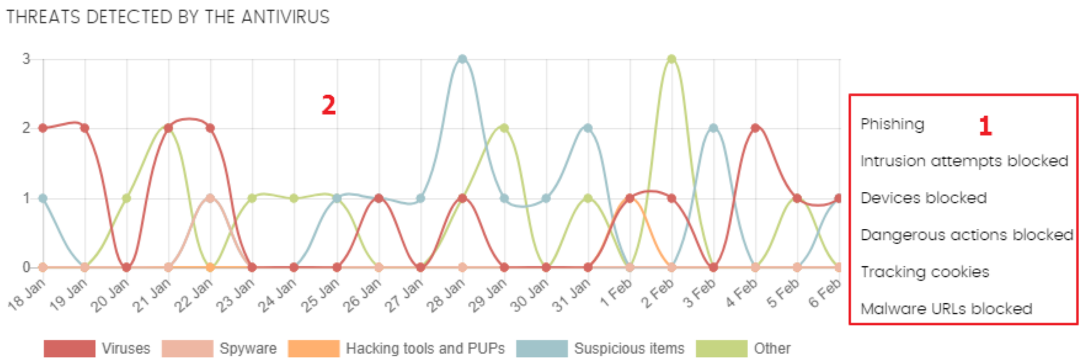


Figure 16.10: hotspots in the 'Threats detected by the antivirus' panel

Click the hotspots shown in the figure 16.10 to access the **Threats detected by the antivirus** list with the following predefined filters.

Hotspot	Filter
(1)	Threat type = Phishing OR Intrusion attempts blocked OR Devices blocked OR Dangerous operations blocked OR Tracking cookies OR Malware URLs.
(2)	No filter.

Table 16.10: lists accessible from the 'Classification of all programs run and scanned' panel

Security lists

'Computer protection status' list

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.

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Endpoint Protection folder tree to which the computer belongs.	• Character string • 'All' group • Native group • Active Directory group

Table 16.11: fields in the 'Computer protection status' list

Field	Description	Values
Antivirus	Antivirus protection status	• Installing • 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).
Last connection	Date when the Panda Endpoint Protection status was last sent to Panda Security's cloud.	Date

Table 16.11: 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 • Mobile device • 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	Description assigned to the computer.	Character string

Table 16.12: fields in the 'Computer protection status' exported file

Field	Description	Values
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**	Status of the associated protection.	• Not installed • Error • Enabled • Disabled • No license
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

Table 16.12: fields in the 'Computer protection status' exported file

Field	Description	Values
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 16.12: fields in the 'Computer protection status' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
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 • 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
Knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Protection status	Status of the protection module installed on the computer.	• Installing... • Properly protected • Protection with errors • Disabled protection • No license • Installation error

Table 16.13: filters available in the 'Computer protection status' list

'Programs allowed by the administrator' list

This list shows in detail all the items being classified, or classified as threats, which the administrator has allowed to run.

This list can only be accessed from the Programs allowed by the administrator widget.

Field	Description	Values
Program	Name of the malware or PUP allowed to run. If it has not been identified, the name of the file will be specified instead.	Character string
Current classification	Type of threat.	• Malware. • PUP. • Blocked. • Blocked reclassified as Malware/PUP. • Blocked reclassified as Goodware.
Threat	Threat name.	Character string
Hash	String identifying the file.	Character string
Allowed by	Console user that created the exclusion.	Character string
Allowed since	Date when the administrator created the exclusion.	Date
Delete 🗑	Lets you remove the exclusion.	

Table 16.14: fields in the 'Programs allowed by the administrator' list

- **Fields displayed in the exported file**

Field	Description	Values
Program	Name and path of the file allowed to run.	Character string
Current type	Current classification of the file.	• Malware. • PUP. • Blocked. • Blocked reclassified as Malware/PUP. • Blocked reclassified as Goodware.

Table 16.15: fields in the 'Programs allowed by the administrator' exported file

Field	Description	Values
Original type	Original classification of the file when it was allowed to run.	• Malware. • PUP. • Blocked. • Blocked reclassified as Malware/PUP. • Blocked reclassified as Goodware.
Threat	Name of the malware or PUP allowed to run. If it has not been identified, the name of the file will be specified instead.	Character string
Hash	String identifying the file.	Character string
Allowed by	Console user that created the exclusion.	Character string
Allowed since	Date when the administrator created the exclusion.	Date

Table 16.15: fields in the 'Programs allowed by the administrator' exported file

- **Filter tool**

Field	Comments	Values
Search	• **Threat**: name of the malware or PUP. • **Allowed by**: console user that created the exclusion. • **Program**: name of the file that was allowed to run. • **Hash**: string identifying the file.	Character string
Current classification	Current classification of the file.	• Malware. • PUP. • Goodware • Being classified (blocked and suspicious items).
Original classification	Original classification of the file when it was allowed to run.	• Malware. • PUP. • Blocked. • Suspicious item.

Table 16.16: filters available in the 'Programs allowed by the administrator' list

'History of programs allowed by the administrator' list

This list displays a history of all events that have taken place over time with respect to the threats and unknown files that the administrator has allowed to run.

This list is not accessible through any panels in the dashboard. To access it, click the **History** link in the top right corner of the **Programs allowed by the administrator** screen.

Field	Description	Values
Program	Name and path of the file allowed to run.	Character string
Current classification	Current classification of the threat.	• Malware • PUP • Blocked. • Suspicious item.
Threat	Name of the malware or PUP allowed to run. If it has not been identified, the column will display the file's name instead.	Character string
Hash	String identifying the file.	Character string
Action	Action taken on the allowed item.	• Exclusion removed by the user. • Exclusion removed after reclassification. • Exclusion added by the user. • Exclusion kept after reclassification.
User	User account under which the file was allowed.	Character string
Date	Date the event took place.	Date

Table 16.17: fields in the 'History of programs allowed by the administrator' list

- **Fields displayed in the exported file**

Field	Description	Values
Program	Name of file that was allowed to run.	Character string
Current type	Current classification of the allowed threat.	• Malware • PUP • Blocked • Suspicious item
Original type	Original classification of the file when it was allowed to run.	• Malware • PUP • Blocked • Suspicious item
Threat	Name of the malware or PUP allowed to run. If it has not been identified, the column will display the file's name instead.	Character string

Table 16.18: fields in the 'History of programs allowed by the administrator' exported file

Field	Description	Values
Hash	String identifying the file.	Character string
Action	Action taken on the allowed item.	• Exclusion removed by the user. • Exclusion removed after reclassification. • Exclusion added by the user. • Exclusion kept after reclassification.
User	User account under which the file was allowed.	Character string
Date	Date the event took place.	Date

Table 16.18: fields in the 'History of programs allowed by the administrator' exported file

- **Filter tool**

Field	Description	Values
Search	• **User**: user account under which the file was allowed. • **Program**: name of the file that was allowed to run. • **Hash**: string identifying the file.	Character string
Current classification	Current classification of the file.	• Malware. • PUP. • Goodware. • Being classified (blocked and suspicious items).
Original classification	Original classification of the file when it was allowed to run.	• Malware. • PUP. • Being classified (blocked item). • Being classified (suspicious item).
Action	Action taken on the allowed item.	• Exclusion removed by the user. • Exclusion removed after reclassification.

Table 16.19: filters available in the 'History of programs allowed by the administrator' list

Field	Description	Values
		• Exclusion added by the user. • Exclusion kept after reclassification

Table 16.19: filters available in the 'History of programs allowed by the administrator' list

‘Threats detected by the antivirus’ list

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

Table 16.20: fields in the 'Threats detected by the antivirus' list

Field	Description	Values
Date	Date when the item was detected.	Date

Table 16.20: 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
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. • Anti-spam for Exchange. • Content filtering for Exchange.

Table 16.21: fields in the 'Threats detected by the antivirus' exported file

Field	Description	Values
		• Mailbox protection for Exchange. • Transport protection for Exchange. • File protection. • Firewall. • Mail protection. • Advanced protection. • On-demand scan. • Web access control. • 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
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 16.21: 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

Table 16.22: filters available in the 'Threats detected by the antivirus' list

Field	Description	Values
Threat type	Type of threat.	• Virus. • Spyware. • Hacking tools and PUPs. • Phishing. • Suspicious items. • Dangerous actions blocked. • Tracking cookies. • Malware URLs. • Other.

Table 16.22: filters available in the 'Threats detected by the antivirus' list

'Blocked devices' list

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
Group	Folder within the Panda Endpoint Protection folder tree that the computer belongs to.	• Character string • 'All' group • Native group • Active Directory group
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 16.23: 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
Name	Name of the peripheral connected to the computer and affected by the security settings.	Character string
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 16.24: 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
Device type	Type of device affected by the security settings.	• Removable storage drives. • Imaging devices • CD/DVD drives. • Bluetooth devices. • Modems. • Mobile devices.

Table 16.25: filters available in the 'Blocked devices' list

'Intrusion attempts blocked' list

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 section "**Block intrusions**" on page **190** for more information on each type of network attack.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check

Table 16.26: fields in the 'Intrusion attempts blocked' list

Field	Description	Values
		• 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 16.26: 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 section “**Block intrusions**” on page **190** 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

Table 16.27: fields in the 'Intrusion attempts blocked' exported file

Field	Description	Values
		• 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
Action	Action taken by the firewall according to its settings. Refer to section "**Firewall (Windows computers)**" on page **185** 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 16.27: 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 section "**Block intrusions**" on page **190** 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
Computer type	Type of device.	- All computer types - Workstation - Laptop - Mobile device - Server

Table 16.28: filters available in the 'Intrusion attempts blocked' list

Chapter 17

Managing threats, quarantined items and items being classified

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 the use of several configurable tools.

CHAPTER CONTENT

Introduction to threat management tools

The solution provides several tools to manage defected threats and unknown files in the process of classification:

- Tools for managing the execution of processes classified as malware.
- Tools for managing the quarantine area.

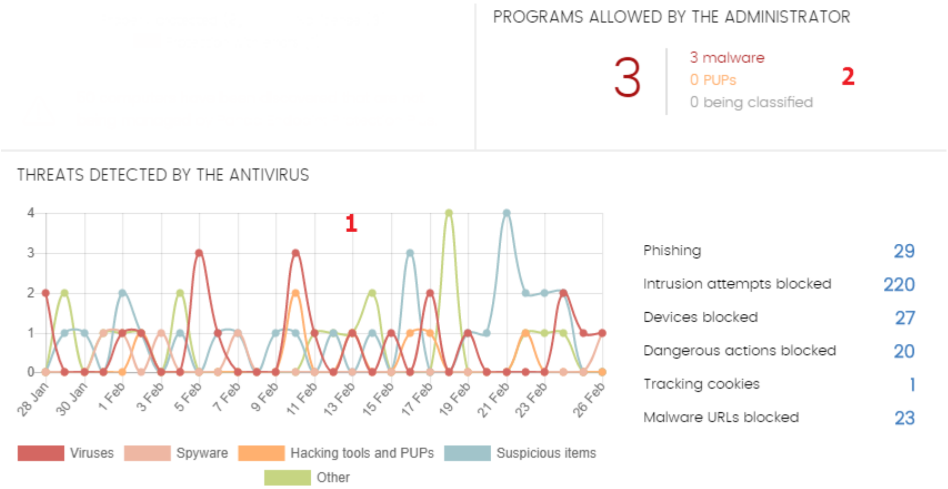
Tools for managing the execution of processes classified as malware

In some cases, the administrator may want to allow the execution of certain types of malware which, despite posing a potential threat, provide features valued by users. This is the case of PUPs, for example. These include toolbars that offer search capabilities but also collect users' private data and confidential corporate information for advertising purposes.

Tools for managing the quarantine area

The quarantine area provides administrators with access to items classified as threats and deleted from users' computers.

Tools for managing threats



Phishing	29
Intrusion attempts blocked	220
Devices blocked	27
Dangerous actions blocked	20
Tracking cookies	1
Malware URLs blocked	23

Figure 17.1: dashboard tools for managing blocked and excluded items

Blocked and excluded items are managed through tools available in the **Status** area of the management console. Below is a quick reference guide for you to find each of these tools.

As previously said, all of these tools are accessible from the **Status (1)** menu at the top of the console**.** Click the appropriate widget shown in figure 17.1.

Tools for displaying the items blocked by Panda Endpoint Protection

- **To get a list of currently blocked items classified as viruses:** 'Threats detected by the antivirus' panel **(1)**.

Tools for displaying items excluded from blocking by the administrator

- **To get a list of all programs classified as a virus and excluded from blocking:** 'Programs allowed by the administrator' panel **(2)**.
- **To get a history of currently excluded programs:** 'Programs allowed by the administrator' panel **(2)**, 'History' link.

- **To see the state changes of excluded programs:** 'Programs allowed by the administrator' panel **(2)**, 'History' link.

Tools for adding and removing exclusions

- **To add a threat exclusion**: 'Threats detected by the antivirus' panel **(2)**, select a threat, click **Restore and do not detect again**.
- **To remove an exclusion:** 'Programs allowed by the administrator' panel **(2)**, select a threat and click the 🗑 icon.

Unblocking items

Excluding items classified as threats

By excluding an item classified as malware from the scans you are allowing the execution of a program that Panda Endpoint Protection has effectively classified as harmful or dangerous.

To do that, go to the **Threats detected by the antivirus** screen, select the threat and click the **Restore and do not detect again** button.

Once excluded from the scans, the item in question will be added to the **Programs allowed by the administrator** list, as explained in the next section.

Managing excluded items

To manage excluded items, as well as configuring the solution's behavior when an unknown item or a known item classified as a threat is reclassified, go to the **Programs allowed by the administrator** screen.

This screen lets you view and manage currently allowed files, as well as accessing a history of all excluded items.

Viewing current exclusions

The **Programs allowed by the administrator** screen displays items with an active exclusion. Every item on the list is allowed to run.

History

Additionally, click the **History** link to view a history of all files excluded via Panda Endpoint Protection and the actions taken on them. This list allows you to view all the states that a file has gone through, from the time it entered the Programs allowed by the administrator list until it exited it, as well as all intermediate states.

Managing the backup/quarantine area

Panda Endpoint Protection's quarantine is a backup area that stores items 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. Thus, it is not possible to directly access or run quarantined items, unless you do it using the Web console's restore tool.

> *The quarantine is compatible with Windows, macOS and Linux devices. Android is not supported.*

Panda Endpoint Protection also quarantines suspicious files automatically, based on the conditions defined by Panda Security's PandaLabs department.

Once a suspicious item is quarantined for further analysis, there are four possible scenarios:

- **If the item is classified as malicious and there is a disinfection routine for it:** it is disinfected and restored to its original location.
- **If the item is classified as malicious, but there is no disinfection routine for it**: it is quarantined for seven days.
- **If the item is identified as harmless:** it is restored to its original location:
- **If the item is categorized as suspicious:** it is quarantined for a maximum of 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 actually sent to the backup area.*

Viewing quarantined items

You can view quarantined items through the **Threats detected by the antivirus** widget and its associated list.

Quarantined items will display **Quarantined** or **Deleted** in the **Action** column.

Restoring items from quarantine

To restore an item from quarantine, click the **Restore and do not detect again** button. This will copy the item to its original location and restore its original permissions, owner, as well as the registry keys and any other information associated with the file.

Chapter 18

Alerts

The alert system is a resource provided by Panda Endpoint Protection to quickly notify administrators of important situations in order to ensure the proper 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.

Configuring email alerts

Go to the **Settings** menu at the top of the Web console. Then, click **My alerts** from the left-hand menu. This screen lets you specify the email addresses to send messages to (**Send the alerts to the following address**). You can also enable and disable each of the alert types to send.

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.
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 and installation 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.

Table 18.1: alert table

Type	Frequency	Condition	Information displayed
			• 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.
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.

Chapter 19

Reports

Panda Endpoint Protection allows administrators to generate and send, automatically or manually, executive reports that consolidate all the information collected by the solution in the selected period.

CHAPTER CONTENT

On-demand generation of executive reports

- Go to the **Status** menu at the top of the console, and click the **Executive report** option from the left-hand menu. This will open the report settings window. This window is divided into two tabs: **View** and **Schedule**.
- Click the **View** tab to configure an executive report and display it immediately.

Information required to generate an on-demand report

Field	Description
Dates	Lets you specify the time interval to be covered in the report. • Last year • Last month. • Last 7 days. • Last 24 hours.
Computers	Lets you specify the computers to extract information from: • **All computers**. • **Selected groups:** displays the group tree. Use the checkboxes to select the groups you want.

Table 19.1: information required to generate an on-demand report

Field	Description
Content	Lets you select the type of information to be included in the report: • **License status**: shows the number of contracted and used licenses, and their expiration date. For more information, refer to section "**Viewing contracted licenses**" on page **110**. • **Security status**: shows the way the Panda Endpoint Protection software is working on those computers where it is installed. It includes information from the **Protection status** widget, and the following sections: **Online computers**, **Up-to-date protection** and **Up-to-date knowledge**. • **Detections:** shows the threats detected across the network. It includes information collected from the following widgets and lists: • Top 10 computers with most detections. • Threats detected by the antivirus. Refer to section "**Security panels/widgets**" on page **250** for more information. • **Available patches**: shows the patch status of the computers on the network. • Patch management status. • Time since last check. For more information, refer to section "**Panda Patch Management widgets and panels**" on page **205**.

Table 19.1: information required to generate an on-demand report

Once you have finished configuring the settings, click the **View** button to display the report in a new window.

Make sure that neither your Internet browser nor any installed extension blocks the display of pop-ups.

Scheduled sending of executive reports

- Go to the **Status** menu at the top of the console, and click the **Executive report** option from the left-hand menu. This will open the report settings window. This window is divided into two tabs: **View** and **Schedule**.
- Click the **Schedule** tab to configure a scheduled executive report.

Information required to generate a scheduled report

The scheduled reports window displays a list of all configured reports.

- Click **Add** to add a new scheduled report.
- To delete a configured report, click the 🗑 icon.
- To edit a configured report, click its name.

To configure a scheduled report, enter the following information:

Field	Description
Name	Name of the scheduled report. This will be displayed on the list of configured reports.
Send automatically	Lets you schedule the sending of the executive report, or save the settings without sending the report.
Date and frequency	Lets you specify the day when the report will be sent and its frequency. • Every day • Every week • Every month The content of the drop-down menus will vary depending on your selection.
The following information	This section displays the following settings: **Dates**, **Computers** and **Content:** • **Dates:** lets you specify the time interval to be covered in the report. • Last year • Last month • Last 7 days • Last 24 hours • **Computers:** lets you specify the computers to extract information from. • **All computers** • **Selected groups:** displays the group tree. Use the checkboxes to select the groups you want. • **Content**: this section lets you select the type of information to be included in the report: • **License status**: shows the number of contracted and used licenses. Refer to section "**Viewing contracted licenses**" on page **110** for more information. • **Security status**: shows the way the Panda Endpoint Protection software is working on those computers where it is installed. It includes information from the **Protection status** widget, and the following sections: **Online computers**, **Up-to-date protection** and **Up-to-date knowledge**. • **Detections**: shows the threats detected across the network. It includes information collected from the following widgets and lists: • Top 10 computers with most detections.

Table 19.2: information required to generate a scheduled report

Field	Description
	• Threats detected by the antivirus. Refer to section "**Security panels/widgets**" on page **250** for more information. • **Available patches**: shows the patch status of the computers on the network. • Patch management status. • Time since last check. For more information, refer to section "**Panda Patch Management widgets and panels**" on page **205**.
To	Enter the email address that the report will be sent to. You can enter multiple addresses separated by commas.
CC	Enter the email address that will receive a copy of the report. You can enter multiple addresses separated by commas.
BCC	Use this field to send a copy of the report to a recipient without notifying other recipients that this was done. You can enter multiple addresses separated by commas.
Subject	Specify the email subject line.
Format	Select the format of the email attachment (the report): PDF, Excel, or Word.
Language	Select the language of the report.

Table 19.2: information required to generate a scheduled report

Parte 6

Security incident and 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 chapter "***Security settings for workstations and servers***" on page* **181** *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.
- **Exchange protection**: detects malware and spam received in the mail server's mailboxes.

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

> *Refer to chapter "***Tasks***" on page* **297** *for more information on how to run tasks on workstations and servers, view their results and change their settings.*

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.

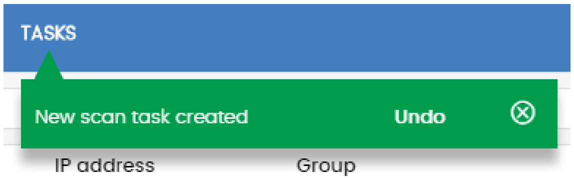
- Go to the **Computers** menu at the top of the console. From the panel on the side, click the 🗀 icon to display the computer tree's folder view.
- From the computer tree, click the context menu icon of the group whose computers you want to scan and disinfect. The context menu of the relevant branch 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 **298**.

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 section "**Task schedule and frequency**" on page **299** for more information.
- **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 **298**. 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.

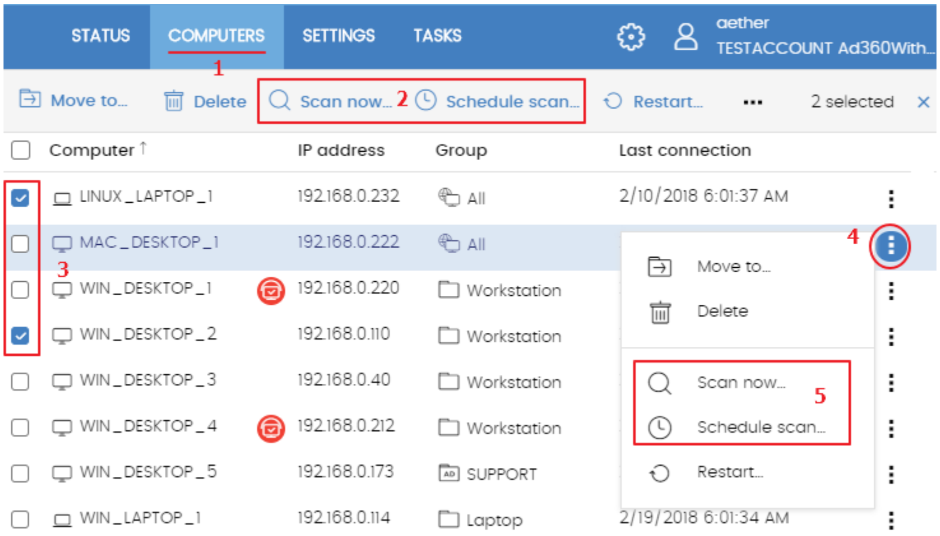
Creating a task from the Computers list

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 **298**.

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 **298**.

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 computer software is scanned statically (without running it). This reduces the chance of detecting certain types of threats. Select this option to use heuristic scanning algorithms and improve detection ratios.
Scan compressed files	This option decompresses compressed files and scans their contents.
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.

Table 20.2: scan options

Value	Description
	• **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

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.

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 stage (scheduled task).

CHAPTER CONTENT

General process of launching a task

The process of launching a task is divided into three steps:

- **Task creation and configuration**: select the computers, the characteristics of the task, the time/date, the frequency, and the way it will behave in the event of an error.

- **Task publication**: once you create a task, you must activate it by entering it in the Panda Endpoint Protection task scheduler. Activated tasks will be run on the scheduled day/time.
- **Task execution**: the task will be run when the configured conditions are met.

Introduction to task creation

Depending on your need to configure all parameters of a task, these can be set up from different areas of the management console:

- Tasks area
- Computer tree
- Computers area
- Lists

The primary resource to create a task is the **Tasks** area accessible from the menu at the top of the console. This area lets you create tasks from scratch, defining all related aspects (recipients, execution time, repetition interval, publication, etc.).

The **Computers** area, the **computer tree** and the lists let you schedule and launch task easily and quickly, without having to go through the entire process of configuring and publishing the task. However, they provide less configuration flexibility.

Creating a task from the Tasks area

To create a task, click the **Tasks** menu at the top of the console. A window will appear where you will see all created tasks, and their status. To create a new task, click **Add task** and select a task type from the drop-down menu. A window will be displayed with the task details, divided into three areas:

- **Overview**: task name and description.
- **Recipients**: computers that will receive the task.
- **Schedule**: task schedule (day and time).

Task recipients

- Click the **No recipients selected yet** link in the **Recipients** section. This will open a window from which to select the computers that will receive the configured task.

- Click ⊕ to add computers, and 🗑 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.*

Task schedule and frequency

You can configure the following parameters:

- **Starts:** indicates the task start time/date.
- **Maximum run time**: indicates the maximum time that the task can take to complete. After that time interval, the task will be canceled returning an error.
- **Repeat**: indicates the frequency of the task from the time/date indicated in the **Starts** field**.**
- **Starts**

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 date, 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 for the computer to be available to launch the task.

Table 21.1: task launch parameters

- **Maximum run time**

Value	Description
No limit	There is no time limit for the task to complete.

Table 21.2: task duration parameters

Value	Description
1, 2, 8 or 24 hours	There is a time limit for the task to complete. After that time interval, the task will be canceled returning an error.
Repeat	Indicates a repeat interval (every day, week or month) from the date specified in the **Starts** field**.**

Table 21.2: task duration parameters

Task publication

Once you have created and configured a task, it will be added to the list of configured tasks. However, the task will not be active until it is published.

To publish a task, click the **Publish now** button. It will be added to the Panda Endpoint Protection task scheduler, which will launch the task based on its settings.

Task management

Click the **Tasks** menu at the top of the console to list, delete, copy, cancel or view the results of created tasks.

List of created tasks

This list shows details of all created tasks, their type, status and other relevant information.

Field	Comments	Values
Icon	The task type	• 🩹 Patch installation task • 🔍 On-demand scan task • ⛑ Disinfection task (immediate scan)
Name	Task name	Character string
Date	Date when the task was created	Date

Table 21.3: fields in the 'Tasks' list

List filter tool

Field	Comments	Values
Type	The task type	• Scan • Disinfection • Patch installation
Search task	Task name	• Character string
Schedule	Task frequency	• All • Immediate • One-time • Scheduled
Sort list	Sorting order for the tasks on the list	• Sort by creation date • Sort by name • Ascending • Descending

Table 21.4: filters available in the 'Tasks' list

Modifying a published task

Click a task's name to display its settings window. There you will be able to edit any of the task's settings.

Published tasks only allow you to change their name and description. To be able to modify a published task, you must copy it.

Canceling a published task

To cancel a published task, click the **Cancel** link. The task will be canceled, but it won't be deleted from the task window so you will still be able to view its results.

Deleting a task

Executed tasks are not deleted automatically. To delete them, you must click the 🗑 icon.

Deleting a task also deletes its results.

Copying a task

Click a task's ⧉ icon to copy it. The new task will have the same settings as the original one.

Viewing a task's results

You can view the current results of any published task by clicking the **View results** link. A window with the results will appear, along with some filters for you to search for specific information.

Field	Description	Values
Computer	Name of the computer where the task took place	Character string
IP address	The computer's primary IP address.	Character string
Status	• **Pending**: the task was launched, but the target computer was not accessible. A wait period starts based on the task settings. • **In progress**: the task is underway. • **Success**: the task finished successfully. • **Failed**: the task failed, returning an error. • **Expired**: the task didn't even start as the configured period expired. • **Canceled**: the task was manually canceled.	Character string
Start date	Task start date.	Date
End date	Task end date.	Date
Detections	Number of detections made on the computer.	Numeric value

Table 21.5: fields available in task results

Task filter tool

Field	Description	Values
Date	Drop-down menu with the date when the task became 'Active' based on the configured schedule. A task will launch immediately, or wait until the target machine is available. This date is specified in the Date column.	Date

Table 21.6: task search filters

Field	Description	Values
Status	• **Pending**: the task has not been run yet as the execution window has not been reached. • **In progress**: the task is underway. • **Success**: 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 of starting the task or during the defined interval. • **Canceled**: the task was manually canceled. • **Canceled (maximum run time exceeded)**: the task was automatically canceled because it exceeded the task's maximum configured run time.	Enumerator

Table 21.6: task search filters

Editing a task

To edit an already created or published task, click its name. This will open the task editing window. This window contains the same fields as the task creation window.

To view the list of computers that will receive a task, click the **View computers** button. This will take you to the **Computers** area, with a computer list filtered by the selected task.

Changing the recipients of tasks

The set of computers that will receive a task may be difficult to determine due to the following reasons:

- Groups are dynamic entities that may change over time.
- Tasks are actions taken on groups and defined at a certain moment in time, although they can be run (repeatedly or not) at a later time.

That is, you can define a task at a specific time (T1) to be run on one or several groups containing a series of computers. However, at the time when the task is run (T2), the computers in those groups 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.
- Scheduled one-time tasks.
- Scheduled recurring 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 task

It is not possible to add new computers to an existing immediate task. Even if you add new computers to the target group, they won't receive the task.

Removing computers from the task

However, you can remove computers from an existing task. If you move a computer from the group set to receive the task to another group, the affected computer won't run the task.

Scheduled one-time tasks

There are two possible scenarios with these tasks:

Tasks which started running less than 24 hours ago

Within the first 24 hours after a task is launched, it is still possible to add or remove computers from the task or 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. However, you can cancel the task on a computer by removing it from the target group.

Scheduled recurring tasks

These tasks allow the addition and removal of target computers at any time before they are canceled or completed.

The status of the task on each computer will be shown gradually in the console as Aether Platform receives the relevant information from each machine.

Part 7

Additional information about Panda Endpoint Protection

Chapter 22: Hardware, software and network requirements

Chapter 23: The Panda Account

Chapter 24: Supported uninstallers

Chapter 25: Key concepts

Chapter 22

Hardware, software and network requirements

Panda Endpoint Protection is a cloud service and, as such, the entire infrastructure required to provide the service to Panda Security's customers is hosted on the company's premises. This frees organizations from the need to deploy additional hardware or software across their corporate networks. Nevertheless, the computers and the network to protect need to meet a series of minimum requirements to ensure that the product operates properly.

CHAPTER CONTENT

Requirements for Windows platforms

Supported operating systems

Workstations

- 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)

Servers

- 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

Hardware requirements

- **Processor:** Pentium 1 GHz
- **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

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 Web filtering and malware detection to work.

Requirements for Linux platforms

Supported 64-bit distributions

- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS and 16.10
- Fedora 23, 24 and 25

Supported kernel versions

- **Minimum supported version**: 3.13
- **Maximum supported version**: 4.10

Supported file managers

- Nautilus
- PCManFM
- Dolphin

Hardware requirements

- **Processor:** Pentium 1 GHz
- **RAM:** 1.5 GB
- **Available hard disk space for installation:** 100 MB.
- **Ports:** ports 3127, 3128, 3129 and 8310 must be accessible for the Web filtering and malware detection to work.

- **Installation package dependencies:**

debconf (>= 0.5) | debconf-2.0	libfreetype6 (>= 2.3.5)	libpng12-0 (>= 1.2.13-4)	libxcb1
dkms (>= 1.95)	libgcc1 (>= 1:4.1.1)	libsm6, libssl1.0.0 (>= 1.0.0)	libxrender1
libc6 (>= 2.17)	libgl1-mesa-glx | libgl1	libstdc++6 (>= 4.6)	make
libc6-dev	libice6 (>= 1:1.0.0)	libstdc++6:i386	notify-osd
libcurl3:i386	libltdl7 (>= 2.4.2)	libuuid1 (>= 2.16)	notification-daemon
libcups2	libnl-3-200 (>= 3.2.7)	libuuid1:i386	python-nautilus (>= 1.1-4)
libdbus-1-3 (>= 1.1.1)	libnl-genl-3-200 (>= 3.2.7)	libx11-6	zlib1g (>= 1:1.1.4)
libfontconfig1 (>= 2.9.0)	libnotify-bin (>= 0.7.6)	libx11-xcb1	

Table 22.1: libraries required for installation

Requirements for Android platforms

Supported operating systems

- Ice Cream Sandwich 4.0
- Jelly Bean 4.1 - 4.2 - 4.3
- KitKat 4.4
- Lollipop 5.0/5.1
- Marshmallow 6.0
- • Nougat 7.0 - 7.1
- Oreo 8.0

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.

https://*.pandasecurity.com
http://*.pandasecurity.com
https://*.windows.net
https://repository.pandasecurity.com/aether
http://*.pandasoftware.com
http://*.globalsign.com
http://*digicert.com

Ports

- Port 80 (HTTP, WebSocket)
- Port 443 (HTTPS)

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

A Panda Account provides administrators with a safer mechanism to register and access the Panda Security services purchased by the organization, than the old method of receiving the relevant access credentials by email.

With a Panda Account, it is the administrator who creates and activates the access credentials to the Panda Endpoint Protection Web console.

CHAPTER CONTENT

Creating a Panda Account

Follow the steps below to create a Panda Account.

Open the email message received from Panda Security

- After purchasing Panda Endpoint Protection, you will receive an email message from Panda Security.
- Click the link in the message to access a site from which you will be able to create your Panda Account.

Fill out the form

- Fill out the form with the relevant data.
- Use the drop-down menu in the bottom-right corner if you want to change the language of the form.
- You can view the license agreement and privacy policy by clicking the corresponding links.
- Click **Create** to receive a message at the email address entered in the form. Follow the instructions in that message to activate your account.

Activating your Panda Account

Once you have created your Panda Account you will need to activate it. You can do this through the email message that you will receive at the email address you specified when creating your Panda Account.

- Find the message in your Inbox.
- Click the activation button. By doing that you will validate the email address that you provided when creating your Panda Account. If the button doesn't work, copy and paste the URL included in the message into your browser.
- The first time that you access your Panda Account you will be asked to confirm your password. Then, click **Activate account**.
- Enter the required data and click **Save data**. If you prefer to enter your data later, click **Not now**.
- Accept the terms and conditions of the License Agreement and click **OK**.

Once your Panda Account has been successfully activated, you will be taken to the Panda Cloud site home page. There, you will able to access your Panda Endpoint Protection Web console. To do that, simply click the solution's icon in the **My Services** section.

Chapter 24

Supported uninstallers

On installing Panda Endpoint Protection, other security products might be detected on the computer. In that case, Table 24.1 shows the products that will be automatically uninstalled before installing Panda Endpoint Protection across the network.

Vendor	Product name
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32-bit Edition) AVG Internet Security 2013 (64-bit Edition) AVG AntiVirus Business Edition 2013 (32-bit Edition) AVG AntiVirus Business Edition 2013 (64-bit Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32-bit* AVG Internet Security Business Edition 2011 64-bit (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVGFree v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir PersonalEdition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x Avira Antivirus 15.x

Table 24.1: list of uninstallers

Vendor	Product name
CA	CA Total Defense for Business Client V14 (32-bit Edition) CA Total Defense for Business Client V14 (64-bit Edition) CA Total Defense R12 Client (32-bit Edition) CA Total Defense R12 Client (64-bit Edition)
Bitdefender	BitDefender Endpoint Protection 6.x BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32-bit) Check Point Endpoint Security 8.x (64-bit)
Eset	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32-bit) ESET NOD32 Antivirus 4.X (32-bit) ESET NOD32 Antivirus 4.X (64-bit) ESET NOD32 Antivirus 5 (32-bit) ESET NOD32 Antivirus 5 (64-bit) ESET NOD32 Antivirus 6 (32-bit) ESET NOD32 Antivirus 6 (64-bit) ESET NOD32 Antivirus 7 (32-bit) ESET NOD32 Antivirus 7 (64-bit)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
iSheriff	iSheriff Endpoint Security 5.x

Table 24.1: list of uninstallers

Vendor	Product name
Kaspersky	Kaspersky Endpoint Security 11 for Windows (32bit- Edition) Kaspersky Endpoint Security 11 for Windows (64bit- Edition) Kaspersky Endpoint Security 10 for Windows (32-bit Edition) Kaspersky Endpoint Security 10 for Windows (64-bit Edition) Kaspersky Endpoint Security 8 for Windows (32-bit Edition) Kaspersky Endpoint Security 8 for Windows (64-bit Edition) Kaspersky Anti-Virus 2010 9.0.0.459* Kaspersky® Business Space Security Kaspersky® Work Space Security Kaspersky Internet Security 8.0, 7.0, 6.0 (with Windows Vista+UAC, UAC must be disabled) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (with Windows Vista+UAC, UAC must be disabled) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee LiveSafe 2016 x86/x64 McAfee SaaS Endpoint Protection 6.x, 5.x McAfee Endpoint Protection 10.5.x (64 bits) McAfee Endpoint Protection 10.5.x (32 bits) McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0 McAfee Internet Security Suite 2007 McAfee Total Protection Service 4.7* McAfee Total Protection 2008
Norman	Norman Security Suite 10.x (32-bit Edition) Norman Security Suite 10.x (64-bit Edition) Norman Security Suite 9.x (32.bit Edition) Norman Security Suite 9.x (64-bit Edition) Norman Endpoint Protection 8.x/9.x Norman Virus Control v5.99
Norton	Norton Antivirus Internet Security 2008* Norton Antivirus Internet Security 2007 Norton Antivirus Internet Security 2006
Microsoft	Microsoft Security Essentials 1.x Microsoft Forefront EndPoint Protection 2010 Microsoft Security Essentials 4.x Microsoft Security Essentials 2.0 Microsoft Live OneCare Microsoft Live OneCare 2.5*
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205
PC Tools	Spyware Doctor with AntiVirus 9.x
Sophos	Sophos Anti-virus 9.5 Sophos Endpoint Security and Control 10.2 Sophos Endpoint Security and Control 9.5 Sophos Anti-virus 7.6 Sophos Anti-virus SBE 2.5* Sophos Security Suite

Table 24.1: list of uninstallers

Vendor	Product name
Symantec	Symantect.cloud - Endpoint Protection.cloud 22.x Symantec.cloud - Endpoint Protection.cloud 21.x (32-bit) Symantec.cloud - Endpoint Protection.cloud 21.x (64-bit) Symantec EndPoint Protection 14.x (32-bit) Symantec EndPoint Protection 14.x (64-bit) Symantec EndPoint Protection 12.x (32-bit) Symantec EndPoint Protection 12.x (64-bit) Symantec EndPoint Protection 11.x (32-bit) Symantec EndPoint Protection 11.x (64-bit) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
Trend Micro	Trend Micro Worry-Free Business Security 9.x (32bit- Edition) Trend Micro Worry-Free Business Security 9.x (64bit- Edition) Trend Micro Worry-Free Business Security 8.x (32-bit Edition) Trend Micro Worry-Free Business Security 8.x (64-bit Edition) Trend Micro Worry-Free Business Security 7.x (32-bit Edition) Trend Micro Worry-Free Business Security 7.x (64-bit Edition) Trend Micro Worry-Free Business Security 6.x (32-bit Edition) Trend Micro Worry-Free Business Security 6.x (64-bit Edition) Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x Trend Micro OfficeScan 11.x
Comodo AntiVirus	Comodo Antivirus V 4.1 32-bit
Panda Security	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX and earlier versions Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX and earlier versions Panda Global Protection 2018* Panda Internet Security 2018* Panda Antivirus Pro 2018* Panda Gold Protection 2018*

Table 24.1: list of uninstallers

Vendor	Product name
	Panda Global Protection 2017* Panda Internet Security 2017* Panda Antivirus Pro 2017* Panda Gold Protection 2017* Panda Global Protection 2016* Panda Internet Security 2016* Panda Antivirus Pro 2016* Panda Gold Protection 2016* Panda Global Protection 2015* Panda Internet Security 2015* Panda Antivirus Pro 2015* Panda Gold Protection* Panda Free Antivirus Panda Global Protection 2014* Panda Internet Security 2014* Panda Antivirus Pro 2014* Panda Gold Protection* Panda Global Protection 2013* Panda Internet Security 2013* Panda Antivirus Pro 2013* Panda Global Protection 2012* Panda Internet Security 2012* Panda Antivirus Pro 2012* Panda Global Protection 2011* Panda Internet Security 2011* Panda Antivirus Pro 2011* Panda Antivirus for Netbooks (2011)* Panda Global Protection 2010 Panda Internet Security 2010 Panda Antivirus Pro 2010 Panda Antivirus for Netbooks Panda Global Protection 2009 Panda Internet Security 2009 Panda Antivirus Pro 2009 Panda Internet Security 2008 Panda Antivirus+Firewall 2008 Panda Antivirus 2008 Panda Internet Security 2007 Panda Antivirus + Firewall 2007 Panda Antivirus 2007
Webroot	Webroot SecureAnywhere 9

Table 24.1: list of uninstallers

* Panda 2017, 2016, 2015, 2014, 2013, 2012 products need a reboot to be uninstalled successfully.

* Comodo Antivirus V4.1 (32-bit) - Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

*F-Secure PSB for Workstations 9.00 - During the installation process of the Endpoint Protection agent on Windows 7 and Windows Vista systems, the user will be prompted to select the Allow option.

*AVG Internet Security Business Edition 2011 (32-bit) - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in several windows.

*AVG Internet Security Business Edition 2011 (64-bit) (10.0.1375) - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in several windows.

* Kaspersky Anti-Virus 6.0 for Windows workstations:

during the installation process of the Endpoint Protection agent on 64-bit platforms, the user will be prompted to select the Allow option in several windows.

To be able to uninstall the protection, the Kaspersky protection must not be password-protected.

Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* F-Secure PSB for Workstations 9.00 - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in two windows.

* AVG Anti-Virus Network Edition 8.5 - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in two windows.

* Panda Antivirus 2011 products do not uninstall correctly on 64-bit platforms. Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* Panda Cloud Antivirus 1.4 Pro and Panda Cloud Antivirus 1.4 Free - Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically on Windows Vista x64 systems.

* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically on Windows Vista x64 systems with UAC enabled.

* ESET NOD32 Antivirus 3.0.XX (2008) does not uninstall automatically on Windows Vista x64 systems.

* ESET NOD32 Antivirus 2.7*: after installing the Endpoint Protection agent on the computer, the system will restart automatically without displaying any notifications or asking for user confirmation.

* ESET NOD332 Antivirus 2.70.39*: after installing the Endpoint Protection agent on the computer, the system will restart automatically without displaying any notifications or asking for user confirmation.

* ESET Smart Security 3.0 does not uninstall automatically on Windows Vista x64 systems.

* Sophos Anti-virus SBE 2.5 does not uninstall correctly on Windows 2008 systems.

* eTrust Antivirus 7.1 does not uninstall correctly on 64-bit platforms.

* Norton Antivirus Internet Security 2008 does not uninstall correctly if the Windows Vista UAC is enabled.

* BitDefender Free Edition 2009 12.0.12.0: on Windows Vista systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

* Kaspersky Anti-Virus 2010 9.0.0.459: on systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

* Kaspersky Anti-Virus 8: on Windows Vista systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

* McAfee Total Protection Services 4.7. The uninstaller does not run correctly if UAC is enabled. Furthermore, 32-bit platforms require user intervention.

* Microsoft Live OneCare 2.5 does not uninstall correctly on Windows Small Business Server 2008.

If you have a program not included on this list, contact the relevant vendor to find out how to uninstall it before installing Panda Endpoint Protection on Aether.

Chapter 25

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.

Alert

See Incident.

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, anti-exploit techniques, 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.

ASLR (Address Space Layout Randomization)

Address Space Layout Randomization (ASLR) is a security technique used in operating systems to prevent buffer overflow-driven exploits. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. This prevents attackers from illegitimately using calls to certain system functions as they will not know where in memory those functions reside.

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.

Compromised process

A vulnerable process hit by an exploit attack in order to compromise the security of a user's computer.

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.

Exploit

Generally speaking, an exploit is a sequence of specially crafted data aimed at causing a controlled error in the execution of a vulnerable program. Once the error occurs, the compromised process will mistakenly interpret certain parts of the data sequence as executable code, taking malicious actions that may compromise the security of the target computer.

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.

Filter tree

Collection of filters grouped into folders, used to organize all computers on the network and facilitate the assignment of settings.

Folder tree

Hierarchical structure consisting of static groups, used to organize all computers on the network and facilitate the assignment of settings.

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 inspect suspicious programs based on hundreds of file characteristics. It can determine the likelihood that a program may take malicious 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.

Peer to Peer (P2P) functionality

Information transfer mechanism that uses the network bandwidth more efficiently on networks with nodes that work simultaneously as clients and servers, establishing a direct two-way communication.

Panda Endpoint Protection implements P2P connections to reduce bandwidth usage, as those computers whose signature file has been already updated will share the update locally with those computers that also need to update it.

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 functionality

This feature allows Panda Endpoint Protection to operate on computers without Internet access, accessing the Web through an agent installed on another computer on the same subnet.

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.

ROP

Return-oriented programming (ROP) is a computer security exploit technique that allows attackers to run arbitrary code in the presence of protection technologies such as DEP and ASLR.

Traditional stack buffer overflow attacks occurred when a program wrote to a memory address on the program's call stack outside of the intended data structure, which is usually a fixed-length buffer. However, those attacks were rendered ineffective when techniques such as DEP were massively incorporated into operation systems. These techniques prevent the execution of code in regions marked as non-executable.

In a ROP attack, the attacker gains control of the call stack to hijack program control flow and then executes carefully chosen machine instruction sequences that are already present in the machine's memory, called "gadgets". Chained together, these gadgets allow the attacker to perform arbitrary operations on the targeted machine.

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.

SCL (Spam Confidence Level)

Normalized value assigned to a message that indicates the likelihood that the message is spam, based on its characteristics (content, headers, etc.)

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 after having been scanned by the Panda Endpoint Protection protection installed on the user’s computer.

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.

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.

Vulnerable process

A program which, due to a programming bug, cannot interpret certain input data correctly. Hackers take advantage of specially crafted data packets (exploits) to cause vulnerable processes to malfunction, and run malicious code designed to compromise the security of the target computer.

Web access control

Technology that allows organizations to control and filter the URLs requested by the network's Internet browsers in order to allow or deny access to them, taking as reference a URL database divided into content categories.

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.