Panda Endpoint Protection Plus

Administration Guide Panda Endpoint Protection Plus

Author: Panda Security

Version: 9.50.00

Date: 7/1/2025

Legal notice.

Registered trademarks.

Contact information.

Corporate headquarters:

Panda Security

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 Spain.

https://www.pandasecurity.com/uk/about/contact/

About the Panda Endpoint Protection Plus Administration Guide

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

https://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONPLUSoAP-guide-EN.pdf

For more information about a specific topic, see the product's online help, available at:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/endpointprotectionplus/latest/en/index.htm

Release notes

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

https://info.pandasecurity.com/aether/?product=EPP&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, go to the following URL:

https://www.pandasecurity.com/en-us/support/endpoint-protection-plus-aether.htm

To access the eKnowledge Base portal, go to the following URL:

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

Panda Endpoint Protection Plus Administration Guide survey

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

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

Table of contents

Chapter 1

Preface

This Administration Guide contains basic information and procedures for making the most out of your Panda Endpoint Protection Plus product.

Chapter contents

Who is this Administration Guide for?

This guide is intended for 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 Plus?

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

- Panda Endpoint Protection Plus
- Aether platform

Panda Endpoint Protection Plus

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

Icons

The following icons are used in this Administration Guide:

Clarification or additional information, such as an alternative way of performing a certain task.

Suggestions and recommendations.

Additional information available in other sections of the Administration Guide.

Chapter 2

Panda Endpoint Protection Plus overview

Panda Endpoint Protection Plus 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 contents

Panda Endpoint Protection Plus benefits

Panda Endpoint Protection Plus is a security solution that leverages multiple protection technologies, enabling 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 Plus also enables organizations to monitor and control user productivity, preventing access to web resources not related to the company activity.

Panda Endpoint Protection Plus 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 Virtual Desktop Infrastructure (VDI) environments. Therefore, it provides a single tool to respond to the security needs of all computers on the corporate network.

Panda Endpoint Protection Plus features

Panda Endpoint Protection Plus is a product that enables organizations to manage the security of all computers across the network, without negatively impacting device performance and at the lowest possible total 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 real-time access to collective intelligence. The malware database has been moved from the user computer to the cloud.
- **Low network usage**: The number of downloads required has been reduced to the minimum.
- **Signature files shared across 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 user computers.

Cross-platform security

The solution covers all infection vectors on Windows, Linux, Android, and macOS devices.

- **Security for all infection vectors**: Browsers, email, file systems, and external devices connected to endpoints.
- **Security against unknown threats**: Through heuristic technologies and contextual analysis.
- **Security on all platforms:** Windows, Linux, macOS, and Android systems, and virtual environments (VMware, Virtual PC, MS Hyper-V, Citrix). Management of licenses belonging to both persistent and non-persistent Virtual Desktop Infrastructure (VDI) environments.

Easy to manage

- Easy-to-manage solution which does not require maintenance or additional infrastructure on the customer network.

- **Easy to maintain**: No specific infrastructure required to host the solution; the IT department can focus on more important tasks.
- **Easy protection for remote users**: Each computer protected with Panda Endpoint Protection Plus communicates with the cloud; remote offices and users are protected quickly and easily, with no additional installations or VPN configurations.
- **Easy to deploy**: Multiple deployment methods, with automatic uninstallers for competitor products to facilitate rapid migration from third-party solutions.
- **Smooth learning curve**: Simple, intuitive web-based management interface, with most-frequently used options one click away.

Maximum productivity

Email and Internet browsing are the main entry points for malware into organizations, and two key factors that affect employee productivity.

Email is a business-critical tool. However, studies reveal that 95 percent of corporate email is either infected, making email the most widely-used attack vector and one that requires the latest protection technologies.

Additionally, Internet browsing is affected by the most recent threats, such as bots, phishing, and malicious active content, capable of attacking users while they browse the Internet and infecting corporate networks.

Panda Endpoint Protection Plus monitors Internet browsing so that companies can focus on their core business and forget about employee unproductive behavior.

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.

The Aether platform manages communications with the agents deployed across the network. Its management console presents the data gathered by Panda Endpoint Protection Plus in a structured and easy 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 the 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 Panda Security products compatible with the platform:

Cloud management platform

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

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

Network administrators can access the management console at any moment and from anywhere, using any compatible Internet browser from a laptop, desktop, or even mobile devices such as tablets or smartphones.

It is a high-availability platform, operating 99.99% of the time. Network administrators do not 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 profiles and scheduled tasks to and from network devices is performed in real time, the moment that administrators apply the new settings profiles 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 nature of corporate IT infrastructures.

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 settings profiles, taking advantage of specific mechanisms such as inheritance and the assignment of settings profiles to individual devices. Network administrators can assign more detailed and specific settings profiles with less effort.

Complete, customized information

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

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

Aether architecture

Aether architecture is designed to be scalable in order to provide a flexible, 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 data consumers such as SIEM systems or mail servers, or web instances for requests for settings changes and the presentation of information to network administrators.

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

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

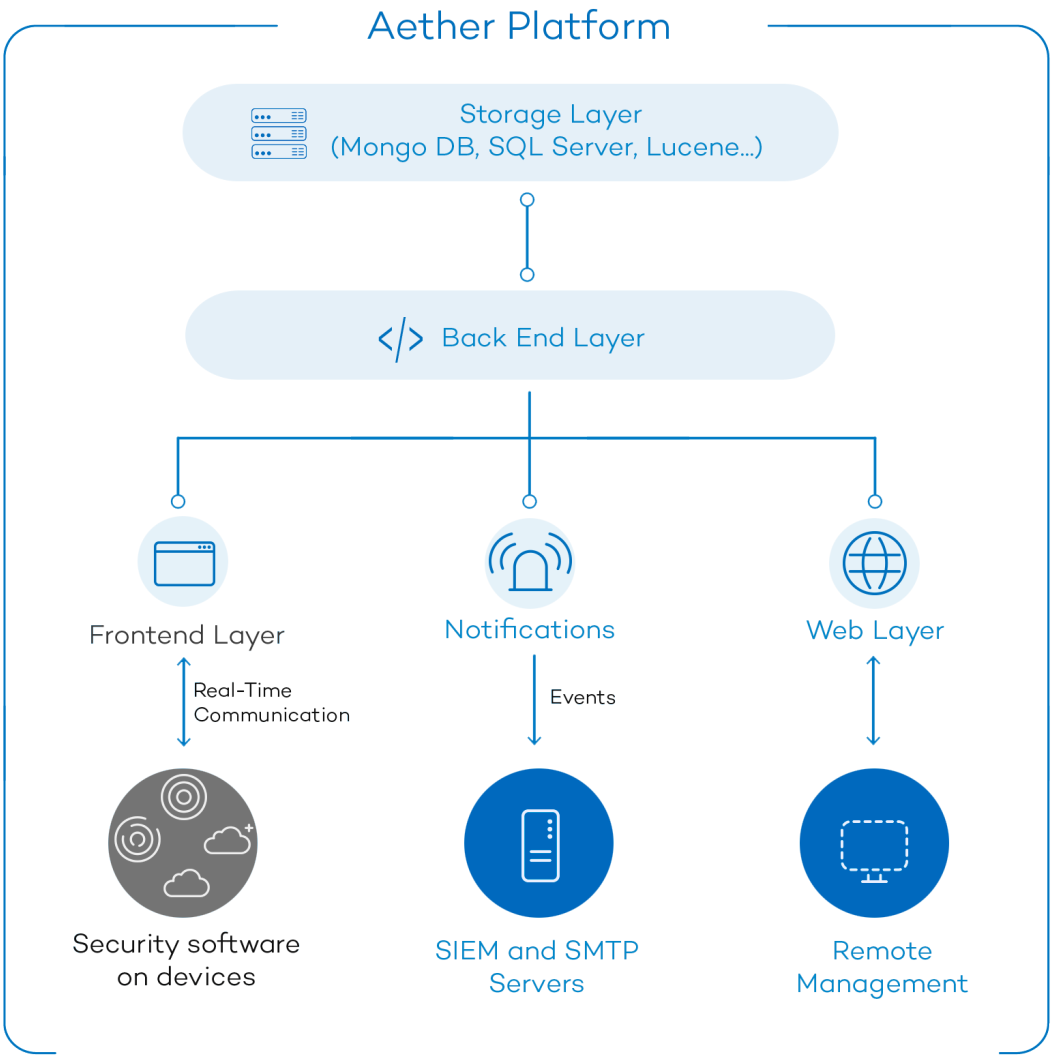


Figure 2.1: Logical structure of Aether

Aether on users' computers

Network computers protected by Panda Endpoint Protection Plus have a software program installed, consisting 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 profiles implemented by the administrator from the management console.
- **Panda Endpoint Protection Plus protection module**: This is responsible for providing effective protection for users' computers. To do this, it uses the communications agent to receive the security settings profiles and sends statistics and detection information as well as details of the items scanned.

Panda real-time communications agent

The Panda agent handles communications between managed computers and the Panda Endpoint Protection Plus 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.

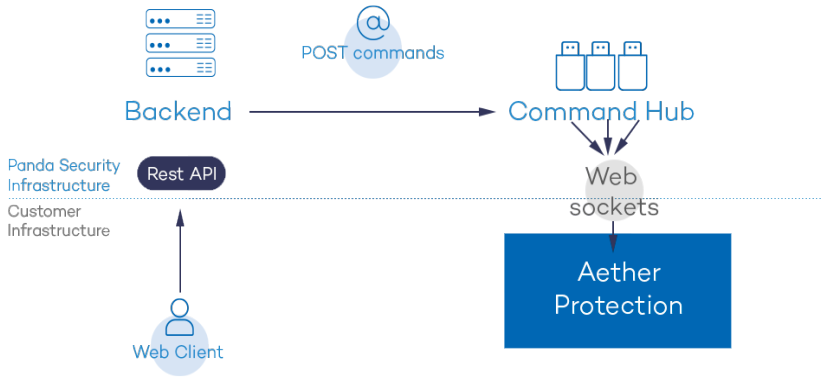


Figure 2.2: Flowchart of the commands entered through the management console

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 profiles configured by the network administrator through the Panda Endpoint Protection Plus 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 correctly.

Key components

Panda Endpoint Protection Plus is a cloud security service that shifts security intelligence and most scanning tasks to the IT infrastructure deployed in the Panda Security data processing centers. This results in an extremely lightweight security software with low resource usage and minimal operating requirements for organizations.

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

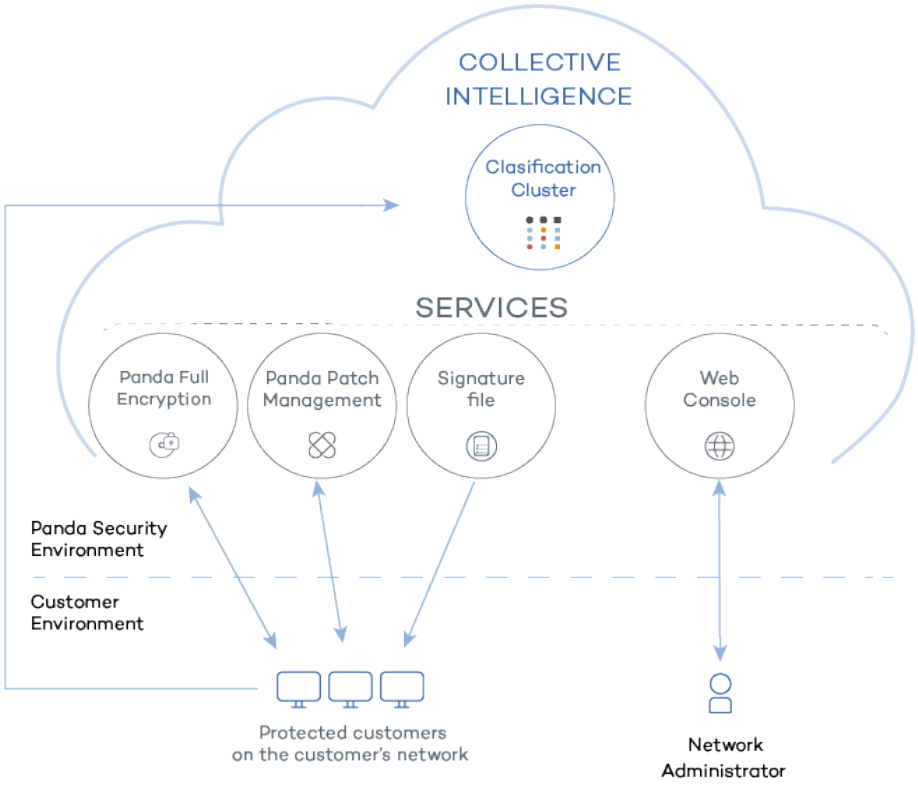


Figure 2.3: Panda Endpoint Protection Plus general structure

- **Collective intelligence servers**: Collect and classify the samples and evidence sent by the Panda Security customers. They also host a database of all detected threats, accessible in real time.
- **Signature file download servers**: Host the signature file downloaded by the Panda Security products.
- **Vulnerability assessment service**: Finds software with vulnerabilities and provides information about available patches.
- **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 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 Plus).
- The computer of the network administrator who 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 the Panda Security cloud-based infrastructure. It is worth noting that the Panda Endpoint Protection Plus 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 Plus to perform detection tasks. Because 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 and calculate the difference between those files and the published version, sending only the necessary data. This way, they reduce the customer's bandwidth costs in relation to updating the antivirus solution installed across their network.

Web management console server

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, see *Access to the web console on page 621.*

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

Computers protected with Panda Endpoint Protection Plus

Panda Endpoint Protection Plus 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 Plus protection module.

Panda Endpoint Protection Plus 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 Plus provides, in a single product, everything necessary to detect malware, as well as productivity management and remediation tools to disinfect compromised computers.

Panda Endpoint Protection Plus services

Panda Security provides other services, some of which are optional, which enable customers to integrate the solution into their current IT infrastructures and benefit directly from the security intelligence generated at Panda Security labs.

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. 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 enables organizations to roll back/uninstall those patches that support this feature, or exclude them from installation tasks, preventing them from being installed.

Vulnerability Assessment service

This free service searches for software with vulnerabilities on computers. To prevent malware from exploiting security holes to damage and infect workstations and servers, it informs about the availability of patches that can mitigate those vulnerabilities.

To centrally install available patches, you must have a Panda Patch Management license.

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 Endpoint Protection Plus uses Windows BitLocker and macOS FileVault technologies 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 enables you to 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 Plus is a managed service that offers security without administrator intervention, 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 detailed description of the platforms and requirements, see Product features and requirements on page 602.

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
- Microsoft Edge
- Firefox
- Opera

Languages supported in the web console

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

Chapter 3

The management console

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

- **It is adaptive**: Its responsive design allows the console to adapt to the size of the screen or web browser you are 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 your needs, enabling you to save settings for future use.
- **It is homogeneous**: It follows well-defined usability patterns to minimize your learning curve.
- **It is interoperable**: The data shown can be exported to `CSV` format with extended fields for later consultation.

Chapter contents

Benefits of the web console

The web console is the main tool with which administrators manage security. Because 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

Through the web console, administrators can deploy the Panda Endpoint Protection Plus installation package to all computers on the network, configure their security settings, monitor the protection status of the network, and benefit from remediation tools 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 remote 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 anywhere and at any time, using a smartphone, a notebook, a desktop PC, etc.

Access to the web console and requirements

Requirements for accessing the web console

- Valid credentials (user account and password) and a second authentication factor (optional). See Accessing, controlling, and monitoring the management console on page 53.
- Latest version of a supported web browser:
    - Google Chrome
    - Internet Explorer
    - Firefox
    - Opera
- Internet connection and communication through port 443 allowed.

Access to the web console

If your security provider is Panda Security:

- Open your web browser and go to https://www.pandacloudsecurity.com/PandaLogin/
- Type the credentials for your user account.

- If your user account has access to multiple different customer accounts, the **Select an account** page opens. Choose the customer whose console you want to access.
- The **Security** dashboard of the Panda Endpoint Protection Plus console opens.

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

- Go to https://www.watchguard.com/. Click **Log In** in the upper-right corner of the page.
- Type your WatchGuard credentials. The **Support Center** page opens.
- Click **MY WATCHGUARD** at the top of the page. A drop-down menu appears.
- Select **Manage Panda Products**. The Panda Cloud page opens, showing all purchased services.
- Click the Panda Endpoint Protection Plus tile. The **Security** dashboard of the management console opens.

General structure of the web console

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

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

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

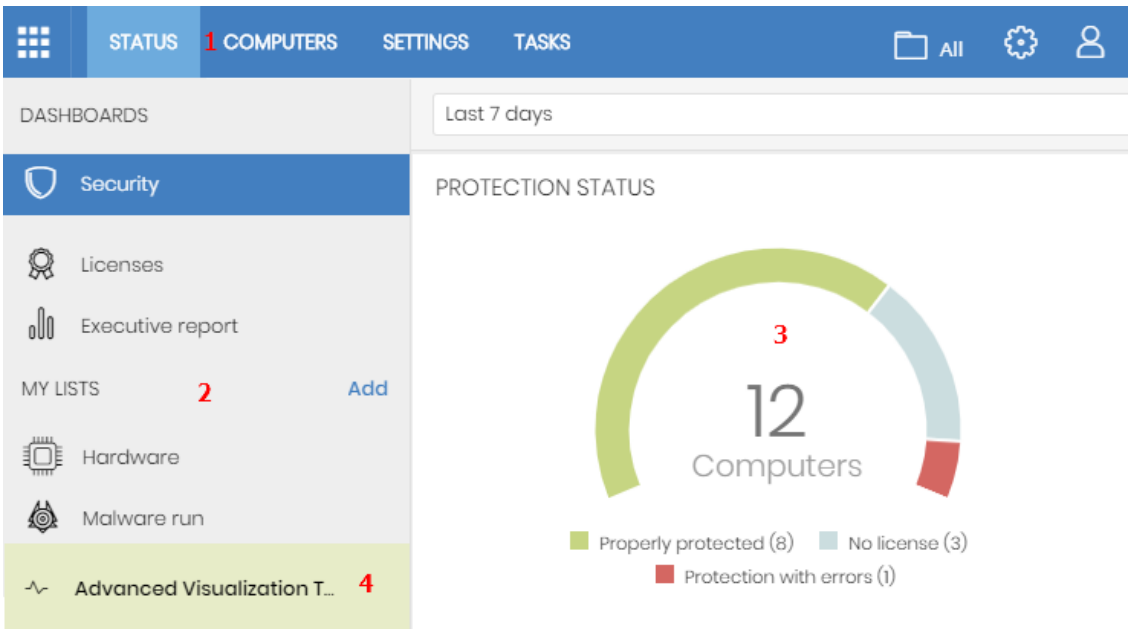


Figure 3.1: Panda Endpoint Protection Plus management console overview

Top menu (1)

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

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

Panda Cloud button

Click the button located in the left corner of the top menu. A page opens from which you can access and manage every security product you have contracted, as well as editing your Panda Account settings.

Status menu

Shows dashboards that provide administrators with an overview of the security status of the network through widgets and a number of lists accessible through the side menu. See Status area overview for more information.

Computers menu

Provides the basic tools for network administrators to define the computer structure that best fits the security needs of their IT network. Choosing the right device structure is essential in order to assign security settings profiles quickly and easily. See The Computers area on page 200 for more information.

Settings menu

Define the behavior of Panda Endpoint Protection Plus on the workstations and servers where it is installed. Settings profiles can be assigned globally to all computers on the network or to some specific computers only through templates, depending on the type of settings profile 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.

See Managing settings on page 261 for more information about how to create settings profiles in Panda Endpoint Protection Plus.

Tasks menu

Schedule security tasks to be run on the day and time you specify. See Tasks on page 581.

Filter by group icon 

Limits the information displayed in the console to the data collected from the computers belonging to the selected group(s). See Filtering results by groups on page 214 for more information.

Web notifications icon 

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

- Planned maintenance tasks
- Alerts regarding critical vulnerabilities
- Security tips
- Messages to start console upgrade processes. See Management console upgrades on page 197.

Each communication has a priority level associated with it:

-  Important
-  Notice
-  Information

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

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

General options icon 

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

Option	Description
Online Help	Enables you to access the product's web help.
Panda Endpoint Protection PlusAdministration Guide	Provides access to the Panda Endpoint Protection PlusAdministration Guide.
Technical Support	Takes you to the technical support website for Panda Endpoint Protection Plus.

Option	Description
Suggestion Box	Launches the mail client installed on the computer to send an email to the Panda Security technical support department.
License Agreement	Shows the product's EULA (End User License Agreement).
Data Processing Agreement	Shows the data processing agreement for the platform in compliance with European regulations.
Panda Endpoint Protection Plus Release Notes	Takes you to a support page detailing the changes and new features incorporated into the new version.
Language	Select the language of the management console.
About...	Shows the version of the different elements that make up Panda Endpoint Protection Plus. • **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 3.1: General options menu

User account icon 

Displays a drop-down menu with the following options:

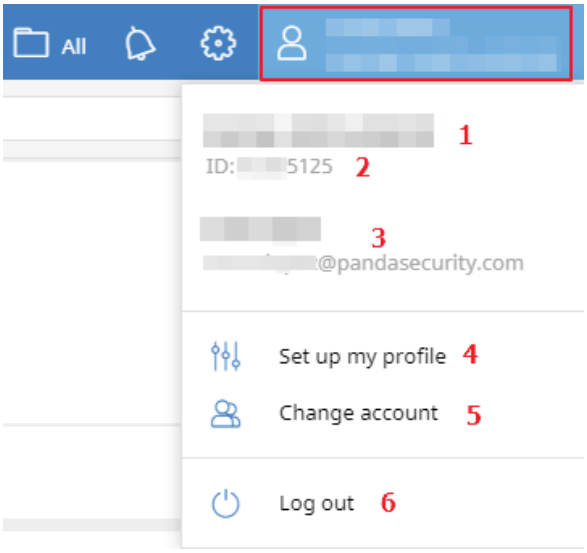


Figure 3.2: User account drop-down menu

Option	Description
Account	Name of the account used to access the console.
Customer ID	This is the number used by Panda to identify the customer. It is sent in the welcome email and requested in all communications with support.
Email address	Email address used to access the console.
Set up my profile	Modify the user account information. See Editing the personal details for a user account on page 59.
Change account	Lists all the accounts that are accessible to the administrator and enables you to select an account to work with.
Log out	Logs you out of the management console and takes you back to the IDP page.

Table 3.2: User account menu

Side menu (2)

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

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

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

Center panel (3)

Shows all relevant information for the area and subarea selected by the administrator. Figure 3.1: shows the **Status** area, **Security** subarea, with widgets that enable you to interpret the security information collected from the network. For more information about the widgets, see Security module panels/widgets on page 445.

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 show the information in an organized way.

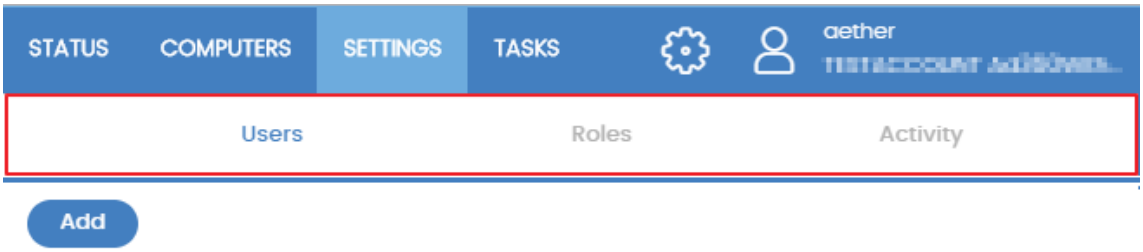


Figure 3.3: Tab menu

Action bar

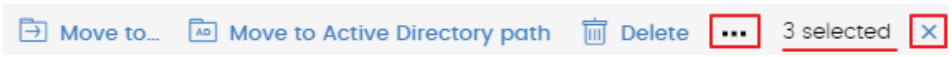


Figure 3.4: Action bar

To make it easier to navigate the console and perform some common operations on workstations and servers, an action bar appears at the top of certain pages in the console. The number of buttons on the action bar adapts to the size of the page. Click the ... icon at the right end of the action bar to view the buttons that do not fit within the allocated space.

Finally, the right corner of the action bar shows the total number of selected computers. Click the cross icon to undo your selection.

Filter and search tools

The filter and search tools enable you to filter and show information of special interest. Some filter tools are generic and apply to an entire page, for example, those shown at the top of the **Status** and **Computers** pages.

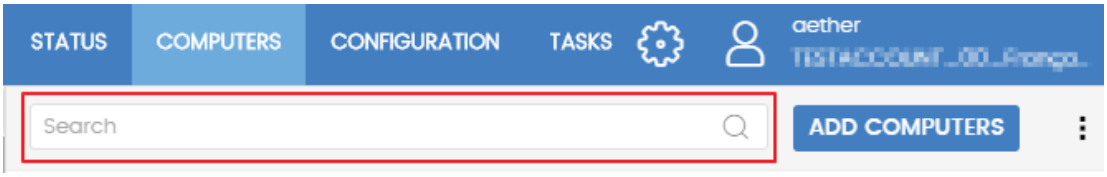


Figure 3.5: Filter tool

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

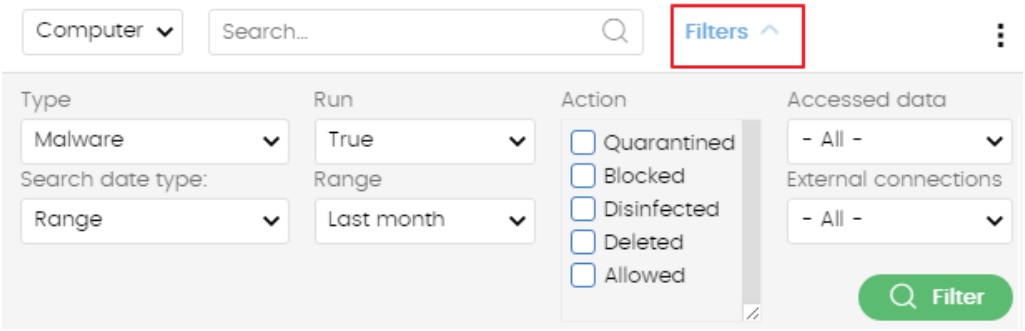


Figure 3.6: Data filter tool in lists

Other interface elements

The Panda Endpoint Protection Plus 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)**

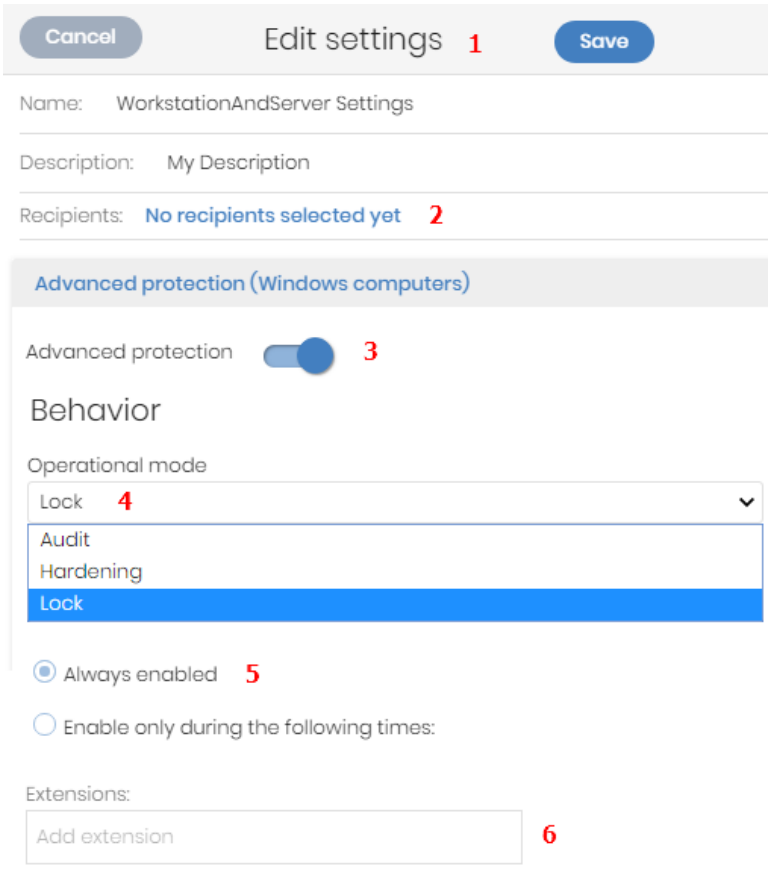


Figure 3.7: Controls for using the management console

Sort by button

Some lists of items, such as those displayed on the **Tasks** page (top menu **Tasks**) or on the **Settings** page (top menu **Settings**), show a sort by button in the upper-right or lower-right corner of the list. This button enables you to sort the items in the list according to different criteria:

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

Context menus

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

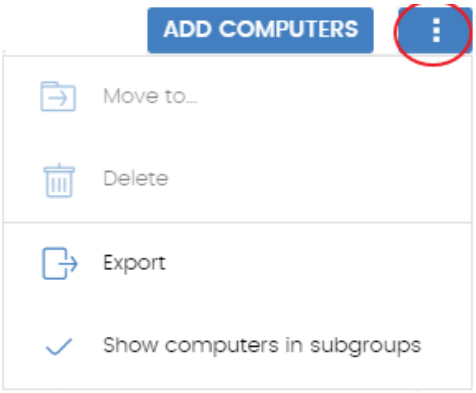


Figure 3.8: Context menus

Copy contents and Delete contents buttons

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

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

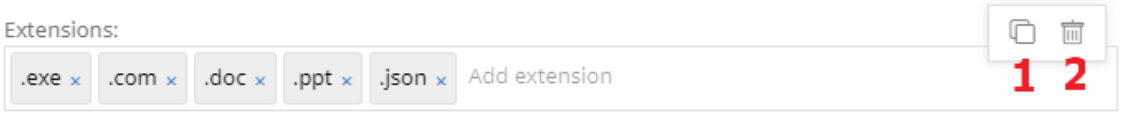


Figure 3.9: Copy and Delete buttons

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

Status area overview

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

Access to dashboards (1)

The **Status** top menu provides access to various types of dashboards. From here, you can also access different widgets and lists.

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

Time period selector (2)

Dashboards show information for the time period you select from the drop-down menu at the top of the **Status** page. You can select these time periods:

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

Some widgets do not show information for the last year. If information from the last year is not available for a specific widget, a notification appears.

Dashboard selector (3)

- **Security**: Information about the security status of the IT network. For more information about the available widgets, see Security module panels/widgets on page 445.
- **Web access**: Web browsing filtering. For more information about the available widgets, see Security module panels/widgets on page 445.
- **Patch Management**: Information about updates for the operating system and third-party software installed on computers. For more information about the available widgets, see Security module panels/widgets on page 445.
- **Panda Full Encryption**: Information about the encryption status of computers internal storage devices. For more information about the available widgets, see Security module panels/widgets on page 445.
- **Licenses**: Information about the status of the Panda Endpoint Protection Plus licenses assigned to the computers on your network. For more information about license management, see Licenses on page 177.
- **Scheduled reports**: For more information about how to configure and generate reports, see Scheduled sending of reports and lists on page 555

My lists (4)

Lists are data tables with the information presented in widgets. They include highly detailed information and have search and filter tools to help you 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 widgets is generated in real time and is interactive: Point the mouse to an item in a widget to display a tooltip with more detailed information.

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

Panda Endpoint Protection Plus uses several types of graphs to show information in the most practical way according to the type of data displayed:

- Pie charts.
- Histograms.
- Line charts.

Managing lists

Panda Endpoint Protection Plus structures the information collected at two levels: a first level that presents the data graphically through dashboards and widgets, and a second, more detailed level, where the data is presented in tables. Most widgets have an associated list, so you can quickly see information graphically in the widget and then get more detail from the list.

Panda Endpoint Protection Plus enables you to schedule and email a report of the list results. This eliminates the need to access the web console to view the details of the events that have taken place across the network. Additionally, this feature makes it easier to share information among departments and enables organizations to build an external repository containing a history of all the events that have occurred, outside the boundaries of the web console. With this repository, the management team can keep track of the generated information free from third-party interference.

Templates, settings, and views

A list consists of two items: a template and a filter.

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

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

A filter applied to a template results in a 'list view' or, simply, a 'list'. Administrators can create and save new lists for later consultation simply by editing the filters associated with a template, saving management time.

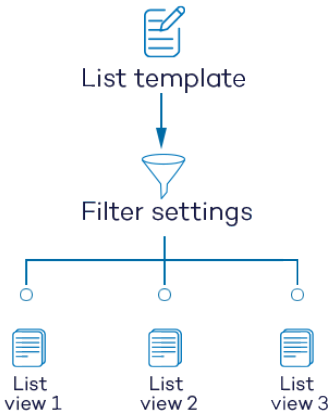


Figure 3.10: Generating three lists from a single template/data source

List templates

Click the **Status** menu at the top of the console. From the left panel, in the **My lists** section, click **Add**. A window opens with all available templates grouped by type:

Group	List	Description
General	Licenses	Shows details of the license status of the computers on your network. See Licenses module lists on page 184 for more information.
	Unmanaged computers discovered	Shows all Windows computers on your network that do not have the Panda Endpoint Protection Plus software installed. See Unmanaged computers discovered list on page 114 for more information.
	Computers with duplicate name	Shows computers with the same name and belonging to the same domain. See Computers with duplicate name on page 233for more information.
	Software	Shows the software installed on the computers on your network. See Software on page 230 for more information.
	Hardware	Shows the hardware installed on the computers on your network. See Hardware on page 228for more information.
Security	Computer protection status	Shows details of the protection status of the computers on your network. See Computer protection status on page 459for more information.
	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. See Threats detected by the antivirus on page 465for

Group	List	Description
		more information.
	Intrusion attempts blocked	Shows the intrusion attempts blocked by the computer's firewall. See Intrusion attempts blocked on page 475for more information.
	Blocked devices	Shows details of all computers on your network with limitations regarding access to peripherals. See Blocked devices on page 471for more information.
	Blocked connections	Shows the connections blocked by the local firewall. See Intrusion attempts blocked on page 475for more information.
Patch Management	Patch management status	Shows details of all computers on the network compatible with Panda Patch Management. See Patch management status on page 371 for more information.
	Available patches	Shows a list of all missing patches on the computers on your network and published by Panda Security. See Available patches on page 361for more information.
	Installation history	Shows the patches that Panda Endpoint Protection Plus tried to install and the computers that received them during the selected time period. See Installation history on page 391for more information.
	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. See End-of-Life programs on page 398for more information.
	Excluded patches	Shows the computer-patch pairs excluded from installation tasks. See Excluded patches on page 401for more information.

Group	List	Description
Activity control	Web access by category	Shows the web pages visited by users on your network, grouped by category. See Top 10 most accessed categories on page 454for more information.
	Web access by computer	Shows the web pages visited by users on your network, grouped by device. See Top 10 most accessed categories by computer on page 455for more information.
Data protection	Encryption status	Shows information about the computers on your network compatible with the encryption feature. See Encryption status on page 435for more information.

Table 3.3: Templates available in Panda Endpoint Protection Plus

Additionally, there are other templates you can directly access from the context menu of certain lists or from certain widgets on the dashboards. See the chapter dealing with the relevant widget.

List sections

Lists have a number of tools in common to make interpretation easier. Following is a description of the main elements in a sample list.

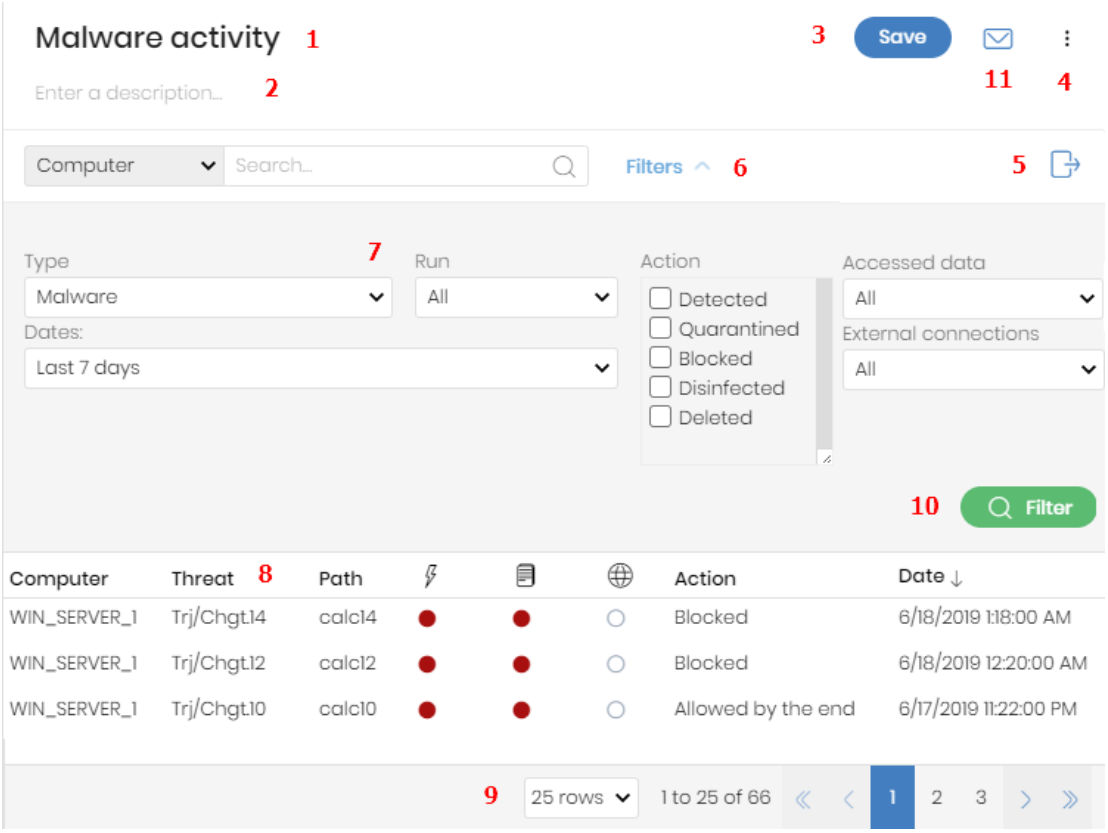


Figure 3.11: List page elements

- **List name (1)**: Identifies the information in the list.
- **Description (2)**: A free text box for specifying the purpose of the list.
- **Save (3)**: A button for saving the current view and creating a new list in the My lists tree.
- **Context menu (4)**: Drop-down menu with the actions you can take on the list (copy and delete). See Operations with lists for more information.
- **Context menu (5)**: Drop-down menu with the list export options.
- **Link to filter and search tools (6)**: Click it to display a panel with the available filter tools. After you configure your search, click the **Filter (10)** button.
- **Filtering and search parameters (7)**: Enable you to filter the data shown in the list.
- **Sorting order (8)**: Click a column header to sort the list by that column. Click the same header a second time to switch between ascending and descending order. This is indicated with arrows (a arrow or a arrow). If you are accessing the management console from a small mobile device, click the icon in the lower-right corner of the list to display a menu with the names of the columns included in the table.
- **Pagination (9)**: At the bottom of the table there are pagination controls to help you quickly move from page to page.

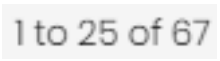
Icon	Description
	Rows per page selector.
	Range of rows displayed out of the total number of rows.
	First page link.
	Previous page link.
	Numbered links to access pages directly.
	Next page link.
	Last page link.

Table 3.4: Pagination controls

- **Scheduled report (11)**: Panda Endpoint Protection Plus enables you to send a CSV file with the contents of the list by email. See Scheduled sending of reports and lists on page 555 for more information.

Operations with lists

From the top menu, select **Status**. In the side menu, go to **My lists** to view all lists created by the administrator as well as a number of predefined lists that Panda Endpoint Protection Plus includes by default. For more information, see Predefined lists.

Creating a custom list

You can create a new custom list/view in multiple ways:

- **From the My lists side panel**
  - From the left panel, in the **My lists** section, click **Add**. A window opens with all available templates.
  - Choose a template, configure the filter tools, edit the name and description of the list, and click the **Save (3)** button.
- **From a dashboard widget**
  - Click a widget on the dashboard to open its associated template.

- Click its context menu **(4)** and select **Copy**. A new list is created.
- Edit the filters, name, and description of the list. Click the **Save** button **(3)**.

- **From an existing list**
  - You can make a copy of an existing list by clicking its context menu **(4)**. Then, click **Copy**. A new list is immediately generated with the name "Copy of...".
  - Edit the filters, name, and description of the list. Click the **Save** button **(3)**.

- **From the context menu of the My lists panel**
  - Click the context menu for the list you want to copy.
  - Click **Make a copy**. A new template view is created with the name “Copy of...”.
  - Edit the filters, name, and description of the list. Click the **Save** button **(3)**.

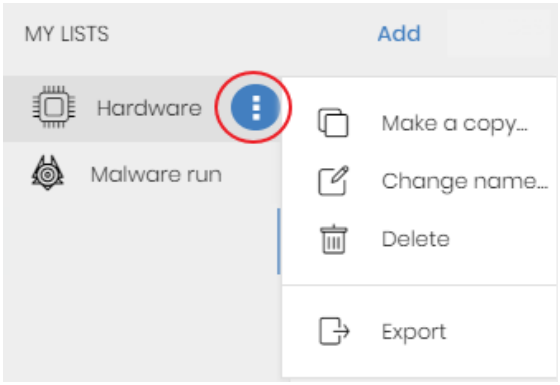


Figure 3.12: Context menu for the lists accessible from the My lists panel

Deleting a list

You can delete a list in multiple ways:

- **From the My lists panel**
  - From the **My lists** panel, click the context menu for the relevant list.
  - Click the icon.

- **From the list**
  - Click the list context menu **(4)**.
  - From the drop-down menu that opens, click the icon.

Copying a list

You can copy a list in multiple ways:

- **From the My lists panel**
  - From the **My lists** panel, click the context menu for the relevant list.
  - Click the icon.
- **From the list**
  - Click the list context menu **(4)**.
  - From the drop-down menu that opens, click the icon.

Exporting a list

You can export lists to CSV format to get more information than is shown in the web console. For information about the fields in each exported file, see the relevant chapter of this Administration Guide. You can export a list in multiple ways:

- **From the My lists panel**
  - If the list does not support export of details, click the icon. A CSV file is downloaded with the list data.
  - If the list supports export of details, click the icon **(5)**. A drop-down menu appears.
  - Click **Export**. A CSV file is downloaded with the list data.
- **From the list**
  - Click the list context menu **(4)**.
  - From the drop-down menu that opens, click the **Export** icon. A CSV file is downloaded with the list data.

Depending on the module or feature, some lists can provide more details in the exported file than others.

Exporting a list details

You can export a list details to get more information than is shown in the exported CSV file. For more information about the fields in each exported file, see the relevant chapter of this Administration Guide. You can export a list in multiple ways:

- **From the My lists panel**
  - Click the icon **(5)**. A drop-down menu opens.
  - Click **Export list and details**. A CSV file is downloaded with the list details.

- **From the list**
  - Click the list context menu **(4)**. A drop-down menu opens.
  - Click the **Export list and details** icon . A CSV file is downloaded with the list details.

> *Depending on the module or feature, some lists can provide more details in the exported file than others.*

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 of" if the list is a copy of a previous one.
- Assign a description **(2)**: This step is optional.
- Click the **Filters** link **(6)** to display the filter and search options.
- Click **Filter (10)** to apply the configured filter and check if it meets your needs. The list shows the search results.
- Click **Save (3)**. The new list appears in the **My lists** section in the left panel. You can access it by clicking its name.

Scheduling a list to be sent by email

- **From the context menu of the My lists panel**
  - Click the context menu for the list you want to send. Select the **Schedule report** option.
  - A dialog box opens where you can enter the necessary information to automatically send the list.
- **From the list**
  - Click the **(11)** icon. A dialog box opens where you can enter the necessary information to automatically send the list.

> *For more information, see Scheduled sending of reports and lists on page 555.*

Available actions for computers in lists

Some lists include checkboxes that enable you to select computers. When you select one or more computers, an action bar appears at the top of the page. This bar makes it easier to manage the selected workstations and servers. See Action bar (8) on page 259.

Each list page shows information about 25 computers. To take action on all computers on a page, select the checkbox in the upper-left corner of the list **(1)**:

With the **Computers** and **Unmanaged computers discovered** lists, after you select this checkbox, you can take action on all computers on all of the list pages **(2)**.

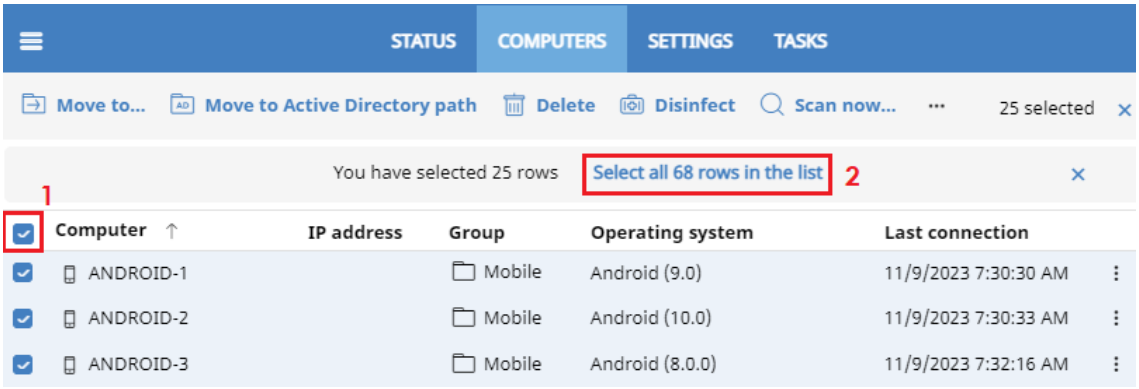


Figure 3.13: Select computers on a list

Predefined lists

The management console includes various predefined lists:

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

Unprotected workstations and laptops

Shows all desktop and laptop computers, regardless of the operating system installed, which could be vulnerable to threats due to a problem with the protection:

- Computers on which the Panda Endpoint Protection Plus software is currently being installed or the installation failed.
- Computers on which the protection is disabled or has errors.
- Computers without a license assigned or with an expired license.
- See Computer protection status on page 459 for more information.

Unprotected servers

Shows all servers, regardless of the operating system installed, which could be vulnerable to threats due to a problem with the protection:

- Servers on which the Panda Endpoint Protection Plus software is currently being installed or the installation failed.

- Servers on which the protection is disabled or has errors.
- Servers without a license assigned or with an expired license. See Computer protection status on page 459 for more information.

Software

Shows a list of the programs installed across your network. See Software on page 230 for more information.

Hardware

Shows a list of the hardware components installed across your network. See Hardware on page 228 for more information.

Chapter 4

Accessing, controlling, and monitoring the management console

Panda Endpoint Protection implements multiple resources for limiting, controlling, and monitoring access to the web management console and the actions that network administrator can take through it:

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

Chapter contents

General concepts

User account

A user account is a resource consisting of a set of data that Panda Endpoint Protection Plus uses to allow administrator to access the web console and set the actions that administrators can take on user computers.

User accounts are used only by the IT administrators who access the Panda Endpoint Protection Plus console. Each administrator can have one or more user accounts assigned.

The main characteristics of user accounts are:

- They are accounts managed by the administrator. The administrator can create or delete accounts, change their passwords, add or remove permissions, or enable two-factor authentication.
- A user account provides access to all products purchased from Panda Security through Panda Cloud.
- A user account can provide access to multiple customers. The administrator can choose the product they want to access in Panda Cloud, and then select the console they want to access on the **Select account** page.

Panda Cloud

This is a portal that centralizes access to all the products included in the Panda Security portfolio. A user account created in a Panda Security product provides access to the portal, from which the administrator can access the consoles of the purchased products.

For more information, see https://documents.managedprotection.pandasecurity.com/Help/PandaCloud/en-us/#t=001.htm.

Customer account

This is a resource consisting of confidential data associated with a customer that has purchased a Panda Security product. The customer's fiscal address, full name, tax identification number, and other data are part of the customer account.

Managing user accounts

A user account consists of multiple pieces of information that are generated when the account is created:

- **Account login email address**: Identifies the users accessing the console.
- **Account password**: Allows or prevents access to the management console.
- **Assigned role**: Determines which computers the account user can manage and the actions they can take.

Differences between WatchGuard and Panda Security customers

Panda Security and WatchGuard customers follow different procedures to create or modify user accounts. Panda Security customers manage user accounts directly from the Panda Endpoint Protection Plus console, whereas WatchGuard customers access the products they have purchased and create their user accounts from the WatchGuard Portal.

Creating the first user account for Panda Security customers

The procedure to create the first user account is different from the steps to create subsequent accounts. The first user account always has the Full Control role assigned. This role enables you to perform any action through the console. You cannot remove or modify this account.

Receive the welcome email

- After you purchase Panda Endpoint Protection Plus, you receive an email message from Panda Security.
- Click the **Click here** link in the message to access the website from which you can create the first user account.

Complete the Create your Panda account form

- Enter your email address and click **Create**. You will receive a new email message at the email address you specified in the form to activate the account you created.

Activate the user account

- Click the activation button in the message you received to verify the email address you provided when you created the user account. If the button does not work, copy and paste the link included in the message into your browser. The **Panda Account** page opens.
- Enter the password for the account. The password length must be at least 8 characters. The password must contain at least one number and at least one letter.
- Choose the country. Click **Activate account**. The **One second and you are done** page opens.
- Enter your first and last name, date of birth, phone number, and address. Click **Save**. You can skip this step by clicking **Not now**. The Panda Cloud end-user license agreement opens.

- Click **Accept and continue**. The Panda Cloud page opens, from which you can access all services purchased from Panda Security.

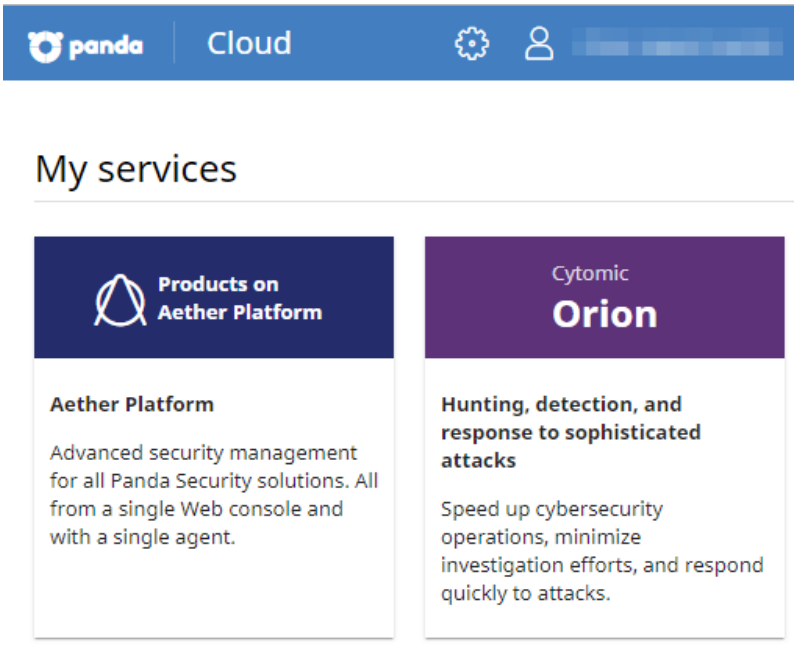


Figure 4.1: Panda Cloud page

- To access the Panda Endpoint Protection Plus console, click the Panda Endpoint Protection Plus tile in **My services**. The first time you access the console, a wizard opens that prompts you to accept the license and data processing agreements.
    - On the **License agreement** page, click the **Accept and continue** button.
    - On the **Data processing agreement** page, click **Go to data processing agreement**.
    - On the **Data processing agreement** page, click **Accept**. The Panda Endpoint Protection Plus console opens.

Creating the first user account for WatchGuard customers

Users that belong to the WatchGuard security vendor and still do not have a Panda Security product must create a customer account and a user account with Panda Security the first time that they activate a commercial license of Panda Endpoint Protection Plus.

If you already have a Panda Endpoint Protection Plus product and want to access its console from WatchGuard, see Accessing the Panda Endpoint Protection Plus console from the WatchGuard Portal with an existing account.

- Go to the WatchGuard Portal at https://www.watchguard.com/. Log in with the user account you want to use to access the Panda Endpoint Protection Plus console.

- Select **MY WATCHGUARD**. Select **Activate Products**. The **Activate Products** page opens.
- Enter the license key of your Panda Security product. Click **Continue**.
- Click **I need a Panda account**. A page opens that shows the newly created account name and ID. We recommend that you save this information. You need this information if you contact Support.
- Click **Submit**. Click **Continue**. The **WatchGuard Support Center** opens.
- If prompted, type or paste your Panda Security product license key again. The **Activate a Product** wizard opens.
- To accept the license terms of use, click **Next**.
- On the **Select a License** page of the wizard, from the drop-down list, select **New License**. Click **Next**.
- Type a name to help you identify your license on the WatchGuard website. Click **Next**.
- Select the **I accept the End-User License Agreement** checkbox. Click **Next**. The **Activation Complete** page appears and your licenses are added to the relevant license contract in Panda Endpoint Protection Plus.

After the process is complete, the WatchGuard user account can access the Panda Endpoint Protection Plus console. See Access to the web console on page 30.

Creating subsequent user accounts from the Panda Endpoint Protection Plus console

After you have created the first user account, you can access the Panda Endpoint Protection Plus management console, from which you can create all other user accounts you may need.

- Make sure the user has the **Manage users and roles** permission assigned. See Understanding permissions.
- From the top menu, select **Settings**. From the side menu, select **Users.**
- Select the **Users** tab. A page opens that shows a list of all users created in the management console.
- Click **Add**. The **Add user** page opens.
- In the **Login email** field, enter the console user email address. Enter a description if needed.
- Choose a role for the user account. See Understanding permissions.
- Click **Save**. Panda Endpoint Protection Plus sends an email to the specified email address so that the user can generate an access password and accept the terms of the license and data processing agreements.

Creating subsequent user accounts in Panda Endpoint Protection Plus from the WatchGuard Portal

User accounts that belong to the WatchGuard security vendor can access the Panda Endpoint Protection Plus console directly from the WatchGuard Portal. You can create a user in the Panda Endpoint Protection Plus console for each account created in the WatchGuard Portal by using the WatchGuard Account Mapper.

User accounts that belong to the same WatchGuard customer always spawn user accounts in the same Panda Security customer. This means that it is not possible to access multiple Panda Endpoint Protection Plus consoles hosted in different Panda Security customer accounts from WatchGuard user accounts belonging to the same customer.

Before you begin this procedure, make sure you have logged out of the WatchGuard Portal and the Panda Endpoint Protection Plus console and you have closed your web browser.

- Open your browser. Go to https://accountmapper.watchguard.com. Click **I have a WatchGuard account and need a Panda account**. The **Create new account with Panda?** dialog box opens.
- Click **Continue** to confirm you want to create a new user account in Panda Endpoint Protection Plus. The **Provide the following details** page opens.
- Enter the user name and password for the WatchGuard user account that you want to use to access the Panda Endpoint Protection Plus console. Click **Continue**. The **Log in to access** Panda Cloud page opens.
- Enter the user name and password for the Panda Endpoint Protection Plus first user. Click **Log in**.
- Click **Continue**. A new user with the prefix "generated" is automatically created in the Panda Endpoint Protection Plus console. This user is linked to the WatchGuard user you used to complete the procedure.

After the process is complete, the WatchGuard user account can access the Panda Endpoint Protection Plus console. See Access to the web console on page 30.

Accessing the Panda Endpoint Protection Plus console from the WatchGuard Portal with an existing account

If there is an existing user account in Panda Endpoint Protection Plus and you want to use it to access the console from the WatchGuard Portal, you must complete a process consisting of linking a WatchGuard user account to the Panda Endpoint Protection Plus user account that will access the console. You must perform the linking procedure only once. After it is complete, you will be able to access the Panda Endpoint Protection Plus console with the account of your choice from the WatchGuard Portal.

> *Before you begin this procedure, make sure you have logged out of the WatchGuard Portal and the Panda Endpoint Protection Plus console and you have closed your web browser.*

- Go to https://accountmapper.watchguard.com. Click **I have both WatchGuard and Panda accounts**. The **Map your existing accounts?** dialog box opens. This dialog box informs you that the mapping option works only if the WatchGuard and Panda accounts are already created but not linked.
- Click **Continue**. A WatchGuard login page opens.
- Type your WatchGuard account user name and password. Click **Log in**. A **Panda login page** opens.
- Type your Panda Endpoint Protection Plus account user name and password. Click **Log in**. A page opens indicating whether the linking process ended successfully or not. If it failed, the reason of the error is shown.
- Click **Continue**. After the process is complete, the WatchGuard user account can access the Panda Endpoint Protection Plus console. See Access to the web console on page 30.

Editing the personal details for a user account

- In the management console, click the  icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**. The procedure varies depending on whether you access the console from Panda Cloud or from the WatchGuard Portal.

Panda Cloud

- The **Panda Account** page opens.
- In the left menu, select **Profile**. Fill the form with the personal details for the account.
- Click **Save**. The changes are stored on the Panda Security server.

WatchGuard Portal

- The **User Information** page opens.
- Click the **Edit** button at the bottom of the page. Fill the form with the personal details for the account.
- Click **Save**. The changes are stored on the WatchGuard server.

Editing the email address or password for a user account

- In the management console, click the  icon in the upper-right corner of the page. A drop-down menu appears.

- Select **Set up my profile**. The procedure varies depending on whether you access the console from Panda Cloud or from the WatchGuard Portal.

Panda Cloud

- The **Panda Account** page opens.
- In the left menu, select **Login**. Click the **Change email address** or **Change password** links. A page opens that prompts you to validate the old data and enter the new one.
- Click **Change**.

WatchGuard Portal

- The **User Information** page opens.
- Click the **Edit** button next to the **EMAIL** field, or the **Change Password** link to change the data.

Removing or blocking user accounts in the Panda Endpoint Protection Plus console

When you remove a Panda Endpoint Protection Plus user account linked to a WatchGuard account, only the Panda Endpoint Protection Plus account is removed.

- Make sure the user has the **Manage users and roles** permission assigned. See Understanding permissions.
- From the top menu, select **Settings**. From the side menu, select **Users.**
- Select the **Users** tab. A page opens that shows a list of all users created in the management console.
- Click the icon for the user account you want to remove.
- To temporarily disable access from a user account to the web console, click the account and enable the **Block this user** toggle. Access from the account to the management console is denied. If the account user is currently logged in, they are logged out immediately. Also, email alerts are no longer sent to the email addresses configured in the account settings.

Enabling two-factor authentication

Panda Endpoint Protection Plus supports the two-factor authentication (2FA) standard to add an additional layer of security beyond that provided by the 'user-password' basic pair. This way, when you try to access the web console, you are prompted to enter an additional authentication item: a code that only the account owner has. This is a random code that is generated on a specific device, typically the Panda Endpoint Protection Plus administrator personal smartphone or tablet.

Requirements for enabling 2FA

- Access to a personal smartphone or tablet with a built-in camera.
- Download the WatchGuard AuthPoint free app (or similar) from:
  - **iOS**: https://apps.apple.com/app/watchguard-authpoint/id1335115425
  - **Android**: https://play.google.com/store/apps/details?id=com.watchguard.authpoint

Enabling 2FA

- In the management console, click the  icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**. The procedure varies depending on whether you access the console from Panda Cloud or from the WatchGuard Portal.

Panda Cloud

- The **Panda Account** page opens.
- From the side menu, select **Login**. In the **Two-factor authentication** section, click the **Enable** link. The **Synchronization using an authentication app** dialog box opens.
- The first time that you use the WatchGuard AuthPoint app on your mobile device, tap **Activate**. If you have used it before, tap the QR code icon in the upper-right corner of the dialog box. The mobile device camera opens.

Figure 4.2: Scanning the QR code with WatchGuard AuthPoint

- Point the camera at the QR code in the Panda Endpoint Protection Plus console. A new entry is added to WatchGuard AuthPoint and a token is generated every 30 seconds.
- Enter the code generated by WatchGuard AuthPoint in the Panda Endpoint Protection Plus console to link the device to the user account. Click **Verify**. A dialog box opens that shows the message **Two-factor authentication is enabled**.
- Click **OK**.

WatchGuard Portal

- The **User Information** page opens.
- Click the **Edit** button next to the **MULTI-FACTOR AUTHENTICATION** field. The **Manage Multi-Factor Authentication** page opens.

- Click **Enable MFA**. The **Are you sure you want to enable MFA?** page opens.
- Click **Continue**. An email is sent to the user email address to generate the token.
- Open the email message and click the **START ACTIVATION** button The **Welcome to AuthPoint** page opens.
- The first time that you use the WatchGuard AuthPoint app on your mobile device, tap **Activate**. If you have used it before, tap the QR code icon in the upper-right corner of the dialog box. The mobile device camera opens.

Figure 4.3: Scanning the QR code with WatchGuard AuthPoint

- Point the camera at the QR code in the Panda Endpoint Protection Plus console. A new entry is added to WatchGuard AuthPoint.

Accessing the web console from Panda Cloud using an account with 2FA enabled

- Go to https://www.pandacloudsecurity.com/PandaLogin/. Enter your user name and password. Click **Log in**.
- Enter the verification code generated by WatchGuard AuthPoint on your mobile device. Click **Verify**. The **Panda Cloud** page opens.

Accessing the web console from the WatchGuard Portal using an account with 2FA enabled

- Go to https://www.watchguard.com/. Log in with your user name and password. Click **Continue**. The **Choose an authentication method** page opens.
- Click **Send Push** button. In the WatchGuard AuthPoint app, the **Are you trying to sign in?** message appears.
- Click **Approve** to complete the process to access the WatchGuard Portal. The **Support Center** page opens.
- Select the **MY WATCHGUARD** menu at the top of the page. A drop-down menu appears.
- Select the **Manage Panda Products** option. The Panda Cloud page opens and shows all purchased services.

Forcing all console users to use 2FA

The user account with which you enforce the use of 2FA must have the **Manage users and roles** permission assigned and full visibility into the IT network. See Managing roles and permissions

- From the top menu, select **Settings**. Select the **Security** tab.
- Select the option **Require users to have two-factor authentication enabled to access this account**.
- If the user account with which you force all console users to use 2FA does not have two-factor authentication enabled, a warning message appears and prompts you to access your **Panda Account** and enable the feature. See Enabling 2FA.

User list

Required permissions

All console users can view the user list.

Accessing the list

- Select the **Settings** menu at the top of the console. Select **Users** in the side menu.
- Select the **Users** tab. A list appears that shows all user accounts created in Panda Endpoint Protection Plus, along with the following information:

Field	Description
Account name	User account name.
Role	Role assigned to the user account.
Email account	Email account assigned to the user.
Padlock	Indicates whether the account has two-factor authentication (2FA) enabled.
Status	Indicates whether the user account is active or blocked.

Table 4.1: Fields in the user list

Sorting and searching in the user list: Click the  icon to sort the user list in ascending/descending order, by name, or by creation date. To search for a user, type the text in the search box and click the  icon.

Fields displayed in the exported file

Field	Definition	Values
Client	Customer account the service belongs to.	Character string
Name	Name of user profile.	Character string
Login email	Email address used to access the console	Character string
Role	Role assigned to the user.	Character string
Description	Description added to the user profile.	Character string
Two-factor authentication	Indicates whether the account has two-factor authentication enabled or disabled.	Boolean
Blocked	Indicates whether the user account is active or blocked.	Boolean

Table 4.2: Fields in the User list exported file

Filter tools

Field	Comment	Values
Search user	Enables you to search by user name and email address. You can type only a partial string.	Character string
Blocked	Finds blocked user accounts in the list.	• All • Yes • No
Two-factor authentication	Finds user accounts that have two-factor authentication enabled.	• All • Enabled • Disabled

Table 4.3: Filters available in the user list

Sorting tools

To display the available sorting criteria, click the  icon.

Managing roles and permissions

Basic concepts

Roles

A role is a specific configuration of permissions that is applied to one or more user accounts. A user account is authorized to view or modify certain resources in the console depending on the role assigned to it.

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

A role consists of the following:

- **Role name**: This is purely for identification and is assigned when the role is created.
- **Visibility**: Restricts access to certain computers on the network.
- **Permission set**: Determines the specific actions that the user account can take on computers belonging to groups defined as accessible.

Predefined roles

A Panda Endpoint Protection Plus license always has two predefined roles. These roles cannot be edited or deleted. Any user account can be assigned these roles through the web console.

Full Control role

The first user account that is created always has the Full Control role assigned. This account enables you to take all the actions available in the console on the computers added to Panda Endpoint Protection Plus.

Read-Only role

This role provides access to all sections of the console, but does not enable you to create, modify, or delete settings profiles, tasks, etc. That is, it provides total visibility of the environment but does not allow you to make any changes. This role is particularly suited for network administrators responsible for monitoring the network, but who do not have enough permissions to take actions such as editing settings profiles or launching on-demand scans.

Permission

A permission controls access to a specific section of the management console. There are different types of permissions that provide access to many sections of the Panda Endpoint Protection Plus console. A specific configuration of all available permissions makes up a role, which can be assigned to one or more user accounts.

Visibility

Each user account enables you to configure the security of a subset of computers from all the computers added to the Panda Endpoint Protection Plus console. This is determined by the account visibility.

Creating a role

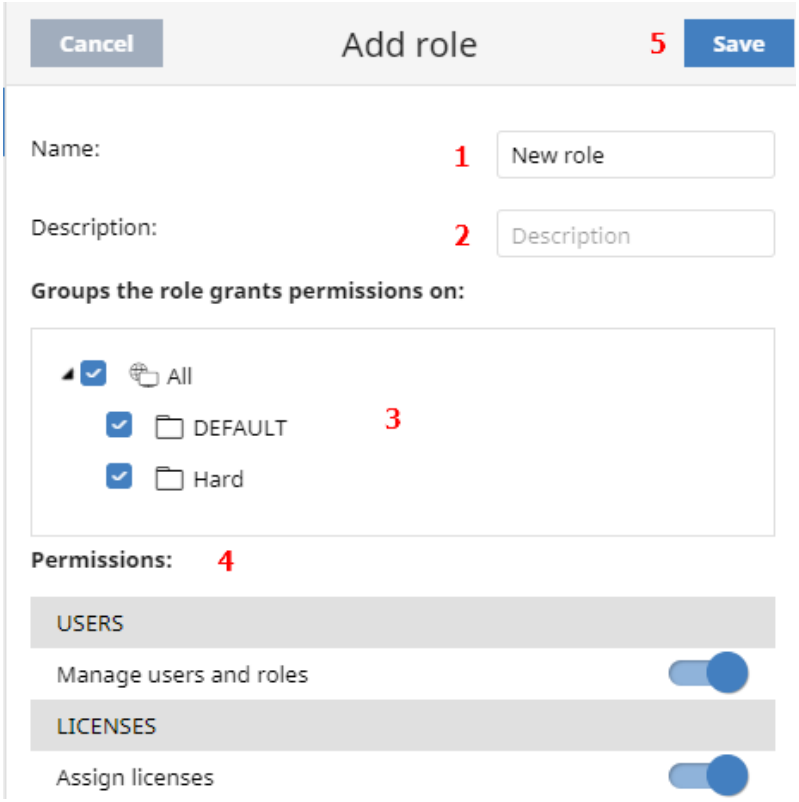


Figure 4.4: Add role page

- Select the **Settings** menu at the top of the console. Select **Users** from the side menu. A page opens that shows a list of all created users.
- Select the **Roles** tab. Select **Add**. The **Add roles** page opens.
- Enter a name for the role **(1)** and, optionally, a description **(2)**.
- Specify the visibility for the role **(3)**.
- Enable or disable permissions **(4)**.
- Click **Save (5)**.

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

Deleting a role

- Select the **Settings** menu at the top of the console. Select **Users** from the side menu.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the  icon of a role to delete it. If the role you are trying to delete has user accounts assigned, the delete operation is canceled.

Copying a role

- Select the **Settings** menu at the top of the console. Select **Users** from the side menu.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the icon of a role to copy it. The **Copy role** page opens. This page shows the settings of the copied role.
- Modify the role settings. Click **Save**.

Modifying a role

- Select the **Settings** menu at the top of the console. Select **Users** in the side menu.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the role you want to edit. The **Edit role** page opens.
- Modify the role settings. Click **Save**.

Understanding permissions

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. The user can view registered users and account details, but not the list of roles created.

Assign licenses

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

Modify computer tree

- **Enabled**: The account user has full access to the group tree, and can create and delete groups, as well as moving computers to groups already created.
- **Enabled with permission conflict**: Because of the inheritance mechanism that applies to the computer tree, any changes made to the tree structure can result in a change to the settings profiles assigned to the affected devices. For example, in cases where the administrator does not have permission to assign settings profiles, if they move a computer from one group to another, the web console will show a warning indicating that, because of the computer move operation and the inheritance mechanism applied, the settings profiles assigned to the computer that was moved might have changed (even if the administrator does not have permission to assign settings profiles). See section Manual and automatic assignment of settings profiles on page 269
- **Disabled**: The account user can view the group tree and the settings profiles assigned to each group, but cannot create new groups or move computers.

Add, discover, and delete computers

- **Enabled**: The account user can deploy the installer to computers on the network and add them to 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 deploy it to computers on the network. Neither can the user delete computers from the console or access the computer discovery feature.

Modify network settings (proxies and cache)

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

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

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

Restart and repair computers

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

Configure security for workstations and servers

- **Enabled**: The account user can create, edit, delete, and assign security settings profiles for workstations and servers.
- **Disabled**: The account user cannot create, edit, delete, or assign security settings profiles for workstations and servers.

If you disable this permission, the **View security settings for workstations and servers** permission appears.

View security settings for workstations and servers

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

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

Configure security for mobile devices

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

If you disable this permission, the **View security settings for mobile devices** permission appears. This permission is explained next.

View security settings for mobile devices

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

- **Enabled**: The account user can only view the settings profiles created for mobile devices, as well as the settings profiles assigned to a specific mobile device or group of mobile devices.
- **Disabled**: The account user cannot view the settings profiles created for mobile devices nor the settings profiles assigned to mobile devices.

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

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

View detections and threats

- **Enabled**: The account user can access the widgets and lists available on the **Security** dashboard accessible from the **Status** top menu, as well as creating new lists with custom filters.
- **Disabled**: The account user cannot access the widgets and lists available on the **Security** dashboard accessible from the **Status** top menu, nor create new lists with custom filters.

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

View access to web pages

- **Enabled**: The account user can access the widgets and lists available on the **Web access** dashboard accessible from the **Status** top menu.
- **Disabled**: The account user cannot access the widgets and lists available on the **Web access** dashboard accessible from the **Status** top menu.

Launch scans and disinfect

- **Enabled**: The account user can create, edit, and delete scan and disinfection tasks.
- **Disabled**: The account user cannot create new scan and disinfection tasks, nor edit or delete existing ones. The user can only view those tasks and 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 or PUPs from scans, nor edit the existing exclusions.

*To enable 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 profiles to Windows, macOS, and Linux computers.
- **Disabled**: The account user cannot create, edit, delete, or assign patch management settings profiles to Windows, macOS, or Linux computers.

If you disable this permission, the **View patch management settings** permission appears.

View patch management settings

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

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

Install, uninstall, and exclude patches

- **Enabled**: The account user can create patch installation, uninstallation, and exclusion tasks, and access these lists: **Available patches**, **End-of-Life programs**, **Installation history**, and **Excluded**

patches.

- **Disabled**: The account user cannot create patch installation, uninstallation, or exclusion tasks.

View available patches

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

- **Enabled**: The account user can access the following lists: **Patch management status**, **Available patches**, **End-Of-Life programs**, and **Installation history**.
- **Disabled**: The account user cannot access these lists: **Patch management status**, **Available patches**, **End-Of-Life programs**, or **Installation history**.

Configure vulnerability assessment

- **Enabled**: The account user can create, edit, delete, and assign vulnerability assessment settings profiles to Windows, macOS, and Linux computers.
- **Disabled**: The account user cannot create, edit, delete, or assign vulnerability assessment settings profiles to Windows, macOS, or Linux computers.

If you disable this permission, the **View vulnerability assessment settings** permission appears.

View vulnerability assessment settings

*This permission is accessible only if you disable the **Configure vulnerability assessment** permission.*

- **Enabled**: The account user can only view the vulnerability assessment settings profiles created as well as the settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the vulnerability assessment settings profiles created, nor access the settings profiles assigned to computers.

View available patches

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

- **Enabled**: The account user can access the following lists: **Vulnerability assessment status**, **Available patchesby computers**, and **End-of-Life programs**.
- **Disabled**: The account user cannot access these lists: **Vulnerability assessment status**, **Available patches by computers**, or **End-of-Life programs**.

Configure computer encryption

- **Enabled**: The account user can create, edit, delete, and assign encryption settings profiles.
- **Disabled**: The account user cannot create, edit, delete, or assign encryption settings profiles.

View computer encryption settings

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

- **Enabled**: The account user can only view the computer encryption settings profiles created, as well as the encryption settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the encryption settings profiles created, nor access the encryption settings profiles assigned to computers.

Access recovery keys for encrypted drives

- **Enabled**: The account user can view the recovery keys for computers that have storage devices encrypted and managed by Panda Endpoint Protection Plus.
- **Disabled**: The account user cannot view the recovery keys for computers that have encrypted storage devices.

User account activity log

Panda Endpoint Protection Plus 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. Select the **Activity** tab.

Session log

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

Fields displayed in the Sessions list

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

Table 4.4: 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 taken by the account	• Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 4.5: Fields in the Sessions exported file

Filter tool

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

Field	Description	Values
Users	User name.	List of all user accounts created in the management console.

Table 4.6: Filters available in the Sessions list

User actions log

The **User actions** section lists all the actions taken by the user accounts and enables you to export the information to a CSV file and filter the data.

Fields displayed in the User Actions list

Field	Description	Values
Date	The date and time when the action occurred.	Date
User	The name of the user who completed the action.	Character string.
Action	The user action completed.	See table Item types and actions.
Item type	The type of console object the action was performed on.	See table Item types and actions.
Item	The name of the console object that the action occurred on.	See table Item types and actions.

Table 4.7: Fields in the User Actions log

Fields displayed in the exported file

Field	Description	Values
Date	The date and time when the action occurred.	Date
User	The name of the user who completed the action.	Character string
Action	The user action completed.	See table Item types and actions.
Item type	The type of console object the action was performed on.	See table Item types and actions.

Field	Description	Values
Item	The name of the console object that the action occurred on.	See table Item types and actions.

Table 4.8: Fields in the User Actions exported file

Filter tool

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

Table 4.9: Filters available in the User Actions log

Item types and actions

Item type	Action	Item
License agreement	Accept	Version number of the accepted End User License Agreement.
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.

Item type	Action	Item
Account	Update console	From Initial version to Target version.
	Cancel console update	From Initial version to Target version.
Apple push certificate	Upload	Name of the certificate imported into the console
Settings - Network settings	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Per-computer settings	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Workstations and servers	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Android devices	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.

Item type	Action	Item
	Delete	Name of the settings profile the action was performed on.
Settings - iOS devices	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Patch Management	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Endpoint Access Enforcement	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Panda Full Encryption	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.

Item type	Action	Item
Settings - Vulnerability assessment	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Trusted network	Edit	Name of the settings profile the action was performed on.
Device	Edit name	Name of the device the action was performed on.
Scheduled report	Create	Name of the scheduled report the action was performed on.
	Edit	Name of the scheduled report the action was performed on.
	Delete	Name of the scheduled report the action was performed on.
Computer	Delete	Name of the device the action was performed on.
	Edit name	Name of the device the action was performed on.
	Edit description	Name of the device the action was performed on.
	Change group	Name of the device the action was performed on.
	Assign 'Proxy and language' settings	Name of the device the action was performed on.

Item type	Action	Item
	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.

Item type	Action	Item
	Remote alarm	Name of the device the action was performed on.
	Locate	Name of the device the action was performed on.
	Designate as Panda proxy	Name of the computer the action was performed on.
	Revoke Panda proxy role	Name of the computer the action was performed on.
	Designate as cache computer	Name of the computer the action was performed on.
	Configure cache computer	Name of the computer the action was performed on.
	Revoke cache computer role	Name of the computer the action was performed on.
	Designate as discovery computer	Name of the computer the action was performed on.
	Configure discovery	Name of the computer the action was performed on.
	Revoke discovery computer role	Name of the computer the action was performed on.
	Discover now	Name of the computer the action was performed on.
	Move to Active Directory path	Name of the computer the action was performed on.
	Enable Verbose mode	Name of the computer the action was performed on.

Item type	Action	Item
	Disable Verbose mode	Name of the computer the action was performed on.
	Uninstall	Name of the device the action was performed on.
	Reinstall agent	Name of the device the action was performed on.
	Reinstall protection	Name of the device the action was performed on
Unmanaged computer	Hide	Name of the unmanaged computer the action was performed on.
	Make visible	Name of the unmanaged computer the action was performed on.
	Delete	Name of the unmanaged computer the action was performed on.
	Edit description	Name of the unmanaged computer the action was performed on.
	Install	Name of the unmanaged computer the action was performed on.
Filter	Create	Name of the filter the action was performed on.
	Edit	Name of the filter the action was performed on.
	Delete	Name of the filter the action was performed on.
Group	Create	Name of the group the action was performed on.

Item type	Action	Item
	Edit	Name of the group the action was performed on.
	Delete	Name of the group the action was performed on.
	Change parent group	Name of the group the action was performed on.
	Assign 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.

Item type	Action	Item
Advanced reports	Access	
List	Create	Name of the list the action was performed on.
	Edit	Name of the list the action was performed on.
	Delete	Name of the list the action was performed on.
Network Access Enforcement	Edit	Name of the settings profile the action was performed on.
Patch	Exclude for a specific computer	Name of the patch the action was performed on.
	Exclude for all computers	Name of the patch the action was performed on.
	Stop excluding for a specific computer	Name of the patch the action was performed on.
	Stop excluding for all computers	Name of the patch the action was performed on.
	Mark as 'Manually downloaded'	Name of the patch the action was performed on.
	Mark as 'Requires manual download'	Name of the patch the action was performed on.
Action to take when a threat is reclassified	Edit	
Email sending option	Edit	
Preference for automatic deletion of computers	Edit	

Item type	Action	Item
Preference for VDI environments	Edit	
Preference for risk assessment	Edit	
Preference for MDR	Edit	
Access permission for the Panda Security team	Edit	
Access permission for resellers	Edit	
Email sending option (reseller)	Edit	
Two-factor authentication selection	Edit	
Role	Create	Name of the role the action was performed on.
	Edit	Name of the role the action was performed on.
	Delete	Name of the role the action was performed on.
Task - Security scan	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was

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

Item type	Action	Item
		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 4.10: Item types and actions

System events

This section lists all events that occurred in Panda Endpoint Protection Plus and were not originated by a user account, but by the system itself as a response to the actions listed in Item types and actions.

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 Plus	See Item types and actions
Type	Type of object the action was performed on.	See Item types and actions
Item	Console object the action was performed on.	See Item types and actions

Table 4.11: 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 Plus	See Item types and actions
Type	Type of object the action was performed on.	See Item types and actions
Item	Console object the action was performed on.	See Item types and actions

Table 4.12: Fields in the System events list

Filter tool

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

Table 4.13: Fields in the System events list

Item types and actions

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

Item type	Action	Item
	automatically	performed on.
	Delete automatically	Name of the computer the action was performed on.
Scheduled report	Disable automatically	Name of the scheduled report the action was performed on.

Table 4.14: Item types and actions

Chapter 5

Installing the client software

Installation of the security software involves a series of processes aimed at integrating software components into customers' devices in order to protect against computer threats. This involves the following stages:

- **Deployment**: Creation of the installation package with the components that make up the security solution and which is sent to devices on the network.
- **Installation**: The installation package is unzipped and the files that make up the security software are integrated into the device's operating system.
- **Configuration**: The security software installed on the device receives the required settings and begins to protect the device from the outset, without the need for user action.
- **Integration in the console**: The Panda Endpoint Protection Plus console displays the device to administrators, who can run any necessary actions on it.

Chapter contents

Installation on Windows systems

Protection deployment overview

The installation process consists of a series of steps that depend on the status of the network at the time of deployment and the number of computers and devices you want to protect:

- Find unprotected devices on the network.
- Verify minimum requirements for target devices.
- Uninstall competitor products and restart computers
- Determine device default settings.

- Select a deployment strategy.
- Check that the security software has been correctly installed.

Find 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 Plus. On large networks, this task can be sped up using discovery features (see Viewing discovered computers).
- Verify that you have purchased enough licenses for the unprotected devices (see Licenses on page 177).

Panda Endpoint Protection Plus enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Verify minimum requirements for target computers

For more information about minimum requirements, see Installation requirements.

Uninstall competitor products and restart computers

To create a security settings profile, see Security settings for workstations and servers on page 299. To assign a settings profile to the computers on your network, see Manual and automatic assignment of settings profiles on page 269.

The Panda Endpoint Protection Plus protection services work without you having to restart your computers if you do not have any previously installed antivirus programs.

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

To install Panda Endpoint Protection Plus on a computer that already has a third-party security solution installed, choose between installing it without removing the previous protection or uninstalling it and working exclusively with Panda Endpoint Protection Plus. Assign a **Workstations and servers** settings profile with the **Uninstall other security products** option enabled based on your needs (see Uninstall other security products on page 302. While looking for updates, Panda Endpoint Protection Plus checks the assigned

settings profiles once a day. For a list of the third-party security products that Panda Endpoint Protection Plus uninstalls automatically, see https://www.pandasecurity.com/en/support/card?id=50021.

When you uninstall a third-party antivirus product, you might have to restart the computer..

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

Trial versions

By default, trial versions of Panda Endpoint Protection Plus 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 Plus on a computer with a solution from another vendor other than Panda Security. If there is an uninstaller available for the other vendor's product, it is uninstalled and Panda Endpoint Protection Plus is installed. Otherwise, the installation process stops.

This default behavior can be configured both for trial and commercial versions by assigning a **Workstations and servers** settings profile with the **Uninstall other security products** option disabled.

Panda Security antivirus products

If the target computer already has Panda Endpoint Protection, Panda Endpoint Protection Plus, or Panda Fusion, the solution automatically uninstalls the communications agent and installs the latest Panda agent. It then checks if a protection upgrade is required. If it is required, the computer restarts.

Table 5.1: summarizes how the computer behaves to complete the installation of Panda Endpoint Protection Plus.

Previous product	Panda Endpoint Protection Plus	Restart
None	Trial or commercial version	NO
Panda Endpoint Protection Legacy, Panda Endpoint Protection Plus Legacy	Commercial version	LIKELY (only if a protection upgrade is required)
Third-party antivirus	Trial	NO (by default, both products will coexist)

Previous product	Panda Endpoint Protection Plus	Restart
Third-party antivirus	Commercial version	POSSIBLE (a restart may be necessary to finish uninstalling the third-party product)
Citrix systems	Trial or commercial version	POSSIBLE (with older versions)

Table 5.1: Probability of a restart when installing a new security product

Determine device default settings

When the software is installed on the computer or device, Panda Endpoint Protection Plus assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. See Managing settings on page 261.

If the network settings for the selected group differ from the settings specified during installation, the installation settings apply. See Generating the installation package and manual deployment.

Select a deployment strategy

The deployment strategy depends on the number of computers to protect, the workstations and servers with a Panda agent already installed, and the company network architecture. Several options are available:

- Manual deployment. See Generating the installation package and manual deployment.
- Centralized distribution tool. See Installation from a gold image.
- Remote deployment from the management console. See Computer discovery and remote installation of the client software.
- Installation using gold image generation. See Installation from a gold image.

Check that the security software has been correctly installed

- Select the **Computers** menu at the top of the console. Find the corresponding computer. For more information about how to find computers, see Managing computers and devices on page 199.
- Click the computer on which the security software has been installed. The computer details page opens.
- Select the **Details** tab. All information collected from the computer is shown, along with the installation status.
- In the **Security** section, check the status of the various modules:

- **Installing...**: The installation process is incomplete or there has been an error. Wait a few minutes.
- **Enabled/Disabled:** After a few minutes, if the installation has been successful, the status of the protection modules is shown.

Detect and resolve installation errors

If, after a few minutes, the **Security** section disappears from the computer details page, it is because the security software did not install correctly. Verify this:

- If you installed the security software manually, make sure the user computer does not show any error messages.
- Verify whether the computer appears in lists. See Checking deployment.
- Check the Event Viewer on the user computer. See Checking deployment
- Verify the user computer meets the requirements specified in Installation requirements. Update the product or operating system version if required. See Product updates and upgrades on page 193.

Installation requirements

Make sure the computer you want to install the security software on meets these system and network requirements.

On 30 June 2025, our Windows protection for these OS versions will become End of Life (EOL): Windows XP, Vista, Server 2003, and Server 2008 (Windows 2008 R2 will continue to be supported). After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

Supported operating systems

Panda Endpoint Protection Plus is compatible with 32- and 64-bit x86 microprocessors, as well as ARM microprocessors. For a complete list, see Supported operating systems on page 608.

Panda Endpoint Protection Plus is compatible with Windows XP Embedded and higher. Embedded systems allow custom installations that could impact the way the security software and its modules work.

Hardware requirements

See Hardware requirements on page 610.

Root certificates

It is necessary to keep the root certificates of workstations and servers up to date to use the Panda Endpoint Protection Plus Panda Patch Management module and to establish real-time communications with the management console. See Root certificates on page 610.

SHA-256 compatibility

Workstations or servers must support SHA-256 signed drivers. For more information about affected operating systems and how to update them, see Support for SHA-256 driver signing on page 611. To find computers that do not support SHA-256 driver signing, see Filter computers not compatible with SHA-256 signed drivers on page 209.

TLS 1.2 support

For the Panda Endpoint Protection Plus agent to connect to the Panda Security servers through the TLS 1.2 protocol, see Communication with the Panda Endpoint Protection Plus server through TLS 1.2 on page 612.

Network requirements

Panda Endpoint Protection Plus requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443.

The Panda Endpoint Protection Plus agent requires access to port 33000 for protected computers on the network to communicate with each other and with the Firebox or Access Point device (see Network Access Enforcement on page 290).

For a complete list of the URLs that Panda Endpoint Protection Plus requires access to, see Local ports and URL access on page 620.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection Plus be synchronized. This synchronization is normally achieved using an NTP server. See Time synchronization of computers (NTP) on page 610.

Internet Explorer 7

For advanced protection to operate correctly on a Windows XP or Windows 2003 computer, Internet Explorer 7 or higher must be previously installed on the computer.

You cannot install or upgrade the security software directly on Windows XP computers. You must use a computer with the cache role. For more information, see Configuring downloads from cache computers on page 286

You can install or upgrade the security software on Windows 2003 computers only when the operating system is fully updated and all required patches are installed. Otherwise, you must use a computer with the cache role. For more information, see Panda Patch Management (Updating vulnerable programs) on page 331.

Generating the installation package and manual deployment

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Panda Endpoint Protection Plus.
- Click the Windows icon, both for devices with an x86 or ARM processor. The **Windows** window opens.

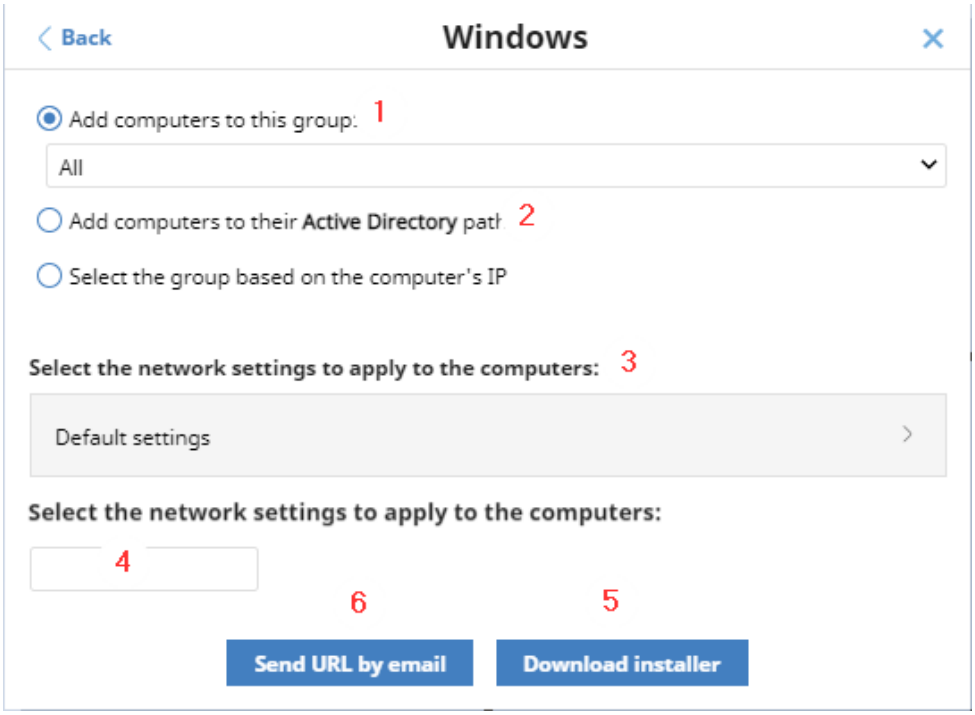


Figure 5.1: Configuring the download package

- Select the group that the computer integrates into in the folder tree (for more information about the different types of groups, see Group types on page 210:
  - To integrate the computer into a native group, click **Add computers to this group (1)**. 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)**.

The security policies assigned to a computer depend on the group it belongs to. If you have selected ***Add computers to their Active Directory path****, and the administrator of the company's Active Directory moves a computer from one organizational unit to another, that change is replicated to the Panda Endpoint Protection Plus console as a group change. Consequently, the security policies assigned to that computer might also change without the administrator of the web management console noticing.*

- To integrate the computer into one group or another based on its IP address, click **Select the group based on the computer's IP (3)** and select the group into which it will be integrated depending on its IP address. See Integrating computers based on their IP address.

- To configure network settings that are different from those assigned to the group which the computer will join, click **Select the network settings to apply to the computers (4)** and choose a network settings profile from the drop-down menu: Initially, all the settings profiles that are applied to a computer upon integration into the console are the profiles that are assigned to the console group it belongs to. However, to avoid connectivity failures and prevent the computer from being inaccessible from the console because of incorrect network settings, you can set an alternative profile. For more information about how to create network settings profiles, see Configuring the agent remotely on page 279.

  - **Native groups and IP groups**: The **Select the network settings to apply to the computers (4)** menu shows the network settings assigned to the group selected in **Add computers to this group (1)**.
  - **Active Directory groups**: The **Select the network settings to apply to the computers (4)** menu shows the network settings assigned to the Active Directory group selected in the group tree. If no Active Directory group was selected before clicking **Add computer**, you need to configure network settings.

- To prevent the installer from being used after a certain date, click the **Indicate whether you want the installer to expire after a specific date** text box and select a date in the calendar.
- To send the installer to the target user by email:
  - Click the **Send URL by email** button **(6)**. The email app installed by default on the administrator's computer opens with a predefined message containing the download URL.
  - Add recipients to the message and click **Send**.
  - The user that receives the message must click the URL from the target device to download the installer.
- To download the installation package and share it with the users on the network, click **Download installer (7)**.

Installing the downloaded package

- Double-click the package and follow the installation wizard. Throughout the process, a window is displayed indicating the progress of the task.
- If there are not enough licenses to allocate one to a computer in the installation process, a warning is displayed on screen. Nevertheless, the computer in question is integrated into the management console but is not protected until sufficient licenses are available.

After it is installed, the agent performs a series of checks automatically:

- **Agent integration into Aether**: The agent sends information from the computer where it is installed to the Panda cloud for integration into the platform.
- **Protection module installer download**: The agent downloads and installs the protection module.
- **Signature file download**: The agent downloads the known malware signature file.
- **Settings download**: The predetermined settings and those created by the administrator are downloaded and applied.
- **Connectivity check to the** Panda **cloud**: If connectivity fails, the error type is reported in the following places:
    - **The agent installation console**: An error message is displayed along with the URLs that could not be accessed. Click the **Retry** button to perform a new check.
    - **The Windows Event Viewer (Event Log)**: An error message is displayed along with the URLs that could not be accessed.
    - **The web console**: An error message is displayed along with the URLs that could not be accessed.

Integrating computers based on their IP address

Panda Endpoint Protection Plus enables IP address ranges and individual IP addresses to be assigned to groups. Computers with an IP address in the group's range are automatically included in it when installed. See Creating and organizing groups on page 211.

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

- If you select **Select the group based on the computer's IP**, Panda Endpoint Protection Plus searches all IPs associated with the group and child groups you select.
- If a single IP address is found, the computer moves to the relevant group.
- If multiple IP groups match the computer IP address, the group that is deepest in the tree is selected. If there are multiple groups at the same level with IP addresses that match the computer IP address, the last one is selected.

- If no matches are found, the computer moves to the selected group. If the selected group does not exist when the computer is integrated, it moves to the **All** group.

After the solution places a computer in a group, if you change the IP address for the computer, the computer does not automatically move to another group. If you change the IP addresses assigned to a group, the computers in the group are not automatically reorganized.

Installation with centralized tools

On medium-sized and large networks, we recommend that you use centralized tools to install the client software for Windows computers.

Using command line tools to install the installation package

You can automate the installation and integration of the the security software into the management console with these command-line parameters:

- **GROUPPATH="group1\group2"**: Path in the group tree where the computer will reside. The 'All' root node is not specified. If the group does not exist, the computer will be integrated into the 'All' root group.
- **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.

This example shows how to use command-line parameters to install the agent:

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="London\AccountingDept"
PRX_SERVER="CorporateProxy" PRX_PORT="3128" PRX_USER="admin" PRX_
PASS="panda"
```

For a silent installation, you must add the `/qn` parameter:

```
Msiexec /i "PandaAetherAgent.msi" /qn
GROUPPATH="Madrid\Contabilidad" PRX_SERVER="ProxyCorporative" PRX_
PORT="3128" PRX_USER="admin" PRX_PASS="panda"
```

Deploying the agent from Panda Systems Management

Panda Systems Management customers can deploy Panda Endpoint Protection Plus for Windows, macOS, and Linux automatically using these 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 do not have any specific requirements besides those described for Panda Systems Management and Panda Endpoint Protection Plus.

Component size:

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

After it is deployed and run, the component downloads the Panda Endpoint Protection Plus installer. Depending on the version, the installer takes up between 6 to 8 MB on each computer.

Deploying the agent with Microsoft Active Directory

Limitations of Microsoft Active Directory when you deploy the security software

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

To prepare the installation GPO (Group Policy Object)

1. Download the Panda Endpoint Protection Plus package and share the installer on the network.
    - Save the Panda Endpoint Protection Plus installer file to a shared folder accessible to all the computers that are to receive the software.
2. Create a new OU (Organizational Unit) called “Aether deployment”.
    - Open the `mmc`. Add the Group Policy Management snap-in.
    - Right-click the domain node. Select **New** and **Organizational Unit**. Create an Organizational Unit called “Aether deployment”.
    - Right-click the new Organizational Unit and select **Block Inheritance**.

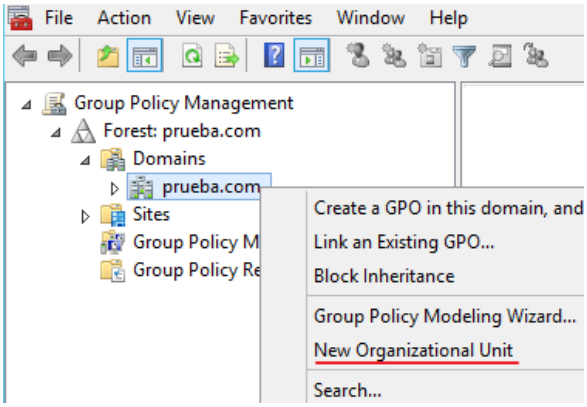


Figure 5.2: New Organizational Unit

3. Create a new GPO with the installation package.

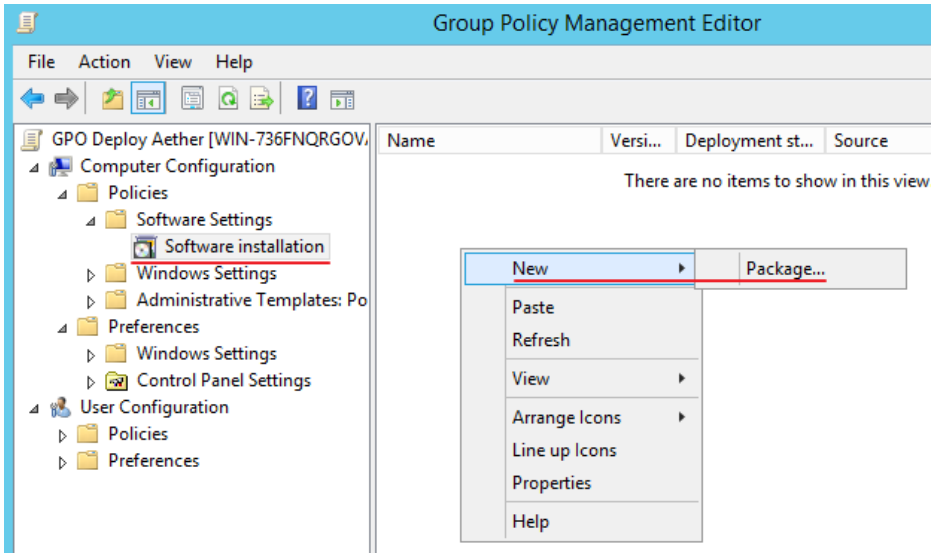


Figure 5.3: New installation package

- Right-click the new Organizational Unit. Select **Create a GPO**. Name the GPO (for example, "Aether deployment GPO").
- Edit the new GPO and add the installation package that contains the Panda Endpoint Protection Plus software. Click **Computer configuration, Policies, Software Settings, Software installation.**
  - Right-click **Software installation**, and select **New**, **Package**.
  - Add the Panda Endpoint Protection Plus `.msi` installation package.

4. Edit the package properties

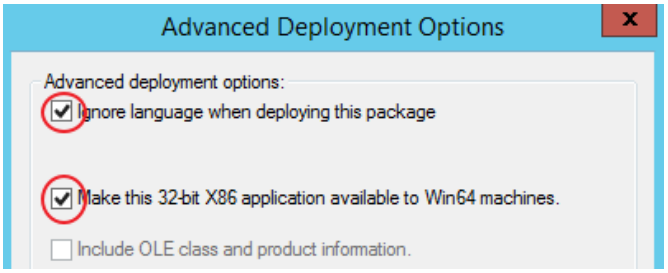


Figure 5.4: Configuring the deployment options

- Right-click the package you added, and select **Properties**, **Deployment** tab, **Advanced**. Select the **Ignore Language when Deploying this Package** and **Make this 32-bit X86 Application Available to Win64 Machines** checkboxes.
- Add all network computers that will receive the agent to the "Aether deployment" Organizational Unit.

Installation from a gold image

Be sure to follow the steps in this section closely to generate and deploy Windows images with Panda Endpoint Protection Plus installed. If you do not follow the procedure exactly as specified, the management and protection capabilities of your product will be reduced.

In large networks with many similar computers, you can automate the process to install the operating system and other software with a gold image. This is sometimes referred to as a master image, base image, or clone image. You then deploy the gold image to all computers on the network, which eliminates most of the manual work required to set up a new computer.

To generate a gold image, install an up-to-date operating system with all the software that users might need, such as security tools, on a computer on your network. When that computer is ready, you must use a virtualization software to 'seal' or 'close' the installation and deploy it to the computers on your network. For specific information about your virtualization solution, see the vendor documentation.

Supported virtual platforms

- VMware Workstation
- VMware Server
- VMware ESX
- VMware ESXi
- Citrix XenDesktop
- XenApp
- XenServer

- MS Virtual Desktop
- MS Virtual Servers

Basic concepts and required tools

ID of VDI computers

Panda Endpoint Protection Plus generates a unique ID in the installation process. The solution uses this ID to identify each computer in the management console.

If you install Panda Endpoint Protection Plus once on the gold image you later copy to the computers on your network, instead of installing it individually on each computer, all cloned computers will inherit the same ID.

Having multiple computers with the same ID leads to the following negative consequences:

- Management capabilities are reduced: The management console shows only one computer, usually the first computer that was added to it. All other cloned computers cannot be accessed from the Panda Endpoint Protection Plus console.
- The protection capabilities of the security software are reduced.

To avoid having multiple computers with the same ID, you must follow a very strict protocol to generate a gold image with no ID. This protocol includes:

- Deleting the ID from the gold image
- Disabling the protection service

Deleting the ID from the gold image

Download the `Endpoint Agent Tool` free tool from the Panda Security support page (password `panda`):

https://www.pandasecurity.com/resources/tools/endpointagenttool.zip

Disabling the protection service

Many virtualization solutions transparently start the newly created gold image as part of the preparation and deployment process. This causes Panda Endpoint Protection Plus to start. When the security software detects that its ID has been deleted, it generates a new ID, rendering the image unusable. To avoid this, you must disable the protection service before you close the gold image, and schedule it to be launched when the cloned computers are started.

There are multiple ways to do this: The most popular method, which we explain in this section, is through a GPO if the computer belongs to a Windows domain. If that is not the case, there are other alternative solutions:

- Some virtualization solutions incorporate this type of tool. For example, VMware Horizon.
- RMM solutions such as Panda Systems Management.
- Tools such as PDQ Deploy, Sysinternals PsExec, Microsoft PowerShell, or scripts that use WMI, among others.

Enabling and disabling Panda Endpoint Protection Plus updates

In non-persistent environments, where the storage system of cloned computers is emptied from time to time, it is important to prevent protection software updates. This can be done when you maintain the gold image, to reduce the bandwidth usage generated by cloned computers and excessive CPU usage on the host system.

To follow the procedures that enable you to successfully generate a gold image, you must assign settings profiles that enable/disable Panda Endpoint Protection Plus updates to the computer you want to clone.

- To enable or disable agent updates, see Communications agent updates on page 196.
- To enable or disable protection updates, see Protection engine updates on page 194.
- To assign settings profiles to computers, see Managing settings on page 261.
- For more information about groups in Panda Endpoint Protection Plus, see Group tree on page 209

Because in some scenarios you must switch between one set of settings profiles and another, we recommend that you create two computer groups in the management console: one with settings profiles that enable Panda Endpoint Protection Plus updates and one with settings profiles that disable them. This way, to enable or disable the updates, you only have to move the computer that has the gold image from one group to another in the console.

Additionally, every time you make changes to a settings profile in the Panda Endpoint Protection Plus console, we recommend that you follow this procedure to make sure that the computer used to generate the gold image receives the new settings:

- Move the computer to the relevant group so that it inherits the new settings.
- In the notification area of the Windows taskbar, right-click the Panda Endpoint Protection Plus icon. A drop-down menu appears.
- Select **Synchronize**. This downloads the new security settings from the server to the target computer.

Creating and deploying a gold image in persistent VDI environments

Steps to take on the computer where the gold image is generated

- Install an updated version of the operating system and all programs that users might need.
- Make sure the computer is connected to the Internet and the MAC address of the computer's network card is static.
- Install Panda Endpoint Protection Plus on a group with updates enabled by following the steps described in Generating the installation package and manual deployment.
- Open the `Endpoint Agent Tool`. Select the checkboxes for **Detections**, **Counters**, and **Check commands**. Click the **Send** button.
- Make sure the **Is a Gold Image** option is not selected.

- If the device is protected by the **anti-tamper protection**, enter the password.
- Click **Prepare image**.
- **Disable the Panda Endpoint Agent service**.
- Turn off the computer and generate the gold image with your virtual environment management software.

Steps to take to enable the protection service

Follow this procedure to enable the Panda Endpoint Agent service on computers cloned through a GPO:

- In the GPO settings, browse to **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **System Services**, **Panda Endpoint Agent**.
- The service appears as **Disabled**. Change it to **Automatic**.

For more information about GPOs, see https://www.microsoft.com/en-us/download/details.aspx?id=21895 .

Creating, deploying, and maintaining a gold image for non-persistent VDI environments

Steps to take on the computer where the gold image is generated

- Install an updated version of the operating system and all programs that users might need.
- Make sure the computer is connected to the Internet.
- Install Panda Endpoint Protection Plus on a group with updates disabled by following the steps described in Generating the installation package and manual deployment.
- Move the computer to a group that has updates enabled.
- If the persistence of the cloned computers is set to be less than one week, it is recommended (although not strictly necessary) to preload the Panda Endpoint Protection Plus caches. Follow one of these two procedures:
    - Open the `Endpoint Agent Tool`. Click the **Start cache scan** button and wait for the process to complete.

      Or
    - Right-click the Panda Endpoint Protection Plus icon on the Windows taskbar.
    - Click **Antivirus**.
    - Click the **Scan now** button and wait for the process to complete.

- Open the `Endpoint Agent Tool`. Select the checkboxes for **Detections**, **Counters**, and **Check commands**. Click the **Send** button.
- Make sure the **Is a gold image** checkbox is selected.
- If the device is protected by the **anti-tamper protection**, enter the password.
- Click **Prepare image**.
- **Disable the Panda Endpoint Agent service**.
- Turn off the computer and generate the gold image with your virtual environment management software.

Steps to take in the Panda Endpoint Protection Plus management console

- Click **Settings** in the top menu. Click **VDI environments** from the side panel.
- Configure the maximum number of non-persistent VDI computers that can be active simultaneously.

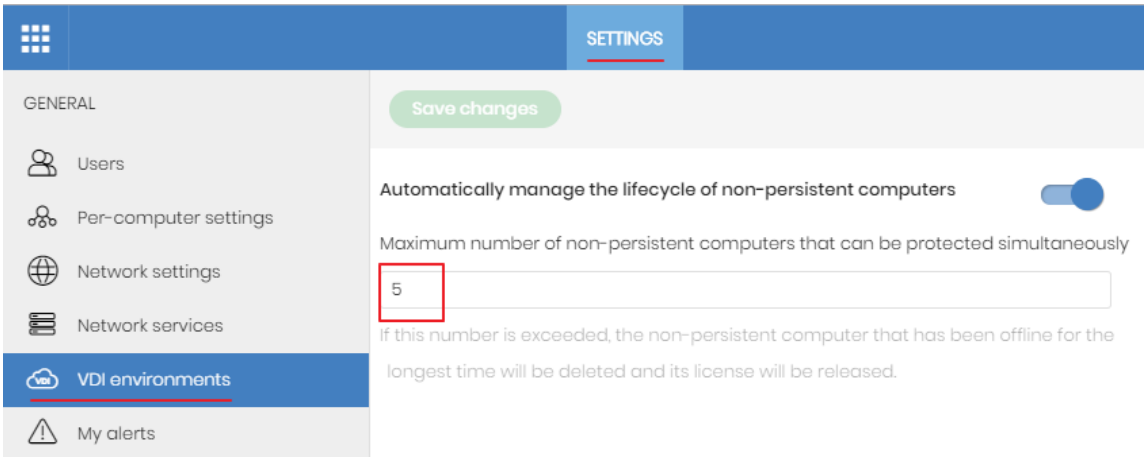


Figure 5.5: Configuring the number of licenses assigned to non-persistent VDI computers

Steps to take to enable the protection service

Follow this procedure to enable the Panda Endpoint Agent service on computers cloned through a GPO:

- In the GPO settings, browse to **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **System Services**, **Panda Endpoint Agent**.
- The service appears as **Disabled**. Change it to **Automatic**.

> *For more information about GPOs, see https://www.microsoft.com/en-us/download/details.aspx?id=21895 .*

Maintaining the gold image in a non-persistent VDI environment

Because the security settings that VDI computers receive have updates disabled, we recommend that you update the gold image manually at least once a month. This makes sure that the VDI computers receive the

latest version of the protection and the signature file. To manually update the gold image in a non-persistent VDI environment:

- Make sure the computer is connected to the Internet.
- Move the computer to a group that has updates enabled.
- Updates are performed silently in the background. We recommend you wait a few minutes to make sure the image is properly updated. If a new version of the protection is available, a restart window is displayed and the computer restarts automatically. When the restart is complete, we recommend you force a new synchronization to make sure Panda Endpoint Protection Plus is fully up to date.
- Preload the Panda Endpoint Protection Plus caches. Follow one of these two procedures:
    - Open the `Endpoint Agent Tool`. Click the **Start cache scan** button and wait for the process to complete.

      Or

    - Right-click the Panda Endpoint Protection Plus icon on the Windows taskbar.
    - Click **Antivirus**.
    - Click the **Scan now** button and wait for the process to complete.
- Open the `Endpoint Agent Tool`. Select the checkboxes for **Detections**, **Counters**, and **Check commands**. Click the **Send** button.
- Make sure the **Is a gold image** checkbox is selected.
- If the device is protected by the **anti-tamper protection**, enter the password.
- Click **Prepare image**.
- Turn off the computer and generate the gold image with your virtual environment management software.
- In the VDI environment, replace the previous image with the new one.
- Repeat this maintenance process at least once per month.

Verifying that all computers are cloned correctly

There is not a single way to verify that computers are cloned correctly in all possible scenarios. The following is a minimum checklist of items to check.

Show persistent and non-persistent VDI computers

The presence of a number of VDI computers in the Panda Endpoint Protection Plus management console lower than the number of VDI computers actually installed on the IT network is a symptom of not having followed the procedure to generate gold images correctly. This can severely affect the management and protection capabilities of your security product.

To view a list of non-persistent VDI computers:

- Go to the **Settings** menu at the top of the console. Click **VDI environments** from the left panel. Click the **Show non-persistent computers** link.
- The **Computers** list shows only non-persistent computers.

To view a list of persistent VDI computers:

- Select the **Computers** menu at the top of the console. Click the folder icon in the left panel. The filter tree appears.
- Click the **All** root node. The right panel shows all computers added to the Panda Endpoint Protection Plus console.
- Verify that all persistent computers are included in the list.

Verify the status of Panda Endpoint Protection Plus updates on cloned computers

- Select the **Computers** menu at the top of the console. Click the folder icon in the left panel. The filter tree appears.
- Find persistent and non-persistent computers in the right panel.
- Click the name of each cloned computer. A page opens that shows the computer details.
- Select the **Settings** tab. A page opens that shows the settings profiles assigned to the computer.
- Verify the **Per-computer settings** and **Security for workstations and servers** profiles have the correct values:
    - For persistent computers, updates must be enabled.
    - For non-persistent computers, updates must be disabled.

Computer discovery and remote installation of the client software

All products based on Aether Platform include tools to find unprotected Windows workstations and servers on the network and to open a remote installation session from the management console.

To remotely install the protection software on a computer using the management console, follow these steps:

- Designate one or more computers on the network as discovery computers. See Designating a discovery computer.
- Make sure the computers on the network meet the minimum requirements. See Operating system and network requirements.
- Start the remote installation of the security software. See Remote installation of the client software.

Discovery computers find computers on the network that the security software does not manage. All computers that meet the necessary requirements appear in the **Unmanaged computers discovered** list, regardless of whether their operating system or device type supports the installation of Panda Endpoint Protection Plus.

> *The first Windows computer that you add to Panda Endpoint Protection Plus is automatically designated as the discovery computer.*

The discovery computer can use one or the two available discovery methods at the same time: discovery using network scanning or discovery using Active Directory. See Using the network to discover computers Using Active Directory to discover computers and Designating a discovery computer.

Designating a discovery computer

- Make sure the computer that you want to designate as a discovery computer has Panda Endpoint Protection Plus installed.
- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab.
- Click the **Add discovery computer** button. From the list, select the computer or computers that you want to perform discovery tasks across the network.

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

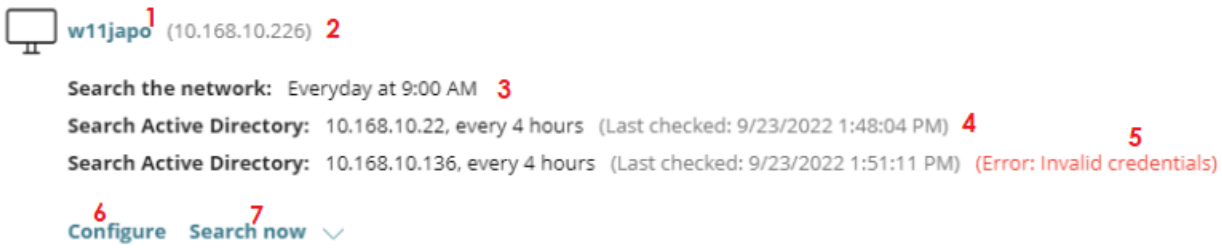


Figure 5.6: Discovery computer information

Field	Description
Computer name (1)	Name of the discovery computer.
IP address (2)	IP address of the discovery computer.
Discovery task settings (3)	Description of the settings of the automatic tasks defined for the discovery computer.

Field	Description
Last checked (4)	Time and date when the discovery task was last launched.
Error codes (5)	• "The computer is turned off or offline": The discovery computer cannot be accessed by the Panda Endpoint Protection Plus server. • Error: Wrong credentials. • Error: Active Directory server not found. • Error (<error code>): If the error is an unknown error.
Configure (6)	Set the discovery task scope and type (automatic or manual). If the task is automatic, it is performed once a day. See Designating a discovery computer.
Search now (7)	Launch the search task manually. See Discovering computers on demand.

Table 5.2: Information displayed for each discovery computer

Using the network to discover computers

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select the discovery computer that you want to configure. Click the **Configure** link. The **Configure discovery on <computer name>** page opens.
- To enable discovery, click the **Discover computers on the network** toggle.
- In the **Discovery scope** section, select an option to limit the scope of the computer search:
    - **Search across the entire network**: The discovery computer uses the network mask configured on the interface to scan its subnet for unmanaged computers. The search is performed only on private IP address ranges.
    - **Search only in the following IP address ranges**: Enter an IP address or IP address range, separated by commas. The IP address ranges must have a "-" (dash or hyphen) in the middle. You can only specify private IP address ranges.
    - **Search for computers in the following domains**: Enter the Windows domains for the discovery computer to search, separated by commas.

The scope settings affect only the subnet where the discovery computer resides. To search for unmanaged devices across all subnets on the network, add at least one discovery computer from each subnet.

Using Active Directory to discover computers

The discovery computer connects to the company's Active Directory to search for computers on the network. Each discovery computer can connect to a maximum of three servers to launch queries against directories.

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select the discovery computer whose scope you want to configure. Click the **Configure** link. The **Configure discovery** page opens.
- To enable discovery, click the **Discover computers in Active Directory** toggle.
- Click the **Add Active Directory server** link. The **Add Active Directory server** window opens.
- Enter the name or IP address (mandatory field) of the server you want to search. Enter the server credentials if required (optional field).
- Click **Save**. The discovery computer asks Active Directory for computers on the network every four hours.

Scheduling computer discovery tasks

You can configure the discovery computer to run discovery tasks at regular intervals.

Network discovery

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. In the list of computers, next to the discovery computer you want to configure, click **Configure**.
- From the **Run automatically** drop-down menu, select **Every day**.
- Select the time of day when the search runs.
- To specify the time based on the time on the discovery computer, select the **Computer's local time** checkbox. If you do not select this checkbox, the time is based on the Panda Endpoint Protection Plus server time.
- Click **Save**. The discovery computer shows a summary of the scheduled task in its description.

Discovery using Active Directory

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select the computer that you want to configure. Click the **Configure** link. The **Configure discovery** page opens.

- Click the Active Directory you want to configure. The **Edit Active Directory server** window opens.
- From the **Recurrence** drop-down menu, select how often searches are run (hours).

Discovering computers on demand

To discover computers on demand, the discovery computer must be up and running and connected to the Panda Endpoint Protection Plus server.

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab.
- Click the **Check now** link next to your chosen discovery computer. If the discovery computer has only one discovery method configured, the **Search for unmanaged computers in progress** message appears and the discovery task is launched in the background.
- If the discovery computer has multiple discovery methods configured, a context menu appears when you click the **Check now** link.
    - **Search everywhere**: The discovery computer scans the network and all configured Active Directory servers.
    - **Search the network**: The discovery computer scans the network.
    - **Search <server_name>**: The discovery computer searches only the selected server.

Viewing discovered computers

Computers discovered using network scanning or Active Directory are shown in the **Unmanaged computers discovered** list.

For more information about computer discovery methods, see Using the network to discover computers and Using Active Directory to discover computers.

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

- **Protection status widget**: Go to the **Status** menu at the top of the console. Go to the Panda Endpoint Protection Plus dashboard that contains the **Protection status** widget. At the bottom of the widget, find the following text: **xx computers have been discovered that are not being managed by Panda Endpoint Protection Plus**. Click the link to open the **Unmanaged computers discovered** list.
- Go to **My lists** in the side menu. Click the **Add** link. A window opens. Select the **Unmanaged computers discovered** list.

Unmanaged computers discovered list

This list shows all computers on the network that do not have Panda Endpoint Protection Plus installed, and those computers where the protection is not working properly, despite being correctly installed.

Field	Description	Values
Computer	Name of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	— **Unmanaged**: The computer is eligible for installation, but the installation process has not started yet. **Installing**: The installation process is in progress. **Installation error**: A message specifying the type of error. For a description of error messages, see Computer notifications section (2) on page 240. With errors whose origin is unknown, the associated error code will be displayed.
IP address	The computer's primary IP address.	Character string
NIC manufacturer	Manufacturer of the discovery computer network interface card.	Character string
Active Directory path	Active Directory path where the computer was last discovered.	Character string
Last discovery computer	Name of the discovery computer that last found the unmanaged workstation or server.	Character string

Field	Description	Values
Last seen	Date when the computer was last discovered.	Date

Table 5.3: Fields in the Unmanaged computers discovered list

If the **Status** field shows the text **Installation error** and the origin of the error is known, a text string is added with a description of the error. For a list of the installation errors reported by Panda Endpoint Protection Plus, see Computer notifications section (2) on page 240.

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Name	Name of the discovered computer.	Character string
IP	The computer's primary IP address.	Character string
MAC address	The computer's physical address.	Character string
NIC manufacturer	Manufacturer of the discovery computer network interface card.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory	Active Directory path where the computer was last discovered.	Character string
First seen	Date when the computer was first discovered.	Character string

Field	Description	Values
First seen by	Name of the discovery computer that first found the user computer.	Character string
Last seen	Date when the computer was last discovered.	Date
Last seen by	Name of the discovery computer that last found the user computer.	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**: A message specifying the type of error. For a description of error messages, see Computer notifications section (2) on page 240.
Error	Error description.	For more information, see Computer notifications section (2) on page 240 .
Installation error date	Date and time when the error occurred.	Date

Table 5.4: Fields in the Unmanaged computers discovered list exported file

Filter tool

Field	Description	Values
Search	Search by computer name, IP address, NIC manufacturer, or discovery computer.	Character string

Field	Description	Values
Status	Panda Endpoint Protection Plus 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**: A message specifying the type of error.
Last seen	Date when the computer was last discovered.	• Last 24 hours • Last 7 days • Last month
Discovery method	Method used to discover the computer	• All • Network scanning. See Computer discovery and remote installation of the client software • Active Directory. See Computer discovery and remote installation of the client software

Table 5.5: Filters available in the Unmanaged computers discovered list

Computer details page

Click any of the rows in the list to open the computer details page.

Discovered computer details

In the **Unmanaged computers discovered** list, click a computer to view its details page. This page is divided into three sections:

- **Computer alerts (1)**: Includes information on alerts or notifications to help you identify 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 found the computer.

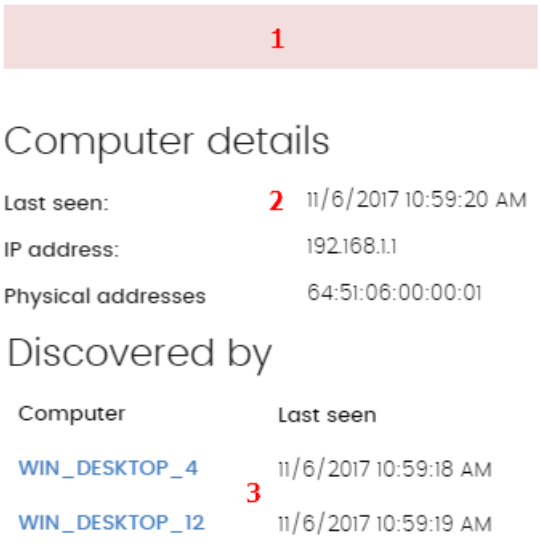


Figure 5.7: Discovered computer details

Computer alerts (1)

Status	Type	Recommended action
Error installing the Panda agent	This message specifies the reason why the agent installation failed.	
	Wrong credentials	Start the installer again with the required credentials 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.
	Unable to register the agent	Make sure the computer is turned on and meets the remote installation requirements.

Status	Type	Recommended action
Error installing the Panda Endpoint Protection Plus protection	This message indicates the reason for the protection installation failure.	
	Insufficient disk space to perform the installation	To see the free space required for installing Panda Endpoint Protection Plus, see Hardware requirements on page 610.
	Windows Installer is not operational	Make sure the Windows Installer service is active. 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	For a list of the third-party solutions that Panda Security can uninstall, see Supported uninstallers.
	There is no uninstaller available to remove the third-party protection installed	Contact technical support to obtain the relevant uninstaller.
Installing the Panda agent	When the installation process is complete, the computer will no longer appear on the list of unmanaged computers discovered.	
Unmanaged computer	The computer does not have the Panda agent installed. Make sure the computer is compatible with Panda Endpoint Protection Plus and meets the requirements specified in Product features and requirements on page 602	

Table 5.6: Computer alerts

Computer details (2)

Field	Description
Computer name	Name of the discovered computer.

Field	Description
Description	Enter a description for the unmanaged computer.
First seen	Date and time when the computer was first discovered.
Last seen	Date and time when the computer was last discovered.
Active Directory path	If the unmanaged computer was discovered using Active Directory, this field indicates the path where it was discovered.
IP address	IP address of the computer network interface card.
Physical addresses (MAC)	Physical address of the computer network interface card.
Domain	Windows domain the computer belongs to.
NIC manufacturer	Manufacturer of the computer network interface card.

Table 5.7: Discovered computer details

Last discovery computer (3)

Field	Description
Computer	Name of the discovery computer that last found the unmanaged computer.
Last seen	Date and time when the computer was last discovered.
Discovery method	Indicates whether the computer was discovered through Active Directory or network scanning.

Table 5.8: Last discovery computer

Deleting and hiding computers

Deleting computers

Panda Endpoint Protection Plus does not automatically delete from the **Unmanaged computers discovered** list computers that are no longer accessible because they were removed from the network (due to theft,

failure, or for other reasons).

To manually delete those computers that are no longer accessible:

- In the **Unmanaged computers discovered** list, click **Discovered** or **Hidden** in the upper-right corner of the page.
- Select the computers you want to remove.
    - To delete multiple computers simultaneously, select the computers. Select **Delete** from the general context menu above the table.
    - To delete a single computer, click the computer's context menu. Select **Delete**.

Any computer you delete from the console without uninstalling the Panda Endpoint Protection Plus software or removing it physically from the network will reappear in the next discovery task. Delete only those computers that you are sure will never be accessible again.

Hiding computers from installation

To minimize long lists of discovered computers that contain devices not eligible for Panda Endpoint Protection Plus, you can hide computers from the installation:

- In the **Unmanaged computers discovered** list, click **Discovered** in the upper-right corner of the page.
- Select the computers you want to hide.
- To hide multiple computers simultaneously, select the computers. Select **Hide and do not discover again** from the general context menu above the table.
- To hide a single computer, click the computer's context menu. Select **Hide and do not discover again**.

Remote installation of the client software

You can remotely install the security software on any unprotected computer discovered. To do that, you must have a discovery computer set up that can connect to the computer you want to install the software on.

Remote installation is only compatible with Windows platforms.

Operating system and network requirements

To install Panda Endpoint Protection Plus remotely, make sure the target computers meet these requirements:

- UDP ports 21226 and 137 must be open for the `system` process.
- TCP port 445 must be open for the `system` process.
- NetBIOS over TCP must be enabled.
- DNS resolution must be enabled.
- Access to the `Admin$` administrative share must be allowed. You must explicitly enable this feature on Windows Home editions.
- You must have domain administrator credentials or credentials for the local administrator account created by default when the operating system was installed.
- Windows Remote Management must be enabled.

To meet these requirements quickly without needing to manually add rules to the Windows firewall, turn on network discovery and file and printer sharing. In ***Control Panel*** *>* ***Network and Sharing Center*** *>* ***Advanced Sharing Settings****, select* ***Turn on network discovery*** *and* ***Turn on file and printer sharing****.*

- Additionally, for a network computer with Panda Endpoint Protection Plus installed to find unmanaged computers on the network, the computers must:
  - Not be hidden by the administrator.
  - Not be currently managed by Panda Endpoint Protection Plus on Aether Platform.
  - Be located on the same subnet segment as the discovery computer.

Remote installation from the Unmanaged computers discovered list

- Go to the **Unmanaged computers discovered** list.
  - Go to the **My lists** section in the left menu. Click the **Add** link. From the window displayed, select the **Unmanaged computers discovered** list.
  - Go to the **Status** menu at the top of the console. In the **Protection status** widget, click the **xx computers have been discovered that are not being managed by Panda Endpoint Protection Plus** link.
  - Go to the **Computers** menu at the top of the console. Click **Add computers**. Select **Discovery and remote installation**. A wizard opens. Click the **View unmanaged computers discovered** link.
- In the **Unmanaged computers discovered** list, click **Discovered** or **Hidden**, based on the status of the relevant computers.
- Select the computer you want to install the software on.

- To install the software on multiple computers simultaneously, select the checkboxes to the left of each computer, then select **Install Panda agent** from the general context menu.
- To install the software on a single computer, click the computer's context menu, then click **Install Panda agent**.

- Configure the installation by following the steps described in Generating the installation package and manual deployment.
- Enter one or multiple installation credentials. Use the local administrator credentials for the target computer(s) or domain administrator credentials.

Remote installation from the computer details page

Select a discovered computer. The computer details page opens. Click **Install Panda agent**. Follow the steps described in Generating the installation package and manual deployment.

Differences in the installation process based on the discovery method used

The procedure to install the protection on selected computers varies based on the method used to discover them.

Installing the protection on computers discovered using network scanning

When a discovery computer discovers another computer using network scanning, it is always connected to the discovered computer. No additional configuration is required beyond what is described in Generating the installation package and manual deployment.

- **If all computers are discovered by the same discovery computer**: The discovery computer launches the installation process on all discovered computers.
- **If NOT all computers are discovered by the same discovery computer**: Each discovery computer launches the installation process on the computers it discovered.

Installing the protection on computers discovered using Active Directory

The fact that a discovery computer discovers another computer by searching in Active Directory does not necessarily mean that it is connected to the discovered computer. In such a case, to remotely install the security software, you must select the discovery computer that will connect to the discovered computer to perform the installation.

- If all selected computers were discovered only through Active Directory, you must select the installer computers that will launch the installation process on the selected computers.
- If the selected computers include computers that were discovered using both methods, you must select the discovery computer that will launch the installation on the selected computers that were discovered only through Active Directory. For all other computers, install the protection as usual by following the steps in Generating the installation package and manual deployment.

Possible installation errors

If the installer computer cannot successfully connect to the discovered computer, the following installation errors are shown:

- In the unmanaged computers discovered list: **Error installing. Unable to connect to the computer.** See Viewing discovered computers.
- On the Computer details on page 236 page: **Error installing the Panda agent**. **Make sure the computer is turned on and meets the remote installation requirements**. See Computer discovery and remote installation of the client software.

Installation on Linux systems

Protection deployment overview

The installation process consists of a series of steps that depend on the status of the network at the time of deploying the software and the number of computers to protect:

- Find unprotected computers on the network
- Verify minimum requirements for target computers
- Uninstall competitor products and restart computers
- Determine computer default settings
- Select an installation method
- Verify the security software has been correctly installed.

Find unprotected computers on the network

Find computers on the network without protection installed or with a third-party security product that needs replacing or complementing with Panda Endpoint Protection Plus. Verify that you have purchased enough licenses for the unprotected computers. See Licenses on page 177.

> *Panda Endpoint Protection Plus enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.*

Verify minimum requirements for target computers

For more information about minimum requirements, see Installation requirements.

Uninstall competitor products

We recommend that you uninstall any third-party antivirus and security software prior to installing Panda Endpoint Protection Plus.

Determine computer default settings

When the software is installed on the computer or device, Panda Endpoint Protection Plus assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. See Managing settings on page 261.

Verify the security software has been correctly installed

- Select **Computers** from the top menu. Find the corresponding computer. For more information about how to find computers, see Managing computers and devices on page 199.
- Select the computer on which the security software has been installed. The computer details page opens.
- Select the **Details** tab. All information collected from the computer is shown, along with the installation status.
- In the **Security** section, verify the status of the various modules:
    - **Installing...**: The installation process is incomplete or there has been an error. Wait a few minutes.
    - **Enabled/Disabled:** After a few minutes, if the installation has been successful, the status of the protection modules is shown.

Detect and resolve installation errors

If, after a few minutes, the **Security** section disappears from the computer details page, it is because the security software did not install correctly. Verify this:

- If the computer has a graphical user interface installed, verify whether there any error messages.
- Verify whether the computer appears in lists. See Checking deployment.
- Verify whether the user computer meets the requirements specified in Installation requirements. Update the product or operating system version if required. See Product updates and upgrades on page 193.

Installation requirements

Make sure the computer you want to install the security software on meets these system and network requirements.

Supported operating systems

See Supported distributions on page 615.

Supported kernels

For more information about the supported Linux kernel versions for each distribution, see Supported kernels.

Hardware requirements

See Hardware requirements on page 616.

Network requirements

Ports 3127, 3128, 3129, and 8310 must be accessible for web filtering and malware web detection to work. On computers with no graphical environment, web filtering and web detection are disabled.

Panda Endpoint Protection Plus requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443.

For a complete list of the URLs that Panda Endpoint Protection Plus requires access to, see Local ports and URL access on page 620.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection Plus be synchronized. This synchronization is normally achieved using an NTP server. See Time synchronization of computers (NTP) on page 610.

Access to the distribution repository

The security software installation process requires access to the repositories that contain the installation packages. These repositories are the responsibility of the distribution vendor who maintains at least one repository for each published version. When a version reaches end-of-life (EOL), the vendor deletes the repository which can cause the security software installation to fail. We recommend that you:

- Use a local repository.
- Install the software without dependencies. See Installation on Linux computers with limited Internet access on page 133.

Packages installed on computers

When you run it, the installation script performs a number of checks that require installation of one of these packages:

- wget
- curl

If neither of these packages are installed, the installation process fails returning an error.

Generating the installation package and manual deployment

- From the top menu, select **Computers**. In the upper-right corner of the page, click **Add computers.** A dialog box opens that shows all platforms supported by Panda Endpoint Protection Plus.
- Click the **Linux** icon. The **Linux** dialog box opens.

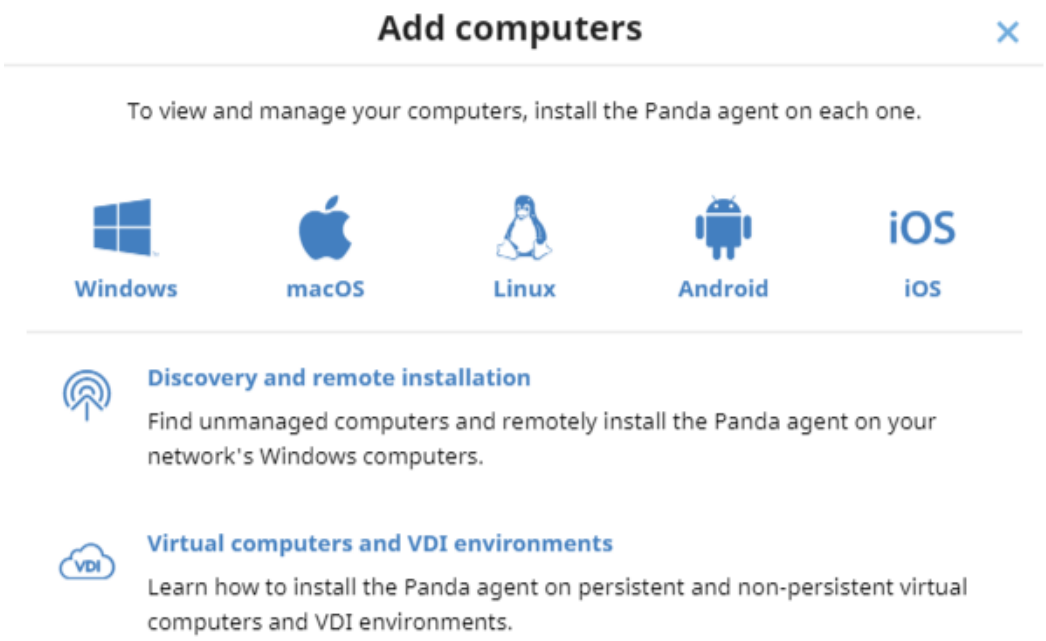


Figure 5.8: Dialog box for selecting a platform supported by Panda Endpoint Protection Plus

- To add the computer to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To add the computer to an Active Directory group, select **Add computers to their Active Directory path**.

> *The security policies assigned to a computer depend on the group it belongs to. If you select **Add computers to their Active Directory path**, and the Active Directory administrator moves a computer from one organizational unit to another, the change is reflected in the Panda Endpoint Protection Plus console as a group change. The security policies assigned to the computer might also change.*

- To establish a network settings profile other than the profile of the group the computer is added to, click **Select the network settings to apply to the computers**. From the drop-down list, select a settings profile. Initially, all the settings profiles that are applied to a computer when you add it to the console are the profiles that are assigned to the console group it belongs to. However, to avoid connectivity issues and prevent the computer from being inaccessible from the console because of incorrect network settings, you can set an alternative profile. For more information about how to create network settings profiles, see Configuring the agent remotely on page 279.
- To send the installer to the target user by email:

- Click the **Send URL by email** button. Your email application opens a new email with the download URL.
- Add recipients to the message. Click **Send**.
- When a user clicks the link, the installer downloads.

- To download the installation package and share it with the users on the network, click **Download installer**.

Installation on Linux computers

Depending on the characteristics of the target computer, you can install the agent in multiple ways:

- Installation on Linux computers with an Internet connection
- Installation on Linux computers with Secure Boot
- Installation on Linux computer with limited Internet access

Installation on Linux computers with an Internet connection

Make sure you have administrator permissions on the device. Make sure the downloaded package has execute permissions. The installer searches the target computer for the libraries it needs. If it cannot find the libraries, it downloads them automatically from the Internet.

- Open a terminal in the folder where the downloaded package is located. Run these commands:

```
$ sudo chmod +x "/DownloadPath/Panda Endpoint Agent.run"
$ sudo "/DownloadPath//Panda Endpoint Agent.run"
```

- On hardened computers, use the `--target ./install/` command to generate a temporary folder in the script location.

```
$ sudo "/DownloadPath/Panda Endpoint Agent.run" --target ./install/
```

- If you use a proxy server to access the Internet, add this parameter: `--proxy`. If you want to specify a list of proxy servers, use this parameter: `--proxy=<proxy-list>` . The installation script uses the first proxy server in the list. If the server fails, the script continues down the list of proxy servers until it finds one that works.

  `<proxy-list>` is a list of proxy servers separated by commas. Users and protocols are indicated with this syntax:

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

  For example, to install a Linux agent that uses two proxy servers:

```
$ sudo "/DownloadPath/Panda Endpoint Agent.run" -- --
proxy=http://user1:pass1@192.168.0.1:3128,
http://user2:pass2@192.168.0.2:3128
```

- To verify that the `AgentSvc` process is running, run this command:

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

- Make sure this installation directory was created:

```
/usr/local/management-agent/*
```

Installation on Linux computers with Secure Boot

Some Linux distributions detect when a computer has Secure Boot enabled. With Secure Boot enabled, the security software that is not correctly signed is automatically disabled. Secure Boot is detected when the software is installed, or later, if the distribution did not initially support this feature but it was added in a later update. In either case, the console shows an error and the protection software does not run. To solve the protection errors related to Secure Boot from the computer experiencing the problem, make sure your system meets these requirements and complete the steps to resolve the errors:

System requirements

- **DKMS (Dynamic Kernel Module Support) systems**: `mokutil` and `openssl` packages.
- **Oracle Linux 7.x/8.x with UEKR6 kernel**: Repository `ol7_optional_latest` enabled, and `openssl`, `keyutils`, `mokutil`, `pesign`, `kernel-uek-devel-$(uname -r)` packages.

Enabling the security software on computers with Secure Boot

To enable the security software on the target computer:

- Check the state of Secure Boot:

```
$ mokutil --sb-state
```

If Secure Boot is enabled on the computer, `Secure Boot enabled` displays.

- Verify that the protection driver is not loaded:

```
$ lsmod | grep prot
```

- Import the protection keys:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

The agent and protection files have this format: ***protection-agent-03.01.00.0001-1.5.0_741_g8e14e52****. The name varies according to the version and the driver.*

A message appears to explain the implications of Secure Boot.

- Press **C** to register the certificate used to sign the modules.
- Enter an eight-character password.
- Restart the computer and complete the registration process:
    - To start the registration process, press any key. This screen appears for a limited time. If you do not press a key, you must restart the registration process.
    - Select **Enroll MOK**. To view the keys that are going to be registered, select **View key**.
    - Confirm the keys belong to Panda Security. Select **Continue**.
    - To enroll the key, select **Yes**.
    - Enter the password created in step 3. Select **Reboot**.
    - Confirm the driver is loaded:

```
$ lsmod | grep prot
```

Oracle Linux 7.x/8.x with UEKR6 kernel

When the distribution installed is Oracle Linux 7.x/8.x with UEKR6 kernel, after you complete the steps to register the certificate, follow these steps:

- Run this command:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

This command adds the certificate used to sign the modules to the list of certificates trusted by the kernel. The modified kernel is signed and added to the list of kernels in GRUB.

- Restart the computer. The module is loaded and started.
- To confirm that the certificate was added correctly, run this command:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

The results should be:

```
The signer’s common name is UA-MOK Driver Signing
```

```
 Image /boot/vmlinuz-kernel-version-panda-secure-boot is already
signed
 Kernel module is successfully loaded
```

Installation on Linux computers with limited Internet access

Panda Endpoint Protection Plus must connect to the Internet to work correctly. However, you might want to restrict Internet access for the servers on which the security software runs to prevent information from being downloaded or sent from or to unknown external sources. In such case, Panda Endpoint Protection Plus cannot complete the installation process because it requires access to external repositories to satisfy its dependencies.

This installation method enables you to install the security software on computers that can access only the Pandacloud, from which they can download a package with all required libraries.

With this installation method, the third-party libraries included in the package that have errors or vulnerabilities do not automatically update on the protected computer.

The installer is compatible with these Red Hat-based distributions:

- Red Hat
- CentOS
- CentOS Stream
- SuSE Linux Enterprise
- openSUSE
- Oracle Linux
- Alma Linux
- Rocky Linux

For more information about the supported versions of these distributions, see Supported distributions on page 615

The installer is compatible with these Linux agent and protection versions:

- Protection version: 3.00.00.0050 and higher.
- Agent version: 1.10.06.0050 and higher.

If you use the package with an unsupported Linux distribution, the installation process will fail. You can use this installation method only if you install the solution on a computer that does not have a previous version of the security software installed. Otherwise, the repository previous settings are kept.

To install the Panda Endpoint Protection Plus agent without an Internet connection, open a terminal in the folder where the downloaded package is located. Run these commands:

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

Installation on macOS systems

Protection deployment overview

The installation process consists of a series of steps that vary depending on the status of the network at the time of deploying the software and the number of computers to protect:

- Find unprotected devices on the network
- Verify minimum requirements for target devices
- Uninstall competitor products
- Determine device default settings
- Verify the security software has been correctly installed.

Find unprotected devices on the network

Find devices on the network without protection installed or with a third-party security product that needs replacing or complementing with Panda Endpoint Protection Plus. Verify that you have purchased enough licenses for the unprotected devices. See Licenses on page 177.

Panda Endpoint Protection Plus enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Verify minimum requirements for target devices

For more information about minimum requirements, see Installation requirements.

Uninstall competitor products

We recommend that you uninstall any third-party antivirus and security software prior to installing Panda Endpoint Protection Plus.

Determine device default settings

When the software is installed on the computer or device, Panda Endpoint Protection Plus assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. See Managing settings on page 261.

Verify the security software has been correctly installed

- Select **Computers** from the top menu. Find the corresponding computer. For more information about how to find computers, see Managing computers and devices on page 199.
- Select the computer on which the security software has been installed. The computer details page opens.
- Select the **Details** tab. All information collected from the computer is shown, along with the installation status.
- In the **Security** section, verify the status of the various modules:
    - **Installing...**: The installation process is incomplete or there has been an error. If the process failed, the status does not change until the installation problem is resolved.
    - **Enabled/Disabled:** After a few minutes, if the installation has been successful, the status of the protection modules is shown.

Detect and resolve installation errors

If, after a few minutes, the **Security** section disappears from the computer details page, it is because the security software did not install correctly. Verify this:

- Verify whether the user computer shows error messages.
- Verify whether the computer appears in lists. See Checking deployment.
- Verify whether the user computer meets the requirements specified in Installation requirements. Update the product or operating system version if required. See Product updates and upgrades on page 193.

Installation requirements

Make sure the computer you want to install the security software on meets these system and network requirements.

On 30 June 2025, our Mac protection for these OS versions will become End of Life (EOL): macOS Yosemite, El Capitan, Sierra, High Sierra, or Mojave. After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

Supported operating systems

See Supported operating systems on page 612.

Hardware requirements

See Hardware requirements on page 613.

Network requirements

Panda Endpoint Protection Plus requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443. For a complete list of the URLs that Panda Endpoint Protection Plus requires access to, see Local ports and URL access on page 620.

To activate the product, access to certain IP address ranges is required. For more information, see IP addresses required for product activation on page 613.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection Plus be synchronized. This synchronization is normally achieved using an NTP server. See Time synchronization of computers (NTP) on page 610.

Required permissions

For the protection to operate correctly, you must enable:

- Network extensions.
- System extensions.
- Full disk access.
- Background execution.

For more information, see Required permissions on page 613.

Manually deploying the macOS agent

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Panda

Endpoint Protection Plus.

- Click the **macOS** icon. The **macOS** window opens.

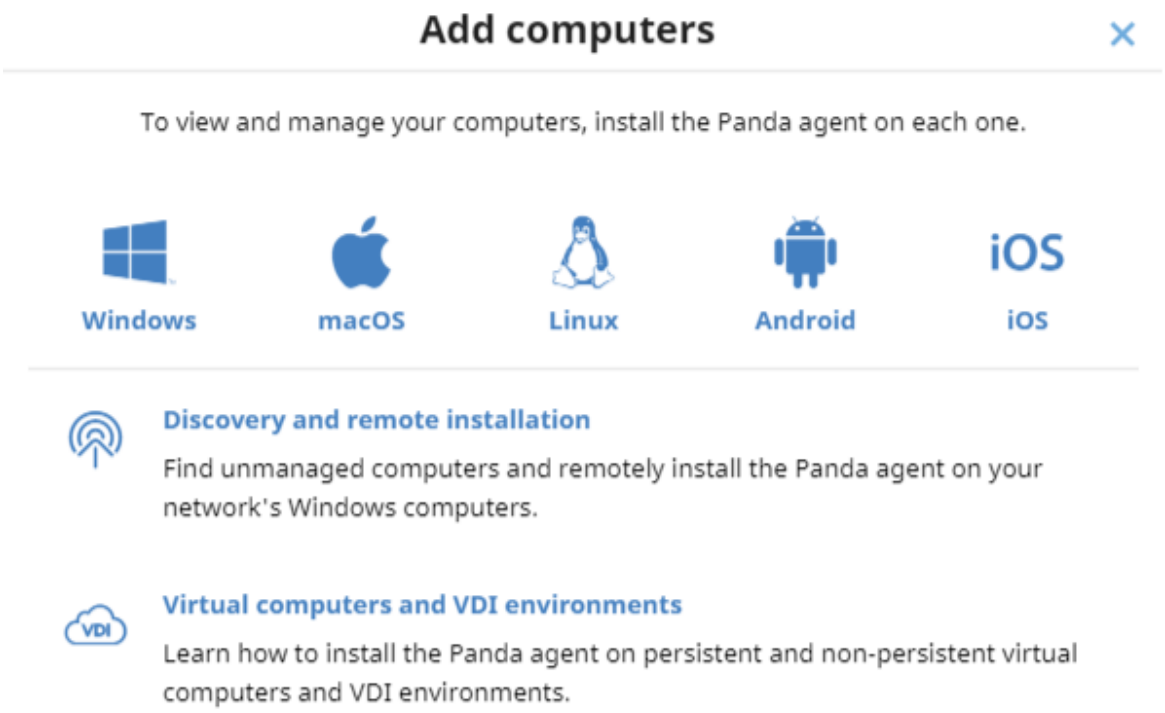


Figure 5.9: Window for selecting a platform supported by Panda Endpoint Protection Plus

- To add the device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To establish a network settings profile other than the profile of the group the computer is integrated into, click **Select the network settings to apply to the computers**. Choose a settings profile from the drop-down list. Initially, all the settings profiles that are applied to a computer upon integration into the console are the profiles that are assigned to the console group it belongs to. However, to avoid connectivity failures and prevent the computer from being inaccessible from the console because of incorrect network settings, you can set an alternative profile. For more information about how to create network settings profiles, see Configuring the agent remotely on page 279.

  To send the installer to the target user by email:

  - Click the **Send URL by email** button. The email app installed on the administrator's computer opens with a predefined message containing the download URL.
  - Add the desired recipients to the message. Click **Send**.
  - The user that receives the message must click the URL from the target device to download the installer.
- To download the installation package and share it with the users on the network, click **Download installer (7)**.

Installing the downloaded package

- Double-click the `.dmg` file. Run the `.pkg` container. A progress bar displays during the installation process. Regardless of whether there are free licenses available, the computer is integrated into the service. However, if there is no available license to assign to the target computer, the computer is not protected.
- When the installation completes, the product checks that it has the latest version of the signature file and the protection engine. If not, it updates them automatically.
- To make sure the agent is installed, and verify that the AgentSvc process is running, run this command:

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

- (Optional) Verify that the installer created these directories:

```
/Applications/Management-Agent.app/
/Library/Application Support/Management Agent/
```

To install the product agent on devices with macOS Catalina, you must assign specific permissions. For more information, see: https://www.pandasecurity.com/en/support/card?id=700079 .

Installation on Android systems

Protection deployment overview

The installation process consists of a series of steps that depend on whether the target devices are managed with an MDM/EMM solution or not.

MDM (Movile Device Management)/EMM (Enterprise Mobility Management) is software that enables organizations to monitor and manage mobile devices regardless of the mobile operator or service provider chosen. MDM/EMM solutions enable you to remotely install apps on managed devices, locate and track managed devices, sync files across them, and report data remotely and centrally. These solutions are commonly found in companies that manage a large number of devices.

To deploy and install the protection software, follow these steps:

- Find unprotected devices on the network.
- Verify minimum requirements for target devices. See Installation requirements.

- Uninstall competitor products prior to installing Panda Endpoint Protection Plus.
- Determine device default settings. See Determine device default settings.
- Select a deployment strategy based on whether the target device is enrolled into an MDM/EMM solution. See Select a deployment strategy.

Find unprotected devices on the network

Find devices on the network without protection installed or with a third-party security product that needs replacing or complementing with Panda Endpoint Protection Plus. Verify that you have purchased enough licenses for the unprotected devices. See Licenses on page 177.

Panda Endpoint Protection Plus enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Determine device default settings

When the software is installed on the computer or device, Panda Endpoint Protection Plus assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. To create and assign new settings profiles, see Managing settings on page 261.

Select a deployment strategy

Depending on whether the target devices are enrolled into an MDM/EMM solution or not, and on the type of solution, the following deployment types are supported:

- Manual deployment on devices not enrolled into an MDM/EMM solution. See Manually deploying and installing the Android agent.
- Deployment using a third-party MDM/EMM solution. See Deploying the Android agent using an MDM/EMM solution .

Installation requirements

Make sure the device you want to install the security software on meets these system and network requirements.

Supported operating systems

See Supported operating systems on page 617.

Hardware requirements

See Hardware requirements on page 618.

Network requirements

In normal conditions, if the device is connected to the network by 2G, 3G, 4G, or higher, there are no specific network requirements. In other scenarios, you must open certain ports to all IP addresses contained in the IP blocks listed in Google's ASN 15169. See Network requirements on page 618.

Permissions required on the device

To use all of the Panda Endpoint Protection Plus features, the user of the device must allow all permissions requested by the application. For a complete list of required permissions, see Permissions required on the device on page 618.

Manually deploying and installing the Android agent

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Panda Endpoint Protection Plus.
- Click the **Android** icon. The **Android** window opens.

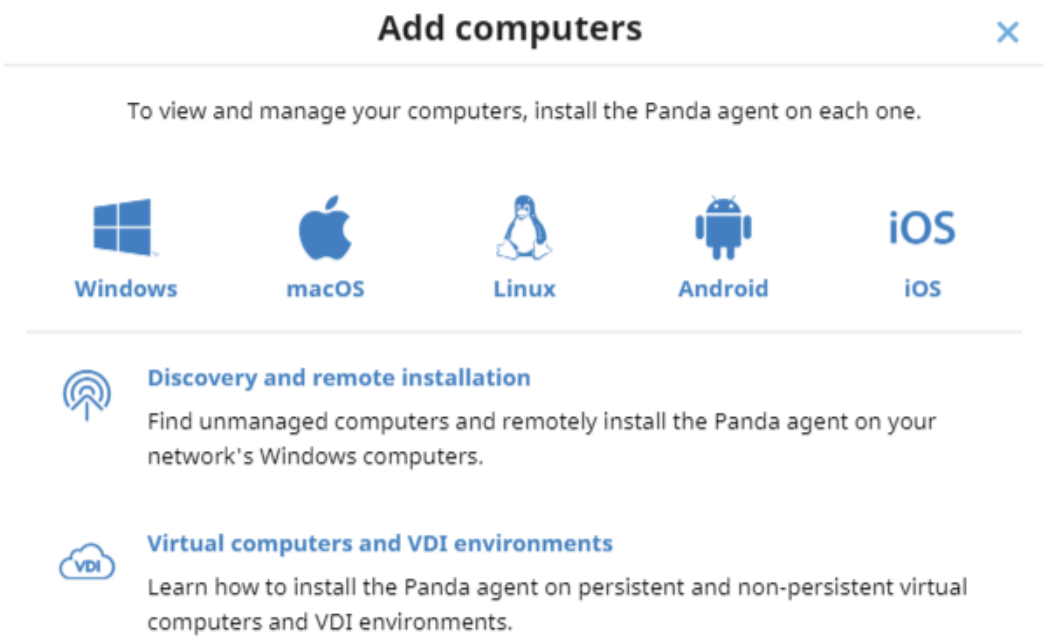


Figure 5.10: Window for selecting a platform supported by Panda Endpoint Protection Plus

- To add the Android device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To install the Android agent on the device using the QR code:
  - Point the device camera at the QR code on the computer screen. You are taken to the **Protection - Panda Aether** app page on Google Play.
  - Tap the **Install** button. The app is automatically downloaded and installed.

- To download the installer to the target device directly from Google Play:
    - Tap the **Go to Google Play** icon from the target device. You are taken to the **Protection - Panda Aether** app page on Google Play.
    - Tap the **Install** button. The app is automatically downloaded and installed.
- To send the installer to the target user by email:
    - Click the **Send URL by email** button. The email app installed by default on the administrator's computer opens with a predefined message containing the download URL.
    - Add the desired recipients to the message. Click **Send**.
    - The user that receives the message must tap the URL from the target device. The user is taken to the **Protection - Panda Aether** app page on Google Play.
    - The user must tap the **Install** button. The app is automatically downloaded and installed.
- The first time the app is launched on the mobile device, the **Enter alias** screen opens.
- Enter the name that will be displayed in the Panda Endpoint Protection Plus console to identify the device. Tap **Continue**. A series of installation status messages is displayed, and a screen for the user to grant a number of permissions to the app. If the user does not grant those permissions to the app, the app will not work correctly. See Permissions required on the device on page 618.
- Regardless of whether the permissions are granted or not, the installation process completes and the device appears in the Panda Endpoint Protection Plus management console.

Deploying the Android agent using an MDM/EMM solution

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection Plus.
- Click the **Android** icon. The **Android** window opens.
- Click the **Send URL by email** button. The email program installed by default on the administrator's computer opens with a predefined message containing the download URL Write down the link to use it as integration URL with your MDM/EMM solution.
- In your MDM or EMM solution, import the **WatchGuard Mobile Security** app that you obtained from Play Store.
- In your MDM or EMM solution, add the following as parameters for the app you imported in the previous step:
    - **Use automatic name**: Boolean parameter. If the value of the parameter is **True**, a name based on the "<Device model>_<Unique identifier>" pattern is automatically assigned.
    - **Device name**: The name that is assigned to the device if the value of the **Use automatic name** parameter is **False**. You can use wildcards and other special characters as per the

specifications of your MDM or EMM solution to generate a different name for each device.

- **Integration URL**: The integration URL shown in the Panda Endpoint Protection Plus console.

- The first time the app is launched on the mobile device, the **Enter alias** screen opens.
- If the **Use automatic name** parameter is set to **False**, and **Device name** is not defined, the app prompts for the name with which it will show the device in the Panda Endpoint Protection Plus console.
- Tap **Continue**. A series of messages showing the status of the installation process is displayed, as well as a screen prompting the user to grant a number of permissions to the app. If the user does not grant those permissions to the app, the app will not work correctly. See Permissions required on the device on page 618.
- Regardless of whether the permissions are granted or not, the installation process completes and the device appears in the Panda Endpoint Protection Plus management console.

Installation on iOS systems

Protection deployment overview

The installation process of the protection on iOS devices consists of a series of steps that depend on whether there is an MDM (Mobile Device Management) solution implemented in the organization:

- Find unprotected devices.
- Verify minimum requirements for target devices. See Installation requirements.
- Uninstall competitor products prior to installing Panda Endpoint Protection Plus.
- Determine device default settings. See Select a deployment strategy.
- Select a deployment strategy based on whether the target device is enrolled into an MDM solution. See Select a deployment strategy.

Find unprotected devices on the network

Find devices on the network without protection installed or with a third-party security product that needs replacing or complementing with Panda Endpoint Protection Plus. Verify that you have purchased enough licenses for the unprotected devices. See Licenses on page 177.

Panda Endpoint Protection Plus enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Determine device default settings

When the software is installed on the computer or device, Panda Endpoint Protection Plus assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required network settings. To create and assign new settings profiles, see Managing settings on page 261.

Select a deployment strategy

The iOS agent deployment process varies depending on whether the target device is managed with an MDM solution or not.

- Manual deployment on devices not enrolled into an MDM solution See Deploying and installing the agent on devices not enrolled into an MDM solution.
- Deployment using the Panda MDM solution. See Deploying and installing the agent on devices enrolled into the Panda MDM solution.
- Deployment using a third-party MDM solution. See Deploying and installing the agent on devices enrolled into a third-party MDM solution.
- Deployment on supervised devices with Panda MDM. See Configuring the device in supervised mode and enrolling it into the Panda MDM solution.
- Deployment on supervised devices with third-party MDM. See Enabling supervised mode and deploying the iOS agent from a third-party MDM solution.

For more information about possible scenarios in Panda Endpoint Protection Plus, see Basic concepts.

If the target device is managed with the Panda MDM solution, see Managing the Apple ID and digital certificates.

Basic concepts

MDM (Movile Debice Management)

MDM is software that enables organizations to monitor and manage mobile devices regardless of the mobile operator or service provider chosen. Most MDM solutions enable you to remotely install apps on iOS devices, locate and track iOS devices, sync files across them, and report data remotely and centrally. These solutions are commonly found in companies that manage a large number of devices.

Managing iOS devices with an MDM solution

An iOS device can only be remotely managed with one MDM solution at a time. To manage an iOS device using an MDM solution, you must first enroll it into the solution. At the end of the enrollment process, a settings profile is sent from the MDM solution to the device, which the user must install on it.

PandaMDM

Because the remote management options for an iOS device are very limited if the device is not enrolled into an MDM solution, Panda Endpoint Protection Plus seamlessly incorporates its own MDM solution into the

management console. Additionally, because each iOS device can only be remotely managed with one MDM solution, it is very important that you make the right decision regarding which MDM solution will manage the organization's devices when integrating them into Panda Endpoint Protection Plus.

If your iOS devices were already enrolled into a third-party MDM solution and you decide to enroll them into the Panda MDM solution, you will lose the centralized management capabilities provided by your MDM solution and will not be able to access any software you deployed through it. See ***Enrollment types supported by Panda Endpoint Protection Plus****.*

Enrollment types supported by Panda Endpoint Protection Plus

Based on the enrollment type, Panda Endpoint Protection Plus provides the administrator with different features from the management console.

Enrollment type	Features available in the Panda Endpoint Protection Plus console
Installation on iOS devices enrolled into the Panda (recommended if you did not already use an MDM solution)	• Hardware inventory • Software inventory • Web protection * • Web filtering * • Geolocation • Remote alarm • Wipe data • Lock
Installation on iOS devices enrolled into a third-party MDM solution (recommended if you already used an MDM solution)	• Hardware inventory • Web protection * • Web filtering * • Geolocation • Remote alarm
Installation on iOS devices not enrolled into an MDM solution	• Hardware inventory • Geolocation • Remote alarm

Table 5.9: Enrollment types supported by Panda Endpoint Protection Plus

* To filter web traffic, the iOS device must be in supervised mode.

Requirements for integrating a device using the Panda MDM solution

To integrate an iOS device into the Panda Endpoint Protection Plus management console using the Panda MDM solution, you need:

- **An Apple user account (Apple ID)**: Required to generate and import certificates into the management console. You can use an existing account or create a new one.
- **A digital certificate issued by Apple**: Required for the iOS devices you want to manage to be able to communicate securely with the Apple servers. Digital certificates are valid for one year, after which they expire. Register all of your company's iOS devices with the same digital certificate.

For more information, see Managing the Apple ID and digital certificates.

Installation requirements

Make sure the device you want to install the security software on meets these system and network requirements.

Supported operating systems

See Supported operating systems on page 618.

Hardware requirements

The minimum space required to install the security software varies depending on the operating system version installed on the device. On average, the security software requires 12 MB of available space for installation.

Network requirements

The application installed on the mobile device uses the Apple Push Notification service to communicate with Panda Endpoint Protection Plus. If the device is connected to the network by 2G, 3G, or 4G, there are no specific network requirements. For other scenarios, see Network requirements on page 619.

Permissions required on the device

To use all of the Panda Endpoint Protection Plus features, the user of the device must allow all permissions requested by the application. For a complete list of required permissions, see Permissions required on the device on page 620.

Deploying and installing the iOS agent

Deploying and installing the agent on devices not enrolled into an MDM solution

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Panda

Endpoint Protection Plus.

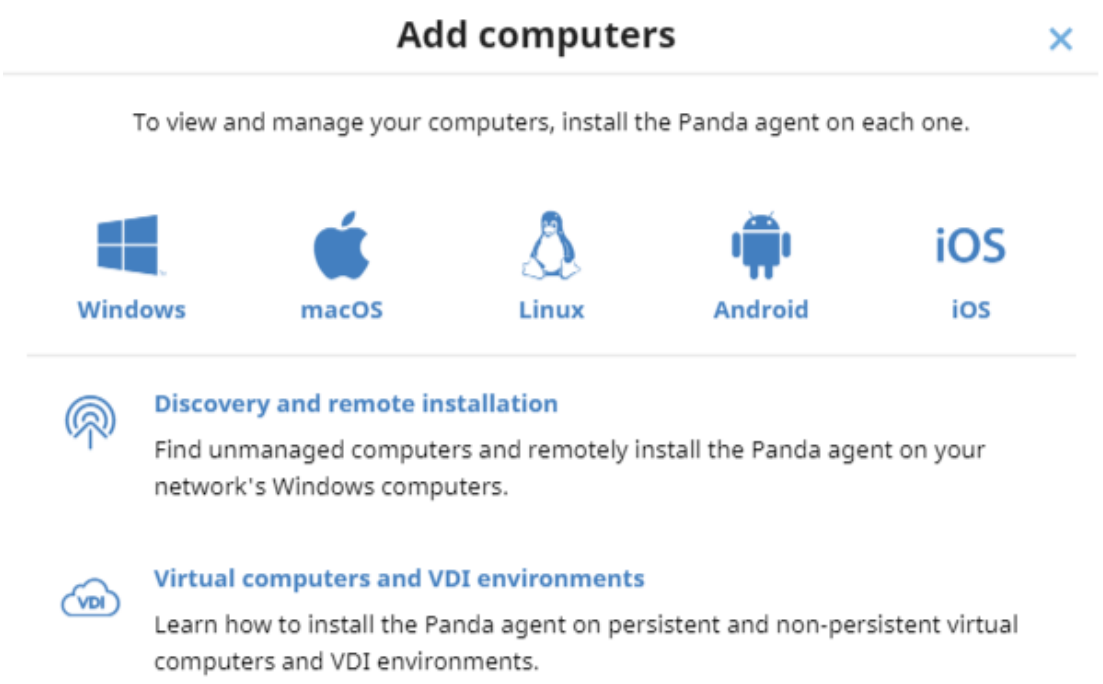


Figure 5.11: Window for selecting a platform supported by Panda Endpoint Protection Plus

- Click the **iOS** icon. The **iOS** window opens.
- Click the **Installation without an MDM solution** link. The **iOS** window opens.
- To add the iOS device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To install the iOS agent on the device using the QR code:
    - Point the device camera at the QR code on the computer screen. You are taken to the **WatchGuard Mobile Security** app page on the App Store.
    - Tap the **Install** button. The app is automatically downloaded and installed.
- To download the installer to the target device directly from the App Store:
    - Tap the **Go to Apple Store** icon from the target device. You are taken to the **WatchGuard Mobile Security** app page on the App Store.
    - Tap the **Install** button. The app is automatically downloaded and installed.
- To send the installer to the target user by email:
    - Click the **Send URL by email** button. The email app installed by default on the administrator's computer opens with a predefined message containing the download URL.
    - Add recipients to the message and click **Send**.

    - The user that receives the message must tap the URL from the target device. The user is taken to the **WatchGuard Mobile Security** app page on the App Store.
    - The user must tap the **Install** button. The app is automatically downloaded and installed.
- The first time the app is launched on the iOS device, a welcome window opens with the text **"WatchGuard Mobile Security" Would Like to Send You Notifications**. Tap the **Allow** button.
- If the **WatchGuard Mobile Security** app was installed by searching for it manually on the App Store, you must integrate it manually into Panda Endpoint Protection Plus.
    - Tap the **Use QR Code** button. The message **"WatchGuard Mobile Security" Would Like to Access the Camera** appears.
    - Tap **Allow**. Point the phone camera at the QR code in the Panda Endpoint Protection Plus management console. The message **Downloading configuration** appears on the mobile phone.
- When the configuration finishes downloading, the message **"WatchGuard Mobile Security" Would Like to Find and Connect to Devices on Your Local Network** appears. Tap **OK**. The **Enter alias** window opens.
- Enter the name that will be used in the Panda Endpoint Protection Plus console to identify the device. Tap **Continue**. A number of installation status messages are shown. Then, the message **"WatchGuard Mobile Security" Would Like To Filter Network Content** appears.
- Tap the **Allow** button. The **Enter the iPhone code** window opens.
- Enter the device password. The **OK** window opens. The installation is complete.

Deploying and installing the agent on devices enrolled into the Panda MDM solution

- Verify you have a valid Apple certificate uploaded to the Panda Endpoint Protection Plus management console. To generate a certificate, see Creating and importing the digital certificate into the Panda Endpoint Protection Plus console. If your certificate is about to expire, see Renewing the Apple certificate.
- Make sure your company's iOS devices do not have a third-party MDM profile already installed. If they do, delete the profile from your devices. For more information about the implications of deleting a third-party MDM profile, see Managing iOS devices with an MDM solution and Enrollment types supported by Panda Endpoint Protection Plus.
- Select the **Computers** menu at the top of the Panda Endpoint Protection Plus management console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. A window opens with information about the previously uploaded certificate.

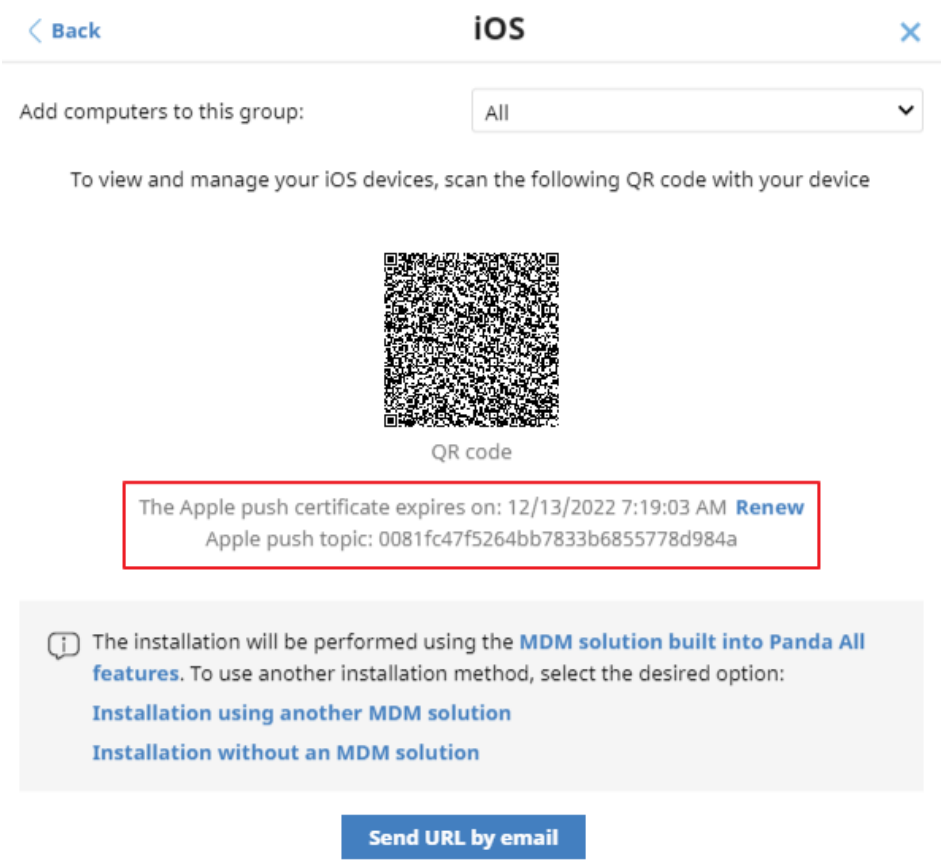


Figure 5.12: Window with the uploaded Apple digital certificate

- To add the iOS device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- Choose a method for sending the installation profile to the target iOS device:
    - To send the installation profile using the QR code, scan the code with the device camera. The device shows the message **This website is trying to download a configuration profile. Do you want to allow this?**
    - To send the installation profile download link to the target user by email, click the **Send URL by email** button. When the device user clicks the link, the device shows the message **This website is trying to download a configuration profile. Do you want to allow this?**
- Tap **Allow**. After the profile has been downloaded to the iOS device, the message **Profile Downloaded** appears.
- Open the **Settings** app on the iOS device.
- Tap **General**.
- Tap **VPN and device management**. The **WatchGuard MDM Service** downloaded profile is shown.
- Tap **WatchGuard MDM Service**. The **Install profile** window opens with information about the security of the downloaded file.

- Tap **Install** in the upper-right corner. You are asked to enter the phone password.
- Enter the password. A **Warning** message appears, indicating that the device will be managed remotely.
- Tap **Install** in the upper-right corner. The **Remote Management** window opens.
- Tap **Trust**. The profile is installed. After a few minutes, the device shows a notification to automatically download and install the Panda Endpoint Protection Plus agent.
- Tap the **Install** button. The app is downloaded and installed on the device.
- After the app is downloaded and installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is integrated into the Panda Endpoint Protection Plus console and the **Enter the iPhone code** window opens.
- Enter the device password. The **OK** window opens. The installation is complete.

Deploying and installing the agent on devices enrolled into a third-party MDM solution

The procedures in this section associated with the MDM software vary based on the vendor you select. See your product help for more information.

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button. A window opens with all platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. The **iOS** window opens.
- Click the **Installation using another MDM solution** link. The **iOS - Another MDM solution** window opens with the information the MDM solution needs to integrate the device.

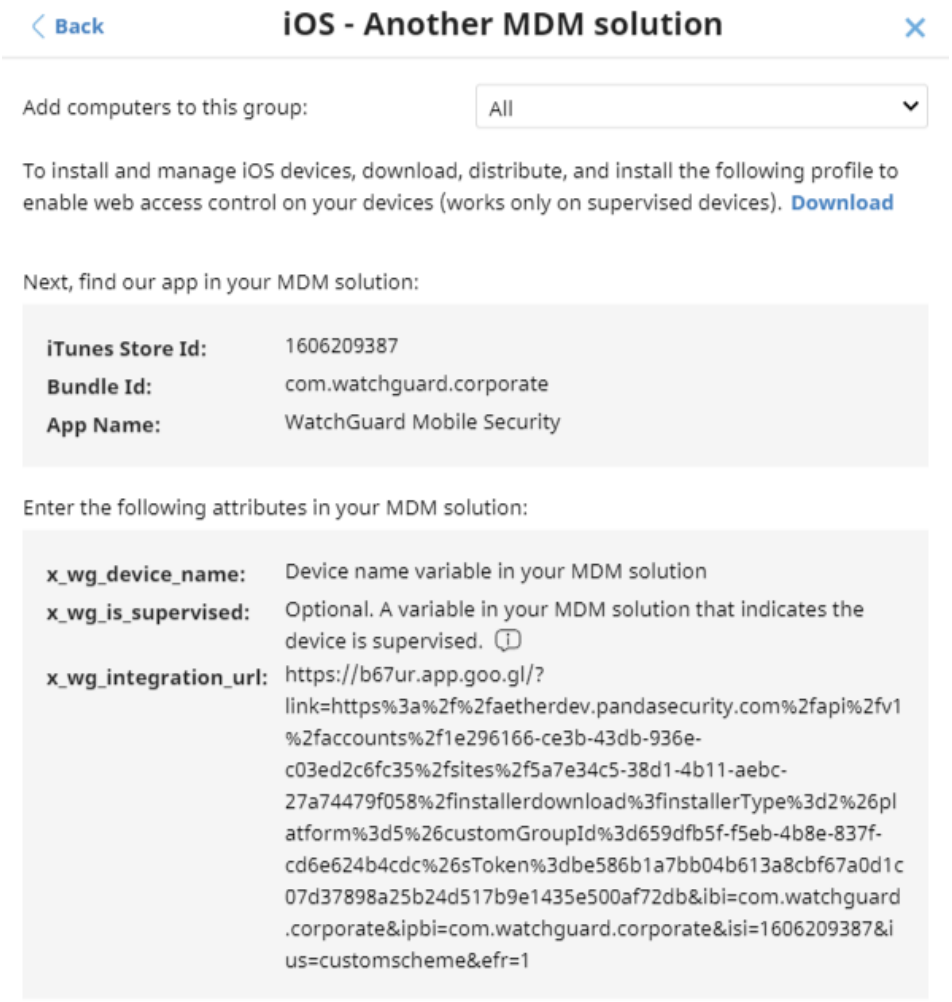


Figure 5.13: Window with the integration parameters for the third-party MDM solution

- In the third-party MDM solution, import the **WatchGuard Mobile Security** app directly from the Apple Store. To do this, use the **iTunes Store Id**, **Bundle Id**, or **App Name** fields in figure Figure 5.13: , or the search features included in the MDM solution.
- Associate and define the parameters **x_wg_device_name** and **x_wg_integration_url** in the **WatchGuard Mobile Security** app imported into the third-party MDM solution repository. The information contained in these parameters is sent along with the **WatchGuard Mobile Security** app when you push the app to the devices managed with the MDM solution.
    - **x_wg_device_name**: Contains the device name that will be shown in the Panda Endpoint Protection Plus console. In the **x_wg_device_name** parameter, enter the variable used by the MDM solution to represent the name of the device that will receive the **WatchGuard Mobile Security** app.
    - **x_wg_integration_url**: Contains the URL that points to the information that **WatchGuard Mobile Security** needs to integrate into the group chosen by the Panda Endpoint Protection Plus administrator. Copy the content of the **x_wg_integration_url** attribute shown in the Panda Endpoint Protection Plus console to the parameter defined in the MDM solution.

Each MDM solution uses a different variable name and syntax. See your product documentation for this information.

Use a variable for the x_wg_device_name parameter. If, instead of the variable that represents the device name, you enter a device name, all the mobile devices that receive ***WatchGuard Mobile Security*** *will be shown with the same name in the Panda Endpoint Protection Plus console.*

- Push the WatchGuard Mobile Security app from the MDM solution to the devices that you want to protect. After a few minutes, the device shows a notification to automatically download and install the Panda Endpoint Protection Plus agent.
- Tap the **Install** button. The app is downloaded and installed on the device.
- After the app is downloaded and installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is integrated into the Panda Endpoint Protection Plus console and the **Enter the iPhone code** window opens.
- Enter the device password. The **OK** window opens. The installation is complete.

Deploying and installing the agent on supervised devices

You must configure iOS devices in supervised mode to leverage the URL filtering capabilities provided by Panda Endpoint Protection Plus.

When you place a device in supervised mode, you must reset the device to factory-default settings. All data, programs, and settings delete. To remove the supervised state, reset the device to factory-default settings again.

Concepts

Supervised mode

It is an execution mode for iOS devices used in corporate environments. It provides administrators with greater flexibility to configure apps and manage devices. In supervised mode, the administrator can, the first time the device is turned on and before it is activated, apply configuration profiles for apps and resources on the phone, schedule the installation of apps, or restrict app usage. To configure an iOS device in supervised mode, you must attach it to a macOS computer using a USB cable.

Apple Configurator 2

An app that is run on the macOS computer and enables you to configure iOS devices in supervised mode.

Finder

This is the native macOS file explorer. It is used to create a full backup of the iOS device and restore it later.

iCloud

Cloud storage service. With an Apple ID, users can access their documents, photos, calendars, and other resources online without the need to store them on their mobile device.

Blueprint

A container that stores the apps that you want to send to a device to configure it. Additionally, the Blueprint has the mobile device management (MDM) information and enables you to enable or disable part of the Setup Assistant that is shown to the user the first time that they turn on the device.

Requirements

- A macOS computer with macOS 10.15.6 or higher.
- The Apple Configurator 2 app. You can download it for free at https://apps.apple.com/us/app/apple-configurator/id1037126344?mt=12
- A USB cable to attach the iOS device to the macOS computer.
- To enable web filtering on supervised iOS devices enrolled into a third-party MDM solution, the MDM solution must allow import of external profiles. Verify whether your MDM solution supports this feature before you begin the procedure described in this section.
- **Optional**: Finder app to create a backup if needed and restore it. See Configuring an iOS device in supervised mode without loss of data.

Configuring the device in supervised mode and enrolling it into the Panda MDM solution

The process to configure an iOS device in supervised mode is carried out independently from the process to enroll it into the Panda MDM solution.

When you configure an iOS device in supervised mode, all data and apps on the device delete. To create a backup of the data and restore it after the procedure has been completed, see Configuring an iOS device in supervised mode without loss of data.

To verify that the iOS device is in supervised mode, see Verifying that the device is supervised

Creating the Blueprint

- On the macOS computer, open the Apple Configurator 2 app. Select **File**, **New Blueprint**. The **All Blueprints** window opens, showing all Blueprints created so far. The newly created Blueprint is automatically selected.
- Type the name of the new Blueprint. Press **Enter**.

Getting the Panda Endpoint Protection Plus MDM solution enrollment URL

- Verify you have a valid Apple certificate uploaded to the Panda Endpoint Protection Plus management console. To generate a certificate, see Creating and importing the digital certificate into the Panda Endpoint Protection Plus console. If your certificate is about to expire, see Renewing the Apple certificate.
- Make sure your company's iOS devices do not have a third-party MDM profile already installed. If they do, delete the profile from your devices. For more information about the implications of deleting a third-party MDM profile, see Managing iOS devices with an MDM solution and Enrollment types supported by Panda Endpoint Protection Plus.
- Select the **Computers** menu at the top of the Panda Endpoint Protection Plus management console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. The **iOS** window opens with information about the previously uploaded certificate.

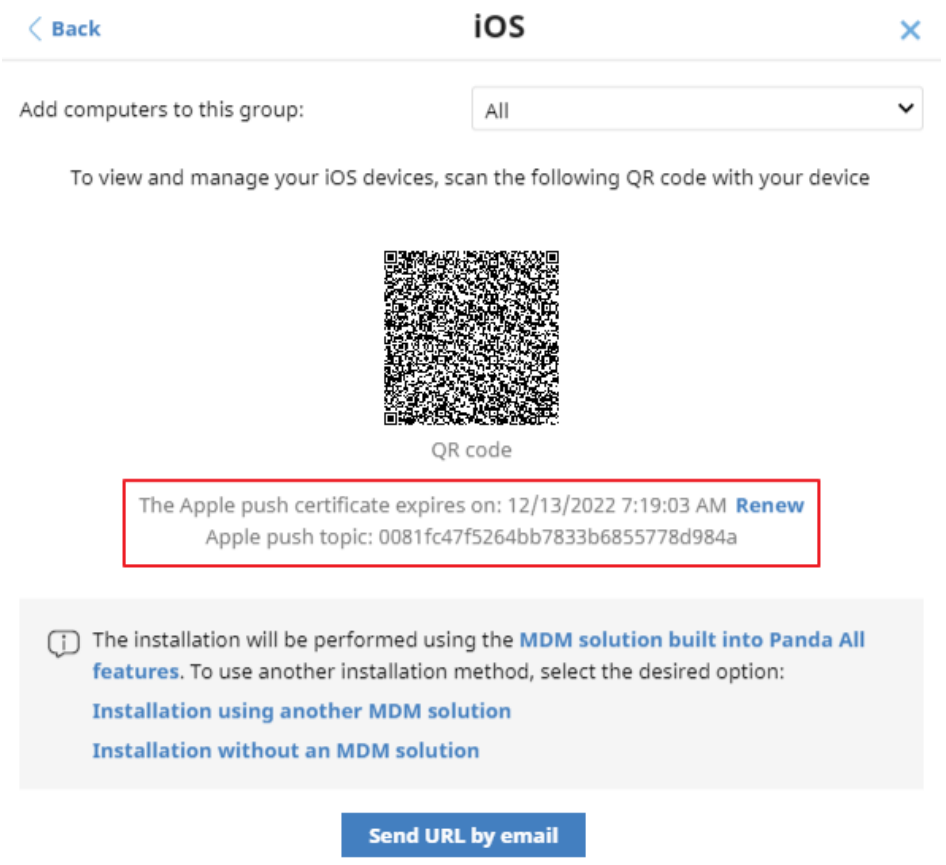


Figure 5.14: Window with the uploaded Apple digital certificate

- To add the iOS device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.

- Click the **Send URL by email** button. The email program installed on the computer opens.
- Enter the email address of the user that will use the iOS device you want to enroll. Click **Send**.

Preparing the device

- In the Apple Configurator 2 app, select the created Blueprint and click **Prepare** in the top bar. The **Prepare devices** window opens.
- In **Prepare with**, select **Manual configuration**, **Supervise devices**, and **Allow devices to pair with other computers**. Click **Next**. The **Enroll in MDM server** window opens.
- In **Server**, select **Do not enroll in MDM**. Click **Next**. The **Sign in to Apple Business Manager or Apple School Manager** window opens.
- Click **Skip**. The **Create an organization** window opens.
- Enter your company's details. Click **Next**.
- Select **Create a new supervision identity**. Click **Next**. The **Configure iOS Setup Assistant** window opens.
- Choose which steps will be presented to the user in the Setup Assistant the first time the user turns on the iOS device. Click **Prepare**. A window opens that prompts for the macOS computer administrator credentials.
- Click **Update settings**. A pop-up window opens that shows the status of the configuration process.
- After the procedure is complete, the Blueprint is created and ready to be applied to all relevant iOS devices.

Applying the Blueprint to iOS devices

> *Before enrolling a supervised iOS device into an MDM solution, make sure the **Find My iPhone** option is disabled.*

- Disable **Find My iPhone** on the user's iOS device.
  - Tap **Settings**.
  - Tap the user's name. Tap **Find My**.
  - Tap **Find My iPhone**, then tap to disable it.
  - Enter the Apple ID password.
  - Tap **Turn off**.
- Connect the iOS device to the macOS computer with a USB cable. The Apple Configurator 2 app must be open during the process. The message **Trust this computer?** appears on the mobile device.
- Tap **Trust**.

- In the Apple Configurator 2 app, click **All devices** in the top bar. After connecting, you can see the device in the Apple Configurator window.
- Right-click the device. A drop-down menu appears.
- Click **Apply**. Select the created Blueprint. A window opens for you to confirm you want to apply the Blueprint.
- When you click **Apply**, the following actions are taken on the iOS device:
    - The device is reset to its factory-default settings.
    - All data and apps are deleted from the device.
    - The device is placed in supervised mode.

Verifying that the device is supervised

- In the Apple Configurator 2 app, click **Supervised** in the top bar. The new supervised device is shown.
- Tap **Settings** on the iOS device. In the upper-left corner, under the phone name, the message “This iPhone is supervised and managed by (company name)” is shown.

Enrolling the supervised device into the Panda MDM solution

- Configure the email app on the supervised iOS device. Download the message that contains the MDM enrollment URL. This message was sent earlier from the Panda Endpoint Protection Plus console.
- Tap the link. A window opens that shows the message **This website is trying to download a configuration profile. Do you want to allow this?**
- Tap **Allow**. After the profile has been downloaded to the iOS device, the message **Profile downloaded** appears.
- Open the **Settings** app on the iOS device. The **Settings** window opens.
- Tap **General**. The **General** window opens.
- Tap **VPN and device management**. The **WatchGuard MDM Service** downloaded profile is shown.
- Tap **WatchGuard MDM Service**. The **Install profile** window opens with information about the security of the downloaded file.
- Tap **Install** in the upper-right corner. You are asked to enter the phone password.
- Enter the password. A **Warning** message appears, indicating that the device will be managed remotely.
- Tap **Install** in the upper-right corner. The **Remote Management** window opens.
- Tap **Trust**. The profile is installed. After a few minutes, the Panda Endpoint Protection Plus agent is downloaded and installed automatically.

- After the app is downloaded and installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is added to the Panda Endpoint Protection Plus console and the configuration process is complete.

Enabling supervised mode and deploying the iOS agent from a third-party MDM solution

The various MDM solutions available on the market support different methods to enable supervised mode on iOS devices. See the documentation to enable supervised mode on the iOS devices enrolled into your MDM solution.

To set WatchGuard Mobile Security as the app in charge of filtering web traffic on iOS devices, the MDM solution that you use must allow import of external configuration profiles. See the documentation for your MDM solution for information about how to enable supervised mode on enrolled iOS devices.

Deploying the WatchGuard Mobile Security app using a third-party MDM solution

The procedures in this section associated with the MDM software vary based on the vendor you select. See your product help for more information.

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button. A window opens that shows all platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. The **iOS** window opens.
- Click the **Installation using another MDM solution** link. The **iOS - Another MDM solution** window opens with the information the MDM solution needs to integrate the device.

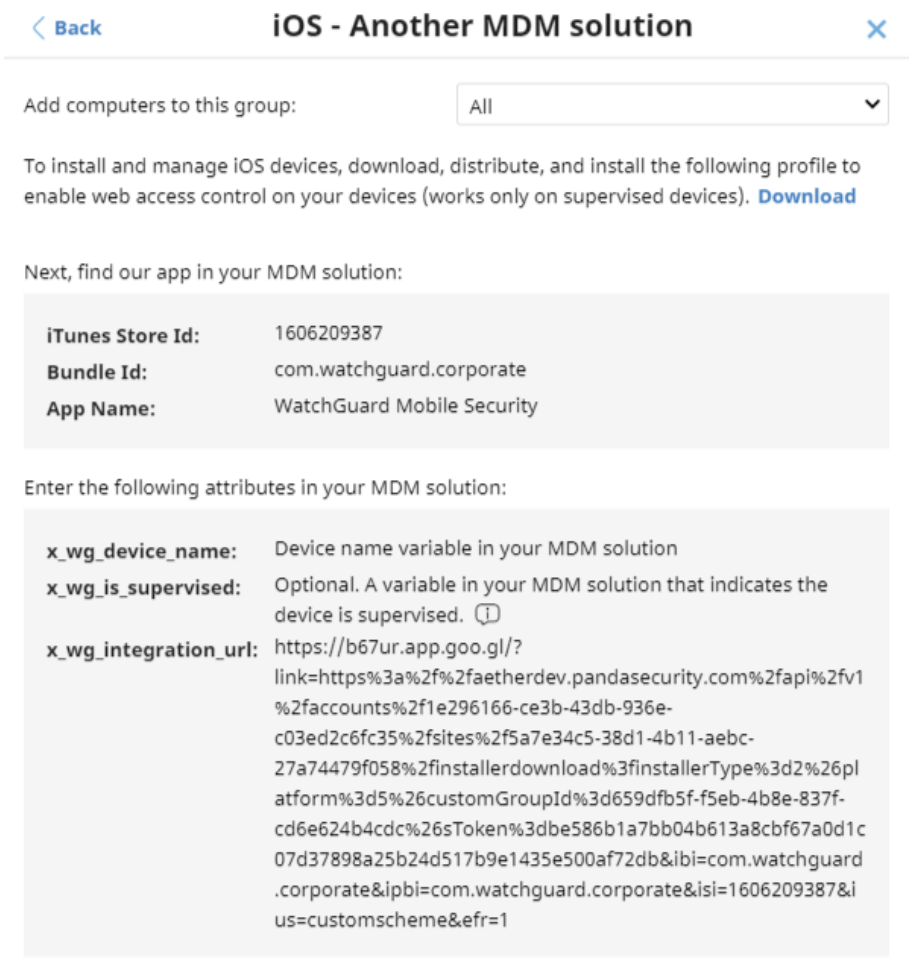


Figure 5.15: Window with the integration parameters for the third-party MDM solution

- Click the **Download** link to get the profile that will set **WatchGuard Mobile Security** as the app configured to filter web traffic on the target iOS devices. An XML file with the .mobileconfig extension downloads to your computer.
- Import the .mobileconfig file into the third-party MDM solution and push it to the iOS devices where you want to enable URL filtering.
- In the third-party MDM solution, import the **WatchGuard Mobile Security** app directly from the Apple Store. To do this, use the **iTunes Store Id**, **Bundle Id**, or **App Name** fields in figure Figure 5.15: , or the search features included in the MDM solution.
- Associate and define the parameters **x_wg_device_name**, **x_wg_integration_url**, and **x_wg_is_supervised** in the **WatchGuard Mobile Security** app imported into the third-party MDM solution repository. The information contained in these parameters is sent along with the **WatchGuard Mobile Security** app when you push the app to the devices managed with the MDM solution.
    - **x_wg_device_name**: Contains the device name that will be shown in the Panda Endpoint Protection Plus console. In the **x_wg_device_name** parameter, enter the variable used by the MDM solution to represent the name of the device that will receive the **WatchGuard**

Mobile Security app.

- **x_wg_integration_url**: Contains the URL that points to the information that **WatchGuard Mobile Security** needs to integrate into the group chosen by the Panda Endpoint Protection Plus administrator. Copy the content of the **x_wg_integration_url** attribute shown in the Panda Endpoint Protection Plus console to the parameter defined in the MDM solution.
- **x_wg_is_supervised**: Tells **WatchGuard Mobile Security** whether the device where it is going to be installed is supervised or not. If your MDM solution has a variable that enables you to dynamically set the content of this parameter, add it. Otherwise, do not add the parameter. **WatchGuard Mobile Security** will try to determine on its own whether it is running on a managed device or not.

Each MDM solution uses different variable names and syntaxes. See your product documentation for this information.

*Use variables with the x_wg_device_name and x_wg_is_supervised parameters. If, instead of the variable that represents the device name, you enter a device name, all the mobile devices that receive **WatchGuard Mobile Security** will be shown with the same name in the Panda Endpoint Protection Plus console.*

- Push the **WatchGuard Mobile Security** app from the MDM solution to the devices that you want to protect. After a few minures, the app is installed silently.
- After the app is installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is added to the Panda Endpoint Protection Plus console and the configuration process is complete.

Configuring an iOS device in supervised mode without loss of data

The following procedure for creating a backup and restoring it later is not officially supported by Apple. For this reason, we recommend that you run it first in a test environment before you apply it to your company's mobile phones.

Determine whether you need to create a manual backup

When you configure an iOS device in supervised mode, you reset it to factory-default settings. As a result, all apps and data stored on the device by the user are lost. To avoid this, you must use a backup and restore

method that will vary based on the type of data stored and the backup software used:

- **iCloud**: If the user uses Apple's cloud storage service, it is very likely that you will not need to create any backups manually; in this case, their documents, photos, and other items are not stored on the mobile device but are automatically stored in the cloud. After the device has been formatted and placed in supervised mode, the user simply has to use their Apple ID to regain access to all their information.

> *To verify whether iCloud stores in the cloud all the types of data you want to recover after having enabled supervised mode, see https://support.apple.com/en-us/HT207428. If iCloud does not store all the types of data you want to keep, use the Finder app as explained in this article.*

- **Finder**: If the user does not use iCloud or wants to keep apps or types of data not supported by Apple's cloud, you must create a backup of the mobile device by following a very specific protocol. This is required because Finder also stores the device state in the backup, so, when you restore the device data, you also restore the previous, non-supervised state of the device.

> *Finder does not store the settings of all the apps that exist on Apple Store. As a previous step, check whether the apps installed on the user's device will require manual configuration after the restore process is performed.*

Requirements for creating a backup using Finder

- A macOS computer with the Catalina operating system or higher and the Finder app.
- The user's iPhone that you want to supervise.
- A secondary iPhone with the same operating system version as the user's iPhone.
- A lightning to USB cable.

Creating and restoring the backup

Back up the user's iPhone

- On the user's mobile phone, disable **Find My iPhone**:
  - Tap **Settings**.
  - Tap the user's name. Tap **Find My**.
  - Tap **Find My iPhone**, then tap to disable it.

    - Enter the Apple ID password.
    - Tap **Turn off**.
- Open the **Finder** app. Connect the user's iPhone to the macOS computer.
- If you are prompted to enter the device code or confirm that you trust the macOS computer, follow the on-screen instructions.
- In the left panel of the Finder, click the user's iPhone.
- On the **General** tab, select **Back up all the data on your iPhone to this Mac**.
- Click the **Back Up Now** button.
- When the process is complete, make a note of the exact time the backup was created.

Restore the user's iPhone backup to the secondary iPhone

- Disable **Find My iPhone** on the secondary mobile phone:
    - Tap **Settings**.
    - Tap the phone name. Tap **Find My**.
    - Tap **Find My iPhone**, then tap to disable it.
    - Enter the Apple ID password.
    - Tap **Turn off**.
- Disconnect the user's iPhone and connect the secondary iPhone to the macOS computer.
- If you are prompted to enter the device code or confirm that you trust the macOS computer, follow the on-screen instructions.
- In the left panel of the Finder, click the secondary iPhone.
- On the **General** tab, select **Restore Backup**.
- Select the backup that you created earlier. You can identify the backup by its timestamp.

Back up the secondary iPhone

- Verify that **Find My iPhone** is disabled on the secondary mobile phone. If it is not disabled:
    - Tap **Settings**.
    - Tap the phone name. Tap **Find My**.
    - Tap **Find My iPhone**, then tap to disable it.
    - Enter the Apple ID password.
    - Tap **Turn off**.
- In the left panel of the Finder, click the secondary iPhone.
- On the **General** tab, select **Back up all the data on your iPhone to this Mac**.

- Click the **Back Up Now** button.
- When the process is complete, make a note of the exact time the backup was created.

Restore the secondary iPhone backup to the user's iPhone

- Verify that **Find My iPhone** is disabled on the user's mobile phone. If it is not disabled:
    - Tap **Settings**.
    - Tap the user's name. Tap **Find My**.
    - Tap **Find My iPhone**, then tap to disable it.
    - Enter the Apple ID password.
    - Tap **Turn off**.
- Disconnect the secondary iPhone and connect the user's iPhone to the macOS computer.
- If you are prompted to enter the device code or confirm that you trust the macOS computer, follow the on-screen instructions.
- In the left panel of the Finder, click the user's iPhone.
- On the **General** tab, select **Restore Backup**.
- Select the backup that you created earlier. You can identify the backup by its timestamp.
- When the process is complete, a **Hello** screen is displayed on the user's iPhone. At this point, it is very important that you do not perform any actions on the device and start the process to put it in supervised mode. See Configuring the device in supervised mode and enrolling it into the Panda MDM solution.

Managing the Apple ID and digital certificates

Creating an Apple ID

- Open a supported web browser and go to https://appleid.apple.com/account. The **Create Your Apple ID** page opens.
- Fill in the form. You must specify an email account and the phone number of the device that will be used to verify the certificate request (usually, this is the device assigned to the Panda Endpoint Protection Plus administrator). Click **Continue**. You will receive a message with a verification code at the email address provided in the form.
- Enter the verification code in the form. Click **Continue**. You will receive a new code by SMS at the phone number provided in the form.
- Enter the SMS code. Click **Continue**. The process is complete and the dashboard associated with the newly created account opens. This dashboard enables you to manage your account and see all certificates generated so far.

Creating and importing the digital certificate into the Panda Endpoint Protection Plus console

To integrate iOS devices into Panda Endpoint Protection Plus using the Panda MDM solution, you must generate a digital certificate that ensures the confidentiality of communications with the Apple servers:

- Select the **Computers** menu at the top of the console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. If no certificate has been previously imported, a window opens with the procedure for creating a valid certificate.

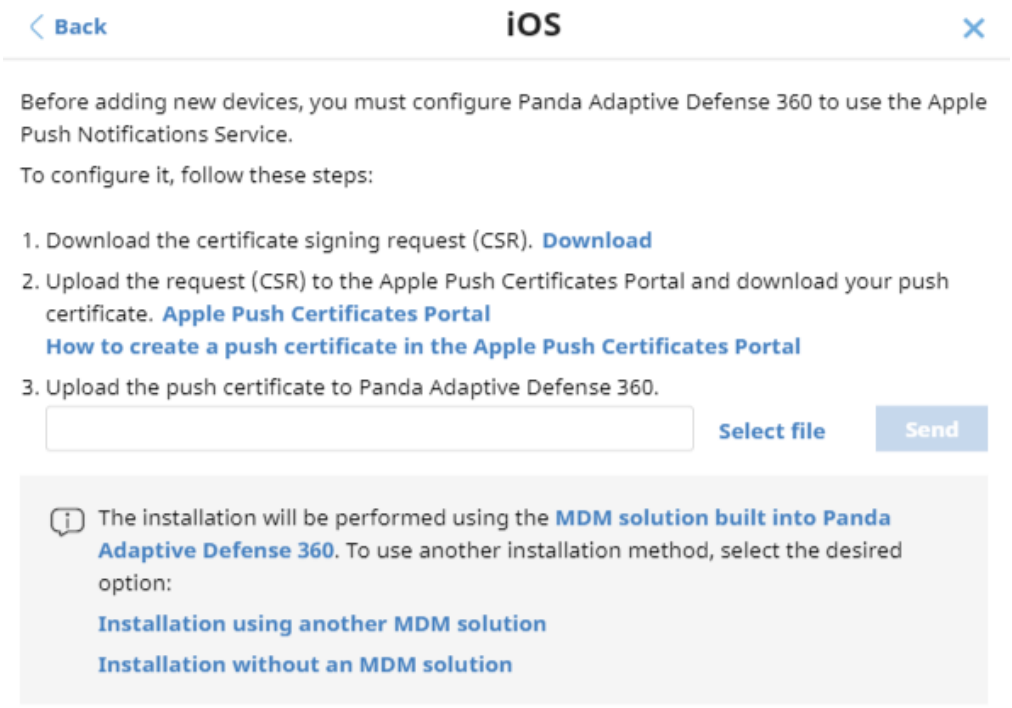


Figure 5.16: Window detailing the procedure for creating and importing an Apple digital certificate

- Click the **Download** link. The `apple_push.csr` file is downloaded. This file contains the signed certificate request encoded as Base64.
- Click the **Apple Push Certificates Portal** link. If you have previously logged in, the web browser opens the page for managing Apple digital certificates. Otherwise, enter your Apple ID credentials. See Creating an Apple ID.
- Click the **Create Certificate** icon. The **Terms of Use** page opens.
- Select **I have read and agree to these terms and conditions**. Click **Accept**. The **Create a New Push Certificate** page opens.
- Click **Choose File**. Select the `apple_push.csr` file you previously downloaded from the Panda Endpoint Protection Plus management console. Click **Upload**. A **Confirmation** page opens with

information about the generated certificate. You will receive an informational email message.

- Click the **Download** button. The `MDM_ Panda Security, S.L._Certificate.pem` file is downloaded. This file contains the digital certificate.
- In the Panda Endpoint Protection Plus management console, click the **Select file** link. Choose the `MDM_ Panda Security, S.L._Certificate.pem` file you downloaded from the Apple portal. The **iOS** window appears, with the ID and expiration date of the imported certificate.

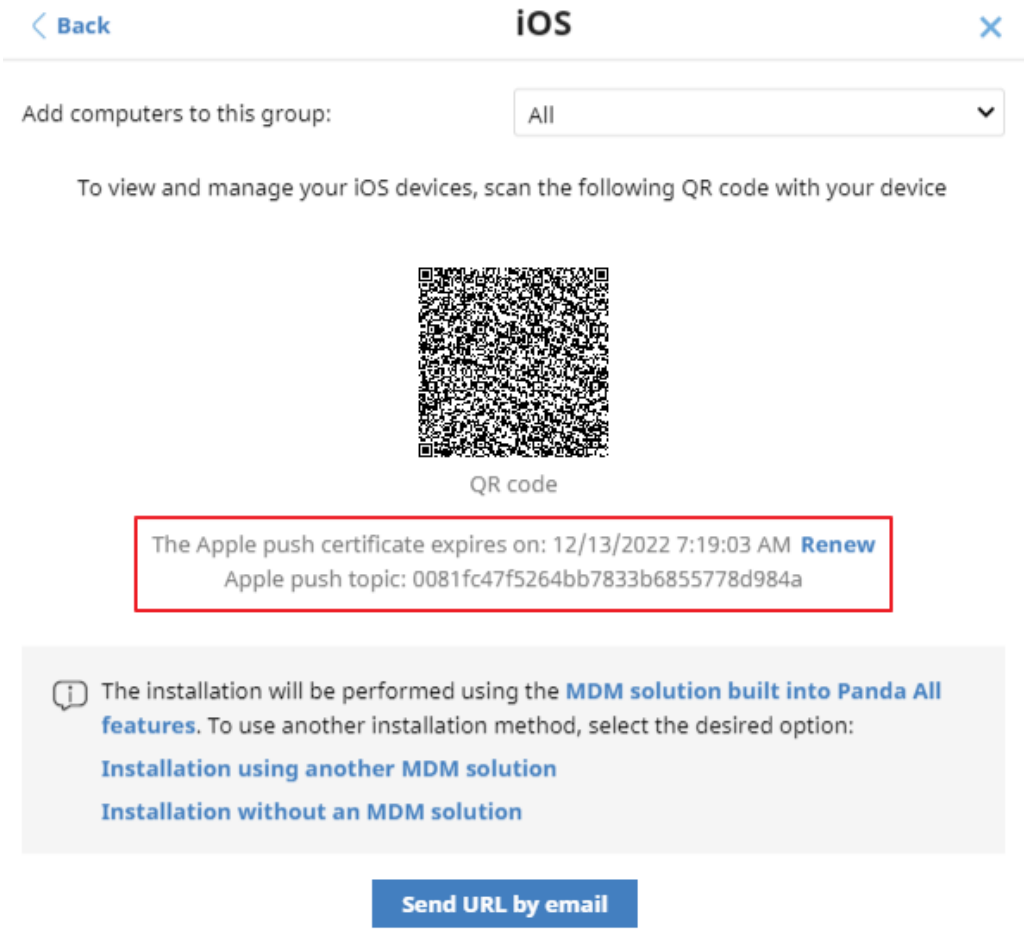


Figure 5.17: Window with information about the uploaded digital certificate

Renewing the Apple certificate

Apple certificates are valid for one year, after which they expire.

> *Renew your Apple certificate well before its expiration date. If your certificate expires, you will no longer be able to manage your devices from the Panda Endpoint Protection Plus management console. You will have to generate a certificate again and reintegrate all of your company's iOS devices.*

- Go to https://identity.apple.com/pushcert/ and log in using your Apple ID credentials (see Creating an Apple ID). The **Certificates for Third-Party Servers** page opens.

Figure 5.18: **Certificates for Third-Party Servers** page

- Click the **Renew** button associated with the certificate in use. The **Renew Push Certificate** page opens.
- Click **Choose File**. Choose the `apple_push.csr` file. If the file is no longer available, you can create a new one. See Creating and importing the digital certificate into the Panda Endpoint Protection Plus console.
- Click the **Upload** button. The **Confirmation** page opens.
- Click the **Download** button. The updated certificate is downloaded.
- Select the **Computers** menu at the top of the Panda Endpoint Protection Plus management console. Click the **Add computers** button. A window opens with all platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. A window opens with information about the previously uploaded certificate.
- Click **Renew**. The **iOS** window opens, with the certificate expiration date and ID (Apple Push Topic).
- Click the **Select file** link. Choose the `apple_push.csr` file you used when you first created the certificate. If the file is no longer available, you can download a new file from the Panda Endpoint Protection Plus management console. See Creating and importing the digital certificate into the Panda Endpoint Protection Plus console.
- Click the **Send** button. The **iOS** window opens, with an updated expiration date for the certificate.

Checking the expiration date of a certificate

- Select the **Computers** menu at the top of the console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection Plus.
- Click the **iOS** icon. If a certificate has been previously imported, its data is shown.
- If the certificate is expired, a warning message is shown.

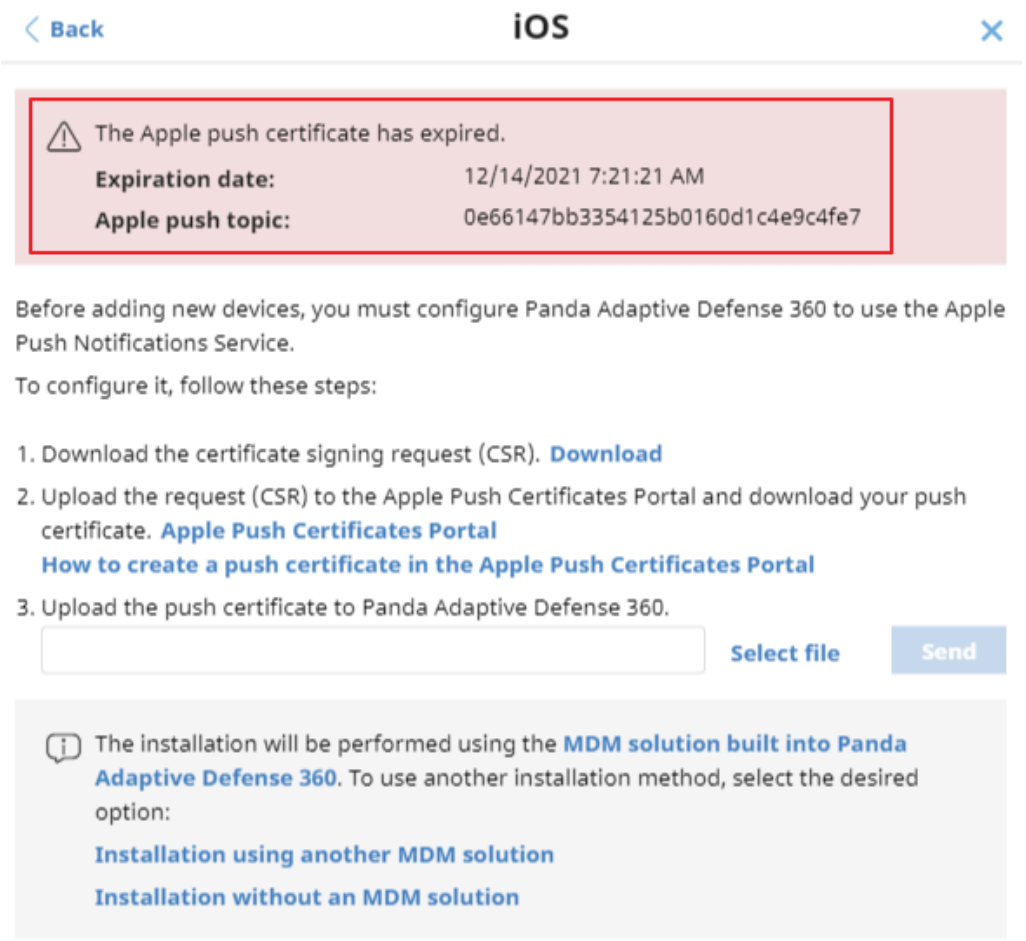


Figure 5.19: Window with information about an expired digital certificate

Checking deployment

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

- Using the **Protection status** widget. See Protection status on page 446 for more information.
- Using the **Computer protection status** list. See Computer protection status on page 459 for more information.
- Using the Event Viewer Application log on Windows computers.

Windows Event Viewer

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

Message	Level	Category	ID
The device %deviceId% was unregistered	Warning	Registration (1)	101
The device %deviceId% was registered	Information	Registration (1)	101
A new SiteId %SiteId% was set	Warning	Registration (1)	102
Error %error%: Cannot change SiteId	Error	Registration (1)	102
Error %error%: Calling %method%	Error	Registration (1)	103
Error %code%: Registering device, %description%	Error	Registration (1)	103
Installation success of %fullPath% with parameters %parameters%	Information	Installation (2)	201
A reboot is required after installing %fullPath% with parameters %parameters%	Warning	Installation (2)	201
Error %error%: executing %fullPath% with parameters %parameters%	Error	Installation (2)	201
Message: %Module% installer error with following data: (optional) Extended code: %code% (optional) Extended subcode: %subCode% (optional) Error description: %description% (optional) The generic uninstaller should be launched (optional) Detected AV: Name = %name%, Version = %version%	Error	Installation (2)	202
Uninstallation success of product with code %productCode% and parameters %parameters%	Information	Uninstallation (4)	401
A reboot is required after uninstalling product with code %productCode% and parameters %parameters%	Warning	Uninstallation (4)	401

Message	Level	Category	ID
Error %error%: Uninstalling product with code %productCode% and parameters %parameters%	Error	Uninstallation (4)	401
Uninstallation of product with code %productCode% and command-line parameters %commandLine% was executed	Information	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and command-line parameters %commandLine%	Error	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and command-line parameters %commandLine%	Error	Uninstallation (4)	401
Generic uninstaller executed: %commandLine%	Information	Uninstallation (4)	402
Error %error%: Generic uninstaller executed %commandLine%	Error	Uninstallation (4)	402
Configuration success of product with code %productCode% and command-line parameters %commandLine%	Information	Repair (3)	301
A reboot is required after configuring product with code %productCode% and command-line parameters %commandLine%	Warning	Repair (3)	301
Error %error%: Configuring product with code %productCode% and command-line parameters %commandLine%	Error	Repair (3)	301

Table 5.10: Agent installation result codes in the Event Viewer

Automatic deletion of computers

This feature releases the security software license from protected computers and removes them from the console. Computers whose license you want to release must meet certain conditions defined in a filter you

must create before enabling the feature. After you have created the filter, it is applied periodically.

Required permissions

Automatic deletion of computers is visible to all users of the web console. However, to configure and modify this feature, the user must have full visibility into all computers and the **Add, discover, and delete computers** permission.

For more information, see Understanding permissions on page 67.

Consequences of deleting computers

Computers are deleted once a day, between 01:00 AM and 03:00 AM UTC.

When you delete a computer:

- The computer and all its information are deleted from the console.
- The computer is unprotected.
- If the computer was encrypted, it remains encrypted but you cannot get the recovery keys.

We recommend that you turn off a computer after it is deleted. Otherwise, it will reappear in the web console as soon as it reconnects to the Aether servers.

The information generated by a protected computer is not permanently deleted from the Panda Endpoint Protection Plus servers: If you reassign a license to the computer and it reconnects to the Aether server, all its information reappears in the web console. Nevertheless, if the filter is not disabled, the computer will be deleted again the next day.

Creating a filter to delete computers

For more information about all items available to configure a filter, see Configuring filters on page 205.

Note that, because this is a feature for deleting computers, we recommend that the filter name be as easy to identify as possible.

To create a filter that finds computers not connected to the Aether server, use the following parameters:

- **Category**: Computer
- **Property**: Last connection

- **Operator:**
  - Is between (finds computers not connected to the server between two specific dates)
  - Before (finds computers not connected to the server before a specific date)
  - After (finds computers not connected to the server after a specific date)

Enabling the feature

- Select the **Settings** menu at the top of the console. Select **Computer maintenance** from the side menu.
- Click the **Enable automatic deletion of computers** toggle.
- From the drop-down menu, select the filter you want to apply.
- Click **Save changes**.

You cannot modify or delete the filter during its execution.

Scheduled reports of the computers to be deleted

You can schedule the automatic sending of a periodic report containing a list of computers to be deleted. See Accessing the sending of reports and lists on page 557

Uninstalling the software

On 30 June 2025, our Windows and Mac protection for these OS versions will become End of Life (EOL): Windows XP, Vista, Server 2003, Server 2008 (Windows 2008 R2 will continue to be supported), macOS Yosemite, El Capitán, Sierra, High Sierra and Mojave. After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

You can uninstall the Panda Endpoint Protection Plus software manually from the control panel of the operating system on each computer, or you can uninstall remotely from the security software management console.

Manual uninstallation

End users can manually uninstall the security software, if the administrator has not configured an uninstallation password in the security settings profile applied to the computer. If an uninstallation password is required, the end user requires authorization or the necessary credentials to uninstall the software.

To set or delete the agent uninstallation password, see *Configuring security against protection tampering on page 292*.

When you install Panda Endpoint Protection Plus, multiple applications are installed, based on the platform:

- **Windows and macOS computers**: Agent and endpoint security product.
- **Linux computers**: Agent, endpoint security product, and kernel module.
- **Android devices**: Endpoint security product.
- **iOS devices**: Endpoint security product and MDM solution management profile.

To completely uninstall Panda Endpoint Protection Plus, you must remove all modules. If you only uninstall the security product, the agent will install it again.

On a Windows 8 or later device

- Control Panel > Programs > Uninstall a program.
- Alternatively, type 'uninstall a program' at the Windows Start screen.

On a Windows Vista, Windows 7, Windows Server 2003, or later device

- Control Panel > Programs and Features > Uninstall or change a program.

On a Windows XP device

- Control Panel > Add or remove programs.

Uninstallation using the uninstallation tool

On Windows computers, during the uninstallation process, some files or libraries might not be completely removed and cause errors. You can use a Panda Security tool to completely uninstall the agent and protection.

The uninstallation process can take a few minutes. When it is complete, restart the computer.

Follow these steps:

- Download and unzip the file GU.zip (Password: panda).
- Run the agent removal file `GU_AGENT.exe`. Restart the computer.
- Run the protection removal file `GU_PROT.exe`. Restart the computer.

On a macOS device

- Open Terminal Finder > Applications > Utilities > Terminal.
- To uninstall the protection software, run this command: `sudo sh /Applications/Endpoint-Protection.app/Contents/uninstall.sh`
- To uninstall the agent, run this command: `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`

On an Android device

- Go to Settings > Security > Device Administrators.
- Clear the Panda Endpoint Protection Plus checkbox. Tap Disable > OK.
- In Settings, tap Apps. Tap Panda Endpoint Protection Plus > Uninstall > OK.

On an iOS device when it is not integrated with an MDM solution

- On the Home screen, press and hold the WatchGuard Mobile Security app.
- Tap the "-" icon on the WatchGuard Mobile Security app. The **Delete WatchGuard Mobile Security** dialog box opens.
- Tap **Delete app**. The **Do you want to delete WatchGuard Mobile Security**? dialog box opens.
- Tap **Delete**. The app is removed from the device.

On an iOS device when it is integrated with the Panda MDM solution

- On the Home screen, tap **Settings**. The **Settings** app opens.
- From the side panel, tap **General**. The **General** page opens.
- Tap **VPN and device management**. The **WatchGuard MDM Service** downloaded profile opens.
- Tap **Remove management**. The **Remove management** window opens.
- Tap **Remove**. The management profile is removed. The WatchGuard Mobile Security app is also removed.

On an iOS device when it is integrated with a third-party MDM solution

If your WatchGuard Mobile Security app is installed on an iOS device and it is integrated with a third-party MDM solution, we recommend that you uninstall the WatchGuard Mobile Security app from the third-party MDM solution. If you delete the management profile manually from the device, all the software that was

installed with the MDM solution is also lost. The device can no longer be centrally managed from the MDM solution.

On a Linux device

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

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

We recommend that you use the command line as `root` to uninstall the product. Use the `--totp` parameter if two-factor authentication is enabled, and `--pass` if agent uninstallation is password protected. See Configuring security against protection tampering on page 292.

```
$ /usr/local/management-agent/repositories/pa/install --remove --
totp=value

(uninstalls the security software)

$ /usr/local/management-agent/repositories/ma/install --remove --
pass="password" --totp=value

(uninstalls the agent and repositories)
```

Manual uninstallation result

When you uninstall the Panda Endpoint Protection Plus software (Panda agent and protection) from a computer, all data associated with the computer disappears from the management console.

When you reinstall the Panda Endpoint Protection Plus software, the associated data and counters are restored.

Uninstallation from the management console

Remote uninstallation of the security software is not supported for computers that run macOS Catalina or Big Sur. In these instances, you must uninstall the software directly on the target computer.

To uninstall the security software from Windows, Linux, or macOS computers from the management console:

- Go to the **Computers** menu (or the **Licenses** or **Computer protection status** lists). Select the checkboxes for the computers that you want to uninstall the security software from.
- From the action bar, select **Delete**. A confirmation dialog box opens.

- In the confirmation dialog box, select the **Uninstall the Panda agent from the selected computers** checkbox to completely remove the Panda Endpoint Protection Plus software.
- To complete uninstallation on macOS computers, the security software prompts the local user of the device for the password of an account with administrative privileges.

Remote reinstallation

To resolve a situation when Panda Endpoint Protection Plus does not run correctly on a workstation or server, you can reinstall it remotely from the management console.

You must reinstall the agent and the protection module separately.

Remote reinstallation requirements

- The target computer must be a Windows workstation or server.
- A computer with the discovery computer role must exist on the same network segment as the computer you want to reinstall software on. The discovery computer and Panda Security server can communicate.
- You have local admin or domain admin account credentials.

Accessing the feature

You can access this feature from any of the lists below. To access these lists, from the top menu, select **Status**. From the side menu, click the **Add** link:

- Computer protection status on page 459.
- Patch management status on page 371.
- Encryption status on page 435.
- Licenses module lists on page 184.
- Hardware on page 228.

Alternatively, to access this feature, from the top menu, select **Computers**. On the **Computers** page, click a branch in the folder or filter tree in the side panel.

*The **Reinstall protection (requires restart)** and **Reinstall agent** options appear only for Windows computers.*

Identifying unprotected computers

Use the **Unmanaged computers discovered** list to find computers and servers on the network that need to have software reinstalled. See Viewing discovered computers.

Reinstalling the software on a single computer

- Use the list to find a computer that needs to have software reinstalled.
- From the computer context menu, select **Reinstall protection (requires restart)** or **Reinstall agent**. A dialog box opens where you can configure the reinstallation options. See Reinstall protection dialog box and Reinstall agent dialog box.

Reinstalling the software on multiple computers

- Use the checkboxes to select the computers that need to have the security software or the agent reinstalled.
- From the toolbar, select **Reinstall protection (requires restart)** or **Reinstall agent**. A dialog box opens where you can configure the reinstallation options. See Reinstall protection dialog box and Reinstall agent dialog box.

Reinstall protection dialog box

When you choose to reinstall a computer security software, a dialog box opens that shows these two options:

- **Reinstall the protection immediately (requires restart)**: The software reinstalls after one minute. If the target computer is not available (offline), the restart command remains active for 1 hour.
- **Delay reinstallation for a certain time**: The software reinstalls after the amount of time you select (5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 8 hours). If the target computer is not available (offline), the restart command remains active for 7 days.

The computer user receives a message to restart the computer immediately or wait until the time configured by the administrator. After the wait period expires, the software is uninstalled, and the computer restarts automatically to reinstall the software.

If an error occurs during the process, Panda Endpoint Protection Plus launches an uninstaller in the background in order to retry the operation and remove any traces of the previous installation. This might require an additional restart.

Reinstall agent dialog box

When you choose to reinstall a computer agent, a dialog box opens that prompts you to enter this information:

Discovery computer from which the agent is reinstalled:

- Make sure the discovery computer is on the same network segment as the computer you want to reinstall the agent on.
- If the discovery computer is turned off, the request is queued until the computer becomes available again. Requests are queued for a maximum of one hour, after which time they are discarded.

Credentials for reinstalling the agent: Enter one or multiple installation credentials. Use the target computer's local or domain administrator account to complete the reinstallation.

After you have entered the information, the discovery computer takes these actions:

- Connects to the computer you want to reinstall the agent on.
- Uninstall the agent installed on the computer.
- Downloads a new agent preconfigured with the customer, group, and network settings assigned to the computer. The agent is copied to the computer and runs remotely.
- If an error occurs during the process, an uninstaller launches and, if needed, a message prompts the user to restart the computer.

Error codes

For information on software reinstallation errors, see Protection software reinstallation errors on page 244.

Chapter 6

Licenses

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

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

Chapter contents

Definitions and basic concepts

The following is a description of terms required to understand the graphs and data provided by Panda Endpoint Protection Plus 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 Plus, Panda Full Encryption, Panda Patch Management, .
- **Contracted licenses**: The number of licenses in the license contract.
- **License type**: NFR, Trial, Commercial, Subscription.
- **Expiration date**: The 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 in Panda Endpoint Protection Plus:

- **Computer with a license**: The computer has a valid license in use.
- **Computer without a license**: The computer does not 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 will not be protected by Panda Endpoint Protection Plus, 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**: Includes all licenses assigned to computers.
- **Unused licenses**: Includes the licenses that are not assigned.

Types of licenses

- **Commercial licenses**: These are the standard Panda Endpoint Protection Plus 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 benefits 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

You can assign licenses in two ways: manually and automatically.

For more information about the search tool, the folder tree, and the filter tree, see Managing computers and devices on page 199.

Automatic assignment of licenses

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

Manual assignment of licenses

Follow these steps to manually assign a license to a computer on the network.

- From the top menu, select **Computers**. Find the computer or device you want to assign the license to. You can use the folder tree, the filter tree, or the search tool.
- Select the computer to open its details page.
- Select the **Details** tab. The **Licenses** section shows the **No licenses** status. 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 Plus 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 are automatically released from computers in accordance with the process explained in the Withdrawal of expired licenses section.

Manual release

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

Follow these steps to manually release a Panda Endpoint Protection Plus license:

- From the top menu, select **Computers**. Find the device whose license you want to release. You can use the folder tree, the filter tree, or the search tool.
- Select the computer to open its details page.
- Select the **Details** tab. The **Licenses** section shows 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: Computers with assigned licenses and excluded computers

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

When a license is manually withdrawn from a computer, its status becomes that of **Excluded computer**. From this point on, the computer does not compete for automatic assignment of unassigned licenses.

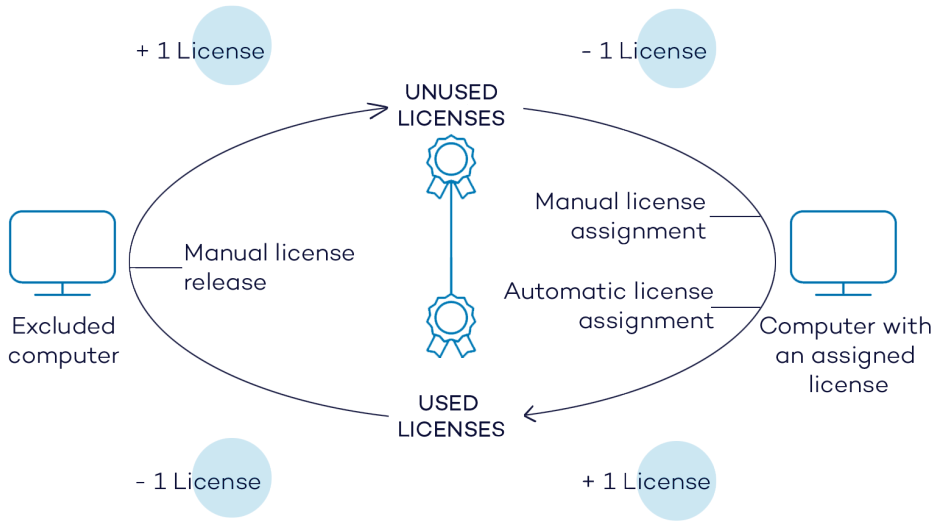


Figure 6.1: Modification of license groups with computers with licenses assigned and excluded computers

Case 2: Computers without an assigned license

As new computers are added to Aether and the pool of unused licenses reaches zero, these computers have the **Computers without a license** status. As new licenses become available, these computers are automatically assigned a license.

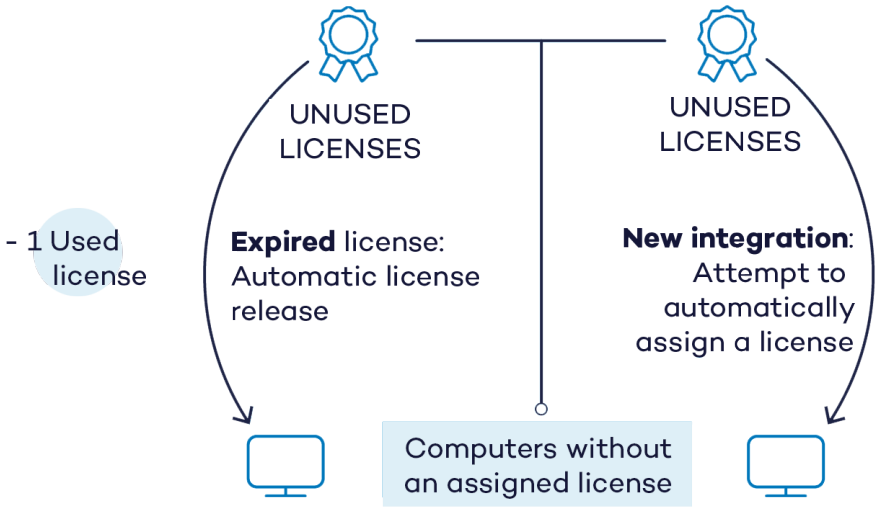


Figure 6.2: Computers without an assigned license due to expiration of the license contract and because the group of unused licenses was empty at the time of onboarding

Similarly, when an assigned license expires, the computer status is **No license** in accordance with the license expiration process explained in the Withdrawal of expired licenses section.

Licenses module panels/widgets

Accessing the dashboard

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

Required permissions

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

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

Licenses

The panel shows how the contracted product licenses are distributed.

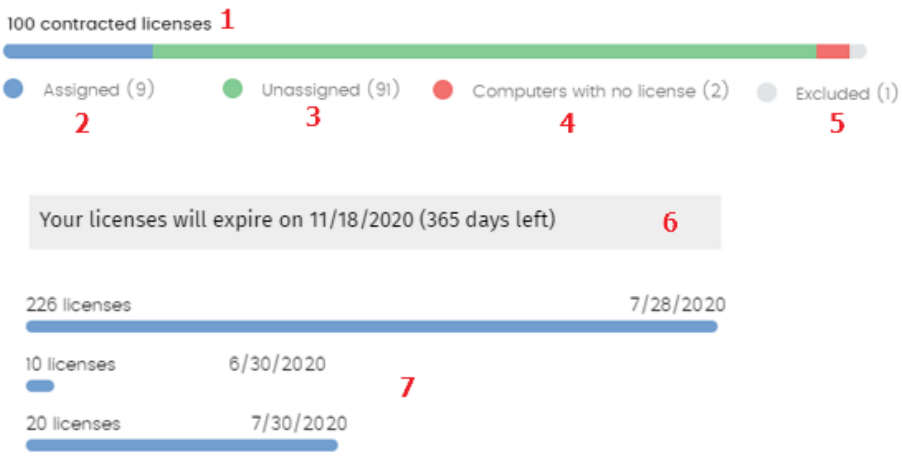


Figure 6.3: License panel with three license contracts

Meaning of the data displayed

Hotspot	Description
Total number of contracted licenses (1)	Maximum number of computers that can be protected if all the contracted licenses are assigned.
Number of assigned licenses (2)	Number of computers protected with an assigned license.
Number of unassigned licenses (3)	Number of licenses contracted that have not been assigned to any computer and are therefore not being used.

Hotspot	Description
Number of computers without a license (4)	Computers that are not protected as there are insufficient licenses. Licenses are assigned automatically as they are bought.
Number of excluded computers (5)	Computers without a license assigned and that are not eligible to have a license.
License expiration date (6)	If there is only one license contract, all licenses expire at the same time, on the specified date.
License contract expiration dates (7)	If one product has been contracted several times over a period of time, a horizontal bar chart is displayed with the licenses associated with each license contract and their expiration date.

Table 6.1: Description of the data displayed in the Licenses panel

Lists accessible from the panel

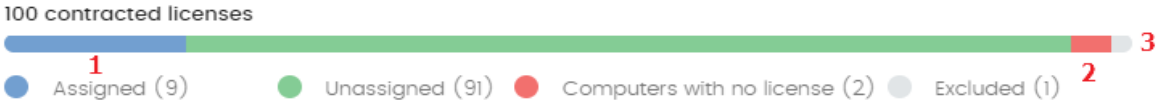


Figure 6.4: Hotspots in the Contracted licenses panel

Click the hotspots shown in the figure to open the **Licenses** list with the following predefined filters:

Filter field	Value
(1) License status	Assigned
(2) License status	No license
(3) License status	Excluded

Table 6.2: Filters available in the Licenses panel

Licenses module lists

Accessing the lists

You can access the lists in two ways:

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

Or,

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

Required permissions

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

Licenses

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

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Endpoint Protection Plus folder tree the computer belongs to.	Character string
License status	The computer's license status.	• Assigned • Computer without a license • Excluded
Last connection	Date when the computer status was last sent to the Panda Security cloud.	Date

Table 6.3: Fields in the Licenses list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account that the product belongs to.	Character string
Computer type	Purpose of the computer within the organization's network	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
Operating system	Operating system installed on the computer, internal version, and patch 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 Plus client software.	Character string
Protection version	Internal version of the protection component that is part of the Panda Endpoint Protection Plus client software.	Character string
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Endpoint Protection Plus software was successfully installed on the computer.	Date
Last	Date when the computer status was last sent to the Panda	Date

Field	Description	Values
connection date	Security cloud.	
License status	The computer's license status.	• Assigned • No license • Excluded
Group	Folder within the Panda Security folder tree 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 6.4: Fields in the Licenses exported file

Filter tool

Field	Description	Values
Search computer	Computer name.	Character string
Computer type	Purpose of the computer within the organization's network	• Workstation • Laptop • Server • Mobile device
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS • Android
Last	Date when the Panda Endpoint Protection Plus status was	• All

Field	Description	Values
connection	last sent to the Panda Security cloud.	• Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
License status	The computer's license status.	• Assigned • No license • Excluded

Table 6.5: Filters available in the Licenses list

Computer details page

Click any of the rows in the list to open the computer details page. See Computer details on page 236 for more information.

Expired licenses

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

Behavior of Aether-based products when their licenses expire

Expiration of Aether-based products has a significant impact on affected computers, because:

- All protections configured for the computers are disabled.
- The signature file is no longer updated on the computers. The computers cannot access the collective intelligence databases.

- Scheduled tasks no longer run on the computers. You cannot run scheduled scans of the computers or install patches to update vulnerable programs.

Computers become very vulnerable to potential data leaks and dangerous infections, from PUPs (potentially unwanted programs), to ransomware and even APTs (advanced persistent threats) with multiple targets.

Seven-day grace period

To prevent this situation, Panda provides a seven-day grace period during which time devices remain protected while you renew their licenses.

This seven-day grace period does not apply to Panda Fusion (Panda Endpoint Protection Plus on Aether + Panda Systems Management). This product does not have a grace period.

Behavior when one of your license contracts expires

In cases where you have multiple license contracts, each for a number of licenses with a different expiration date, computers with licenses assigned do not belong to a particular license contract. Instead, all licenses from all license contracts are included in a single pool of available licenses, which are then distributed to the computers on your network.

When a license contract expires, Panda Endpoint Protection Plus determines the number of licenses assigned to that contract. Then, the solution sorts the computers on the network that have an assigned license by the **Last connection** field, which indicates the date the computer last connected to the Panda Security cloud.

Computers and devices that have been offline for the longest time lose their license and are unprotected.

Selecting which computers are the first to lose their license

Aether enables you to select which computers will lose their license before it expires.

To do that, you can:

- Remove computers from the console. The computer list management tools provides an option to remove computers. See Management tools on page 225.
- Disable computers you do not want to protect but still want to manage from the console. For more information, see Manual release.

When you remove a computer from the console, make sure that you uninstall the agent. Otherwise, the next time the agent contacts the Panda Endpoint Protection Plus server, the computer is re-added to the console and takes up a license.

Panda Endpoint Protection Plus behavior after all licenses expire

From the time all licenses expire until the end of the seven-day grace period (day N to day N+7):

- You can access the console
- Protections continue to update and work correctly

After the grace period (day N+8) and for the next 83 days (day N+8 to day N+90), the license contract data is kept, but computers are unprotected. During this time:

- You cannot access the console
- All protections are disabled

Renewal within 90 days after license expiration

If licenses are renewed within 90 days after they expire:

- Device protection is automatically re-enabled and updated on devices connected to the Internet (usually within 4 hours).

Renewal more than 90 days after license expiration

Ninety days after your licenses expire (day N+90), the agent and the protections are automatically uninstalled. Additionally, the license contract data is deleted from the Panda Security databases.

If you renew the licenses, you must:

- Create users
- Reinstall the agent and the protections
- Create and assign all settings again

Expiration notifications

Thirty days before a license contract expires, the **Licenses** page shows a message indicating the remaining days and the number of licenses that are affected.

Additionally, you can see the license contracts that have expired during the last thirty days.

When all products and license contracts have expired, you can no longer access the management console.

Adding trial licenses to commercial licenses

Where a customer has commercial licenses of Panda Endpoint Protection, Panda Endpoint Protection Plus, or Panda Fusion on the Aether platform and they get a trial version of Panda Endpoint Protection Plus, 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 is created for the trial period, with as many licenses as previously available plus the licenses contracted for the trial.
- The commercial license contracts are temporarily deactivated during the trial period, though their expiration and renewal cycles are unaffected.
- The trial product's functionality is enabled for the trial with no need to update the computers.
- Panda Endpoint Protection Plus is, by default, enabled on all computers in Audit mode. If you do not want to enable Panda Endpoint Protection Plus on all computers or you want to set a different protection mode, this can be configured accordingly.

See Manual and automatic assignment of settings profiles on page 269 for more information about how to assign settings profiles to network computers.

- After the trial period is over, the license contract created for the trial is canceled and the commercial license contract is reactivated. Network computers are automatically downgraded and have their previous settings.

Computer search based on license status

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

See Creating and organizing filters on page 204 for more information about how to create filters in Panda Endpoint Protection Plus.

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

Category	Property	Value	Description
License	Status	Create filters based on the following license statuses:	
		Assigned	Lists computers with a Panda Endpoint Protection Plus license assigned.
		Not assigned	Lists computers that do not have a Panda Endpoint Protection Plus license assigned.
		Unassigned manually	Lists computers whose Panda Endpoint Protection Plus license was manually released by the network administrator.
		Unassigned automatically	Lists computers whose Panda Endpoint Protection Plus license was automatically released by the system.

Table 6.6: Fields in the License filter

Chapter 7

Product updates and upgrades

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

Chapter contents

Updatable modules in the client software

The components installed on user computers are these:

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

The update procedure and options vary depending on the operating system of the device to update, as indicated in Table 7.1: .

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

Table 7.1: Update procedures based on the client software component

- **On demand**: You can launch the update when you want, provided there is an update available, or postpone it for as long as you want.
- **Configurable**: You can configure update windows for future and recurrent updates, and disable them as well.
- **Enable/Disable**: You can enable and disable updates. If updates are enabled, they will run automatically when they are available.
- **No**: You cannot influence the update process. Updates run as soon as they are available, and you cannot disable them.

Protection engine updates

To configure protection engine updates, you must create and assign a **Per-computer settings** profile. To do this, select **Settings** in the top menu. In the left menu, select **Per-computer settings**.

Limits to downloading engine updates from cache and Panda proxy computers

You can download protection engine updates directly from the Internet or through a cache or Panda proxy computer. See Configuring downloads from cache computers on page 286 and Configuring proxies lists for Internet access on page 284.

There are limitations to using one method or another, depending on the computer operating system:

- **Computers with a Windows or macOS operating system**: They can download installation packages from cache computers, proxy computers, and the Internet.

- **Computers with a Linux operating system**: They use the distribution's own package manager to perform downloads. Therefore, they cannot download installation packages through a cache or Panda Endpoint Protection Plus proxy computer.

Cache computers store installation packages until they are no longer valid, at which time they are deleted.

Updates

To enable automatic updates of the Panda Endpoint Protection Plus protection module, click the **Automatically update Panda Endpoint Protection Plus on devices** toggle. This enables all other configuration options on the page. If this option is disabled, the protection module will never be updated.

We recommend that you do not disable protection engine updates. A computer with out-of-date protection becomes more vulnerable to malware and advanced threats over time.

Running updates at specific time intervals

Configure these 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 does not link Panda Endpoint Protection Plus updates to specific days.
- **Days of the week**: Use the checkboxes to select the days of the week on which the Panda Endpoint Protection Plus 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 drop-down menus to set a range of days of the month for the Panda Endpoint Protection Plus 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 drop-down menus to set a specific date range for the Panda Endpoint Protection Plus updates. This option enables you to select update intervals that will not repeat over time. After the specific date range, no updates will be run. This option forces you to constantly establish a new update interval as soon as the previous one expires.

Computer restart

Panda Endpoint Protection Plus enables you to define a logic for computer restarts, if needed, through the drop-down menu at the bottom of the settings page:

- **Do not restart automatically**: A restart dialog box on the target computer prompts the user to restart the computer. The dialog box continues to open until the computer restarts.
- **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 Plus shows a notification in the management console every time a new agent version is available. After that, 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 facilitate security management.

Limits to downloading communications agent updates from cache and Panda proxy computers

You can download communications agent updates directly from the Internet or through a cache or Panda proxy computer. See Configuring downloads from cache computers on page 286 and Configuring proxies lists for Internet access on page 284.

There are limitations to using one method or another, depending on the computer operating system:

- **Computers with a Windows or macOS operating system**: They can download installation packages from cache computers, proxy computers, and the Internet.
- **Computers with a Linux operating system**: They use the distribution's own package manager to perform downloads. Therefore, they cannot download installation packages through a cache or Panda proxy computer.

Cache computers store installation packages until they are no longer valid, at which time they are deleted.

Knowledge updates

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

Knowledge downloads from cache and Panda proxy computers

Computers with a Windows, macOS, or Linux operating system can download knowledge directly from the Internet or through a cache or Panda proxy computer.

Cache computers store signature files until they are no longer valid, at which time they are deleted.

Windows, Linux, and macOS devices

In the top menu, select **Settings**. In the left menu, select **Workstations and servers**.

Go to **General**. These options are shown:

- **Automatic knowledge updates**: Enable or disable signature file downloads. If you clear this option, the signature file will never be updated.

We recommend that you do not disable automatic knowledge updates. A computer with out-of-date protection becomes more vulnerable to malware and advanced threats over time.

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

Android devices

In the top menu, select **Settings**. In the left menu, select **Mobile devices**.

Panda Endpoint Protection Plus enables you to restrict software updates so that they do not consume mobile data.

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

Management console upgrades

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

To carry out this operation, the user account that accesses the web console must have the Full Control role. See Full Control role on page 65.

Considerations prior to upgrading the console version

Although this is a process that takes place entirely on the Panda Security servers, upgrading the console version can push new versions of the security software to customer computers. This can result in traffic

loads and the need to restart the computers on the network in some cases. To reduce traffic during upgrades, see “Configuring downloads from cache computers on page 286”.

Console upgrades are transparent to administrators. They do not affect the console operation. When the process completes, the console closes automatically. When you log in again, you access the upgraded version of the console.

Starting the management console upgrade

- In the upper-right corner of the top menu, click the **Web notifications** icon  . The unread notifications appear.
- If there is a console upgrade available, a message entitled **New management console version** is shown, along with the **New features and improvements** link, the version to which the console will be upgraded, and the **Upgrade console now** button. This type of notification cannot be deleted, as it does not show the  icon. See Web notifications icon on page 33.

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

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

Canceling the upgrade

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

Chapter 8

Managing computers and devices

The web console shows managed devices in an organized and flexible way, enabling you to apply different strategies to rapidly find and manage them.

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

Chapter contents

The Computers area

The **Computers** area in the web console enables you to manage all devices integrated into Panda Endpoint Protection Plus.

To access the computer management page, 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.

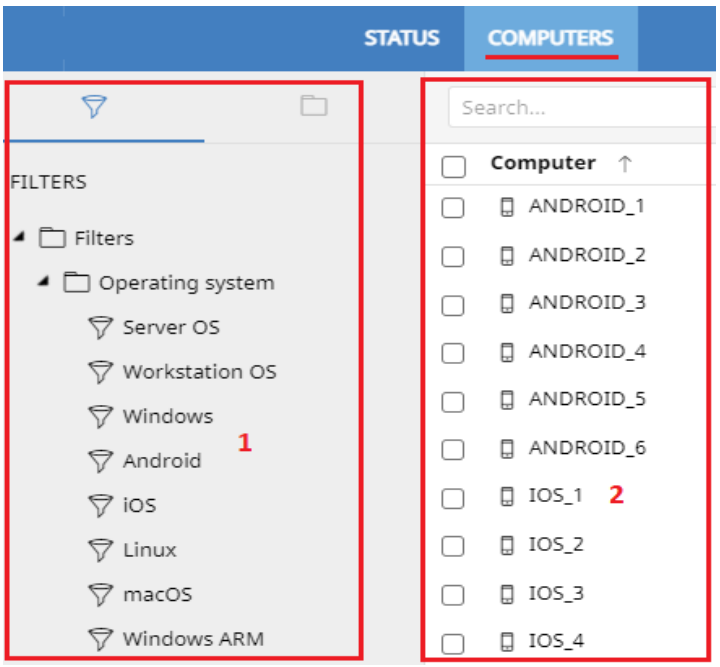


Figure 8.1: General view of the panels in the Computers area

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 are displayed.
- If the option is cleared, only those computers that belong to the selected branch of the tree are displayed.

The Computer tree panel

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

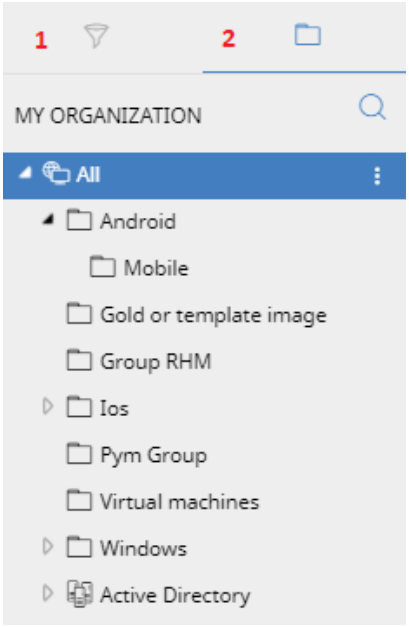


Figure 8.2: The Computer tree panel

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

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

- Find 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 about how to find unprotected computers or those with certain security characteristics or protection status, see Malware and network visibility on page 445. For information about how to assign security settings profiles, see Manual and automatic assignment of settings profiles on page 269. For more information about how to take remediation actions, see Remediation tools on page 567.*

Point the mouse to 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 enables you to 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 panel, by clicking the filter icon . Clicking different items in the tree updates the right panel, presenting all the computers that meet the criteria established in the selected filter.

About filters

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 consists of 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 automatically ceases 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 Plus includes common filters that you can use to organize and locate network computers. You can edit or delete these predefined filters.

> *Cannot recover a predefined filter after you delete it.*

Name	Group	Description
Server OS	Operating system	Lists computers with a server type operating system installed.
Workstation OS	Operating system	Lists computers with a workstation type operating system installed.
Windows	Operating system	Lists all computers with a Windows operating system installed.
Android	Operating system	Lists all devices with an Android operating system installed.
iOS	Operating system	Lists all devices with an Android operating system installed.
Linux	Operating system	Lists all computers with a Linux operating system installed.
macOS	Operating system	Lists all computers with a macOS operating system installed.
Windows ARM	Operating system	List all computers with Windows operating system and ARM microprocessor
Workstations and servers	System type	Lists physical workstations and servers.
Laptops	System type	Lists physical laptops.
Smartphones and tablets	System type	Lists smartphones and tablets.
Virtual machines	System type	Lists virtual machines.
<2GB of memory	Hardware	Lists computers with memory less than 2 GByte
Java	Software	Lists all computers with the Java JRE SDK installed.
Adobe Acrobat	Software	Lists all computers with Acrobat Reader installed.

Name	Group	Description
Reader		
Adobe Flash Player	Software	Lists all computers with the Flash Player plugin installed.
Google Chrome	Software	Lists all computers with the Chrome browser installed.
Mozilla Firefox	Software	Lists all computers with the Firefox browser installed.

Table 8.1: 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 is displayed with the actions available for that particular branch.

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**.

You cannot add a folder below a filter. If you select a filter and then add a folder, the folder is added at the same level as the filter, in the same parent folder.

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**.
- Type the name of the filter. It does not have to be a unique name. See Configuring filters for more information.

Deleting filters and folders

To delete a filter or a folder, click the context menu of the branch to delete, and click **Delete**. This deletes the folder and all of the filters in it.

You cannot delete the Filters root folder.

Moving and copying filters and folders

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

You cannot copy filter folders. Only filters can be copied.

Renaming filters and folders

- Click the context menu of the branch you want to rename.
- Click **Rename**.
- Type a new name.

You cannot rename the root folder. Additionally, to rename a filter you must edit it.

Searching for filters

In very large IT infrastructures, the filter tree can contain a large number of items. This makes finding specific filters difficult.

To find a filter:

- Click the icon at the top of the filter tree. A text box appears.
- Type the letters of the name of the filter you want to find. All filters whose name starts with, ends with, or contains the character string entered are shown.
- After the search is complete, select the filter you wanted to find. Click the icon. The full filter tree is shown again and the filter you searched for appears selected.

Configuring filters

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

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

A filter has four sections:

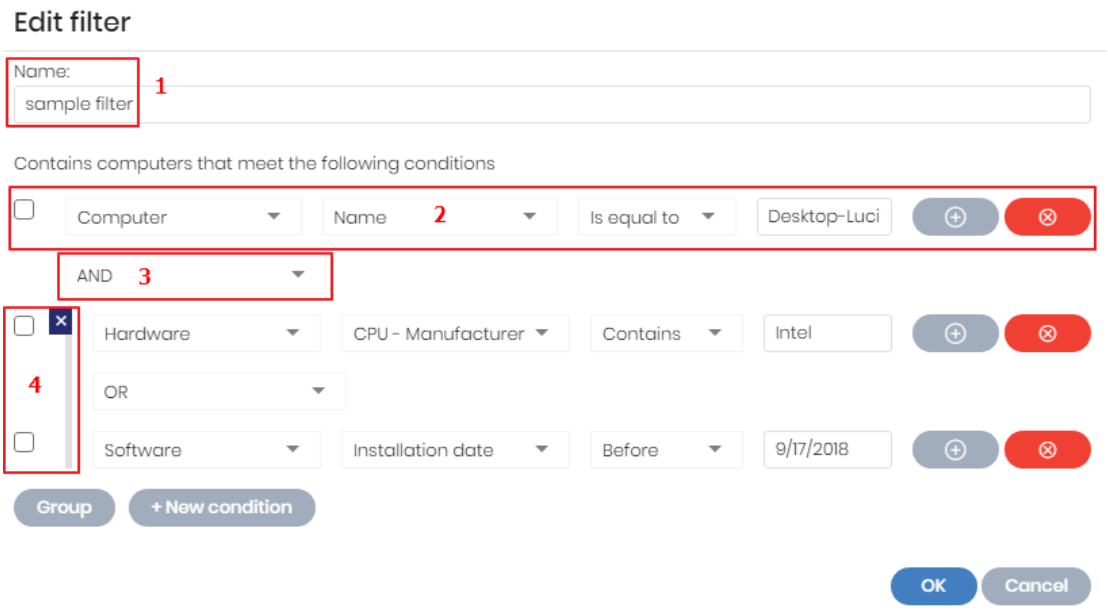


Figure 8.3: Filter settings overview

- **Filter name (1)**: Identifies the filter.
- **Filter rules (2)**: Enables you to set the conditions for belonging to a filter. A filter rule defines only one characteristic of the computers on the network.
- **Logical operators (3)**: Enable you to combine filter rules with the logical operators AND or OR.
- **Groupings (4)**: Enable you to change the order of the filter rules related with logical operators.

Filter rules

A filter rule consists of the items described below:

- **Category**: 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**: 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 reflects 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 automatically appear to establish the

relation between the rules.

Filter rule groupings

In a logical expression, parentheses are used to change 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 conditions**. A thin line appears covering the filter rules that are part of the grouping.

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

Example filters

This topic includes examples of filters commonly created by network administrators:

Filter Windows computers based on the installed processor (x86, x64, ARM64)

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

This filter has two conditions linked by the AND operator:

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

Filter computers without a specific patch installed

Lists computers that do not have a specific patch installed. See Panda Patch Management (Updating vulnerable programs) on page 331 for more information about Panda Patch Management.

- **Category**: Software
- **Property**: Software name
- **Condition**: Doesn't contain
- **Value**: {Patch name}

Filter computers that have not connected to the Panda Security cloud in X days

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

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

Filter computers that cannot connect to the Panda Security security intelligence services

Finds all computers that have problems connecting to any of the Panda Security security intelligence services. Create the following rules linked by the OR operator:

- **Rule**:
    - **Category**: Security
    - **Property**: Connection for collective intelligence.
    - **Condition**: Is equal to
    - **Value**: With problems
- **Rule**:
    - **Category**: Security
    - **Property**: Connection for web protection.
    - **Condition**: Is equal to
    - **Value**: With problems

Filter computers integrated with other management tools

Lists computers with a name that matches a computer name specified in a list obtained by a third-party tool. Each line in the list must end with a carriage return and is considered a computer name.

- **Category**: Computer
- **Property**: Name
- **Condition**: In
- **Value**: Computer name list

Filter computers not compatible with SHA-256 signed drivers

- **Category**: Computer
- **Property**: Supports SHA-256 signed drivers
- **Condition**: Is equal to
- **Value**: False

Computers with a public IP address

Lists computers that accessed the Internet through a device (router/proxy/VPN endpoint) that has the specified IP address.

- **Category**: Computer
- **Property**: Public IP address
- **Condition**: Is equal to (lists computers that accessed the Internet through a device with a specific IP address).

Computers discovered in Active Directory

Lists managed and unmanaged computers that have been discovered using Active Directory.

- **Category**: Computer
- **Property**: Last seen in Active Directory
- **Condition**: Is between (to list computers discovered between two specific dates).

Group tree

The group tree enables you to statically arrange the computers on the network in the groups that you choose.

To access the group tree, follow the steps below:

- Click the folder icon  from the left 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.

About groups

A group contains computers manually assigned by the administrator. The group tree enables you to 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 top group under which all other groups reside.
Native groups 	These are Panda Endpoint Protection Plus groups, some of which are predefined. These groups support all operations (such as move, rename, or delete) and can contain other groups and computers.
IP-based groups 	Native group with associated IPs or IP ranges to speed up integration of new computers in the security service.
Active Directory groups 	These groups replicate your Active Directory structure. These groups do not support some operations. They can contain other Active Directory groups and computers..
Active Directory root group 	This group contains all Active Directory domains configured on the organization's network.. It contains Active Directory domain groups.
Active Directory domain group 	These groups are Active Directory branches that represent domains. They contain other Active Directory domain groups, Active Directory groups, and computers.

Table 8.2: Group types in Panda Endpoint Protection Plus

The size of the organization, the uniformity of the managed computers, and the presence or absence of an Active Directory server on the company network determines the structure of the group tree. The group structure may vary from a flat tree with a single level for the simplest cases, to a complex structure with several levels for large networks made up of highly heterogeneous computers.

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

Active Directory groups

For organizations with an Active Directory server, Panda Endpoint Protection Plus can automatically replicate the Active Directory structure on the My Organization tab. This works as follows: The Panda agent

installed on each computer reports the Active Directory group it belongs to to the web console and, as agents are deployed, the tree is populated with the various organizational units. This way, the branch shows a structure familiar to you, helping you find and manage your computers faster.

To make sure the structure is consistent between Active Directory and the My Organization tab, you cannot modify Active Directory groups in Panda Endpoint Protection Plus. Panda Endpoint Protection Plus automatically updates Active Directory groups within one hour when you make changes to your Active Directory structure.

In Panda Endpoint Protection Plus, if you move a computer from an Active Directory group to a native group or to the root group, the synchronization relationship with Active Directory breaks. Any changes you make to Active Directory groups that affect the moved computer are not reflected in Panda Endpoint Protection Plus.

For information on how to reestablish the synchronization relationship between Active Directory and Panda Endpoint Protection Plus, see Returning multiple computers to their Active Directory group.

Creating and organizing groups

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

Creating a group

- Click the context menu of the parent group to which the new group will belong, and click **Add group**.
- Type the name of the group in the **Name** text box and click the **Add** button.

> *You cannot create Active Directory groups from the group tree. The tree replicates the groups and organizational units that already exist on your Active Directory server.*

To automatically assign computers to a group when you install the Panda Endpoint Protection Plus agent, you can specify the IP addresses or an IP address range for the group:

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

Computers are added to the group when you install the Panda Endpoint Protection Plus agent. If the computer IP address changes, the computer remains in the original group.

Deleting groups

Click the context menu of the group you want to delete. To delete a group, it must be empty. If the group contains subgroups or computers, an error message appears.

You cannot delete the All group.

To delete 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 you want to move.
- Click **Move**. A pop-up window appears with the target group tree.
- Select the target group and click **OK**.

You cannot move the All group or any Active Directory groups.

Renaming groups

- Click the context menu of the group you want to rename.
- Click **Change name**.
- Type a new name.

You cannot rename the All group or any Active Directory groups.

Importing IP-based assignment rules to existing groups

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

- Select the context menu of a native group other than the Al' group and select the **Import IP-based assignment rules** option. A window opens for you to drag a file with the IP addresses to add.
- The import file must contain one or more rows of text with the following format:
    - For individual IP addresses, include one address per row. For example:
        - `.\Group\Group\Group (Tab) IP address`
    - For IP address ranges, include one range per row. For example:

- `.\Group\Group\Group (Tab) Start IP-End IP`

- Panda Endpoint Protection Plus interprets all specified paths as part of the selected group.
- If the groups indicated in the file do not already exist, Panda Endpoint Protection Plus creates them and assigns the specified IP addresses to them.

- Click **Import**. The IP addresses are assigned to the groups specified in the file. The icons on the My Organization tab update to reflect any changes to group type.

> *When you import a file with new group-IP pairs, the solution deletes all IP addresses previously assigned to an IP-based group.*

When the process is complete, as new computers are integrated into Panda Endpoint Protection Plus, they move to the relevant groups based on their IP address.

Exporting IP-based assignment rules

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

- Click the context menu of a group from which you want to export IP-based rules, and select the option **Export IP-based assignment rules**. A CSV file downloads with the IP-based assignment rules defined for the group and its subgroups.
- The CSV file has the format specified in section Importing IP-based assignment rules to existing groups.

Moving computers from one group to another

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

Moving groups of computers to groups

- Select the group **All** in order to list all managed computers, or use the search tool to locate a specific group of computers you want to move.
- In the list of computers, select the checkboxes next to the computers you want to move.
- Click the ⋮ icon to the right of the search bar. A drop-down menu appears with the option **Move to**. Click it to show the target group tree.
- Select the target group you want 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 page 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** property and click **Change**. A window opens with the target group tree.
    - Select the target group to move the computer to. Click **OK**.

Moving computers from an Active Directory group

A computer that belongs to an Active Directory group is synchronized with your Active Directory server and cannot be moved to another Active Directory group through Panda Endpoint Protection Plus. To do this, you must move the computer in Active Directory and then wait up to one hour for Panda Endpoint Protection Plus to synchronize the change. However, computers belonging to an Active Directory group can be moved to a native group.

If you move a computer from an Active Directory group to a native group, any changes made to the company's Active Directory groups will not be reflected in the web console. See Active Directory groups for more information.

Moving computers to an Active Directory group

You cannot move a computer from a native group to a specific Active Directory group. You can only return a computer to the Active Directory group that it previously belonged 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 in the group that you moved to other groups return to their original Active Directory group.

Filtering results by groups

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

Configuring the filter by groups

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

- Click the relevant button from the top menu. A window with the group tree is displayed.
- Select the groups you want to see from the computer tree and click **OK**.

The console only displays information for the computers from the selected groups.

Filters do not affect task visibility, email alerts, or scheduled executive reports.

Filtering groups

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

- Click the  icon at the top of the group tree. A text box appears.
- Type the letters of the name of the group you want to find. All groups whose name starts with, ends with, or contains the character string entered are shown.
- After you have completed your search, select the group you are interested in and click the  icon to show the full group tree again, maintaining your selection.

Available lists for managing computers

Computers list

Accessing the list

- From the top menu, select **Computers**. The left pane shows the computer or folder tree. The right pane shows a detailed table of the managed computers on the network.
- Click an item from the group tree or filter tree on the left. The right pane updates with details of the selected item.

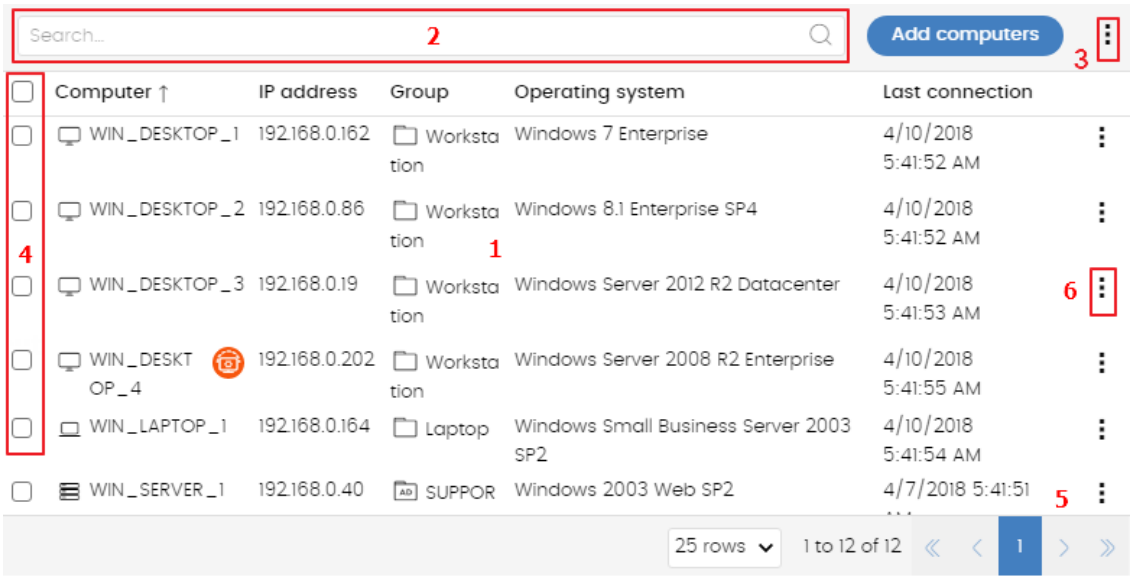


Figure 8.4: Computers list

Required permissions

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

Computers

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

The items that appear in the computer list are these:

- **(1)** List of computers that belong to the selected branch.
- **(2)** Search tool: Find computers by their name, description, IP address, last logged-in user, or MUID (computer ID used in Orion). It supports partial matches. Search terms are not case-sensitive.
- **(3)** General context menu: Apply an action to multiple computers.
- **(4)** Computer selection checkboxes.
- **(5)** Pagination controls at the bottom of the pane.
- **(6)** Context menu for each computer.

You can configure the computer list to adapt the data shown to your needs.

To add or remove columns in the table, click the context menu in the upper-right corner of the page. Select **Add or remove columns**. A dialog box opens that shows the available columns and a **Default columns** link to reset the list to its default values.

Use the context menu to export the computer list. The exported file can contain all data in the computer list (see Fields displayed in the exported file) or a shortened version of it (see Fields displayed in the shortened exported file). The latter option is very useful when there is a large number of computers.

- Click the icon to show the list options.
- Click the  icon to export the computer list or a shortened version of it.

You can see this detailed information for each computer:

Field	Description	Values
Computer	Computer name and type.	Character string: • Workstation or server • Laptop • Mobile device (Android smartphone or tablet)
Computer status	Agent reinstallation: • Reinstalling the agent. • Error reinstalling the agent. Protection reinstallation: • Reinstalling the protection. • Error reinstalling the protection. • Pending restart.	Icon
IP address	The computer primary IP address.	IP address
Last logged-in user	Names of the user accounts that have an active session on the computer.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder within the Panda Endpoint Protection Plus group tree to which the computer belongs, and its type.	Character string: • Group • IP-based group

Field	Description	Values
		•  Active Directory AD or root domain •  Organizational unit •  Group tree root
Active Directory path	Full path to the computer in the company Active Directory.	Character string
Domain	Windows domain the computer belongs to.	Character string
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 the Panda Security cloud.	Date

Table 8.3: Fields in the Computers 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
Computer	Computer name.	Character string
IP address	Comma-separated list of the IP addresses of all cards installed on the computer.	Character string
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.	IP address

Field	Description	Values
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	Full path to the computer in the company Active Directory.	Character string
Group	Folder within the Panda Endpoint Protection Plus group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Endpoint Protection Plus 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
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Virtual machine	Shows whether the computer is physical or virtual.	Boolean
Is a non-persistent computer	Shows whether 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

Field	Description	Values
Last update on	Date when the protection was last updated.	Date
Licenses	Licensed product.	Panda Endpoint Protection Plus
Network settings	Name of the network settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the network settings profile.	Character string
Security for workstations and servers	Name of the security settings profile applied to the workstation or server.	Character string
Settings inherited from	Name of the folder from which the device inherited the security settings profile.	Character string
Security for Android devices	Name of the security settings profile applied to the mobile device.	Character string
Settings inherited from	Name of the folder from which the device inherited the security settings profile.	Character string
Security for iOS devices	Name of the security settings profile applied to the mobile device.	Character string
Settings inherited from	Name of the folder from which the device inherited the security settings profile.	Character string
Per-computer settings	Name of the settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the settings profile.	Character string
Data Control	Name of the personal data monitoring (Panda Data Control) settings profile applied to the computer.	Character string

Field	Description	Values
Settings inherited from	Name of the folder from which the computer inherited the personal data monitoring settings profile.	Character string
Patch management	Name of the patching (Panda Patch Management) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the patching settings profile.	Character string
Encryption	Name of the encryption (Panda Full Encryption) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the encryption settings profile.	Character string
Program blocking	Name of the program blocking settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the program blocking settings profile.	Character string
Description	Description assigned to the computer.	Character string
Last logged-in user	Comma-separated names of the user accounts that have an interactive session active on the Windows computer.	Character string
Requested action	Requested action that is pending execution or is in progress.	• Restart • Protection reinstallation • Agent reinstallation
Requested action failed	Type of error reported by the requested action.	• Wrong credentials • Discovery computer not available • Unable to connect to

Field	Description	Values
		the computer • Operating system not supported • Unable to download the agent installer • Unable to copy the agent installer • Unable to uninstall the agent • Unable to install the agent • Unable to register the agent • Action requires input from the user
Last proxy used	Access method used by Panda Endpoint Protection Plus the last time it connected to the Panda Security cloud. This data is not updated immediately. It might take up to 1 hour for the correct value to show.	Character string
Shadow Copies	Shows the feature status: • Enabled • Disabled • **Error 2010**: The Shadow Copies service could not be enabled. • **Error 2011**: An error occurred creating the last Shadow Copy.	Enumeration
Last copy	Date and time the last copy was made.	Date

Table 8.4: Fields in the Computers list exported file

Fields displayed in the shortened exported file

When you select **Reduced export**, a file is generated that contains this information:

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
IP address	Comma-separated list of the IP addresses of all cards installed on the computer.	Character string
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.	IP address
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	Full path to the computer in the company Active Directory.	Character string
Last seen in Active Directory	Date when the computer was last seen in Active Directory.	
Group	Folder in the Panda Endpoint Protection Plusgroup tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last bootup date	Date when the computer was last booted.	Character string
Installation date	Date when the Panda Endpoint Protection Plus 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

Field	Description	Values
		• macOS
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Virtual machine	Shows whether the computer is physical or virtual.	Boolean
Is a non-persistent computer	Shows whether 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 Plus
Description	Description assigned to the computer.	Character string
Last logged-in user	Comma-separated names of the user accounts that have an interactive session active on the Windows computer.	Character string
Requested action	Requested action that is pending execution or is in progress.	• Restart • Protection reinstallation • Agent reinstallation
Requested action failed	Type of error reported by the requested action.	• Wrong credentials • Discovery computer not available • Unable to connect to the computer • Operating system

Field	Description	Values
		not supported • Unable to download the agent installer • Unable to copy the agent installer • Unable to register the agent • Action requires input from the user
Last proxy used by the agent	Access method used by Panda Endpoint Protection Plus the last time it connected to the Panda Security cloud. This data is not updated immediately. It might take up to 1 hour for the correct value to show.	Character string
Shadow Copies	Shows the feature status: • **Enabled** • **Disabled** • **Error 2010**: The Shadow Copies service could not be enabled. • **Error 2011**: An error occurred creating the last Shadow Copy.	Enumeration
Last copy	Date and time the last copy was made.	Date

Table 8.5: Fields in the Computers list shortened exported file

Filter tools

Field	Description	Values
Computer	Computer name.	Character string.

Table 8.6: Filters available in the Computers list

Management tools

To access the management tools:

- Select one or more computers using the checkboxes **(4)**. The search tool **(2)** hides and the action bar **(7)** appears.

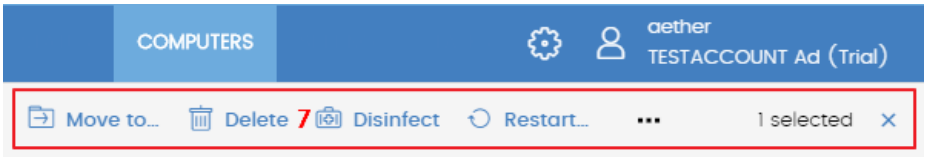


Figure 8.5: Action bar

Select the checkbox in the table header **(4)** to select all computers on the current page of the list. The **Select all xx rows in the list** option appears, which enables you to select all computers on the list regardless of the page you are on.

- Click the context menu **(6)** for a computer or mobile device.

Action	Description
Move to	Opens a dialog box that shows the group tree. Select the group you want to move the computer to. The computer inherits the settings profiles assigned to the target group. For more information, see Creating and managing settings profiles on page 267.
Move to Active Directory path	Moves the computer to a group that corresponds with its organizational unit in Active Directory.
Delete	Deletes the computer from the console and uninstalls the Panda Endpoint Protection Plus endpoint software. For more information, see Uninstalling the software on page 169.
Scan now	For an introduction to scan tasks, see On-demand computer scanning and disinfection on page 568. For a full description, see Tasks on page 581.
Schedule scan	For an introduction to scan tasks, see On-demand computer scanning and disinfection on page 568. For a full description, see Tasks on page 581.
Restart	Restarts the computer. For more information, see Computer restart on page 577.
View available patches	Opens the **Available patches** list filtered for the selected computer. See Available patches on page 376.
Schedule patch	For more information about how to install patches on Windows computers,

Action	Description
installation	see Panda Patch Management (Updating vulnerable programs) on page 331.
Reinstall protection (requires restart)	Reinstalls the security software if a malfunction occurs. For more information, see Remote reinstallation on page 173.
Reinstall agent	Reinstalls the agent if a malfunction occurs. For more information, see Remote reinstallation on page 173.
Selected	Undoes the current selection.
Report a problem	Sends a report to Panda Security technical support to diagnose problems with the computer.

Table 8.7: Computer management tools

My lists panel

Accessing the My lists panel

- Go to top menu **Status**. Click **Add** in the **My lists** section in the side panel. A window appears with all available lists.
- From the **General** group, select the **Hardware**, **Software**, or **Computers with duplicate name** list.

See Managing lists on page 41 for more information about the types of lists and how to work with them.

For more information about the fields as well as the filter and search tools implemented in each list, see the chapter on the group the list belongs to.

Required permissions

No additional permissions are required to access the **My lists** panel.

Hardware

Shows the hardware components installed on each computer on the network. Each hardware component is shown independently each time it is detected on a computer.

Field	Description	Values
Computer	Name and type of computer that contains the hardware component.	Character string: •  Workstation or server. •  Laptop. •  Mobile device (Android smartphone or tablet).
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
CPU	Make and model of the microprocessor installed on the computer. The number of installed cores is shown in brackets.	Character string
Memory	Total amount of RAM memory installed.	Character string
Disk capacity	Sum of the capacity of all the internal hard disks connected to the computer.	Character string
Last connection	Date when the Panda Endpoint Protection Plus status was last sent to the Panda Security cloud.	Date
Context menu	Management tools. See Management tools for more information.	

Table 8.8: Fields in the Hardware list

Fields displayed in the exported file

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

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder in the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last connection	Date when the Panda Endpoint Protection Plus status was last sent to the Panda Security cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
System	Name of the computer's hardware model.	Character string
CPU-N	Model, make, and characteristics of CPU number N.	Character string
CPU-N Number	Number of cores in CPU number N.	Numeric value

Field	Description	Values
of cores		
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
BIOS - Serial number	The computer's BIOS serial number.	Character string

Table 8.9: Fields in the Hardware exported file

Filter tool

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

Table 8.10: Filters available in the Hardware list

Software

Shows all programs installed on the computers on the 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 Computers list filtered by the selected package. The list shows all computers on the network that have that package installed.

Field	Description	Values
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Version	Internal version of the software package.	Character string
Computers	Number of computers that have the package installed.	Numeric value

Table 8.11: Fields in the Software exported file

Fields displayed in the exported file

Field	Description	Values
Client	Customer account 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 8.12: Fields in the Software exported file

Fields displayed in the detailed Excel export file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device

Field	Description	Values
Computer	Computer that contains the package found.	Numeric value
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Installation date	Date the software was installed.	Date
Size	The size of the installed software.	Numeric value
Version	Internal version of the software package.	Character string
Group	Folder in the Panda Endpoint Protection Plus group 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 by the administrator.	Character string

Table 8.13: Fields in the detailed export file

Filter tool

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

Table 8.14: Filters available in the Software list

Computer list page

Click any of the rows in the list to display a list of computers filtered by the selected software. See Computers for more information.

Computers with duplicate name

Shows computers on the network with the same name and belonging to the same domain. Where computers have the same name, Panda Endpoint Protection Plus considers the computer that has most recently connected to the Panda Security cloud to be the only correct one. This computer is not shown in the list.

To delete duplicate computers, select them using the relevant checkboxes and click **Delete** from the toolbar. A window is shown asking you if you wish to uninstall the Panda Endpoint Protection Plus agent.

*Deleting computers from the **Computers with duplicate name** list without uninstalling the Panda Endpoint Protection Plus agent removes them from the Panda Endpoint Protection Plus console. However, those computers reappear in the Panda Endpoint Protection Plus console the next time they connect to the cloud. To avoid deleting multiple computers if you are not sure which ones are true duplicates, we recommend that you do not remove the agent from the computers and see which ones reappear in the console.*

Field	Description	Values
Computer	Computer name and type.	Character string: • Workstation or server • Laptop. • Mobile device (Android smartphone or tablet).
IP address	The computer's primary IP address.	Character string
Group	Folder in the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string

Field	Description	Values
Last connection	Date when the Panda Endpoint Protection Plus status was last sent to the Panda Security cloud.	Date

Table 8.15: Fields in the Computers with duplicate name 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
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 in the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Protection version	Internal version of the protection module installed on the computer.	Character string
Installation date	Date when the Panda Endpoint Protection Plus software was successfully installed on the computer.	Date
Last connection date	Date when the Panda Endpoint Protection Plus status was last sent to the Panda Security cloud.	Date
Platform	Type of operating system installed.	• Windows

Field	Description	Values
		• Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Active Directory	Full path to the computer in the company's Active Directory.	Character string
Last logged-in user	Names of the user accounts that have an active session on the computer.	Character string
Last bootup date	Date when the computer was last booted.	Date

Table 8.16: Fields in the Computers with duplicate name exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	• All • Windows • Linux • macOS • Android
Last connection	Date when the Panda Endpoint Protection Plus status was last sent to the Panda Security cloud.	• All • Less than 24 hours ago • Less than 3

Field	Description	Values
		days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago

Table 8.17: Filters available in the Computers with duplicate name list

Computer details page

Click any of the rows in the list to open the computer details page. See Computer details for more information.

Computer details

When you select a device from the list of computers, a page opens and shows details of the hardware, software, and security settings of the computer.

To show or hide the general details section and notifications, click or .

The details page is divided into these sections:

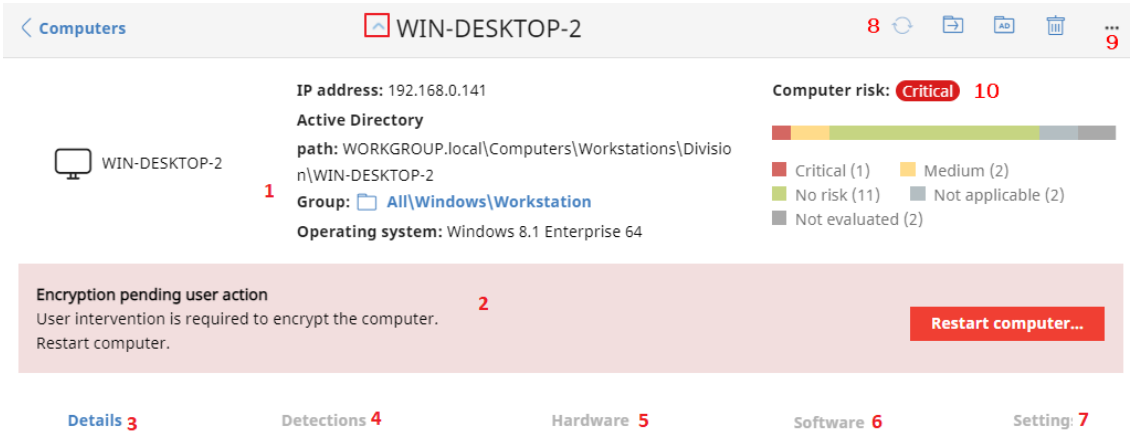


Figure 8.6: Computer overview

- **General (1)**: Information to help you identify the computer.
- **Notifications (2)**: Notifications that might indicate potential problems.
- **Details (3)**: Lists a summary of the hardware, software, and security settings of the computer.
- **Detections (4)**: Indicates the security status of the computer.
- **Hardware (5)**: Lists hardware installed on the computer, its components and peripherals, as well as resource consumption and use.
- **Software (6)**: Lists software packages installed on the computer, as well as versions and changes.
- **Settings (7)**: Lists security settings and other settings assigned to the computer.
- **Toolbar (8)**: Includes buttons for each action you can take for managed computers.
- **Hidden icons (9)**: Based on the size of the screen, some tools might be hidden in an options menu.
- **Computer risk (10):** Risk information for the computer, including the risk level. See Risk assessment module lists on page 490.

General section (1)

Contains the following information for all types of devices:

Field	Description
Computer	Computer name and icon indicating the computer status.
IP address	The computer's IP address.
Last logged-in user	Last logged-in user on the computer.
Description	Computer description assigned by the network administrator.
Group	Folder in the group tree to which the computer belongs.
Active Directory path	Full path to the computer in the company's Active Directory.
Domain	Domain the computer belongs to.
Operating system	Full version of the operating system installed on the computer.
Last	Date when the client software last connected to the Panda Endpoint Protection

Field	Description
connection	Plus cloud.
Computer risk	Distribution graph that shows the overall risk level for the computer and the risks detected on it. See Risk assessment module lists on page 490.

Table 8.18: Fields in the General section of a computer's details

General section for mobile devices

With mobile devices, the General **(1)** and Computer notifications **(2)** sections are replaced with the anti-theft dashboard, from which you can take remote actions on managed devices.

In the case of iOS devices, the actions you can take vary depending on whether the mobile device is enrolled in an MDM solution or not. See Installation on iOS systems on page 142.

See Anti-theft on page 325 for more information about how to enable the anti-theft feature for mobile devices and configure private mode.

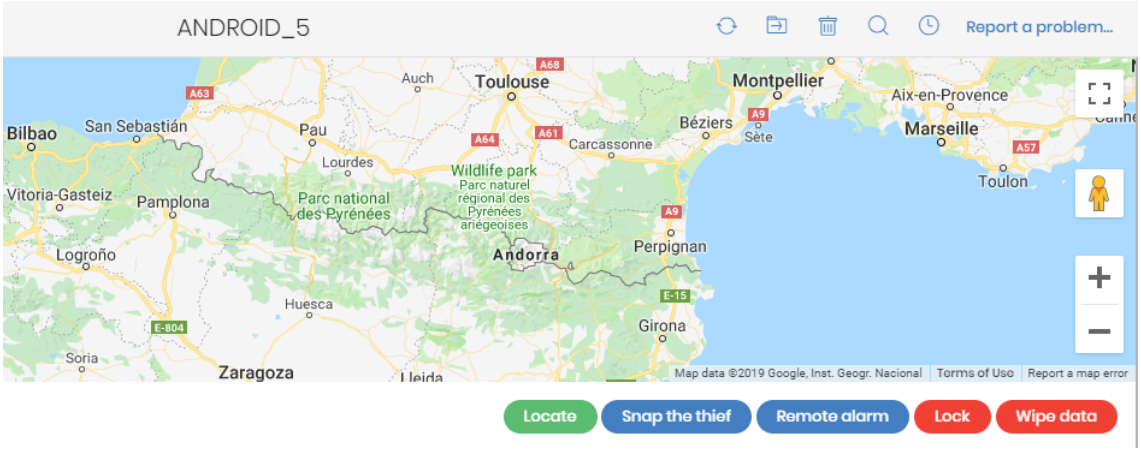


Figure 8.7: Anti-theft dashboard for mobile devices

The available actions are:

Action	Description
Locate	Panda Endpoint Protection Plus uses the device GPS to locate it. If this feature is unavailable, it tries to locate the device through Wi-Fi or the carrier communication infrastructure.

Action	Description
	• **With private mode enabled**: The console opens a window that prompts you to enter the code entered by the device user to enable private mode. When you enter the correct code, Panda Endpoint Protection Plus gets the device coordinates and shows the device location on the map. • **With private mode disabled**: The Panda Endpoint Protection Plus server gets the device coordinates and shows the device location on the map.
Snap the thief	This option is not available on iOS devices. When anti-theft is enabled, you can take a photo of the person using the Android device. The feature shows a window where you can enter an email address to send a photo of the potential thief to. Specify when you want the photo to be taken: • **Now**: The Panda Endpoint Protection Plus agent immediately takes a photo from the device and sends it to the specified address. • **When the screen is touched**: The Panda Endpoint Protection Plus agent takes a photo and sends it to the specified address when the user or potential thief touches the device screen.
Remote alarm	Shows a window where you can send a remote alarm and message to the mobile device. By default, the alarm sounds immediately, even if the device is locked. The screen shows the message and phone number you specify. To prevent an alarm sound, select the **Don't play any sound** checkbox.
Lock	Locks the mobile phone to prevent it from being used in the event of loss or theft, and requires the user to enter the PIN specified in the administrator console to open the device. Even though the administrator console always requires the user to enter the unlock PIN when you enable this feature, the behavior varies depending on the Android or iOS version used by the device. **Android**: • **Versions lower than 7**: The web console prompts you to create a PIN, which is then used to lock the device. • **Versions 7 to 10**: If a PIN was never created, the web console prompts you to create one and uses it to lock the phone. If a PIN was previously created by the user, it is used to lock the phone, regardless of the PIN you specify in the console. • **Versions 11 or higher**: If a PIN was previously created by the user, it is used to lock the phone, regardless of the PIN you specify in the console. If a PIN was never

Action	Description
	created, the device screen turns off and there is no lock PIN. **iOS**: • **Versions 13 or higher**: If a PIN was previously created by the user, it is used to lock the phone, regardless of the PIN you specify in the console. If a PIN was never created, the device screen turns off and there is no lock PIN.
Wipe data	This option deletes all device contents and applications and returns the device to factory settings.

Table 8.19: Actions supported by the anti-theft module for mobile devices

Computer notifications section (2)

These notifications describe problems encountered on computers with regard to the operation of Panda Endpoint Protection Plus and provide instructions for resolving them.

Occasionally, notifications **(1)** are accompanied by codes **(2)**.

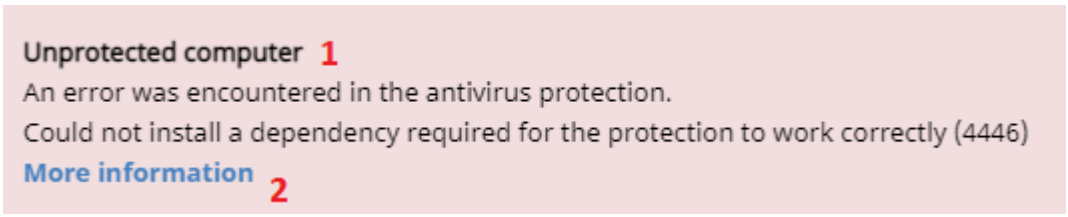


Figure 8.8: Unprotected computer notification and associated code

Each code is related to an error that occurs before or during the installation of the protection on computers. For more information about these codes, see https://www.pandasecurity.com/en/support/card?id=700031.

These tables list the types of notifications generated and recommended actions.

Licenses

Notification	Description	Reference
Computer without a license	There are no available licenses to assign to the computer. Release an assigned license or purchase more Panda Endpoint Protection Plus licenses.	For more information, see Releasing licenses on page 180.
	There are free licenses but none of them have been assigned to this computer.	For more information, see

Notification	Description	Reference
		Assigning licenses on page 179.

Table 8.20: Notifications related to license assignment

Protection software installation errors

Errors that occur during the protection software installation process are shown with an error code, its associated extended error code, and an extended error subcode, where available. For more information, see table on page 461.

Notification	Description	Reference
Unprotected computer	There was an error during installation of the security product on the computer. With errors whose origin is known, a description of the cause is displayed. If the origin is unknown, the associated error code is displayed.	For more information, see Product features and requirements on page 602.
	A reboot is required to complete the installation due to a previous uninstallation.	For more information, see Computer restart on page 577.
	The agent does not have the permissions required on macOS computers.	For more information, see Requirements for macOS platforms on page 612.
	Error when installing the protection on macOS 13 Ventura. The user must allow	For more information, see Requirements for macOS platforms on page 612.

Notification	Description	Reference
	EndpointProtectionService from Login Items.	
	Unsupported Linux kernel.	For more information, see https://www.pandasecurity.com/en/support/card?id=700031.
	Unsupported Unbreakable Enterprise Kernel (UEK) release.	For more information, see https://www.pandasecurity.com/en/support/card?id=700031.
Error installing Data Control	There was an error during installation of Panda Data Control on the computer.	For more information, see Panda Data Control requirements.
Error installing the protection and Data Control	There was an error during installation of the protection and the module on the computer.	For more information, see Product features and requirements on page 602 and Panda Data Control requirements.
Error installing the patch manager	There was an error during installation of the patch management module.	For more information, see Make sure that Panda Patch Management works correctly on page 336.
Error installing the encryption module	There was an error during installation of the encryption module.	For more information, see Panda Full Encryption minimum requirements on page 416.
Error installing the Panda agent	Wrong credentials.	For more information, see Offline computers on page 449.
	The discovery computer is not available.	For more information, see Security module panels/widgets on page 445, and Designating a discovery computer on page 111.
	Unable to connect to the target computer	For more information, see Security module panels/widgets on page 445, and Product features

Notification	Description	Reference
	because it is turned off or does not comply with the hardware or network requirements.	and requirements on page 602.
	The computer operating system is not supported.	For more information, see Product features and requirements on page 602.
	Unable to download the agent installer due to a network error.	For more information, see Product features and requirements on page 602.
	Unable to copy the agent installer due to low free disk space on the computer.	For more information, see Product features and requirements on page 602.
	Unable to copy the agent installer because the target computer is turned off or does not meet the remote installation requirements.	For more information, see Offline computers on page 449, and Product features and requirements on page 602.
	Unable to register the agent.	For more information, see Offline computers on page 449, and Product features and requirements on page 602.
Error communicating with servers	The computer cannot connect to one or more servers in the Panda cloud.	For more information, see Product features and requirements on page 602.

Table 8.21: Notifications related to the installation of the Panda Endpoint Protection Plus software

Protection software reinstallation errors

Errors that occur during the protection software reinstallation process are shown with an error code, its associated extended error code, and an extended error subcode, where available. For more information, see table Table 15.16: on page 463.

Notification	Description	Reference
Pending protection reinstallation	The administrator requested reinstallation of the security product. Reinstallation is incomplete because the computer is off or offline, or there is still time before the forced restart.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
Pending agent reinstallation	The administrator requested reinstallation of the agent. Reinstallation is not complete because the computer is off or offline, or there is still time before the forced restart.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
Error installing the Panda agent	Wrong credentials.	For more information, see Offline computers on page 449.
	The discovery computer is not available.	For more information, see Offline computers on page 449.
	Unable to connect to the computer. It is off or offline, or does not meet remote installation requirements.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
	The operating system is not supported. It does not meet remote installation requirements.	See Remote reinstallation requirements on page 173.

Notification	Description	Reference
	Unable to download the agent installer to the target computer. The computer is turned off or does not meet remote installation requirements.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
	Unable to copy the agent installer to the target computer. It is turned off or does not meet remote installation requirements.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
	Unable to uninstall the agent from the target computer. It is turned off or does not meet remote installation requirements.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
	Unable to install the agent on the target computer. It is turned off or does not meet remote installation requirements.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
	Unable to register the agent because the computer is turned off or does not meet remote installation requirements.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.
	Action requires input from the user.	See Offline computers on page 449 and Remote reinstallation requirements on page 173.

Table 8.22: Notifications related to the reinstallation of the Panda Endpoint Protection Plus agent

Panda Endpoint Protection Plus software issues

Notification	Description	Reference
Unprotected computer	An error was encountered in the antivirus protection. Restart the computer to fix the problem.	See Computer restart on page 577.
Error encrypting the computer	Unable to encrypt the computer due to an error.	See Computer restart on page 577.

Table 8.23: Notifications related to Panda Endpoint Protection Plus software issues

Pending user or administrator action

Notification	Description	Reference
Encryption pending user action	The user must restart the computer or enter the relevant encryption credentials to complete the encryption process.	See Encryption and decryption on Windows computers on page 418 and Encryption and decryption on macOS computers
Pending restart	The administrator has requested that the computer be restarted but it has not restarted yet as it is offline or the time period for a forced reboot has not ended yet.	See Offline computers on page 449.
Reinstalling the protection.	The administrator has requested that the computer protection be reinstalled but the operation is not yet complete because the computer is turned off or offline, the amount of time to wait before the reinstallation is forced has not passed, or the reinstallation is in progress.	See Remote reinstallation on page 173
Unprotected computer	The antivirus protection is disabled. Enable the protection.	See Manual and automatic assignment of settings profiles on page 269, Creating and managing settings profiles on page 267, and Antivirus on page 304.

Notification	Description	Reference
Computer offline for N days	The computer is turned off or does not meet the network access requirements.	See Product features and requirements on page 602
Outdated protection	The protection requires the local user to manually restart the computer to complete the installation.	This is only on computers with the Home and Starter versions of Windows.
Connection problems with the Panda Security servers	The computer cannot successfully connect to the servers that store the security intelligence.	See Product features and requirements on page 602
The administrator has changed the protection status from the computer local console	The administrator has changed the protection settings from the agent installed on the workstation or server. The current settings do not match the settings defined from the web console.	
Cannot upgrade this computer's protection to the latest version	The new versions of the protection require that the operating system recognize SHA-256 signed drivers. This computer does not support that signature format and therefore the installed protection cannot be upgraded to the latest version	See Support for SHA-256 driver signing on page 611.

Table 8.24: Notifications related to lack of user or administrator action

Computer with out-of-date protection

Notification	Description	Reference
Outdated protection	A reboot is required to complete the protection update process.	For more information, see Computer restart on page 577.
	An error occurred during the update process. Make sure the computer meets the hardware and network requirements.	See Product features and requirements on page 602 and the amount of available disk space in the Hardware section (5).

Notification	Description	Reference
	Updates are disabled for the computer. Assign the computer a settings profile with updates enabled.	See Protection engine updates on page 194.
Malware and threat knowledge out of date	Knowledge updates are disabled for this computer. Assign the computer a settings profile with updates enabled.	See Knowledge updates on page 196.

Table 8.25: Notifications related to out-of-date Panda Endpoint Protection Plus software

Mobile device notifications

Notification	Description	Reference
The iOS device has been jailbroken	The device has been jailbroken and allows the installation of unsigned apps. The device is exposed to confidential data leaks or removal of the security software.	Contact the user.
iOS or Android device with permission problems	The device user has not granted permissions required by Panda Endpoint Protection Plus, affecting its performance.	See Requirements for iOS platforms on page 618 and Requirements for Android platforms on page 617

Table 8.26: Mobile device notifications

Details section (3)

The information on this tab is divided into three sections:

- **Computer**: Information about the device settings. This information is provided by the Panda agent.
- **Security**: The status of the Panda Endpoint Protection Plus protection modules.
- **Data protection** (Windows computers only): The status of the modules that protect the data stored on computers.

Computer

Field	Description
Risk	For Android devices, distribution graph that shows the overall risk level for the device and the risks detected on it. See Risk assessment module lists on page 490.
Name	Computer name.
Description	Descriptive text provided by the administrator.
IP addresses	List of all the IP addresses (primary addresses and aliases).
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.
Physical addresses (MAC)	Physical addresses of the network interface cards installed.
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 that the computer belongs to. To change the computer's group, click **Change**.
Operating system	Operating system installed on the computer.
Virtual machine	Shows whether the computer is physical or virtual.
Is a non-persistent desktop	Shows whether 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. See Licenses on page 177 for more information.
Agent version	Internal version of the Panda agent installed on the computer.

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 proxy used	Access method used by Panda Endpoint Protection Plus the last time it connected to the Panda Security cloud. This data is not updated immediately. It might take up to 1 hour for the correct value to show.
Last connection with the Panda Security infrastructure	Date when the client software last connected to the Panda Security cloud. The communications agent connects at least every four hours.
Last settings check	Date Panda Endpoint Protection Plus last connected to the Panda Security cloud checking for changes to the settings.
Shadow Copies	Shows the feature status: • Enabled • Disabled • Error code
Last copy	Shows the date and time of the last copy made.
Last logged-in user	Names of the user accounts that have an active session on the computer.

Table 8.27: Fields in the Computer section

Security

This section shows the status (Enabled, Disabled, Error) of the Panda Endpoint Protection Plus technologies that protect the computer against malware.

Field	Description
File antivirus	Protection for the file system.
Anti-theft	Actions for mitigating data exposure in the event of theft of a mobile device. This feature is not available for iOS devices not installed with an MDM solution. See Installation on iOS systems on page 142.

Field	Description
Mail antivirus	Protection for the protocols used for sending and receiving email messages.
Web browsing antivirus	Protection against malware downloaded from web pages. This feature is not available for iOS devices not installed with an MDM solution. See Installation on iOS systems on page 142.
Firewall	Protection for the network traffic generated by applications.
Device control	Protection from infections stemming from external storage devices or devices that enable computers to connect to the Internet without passing through the organization's communications infrastructure (modems).
Web access control	Protection that enables you to prevent access to unauthorized web pages. This feature is not available for iOS devices not installed with an MDM solution. See Installation on iOS systems on page 142.
Patch management	Installation of patches and updates for Windows, macOS, and Linux operating systems and third-party applications. Detection of the patch status of the computers on the network and removal of problematic patches.
Patch installation	Indicates whether patch installation is allowed or denied on the computer, or whether the computer is a test computer for patch installation. For more information, see Panda Patch Management features
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.
Protection version	Internal version of the protection module installed on the computer.
Knowledge update date	Date when the signature file was last downloaded to the computer.
Hard disk encryption (Mac computers only)	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.

Field	Description
	• **Disabled**: The computer has a settings profile assigned to decrypt its storage devices and no errors have occurred. • **Error installing**: Error downloading or installing the executables required to manage the encryption service if they were not already installed on the computer. • **No license**: The computer does not have a Panda Endpoint Protection Plus license assigned. **Get recovery key**: Opens a dialog box that shows the ID of the recovery key associated with the computer and the corresponding recovery key. For more information, see Obtaining a recovery key on page 423. Encryption process status: • **Unknown**: There are disks whose status is unknown. • **Unencrypted disks**: For the computer encryption process to start, the user must enter administrator credentials. • **Encrypted disks**: All disks compatible with the encryption technology are encrypted. • **Encrypting**: At least one disk is currently in the encryption process. • **Decrypting**: At least one disk is currently in the decryption process. • **Encrypted by the user**: The user encrypted all of the disks. • **Encrypted by the user (partially)**: The user encrypted some of the disks.
Authentication method (Mac computers)	• **Password:** While booting, the computer requests a PIN or password for authentication.
Connection to knowledge servers	Status of the connection between the computer and the Panda Security servers. In case of errors, links are shown to support pages with information about the requirements that must be met.

Table 8.28: Fields in the Security section

Data protection (Windows)

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

Field	Description
Hard disk encryption	Encryption module status: • **Not available:** The computer is not compatible with Panda Full Encryption. • **No information**: The computer has not yet sent any information about the encryption module. • **Enabled**: The computer has a settings profile assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: The computer has a settings profile assigned to decrypt its storage devices and no errors have occurred. • **Error**: The settings configured by the administrator do not 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 executables required to manage the encryption service if they were not already installed on the computer. • **No license**: The computer does not have a Panda Endpoint Protection Plus license assigned. **Get recovery key**: Opens a dialog box that shows the IDs of the computer encrypted disks. Click an ID to show the relevant recovery key. For more information, see Obtaining a recovery key on page 423.
Encryption process status:	• **Unknown**: There are disks whose status is unknown. • **Unencrypted disks**: Some of the disks compatible with the encryption technology are neither encrypted nor in the process of being encrypted. • **Encrypted disks**: All disks compatible with the encryption technology are encrypted. • **Encrypting**: At least one disk is currently in the encryption process. • **Decrypting**: At least one disk is currently in the decryption process. • **Encrypted by the user**: The user encrypted all of the disks. • **Encrypted by the user (partially)**: The user encrypted some of the disks.
Authentication method	• **Unknown**: The authentication method is not compatible with those supported by Panda Patch Management. • **Security processor (TPM).** • **Security processor (TPM) + Password**

Field	Description
	• **Password**: Authentication method based on a PIN, extended PIN, or passphrase. • **USB drive**: Authentication method based on a USB drive. • **None**: None of the drives compatible with the encryption technology is encrypted or in the process of being encrypted.
Encryption date	Date when the computer was fully encrypted for the first time.
Removable storage drive encryption	Encryption module status: • **Not available:** The computer is not compatible with Panda Full Encryption. • **No information**: The computer has not yet sent any information about the encryption module. • **Enabled**: The computer has 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 do not 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 executables required to manage the encryption service if they were not already installed on the computer. • **No license**: The computer does not have a Panda Endpoint Protection Plus license assigned. **View encrypted devices on this computer:** Opens a dialog box that shows the IDs of the computer encrypted external storage media. Click an ID to show the relevant recovery key. For more information, see Obtaining a recovery key on page 423.

Table 8.29: Fields in the Data Protection section

Detections section (4) for Windows, Linux, and macOS computers

Shows counters associated with the computer's security and patch level through the following widgets:

Panel	Description
Threats detected by the antivirus	See Threats detected by the antivirus on page 451.
Available patches	See Available patches on page 361.
Available patches trend	See Available patches trend on page 358.
End-of-Life programs	See End-of-Life programs on page 357.

Table 8.30: List of widgets available in the Detections section

Detections section (4) for Android and iOS devices

Shows counters associated with the device's security through the following widgets:

Panel	Description
Threats detected by the antivirus	See Threats detected by the antivirus on page 451.

Table 8.31: List of widgets available in the Detections section

Hardware section (5)

This tab shows information about the hardware resources installed on the computer:

Field	Description	Values
CPU	Information about the computer microprocessor, along with a line chart that shows CPU usage 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 that shows memory usage 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

Field	Description	Values
		last 24 hours.
Disk	Information about the mass storage system, along with a pie chart that shows the current percentage of free/used space.	• Device ID • Size • Type • Partitions • Firmware revision • Serial number • Name
BIOS	Information about the BIOS installed on the computer.	• Version • Manufacture date • Serial number • Name • Manufacturer

Field	Description	Values
TPM	Information about the security chip located on the computer motherboard. For Panda Endpoint Protection Plus to use the TPM chip, it must be enabled, activated, and owned.	• **Manufacturer version**: Internal version of the chip. • **Spec version**: Supported API versions. • Version • Manufacturer • **Activated**: The TPM chip is ready to receive commands. This is used on systems with multiple TPM chips. • **Enabled**: The TPM chip is ready to work as it has been enabled in the BIOS. • **Owned**: The operating system can interact with the TPM chip.

Table 8.32: Fields in the Hardware section of a computer details

Software section (6)

This tab provides information about the software packages installed on the computer, the Windows operating system updates, and a history of all software installations and uninstallations.

Filter tool

To perform a search, type a software package name or publisher in the **Search** text box. Press **Enter**. This information appears for each program found:

Field	Description
Name	Name of the installed program.
Publisher	Company that developed the program.
Installation date	Date when the program was last installed. With iOS devices enrolled in an MDM solution, this field indicates the date when apps were first seen on the device. See Deploying and installing the iOS agent on

Field	Description
	page 145. This information is not available for iOS devices not enrolled in an MDM solution. Devices enrolled in the Panda MDM solution send the server a daily report that includes the third-party apps they have installed.
Size	Program size.
Version	Internal version of the program.

Table 8.33: Fields in the Software section of a computer details

- 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

- To show a history of all software changes made to the computer, click the **Installations and uninstallations** link:

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 8.34: Fields in the Installations and Uninstallations section

Settings section (7)

This tab shows the various settings profiles assigned to the computer and enables you to edit and manage them:

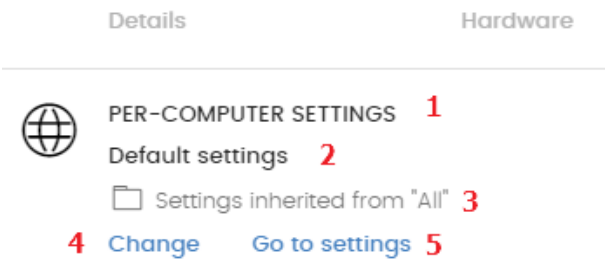


Figure 8.9: Example of inherited and manually assigned settings profiles

- **(1) Settings type**: Indicates the type of settings profile assigned to the computer. For more information about the types of settings available in Panda Endpoint Protection Plus, see Introduction to the various types of settings profiles on page 263.
- **(2) Settings profile name.**
- **(3) Method used to assign the settings profile**: 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**.

> *For more information about how to create and edit settings profiles, see Creating and managing settings profiles on page 267.*

Action bar (8)

This resource groups together multiple actions you can take 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 Plus license and removes the computer from the web console.

Action	Description
Scan now	Enables you to run a scan task immediately. For more information, see On-demand computer scanning and disinfection on page 568.
Schedule scan	Enables you to schedule a scan task. For more information, see On-demand computer scanning and disinfection on page 568.
View available patches	Opens the **Available patches** list which shows patches that are pending installation on the computer. See Panda Patch Management module lists on page 370.
Schedule patch installation	Creates a task that installs all released patches missing from target computers. For more information, see Download and install patches on page 337.
Restart	Restarts the computer immediately. For more information, see Computer restart on page 577.
Reinstall protection (requires restart)	Reinstalls the security software if a malfunction occurs. See Remote reinstallation on page 173.
Reinstall agent	Reinstalls the agent if a malfunction occurs. See Remote reinstallation on page 173.
Report a problem	Creates a support ticket for the Panda Security support department. For more information, see Reporting a problem on page 577.

Table 8.35: Actions available from a computer details page

Hidden icons (9)

Depending on the size of the screen and the number of icons to show, some icons might be hidden under the ... icon. Click it to show the remaining icons.

Chapter 9

Managing settings

Settings, also called “settings profiles” or simply “profiles”, offer administrators a simple way of establishing security, productivity, and connectivity parameters for the computers managed through Panda Endpoint Protection Plus.

Chapter contents

Strategies for creating settings profiles

Administrators can create as many settings profiles with different settings as necessary to manage network security for different types of computers and devices. We recommend that you create separate settings profiles for groups 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 who 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 profiles to computers

In general, assigning settings profiles 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 groups.
3. Assigning settings profiles to groups.
4. Deployment of settings profiles to network computers.

All these operations are performed from the group tree, which is accessed from the **Computers** menu at the top of the console. The group tree is the main tool for assigning settings profiles quickly and to large groups of computers.

Therefore, administrators must 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 about the group tree and how to assign computers to groups, see The Computer tree panel on page 201.

Immediate deployment of settings profiles

After a settings profile is assigned to a group, it is applied to the computers in the group immediately and automatically, in accordance with the inheritance rules described in section Indirect assignment of settings profiles: the two rules of inheritance. These settings are applied to computers in just a few seconds.

For more information about how to disable the immediate deployment of settings profiles, see *Configuring real-time communication on page 288*.

Multi-level tree

In medium-sized and large organizations, there can be a wide range of settings profiles. To make it easier to manage large networks, Panda Endpoint Protection Plus enables you to create multi-level group trees so that you can manage all computers on the network with sufficient flexibility.

Inheritance

In large networks, it is highly likely that the administrator wants to reuse existing settings profiles already assigned to groups higher up in the group tree. The inheritance feature enables you to assign a settings profile to a group, applying it automatically to all groups below it in order to save time.

Manual settings

To prevent settings profiles from being applied to all lower levels in the group tree, or to assign settings profiles different from the inherited ones to a certain computer on a branch of the tree, you can manually assign settings profiles to groups or individual computers.

Default settings

Initially, all computers in the group tree inherit the settings profile established for the **All** root node. This node comes with a series of default settings created in Panda Endpoint Protection Plus with the purpose of protecting all computers from the outset, even before the administrator accesses the console to configure a security settings profile.

Introduction to the various types of settings profiles

A security settings profile is a group of settings for a specific security area that you use to configure the endpoint security product and specify how it operates on your network computers and devices. You assign profiles to one or more groups and all computers and devices in the groups receive the settings in the profile.

This is an introduction to the different types of settings profiles supported by Panda Endpoint Protection Plus.

Panda Endpoint Protection Plus enables you to configure these aspects of the service:

Settings	Description
Users	Manage the user accounts that can access the management console, the actions they can take (roles), and their activity. For more information, see Accessing, controlling, and monitoring the management console on page 53.

Settings	Description
Per-computer settings	Specify how often to install Panda Endpoint Protection Plus updates on workstations and servers. You can also define settings to prevent tampering and unauthorized uninstallation of the protection software. For more information, see Configuring the agent remotely on page 279.
Network settings	Specify the language of Panda Endpoint Protection Plus installed on workstations and servers. You can also define the type of connection to the Panda Security cloud. For more information, see Configuring the agent remotely on page 279 .
Network services	Specify how Panda Endpoint Protection Plus communicates with computers on the network: • **Proxy**: Define computers that act as a proxy to enable isolated computers with Panda Endpoint Protection Plus installed to access the cloud. For more information, see Panda proxy role on page 280. • **Cache**: Define computers that act as a cache for signature files, security patches, and other components used to update the Panda Endpoint Protection Plus software installed on other computers and devices on the network. For more information, see Cache role on page 282. • **Discovery**: Define computers that discover unprotected computers on the network. For more information, see Discovery computer role on page 284.
VDI environments	Define the maximum number of computers that can be simultaneously active in a non-persistent virtualization environment.
My alerts	Configure alerts to send to the network administrator by email. For more information, see Alerts on page 547.
Workstations and servers	Define how Panda Endpoint Protection Plus protects the computers on your network against threats and malware. For more information, see Security settings for workstations and servers on page 299.
Mobile devices	Protect tablets and smartphones against threats, malware, and theft. For more information, see Security settings for mobile devices on page 323.
Patch management	Specify when the protection software searches for new patches and software updates for the Windows operating systems and third-party applications installed across the network. For more information, see Panda Patch Management

Settings	Description
	(Updating vulnerable programs) on page 331.
Endpoint Access Enforcement	
Encryption	Encrypt the content of your computer internal and external storage devices. For more information, see Panda Full Encryption (Device encryption) on page 411.

Table 9.1: Description of the types of settings profiles available in Panda Endpoint Protection Plus

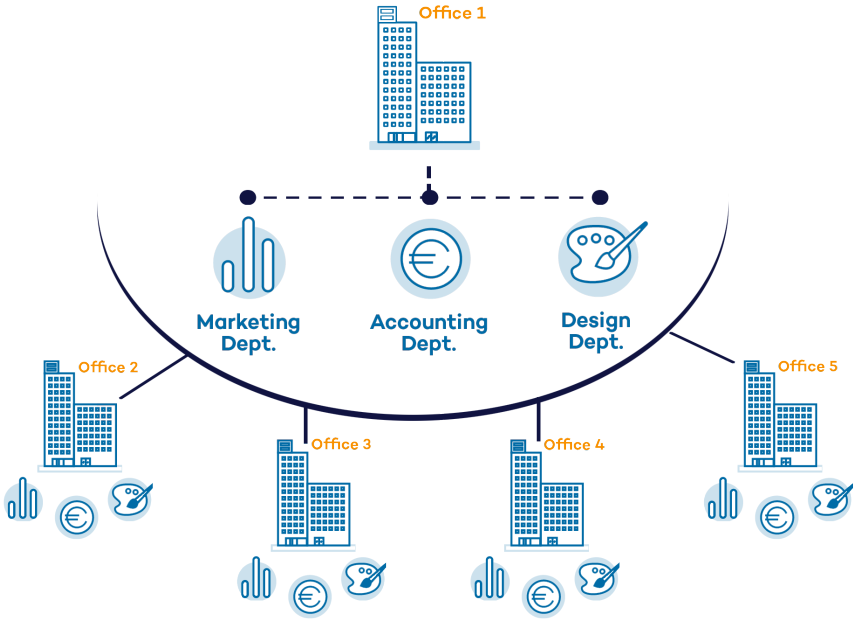
Modular vs. monolithic settings profiles

By supporting different types of profiles, Panda Endpoint Protection Plus uses a modular approach to creating and deploying the settings you want 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 reduces the time that administrators have to spend managing the profiles created. Modular profiles are lighter than monolithic profiles, which would result in numerous large and redundant settings profiles with little differences between each other.

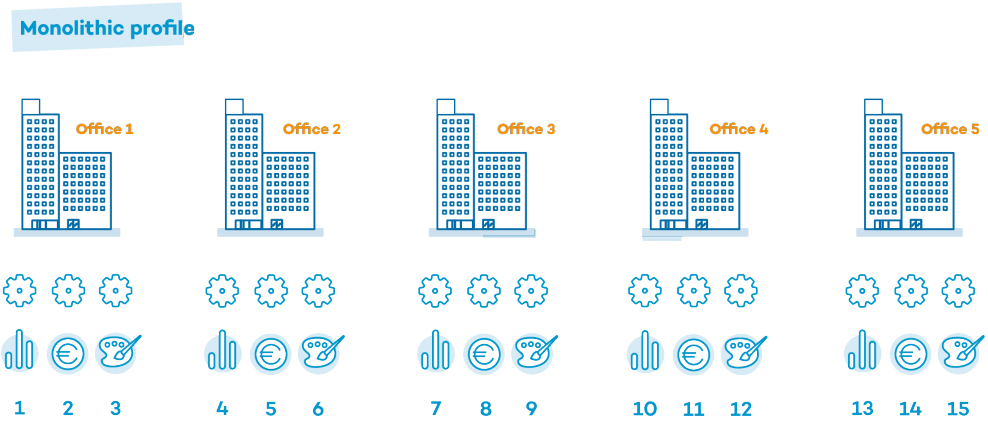
Case study: Creating settings profiles for multiple offices

This example uses a company with five offices, each with a different communications infrastructure and therefore different proxy settings. Also, each office requires three different security settings profiles: one for the Design department, one for the Accounting department, and one for Marketing.

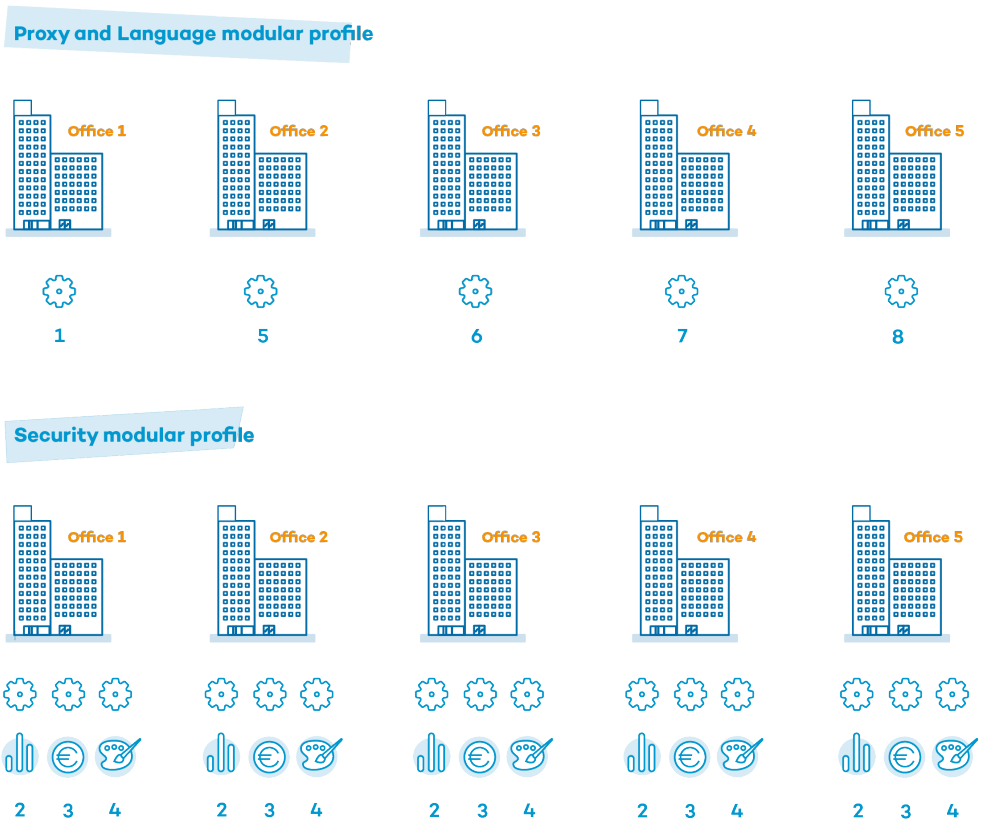
Network of a company with several offices



Using monolithic profiles, the company would require 15 different settings profiles (5 offices x 3 security settings profiles in each office = 15) to adapt to the needs of all three departments in the company offices.



However, because Panda Endpoint Protection Plus 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 profiles

From the top menu, select **Settings** to create, copy, and delete settings profiles.

The left pane shows the available types of security settings **(1)**. The right pane shows the settings profiles already created for the selected type **(2)**, and buttons to add **(3)**, copy **(4)**, and delete profiles **(5)**. To search for a settings profile, type the name in the **Search** box **(6)**.

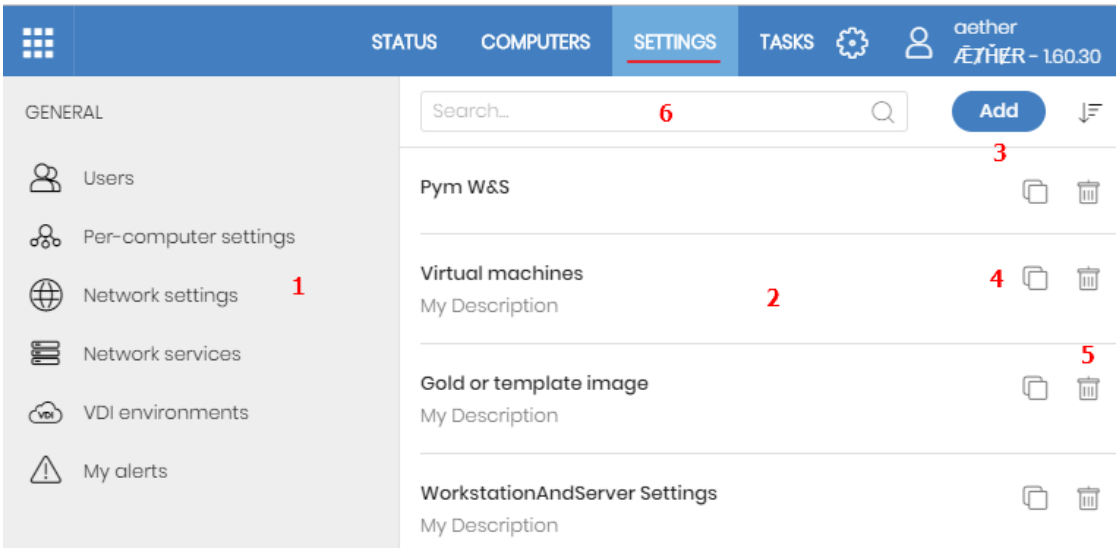


Figure 9.1: Page for creating and managing settings profiles

Settings profiles created from Panda Partner Center and inherited from a service provider account display with a green Panda Partner Center. When you point the mouse to the label, this message appears: "These settings are managed from Panda Partner Center". Settings profiles created from Panda Partner Center are read only. You can edit only their recipients. For more information, see section Settings management for Panda-based products in the CYTOMIC Nexus Administration Guide.

Creating a settings profile

Click **Add**. The **Add Settings** page opens. All profiles have a name and a description, which appear in the list of settings profiles.

To create a settings profile, bear in mind these limitations regarding permissions and visibility:

- To create a settings profile, the user account must have the relevant permission assigned. See Understanding permissions on page 67.
- To assign recipients to a settings profile, the user account must have visibility of the computers to assign. See Managing roles and permissions on page 65

Listing and sorting settings profiles

To see settings profiles of a specific type, the user account must have at least read permissions. See Understanding permissions on page 67.

Click the  icon **(7)** to expand a context menu with these sort options:

- Sorted by creation date
- Sorted by name
- Ascending
- Descending

Copying a settings profile

To copy a settings profile, click the **(4)** icon. All settings are copied, except for the content of the **Recipients** field, which is empty.

To copy a settings profile, the user account must have the relevant edit permission assigned. See Understanding permissions on page 67.

Editing a settings profile

> *When you edit an existing settings profile, your endpoint security product automatically applies your changes to computers on the network that use that settings profile.*

- To edit a settings profile, select it. The **Edit settings** page opens.
- To save your changes, click **Save**.

To edit a settings profile, bear in mind these limitations regarding permissions and visibility:

- The user account must have the relevant edit permission assigned. See Understanding permissions on page 67.
- To add recipients to a settings profile, the user account must have visibility of the relevant computers. See Managing roles and permissions on page 65
- To remove recipients, the user account must have visibility of the relevant computers. See Managing roles and permissions on page 65

Deleting a settings profile

To delete a settings profile, click the **(5)** icon. You cannot delete a settings profile that is assigned to a device or computer.

To delete a settings profile, the user account must have the relevant permission assigned. See Understanding permissions on page 67.

Manual and automatic assignment of settings profiles

After you create a settings profile, you can assign it to one or more computers in two different ways:

- Manually (directly).
- Automatically (indirectly) through inheritance from a group to subgroups, computers, and devices.

Both strategies 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 to minimize the workload of daily maintenance tasks.

Manual/direct assignment of settings profiles

Consists of directly assigning settings profiles to computers or groups. It is the administrator who manually assigns a profile to a computer or computer group.

After you create a settings profile, there are many ways to manually assign it:

- From the **Computers** menu at the top of the console, from the group tree in the left panel.
- From the target computer's details, accessible from the **Computers** list.
- From the profile when it is created or edited.

For more information about the group tree, see Group tree on page 209.

From the group tree

To assign a settings profile to a computer group:

- Click the **Computers** menu at the top of the console. From the left panel, select a filter or group.
- Click the group's context menu.
- Click **Settings**. A window opens with the profiles already assigned to the selected group and the type of assignment:
- **Manual/Direct assignment**: The text **Directly assigned to this group** is displayed.
- **Inherited/Indirect assignment**: The text **Settings inherited from** is displayed, followed by the name and full path of the group the settings profile is inherited from.

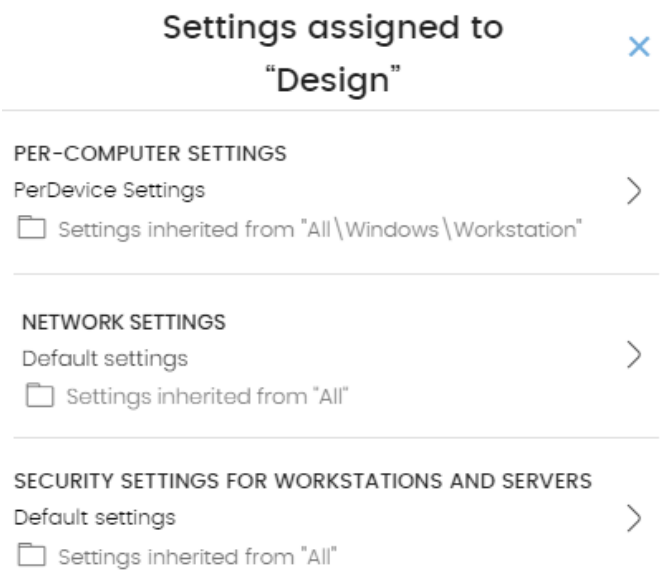


Figure 9.2: Example of inherited and manually assigned settings profiles

Select one of the available types of settings profiles. Select the specific settings profile to apply. Click **OK**. The profile is immediately deployed to all members of the group and its subgroups.

From the Computers list panel

To assign a settings profile to a specific computer or device:

- Go to the **Computers** menu at the top of the console. From the left panel, select the filter or group that contains the computer you want to assign the settings to. From the list of computers, select the computer. The computer details page opens.
- Select the **Settings** tab. A window opens with the profiles already assigned to the selected computer and the type of assignment:
    - **Manual/Direct assignment**: The text **Directly assigned to this group** is displayed.
    - **Inherited/Indirect assignment**: The text **Settings inherited from** is displayed, followed by the name and full path of the group the settings profile is inherited from.
- Select one of the available types of settings profiles. Select the specific settings profile to apply. Click **OK**. The profile is immediately applied to the computer.

From the settings profile

The fastest way to assign a settings profile to several computers belonging to different groups is from the settings profile itself.

To assign a settings profile to multiple computers or computer groups:

- Go to the **Settings** menu at the top of the console. From the left panel, select the type of settings you want to assign.
- Select a settings profile from the list. Click **Recipients**. The **Recipients** page opens. This page is 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 is assigned to the selected computers and the settings are applied immediately.

If you remove a computer from the list of computers assigned to a settings profile, it re-inherits the security settings profile from the group it belongs to. A warning message is displayed in the management console before the computer is removed and the changes are applied.

Indirect assignment of settings profiles: the two rules of inheritance

Indirect assignment of settings profiles takes place through inheritance, which enables automatic deployment of a settings profile to all computers below the node to which the settings were initially assigned.

The following is a description of the rules that govern the interaction between the two ways of assigning profiles (manual/direct and automatic/inheritance):

Automatic inheritance rule

A computer or computer group automatically inherits the settings of its parent group (the group above it in the hierarchy).

The settings are manually assigned to the parent group and automatically deployed to all child nodes (computers and computer groups with computers inside).

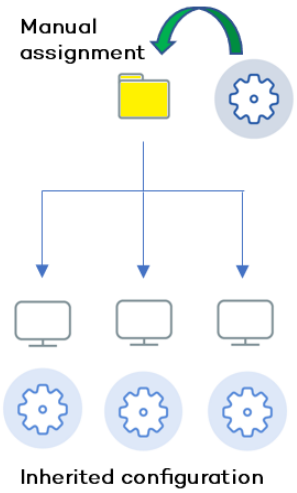


Figure 9.3: Inheritance/indirect assignment

Manual priority rule

Manually assigned settings take precedence over inherited settings.

When you manually assign a new settings profile to a group, all computers and devices below that group use the manually assigned settings, not the inherited or default ones.

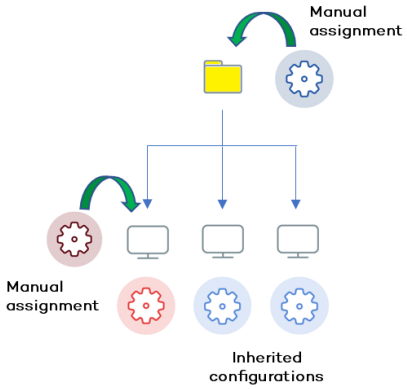


Figure 9.4: Precedence of manually assigned settings over inherited settings

Inheritance limits

Manually assigned settings override inherited settings from the higher-level group. That is, settings assigned to a group (manual or inherited) apply to all subgroups, computers, and devices unless manually assigned

settings apply.

When the solution encounters manually assigned settings, that group and all of its subgroups, computers, and devices receive the manually assigned settings and not the original inherited ones.

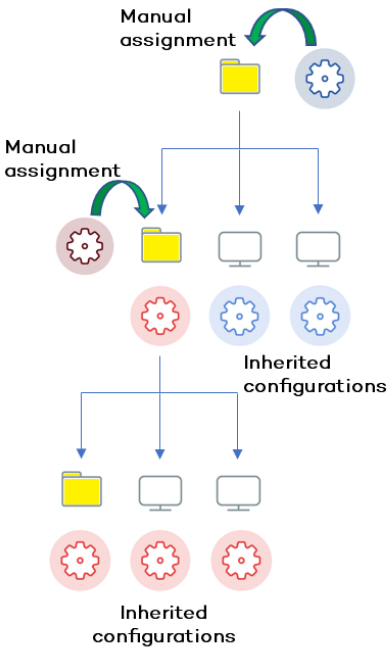


Figure 9.5: Inheritance limits

Overwriting settings

Manually assigned settings take precedence over inherited settings. When you manually assign a new settings profile to a group, all computers and devices below that group use the manually assigned settings, not the inherited or default ones.

Bearing that in mind, changes you make to settings in a higher-level group affect the groups, computers, and devices that inherit the settings differently, based on whether they have existing manually assigned or inherited settings. There are two scenarios:

- **Subgroups and computers with no manually assigned settings**: When you change settings in a group that are inherited by subgroups and computers that have no manual settings applied, the new settings automatically apply to all subgroups, computers, and devices in the group.
- **Subgroups and computers with manually assigned settings**: When you change settings in a group that are inherited by subgroups and computers that have manually assigned settings applied, any subgroups or computers with manually assigned settings do not inherit the new settings, regardless of the level.

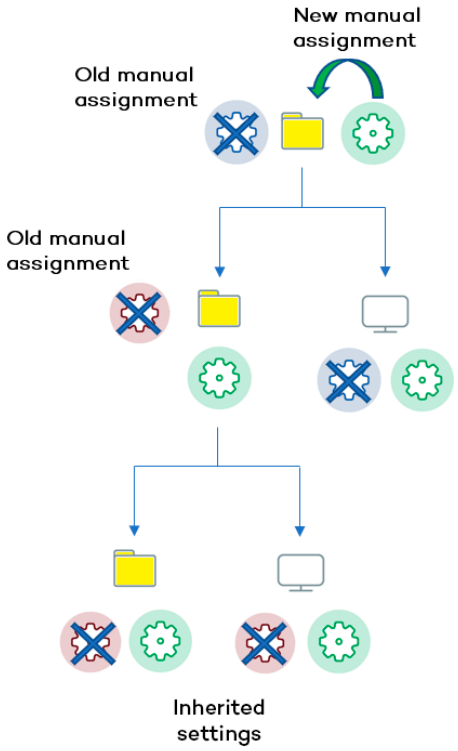


Figure 9.6: Overwriting manual settings

The solution prompts you to specify whether to **inherit the settings** or **keep the manually assigned settings**.

Make all inherit these settings

> *Be careful when you choose this option as this action is irreversible! When you select this option, all manually assigned settings below the parent node are removed and all groups and computers inherit the new settings. The wayPanda Endpoint Protection Plus behaves might change on many computers on the network.*

The new directly assigned settings propagate through inheritance across the entire tree, overwriting the previously assigned settings up to the last-level child nodes.

Keep all settings

When you select this option, new settings apply only to groups and computers that do not have manually assigned settings.

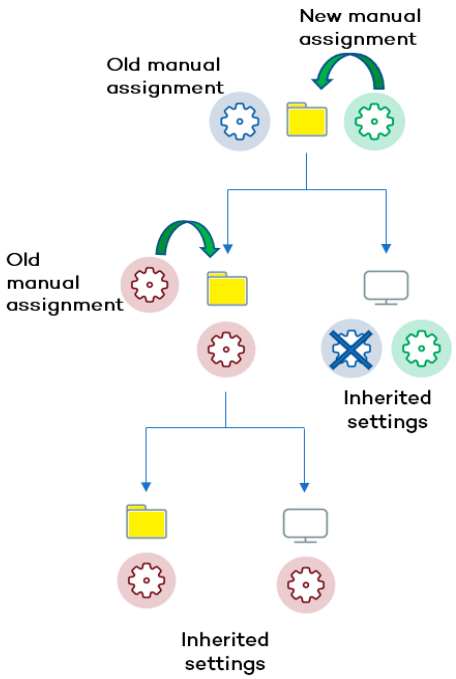


Figure 9.7: Keeping manual settings

Existing manual settings are retained and the application of new inherited settings stops at the first group or computer with manually configured settings.

Deleting manually assigned settings and restoring inheritance

To restore inheritance to a group or computer with manually assigned settings, you must delete the manually assigned settings:

- Go to the **Computers** menu at the top of the console. From the left panel, click the group with manually assigned settings that you want to delete.
- Click the branch's context menu icon and select **Settings**. A pop-up window opens with the profiles assigned to the group. Select the manually assigned profile you want to delete.
- A list is shown with all available settings profiles and the **Inherit from parent group** button. Click **Inherit from parent group**. The manually assigned settings are removed. The group inherits profile settings from the specified group.

Moving groups and computers

When you move computers from one branch in the tree to another, the way Panda Endpoint Protection Plus operates with respect to the settings profile to apply varies depending on whether the items moved are groups or individual computers.

Moving individual computers

All settings profiles that were manually assigned to the computer are kept. Inherited profiles are overwritten with the settings established in the new parent group.

Moving groups

A dialog box appears with the following question: "**Do you want the settings inherited by this group to be replaced by those in the new parent group?**"

- If the answer is **YES**, the process is the same as when you move a single computer: The manual settings are kept and the inherited settings are overwritten with those established in the parent node.
- If the answer is **NO**, both the manual settings and the original inherited settings of the group are kept.

Exceptions to indirect inheritance

All computers that are integrated into a native group in the web console automatically receive, from Panda Endpoint Protection Plus, the network settings assigned to the target group by means of the standard indirect assignment/inheritance mechanism. However, if a computer is a member of an Active Directory or IP-based group, you must manually assign network settings. This change in the way network settings are assigned results in a change in behavior if that computer is moved from an Active Directory or IP-based group to another group: It does not automatically inherit the network settings assigned to the target group, but retains its own.

This particular behavior of the inheritance feature is due to the fact that, in midsize and large companies, the department that manages security might not be the same as the one that manages the company's Active Directory. Therefore, a group membership change made by the technical department that maintains the Active Directory could inadvertently change network settings in the Panda Endpoint Protection Plus console and leave the protection agent installed on the affected computer without connectivity and full protection. To prevent settings changes when a computer changes groups in the Panda Endpoint Protection Plus console because of a group change in Active Directory, you must manually assign network settings.

Settings profiles inherited from a partner

Partners are companies or organizations that deliver and manage security solutions remotely for their customers.

There are two types of partners:

- Resellers who assign products to their customers and manage them remotely.
- Companies that delegate security service management to each department, but also want to centrally oversee compliance of the protection policies that are common to the entire company.

To manage the protection software remotely, partners send settings profiles to their customers. These profiles appear in the management console with the Panda Partner Center label.

Features of the settings profiles inherited from a partner

By default, you cannot edit or delete the settings profiles you inherit from a partner in the management console. Only if the partner marks them as editable can you modify certain aspects of their configuration. For

more information, see Exclusions set by a partner on page 302 and Software authorized by a partner.

Requirements

To receive settings profiles from a partner, follow these steps:

- From the top menu, select **Settings (1)**. From the left panel, select **Users (2).**
- Select the **Users** tab. Select **Allow my reseller to access my console (3)**.

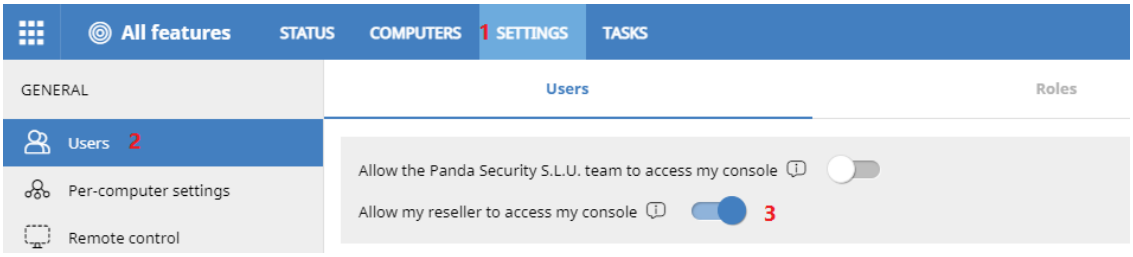


Figure 9.8: Option **Allow my reseller to access my console**

Viewing assigned settings profiles

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 a computer's **Settings** tab.
- From the exported list of computers.

Viewing settings profiles from the group tree

- Click the **Computers** menu at the top of the console. Click the tab from the left panel to show the group tree.
- Click the context menu of the relevant branch. Select **Settings** from the pop-up menu displayed. A window opens with the settings profiles assigned to the folder.

The following is a description of the information displayed in the window:

- **Settings type**: Indicates the settings class the profile belongs to.
- **Name of the settings profile**: Name given by the administrator when configuring the profile.
- **Inheritance type**:

- **Settings inherited from...:**  The settings profile was assigned to a higher-level folder and every computer on the current branch has inherited it.
- **Directly assigned to this group**: → The settings profile applied to the computers was manually assigned to the folder by the administrator.

Viewing settings profiles from the Settings menu at the top of the console

Go to the **Settings** menu at the top of the console. Select a type of settings from the left menu.

Select a settings profile from the list.

If the settings profile is assigned to one or more computers or groups, the **View computers** button is displayed.

Click the **View computers** button. The **Computers** page opens, with a list of all computers with the settings profile assigned, regardless of whether it was assigned individually or through computer groups. At the top of the page you can see the filter criteria used to generate the list.

Viewing settings profiles from a computer's Settings tab

Go to the **Computers** menu at the top of the console. Select a computer from the right panel. Click it to view its details. Go to the **Settings** tab to see the profiles assigned to the computer.

Viewing settings profiles from the exported list of computers

From the computer tree (group tree or filter tree), click the general context menu and select **Export**.

See Fields displayed in the exported file on page 218 for more information.

Chapter 10

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 a computer's role towards the other protected workstations and servers.
- Protect the Panda Endpoint Protection Plus client software from unauthorized tampering by hackers and advanced threats (APTs).
- Define the visibility of the agent on the workstation or server, and the language it is displayed in.
- Configure the communications established between the computers on the network and the Panda Security cloud.
- Apply an additional layer of protection for VPN connections between remote computers and corporate networks.

Chapter contents

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, select **Settings** from the top menu. Select **Network services** from the side menu. Four tabs appear: **Panda Endpoint Protection Plus proxy**, **Cache**, **Discovery**, and **Network Access Enforcement**.

Only computers that use the Windows operating system can take on the Proxy, Cache, or Discovery Computer roles.

Panda proxy role

To access the Panda cloud, the security software installed on computers requires access to the Internet. Isolated computers can access the Internet through the organization corporate proxy. If there is no corporate proxy, Panda Endpoint Protection Plus enables you to add or designate more than one computer on the network as a Panda proxy.

Computers designated as a Panda proxy can listen to requests from other computers and redirect them to the Panda cloud using a valid connection.

We recommend that you configure a Panda proxy only to enable isolated computers (those without an Internet connection, either direct or through a corporate proxy) to access the Panda cloud. A Panda proxy does not provide all the features of a corporate proxy and is designed only to access resources hosted in the Panda cloud.

Panda proxy computers can serve a variable number of devices, depending on the hardware resources installed. As a general rule, a proxy computer can serve a maximum of 100 computers.

Limitations of Panda proxy computers

For security reasons, when Panda Endpoint Protection Plus has the Panda proxy role assigned, it can connect only to the Panda cloud. For this reason, there are certain limitations with regard to the items the security software can download when it is configured to access the Internet through a Panda proxy node:

- **Windows and macOS**:
  - The security software cannot download patches through Panda Patch Management, but can report patches that are pending installation. See Download and install patches on page 337.
- **Linux**:
  - The security software cannot download patches through Panda Patch Management, but can report patches that are pending installation. See Download and install patches on page 337.
  - If the security software needs to download packages from repositories that are not accessible to the Panda proxy, installation is not possible. See Protection engine updates on page 194.

These limitations do not apply to the company corporate proxy.

Requirements for designating a computer as a Panda proxy

- Windows operating system and Panda Endpoint Protection Plus product installed.
- Support for the 8.3 filename format. For more information on file name requirements, see this MSDN article: https://docs.microsoft.com/en- us/previous- versions/windows/it- pro/windows- server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN.
- TCP port 3128 must not be in use by other applications.
- Port 3128 must be open for inbound and outbound connections.
- The proxy computer name must be resolved from the computer that uses it.

Designating a computer as a Panda proxy

- From the top menu, select **Settings**. From the side menu, select **Network services**. Select the **Proxy** tab. A list appears and shows all computers that have been designated as a proxy.
- Click **Add proxy server**. A dialog box opens and shows all computers managed by Panda Endpoint Protection Plus that meet the requirements for acting as a proxy on the network.
- Use the search box to find a specific computer and click it to add it to the list of computers designated as a proxy.

Removing a Panda proxy

- From the top menu, select **Settings**. From the side menu, select **Network services**. Select the **Proxy** tab. A list appears and shows all computers that have been designated as a proxy.
- Next to the computer you want to remove from the list, click  .

> *For information about how to configure the use of a proxy computer, see Configuring proxies lists for Internet access.*

Cache role

Panda Endpoint Protection Plus enables you to assign the cache role to one or more computers on your network. These computers automatically download and store all files required by other computers with Panda Endpoint Protection Plus installed. This saves bandwidth because not every computer has to separately download the updates they need. All updates are downloaded centrally and only once for all computers that require them.

Limitations of cache computers

For security reasons, when Panda Endpoint Protection Plus has the cache role assigned, it can connect only to the Panda cloud. For this reason, there are certain limitations with regard to the items the security software can download when downloads are configured to occur through a cache node:

- Linux computers cannot download update patches through Panda Patch Management. See Download and install patches on page 337.
- Linux computers cannot download packages to install or update the security software. See Protection engine updates on page 194.

Cached items

A computer designated with the cache role can cache these items:

- **Signature files**: Cached until they are no longer valid.
- **Installation packages**: Cached until they are no longer valid.
- **Update patches for** Panda Patch Management: Cached for 30 days.

Cache computer capacity

The capacity of a cache computer depends on the number of simultaneous connections it can accommodate and the type of traffic it manages (such as signature file downloads or installer downloads). A cache computer can serve approximately 1,000 computers simultaneously.

Designating a computer as a cache computer

- Go to the **Settings** menu at the top of the console. Select **Network services** from the menu on the left. Select the **Cache** tab.
- Click **Add cache computer**.
- Use the search tool at the top of the window to quickly find those computers you want to designate as cache computers.
- Select a computer from the list and click **OK**.

The selected computer then has the role of cache, and downloads all files required to keep its repository automatically synchronized. All other computers on the same subnet contact the cache computer to download updates.

Removing the cache role from a computer

Go to the **Settings** menu at the top of the console. Select **Network services** from the menu on the left. Select the **Cache** tab.

Click next to the computer you want to remove from the list.

Specifying the storage drive

You can configure the Panda Endpoint Protection Plus agent to store cached items on a specific drive of the cache computer. To specify the cache drive:

- Go to the **Settings** menu at the top of the console. Select **Network services** from the menu on the left. Select the **Cache** tab.
- Select a computer from the list of cache computers. Click the **Change** link. A dialog box opens and shows the available drives.
- The following information is shown for each drive: volume name, mapped drive, free space, and total space.

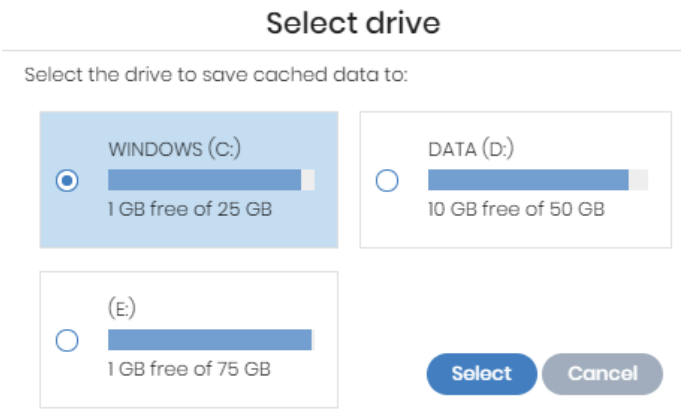


Figure 10.1: Volume selection window for a cache computer

- To view the space on a drive, point the mouse at the relevant bar. A tooltip shows the percentage of used and free space.
- Only drives with 1 GB or more of free space are available to store cached items. Select the drive where you want to store the cached items and click the **Select** button. Panda Endpoint Protection Plus starts to copy the cached items. When the process is complete, the items are deleted from their original location.

*You can only select a drive on a computer which has reported its status to the Panda Endpoint Protection Plus server. If the drive has not reported its status, the drive that stores the Panda Endpoint Protection Plus installation files is selected by default. After the status has been reported, the **Change** link for the cache computer is shown, and you can select the storage drive. It might take several minutes for a computer to report its status.*

If there is not enough free space or a write error occurs when you select the drive, an error message appears below the cache computer and indicates the cause of the problem.

Discovery computer role

Click the **Settings** menu at the top of the console and select **Network services** from the menu on the left. You will find the **Discovery** tab, which is directly related to the installation and deployment of Panda Endpoint Protection Plus across a customer's network.

See Viewing discovered computers on page 114 for more information about the Panda Endpoint Protection Plus discovery and installation processes.

Configuring proxies lists for Internet access

Panda Endpoint Protection Plus enables you to assign computers on the network one or more Internet connection methods, based on the resources available in the company's IT infrastructure.

There are two lists of connection methods:

- **Access list**: Contains the connection methods you configure.
- **Fallback list**: This is a non-editable list included by default in Panda Endpoint Protection Plus.

If a connection method appears in both lists, it is automatically removed from the fallback list.

Access list

This list contains the access methods you configure. The agent traverses the list from the start when it needs to connect to the Panda Security cloud. After it finds an access method that works, the agent continues to use it until it fails, at which point Panda Endpoint Protection Plus traverses the list from the start again until it finds one that works. If the solution reaches the end of the list without finding an access method that works, it searches for one in the fallback list. See Fallback list.

The connection types supported in the access list are:

Proxy type	Description
Do not use proxy	Direct access to the Internet. Computers access the Panda Security cloud directly to download updates and report their status. If you select this option, the Panda Endpoint Protection Plus software communicates with the Internet using the computer settings.
Corporate proxy	Access to the Internet through a proxy installed on the company's network. • **Address**: The proxy server IP address. • **Port**: The proxy server 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 proxy account password.
Automatic proxy discovery using the Web Proxy Auto-Discovery Protocol (WPAD)	Queries the network using DNS or DHCP to get the discovery URL that points to the PAC configuration file. Alternatively, you can directly specify the HTTP or HTTPS resource that hosts the PAC configuration file. This option is not supported on Linux. It is ignored. We recommend that you do not use it for that operating system.
Panda Endpoint Protection Plus proxy	Access to the Panda Security cloud through a computer on the network with the Panda proxy role assigned. An access list can contain multiple Panda proxies. For more information about the access limitations of a Panda proxy and how to assign that role to a computer on the network, see Panda proxy role.

Table 10.1: Types of Internet access methods supported by Panda Endpoint Protection Plus

Configuring an access list

To configure an access list, create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Click the **Add** button or select an existing settings profile to edit it.
- In the **Proxy** section, click the icon. A window opens with a list of all available connection types.
- Select one of the connection types (Types of Internet access methods supported by Panda Endpoint Protection Plus) and click the **OK** button. The connection type is added to the list.
- To modify the order of the connection methods, select an item by clicking its checkbox and use the and arrows to move it up and down in the list.
- To delete a connection method, click the icon.
- To modify a connection method, select it by clicking its checkbox and click the icon. A window opens, where you can edit the method settings.

Fallback list

When the agent cannot connect to the Aether platform despite having tried all the connection methods in the access list you configured, it traverses the fallback list from the start. This list cannot be edited by you. After the Panda agent finds a connection method that works, it continues to use it until it fails, at which point the agent traverses the access list you configured from the start until it finds one that works. If none of the access methods in the access list or the fallback list works, the agent returns a communication error.

The fallback list is fixed and contains these access methods (not all access methods are available for all platforms):

- **Internet Explorer**: Panda Endpoint Protection Plus tries to retrieve the Internet Explorer proxy settings by impersonating the user account that logged in to the computer. This method is only available for Windows operating systems.
    - This method cannot be used if the proxy credentials have been explicitly defined.
    - If the Internet Explorer proxy settings have been configured using a proxy auto-config (PAC) file, the solution will obtain the URL of the configuration file only if the protocol for accessing the resource is HTTP or HTTPS.
- **Default proxy**: Panda Endpoint Protection Plus reads the operating system's default proxy settings.
- **WPAD**: Panda Endpoint Protection Plus uses DNS or DHCP to query the network and get the discovery URL that points to the proxy auto-configuration (PAC) file. This option is not supported on Linux.
- **Direct connection**: Panda Endpoint Protection Plus tries to connect directly to the Panda Security cloud.

Configuring downloads from cache computers

There are two ways to use computers with the cache role:

- **Automatic mode**: In this mode, a computer that starts a download uses cache computers found on the network that meet the requirements specified in section Requirements for using a computer with the cache role assigned. If multiple cache computers are found, the solution automatically balances the downloads so that a single cache computer is not overloaded.
- **Manual mode**: In this mode, you select the cache computers that download data from the Panda Security cloud. You order these computers in a list in the Network Settings. Manually selected cache computers differ from automatically selected ones in the following aspects:
    - When a computer has multiple cache computers assigned, it does not automatically share downloads among them.
    - If the first cache computer in the list is not available, the computer tries the next computer until it finds one that works. If it cannot find any available computers, the solution will try to access the Internet directly.

Requirements for using a computer with the cache role assigned

Automatic mode

- The computer with the cache role assigned and the computer that downloads items from it must be on the same subnet. If a cache computer has multiple network cards, it is able to act as a repository on each network segment to which it is connected.

We recommend that you designate a computer with the cache role on each network segment on the corporate network.

- All other computers automatically discover the presence of the cache computer and redirect their update requests to it.
- The cache computer must have a protection license assigned.
- The firewall must be configured to allow incoming and outgoing Universal Plug and Play (UPnP) and Simple Service Discovery Protocol (SSDP) traffic on:
    - UDP port 21226
    - TCP port 18226

Manual mode

- The computer with the cache role assigned and the computer that downloads items from do not need to be on the same subnet.

- The cache computer must have a protection license assigned.
- The firewall must be configured to allow incoming and outgoing traffic on:
    - UDP and TCP port 21226
    - TCP port 18226

Discovery of cache computers

When you designate a computer as cache, it broadcasts its status to the network segments to which its interfaces connect. All workstations and servers set to automatically detect cache computers receive the notification and connect to the cache computer. If there is more than one designated cache computer on a network segment, computers on the subnet connect to the most appropriate one based on the amount of free resources it has.

Occasionally, computers on the network set to automatically detect cache computers check whether there are new computers with the cache role.

Configuring the assignment method for cache computers

- Select the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Select one of the existing settings profiles.
- Go to the **Cache** section. Select one of the following two options:
    - **Automatically use the cache computers seen on the network**: Computers that receive these settings automatically look for cache computers on their network segment.
    - **Use the following cache computers (in order of preference)**: Click the ⊕ icon to add computers designated as a cache and set up a list of cache computers. Computers that receive these settings connect to the cache computers specified in the list.

Configuring real-time communication

Panda Endpoint Protection Plus communicates with the Aether platform in real time to retrieve the settings profiles configured for protected computers in the console. Therefore, only a few seconds pass between the time the administrator assigns a settings profile to a computer and the time it is applied.

Real-time communication between the protected computers and the Panda Endpoint Protection Plus server requires that each computer keep a connection open at all times. However, in organizations where the number of open connections might 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 might impact bandwidth usage.

Requirements for real-time communication

- Real-time communications are compatible with all operating systems supported by Aether, except Windows XP and Windows 2003.
- If a computer accesses the Internet through a corporate proxy, the HTTPS connections must not be manipulated. Many proxies use Man-in-the-Middle techniques to scan HTTPS connections or work as cache proxies. When that happens, real-time communications do not work.

Disabling real-time communication

- Click the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Click the **Add** button or select an existing settings profile to edit it.
- In the **Proxy** section, click **Advanced options**. Clear the **Enable real-time communication** checkbox.

If you disable real-time communication, your computers will communicate with the Panda Endpoint Protection Plus server every 15 minutes.

Configuring the agent language

To configure the language of the Panda agent for one or more computers, you must create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Click the **Add** button or select an existing settings profile to edit it.
- Go to the **Language** section and select a language from the list:
    - German
    - Spanish
    - Finnish
    - French
    - Hungarian
    - English
    - Italian
    - Japanese
    - Portuguese
    - Russian
    - Swedish

If the language is changed while the Panda Endpoint Protection Plus local console is open, the system will prompt the computer user to restart the local console. This does not affect the security of the computer.

Configuring the agent visibility

In those companies where the security service is 100% managed by the IT Department, there is no need for the Panda Endpoint Protection Plus agent icon to be shown in the notification area of managed computers. To show or hide the icon, follow the steps below:

- Click the **Settings** menu at the top of the console. Select **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Open the **Preferences** section and select or clear the **Show icon in the system tray** option.

Network Access Enforcement

Network Access Enforcement provides an extra layer of security when a user device (desktop, server, laptop, or mobile device) connects to your corporate network either remotely using a VPN connection or locally using a Wi-Fi connection.

The user device that tries to connect to the corporate network using a VPN or a Wi-Fi connection must meet a series of security requirements for the connection to be allowed. If it does not meet those requirements, the connection is rejected.

The Panda agent installed on the user device collects and sends the information that the Firebox or access point requires to verify that the device meets the necessary requirements.

Random UUID and authentication key generation

A UUID (Universal Unique Identifier) is a character string used to uniquely identify a device.

The Firebox or access point uses a UUID and authentication key to validate VPN or Wi-Fi network connections. Specify the same UUID-authentication key pair on the Firebox and in the Panda Endpoint Protection Plus console.

If you have not configured a UUID on a local-managed Firebox, you must generate one. UUID is an open format. To generate a random UUID, there are free tools available from vendors such as Microsoft or https://www.uuidgenerator.net/.

Use a long authentication key that includes uppercase, numeric, and special characters.

For more information about the Firebox and the VPN connection settings, see Network Access Enforcement Overview.

Requirements

For a user device to connect to the corporate network, it must meet these security requirements:

- It must have the security software installed, running, and correctly configured.
- You must have a valid UUID and authentication key configured on the device that validates the connection and in the Panda Endpoint Protection Plus console.
- **Operating system installed on the user device**:
  - Windows 8.1 or higher.
  - macOS Catalina 10.15 or higher.
  - Android 6 or higher.

With Android, unlike Windows or macOS, the Firebox console user cannot select the operating system version. On devices that run Android 6.0 or higher, Network Access Enforcement enables after they receive the relevant settings from the Aether servers.

- **Open ports on the user device**: The Panda agent requires that TCP port 33000 be open to communicate with the device that validates the connection.
- **Security software settings**: Panda Endpoint Protection Plus antivirus must be enabled and running.

Network Access Enforcement does not support Linux devices.

Requirements verification

When a user device tries to connect to the corporate network, the device that validates the connection performs these actions:

- Requests information about the status of the protection installed on the user device.
- Verifies the account UUID and the authentication key are valid.
- Verifies the user device operating system against the operating systems defined in its settings.

If all requirements are met, the user device is allowed to access the corporate network. Otherwise, the connection is rejected.

By default, all devices are forced to comply with the security requirements to connect to the corporate network.

Accessing the Network Access Enforcement settings

- From the side menu, select **Network services**.
- Select the **Network Access Enforcement** tab.
- To enable the protection, click the toggle.
- Enter the account UUID and the authentication key.
- Click **Save changes**.

Configuring security against protection tampering

To prevent unauthorized users from disabling the protection, Panda Endpoint Protection Plus enables you to set these limitations for the uninstallation and configuration of the security software on user computers:

- **Set a first authentication factor** (based on a password) to configure, disable, or uninstall the security software from the computer. Compatible with Windows and Linux computers.
- **Set a second authentication factor** (based on a QR code) to configure, disable, or uninstall the security software from the computer. Compatible with Windows and Linux computers. To use the second authentication factor, you must:
    - Have access to a smartphone or tablet with a built-in camera.
    - Download the WatchGuard AuthPoint app (or another authenticator app) for free from:
        - **iOS**: https://apps.apple.com/app/watchguard-authpoint/id1335115425
        - **Android**: https://play.google.com/store/apps/details?id=com.watchguard.authpoint
- **Enable anti-tamper protection**: Many advanced threats use techniques for disabling the security software installed on computers. Anti-tamper protection prevents tampering of the security software operation by enabling you to configure a password that prevents the software from being stopped, paused, or uninstalled. Compatible with Windows and Linux computers.
- **Enable protection when the computer starts in Safe Mode**: Some types of malware force Windows computers to restart in Safe Mode with networking enabled. In this mode, antivirus is automatically disabled and computers are vulnerable. You can configure Panda Endpoint Protection Plus to protect computers when they start in Safe Mode with networking enabled, so that all configured protections remain active and working normally. Compatible with Windows computers.

> *If a computer loses its license because it is manually removed or because it expires or is canceled, the anti-tamper protection and password-based uninstallation protection are disabled.*

To configure security against tampering:

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select an existing settings profile, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**:
- To **Request password to uninstall the protection from computers**, enable the toggle. In the **Password required to perform advanced management tasks locally from your computers** text box, type a password that is between 6 and 15 characters in length.
- To **Allow the protections to be temporarily enabled/disabled from the computers' local console**, enable the toggle. In the **Password required to perform advanced management tasks locally from your computers** text box, type a password that is between 6 and 15 characters in length.
- To **Enable Anti-Tamper protection (prevents users and certain types of malware from stopping the protections)**, enable the toggle. In the **Password required to perform advanced management tasks locally from your computers** text box, type a password that is between 6 and 15 characters in length.
- To **Enable protection when Windows computers start in Safe Mode**, enable the toggle. The protection starts working when a computer starts in Safe Mode with networking.
- To enable the second authentication factor, see Enabling two-factor authentication (2FA).

Enabling two-factor authentication (2FA)

Generally, the security software is protected against tampering from third parties through a single password mechanism. Nevertheless, you can add an additional authentication factor for the security software. This additional authentication factor is obtained through a QR code generated in the console and which must be imported to the AuthPoint app or another app that generates authentication tokens.

To generate the QR code, Panda Endpoint Protection Plus requires a keyword. Each keyword generates a specific QR code.

After you enable two-factor authentication in a **Per-computer settings** profile, and the authenticator app reads the QR code, the administrator must provide both the password set in the console and the token generated by the authenticator app to uninstall the agent or change its settings.

Depending on the number of administrators who use the console, you can generate a single QR code for the entire account or multiple different codes. You can share a QR code to all **Per-computer settings** profiles in the account, to some profiles only, or even assign a unique QR code to each **Per-computer settings** profile.

Generating a unique QR code at account level

The QR code is automatically generated at account level and applied to all settings profiles that have the **Use a QR code shared across the entire account** setting enabled.

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select an existing settings profile, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**.
- Select the **Enable Two-Factor Authentication (2FA)** toggle.
- Select **Use a QR code shared across the entire account**.
- Click **Show QR code**. A dialog box opens that shows the QR code generated for all the **Per-computer settings** profiles in the account.
- Scan the QR code in the AuthPoint app (or another authenticator app).
- Click **Close**.
- Click **Save**.

Generating a QR code for a single settings profile

The console prompts for a keyword to generate a QR code that is applied to a specific **Per-computer settings** profile.

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select an existing settings profile, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**.
- Select the **Enable Two-Factor Authentication (2FA)** toggle.
- Select **Generate a QR code for this configuration**.
- Click **Generate code**.
- Enter a 6- to 20-character combination of letters and numbers for the QR code key. This QR code key (passphrase) is linked to the generated QR code. You can reuse the QR code key in other **Per-computer settings** profiles to enable two-factor authentication.
- Click **Generate code**.
- Click **Close**.
- Click **Save**.

Sharing a QR code to multiple settings profiles

To assign an existing QR code to another **Per-computer settings** profile:

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select the settings profile from which you want to copy the QR code.

- Select **Security against unauthorized protection tampering**.
- In **Generate a QR code for this configuration**, click **Show QR code**. A dialog box opens and shows the QR code and the QR code key.
- Copy the QR code key to the clipboard.

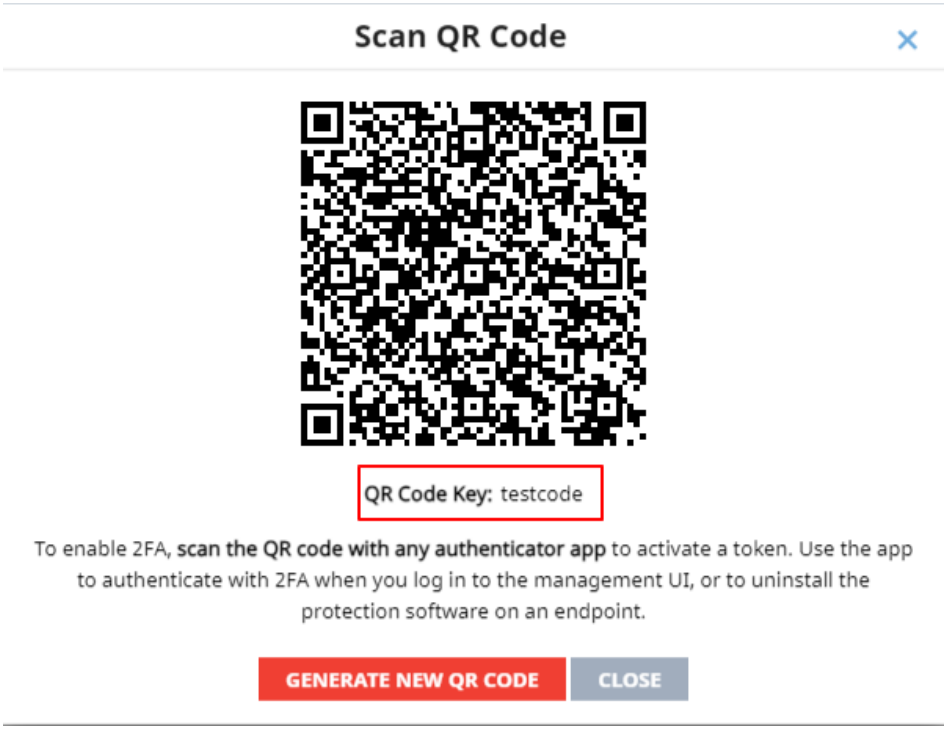


Figure 10.2: QR code and associated QR code key

- In the dialog box, click **Close**. On the settings profile page, click **Close**.
- Select the settings profile where you want to use the QR code you copied, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**.
- Select the **Enable Two-Factor Authentication** toggle.
- Select **Generate a QR code for this configuration**.
- Click **Generate code**.
- In the text box, paste the QR code key you copied.
- Click **Generate code**.
- Click **Close**.
- Click **Save**.

Exceptions when you copy a security settings profile with anti-tamper protection enabled

When you copy a settings profile with a password and/or two-factor authentication enabled, the security software behaves as described in Copying a settings profile on page 268, except:

- The copied profile does not include the password specified in the **Password required to perform advanced management tasks locally from your computers** text box. The administrator must enter a new password.
- If the administrator copies a settings profile inherited from a partner, Panda Endpoint Protection Plus automatically enables the **Generate a QR code for this configuration** option and generates a new QR code. It does not copy the password specified in the **Password required to perform advanced management tasks locally from your computers** text box.

Configuring shadow copies

Shadow copies is a technology included in Windows computers that can create a snapshot of computer files, even when they are in use.

From Panda Endpoint Protection Plus, you can remotely interact with the Windows Shadow Copies service on the computers on the network, using it as a remediation tool against ransomware attacks.

Characteristics of shadow copies in Panda Endpoint Protection Plus

Panda Endpoint Protection Plus complements the Shadow Copies service included in Microsoft Windows with additional features to protect user data from threats:

- Enables you to configure and manage a backup (snapshot) repository separately from other repositories the user might have created.
- Protects the service and the snapshots from changes made by threats or the user. This prevents the service from being stopped or the backup copies made by Panda Endpoint Protection Plus from being deleted.
- Enables you to specify the percentage of hard disk space to use for backup copies (this is 10% by default).
- Makes a backup copy of the files every 24 hours. The first copy is made when you enable the feature (it is disabled by default).
- Retains up to 7 copies of each file at a given time, depending on the free space allocated to the repository. If there is not enough space, older backup copies are deleted.

Requirements

- Operating system:
    - Windows Vista, Windows 7, or higher.
    - Windows 2003 Server 2012 or higher.
- Enough free disk space to make backup copies.
- Storage media identified by the operating system as fixed (internal and USB-connected hard disks) and NTFS disks.

Accessing the shadow copies feature

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**. A list opens and shows all created settings profiles.
- Select an existing settings profile or create a new one.
- In the **Shadow Copies** section, click the toggle to enable the feature. Specify the percentage of disk space you want to use for backup copies on user computers.

> *Although Panda Endpoint Protection Plus uses snapshots that are independent of the ones created by the user or the network administrator, all of them share the same settings. Additionally, the maximum space value you set for shadow copies in the management console has priority over other space settings established by the network administrator.*

Using filters to find computers with shadow copies enabled

- From the top menu, select **Computers**.
- In the side panel, click the  icon. The filter tree appears.
- Select a folder. Click the icon. A context menu appears.
- Select **Add filter**. The **Add filter** dialog box opens.
- Configure the filter with these values:
    - **Category**: Computer
    - **Property**: Shadow Copies
    - **Operator**: Is equal to
    - **Value**: Enabled

For more information, see *Configuring filters* on page *205*.

Chapter 11

Security settings for workstations and servers

Configure security settings profiles for workstations and servers to define how Panda Endpoint Protection Plus protects the computers on your network against threats and malware.

Next is a description of the options available for configuring the security of your workstations and servers. We also provide practical recommendations on how to protect all computers on your network, without negatively impacting users' activities.

> *For additional information about the Workstations and servers module, see:*
>
> 
>
> *Creating and managing settings profiles on page 267: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*
>
> *Accessing, controlling, and monitoring the management console on page 53: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

Chapter contents

Accessing the settings and required permissions

Accessing the settings

- Click the **Settings** menu at the top of the console. Select **Workstations and servers** from the side menu.
- Click the **Add** button. The **Workstations and servers** settings page opens.

Required permissions

Permission	Access type
Configure security for workstations and servers	Create, edit, delete, copy, or assign settings profiles for workstations and servers.
View security settings for workstations and servers	View the Workstations and servers settings profiles.

Table 11.1: Permissions required to access the Workstations and servers settings

Introduction to the security settings

The parameters for configuring the security of workstations and servers are divided into various sections. Click each of them to display a drop-down panel with the associated options. Next is a brief explanation of each section:

Section	Description
General	Configure updates, the removal of other security products, and file exclusions from scans.
Antivirus	Configure parameters that control the traditional anti-malware protection against viruses and threats.
Firewall (Windows devices)	Configure parameters that control the firewall and the intrusion detection system (IDS) against network attacks.
Device control (Windows devices)	Configure parameters that control user access to the peripheral devices connected to the computer.

Section	Description
Web access control	Restrict access to web content categories and unknown pages.

Table 11.2: Available modules in Panda Endpoint Protection Plus

Not all features are available for all supported platforms. This table provides a summary of the features in Panda Endpoint Protection Plus that are available for each supported platform:

Feature	Windows	macOS	Linux
Antivirus (1)	X	X	X
Firewall & Intrusion Detection System (IDS)	X		
Email protection	X		
Web protection	X	X	
Device control	X		
Web access	X	X	

Table 11.3: Supported security features by platform

General settings

The general settings enable you to configure how Panda Endpoint Protection Plus behaves with respect to updates, the removal of competitor products, and file and folder exclusions from scans.

Local alerts

Field	Description
Show malware, firewall, and device control alerts	In the text box, type a custom message to include in the alert. The Panda Endpoint Protection Plus agent will show a pop-up window with the content of the message. This feature is available for computers with a Windows, macOS, or Linux operating system installed.
Show an alert every time the web access control	A pop-up window displays on the workstation or server every time Panda Endpoint Protection Plus blocks a web page. This feature is available for computers with a Windows or macOS operating system installed.

Field	Description
feature blocks a page	

Table 11.4: Fields in the Local Alerts section

Updates

For more information about how to update the agent, the protection, and the signature file of the client software installed on user computers, see *Product updates and upgrades on page 193*.

Uninstall other security products

For more information about how to configure the action to take if another security product is already installed on user computers, see *Protection deployment overview on page 92*.

For a complete list of the competitor products that Panda Endpoint Protection Plus uninstalls automatically from user computers, see Supported uninstallers.

Files and paths excluded from scans

Configure items on your computers that you do not want the security software to delete or disinfect when it scans for malware.

Exclusions disable antivirus protection for the specified files and file paths. Because this setting can cause security issues, we recommend that you only exclude files and paths to resolve performance problems.

Exclusions set by a partner

If your service provider changes the status of the settings profile from editable to non-editable, the exclusions you added no longer apply. Only the exclusions from the service provider apply. If the service provider changes the configuration again to be editable, then the exclusions you previously added are restored and applied..

Exclude the following disk files

Specify the files on the hard disk of your protected computers that you do not want Panda Endpoint Protection Plus to delete or disinfect.

We recommend that you use wildcards for Windows computers or substring matches for Linux/macOS computers as little as possible to be as specific as possible with regard to the files to exclude from scans.

Field	Description
Extensions	Specify the extensions of files you do not want to scan.
Folders	Specify the folders whose files you do not want to scan. **Windows:** • You can use system variables. • You cannot use user-created variables. • You cannot use willdcards. **Linux/macOS:** • You cannot use system or user variables. • You can specify partial paths.
Files	Specify the files you do not want to scan. **Windows:** • You can use the wildcard characters ? and * when you do not specify the path and you indicate the file name only. • You cannot use wildcards when you specify the full path to a file. • If you do not specify a file path, the file is excluded from scans in all folders where it is located. If you specify the path, the file is excluded from scans only in that folder. **Linux/macOS:** • You cannot use wildcard characters ? or *. • If you do not specify a file path, the file is excluded from scans in all folders where it is located. If you specify the path, the file is excluded from scans only in that folder.

Field	Description
	• You can specify the partial name of a file.

Table 11.5: Disk files you do not want Panda Endpoint Protection Plus to scan

Example: Exclude files on Windows computers

To exclude file `C:\Users\mike\desktop\data.txt`:

- **Files** = `C:\Users\mike\desktop\data.txt` (recommended option).
- **Files** = `data.txt` (not recommended; this excludes all data.txt files regardless of their path).
- **Files** = `C:\Users\mike\desktop\data.*` (wrong; you cannot exclude files using widcards when you specify the path).

Example: Exclude paths on Windows computers

To exclude folder `C:\Users\mike\desktop\`:

- **Folders** = `C:\Users\mike\desktop\` (recommended option).
- **Folders** = `C:\Users\%USERNAME%\desktop\` (excludes the desktop folder for all of the computer users).
- **Folders** = `C:\Users\*\desktop\` (wrong; you cannot exclude folders using widcards in paths).

Example: Exclude files or folders on Linux/macOS computers

To exclude file `/home/mike/data.txt`:

- **Files** = `/home/mike/data.txt` (recommended option).
- **Folders** = `/home/$USER/` (wrong; you cannot use environment variables).
- **Files** = `/home/mike/*.txt` (wrong; you cannot use wildcards).
- **Files** = `mik` (not recommended, this excludes all files whose name or path contains the `mik` substring).

Exclude the following email attachments

Specify email attachments with specific file extensions that you do not want to scan.

Antivirus

This section enables you to configure the general behavior of the signature-based antivirus engine.

Field	Description
File antivirus	Enable or disable the antivirus protection for the file system.

Field	Description
Mail protection	Enable or disable the antivirus protection for the mail client installed on user computers. Panda Endpoint Protection Plus detects threats received over the POP3 protocol and encrypted variants.
Web browsing antivirus	Enable or disable the antivirus protection for the web browser installed on user computers. Panda Endpoint Protection Plus detects threats received over the HTTP protocol and encrypted variants.

Table 11.6: Antivirus protection modules available in Panda Endpoint Protection Plus

When Panda Endpoint Protection Plus detects malware or the Panda Security anti-malware laboratory identifies a suspicious file, Panda Endpoint Protection Plus takes one of these actions:

- **Known malware files when disinfection is possible**: Replaces the infected file with a clean copy.
- **Known malware files when disinfection is not possible**: Makes a copy of the infected file and deletes the original file.

AMSI (AntiMalware Scan Interface) technology

The Windows AntiMalware Scan Interface (AMSI) is a versatile interface that allows your applications and services to integrate with any anti-malware product that is present on a computer. AMSI provides enhanced malware protection for your users and their data, applications, and workloads.

For more information, see https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal.

This feature is only available for computers with a Windows operating system installed.

To enable or disable AMSI technology, enable the **Enable advanced scanning with AMSI** toggle.

Exclusions

You can add exclusions for programs that might cause performance issues when you enable advanced scanning with AMSI. In the text box, type the names of the programs and press Enter. For more information about how the console behaves when you edit exclusions for a settings profile managed by a partner, see Exclusions set by a partner.

Threats to detect

Configure the types of threats that Panda Endpoint Protection Plus searches for and removes from the file system, mail client, and web client installed on user computers.

Field	Description
Detect viruses	Detects files that contain patterns classified as dangerous.
Detect hacking tools and PUPs	Detects unwanted programs (such as programs with intrusive ads and browser toolbars) and tools used by hackers to gain access to your system.
Block malicious actions	Enables anti-exploit and heuristic technologies that analyze process behavior locally and detect suspicious activity.
Detect phishing	Detects fraudulent emails and websites.
Do not detect threats at the following addresses and domains	Type IP addresses and domains you want to exclude from phishing scans, separated by commas. This text box is not case-sensitive. Access is allowed to all addresses that start with the specified IP addresses and domains, even if the full URL is longer.
Create Decoy Files to help detect ransomware	Creates decoy files as bait on computers. These files are permanently monitored by Panda Endpoint Protection Plus. When there is an attempt to modify a decoy file, the security software identifies the process as ransomware and ends the process.

Table 11.7: Malware types detected by the Panda Endpoint Protection Plus antivirus protection

File types

Specify the types of files to be scanned by Panda Endpoint Protection Plus:

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	Many types of data files do not pose a threat to the security of computer

Field	Description
of their extension when they are created or modified (Not recommended)	networks. When you enable this option, the security software scans all files when they are created or modified. For best performance, we recommend that you do not enable this option.

Table 11.8: File types scanned by the Panda Endpoint Protection Plus antivirus protection

Firewall (Windows computers)

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

- **System rules**: Describe communication characteristics (ports, IP addresses, protocols, etc.), allowing or denying the data flows that match the configured rules.
- **Program rules**: 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)**: Enables users to manage the firewall protection from the local console installed on their computers.
- **Disabled (administrator-mode firewall)**: You configure the firewall protection of all computers on the network through settings profiles.

Network types

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. You have two options to set the default behavior of the firewall protection: manually select the type of network that the computers in the configured profile usually connect to, or let Panda Endpoint Protection Plus select the most appropriate network type.

Network type	Description
Public network	Networks in public places such as airports, Internet cafés, and universities.

Network type	Description
	Computers are not visible to other users on the network and some programs have limited access to the network. Limitations must be established on the way protected computers are used and accessed, especially with regard to file, resource, and directory sharing. Panda Security rules are enabled or disabled according to the administrator's criteria.
Trusted network	Home or office networks when you know and trust the other users and devices on the network. Computers are visible to other computers and devices on the network. Panda Security rules are not applied, so there are no restrictions on sharing files, resources, or directories.
Detect automatically	The network type (public or trusted) is selected automatically based on the rules you specify. Click the link **Configure rules to determine when a computer is connected to a trusted network**.

Table 11.9: Network types supported by the firewall

Panda Endpoint Protection Plus behaves differently and applies 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.

Each network interface on a computer has a specific type of network assigned to it. Computers with multiple network interfaces can have different network types assigned, and different firewall rules for each network interface.

Configuring rules for trusted access

Panda Endpoint Protection Plus enables you to add and configure rules to determine whether a computer is connected to a **trusted network**. If none of these conditions is met, then the network type selected for the network interface is **public network**.

To be considered on a trusted network, the computer must be able to resolve a domain previously defined on an internal DNS server. If the computer can connect to the DNS server and resolve the configured domain, then it is connected to the company network, and the firewall assumes the computer is connected to a trusted network.

Next is a configuration example:

- In this example, the organization's primary DNS zone is "`mycompany.com`".
- Add a Type A record with the "`firewallcriterion`" name to the primary zone of your organization's internal DNS server ("`mycompany.com`"). You do not need to specify an IP address because it is not used to validate the criterion.
- Based on these settings, "`firewallcriterion.mycompany.com`" is the domain that Panda Endpoint Protection Plus tries to resolve in order to check that it is connected to the company's network.
- Restart the DNS server if required and make sure "`firewallcriterion.mycompany.com`" is resolved successfully from all segments of the internal network with the tools `nslookup`, `dig`, or `host`.
- From the Panda Endpoint Protection Plus console, click the link **Configure rules to determine when a computer is connected to a trusted network**. A dialog box opens. Enter the following data:
  - **Criterion name**: Type a name for the rule you want to add.. For example "`myDNScriterion`".
  - **DNS server**: Type the IP address of the DNS server in your company network that can resolve DNS requests.
  - **Domain**: Type the domain to send to the DNS server for resolution. Enter "`firewallcriterion.mycompany.com`".
- Click **OK** and **Save**. Click **Save** again.
- After the criterion has been configured and applied, the computer tries to resolve the "`firewallcriterion.mycompany.com`" domain on the specified DNS server every time an event occurs on the network interface (connect, disconnect, IP address change, etc.). If DNS resolution succeeds, the settings assigned to the trusted network are assigned to the network interface used.

Program rules

In this section you can configure program rules to control which programs can communicate with the local network and Internet.

To build an effective protection strategy, follow these steps 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 have not configured a specific rule in step 3. This is the default, basic mode.

Action	Description
Deny	Implements a restrictive strategy based on always denying connections for all programs for which you have not 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 11.10: Types of default actions supported by the firewall for the programs installed on computers

2. **Enable or disable Panda Security rules.**

This only applies if the computer is connected to a public network.

3. **Add rules to define the specific behavior of your applications**.

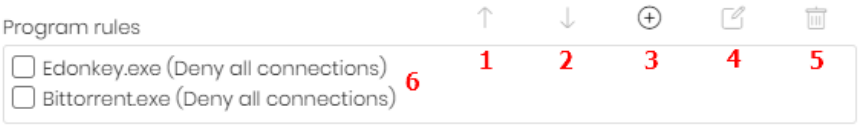


Figure 11.1: Edit controls for connection rules

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 you want to apply each action to.

Complete the following fields to create a rule:

- **Description**: Type a description of the new rule.
- **Program**: Select a program you want to configure connection options for.
- **Connections allowed for this program**: Select an option to specify whether to allow or deny connections for the program:

Field	Description
Allow inbound and outbound connections	The program can connect to the local network and Internet. Also, other programs or users can 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 local network and Internet, but does not accept inbound connections from other users or applications.
Allow inbound connections	The program accepts connections from programs or users from the local network and Internet, but is not allowed to establish outbound connections.

Field	Description
Deny all connections	The program cannot connect to the local network or Internet.

Table 11.11: Communication modes for allowed programs

- **Advanced permissions**: Specify parameters of the traffic you want to allow or deny.

Field	Description
Action	Defines the action that Panda Endpoint Protection Plus takes when 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	Applies only if the zone matches the zone configured in Network types. Rules whose **Zone** is set to **All** are applied at all times irrespective of the network type configured in the Firewall settings.
Protocol	Establish the layer 3 protocol for the traffic generated by the program you want to control: • All • TCP • UDP

Field	Description
IP	• **All**: The rule does not take into account the connection source and target IP addresses. • **Custom**: Specify the source or target IP address of the traffic to control. You can enter multiple addresses, separated by commas (,). To specify a range, use a hyphen (-). From the drop-down menu, select if the IP addresses are IPv4 or IPv6. You cannot mix different types of IP addresses in the same rule. • **Ports**: Specify the communication port. Select **Custom** to enter multiple ports, separated by commas (,). To specify a range, use a hyphen (-).

Table 11.12: Advanced communication options for allowed programs

Connection rules

Connection rules define traditional TCP/IP traffic filtering. Panda Endpoint Protection Plus extracts the values of fields in the headers of each packet sent and received by protected computers and checks them against the predefined rules and any custom rules you create If the traffic matches any of the rules, the solution takes the specified action.

Connection rules affect the entire system (regardless of the process that manages them). They have priority over program rules that control the connection of programs to the Internet and local network.

To build an effective strategy to protect the network against dangerous and unwanted traffic, follow these steps in the order listed:

1. **Specify the firewall's default action in the Program rules section**.

Action	Description
Allow	Implements a permissive strategy based on always accepting all connections for which you have not configured a specific rule in step 3. This is the default, basic configuration mode: All connections for which there is not an existing rule are automatically accepted.
Deny	Implements a restrictive strategy based on always denying all connections for which you have not configured a specific rule in step 3. This is an advanced mode: All connections for which there is not an existing rule are automatically denied.

Table 11.13: Types of default actions supported by the firewall for the programs installed on users' computers

2. **Enable or disable Panda Security rules.**

This only applies if the computer is connected to a public network.

3. **Add rules that describe specific connections along with the associated action**.

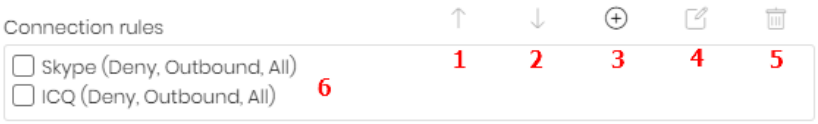


Figure 11.2: Edit controls for connection rules

You can change the order of the firewall 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 you want to apply each action to.

The order of the rules in the list is not random. They are applied in descending order. If you change the position of a rule, you also change its priority.

The following is a description of the fields found in a connection rule:

Field	Description
Name	Type a name for the rule.
Description	Type a description of the traffic filtered by the rule.
Direction	Sets the traffic direction for connection protocols such as TCP. • **Outbound**: Outbound traffic. • **Inbound**: Inbound traffic.
Zone	The rule only applies if the value specified here matches the network type configured in Network types. If you select **All**, then the rule applies at all times, regardless of the network type configured.

Protocol	Select the traffic protocol. The options vary for the protocol you select:
	• **TCP, UPD, TCP/UDP**: Define TCP and/or UDP rules, including local and remote ports.
	  • **Local ports**: Select the connection port used on the user's computer. Select **Custom** to enter multiple ports separated by commas (,) or a range separated with a hyphen (-).
	  • **Remote ports**: Select the connection port used on the remote computer. Select **Custom** to enter multiple ports separated by commas (,) or a range separated with a hyphen (-).
	• **ICMP services**: Create rules that describe ICMP messages, indicating their type and subtype.
	• **ICMPv6 services**: Create rules that describe ICMP messages over IPv6,

Field	Description
	indicating their type and subtype. • **IP Types**: Select the higher-level protocols you want to apply the rule to.
IP addresses	Specify the source or target IP address of the traffic to control. You can enter multiple addresses, separated by commas. To specify a range, use a hyphen (-). From the drop-down menu, select if the IP addresses are IPv4 or IPv6. You cannot mix different types of IP addresses in the same rule.
MAC addresses	Specify the source or target MAC address of the traffic to control.

Table 11.14: Settings options for connection rules

The source and target MAC addresses included in packet headers are overwritten every time the traffic goes through a proxy, router, etc. The data packets reach their destination with the MAC address of the last device that handled the traffic.

Block intrusions

The intrusion detection system (IDS) enables you to detect and reject malformed traffic specially crafted to impact the security and performance of protected computers. This traffic can cause malfunction of user programs, lead to serious security issues, and allow remote execution of applications by hackers, data theft, etc.

The following 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. Routing information is defined beforehand.
Land Attack	Stops denial-of-service attacks that use TCP/IP stack loops. Detects packets with identical source and target addresses.
SYN Flood	This attack type launches TCP connection attempts 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 saturation of the computer under attack.

Field	Description
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. The attacking computer is unable to obtain 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. It blocks attacks 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 a IP header length that exceeds a specific limit. • **TCP**: Rejects inbound packets with a TCP header length that exceeds a specific limit. • **Fragmentation Overlap**: Checks the status of the packet fragments to be reassembled at the destination, which protects 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**: Detects invalid MTU values used to generate a denial-of-service attack or slow down outbound traffic. • **SMURF**: 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, which multiplies traffic flows. The solution rejects unsolicited ICMP replies if they exceed a certain threshold in a specific time period. • **Drop Unsolicited ICMP Replies**: Rejects all unsolicited and expired ICMP replies.

Field	Description
ICMP Filter Echo Request	Rejects ICMP echo request packets.
Smart ARP	Rejects ARP replies that do not correspond to requests sent by the protected computer to avoid ARP cache poisoning scenarios.
OS Detection	Falsifies data in replies to the sender to trick operating system detectors. It prevents attacks on vulnerabilities associated with the operating system. . This protection complements the TCP Flag Checker.

Table 11.15: Supported types of malformed traffic

Do not block intrusions from the following IP addresses:

Enables you to exclude certain IP addresses and/or IP address ranges from the detections made by the firewall.

Device control (Windows computers)

This feature enables you to control the behavior of protected Windows computers when they connect to a removable or mass storage device:

- From the top menu, select **Settings**.
- From the side menu, select **Workstations and servers**. A page opens that shows all settings profiles created so far.
- Select an existing security settings profile to edit, or in the upper-right corner of the page, click **Add** to create a new profile.
- Select **Device control**.
- Enable the **Enable device control** toggle.
- For each type of device, specify the authorized use:
    - **Removable storage drives and CD/DVD drives**: Choose among **Block**, **Allow read access**, or **Allow read & write access**.
    - **Bluetooth devices, mobile devices, imaging devices, and modems**: Choose among **Allow** and **Block**.
- To **Disable AutoPlay on removable storage devices**, enable the toggle. The Windows operating system blocks the `autorun.inf` file on storage devices and does not automatically run the

predefined application or action. Neither does it show the menu with the available actions for the device.

Allowed devices

This section enables you to configure an allowlist of specific devices you want to allow despite belonging to a blocked device category.

- Click the ⊕ icon in the **Allowed devices** section to show a list of all devices connected to the computers on your network.
- Select the devices you want to exclude from the configured general blocking rules.
- Use the 🗑 button to delete existing exclusions.

Exporting and importing a list of allowed devices

Use the **Export** and **Import** options available from the context menu ⋮.

Determining a device unique ID

To manage a specific device without having to wait for a user to connect it to their computer, or to exclude it manually, you need to determine the device ID:

- Open Windows Device Manager. Select the device you want to obtain the ID for. Right-click the device name and select **Properties**.
- Select the **Details** tab.
- From the **Property** drop-down list, select **Device Instance Path**. The **Value** box shows the device unique ID.

If no value appears in Device Instance Path, you are not able to obtain the device ID. You can instead use the Device Hardware ID to identify it:

- To show the Device Hardware ID, from the **Property** drop-down list, select **Hardware IDs**.

> *A device Hardware ID does not identify it uniquely. It identifies all devices of the same hardware type.*

In a text file, add the IDs of the devices you want to allow, as indicated in Exporting and importing a list of allowed devices

Renaming devices

The name assigned to a computer devices by Panda Endpoint Protection Plus can sometimes lead to confusion or prevent you from correctly identifying them. To resolve this, you can assign a custom name for a device:

- In the **Allowed devices** list, select the computer or device.
- Click the  icon. A dialog box opens for you to enter a new name for the device.
- Click **OK**. The **Allowed devices** list updates with the new name.

Web access control

With this protection, you can limit access to specific web content categories and individual URLs to optimize network bandwidth and increase business productivity.

To enable or disable it, click the **Enable Web access control** toggle.

Limitations with HTTP/3 (QUIC) protocol

Because the security software does not inspect the HTTP/3 (QUIC) protocol, the web access control feature does not support browsers with that protocol.

To resolve this issue, use one of these options:

Add a filter rule from the Panda Endpoint Protection Plus console to block traffic on port 80, port 8080, and port 443

This procedure is effective on Windows devices only.

- From the top menu, select **Settings**. From the side menu, select **Workstations and servers**. A page opens that shows all settings profiles created so far.
- Select an existing security settings profile to edit, or in the upper-right corner of the page, click **Add** to create a new profile. The **Add settings** or **Edit settings** page opens.
- Select the **Firewall (Windows computers)** section. The settings associated with the firewall appear.
- Click **Enable the firewall** (if it is disabled).
- In **Connection rules**, click the  icon to create a new filter rule.
- In the **Name** and **Description** fields, enter a name for the filter rule and a description (optional).
- In the **Action** field, select **Deny**.
- In the **Direction** field, select **Outbound**.
- In the **Zone** field, select the type of network for which you want to apply the block rule on the user computer. See Network types.
- In the **Protocol** field, select **UDP**.
- In the **Remote ports** field, select **Custom**. A new field appears.
- In the **Custom** field, add port 80, port 8080, and port 443 separated by a comma.

- Click **OK**. Click **Save**. The settings profile is saved and automatically sent to all computers that have it assigned.

After the firewall rule is applied to the computers on the network, the user browser cannot send requests that use the UDP protocol on port 80, 8080, or 443. This forces the browser to send its requests with the TCP protocol on port 80, which corresponds to HTTP/2.

For more information about how to create firewall rules in Panda Endpoint Protection Plus, see Connection rules.

Disable HTTP/3 (QUIC) protocol in browsers on user devices

Browser settings can vary for different versions.

- Google Chrome
  - In the browser address bar, type **chrome://flags**.
  - Disable the **Experimental QUIC protocol** option.
- Microsoft Edge
  - In the browser address bar, type **edge://flags/**.
  - Disable the **Experimental QUIC protocol** option.
- Mozilla Firefox
  - In the browser address bar, type **about:config**.
  - Disable the **network.http.http3.enabled** option.
- Opera
  - In the browser address bar, type **opera://flags/#enable-quic**.
  - From the **Experimental QUIC protocol** drop-down menu, select **Disabled**.

Configuring time periods for the web access control feature

This option enables you to limit access to certain website categories and denied sites during business hours and authorize it during non-business hours and weekends.

To configure Internet access time limits, select the **Enable only during the following times** option.

Specify when you want to enable web access control. On the calendar, select the days and hours when you want to enable it.

- Click the day to select the whole day.
- Click and drag the squares to select multiple days and times.
- To select every day of the month, click the **Select all** button.
- Click **Clear** to disable web access control for all of the times selected.

Denying access to specific web pages

Panda Endpoint Protection Plus groups the web pages it classifies into 160 content categories. To deny access to a certain type of web content category, select it from the list.

If a user visits a web page that belongs to one of the forbidden categories, a warning page appears that indicates that access is denied and the reason.

Denying access to pages categorized as unknown

To deny access to pages characterized as unknown, enable the **Deny access to pages categorized as unknown** toggle.

> *Internal and intranet sites accessible on ports 80 and 8080 could be categorized as unknown. To avoid this, add exclusions for internal pages you want to allow.*

List of allowed/denied addresses and domains

You can set a list of pages that are always allowed (allowlist) or blocked (blocklist), regardless of the category that they belong to:

- In the text box, enter the URL of the relevant IP address or domain.
- Click **Add**.
- Use the **Delete** and **Clear** buttons to edit the list according to your needs.
- Click **OK** to save the settings.

To add multiple similar domains to a list without having to specify each domain separately, you can add the part of the domain names that is common to all of them. The wildcard character (*) is not supported.

For example, **https://www.mydomain.com/test** represents these domains (among others):

- https://www.mydomain.com/test/test2.htm
- https://www.mydomain.com/testing.htm
- https://www.mydomain.com/test/test2/

Database of URLs accessed from computers

Each computer on the network keeps a database of the URLs accessed from it. This database is located in:

```
%programdata%\Panda Security\Security Protection\urlcounters.dg
```

This database is in SQLite3 format and can only be accessed from the computer for a period of 30 days.

The data stored is this:

- User ID.
- Protocol (HTTP or HTTPS).
- Domain.
- URL
- Returned category.
- Action (Allow/Deny).
- Date accessed.
- Access count (by category and domain).

Chapter 12

Security settings for mobile devices

The **Settings** menu at the top of the Panda Endpoint Protection Plus console provides the parameters required to configure the security of the smartphones and tablets in the organization. Select the **Mobile devices** option in the menu on the left to view a list of the security profiles already created, or to create a new one.

The following is a description of the available security and anti-theft configuration options for mobile devices, and recommendations to protect smartphones and tablets without interfering with user activity.

*For more information about the **Mobile devices** module, see:*

Creating and managing settings profiles on page 267: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

Accessing, controlling, and monitoring the management console on page 53: Managing user accounts and assigning permissions.

Chapter contents

Security settings for Android devices

Accessing the settings

- From the top menu, select **Settings**.
- From the side menu, select **Mobile devices**.
- Select the **Android devices** tab. Click **Add**. The **Add settings** page opens.

Required permissions

Permission	Access type
Configure security for mobile devices	Create, edit, delete, copy, or assign settings profiles for mobile devices.
View security settings for mobile devices	View the security settings profiles for mobile devices defined.
Use the anti-theft protection for mobile devices (locate, wipe, lock, etc.)	Send actions to target mobile devices to prevent data loss, locate them in the event of loss or theft, and lock them.

Table 12.1: Permissions required to access the Android device security settings

Updates

Define the type of connection to be used by the device to download updates from the Panda Security cloud.

For more information about how to configure updates, see Product updates and upgrades on page 193.

Antivirus

The antivirus protection for Android mobile devices scans both devices and their SD cards permanently and on demand. It also protects against the installation of apps from unknown sources that could be infected with malware and PUPs.

To enable the antivirus protection and scan apps from unknown sources, enable the toggles.

Exclusions

This option enables you to select installed apps that you do not want to be scanned. Enter the names of the packages you want to exclude from the scans, separated by commas (“,”).

To look up an app package name, find the app in the Google Play store using a web browser. The package name appears at the end of the URL after the '`?id=`'.

Anti-theft

The anti-theft feature enables you to send actions to target Android devices to prevent data loss or locate them in the event of loss or theft.

Accessing the anti-theft feature

- From the top menu, select **Settings**. From the side menu, select **Mobile devices**.
- Select the **Android devices** tab. A list opens and shows all created settings profiles.
- To create a new setting profile, click the **Add** button. The **Add settings** page opens.
- To edit an existing setting profile, click it. The **Edit settings** page opens.
- Select the **Anti-Theft** section. Use the toggle to enable or disable the anti-theft feature.
- Click **Save**.

For more information about the anti-theft actions available in Panda Endpoint Protection Plus, see *General section for mobile devices on page 238*.

Anti-theft protection settings

Field	Description
Report the device's location	Panda Endpoint Protection Plus uses the device GPS to get its GPS coordinates and send them to the Panda Endpoint Protection Plus server. If this feature is unavailable, it tries to get them through Wi-Fi or the carrier communication infrastructure. To enable or disable this option, use the toggle.
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 is taken and sent by email to the email addresses entered in the text box. You can enter multiple addresses separated by a comma. To enable or disable this option, use the toggle.
Privacy	Enables users to enable private mode. Private mode disables geolocation tracking. To enable or disable this option, use the toggle.

Table 12.2: Anti-theft features for Android devices

Security settings for iOS devices

Accessing the settings

- From the top menu, select **Settings**.
- From the side menu, select **Mobile devices**.
- Select the **iOS devices** tab. Click **Add**. The **Add settings** page opens.

Required permissions

Permission	Access type
Configure security for mobile devices	Create, edit, delete, copy, or assign settings profiles for iOS devices.
View security settings for mobile devices	View the settings profiles for iOS devices defined.
Use the anti-theft protection for mobile devices	Send actions to target mobile devices to prevent data loss, locate them in the event of loss or theft, and lock them.

Table 12.3: Permissions required to access the iOS device security settings

Antivirus for web browsers

The antivirus protection for iOS devices scans the URLs that the device connects to to prevent the installation of malware apps and phishing attacks.

To enable detection of malware and phishing URLs, enable the toggles.

This feature is not available for iOS devices not enrolled into an MDM solution. See *Installation on iOS systems* on page 142.

Exclusions

You can exclude certain URLs and domains from scans. In the text box, type the URLs and domains that you want to exclude.

Anti-theft

The anti-theft feature enables you to send actions to target iOS devices to prevent data loss or locate them in the event of loss or theft.

Accessing the anti-theft protection

- From the top menu, select **Settings**. From the side menu, select **Mobile devices**.
- Select the **iOS devices** tab. A list opens and shows all created settings profiles.
- To create a new setting profile, click the **Add** button. The **Add settings** page opens.
- To edit an existing setting profile, click it. The **Edit settings** page opens.
- Select the **Anti-Theft** section. To enable or disable the anti-theft feature, use the toggle.
- Click **Save**.

For more information about the anti-theft actions available in Panda Endpoint Protection Plus, see *General section for mobile devices on page 238*.

Anti-theft protection settings

Field	Description
Behavior	Panda Endpoint Protection Plus uses the device GPS to get its GPS coordinates and send them to the Panda Endpoint Protection Plus server. If this feature is unavailable, it tries to get them through Wi-Fi or the carrier communication infrastructure. To enable or disable this option, use the toggle.
Privacy	Enables users to enable private mode. Private mode disables geolocation tracking. To enable or disable this option, use the toggle.

Table 12.4: Anti-theft features for iOS devices

Web access control

This protection enables you to limit access to specific web content categories and configure a list of URLs to allow and deny access to.

This feature is not available for iOS devices not enrolled into an MDM solution. See *Installation on iOS systems on page 142*.

Namely, web access control enables you to:

- Select the days and hours when you want to enable web access control.
- Deny access to specific web pages.
- Configure lists of allowed/denied addresses and domains.
- Keep a database of the URLs accessed from each computer.

Enabling web access control

- From the top menu, select **Settings**.
- From the side menu, select **Mobile devices**.
- Select the **iOS devices** tab.
- Click **Add**.
- Select the **Web access control** section.

To enable or disable the feature, click the **Enable web access control** toggle.

Configuring time periods for web access control

This option enables you to limit access to certain website categories and denied sites during business hours and authorize it during non-business hours and weekends.

To specify when you want to enable web access control, select the **Enable only during the following times** option.

On the calendar, select the days and hours when you want to enable web access control.

- Click the day to select the whole day.
- Click and drag the squares to select multiple days and times.
- To select all times every day of the month, click the **Select all** button.
- Click **Clear** to disable web access control for all of the times selected.

Click the **Save** button.

Denying access to specific web pages

Panda Endpoint Protection Plus groups the web pages it classifies into 160 content categories. To prevent users from accessing a specific set of web pages:

- Select the web page categories.
- In the upper-right corner of the page, click **Save**.

To select all categories, click **Select all**. To clear all selections, click **Clear**.

If a user visits a web page that belongs to a forbidden category, a warning page appears that indicates that access is denied and the reason.

Denying access to pages categorized as unknown

To **Deny access to pages categorized as unknown**, select the toggle.

> *Internal and intranet sites accessible on ports 80 and 8080 could be categorized as unknown. To avoid this, add exclusions for internal pages you want to allow.*

List of allowed/denied addresses and domains

You can set a list of pages that are always allowed (allowlist) or blocked (blocklist), regardless of the category that they belong to:

- In the text box, enter the URL of the relevant IP address or domain. Press **Enter**. The URL appears inside a tag.
- To add another domain or address, click **Add URL**.
- To edit the list, use the **Copy** and **Clear** buttons. These buttons appear when you point the mouse to the text box.
- To save the settings profile, click **Save** in the upper-right corner of the page.

URL matches can be full or partial. With long URLs, it is enough to enter the beginning of the URL in the text box to allow/block all URLs that start with the entered characters.

Chapter 13

Panda Patch Management (Updating vulnerable programs)

Panda Patch Management is a built-in module on Aether platform that finds computers on the network with known software vulnerabilities and updates them centrally and automatically. It minimizes the attack surface and prevents malware attacks on vulnerable workstations and servers.

Panda Patch Management supports Windows, macOS, and Linux operating systems. It detects both third-party applications with missing patches or in EOL (end of life), as well as all patches and updates published by Microsoft for all of its products (operating systems, databases, Office applications, etc.).

For more information about the vendors and applications supported by Patch Management, see https://info.pandasecurity.com/patchmanagementapp/?type=windows.

Panda Patch Management does not support Extended Security Updates (ESU licenses). These licenses enable you to run Microsoft products past the end of support. For more information about ESU licenses, their availability, and end dates, see https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates.

For more information about the Panda Patch Management module, see:

Creating and managing settings profiles on page 267: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

Accessing, controlling, and monitoring the management console on page 53: Managing user accounts and assigning permissions.

Managing lists on page 41: Information about how to manage lists.

Chapter contents

Panda Patch Management features

You can access the features provided by Panda Patch Management from these sections in the management console:

- **To configure the discovery of missing patches**: Go to the **Patch management** settings section (top menu **Settings**, side panel **Patch management**). For more information, see Configuring the discovery of missing patches.
- **To configure patch exclusions**: Go to the **Available patches** list. For more information, see Exclude patches for all or certain computers.
- **To have visibility into the update status of the entire IT network**: Go to the **Patch Management** dashboard (top menu **Status**, side panel). For more information, see Patch management status.
- **To view lists of missing patches**: Check the **Patch management status**, **Available patches**, and **End-of-Life programs** lists (top menu **Status**, side panel **My lists - Add**). For more information, see Panda Patch Management module lists.
- **To view a history of all installed patches**: Check the **Installation history** list (top menu **Status**, side panel **My lists - Add**). For more information, see Installation history.
- **To patch computers**: From the **Tasks** top menu, create an **Install patches** scheduled task. You can also patch computers from the context menus in the group tree available from the **Computers** top

menu, from lists, and from **Computer details**. For more information, see Download and install patches.

- **To exclude computers from patch installation tasks**: You can exclude computers and computer groups from patch installation tasks. The ability to exclude computers from patch installation tasks is a feature aimed at service providers that use Panda Partner Center to manage multiple customers.

  For more information, see **Security product settings** in the Panda Partner Center Administration Guide.

- **To patch test computers**: When you configure Patch Management, you can designate test computers to install patches on and verify the installation results before you install the patches on the other computers on the network. To designate test computers:

  - Create a Panda Patch Management settings profile. From the **Patch installation** drop-down menu, select **Designate as test computers and install patches**. Assign the settings profile to the computers you want to designate as test computers. For more information, see Patch installation.
  - Create a Panda Patch Management task. Enable the **Run the task only on test computers** toggle. For more information, see Configuring a patch installation task.

- **To uninstall patches**: Choose one of these options:

  - From the **Last patch installation tasks** widget, click the **View installation history** link. For more information, see Last patch installation tasks.
  - From the top menu, select **Status**. Click **My lists - Add**. Select the **Installation history** list. For more information, see Installation history.
  - From the top menu, select **Tasks**. Select the task that installed the patch you want to uninstall. Click **View installed patches**.

- Click the patch you want to uninstall. A page opens and shows the patch details and the **Uninstall** button if the patch supports this option. For more information, see Uninstalling a patch.

Panda Patch Management requirements

On 30 June 2025, our Windows and Mac protection for these OS versions will become End of Life (EOL): Windows XP, Vista, Server 2003, Server 2008 (Windows 2008 R2 will continue to be supported)and macOS Yosemite, El Capitán, Sierra, High Sierra and Mojave. After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

Supported Windows operating systems

Workstations

- 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)
- Windows 11 (64-bit)

Servers

- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2, and 2016
- Windows Server 2022

Support for Windows ARM-based computers

Panda Patch Management is partially compatible with Windows ARM systems:

- Detects 32-bit and 64-bit patches.
- Installs only 32-bit patches.
- Does not detect operating system patches.

These limitations do not apply to Linux or Mac computers.

Supported macOS operating systems

- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura
- macOS Sonoma

Installing operating system patches on Apple Silicon macOS computers

To install operating system patches on these computers, the computer user must enter their user name and password. The user has three attempts to enter valid credentials. After the patch is installed, the computer restarts automatically.

If the installation task includes other patches that do not require credentials, they install normally. See Installing operating system patches on macOS computers.

Supported Linux operating systems

Supported 64-bit distributions:

- **Red Hat**: 7.0 and higher; 8.0 and higher.
- **CentOS**: 7.0 and higher.
- **SUSE Linux Enterprise**: 12.0 and higher; 15.0 and higher.

To install patches correctly, make sure the computer repository settings have not been modified and point to the distribution vendor servers.

Unsupported computers

On computers not compatible with Panda Patch Management:

- Panda Patch Management does not install.
- Computers keep the Panda Patch Management settings profiles and tasks assigned to them, but they are not applied.
- The **Available patches** list does not show information about these computers or about the status of the patches installed.
- These computers do not count toward the number of Panda Patch Management licenses used.
- The installation history reports previous installations of Panda Patch Management as **Not available**.

Required URLs

- https://content.ivanti.com
- https://application.ivanti.com
- https://stlicense.ivanti.com
- https://help.ivanti.com
- https://license.shavlik.com

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 these steps:

- Make sure Panda Patch Management works correctly on the protected computers on your network.
- Make sure that all published patches are installed.
- Install the selected patches.
- Uninstall any patches that are causing malfunction problems (rollback).
- Exclude patches for all or certain computers.
- Make sure the programs installed on your computers are not in EOL (End-Of-Life) stage.
- Regularly check the history of patch and update installations.
- Regularly check the patch status of those computers where incidents have been recorded.

Make sure that Panda Patch Management works correctly

Follow these steps:

- 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 are to receive the patches have the Windows Update service running with automatic updates disabled.

> *Enable the **Disable Windows Update on computers** toggle in the patch management settings profile for Panda Endpoint Protection Plus to manage the service correctly. For more information, see General options.*
> *On devices running Windows 10 and higher, the operating system enables you to defer quality updates but not disable them. Therefore, these updates will be applied after 30 days despite you select **Disable Windows Update on computers**.*

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**, **My organization** tab in the side panel). Click the context menu of the computer group. Select **View available patches**. The Available patches list opens, filtered by the relevant group.

  Or,

    - Go to the computer list (top menu **Computers**). Click a computer's context menu. Select **View available patches**. The Available patches list opens, filtered by the relevant computer.
- To get an overview of all missing patches:
    - Go to **Status** in the top menu. Click **Add** in the **My lists** section of the side panel. Select the Available patches list.
    - Use the filter tool to narrow your search.
- To find computers that do not have a specific patch installed:
    - Go to **Status** in the top menu. Click **Add** in the **My lists** section of the side panel. Select the Available patches list.
    - Use the filter tool to narrow your search.
    - Click the context menu of the specific computer-patch you want to look for and select the option **View which computers have the patch available**.

Download and install patches

To install patches and updates, Panda Patch Management uses the task infrastructure implemented in Panda Endpoint Protection Plus.

Requirements

Patches released by Microsoft are installed using the Windows Update service on the target workstation or server. However, to prevent Panda Patch Management from overlapping with the Windows Update service, the latter should be configured to be inactive on the computer. See General options

Required permissions

The user account used to access the web console must have the **Install, uninstall, and exclude patches** permission assigned to its role. For more information about the permissions system, see Managing roles and permissions on page 65.

Patch download and bandwidth savings

Before the solution installs a patch, the computer downloads it from the software vendor. The download occurs in the background on each computer when a patch installation task starts. To minimize bandwidth usage, the solution uses cache computers on the network to download and disseminate patches and updates.

Limits to downloading patches from proxy and cache computers

Patches can be downloaded directly from the Internet and also through a Panda Endpoint Protection Plus proxy or cache computer. See Configuring downloads from cache computers on page 286 and Configuring proxies lists for Internet access on page 284.

There are limitations to using one method or another, depending on the computer operating system:

- **Computers with a Windows or macOS operating system**: They can download patches from cache computers and the Internet. They cannot download patches from the Panda Endpoint Protection Plus proxy.
- **Computers with a Linux operating system**: Linux computers use the distribution package manager to download patches from the Internet. They cannot download patches from the Panda Endpoint Protection Plus proxy or cache computers.

Cache computers store patches for up to 30 days, after which patches are deleted. If a computer requests a patch from a cache computer, but the cache computer does not have the patch in its repository, the computer waits for the cache computer to download it. The wait time depends on the size of the patch to download. If the cache computer cannot download the patch, the target computer tries to download the patch instead.

After patches are applied to a target computer, they are deleted from the storage media.

Types of patch installation tasks

- **Quick (Install option)**: Downloads and installs the patch in real time but does not restart the computer, even if the installation requires a restart. Quick tasks start to download patches as soon as you create the task. This can result in high bandwidth usage if the task applies to many computers or the patches are large.

- **Scheduled (Schedule installation option):** Enables you to configure all settings related to the patch installation and start the task when you want. If the start time of multiple tasks coincides, the solution delays tasks up to 2 minutes to prevent simultaneous downloads and minimize bandwidth usage.

Interrupting patch installation tasks

You can cancel patch installation tasks if the installation process has not started yet on the target computers. If the installation process has already begun, however, you cannot cancel the task as doing so could cause errors on computers.

Patches corresponding to the operating system

Even if you set a computer with an incompatible operating system as the target for a specific patch, computers receive only patches that correspond to their operating systems.

Installing operating system patches on macOS computers

Some operating system patches for macOS computers require that the computer restart to complete patch installation, regardless of the restart options you select when configuring the patch installation task.

These patches contain new features, bug fixes, and enhancements for the operating system installed, but do not upgrade the operating system to a higher version. You can identify these patches because they include the text *SoftwareUpdate* in their name. This name appears on the **Detected patch** page and in the **Available patches** list.

Warning messages

Because installing these patches restarts the computer automatically, a warning message is shown to you and the computer user in these circumstances:

- When you select any of these patches from the list of available patches to create a quick or scheduled task. If you accept the message, the task runs (quick task), or you are taken to the task settings (scheduled task). See From the Available patches list.
- When you select **macOS** from **Install patches for the following products** upon configuring a patch installation task. A warning message appears for you to confirm whether you want to include those patches in the task. This option is disabled by default. See Configuring a patch installation task.
- The target computer for the task shows a message to the computer user informing that a patch installation task is in progress and the computer will restart.

Installation on Apple macOS computers

With Apple macOS computers, you must enter the volume owner user name and password to install operating system patches.

- **If the credentials are correct**: The **Installation** column in the **Available patches** list shows the **Pending restart** text. When patch installation is complete, the computer restarts automatically and the patch disappears from the list.

- **If the computer user cancels the installation**: The computer shows an error code on the task results page. See Task results on page 591.

> *If the patch installation task for a macOS computer includes patches that do not require credentials, the patches proceed to install.*

Installation on Intel macOS computers

In this case, you do not need to enter any credentials. The target computer for the task shows a message to the computer user informing that a patch installation task is in progress.

> *Because you cannot postpone the automatic restart, we recommend that you close and save any open files.*

Patch installation in the console

From the Available patches list

- From the top menu, select **Status**.
- In the **My lists** section of the side panel, click **Add**. Select Available patches
- Use the filter tool to narrow your search.
- Select the checkboxes for the computers/patches you want to install.
- To create a quick task, select **Install** in the toolbar. To create a scheduled task, select **Schedule installation**. For more information about how to configure a scheduled task, see Configuring a patch installation task.

> *If the patches you select to install include operating system patches for macOS that require the computer to automatically restart, a warning message appears. See Installing operating system patches on macOS computers*

From the Available patches by computers list

- From the top menu, select **Status**.
- In the **My lists** section of the side panel, click **Add**. Select Available patches by computers.
- Use the filter tool to narrow your search.
- Click the context menu associated with the patch. A list appears and shows the Available patches. See From the Available patches list.

From the computer tree

- From the top menu, select **Computers**. From the left panel, select the **My organization** tab in the computer tree.
- To install patches on a group of computers, click the group context menu. Select **View available patches**. A list appears and shows the Available patches. See From the Available patches list.
- To schedule the installation of patches on a group of computers, click the group context menu. Select **Schedule patch installation**. A new patch installation task is created. For more information about how to configure it, see Configuring a patch installation task.

From the computer tree list

- From the top menu, select **Computers**. From the left panel, select the **My organization** tab in the computer tree.
- Select the group of computers. Select the checkboxes for the computers you want to patch.
- If you selected a single computer, click the computer context menu. Select **View available patches**. If you selected more than one, select **View available patches** in the toolbar above. A list appears and shows the Available patches. See From the Available patches list.
- To schedule installation of groups of patches, if you selected a single computer, click the computer context menu. Select **Schedule patch installation**. If you selected more than one, select **Schedule patch installation** in the toolbar above. A new patch installation task is created. For more information about how to configure it, see Configuring a patch installation task.

From the Tasks menu

From the top menu, select **Tasks**. Click **Add task**. Select **Install patches**.

Configuring a patch installation task

- Enter general details of the task in the **Name** and **Description** fields.
- If no recipients are defined, click the **No recipients selected** link in the **Recipients** section. A page opens where you can select the computers that will receive the configured task.

> *To access the computer selection page, you must first save the task. If you did not save the task, a warning message appears.*

- If you want to send the patch installation task only to computers you designated as test computers on your network, enable the **Run the task only on test computers** toggle. You designate a computer as a test computer in the Panda Patch Management settings profile you assign to it. See Panda Patch Management features.
- Select the types of computers you want to receive the task: **Workstation**, **Laptop**, or **Server**.

- Click ⊕ to add individual computers or computer groups. Click 🗑 to remove them.
- On the **Edit task** page, click the **View computers** button to view the computers that will receive the task.
- Schedule the task. You can configure these parameters:
  - **Starts:** Indicates the task start date/time.

Value	Description
As soon as possible (selected)	The task runs 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 in the **If the computer is turned off** section
As soon as possible (cleared)	The task runs on the date selected in the calendar. Specify whether the time is based on the computer local time or the Panda Endpoint Protection Plus server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task does not run. The task scheduler enables you to establish the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** Define a time interval during which the task will run if the computer becomes available. • **Run when the computer is turned on:** There is no time limit. The solution waits indefinitely for the computer to be available to run the task.

Table 13.1: Task execution parameters

  - **Frequency**: Set a repeat interval (every day, week, month, or year) from the date specified in the **Starts:** field.

Value	Description
One time	The task runs only once at the time specified in the **Starts:** field.
Daily	The task runs every day at the time specified in the **Starts:** field.

Value	Description
Weekly	Use the checkboxes to select the days of the week on which the task must run, at the time specified in the **Starts:** field.
Monthly	Choose an option: • Run the task on a specific day of every month. If you select the 29th, 30th, or 31st of the month, and the month does not have that day, the task runs on the last day of the month. • Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 13.2: Task frequency parameters

- In **Security patches**, select the criticality or importance of the patches to install.
- In **Install patches for the following products**, specify which products to install patches for. The product tree appears ordered by operating systems. Each operating system contains the patches that are available for it. Specify which products are to receive patches by selecting the relevant checkboxes in the product tree.

If the patches you select to install include operating system patches for macOS that require the computer to automatically restart, a message appears for you to confirm whether you want to include those patches in the task. See Installing operating system patches on macOS computers

Because the product tree is a dynamic resource that changes over time, keep these rules in mind when you select items from the tree:

- When you select a node, you also select all of its child nodes and all items dependent on them. For example, when you select Adobe you also select all nodes below that node.
- If you select a node, and Panda Patch Management automatically adds a child node to that branch, that node is selected as well. For example, as previously explained, selecting Adobe also selects all of its child nodes. Additionally, if, later, Panda Patch Management adds a new program or family to the Adobe group, that program or family is selected as well. Conversely, if you manually select a number of child nodes from the Adobe group, and later Panda Patch Management adds a new child node to the group, this is not automatically selected.
- The programs to patch are evaluated at the time when tasks run, not at the time when they are created or configured. For example, if Panda Patch Management adds an entry to the tree after you have created a patch task, and that entry is selected automatically in

accordance with the aforementioned mechanism, the task installs the patches associated with that new program when it runs.

- In the **Restart options** section, select an option to specify whether computers must restart automatically after patches install.
    - **Do not restart automatically**: If you select this option, users see a message indicating that their computer must restart and can select whether to restart **immediately** or **later**. If the latter is selected, a reminder appears 24 hours later.

      Computers with a Linux operating system without a GUI are sent a message reminding of the need to restart to complete the patch installation.

    - **Automatically restart workstations only**: Select the time interval to restart workstations. At the end of the set time, the agent shows the computer user a reminder message with the **Restart now** button and a countdown timer indicating how much time they have left before the computer restarts.

      Computers with a Linux operating system without a GUI are sent a message informing of the time remaining until the restart.

      As the restart approaches, you are no longer able to close the notification message. Every 30 minutes, the message appears on screen to remind the user of the need to restart. When the countdown finishes, the computer restarts automatically.

    - **Automatically restart servers only**: This option behaves in the same way as **Automatically restart workstations only**, but applies to servers only.
    - **Automatically restart both workstations and servers**: This option behaves in the same way as **Automatically restart workstations only**, but applies to both workstations and servers.
- Click **Save**. The task is added to the list of configured tasks. However, it shows the **Unpublished** label, meaning that it is not yet active.
- To publish a task, click the **Publish** button. The task is added to the Panda Endpoint Protection Plus task scheduler, which runs it in accordance with its settings.

When two or more patch installation tasks that require a restart overlap in time, Panda Endpoint Protection Plus restarts the computer when indicated by the task whose restart interval is closer in time. This avoids postponing the computer restart indefinitely if multiple successive patch installation tasks are chained together.

Lower versions of the security software

Lower versions of Panda Endpoint Protection Plus that do not support the feature of setting the restart interval set it to 4 hours automatically.

If the recipient computers have a lower version of the security software installed, they might not correctly interpret frequency settings. These computers interpret the task frequency settings as follows:

- **Daily tasks**: Unchanged.
- **Weekly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 7 days.
- **Monthly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 30 days.

Download patches manually

In some cases, Panda Endpoint Protection Plus cannot get a download URL to install a patch automatically. This can occur for several reasons:

- The patch requires payment, is not a publicly available patch, or requires user registration to download.
- Patches protected by an EULA cannot be downloaded and distributed by Panda Security.

In such cases, Panda Patch Management provides a link to manually download the patch. If the link is not helpful, contact the vendor of the software to patch.

For these patches, you can download the patch manually and add it to the patch repository so other computers can install it.

You cannot download patches manually on Linux or macOS computers or devices.

To manually add a patch to the repository, you must have the download URL of the patch. To install patches that require manual download, follow these steps:

- Identify patches that you must manually download.
- Get the patch download URL from the vendor and download the patch.

- Add the downloaded patch to the patch repository.
- Mark the patch as manually downloaded and available to install.
- Optional: Disable a manually downloaded patch for installation.

Identify patches that require manual download

- From the top menu, select **Status**. In the **My lists** side panel, click **Add**. A dialog box opens that shows all available lists.
- Select the **Available patches** list. Configure these filters:
  - **Installation**: Requires manual download.
  - **Show non-downloadable patches**: Yes.
- Click the **Launch query** button. The list shows all patches that computers on the network require which Panda Patch Management cannot download automatically.

Get the download URL and download the patch

- After following the steps in the previous section, in the Identify patches that require manual download list, click a patch that requires manual download. The **Patch detected** page opens and shows details of the patch.
- Note the file name shown in the **Patch details** section. To download the patch, click the **Download URL** link.

Add the downloaded patch to the patch repository

- Identify a computer on the network that has Panda Endpoint Protection Plus installed and has the cache role. Copy the downloaded file to this path on the cache computer:

```
C:\ProgramData\Panda Security\Panda Aether
Agent\Repository\ManuallyDeploy.
```

If you installed Panda Endpoint Protection Plus on a computer drive that differs from the default installation drive, copy the file to:
X:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy
Where X is the drive where the repository is located. For more information, see Specifying the storage drive on page 283.

- If the **ManuallyDeploy** folder does not exist, create it with read and write administrator permissions.
- If needed, rename the downloaded file to match the File Name you noted in the Get the download URL and download the patch section.

Mark the patch as Manually downloaded

- After you copy the patch to the repository, go to the **Available patches** list. Click the context menu associated with the patch.
- From the drop-down menu, select **Mark as manually downloaded**. After you mark a patch as manually downloaded, its status changes from **Requires manual download** to **Pending (manually downloaded)** for all computers that need to install it and the patch can be installed like an automatically downloaded patch. For more information, see Download and install patches.

> *Panda Patch Management does not check whether there are patches with the **Pending (manually downloaded)** status on cache computers, or whether computers on the network that require a patch have a cache computer assigned that has the patch in its repository. You must make sure that cache computers used for patch downloads have all necessary manually downloaded files in the **ManuallyDeploy** folder.*

Disable a manually downloaded patch for installation

If you no longer want a manually downloaded patch to be available to install, you can disable the patch for installation. To disable a manually downloaded patch for installation:

- Go to the **Available patches** list and configure a filter with these characteristics:
  - **Installation**: Pending (manually downloaded).
  - **Show non-downloadable patches**: Yes.
- Click the **Filter** button. The list shows all patches manually downloaded and enabled for installation.
- Click the context menu of any patches you want to disable installation for. Select **Mark as 'Requires manual download'**. The patch disappears from the repository of installable patches, and you cannot install it.

Uninstall problematic patches

Sometimes, the patches published by software vendors do not work correctly, which can lead to serious problems. This can be avoided by selecting a small number of test computers prior to deploying a patch across the entire network. In addition to this, Panda Patch Management also enables you to remove (roll back) installed patches.

Linux and macOS do not support patch uninstallation.

Requirements for uninstalling an installed patch

- You must have the **Install/Uninstall patches** permission enabled. See Install, uninstall, and exclude patches on page 71 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 page. There are three ways to do this:
  - Go to the **Status** menu at the top of the console. Click **My lists - Add** in the side panel. Select Installation history
  - Go to the **Tasks** menu at the top of the console. Select the task that installed the patch you want to uninstall. Click the **View installed patches** link in the upper-right corner of the page.
  - Access the Last patch installation tasks widget. To do this, go to the **Status** menu at the top of the console and select **Patch Management** from the side menu. Click **Installation history**.
- From the list displayed, select the patch you want to uninstall.
- If the patch can be removed, the **Uninstall the patch** button is displayed. Click the button. The computer selection window appears.
  - Select **Uninstall from all computers** to remove the patch from all computers on the network.
  - Select **Uninstall from "{{hostName}}" only** to remove the patch from the selected computer only.
- Panda Patch Management creates an immediate execution task to uninstall the patch.
- If a restart is required to finish uninstalling the patch, the solution waits for the user to restart it manually.

An uninstalled patch is displayed again in the list of available patches unless it is excluded. If a scheduled patch installation task has been configured and the patch has not been excluded, it will be reinstalled on the next execution. However, if a patch is withdrawn by the corresponding vendor, it will no longer be shown or installed. See Exclude patches for all or certain computers for more information.

Check the result of patch installation/uninstallation tasks

Go to the **Tasks** menu at the top of the console to view those tasks in which patches have been installed or uninstalled from computers. Both provide a **View results** option that enables you view on which computers the action was taken and which patches were installed/uninstalled. See Patch installation/uninstallation task results and View installed/uninstalled patches for more information.

Exclude patches for all or certain computers

You have the option to prevent the installation of malfunctioning patches or patches that significantly change the characteristics of the target program. This is called excluding the patch. To do this, follow these steps:

- Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** menu on the left. Click the **Available patches** list. This list displays a line for each computer-available patch pair. An available patch is a patch that has not been installed yet on a specific computer or has been uninstalled from it.
- To exclude a single patch, click the context menu associated with the patch. Select the **Exclude** option. A window opens for you to select the exclusion type.
    - **Exclude for X only**: Excludes the patch for the selected computer only.
    - **Exclude for all computers**: Excludes the patch for all computers on the network.
- To exclude several patches and/or a single patch for multiple computers, select them using the relevant checkboxes. From the action bar, choose **Exclude**. A window opens for you to select the exclusion type.
    - **Exclude for the selected computers only**: Excludes the patches for the selected computers only.
    - **Exclude for all computers**: Excludes the patches for all computers on the network.

> *When you exclude a patch, you exclude a specific version of the patch. That is, if you exclude a patch, and later the software vendor releases a later version of that patch, this is not automatically excluded.*

Make sure the programs installed are not in EOL (End-Of-Life) stage

Programs in EOL (End-Of-Life) stage do not receive any type of update from the relevant software vendor, therefore it is advisable to replace them with an equivalent program or a more advanced version.

Follow these steps to find those programs on the network that have reached their EOL or will reach it shortly:

- Go to the **Status** menu at the top of the console. Select **Patch Management** from the side panel.
- Find 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**. Click **Add** in the **My lists** section in the side panel.
- Select End-of-Life programs.

The list displays a line for each computer-EOL program combination found.

Check the history of patch and update installations

To find out if a specific patch is installed on the computers on your network:

- Go to top menu **Status**. Click **Add** in the **My lists** section in the side panel.
- Select Installation history.

The list displays a line for each computer/installed patch combination found, with information about the affected program's or operating system's name and version, and the patch criticality/type.

Click a computer's context menu to display a number of options that enable you to:

- View the patch installation or uninstallation task.
- View all patches installed on the computer.
- View all computers that have the selected patch installed.

Check the patch status of computers with incidents

Panda Patch Management correlates those computers where incidents have been recorded with their patch status so that you can determine whether an infected computer or a computer where threats have been detected has missing patches.

To check whether a computer where an incident has been detected has missing patches:

- Go to top menu **Status**, in the widget **Threats detected by the antivirus**, click a computer or incident. Information about the threat detected on the computer is displayed.
- In the **Affected computer** section, click the **View available patches** button. The **Available patches** list opens, 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.

> *Because the patching process may require downloading patches from the software vendor's servers and therefore delay their application, it is advisable to isolate any infected computer that needs patching and shows network traffic in the threat's life cycle. This minimizes the risk of spreading the infection to other computers on the corporate network while the patch operation is taking place. See Forensic analysis for more details of the malware life cycle and Isolating one or more computers from the organization's network for more information.*

Configuring the discovery of missing patches

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Patch management**.
- Click the **Add** button. The settings page opens.

Required permissions

Permission	Access type
Patch management	Create, edit, delete, copy, or assign patch management settings profiles.
View patch management settings	View patch management settings profiles.

Table 13.3: Permissions required to access the patch management settings

General options

- Enter a name and description for the settings profile.
- To make sure that Panda Patch Management manages Windows updates on your computers, enable the **Disable Windows Update on computers** toggle.

> *On devices running Windows 10 and higher, the operating system enables you to defer quality updates, but not disable them. Therefore, these updates are applied after 30 days despite you select* ***Disable Windows Update on computers****.*

- Click **Save**.
- From the list of profiles, select the profile you created. The **Edit settings** page opens. To select the computers you want to assign the settings profile to, click the **Recipients (No recipients selected)** link.
- To add computers individually, click . To remove them, click .
- On the **Edit settings** page, enable the **Automatically search for patches** toggle to enable patch search functionality.If the toggle is not enabled, patch management lists do not show missing patches, although you can use patch installation tasks to install missing patches on computers.

Patch installation

When you configure Patch Management, you can select different patch installation options to apply to recipient computers and computer groups:

- **Install patches:** Installs patches on recipient computers and computer groups.
- **Designate as test computers and install patches**: Identifies recipient computers and computer groups as test computers for patch installation. For more information, see Panda Patch Management features.
- **Do not install patches**: Does not install patches on recipient computers or computer groups. This option is applicable to service providers who purchased Panda Partner Center. For more information, see **Security produc settings** chapter in Administration Guide of Panda Partner Center.

Search frequency

Search for patches with the following frequency specifies how often Panda Patch Management searches the cloud-based patch database to check for missing patches for your computers.

Patch criticality

Specifies the importance (or criticality) of the patches that Panda Patch Management searches for in the databases of available patches.

Windows Service Packs are not applied to macOS or Linux computers or devices.

Software vendors define the importance of the security patches they make available to address vulnerabilities. Patch classifications are not universal and vary by vendor. To determine whether you want to

install a patch, we recommend that you review its description, especially for patches that a vendor does not classify as Critical.

> *The **Other patches** category includes patches with bug fixes and feature enhancements for macOS and Linux.*

Panda Patch Management widgets/panels

Accessing the dashboard

To access the dashboard, select the **Status** menu at the top of the console. Select Panda Patch Management from the side menu.

Required permissions

Permissions	Access to widgets
No permissions	• Patch management status • Time since last check
Install, uninstall, and exclude patches	• End-of-Life programs • Available patches • Last patch installation tasks
View available patches	• End-of-Life programs • Available patches • Last patch installation tasks

Table 13.4: Permissions required to access the Patch management widgets

Patch management status

Shows computers where Panda Patch Management is working correctly and computers 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 provides a graphical representation and percentage of computers with the same status.

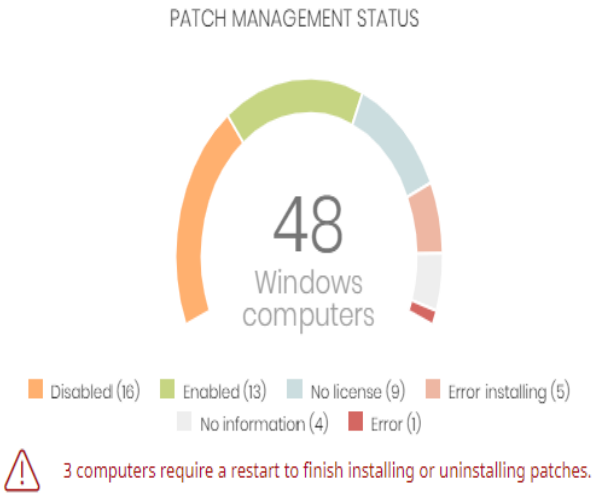


Figure 13.1: Patch management status panel

Meaning of the data displayed

Data	Description
Enabled	Panda Patch Management installed successfully, runs with no issues, and the assigned settings enable the module to search for patches automatically.
Disabled	Panda Patch Management installed successfully, runs with no issues, but the assigned settings do not enable the module to search for patches automatically.
No license	Computers that are compatible with Panda Patch Management, but do not have a Panda Endpoint Protection Plus license assigned.
Error installing	The module could not install.
No information	The computer has a license, but has not yet reported status to the server, or has an outdated agent installed.
Error	Panda Patch Management does not respond to requests sent from the server, or has settings that are different from those configured in the web console.
Central area	Shows the total number of computers compatible with the Panda Patch Management module.
Pending restart	Shows the number of computers that require a restart to finish installing or uninstalling patches.

Table 13.5: Description of the data displayed in the Patch management status panel

Lists accessible from the panel

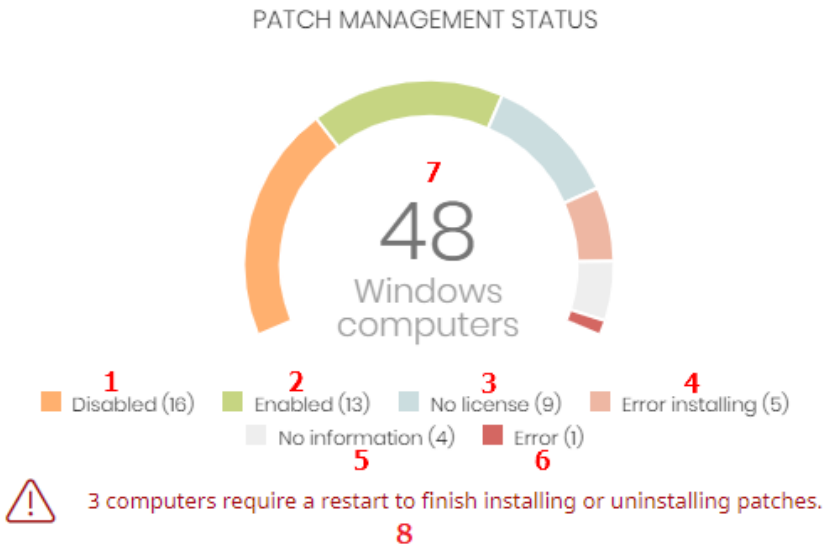


Figure 13.2: Hotspots in the Patch management status panel

Click the hotspots shown in Figure 13.2: 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. The computer does not have a Panda Endpoint Protection Plus license assigned.
(4)	Patch management status = Error installing.
(5)	Patch management status = No information.
(6)	Patch management status = Error.
(7)	No filter.
(8)	Patch management status = Pending restart.

Table 13.6: Filters available in the Patch management status list

Time since last check

Shows the number of computers that have not connected to the Panda Security cloud and reported patch status for more than 3, 7, and 30 days. Use this panel to identify computers that might be at risk and require

your attention.

Figure 13.3: Time since last check panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported patch status in the last 72 hours.
7 days	Number of computers that have not reported patch status in the last 7 days.
30 days	Number of computers that have not reported patch status in the last 30 days.

Table 13.7: Description of the data displayed in the Time since last check panel

Lists accessible from the panel

Figure 13.4: Hotspots in the Time since last check panel

Click the hotspots shown in Figure 13.4: to open the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago and Patch management status = Enabled or Disabled or No information or Error.
(2)	Last connection = More than 7 days ago and Patch management status = Enabled or Disabled or No information or Error.
(3)	Last connection = More than 30 days ago and Patch management status =

Hotspot	Filter
	Enabled or Disabled or No information or Error.

Table 13.8: Filters available in the Patch management status list

End-of-Life programs

Shows information about programs that have reached or are close to end-of-life, grouped by end-of-life date.

Figure 13.5: End-of-Life programs panel

Meaning of the data displayed

Data	Description
Currently in EOL	Programs that have reached end-of-life.
In EOL (currently or in 1 year)	Programs that have reached end-of-life or will in the next year.
With known EOL date	Programs that have a known end-of-life date more than one year in the future.

Table 13.9: Description of the data displayed in the End-of-Life programs panel

Lists accessible from the panel

Figure 13.6: Hotspots in the End-of-Life programs panel

Click the hotspots shown in Figure 13.6: to open 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 13.10: Filters available in the End-of-Life programs list

Last patch installation tasks

See Task management on page 588 for more information about how to modify an existing task.

Lists recently created patch installation tasks and shows their status. Use the options in this widget to manage patch installation tasks:

Figure 13.7: Last patch installation tasks panel

- To edit a task, click its name.
- To view all tasks in the **Tasks** page, click **View all**.
- To view details of all patch installation tasks, click **View installation history**.
- Click the context menu next to a task to display a drop-down menu with the following options:
  - **Cancel**: Cancels the task before it starts to install patches on the target computer.
  - **View results**: Shows the results of a task.

Available patches trend

Shows the evolution of the number of patches that are pending installation on the computers on the network, grouped by severity.

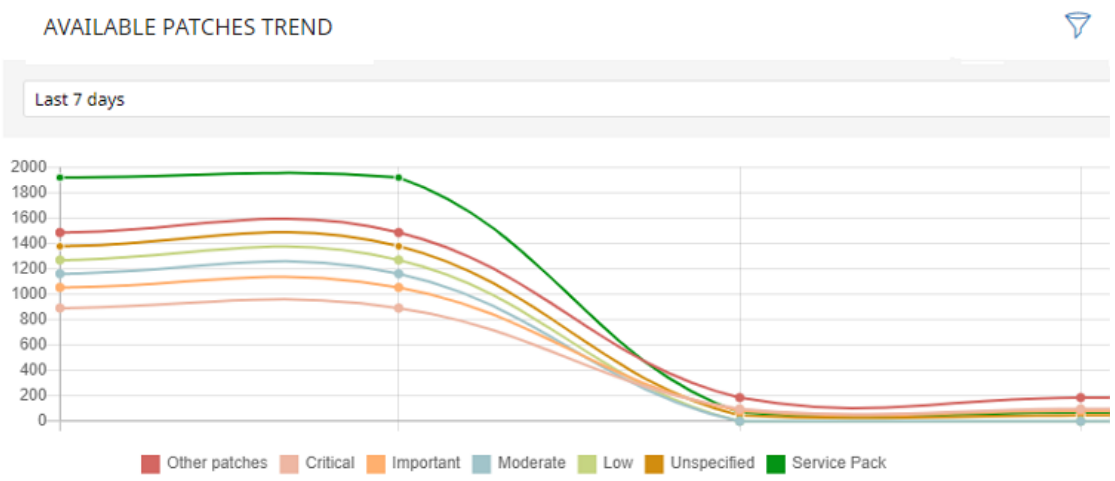


Figure 13.8: Available patches trend graph

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as 'Critical' and pending application.
Security patches - Important	Number of security patches classified as 'Important' and pending application.
Security patches - Low	Number of security patches classified as 'Low' and pending application.
Security patches - Unspecified	Number of security patches that do not have a severity classification and are pending application.
Other patches (non-security related)	Number of patches not related to security that are pending application.
Service Packs	Number of patch and hotfix bundles that are missing from computers. Not applicable for Linux or macOS computers.

Table 13.11: Description of the data displayed in the Availabre patches trend panel

Point to a node on the graph to display a tooltip with the following information:

- Date
- Type
- Number of patches

Lists accessible from the panel

Click the legend items under the graph to open the Available patches list filtered by the selected item. Click the graph to open the full Available patches list with no filters applied.

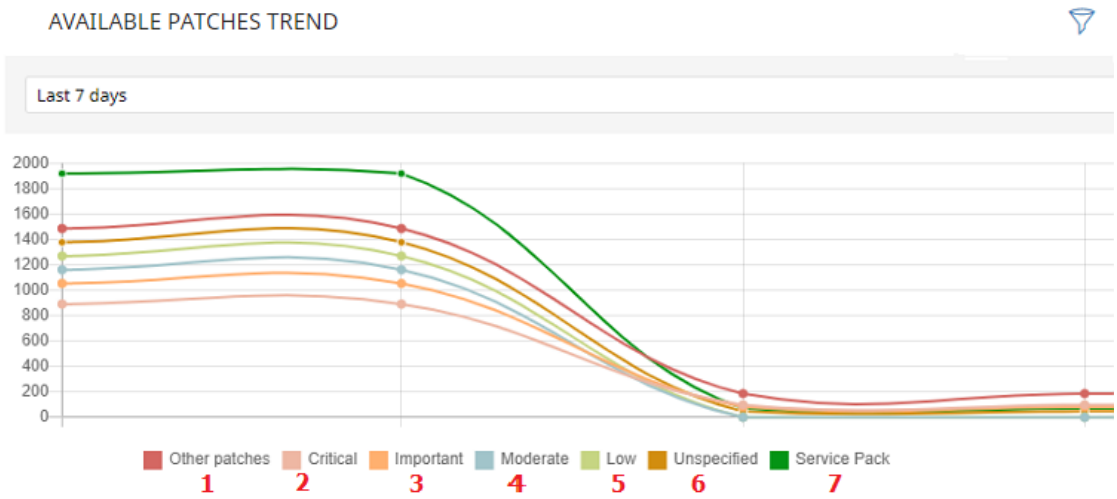


Figure 13.9: Hotspots in the Available patches trend panel

Hotspot	Filter
(1)	Criticality = Other patches (non-security-related).
(2)	Criticality = Critical (security-related).
(3)	Criticality = Important (security-related).
(4)	Criticality = Moderate (security-related).
(5)	Criticality = Low (security-related).
(6)	Criticality = Unspecified (security-related).
(9)	Criticality = Service Pack.

Table 13.12: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation

Filter	Definition
	• Laptop • Server
Platform	Operating system installed on the computer.
Operating system patches	Patches available for Windows operating systems.
App patches	Patches available for apps. For a full list of the apps supported by Panda Patch Management, see https://info.pandasecurity.com/patchmanagementapp/. For more information about how to select the apps you want to patch, see Configuring a patch installation task.

Table 13.13: Filters available in the Available patches trend widget

Available patches

Shows the number of patches of different types that are available for computers on the network. Numbers in this widget count the same patch multiple times if multiple computers do not have the patch installed.

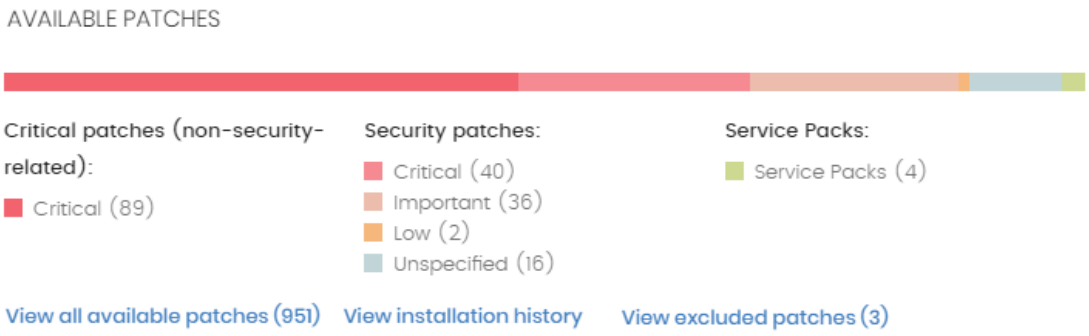


Figure 13.10: Available patches panel

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as 'Critical' and pending application.
Security patches - Important	Number of security patches classified as 'Important' and pending application.

Data	Description
Security patches - Low	Number of security patches classified as 'Low' and pending application.
Security patches - Unspecified	Number of security patches that do not have a severity classification and are pending application.
Other patches (non-security related)	Number of patches not related to security that are pending application.
Service Packs	Number of patch and hotfix bundles that are pending application.
View all available patches	Number of patches of all types that are pending application.
View excluded patches	Number of patches excluded from installation.

Table 13.14: Description of the data displayed in the Availabre patches trend panel

Lists accessible from the panel

Figure 13.11: Hotspots in the Available patches panel

Click the hotspots shown in Description of the data displayed in the Availabre patches trend panel to open the **Available patches** list with the following predefined filters:

Hotspot	List	Filter
(1)	Available patches	Criticality = Critical (security-related).
(2)	Available patches	Criticality = Important (security-related).
(3)	Available patches	Criticality = Low (security-related).
(4)	Available patches	Criticality = Unspecified (security-related).

Hotspot	List	Filter
(5)	Available patches	Criticality = Other patches (non-security-related).
(6)	Available patches	Criticality = Service Pack.
(7)	Available patches	No filter.
(8)	Installation history	No filter.
(9)	Excluded patches	No filter.

Table 13.15: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.
Operating system patches	Patches available for Windows operating systems.
App patches	Patches available for apps. For a full list of the apps supported by Panda Patch Management, see https://info.pandasecurity.com/patchmanagementapp/. For more information about how to select the apps you want to patch, see Configuring a patch installation task.

Table 13.16: Filters available in the Available patches trend widget

Most available patches for computers

Lists available patches and the number of devices the patch is available for (is in **Pending** or **Pending restart** status).

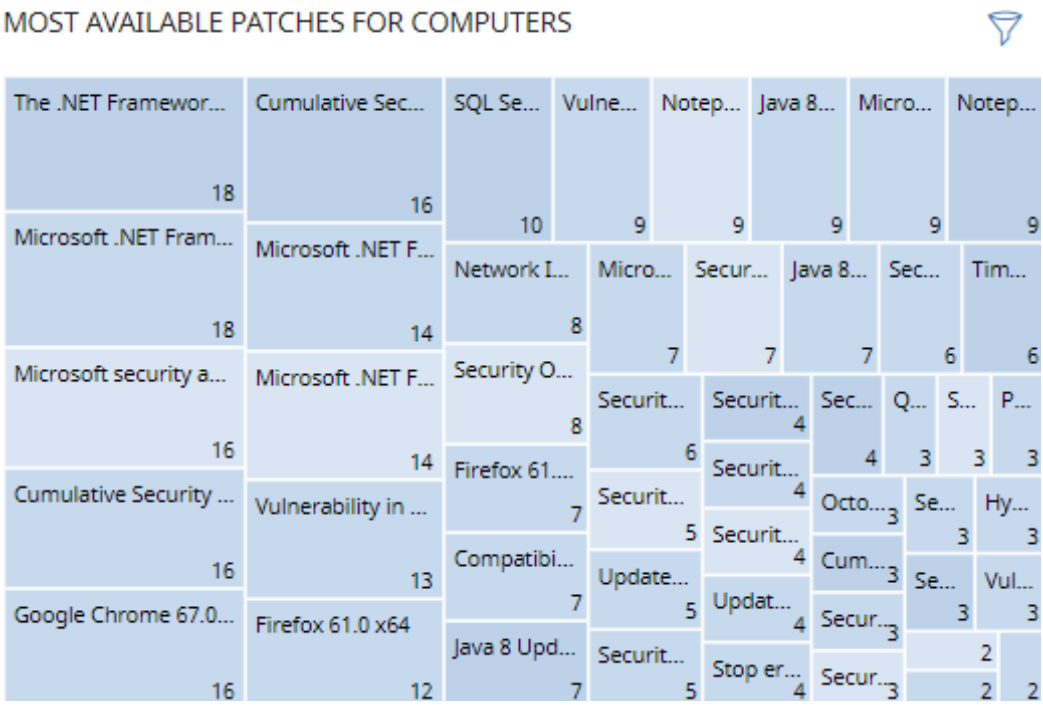


Figure 13.12: Most available patches for computers panel

Meaning of the data displayed

Data	Description
Patch name	Name of the available patch.
Number of computers	Number of computers the patch is available for (is in **Pending** or **Pending restart** status).
View all available patches link	Access to the Available patches by computers full list.

Table 13.17: Description of the data displayed in the Most available patches for computers panel

Point to a box in the widget to see a summary of the patch, including:

- Patch name.
- Number of affected computers.
- Program (or operating system family).
- Criticality.
- Release date.
- CVE (Common Vulnerabilities and Exposures) ID.

Lists accessible from the panel

Click a box in the panel to open the **Available patches** list filtered to the selected patch.

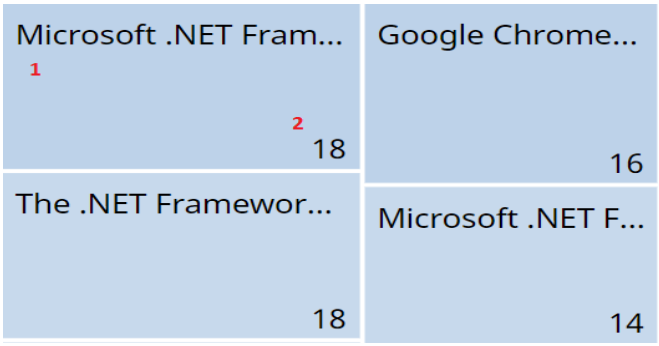


Figure 13.13: Hotspots in the Most available patches for computers panel

Hotspot	Filter
(1)	Patch = Name of the selected patch

Table 13.18: Lists available from the Most available patches for computers panel

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS

Filter	Description	Values
Patch type	Type of software affected by the patch.	• App patches • Operating system patches

Table 13.19: Filters available in the Most available patches for computers panel

Computers with most available patches

Lists the devices that are missing patches, as well as the number of patches the device is missing.

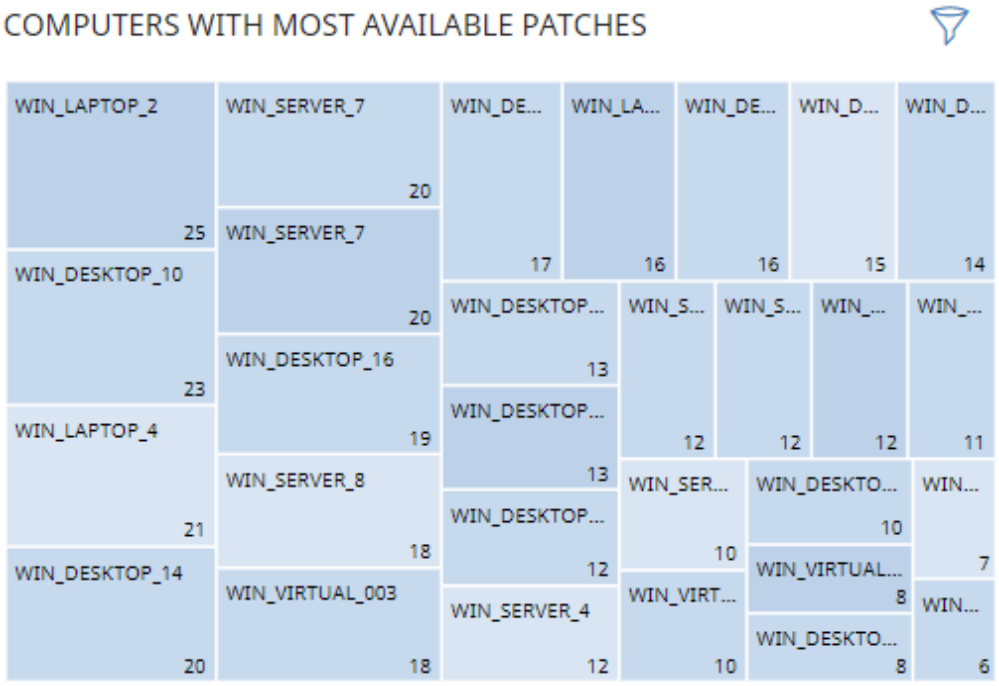


Figure 13.14: Computers with most available patches panel

Meaning of the data displayed

Data	Description
Name	Name of the computer that has patches available.
Number of computers	Number of patches available for the computer.

Table 13.20: Description of the data displayed in the Computers with most available patches panel

Point to a box in the widget to see the following information:

- Computer name.
- Number of patches the computer is missing.

Lists accessible from the panel

Click a box in the panel to open the **Available patches** list filtered to the selected computer.

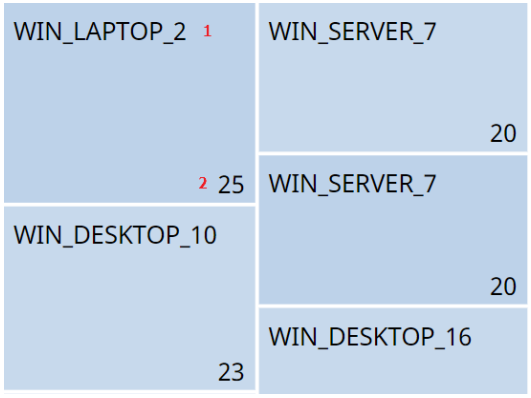


Figure 13.15: Hotspots in the Computers with most available patches panel

Hotspot	Filter
(1)	Computer = Name of the selected computer

Table 13.21: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see the available filters:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server

Filter	Description	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Windows operating system patches

Table 13.22: Filters available in the Computers with most available patches panel

Programs with most available patches

Lists the programs that are missing most patches, as well as the number of patches the program is missing

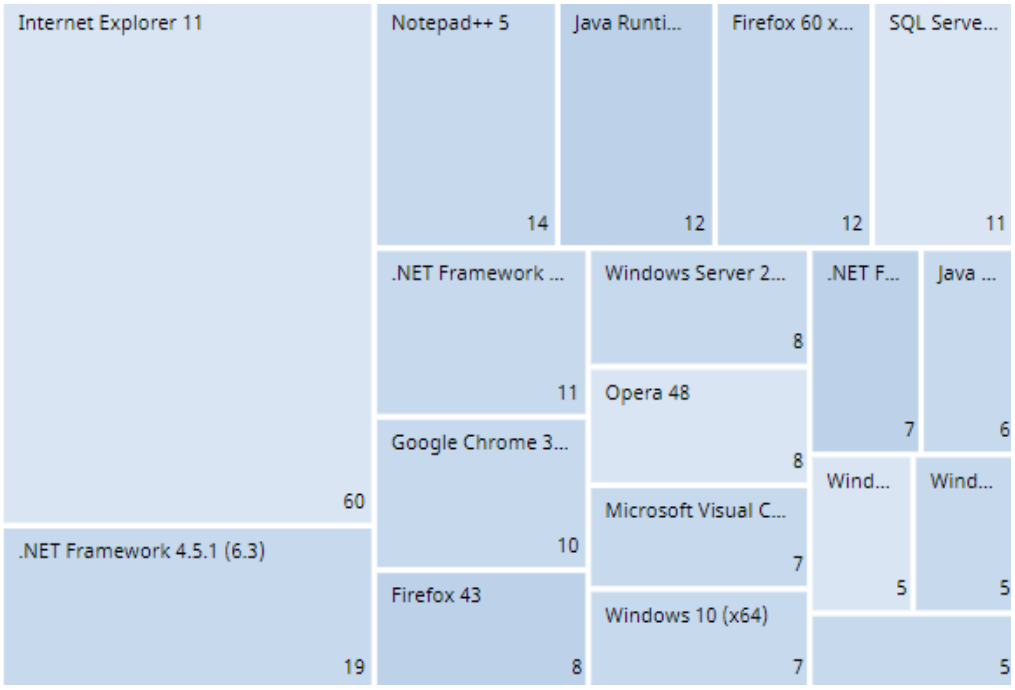


Figure 13.16: Programs with most available patches panel

Meaning of the data displayed

Data	Description
Patch name	Program name.

Data	Description
Number of computers	Number of patches the program is missing.

Table 13.23: Description of the data displayed in the Programs with most available patches panel

Point to a box in the widget to see the following information:

- Program name.
- Number of patches the program is missing.

Lists accessible from the panel

Click a box in the panel to open the **Available patches** list filtered to the selected computer.

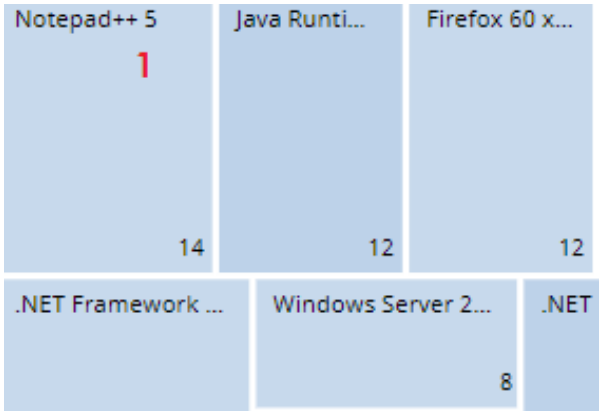


Figure 13.17: Hotspots in the Programs with most available patches panel

Hotspot	Filter
(1)	Program = Name of the selected program

Table 13.24: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see the available filters:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related)

Filter	Description	Values
		• Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Windows operating system patches

Table 13.25: Filters available in the Programs with most available patches panel

Panda Patch Management module lists

Accessing the lists

There are two ways to access the lists:

- From the top menu, select **Status**. From the side menu, select **Patch Management**. Click the relevant widget.

  Or,

- From the top menu, select **Status**. From the side menu, click the **Add** link. A window opens that shows the available lists.
- From the **Patch management** section, select a list to view the associated template. Edit it and click **Save**. The list is added to the side menu.

You can access the patch installation and uninstallation lists from the **Last patch installation tasks** widget by clicking **View installation history**.

You can access the **Patch installation/uninstallation task results** and **View installed/uninstalled patches** lists from the top menu **Tasks** by clicking **View results** in a patch installation or uninstallation task.

Required permissions

Permissions	Access to lists
No permissions	• Patch management status.
Install, uninstall, and exclude patches	Access to lists and context menus to install and uninstall patches: • Available patches. • Installation history. • End-of-Life programs. • Excluded patches. • Patch installation/uninstallation task results. • View installed/uninstalled patches.
View available patches	Read-only access to lists: • Available patches. • Installation history. • End-of-Life programs. • Excluded patches. • Patch installation/uninstallation task results. • View installed/uninstalled patches. • Available patches trend. • Most available patches for computers. • Computers with most available patches. • Programs with most available patches.

Table 13.26: Permissions required to access the Patch Management lists

Patch management status

This list shows all computers on the network that are compatible with Panda Patch Management (with filters that enable you to identify workstations and servers that are not using the service due to the reasons shown in the associated panel).

Field	Comment	Values
Computer	Computer name.	Character string
Computer status	Agent reinstallation: • Reinstalling the agent. • Agent reinstallation error. Protection reinstallation: • Reinstalling the protection. • Protection reinstallation error. • Pending restart. Computer isolation status: • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated. “RDP attack containment” mode: • Computer in “RDP attack containment” mode. • Ending "RDP attack containment" mode. Patch installation • Do not install patches • Designate as test computers and install patches	Icon
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Patch management	Module status.	• Enabled • Disabled • Installation error (failure reason)

Field	Comment	Values
		• 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 Plus status was last sent to the Panda Security cloud.	Date

Table 13.27: Fields in the Patch Management Status list

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Patch installation	Patch installation option applied to the computer: • Patch installation enabled: The computer has Patch Management enabled. Patch Management installs patches on the computer.	Enumeration

Field	Comment	Values
	• Test computer for patch installation: The computer has Patch Management enabled and is designated as a test computer for patch installation. • Patch installation disabled: The computer has Patch Management disabled. Patch Management does not install patches on the computer.	
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
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether the protection module installed on the computer is updated to the latest version or not.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date the signature file was last updated.	Date
Patch management status.	Module status.	• Enabled • Disabled • Error installing • No license • No information • Error

Field	Comment	Values
Requires restart	The computer requires a reboot to finish installing or uninstalling one or more downloaded patches.	Boolean
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date
Installation error date	Date of the unsuccessful attempt to install Panda Patch Management.	Date
Installation error	Reason for the installation error.	• Download error • Execution error

Table 13.28: Fields in the Patch Management Status exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	• All • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the agent last connected to the Panda	Date

Field	Comment	Values
	Security cloud.	
Pending restart to complete patch installation or uninstallation	The computer requires a reboot to finish installing or uninstalling one or more patches.	Boolean
Patch installation	Patch installation option.	• Patch installation enabled • Test computer for patch installation • Patch installation disabled
Patch management status.	Module status.	• Enabled • Disabled • Error • Error installing • No license • No information

Table 13.29: Filters available in the Patch Management Status list

Computer details page

Click a row in the list to open the computer details page. For more information, see Computer details on page 236.

Available patches

This list shows all missing patches on the network computers and information about patches in the process of installation. Each line in the list corresponds to a patch/computer pair.

Field	Comment	Values
Computer	Name of the computer with outdated software and patch installation option assigned to the computer in the Panda Patch Management settings: • Do not install patches	Character string

Field	Comment	Values
	• Designate as test computers and install patches	
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Indicates the patch installation status: • **Pending**: The patch is available for the computer but has	Enumeration

Field	Comment	Values
	not been installed yet. • **Requires manual download**: The patch must be manually downloaded and copied to a cache computer by the administrator. For more information, see Download patches manually. • **Pending (manually downloaded)**: The patch was downloaded manually and is already included in the patch repository. For more information, see Download patches manually. • **Pending restart**: The patch was installed but the computer was not restarted. Some patches might not be applied until the computer is restarted.	
Context menu	Shows an action menu: • **Install**: Create a quick task to immediately install the patch on the computer. • **Schedule installation**: Create a scheduled task to install the patch on the computer. • **Exclude**: Select the computers for which you want to exclude the patch. • **View all available patches for the computer**: Shows all available patches for the computer that have not been installed yet. • **View which computers have the patch available**: Shows all computers that have the patch available for installation.	Enumeration

Table 13.30: Fields in the Available Patches list

Fields displayed in the exported file

Use the context menu to export the data. The export file can include all data in the list of available patches or a smaller version that shows the trend of the number of available patches in the last 7 days, the last month, or the last year.

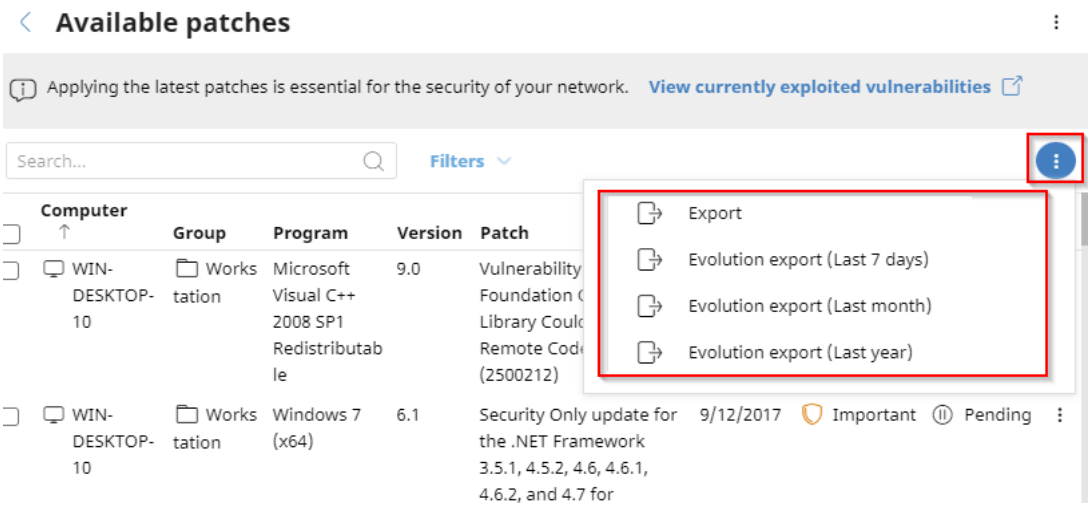


Figure 13.18: Context menu for data export

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer with outdated software.	Character string
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Patch installation	Patch installation option applied to the computer.	• Patch

Field	Comment	Values
		installation enabled • Test computer for patch installation • Patch installation disabled
Vendor	The company that created the outdated program.	Character string
Product family	Name of the product with patches pending installation or a reboot.	Character string
Program version	Version number of the outdated program.	Numeric value
Program	Name of the outdated program or operating system version 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)

Field	Comment	Values
		• Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch 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 whether the patch is available for download or requires an additional support contract with the software vendor to access it.	Boolean
Download size (KB)	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
Status	Indicates the patch installation status: • **Pending**: The patch is available for the computer but has not been installed yet. • **Pending (manually downloaded)**: The patch was downloaded manually and is already included in the patch repository. For more information, see Download patches manually. • **Requires manual download**: The patch must be manually downloaded and copied to a cache	Enumeration

Field	Comment	Values
	computer by the administrator. For more information, see Download patches manually.	
File name	Name of the file that contains the patch.	Character string
Download URL	HTTP resource in the software vendor infrastructure to download the patch.	Character string

Table 13.31: Fields in the Available Patches exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch release	Date when the patch was released and made available for download.	• All • Less than 7 days ago • Less than 14 days ago • Less than 1 month ago • Less than 2 months ago • More than 7 days ago • More than 14 days ago • More than 1 month ago • More than 2 months ago

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Patch type	Type of patch.	• App patches • Operating system patches
Search computer	Computer name.	Character string
Computer	Name of the computer with outdated software.	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Program, family, or vendor	The search applies to the selected program, product family, or company.	Character string
Patch installation	Patch installation option.	• Patch installation enabled • Test computer for patch installation • Patch installation disabled
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related)

Field	Comment	Values
		• Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Shows patches that are in the process of installation, filtering them by the installation stage they are in.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Show non-downloadable patches	Shows patches that cannot be directly downloaded by Panda Patch Management because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.).	Boolean

Table 13.32: Filters available in the Available Patches list

Detected patch page

Click a row in the list. The **Detected patch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the computer.

This page can provide this content:

- Information about the available patch and the **Install patch** button.
- Information about the patch in the process of installation. The text **Pending restart** appears next to the **Install patch** button.

Click the **Install patch** button. A dialog box opens for you to select the recipients of the patch installation task:

- **Install on the current computer only**: The task is performed on the computer selected in the list.
- **Install on all computers in the selected filter**: Select a filter from the filter tree shown. The patch is installed on all computers in the selected filter.
- **Install on all computers**: The patch is installed on all computers on the network.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Program version	Version number of the outdated program.	Character string
Family	Name of the product with patches pending installation or a reboot.	Character string
Vendor	The company that created the outdated program.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string

Field	Comment	Values
Computer	Name of the computer with outdated software.	Character string
Installation status	Indicates whether the patch is already included in the repository that contains the patches to be applied to computers or must be manually downloaded and added to the patch repository by the administrator.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Download URL	URL for downloading the patch individually.	Character string
File name	Name of the file that contains the patch.	Character string
Description	Information about the impact the vulnerability could have on computers.	Character string

Table 13.33: Fields on the Detected Patch page

Available patches by computers

This list shows available patches and the number of computers each patch is available for.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Field	Comment	Values
Program	Name of the outdated program or operating system version with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computers	Number of computers the patch is available for.	Numeric value
Context menu	**View which computers have the patch available**: Shows all computers that have the patch available for installation.	

Table 13.34: Fields in the Available Patches by Computers list

Fields displayed in the exported file

Use the context menu to export the data. The export file can include all data in the list of available patches or a smaller version that shows the trend of the number of available patches in the last 7 days, the last month, or the last year.

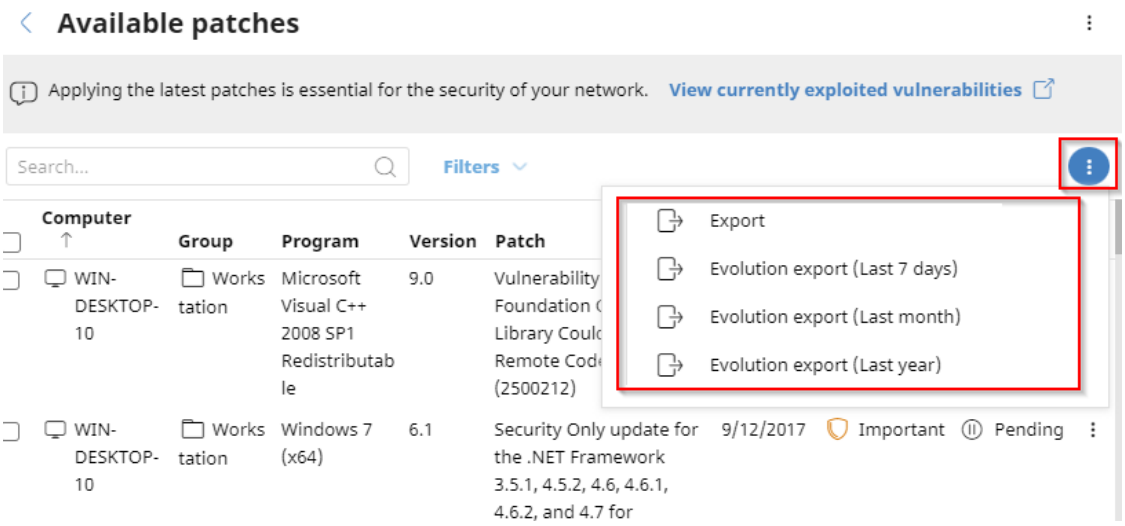


Figure 13.19: Context menu for data export

Field	Comment	Values
Vendor	The company that created the outdated program.	Character string
Product family	Name of the product with patches pending installation or a reboot.	Character string
Program version	Version number of the outdated program.	Numeric value
Program	Name of the out-of-date program or operating system version 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)

Field	Comment	Values
		• Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Computers	Number of computers the patch is available for.	Numeric value
Platform	Operating system installed on the computer.	• Windows • macOS • Linux

Table 13.35: Fields in the Available Patches by Computers exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server

Field	Comment	Values
Patch type	Type of patch.	• App patches • Operating system patches
Search computer	Computer name.	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Select a program version, family, or vendor	The search applies to the selected program, product family, or company.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Show non-	Shows patches that cannot be directly downloaded	Boolean

Field	Comment	Values
downloadable patches	by Panda Patch Management because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.).	

Table 13.36: Filters available in the Available Patches by Computers list

Detected patch page

Click a row in the list. The **Detected patch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the computer. See Detected patch page.

Installation history

This list shows the operations performed by Panda Patch Management on the computers on the network in the specified time period.

Field	Comment	Values
Date	Date the operation was logged.	Date
Computer	Computer name.	Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Program	Program name or operating system version.	Character string
Version	Program or operating system version.	Character string
Patch	Patch name.	Character string
Criticality	Severity rating of the patch.	• Other patches • Critical • Important • Moderate • Low • Unspecified

Field	Comment	Values
		• Service Pack
Installation	Status of the logged operation.	• Installed • Requires restart • The patch is no longer required • Uninstalled (requires restart) • Error
Context menu ⋮	Shows a drop-down menu with options.	• **View task**: Shows the settings of the task associated with the logged operation. • **View patches installed on the computer**: Shows all patches installed on the selected computer. • **View computers with the patch installed**: Shows all computers that have the selected patch installed.

Table 13.37: Fields in the Installation History list

Fields displayed in the exported file

Use the context menu to export the data. You can download a detailed file that includes all data in the list or a reduced version. In either case, the file contains information about the patches installed in the selected time period.

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string

Field	Comment	Values
Domain	Domain the computer belongs to.	Character string
Description		Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Date	Date of the logged operation.	Date
Program	Program name or operating system version.	Character string
Version	Program or operating system version.	Character string
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the 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 that describes the vulnerability associated with the patch.	Character string

Field	Comment	Values
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Installation	Indicates whether the patch is already included in the repository that contains the patches to be applied to computers or must be manually downloaded and added to the patch repository by the administrator.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Installation error	The Panda Patch Management module did not install correctly.	• **Unable to download**: Installer not available • **Unable to download**: The file is corrupted • **Not enough disk space** • Installation error • Download error
Download URL	URL for downloading the patch individually.	Character string
Result code	Operation result code. See the vendor documentation for information about result codes.	Numeric value
Task name	Name of the patch installation task. This column appears only in the extended export.	Character string
Task launch date	Date when the Panda Patch Management task associated with the computer was scheduled to run. This column appears only in the extended export.	Date

Field	Comment	Values
Task start date	Date when the Panda Patch Management task associated with the computer started to run. This column appears only in the extended export.	Date
Task end date	Date when the Panda Patch Management task associated with the computer finished to run. This column appears only in the extended export.	Date

Table 13.38: Fields in the Installation History exported file

Filter tool

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Search computer	Computer name.	Character string
Date	Time period in which the patches were installed.	• Last 24 hours • Last 7 days • Last month • Custom range
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related)

Field	Comment	Values
		• Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Status of the logged operation.	• Installed • Requires restart • The patch is no longer required • Uninstalled (requires restart) • Error • Download error • Installation error
Program	Program name or operating system version.	Character string
Patch	Name of the installed patch.	Character string
Installation Attempts	Shows all failed patch installation attempts or only the latest attempt.	• Show only the latest attempt • Show all attempts

Field	Comment	Values
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string

Table 13.39: Filters available in the Installation History list

Installed patch page

Click a row in the list. The **Installed patch** page opens and shows details of the logged operation. This data might vary depending on the operating system installed on the computer.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the out-of-date program or operating system version.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string

Field	Comment	Values
Computer	Computer name.	Character string
Installation date	Date the operation was logged.	Date
Result	Status of the logged operation.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled • Installation error • Download error
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 13.40: Fields on the Installed Patch page

End-of-Life programs

This list shows programs that are no longer supported by the relevant vendor. These programs are particularly vulnerable to malware and other security threats.

Field	Comment	Values
Computer	Name of the computer with EOL software.	Character string
Group	Folder in the Panda Endpoint Protection Plus 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 reached its end of life.	Date (in red if the program reached its end of life)

Table 13.41: Fields in the End-of-Life Programs list

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string

Field	Comment	Values
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program reached its end of life.	Date
Last seen	Date when the computer was last discovered.	Date

Table 13.42: Fields in the End-of-Life Programs exported file

Filter tool

Field	Comment	Values
Search computer	Computer name.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
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 13.43: Filters available in the End-of-Life Programs list

Program details page

Click a row in the list. The **Program details** page opens.

Field	Comment	Values
Program	Name of the program or operating system version that	Character

Field	Comment	Values
	received the patch.	string
Family	Bundle, suite, or program group the software belongs to.	Character string
Publisher/Company	Company that designed or published the program.	Character string
Version	Program version.	Character string
EOL	Date when the program reached its end of life.	Date

Table 13.44: Fields on the Program Details page

Excluded patches

This list shows patches that you marked as excluded, preventing them from being installed on the computers on the organization network. The list shows a line for each computer-excluded patch pair, except for patches excluded for all computers on the network, for which a single line appears.

Field	Comment	Values
Computer	The content of this field varies depending on the target of the exclusion: If the patch was excluded for a single computer, the field shows the computer name. If the patch was excluded for all computers in the account, the text "(All)" is shown.	Character string
Group	Folder in the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-

Field	Comment	Values
		security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 13.45: Fields in the Excluded Patches list

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	The content of this field varies depending on the target of the exclusion: If the patch was excluded for a single computer, the field shows the computer name. If the patch was excluded for all computers in the account, the text "(All)" is shown.	Character string

Field	Comment	Values
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description	The computer description assigned by the network administrator.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related)

Field	Comment	Values
		• Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Download size (KB)	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 13.46: Fields in the Excluded Patches exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer for which patches were excluded.	Character string

Field	Comment	Values
Program	Name of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Show non-downloadable patches	Shows patches that cannot be directly downloaded by Panda Patch Management because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.).	Boolean
CVEs	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 13.47: Filters available in the Excluded Patches list

Excluded patch page

Click a row in the list. The **Excluded patch** page opens and shows details of the patch excluded from installation tasks. This data might vary depending on the operating system installed on the computer.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date and time the patch was excluded.	Numeric value
Release date	Date when the patch was released for download and application.	Date
KB ID	ID of the Microsoft Knowledge Base article that	Character string

Field	Comment	Values
	describes the vulnerability fixed by the patch and the patch requirements (if any).	
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 13.48: Fields on the Excluded Patch page

Patch installation/uninstallation task results

This list shows the results of the patch installation or uninstallation tasks performed on the computers on your network.

Field	Description	Values
Computer	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Panda Endpoint Protection Plus group the computer belongs to.	Character string
Status	Task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Patches installed/uninstalled	Number of patches installed/uninstalled.	Character string.
Start date	Date the installation task started.	Date

Field	Description	Values
End date	Date the installation task ended.	Date

Table 13.49: Fields in the Installation/Uninstallation Task Results list

Filter tool

Field	Description	Values
Status	Installation/uninstallation task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Applied/Uninstalled patches	Computers on which patches were installed/uninstalled.	• All • No patches installed/uninstalled • With patches installed/uninstalled

Table 13.50: Filters available in the Patch Installation/Uninstallation Task Results list

View installed/uninstalled patches

This list shows the patches installed/uninstalled from computers and other additional information.

Field	Description	Values
Computer	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Panda Endpoint Protection Plus group the computer belongs to.	Character string

Field	Description	Values
Program	Patched program.	Character string
Version	Program version.	Character string
Patch	Installed/uninstalled patch.	Character string
Criticality	Severity rating of the installed/uninstalled patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Result	Indicates whether the task was completed successfully or failed.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Date	Date the task ran.	Date

Table 13.51: Fields in the View Installed/Uninstalled Patches list

Chapter 14

Panda Full Encryption (Device encryption)

Panda Full Encryption is a built-in module on Aether platform that encrypts the content of the data storage media connected to the computers managed by Panda Endpoint Protection Plus. 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 certain versions of Windows 7 and higher and certain versions of macOS (see Supported Windows operating systems). It enables you to monitor the encryption status of network computers and centrally manage their recovery keys. It also takes advantage of hardware resources such as TPM chips, delivering great flexibility when it comes to choosing the optimum authentication system for each computer.

For more information about the Panda Full Encryption module, see:

Creating and managing settings profiles on page 267: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

Accessing, controlling, and monitoring the management console on page 53: Managing user accounts and assigning permissions.

Managing lists on page 41: Information about how to manage lists.

Chapter contents

Introduction to encryption concepts

Panda Full Encryption uses tools integrated in the Windows and macOS operating systems to manage encryption on network computers protected with Panda Endpoint Protection Plus.

To help you understand the processes involved in the encryption and decryption of information, we present some concepts related to the encryption technology we use.

TPM

TPM (Trusted Platform Module) is a chip installed on the motherboard of some desktops, laptops, and servers. Its main aim is to protect user sensitive data, stored passwords, and other information used in login processes.

TPM also detects any changes in the boot events of the computer, for example preventing access to a hard drive from a computer other than the one used for its encryption.

Panda Full Encryption supports TPM versions 1.2 and higher. If possible, use TPM technology along with other supported authentication systems. If you disabled the TPM chip in the BIOS settings of your computer, you might have to manually enable the chip from the BIOS.

Supported authentication types

Login password

On macOS operating systems, the authentication method used is a login password. Compatible with all macOS versions supported by Panda Full Encryption.

PIN

A PIN (Personal Identification Number) is a sequence of numbers that works as a simple password and is requested when you boot a computer that has an encrypted drive. Without the PIN, the boot sequence is not completed and you cannot access the computer. Compatible with all supported versions of Windows.

Extended PIN

If the hardware is compatible, Panda Full Encryption uses an extended or enhanced PIN which combines letters and numbers to increase the complexity of the password.

Because the extended PIN is requested in the computer boot process prior to loading the operating system, BIOS limitations might restrict keyboard input to the 7-bit ASCII table.

Additionally, on computers with a keyboard layout other than EN-US, such as QWERTZ or AZERTY keyboards, there can be errors when you enter the extended PIN. For this reason, Panda Full Encryption checks that the characters entered by the user belong to an EN-US keyboard layout, before setting the extended PIN for the computer encryption process.

Compatible with all supported versions of Windows.

Passphrase

A passphrase is similar to a password, but is typically longer. It consists of alphanumeric characters and is equivalent to the extended PIN.

Panda Full Encryption prompts users for different types of passwords based on these circumstances:

- Passphrase: If the computer has a TPM chip installed.
- Extended PIN: If the computer operating system and hardware support it.
- PIN: If the other options are not valid.

Only available on Windows 8 computers and higher without a TPM chip.

USB key

Enables you to store the encryption key on a USB device formatted with the NTFS, FAT, or FAT32 file system. With a USB key, you do not need to enter a password to boot the computer. However, the USB device with the startup password must be plugged into the computer USB port.

Required on Windows 7 computers without a TPM chip.

Some older PCs cannot access USB drives during the boot process. Verify whether the computers in your organization have access to USB drives from the BIOS.

Recovery key

When Panda Full Encryption detects unusual activity on a protected computer, it prompts the user to enter a BitLocker recovery key. This key is managed from the management console and must be entered to complete the boot process.

Panda Full Encryption stores the recovery keys for all encrypted computer drives that it manages. The management console does not show keys for computers encrypted by users or not managed by Panda Security.

The recovery key is requested in these scenarios:

- A user makes repeated attempts to enter an incorrect PIN or password while the device boots up.
- A Trusted Platform Module (TPM) chip detects a change in the boot sequence.
- Changes are made to the computer motherboard.
- Deletion or disablement of TPM content
- Changes are made to the computer boot 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 (Option ROM) in certain components that are part of the boot process (video cards, disk controllers, etc).
    - Changes to other components that are part of the initial boot phases.

BitLocker

BitLocker is software installed on some versions of Windows 7 and higher operating systems. It encrypts and decrypts the data stored on computer drives. If not already installed, Panda Full Encryption automatically installs BitLocker on supported drives and then manages the drives.

FileVault

FileVault is built-in software on macOS operating systems. It automatically encrypts all files in a computer hard disk or SSD memory.

System partition

On Windows operating systems, a system partition is a small area of the hard disk which remains unencrypted and is required for the computer to correctly complete the boot process. Panda Full Encryption automatically creates this system partition if it does not already exist.

Encryption algorithm

For Windows, the encryption algorithm Panda Full Encryption uses is AES (256-bit), although computers with drives encrypted by users using other algorithms are also compatible.

For macOS, the algorithm used is AES-XTS.

Panda Full Encryption service overview

The general encryption process covers several areas that you must be aware of to adequately manage network resources that could contain sensitive information or compromising data if a drive were to be lost or stolen:

- **Meeting minimum hardware and software requirements**: See Panda Full Encryption minimum requirements to see the limitations and specific conditions applicable to each supported platform.
- **Previous encryption status of the user computer**: Depending on whether BitLocker or FileVault is already being used on the user computer, the process of integration in Panda Full Encryption might vary slightly.
- **Assigning encryption settings profiles**: 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. For more information, see Encryption of unencrypted drives.
- **Viewing the encryption status of the network**: Through the widgets/panels in the **Status** menu, side panel **Panda Full Encryption**. For a complete description of the widgets included in Panda Full Encryption, see Panda Full Encryption module panels/widgets. Filters are also supported to find computers in lists according to their status. For more information, see Available filters.
- **Restriction of encryption permissions to security administrators**: The role system described in Understanding permissions on page 67 covers the encryption feature and the ability to view the encryption status of network computers.
- **Access to recovery keys**: Where the user forgets their password or PIN/passphrase, or when the TPM chip detects an irregular situation on a computer it protects, the network administrator can centrally obtain the recovery key and send it to the user. For more information, see Obtaining a recovery key.

General features of Panda Full Encryption

Supported authentication types

Panda Full Encryption supports various methods to authenticate encrypted disks. The operating system version and the presence of a Trusted Platform Module (TPM) chip determine the type of authentication to use. The supported authentication methods are (in the order we recommend them):

Windows

- **Security Processor (TPM) and Password**: Compatible with all supported versions of Microsoft Windows. The TPM chip must be enabled in the BIOS, and a PIN must be established.
- **Security Processor (TPM)**: Compatible with all supported versions of Microsoft Windows. The TPM chip must be enabled in the BIOS, except in Windows 10, where it is automatically enabled.

- **USB drive**: Requires a USB key and a computer that can read USB devices while booting. Required on Windows 7 computers without a TPM chip.
- **Password**: Only available on computers than run Windows 8 or higher without a TPM chip.

macOS

On macOS operating systems, the authentication method used is a login password. Compatible with all macOS versions supported by Panda Full Encryption. See Supported Windows operating systems.

By default, Panda Full Encryption uses an encryption method that includes the use of a TPM chip, if available. If you choose an authentication method not included in the above list, the management console shows a warning indicating that the computer will not be encrypted.

Supported storage devices

Panda Full Encryption supports these internal storage devices:

Windows and macOS

- Fixed storage drives on a computer (system and data).

Windows

- Used storage space on virtual hard drives (VHD).
- Removable hard drives.
- USB drives.

These storage devices are not supported:

- Dynamic hard drives.
- Small partitions.
- Other external storage devices.

Panda Full Encryption minimum requirements

The minimum requirements are divided into these categories:

- Supported Windows operating systems.
- Supported macOS operating systems.
- Hardware requirements for Windows computers.

On 30 June 2025, our Windows and Mac protection for these OS versions will become End of Life (EOL): Windows XP, Vista, Server 2003, and Server 2008 (Windows 2008 R2 will continue to be supported) and macOS Yosemite, El Capitán, Sierra, High Sierra and Mojave. After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

Supported Windows operating systems

- Microsoft Windows 7 (Ultimate, Enterprise)
- Microsoft Windows 8/8.1 (Pro, Enterprise)
- Microsoft Windows 10 (Pro, Enterprise, Education)
- Microsoft Windows 11 (Pro, Enterprise, Education)
- Windows Server 2008 R2, Windows Server 2012, and higher (includes Server Core editions)

Supported macOS operating systems

- macOS 10.15 Catalina
- macOS 11.0 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma

Hardware requirements for Windows computers

- Trusted Platform Module (TPM) 1.2 and higher (if used to authenticate).
- USB key and a computer that can read USB drives from the BIOS (Windows 7).

For macOS operating systems, there are no specific hardware requirements.

Management of computers according to their prior encryption status

Management of computers by Panda Full Encryption

For a computer on the network 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 received, at least once, a settings profile from the management console that establishes the encryption of its drives, and these have been encrypted successfully.

Computers that previously had some drives encrypted and have not received a settings profile to encrypt their drives are not managed by Panda Full Encryption and, therefore, the administrator does not have access to the recovery key or the status of the computer.

However, computers that have received a settings profile to encrypt their drives are managed by Panda Full Encryption regardless of their previous status (encrypted or not).

Uninstallation of the Panda Endpoint Protection Plus agent

Regardless of whether a computer is managed by Panda Full Encryption or not, if its drives are encrypted, when uninstalling Panda Endpoint Protection Plus they are left as they are. However, centralized access to the recovery key is lost.

If the computer is subsequently reinstated in Panda Endpoint Protection Plus, the last stored recovery key is displayed.

Encryption and decryption on Windows computers

Encryption of unencrypted drives

Encryption begins when the Panda Endpoint Protection Plus agent, installed on a computer, downloads encryption settings. A wizard on the computer guides the user through the encryption process.

The number of encryption steps to take depends on the type of authentication chosen by the network administrator and the previous status of the computer. If any of the steps fails, the agent reports it to the management console and the process stops.

You cannot encrypt computers from a remote desktop session. You must restart the computer and enter a password before the operating system is loaded, and this is not possible with a standard remote desktop tool

If there is a patch installation or uninstallation task in progress managed by Panda Full Encryption, the encryption process begins when that task has completed.

This section describes the entire encryption process, whether feedback is shown to the computer user, and whether a restart is required:

Step	Process on the computer	User interaction
1	The agent receives settings from the encryption module. The settings establish the encryption of drives.	None
2	If a computer is a server and does not have BitLocker installed, it is downloaded and installed.	The computer user is prompted to restart the computer to complete the install. If the user chooses to postpone the restart, they are prompted again during the next login. Requires restart.
3	If a computer has no previous encryption, a system partition is created.	The computer user must restart the computer to complete the creation of the partition. If the user chooses to postpone the restart, they are prompted again during the next login. Requires restart.
4	If a group policy exists that conflicts with the settings in Panda Full Encryption, an error message shows and the process stops. The group policies configured by Panda Full Encryption are: In the Local Group Policy Editor, navigate to: Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System	If you have not defined global group policies that conflict with the local policies defined by Panda Full Encryption, no message appears.

Step	Process on the computer	User interaction
	Drives. Select Not Set for the specified policies to avoid this error.	
5	If a computer has a TPM chip installed, the computer user might have to enable the TPM chip from the BIOS for the computer.	The computer must restart for the user to access the BIOS. On Windows 10 systems, you do not need to changer the BIOS settings but the restart is required. The restart in step 3, if required, combines with this one.
6	If a computer uses a USB device for authentication, prepare it.	The computer user must insert the USB device when the computer boots.
7	If a computer uses a PIN for authentication, prepare it.	The computer user must type the PIN. If alphanumeric characters are used and the hardware is not compatible with those characters, error -2144272180 appears. In that case, you must enter a numerical PIN.
8	If a computer uses a passphrase for authentication, prepare it.	The computer user must type the passphrase.
9	A recovery key is generated and sent to the Panda Security cloud. After it has been received, the process continues on the user computer.	None.
10	Check that the hardware on the computer is compatible with the encryption technology. The encryption process begins.	Restart the computer to check the hardware used in the various authentication methods. Requires restart.
11	Drive encryption.	The encryption process begins. It runs in the background, without any impact to users. The length of the process varies depending on the drive that is encrypted.

Step	Process on the computer	User interaction
		On average, encryption takes approximately 2-3 hours. Users can use and shut down computers normally. In the latter case, the process continues when the computer is restarted.
12	The encryption process takes place silently, without any impact to users.	Depending on the authentication method selected, the user might need to plug a USB key, enter a PIN, a passphrase, or nothing when the computer boots.

Table 14.1: Steps for encrypting unencrypted drives

Encryption of previously encrypted drives

If a computer already has encrypted drives, Panda Full Encryption modifies certain parameters so that the drives can be centrally managed. The actions taken are as follows:

- If a computer user selects an authentication method that differs from the method specified in the settings profile, a prompt shows on the user's computer that asks for passwords or other hardware resources. If it is not possible to use an authentication method compatible with the operating system, and specified by the network administrator, the existing encryption method remains in place. Panda Full Encryption does not manage the computer.
- If the encryption algorithm is not AES-256, Panda Full Encryption makes no encryption changes to the computer drive. Panda Full Encryption manages the computer.
- If both encrypted and unencrypted drives exist, ll drives are encrypted with the same authentication method.
- To unify authentication methods, if a previous authentication method requires a password, and the method is compatible with the authentication methods supported by Panda Full Encryption, a prompt shows on the user's computer that requests the password.
- If computer user encryption settings differ from those configured by the administrator, to minimize the encryption process, no changes are made.
- When you manage a drive with Panda Full Encryption, at the end of the process, Panda Security generates a recovery key and sends it to the Panda Security cloud.

Encryption of new drives

f you create a new drive entry after the encryption process is complete, Panda Full Encryption encrypts the drive immediately and according to the encryption settings.

Decrypting drives

There are three scenarios:

- If Panda Full Encryption uses settings to encrypt a computer, Panda Full Encryption can also decrypt it.
- If a computer was previously encrypted and the agent assigns encryption settings settings on install, Panda Full Encryption sees the computer as encrypted and you can use Panda Full Encryption settings to decrypt the computer.
- If a computer was previously encrypted and the agent does not assign encryption settings on install, Panda Full Encryption does not class the computer as encrypted and you cannot use Panda Full Encryption settings to decrypt the computer.

Local editing of BitLocker settings

When using BitLocker to manually decrypt a drive from the Control Panel in Microsoft Windows, changes made to local settings automatically revert to settings made in the management console. The way that Panda Full Encryption responds to a change of this type is as follows:

- **Disable automatic locking of a drive**: It reverts to automatic locking.
- **Remove the password for a drive**: A new password is requested.
- **Decrypt a drive previously encrypted by** Panda Full Encryption: The drive is automatically encrypted.
- **Encrypt a decrypted drive**: If the Panda Full Encryption settings profile implies decrypting drives, the user action takes precedence and the drive is not decrypted.

Encrypting and decrypting external hard drives and USB drives

Because users can connect and disconnect external storage devices from their computers at any time, the way Panda Full Encryption works with these devices is as follows:

- If the workstation or server does not have BitLocker installed and running, the agent does not download the required packages and the device is not encrypted. Nor are any messages shown to the user.
- If the computer has BitLocker installed and running, a pop-up message is shown to the user prompting them to encrypt the device in these following situations:
    - Each time a user connects an unencrypted drive.
    - If there is an unencrypted device connected to the computer at the time the administrator enables the encryption settings profile from the web console.
- The message shows for five minutes. Regardless of whether the user agrees to encrypt the device or not, they are able to use it normally, unless a settings profile has been configured that prevents the use of unencrypted devices. For more information, see Write to removable storage drives.

- The encryption process does not require the creation of a system partition.
- If the external storage device is already encrypted by a solution other than Panda Full Encryption, and the user connects it to their computer, the encryption message is not shown and the device can be used normally. Panda Full Encryption does not send the recovery keys to the web console.
- Unless configured otherwise, you can use an unencrypted drive. However, in Panda Data Control settings, if you enable the **Write to removable storage drives** option, and Panda Full Encryption or BitLocker did not encrypt the drive, you cannot write to the drive. For more information, see Write to removable storage drives.
- To decrypt a device encrypted by Panda Full Encryption, the user can use BitLocker manually.
- Only the used space of a drive is encrypted.
- The same key encrypts all partitions on the external drive.

If you remove an external drive while encryption is in progress, the contents of the drive might be corrupted.

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 automatically begins encryption.
- **Error creating the system partition**: Many of the errors that occur when creating the system partition can be rectified by the user (for example, lack of space). Periodically, Panda Full Encryption will automatically try to create the partition.
- **User refusal to enable the TPM chip**: The computer will show a message at startup asking the user to enable the TPM chip. Until this condition is resolved, the encryption process will not start.

Obtaining a recovery key

Users are prompted to enter the recovery key:

- **Windows**: When the user has lost their PIN/passphrase/USB device, or the Trusted Platform Module (TPM) chip detects a change in the computer boot sequence.
- **macOS**: When the user has lost their login password, or a change is detected in the computer boot sequence.

Panda Full Encryption stores the recovery keys for all encrypted computer drives that it manages. Therefore, you can obtain these recovery keys through the web management console. To obtain a recovery key, you need this data depending on the operating system installed on the computer:

- **Windows**: You need the recovery key ID. The recovery key ID is a unique 40-digit string associated with each encrypted drive.
- **macOS**: You need the ID of the recovery key associated with the computer. The same recovery key is used for all drives on a Mac computer.

Required permissions

Permission	Access type
Access recovery keys for encrypted drives	To obtain and find the recovery key for an encrypted drive.

Table 14.2: Permissions required to obtain a recovery key

Obtaining the recovery key ID for an encrypted drive (Windows computers)

When a user makes repeated attempts to enter an incorrect PIN or password while the device boots up, they are prompted to enter a BitLocker recovery key:

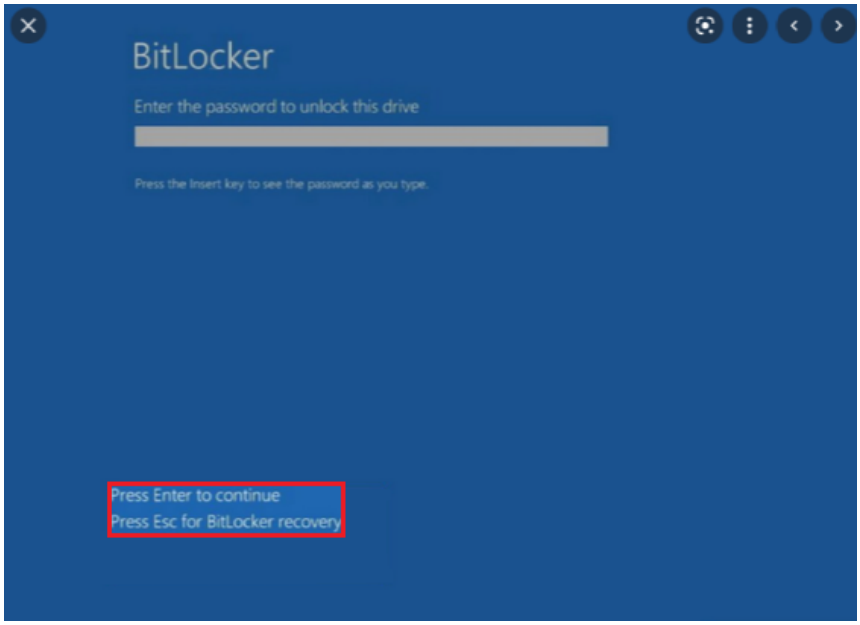


Figure 14.1: Accessing the recovery key ID for an encrypted drive
Figure 14.2:

Press **ESC** to access the screen that shows the recovery key ID for the encrypted drive:

Figure 14.3: Recovery key ID for an encrypted drive

In the case of a recovery key ID for an encrypted partition, the screen shows only the first eight digits of the recovery key ID:

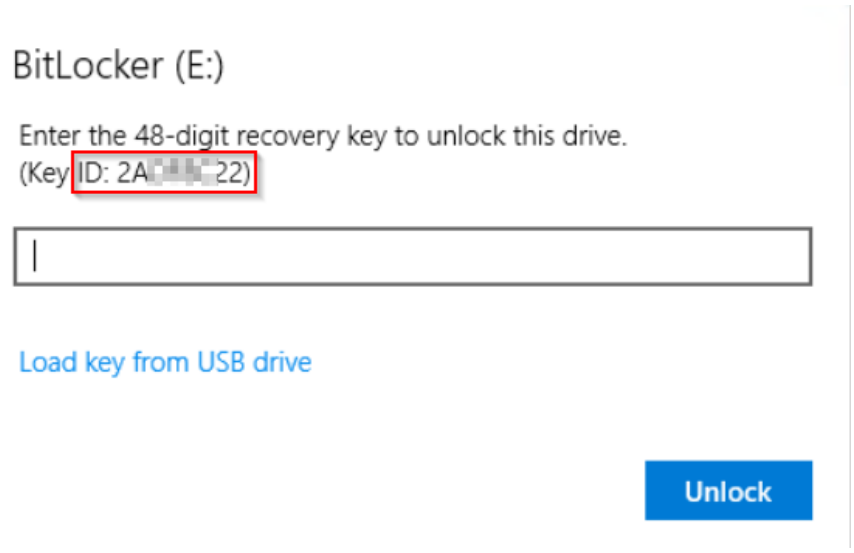


Figure 14.4: Recovery key ID for an encrypted disk partition

For more information about the encryption of drives on computers, see section Encryption and decryption on Windows computers.

Obtaining the ID of the recovery key associated with a computer (macOS computers)

When you try to access an encrypted computer, the login screen shows a message that contains the ID of the recovery key associated with the computer. The screen also recommends that you contact the encryption settings administrator.

Obtaining a recovery key

- From the top menu, select **Computers**. Select the computer you want to obtain the recovery key for.
- On the **Details** tab, **Data protection** section, click the **Get recovery key** link. To obtain a removable drive recovery key, click **View encrypted devices on this computer**.

  The **Get recovery key** dialog box opens and shows the IDs of the encrypted drives on the computer.
- Click the encrypted drive ID of the key you want to recover. The **Get recovery key** dialog box opens.
- Click **Copy recovery key** and send it to the user.

Finding a recovery key

If the user has visibility of all the computers in an account, the search results also include the IDs of drives on computers that were deleted.

Finding a recovery key from the Encrypted Computers widget

- From the top menu, select **Status**. From the side menu, select **Full Encryption**.
- In the **Encrypted Computers** widget, click **Recovery key search**.

Figure 14.5: Finding a recovery key

- Type the ID of the recovery key you want to find. The recovery key that the user can use to unlock the encrypted drive is shown.
- In the case of a recovery key ID for an encrypted partition, enter the first eight digits. The recovery key that the user can use to unlock the encrypted disk partition is shown.

> *If the first eight digits of a recovery key are the same for more than one key, all keys appear in the search results.*

Finding a recovery key from the Computer Details page

- From the top menu, select **Computers**. Select the computer you want to find the recovery key for.
- On the **Details** tab, **Data protection** section, click the **Get recovery key** link. To obtain a removable drive recovery key, click **View encrypted devices on this computer**.

  The **Get recovery key** dialog box opens and shows the IDs for all encrypted drives on the computer.
- To find another recovery key, click **Find another key**.

Panda Full Encryption module panels/widgets

Accessing the dashboard

From the top menu, select **Status**. From the side menu, select Panda Full Encryption.

Required permissions

You do not need additional permissions to access the widgets associated with **Panda Full Encryption**.

Encryption status

This widget shows the computers that support Panda Full Encryption and their encryption status.

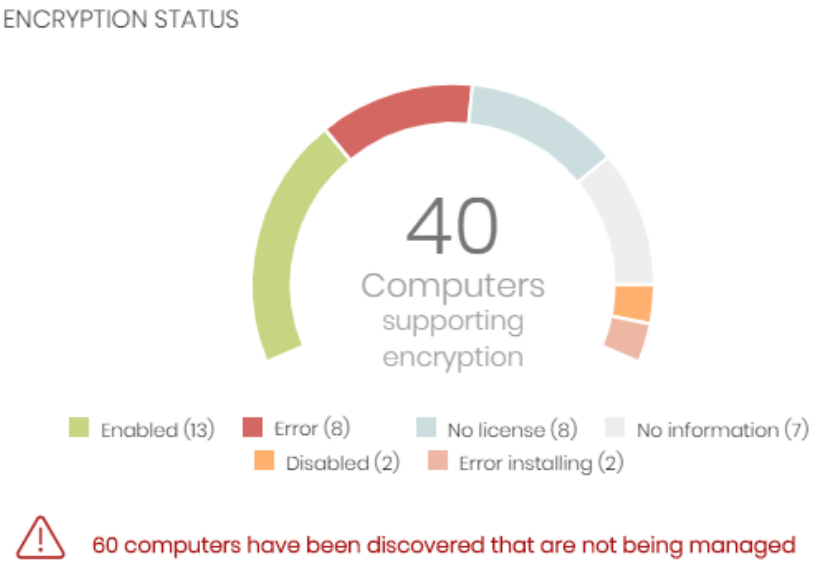


Figure 14.6: Encryption Status panel

Meaning of the data displayed

Data	Description
Enabled	Computers with Panda Full Encryption installed. Settings are assigned to encrypt the computer, and there are no reports of any encryption or installation errors.
Disabled	Computers with Panda Full Encryption installed. Settings are assigned to not encrypt the computer, and there are no reports of any encryption or installation errors.
Error	Computers not able to perform actions that are specified in the encryption or decryption settings.
Error installing	Computers, when required, not able to download and install BitLocker.
No license	Computers that are compatible with Panda Full Encryption, but do not have a Panda Endpoint Protection Plus license assigned.
No information	Computers with a recently assigned license that have not reported their status to the server, or computers with an expired agent.

Table 14.3: Description of the data displayed in the Encryption Status panel

Lists accessible from the panel

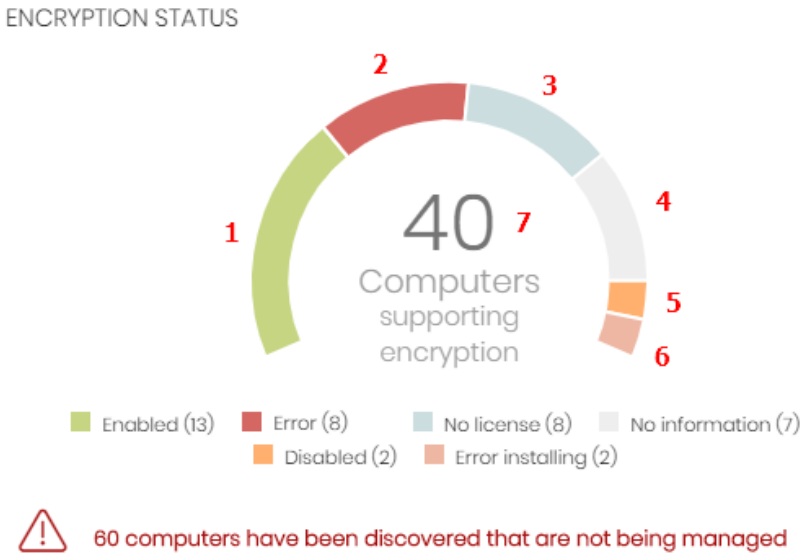


Figure 14.7: Hotspots in the Encryption Status panel

Click the hotspots shown in Figure 14.7: to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Encryption status = Enabled.
(2)	Encryption status = Error.
(3)	Encryption status = No license. The computer does not have a Panda Endpoint Protection Plus license assigned.
(4)	Encryption status = No information.
(5)	Encryption status = Disabled.
(6)	Encryption status = Error installing.
(7)	No filter.

Table 14.4: Lists accessible from the Encryption Status panel

Computers supporting encryption

This widget shows computers that support encryption technology, grouped by type. The color green indicates devices that support encryption, and the color red indicates devices that do not.

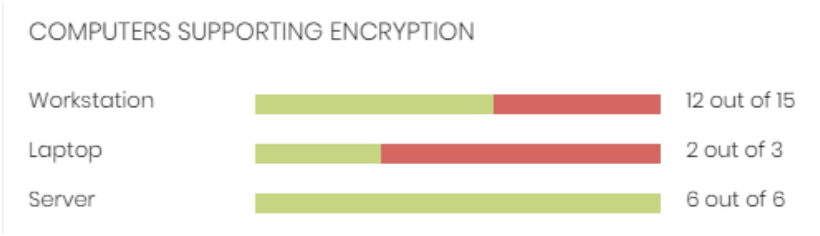


Figure 14.8: Computers Supporting Encryption panel

Meaning of the data displayed

Data	Description
Workstation - green	Workstations that support encryption.
Workstation - red	Workstations that do not support encryption.
Laptop - green	Laptops that support encryption.
Laptop - red	Laptops that do not support encryption.
Server - green	Servers that support encryption.
Server - red	Servers that do not support encryption.

Table 14.5: Description of the data displayed in the Computers Supporting Encryption panel

Lists accessible from the panel

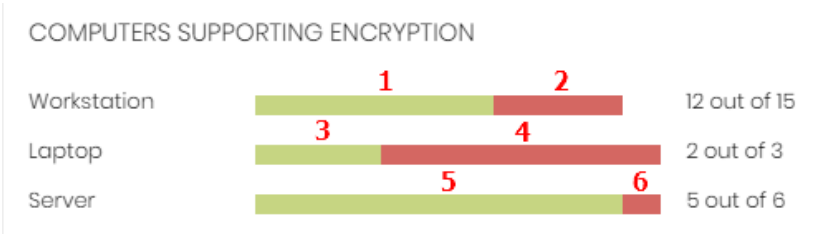


Figure 14.9: Hotspots in the Computers Supporting Encryption panel

Click the hotspots shown in Figure 14.9: to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Computer type = Workstation.
(2)	Computer list filtered by **Encryption not supported**.

Hotspot	Filter
(3)	Computer type = Laptop.
(4)	Computer list filtered by **Encryption not supported**.
(5)	Computer type = Server
(6)	Computer list filtered by **Encryption not supported**.

Table 14.6: Lists accessible from the Computers Supporting Encryption panel

Encrypted computers

This widget shows the encryption status of computers that support Panda Full Encryption.

> *For more information about how to search for recovery keys, see section Obtaining a recovery key.*

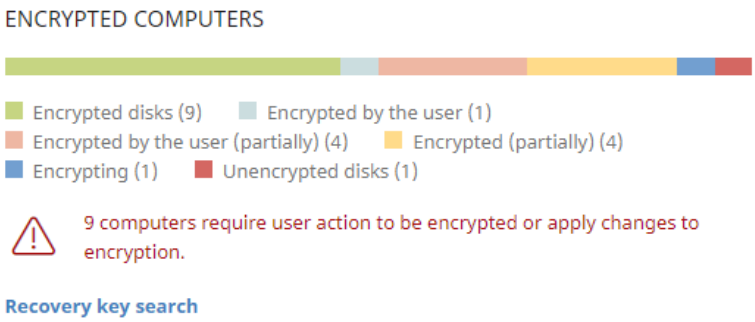


Figure 14.10: Encrypted Computers panel

Meaning of the data displayed

Data	Description
Unknown	Disks encrypted with an authentication method that Panda Full Encryption does not support.
Unencrypted disks	Neither the user or Panda Full Encryption has encrypted a disk.
Encrypted disks	Panda Full Encryption has encrypted all disks.
Encrypting	At least one disk is currently in the encryption process.

Data	Description
Decrypting	At least one disk is currently in the decryption process.
Encrypted by the user	A user encrypted some or all of the disks.
Encrypted by the user (partially)	A user encrypted some or all of the disks. Panda Full Encryption encrypts or decrypts the remainder.
Encrypted (partially)	Panda Full Encryption encrypted at least one of the disks. The remaining disks are unencrypted.

Table 14.7: Description of the data displayed in the Encrypted Computers panel

Lists accessible from the panel

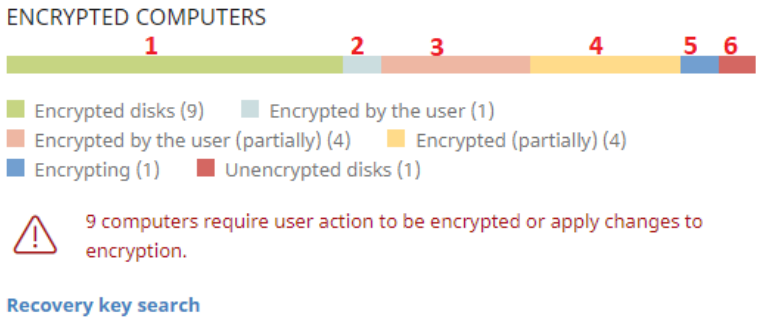


Figure 14.11: Hotspots in the Encrypted Computers panel

Click the hotspots shown in Figure 14.11: to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Disk encryption = Encrypted disks.
(2)	Disk encryption = Encrypted by the user.
(3)	Disk encryption = Encrypted by the user (partially).
(4)	Disk encryption = Encrypted (partially).
(5)	Disk encryption = Encrypting.
(6)	Disk encryption = Unencrypted disks.

Hotspot	Filter
(7)	Disk encryption = Decrypting.
(8)	Disk encryption = Unknown.

Table 14.8: Lists accessible from the Encrypted Computers panel

Authentication method applied

This widget shows encrypted computers and the type of authentication used. For more information about the supported authentication methods, see General features of Panda Full Encryption.

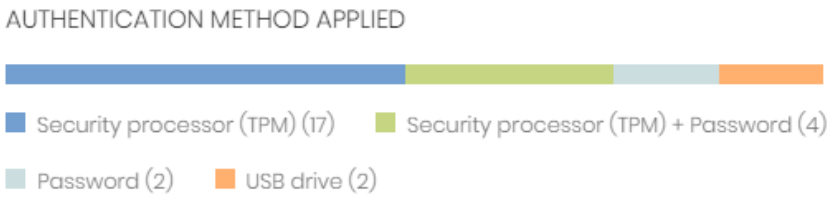


Figure 14.12: Authentication Method Applied panel

Meaning of the data displayed

Data	Description
Unknown	Panda Full Encryption does not support the user-selected authentication method.
Security processor (TPM)	The computer uses a Trusted Platform Module (TPM) chip for authentication.
Security processor (TPM) + Password	While booting, the computer uses a TPM chip and PIN or password for authentication.
Password	• **Windows computers:** While booting, the computer requests a PIN or passphrase for authentication. • **Mac computers:** While booting, the computer requests a password for authentication.
USB drive	While booting, the computer uses a USB key for authentication.
None	The computer has no encrypted disks.

Table 14.9: Description of the data displayed in the Authentication Method Applied panel

Lists accessible from the panel

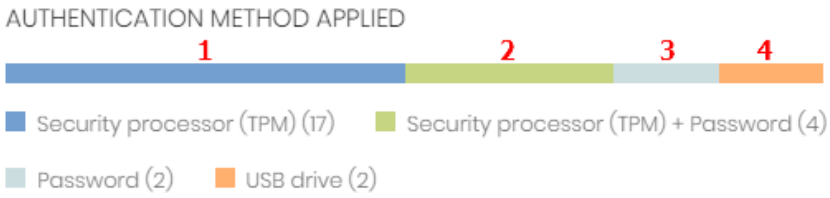


Figure 14.13: Hotspots in the Authentication Method Applied panel

Click the hotspots shown in Figure 14.13: to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Authentication method = Security processor (TPM)
(2)	Authentication method = Security processor (TPM) + Password
(3)	Authentication method = Password
(4)	Authentication method = USB drive
(5)	Authentication method = Unknown
(6)	Authentication method = None

Table 14.10: Description of the list filters

Panda Full Encryption lists

Accessing the lists

You can access the lists in two ways:

- From the top menu, select **Status**. From the side menu, select **Panda Full Encryption**. Click the relevant widget.

  Or,

- From the top menu, select **Status**. From the side menu, click the **Add** link. A window opens that shows the available lists.
- From the **Data protection** section, select a list to view the associated template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

You do not need additional permissions to access the **Encryption status** list.

Encryption status

This list shows all computers on the network managed by Panda Endpoint Protection Plus and compatible with Panda Full Encryption. It includes filters related to the module to monitor the encryption status of the network.

Field	Comment	Values
Computer	Name of the computer compatible with the encryption technology.	Character string
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Agent reinstallation error Protection reinstallation: •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated. •  Isolated computer. •  Computer in the process of stopping being isolated. “RDP attack containment” mode: •  Computer in “RDP attack containment” mode. •  Ending "RDP attack containment" mode.	Icon
Group	Folder within the Panda Endpoint Protection Plus folder tree the computer belongs to.	Character string
Operating system	Operating system and version installed on the workstation or server.	Character string
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled

Field	Comment	Values
		• Disabled • Error • Install error • No license
Disk status	Encryption status of the computer internal storage media.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted by the user (partially) • Encrypted (partially)
Authentication method	Authentication method selected to encrypt disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • None
Last connection	Date when the agent last connected to the Panda Security cloud.	Date

Table 14.11: Fields in the Encryption Status list

To view a graphical representation of the list data, see the Encrypted computers widget.

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer compatible with the encryption technology.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder within the Panda Endpoint Protection Plus folder tree the computer belongs to.	Character string
Agent version	Internal version of the Panda agent module.	Character string
Installation date	Date when the Panda Endpoint Protection Plus software was successfully installed on the computer.	Date
Last connection date		Date
Platform	Operating system installed on the computer.	Character string
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.	Boolean
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.	Boolean

Field	Comment	Values
Last update	Date when the signature file was last updated.	Date
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Disk status	Encryption status of the computer internal storage media.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Encryption pending user action	The user must restart the computer or enter data to complete the encryption process.	Boolean
Authentication method	Authentication method selected to encrypt disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password

Field	Comment	Values
		• USB drive • None
Encryption date	Date when the first drive was encrypted on a fully encrypted computer (all compatible drives are 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 the Panda Full Encryption module on the computer.	Character string
Encryption error date	Last date when an encryption error was reported on the computer.	
Encryption error	The encryption process returned an error.	Character string

Table 14.12: Fields in the exported file

Filter tool

Field	Comment	Values
Encryption date from	Start point of the date range for fully encrypted computers.	Date
Encryption date to	End point of the date range for fully encrypted computers.	Date
Platform	Operating system installed on the computer.	• All • Windows • macOS
Computer type	Type of device.	• Workstation

Field	Comment	Values
		• Laptop • Server
Disk status	Encryption status of the computer internal storage media.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Authentication method	Authentication method selected to encrypt disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • None

Field	Comment	Values
Last connection	Date when the Panda Endpoint Protection Plus status was last sent to the Panda Security cloud.	Date
Encryption pending user action	Indicates whether the user must take action to complete the encryption process.	• All • Yes • No

Table 14.13: Filters available in the list

Computer details page

Click a row in the list to open the computer details page. For more information, see Computer details on page 236.

Encryption settings

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Encryption**.
- Click the **Add** button. The settings page opens.

Required permissions

Permission	Access type
Configure computer encryption	Create, edit, delete, copy, or assign encryption settings profiles.
View computer encryption settings	View encryption settings profiles.

Table 14.14: Permissions required to access the encryption settings

Panda Full Encryption settings

Encrypt all hard disks on computers

Specify whether the computers will be encrypted or not. Depending on the previous status of a computer, the way that Panda Full Encryption behaves varies:

- If a computer is encrypted with Panda Full Encryption and you disable **Encrypt all hard disks on computers**, all encrypted drives are decrypted.

- If a computer is encrypted with a product other than Panda Full Encryption, and you disable **Encrypt all hard disks on computers**, there are no changes.
- If a computer is encrypted with a product other than Panda Full Encryption, and you enable **Encrypt all hard disks on computers**, the internal encryption settings are adjusted to match the encryption methods supported by Panda Full Encryption, thereby avoiding re-encrypting the drive. For more information, see Encryption of previously encrypted drives.

  With macOS computers, a new recovery key is generated. See Encryption and decryption on macOS computers
- If a computer is not encrypted, and you enable **Encrypt all hard disks on computers**, all the computer drives are encrypted. See Encryption and decryption on Windows computers and Encryption and decryption on macOS computers.

Ask for password to access the computer (Windows computers)

Enable password authentication when a computer or device starts. Depending on the platform and whether there is TPM hardware, two types of passwords are permitted:

- **Computers with TPM**: Require a PIN type password.
- **Computers without TPM**: Require a passphrase.

If you disable this option and the computer does not have access to a compatible TPM security processor, the disks are not encrypted.

Do not encrypt computers that require a USB drive for authentication (Windows computers)

To prevent the use of USB devices supported by Panda Full Encryption in authentication, you can disable them.

Only Microsoft Windows 7 without TPM can use USB authentication. If you disable USB devices, these computers are not encrypted.

Encrypt used disk space only (Windows computers)

To minimize the encryption time, enable **Encrypt used disk space only** to only encrypt sectors of the hard disk that are used. Sectors released after a file is deleted remain encrypted, but the space that was free before encryption of the hard disk remains unencrypted. It will be accessible to third parties with tools to recover deleted files.

Prompt for removable storage drive encryption (Windows computers)

When a user inserts an unencrypted removable drive in a computer that has Microsoft BitLocker technology enabled, they receive a prompt to encrypt its contents. For more information about this setting, see Encrypting and decrypting external hard drives and USB drives.

Available filters

To find network computers with any of the encryption statuses defined in Panda Full Encryption, use the filter tree resources shown in section Filter tree on page 202. The available filters are as follows:

- Encryption:
    - Encryption pending user action.
    - Disk status.
    - 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.

Chapter 15

Malware and network visibility

Panda Endpoint Protection Plus provides administrators with 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.
- Network status reports with information collected and consolidated over time.

For more information about consolidated reports, see *Scheduled sending of reports and lists on page 555*.

The visualization and monitoring tools determine, in real time, the network security status as well as the impact of any security breach that may occur in order to facilitate the implementation of appropriate security measures.

Chapter contents

Security module panels/widgets

Panda Endpoint Protection Plus shows an overview of the security status of the entire IT network or specific computers through widgets:

- **IT network**: From the top menu, select **Status**. From the side menu, select **Security**  . A page opens and shows counters that display the security status of the computers that are visible to you. For more information about how to set the computer groups that are visible to the account used to access the management console, see Managing roles and permissions on page 65. For more information about how to restrict the visibility of the groups defined in a role, see Filter by group icon on page 33.
- **Computer**: From the top menu, select **Computers**. Select a computer from the network. Select the **Detections** tab. A page opens and shows counters that display the security status of the selected computer. See Detections section (4) for Windows, Linux, and macOS computers on page 254.

The following is a description of the different widgets implemented on the Panda Endpoint Protection Plus dashboard, their areas and hotspots, as well as their tooltips and what they mean.

Protection status

This widget shows computers where Panda Endpoint Protection Plus is working correctly and computers with errors or problems installing or running the product. The status of the network computers is represented with a circle with different colors and associated counters.

The bottom of the widget shows the number of computers that are in Audit more, if any. For more information, see Audit mode.

> *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.*

The panel provides a graphical representation and percentage of computers with the same status.

> *The total number of computers and devices at the center of the widget includes iOS devices. The widget includes no other information about iOS devices. iOS devices do not have advanced or antivirus protection. For more information, see Security settings for iOS devices on page 326.*

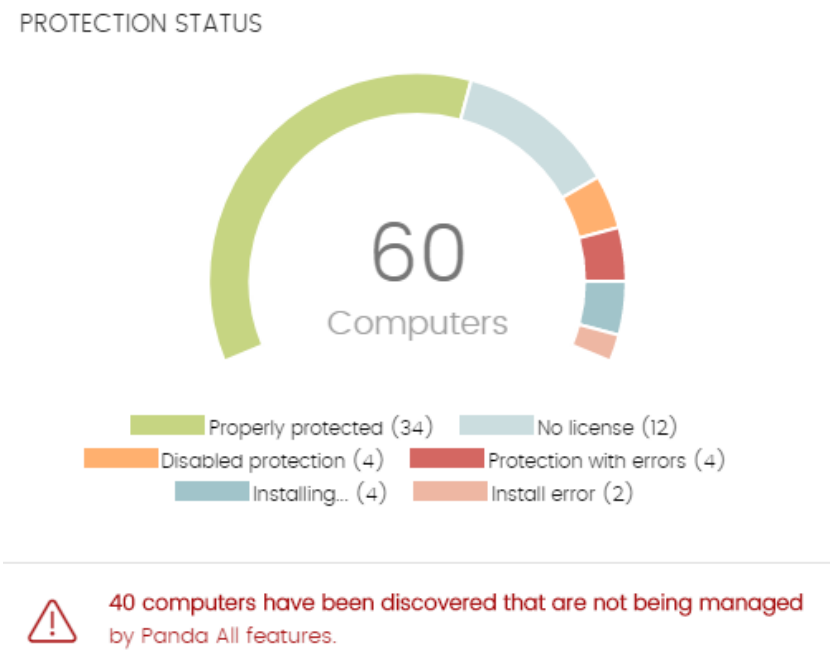


Figure 15.1: Protection Status panel

Meaning of the data displayed

Data	Description
Properly protected	Percentage of computers where Panda Endpoint Protection Plus installed without errors and is working correctly.
Installing...	Percentage of computers on which Panda Endpoint Protection Plus 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 Plus installed, but whose protection module does not respond to the requests sent from the Panda Security servers.
Install error	Computers on which the installation process could not be completed.
Central area	Number of computers with a Panda agent installed.

Table 15.1: Description of the data displayed in the Protection Status panel

Lists accessible from the panel

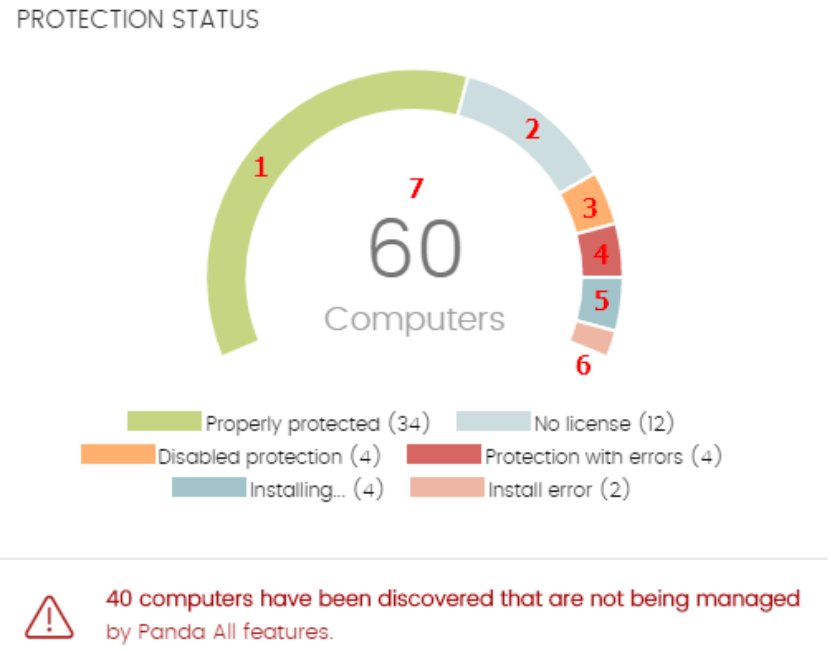


Figure 15.2: Hotspots in the Protection Status panel

Click the hotspots shown in Figure 15.2: to open the **Computer protection status** list with these predefined filters:

Hotspot	Filter
(1)	Protection status = Properly protected.
(2)	Protection status = Installing...
(3)	Protection status = Disabled protection.
(4)	Protection status = Protection with errors.
(5)	Protection status = No license.
(6)	Protection status = Install error.
(7)	No filter.

Table 15.2: Filters available in the Computer Protection Status list

Offline computers

This widget shows the number of computers that have not connected to the Panda Security cloud for a number of days. These computers might be susceptible to security problems and require attention.

Figure 15.3: 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 15.3: Description of the data displayed in the Offline Computers panel

Lists accessible from the panel

Figure 15.4: Hotspots in the Offline Computers panel

Click the hotspots shown in Figure 15.4: to open the **Offline computers** list with these predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.

Hotspot	Filter
(3)	Last connection = More than 30 days ago.

Table 15.4: Filters available in the Offline Computers list

Outdated protection

This widget shows the number of computers with a signature file that is more than three days older than the latest released file. It also shows the computers with an antivirus engine that is more than seven days older than the latest released engine. These computers might be vulnerable to attacks from threats.

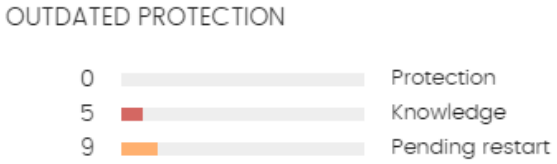


Figure 15.5: Outdated Protection panel

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	The computer has had a version of the antivirus engine older than the latest released engine for at least seven days.
Knowledge	The computer has not updated its signature file for at least three days.
Pending restart	The computer requires a restart to complete the update.

Table 15.5: Description of the data displayed in the Outdated Protection panel

Lists accessible from the panel

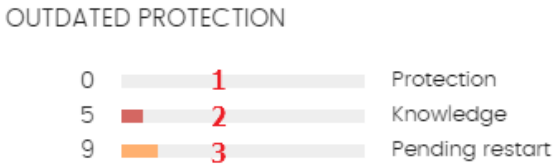


Figure 15.6: Hotspots in the Outdated Protection panel

Click the hotspots shown in Figure 15.6: to open the **Computer protection status** list with these predefined filters:

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

Table 15.6: Filters available in the Computers with Out-of-Date Protection list

Threats detected by the antivirus

This widget shows all intrusion attempts that Panda Endpoint Protection Plus detected in the selected time period.

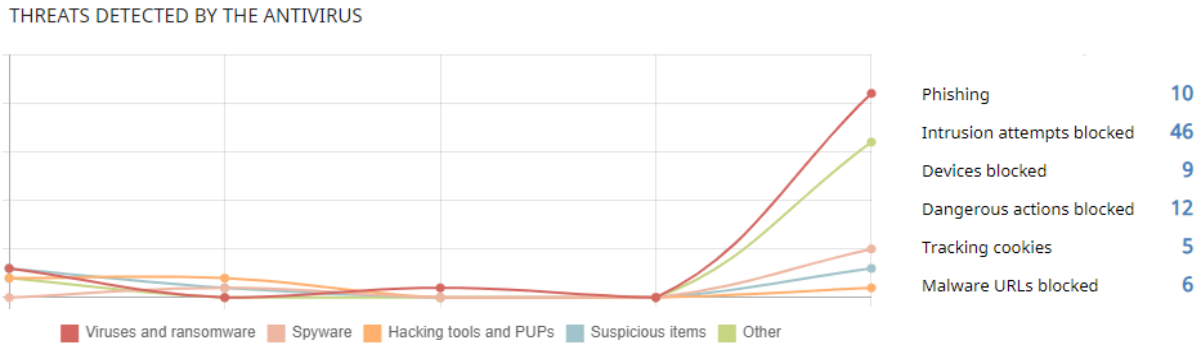


Figure 15.7: Threats Detected by the Antivirus panel

The data covers all infection vectors and all supported platforms. Administrators can get specific data (volume, type, form of attack) related to the malware.

Meaning of the data displayed

This panel includes two sections: a line chart and a summary list.

The line chart represents detections on the network over time, split into malware categories:

Data	Description
Viruses and ransomware	Programs that 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 perform actions that cause problems for the user of the affected computer (control the computer, steal confidential information, scan communication ports, etc.).
Suspicious items	Files with a high probability of being malware after having been analyzed by our

Data	Description
	heuristic technologies. This type of technology is used only in the on-demand scans performed from scheduled tasks. In this type of scan, the investigated file is not executed. Therefore, the security software has far less information to evaluate the file's behavior, which reduces the classification accuracy. To compensate for the reduced accuracy of the static scan, the heuristic technologies are used.
Phishing	A technique for obtaining confidential information from users fraudulently. The targeted information includes passwords, credit card numbers, and bank account details.
Other	Hoaxes, worms, Trojans, and other types of viruses.

Table 15.7: Description of the data displayed in the Threats Detected by the Antivirus panel

The list to the right of the chart shows events that you might want to monitor to look for symptoms or potentially dangerous situations.

Data	Description
Dangerous actions blocked	Detections made by analyzing local behavior.
Intrusion attempts blocked	Detections of malformed network traffic specially crafted to cause an execution error in one of the components on the targeted computer that leads to unwanted system behavior.
Devices blocked	Detection of a user attempt to use a device whose access is restricted according to the settings established by the network administrator in the Device Control module.
Tracking cookies	Detection of cookies used to track the web activity of users.
Malware URLs blocked	Web addresses that point to pages containing malware.

Table 15.8: Description of the data displayed in the Threats Detected by the Antivirus panel

Lists accessible from the panel

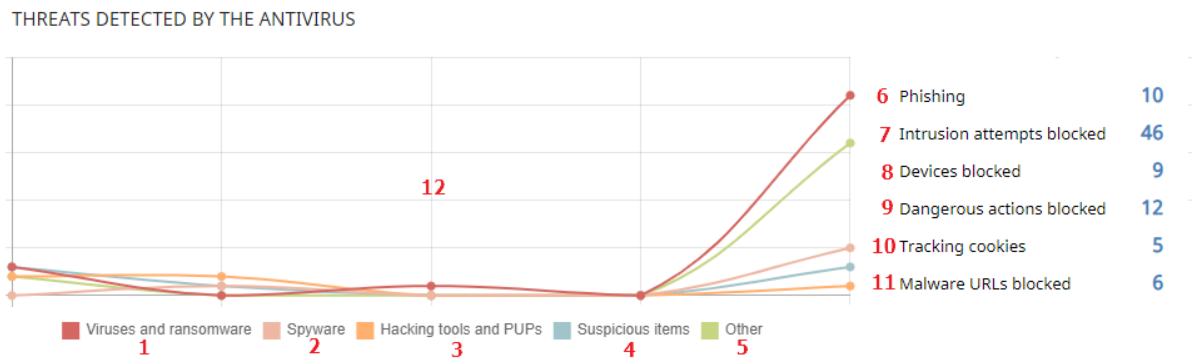


Figure 15.8: Hotspots in the Threats Detected by the Antivirus panel

Click the hotspots shown in Figure 15.8: to access these list with these predefined filters:

Hotspot	List	Filter
(1)	Threats detected by the antivirus.	Threat type = Viruses and ransomware.
(2)	Threats detected by the antivirus.	Threat type = Spyware.
(3)	Threats detected by the antivirus.	Threat type = Hacking tools and PUPs.
(4)	Threats detected by the antivirus.	Threat type = Suspicious items.
(5)	Threats detected by the antivirus.	Threat type = Other.
(6)	Threats detected by the antivirus.	Threat type = Phishing.
(7)	Intrusion attempts blocked	No filter.
(8)	Devices blocked	No filter.
(9)	Threats detected by the antivirus.	Threat type = Dangerous actions blocked.
(10)	Threats detected by the antivirus.	Threat type = Tracking cookies.
(11)	Threats detected by the antivirus.	Threat type = Malware URLs.
(12)	Threats detected by the antivirus.	No filter.

Table 15.9: Filters available in the Threats Detected by the Antivirus list

Web access

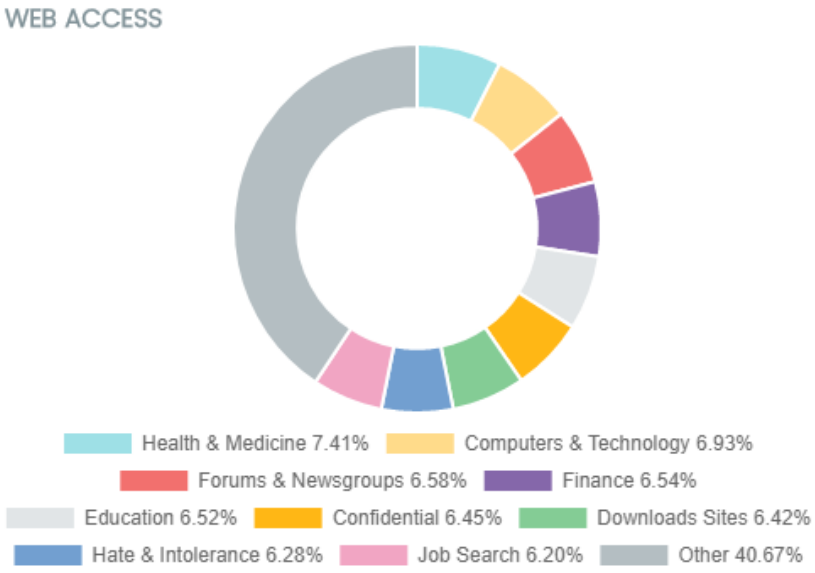


Figure 15.9: Web Access panel

This widget shows a pie chart with the categories of web pages most visited by users on the network.

Meaning of the data displayed

The pie chart shows the ten most visited web page categories supported by Panda Endpoint Protection Plus when categorizing the pages accessed by users.

The pie chart key shows the percentage of web page requests for each category.

Lists accessible from the panel

Click the categories shown in Figure 15.9: to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Any	Category = Selected category.

Table 15.10: Filters available in the Web Access by Computer list

Top 10 most accessed categories

This widget shows the number of visits and the number of computers that have accessed the 10 most visited web page categories.

Each category shows the total number of visits in the selected date range, and the number of computers that accessed it one or more times.

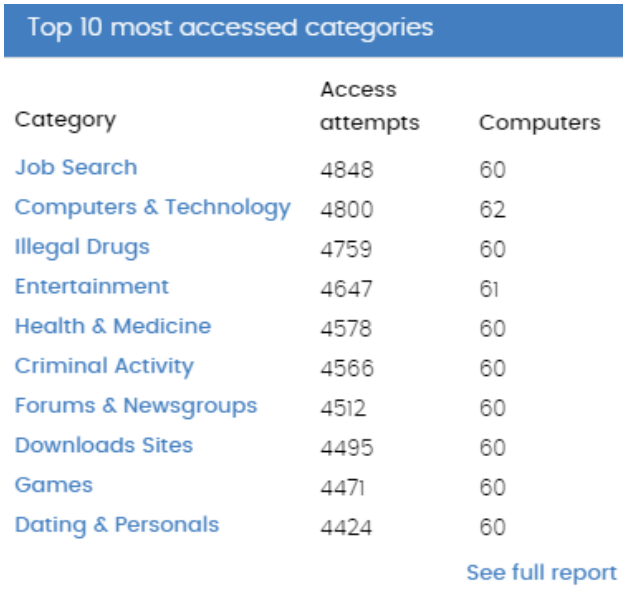


Figure 15.10: Most Accessed Categories panel

Lists accessible from the panel

Click the panel to open the **Web access by computer** list with different predefined filters depending on the area clicked.

Hotspot	Filter
Category	Category = Selected category.
See full report	Opens the Web Access by Category list with no filters.

Table 15.11: Filters available in the Web Access by Computer list

Top 10 most accessed categories by computer

This widget shows the number of web page visits, ordered by category, of the 10 computers that used the Web the most.

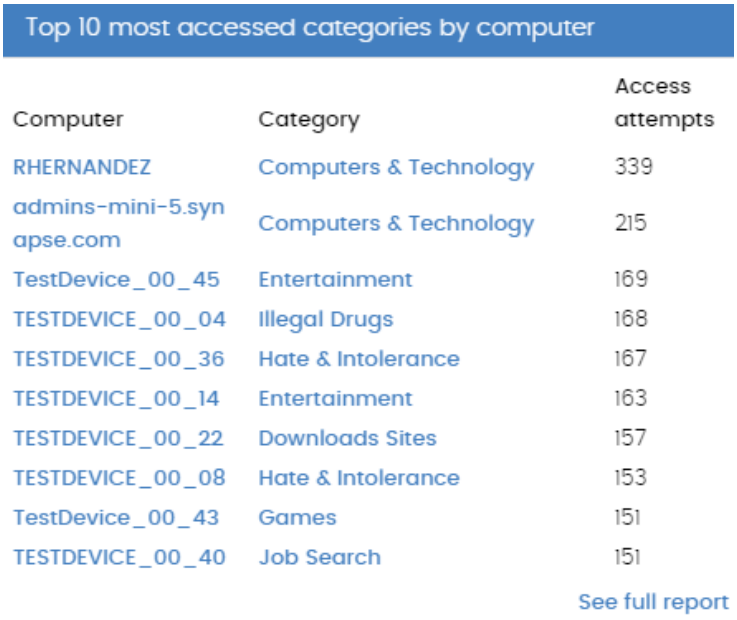


Figure 15.11: Top 10 Most Accessed Categories by Computer panel

Lists accessible from the panel

Click the hotspots shown in figure Figure 15.11: to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Computer	Computer = Selected computer.
Category	Category = Selected category.
See full list	No filter.

Table 15.12: Filters available in the Web Access by Computer list

Top 10 most blocked categories

This widget shows the 10 most frequently blocked web page categories, the number of access attempts blocked, and the number of computers that tried to access them and were blocked.

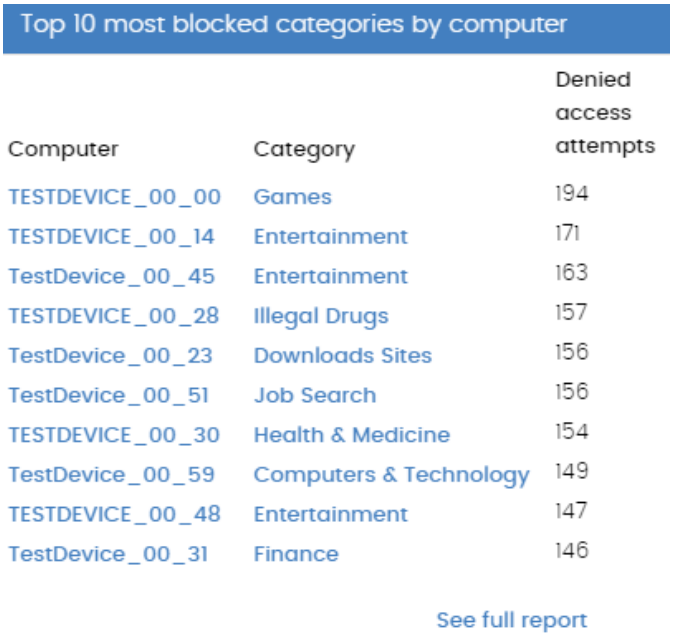


Figure 15.12: Hotspots in the Most Blocked Categories panel

Lists accessible from the panel

Click the hotspots shown in Figure 15.12: to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Category	Category = Selected category.
See full list	Opens the Web Access by Category list with no filters.

Table 15.13: Filters available in the Web Access by Computer list

Top 10 most blocked categories by computer

This widget shows the computer-category pairs with the most visits blocked, the name of the computer, the web content category, and the number of access attempts denied for each computer-category pair.

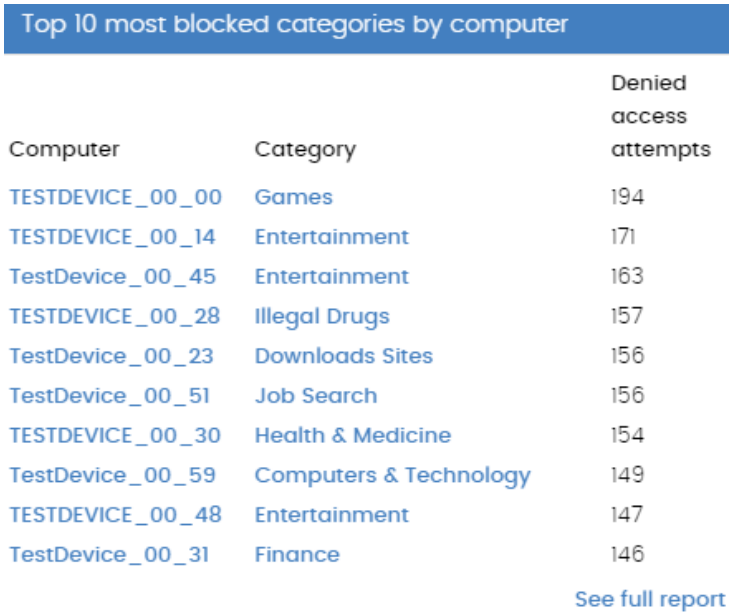


Figure 15.13: Top 10 Most Blocked Categories by Computer panel

Lists accessible from the panel

Click the hotspots shown in Figure 15.13: to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Computer	Computer name = Selected computer.
Category	Category = Selected category.
See full list	No filter.

Table 15.14: Filters available in the Web Access by Computer list

Security module lists

The security lists show the information collected by Panda Endpoint Protection Plus in connection with computer protection activities. They provide highly detailed information because they contain the raw data used to generate the widgets.

There are two ways to access the security lists:

- From the top menu, select **Status**. From the side panel, select **Security**. Click any of the available widgets to access its associated list. Depending on the item you click on the widget, you access different lists with predefined filters.

  Or

- From the top menu, select **Status**. From the **My lists** side panel, click **Add**. A dialog box opens that shows all lists available in Panda Endpoint Protection Plus.
- Select any of the lists in the **Security** section. The list opens with no filters applied.

Select any of the entries on the list to open a new page with more details about that particular item.

Computer protection status

This list shows all computers on the network, with filters that enable you to search for computers and mobile devices that are unprotected for some specific reason.

To ensure correct operation of the security software, the computers on the network must communicate with the Panda Security cloud. For the list of URLs that must be accessible from your computers, see section Access to service URLs on page 621.

Field	Description	Values
Computer	Computer name.	Character string
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Agent reinstallation error. Protection reinstallation: •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. “RDP attack containment” mode: •  Computer in “RDP attack containment” mode. •  Ending "RDP attack containment" mode.	Icon
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string •  'All' group

Field	Description	Values
		•  Native group •  Active Directory group
Antivirus	Antivirus protection status.	•  Installing •  Error. If it is a known error, the cause of the error appears. If it is an unknown error, the error code appears instead. •  Enabled •  Disabled •  No license
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released. Point the mouse to 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. Point the mouse to the field to see the date that the file was last updated.	•  Updated •  Not updated (3 days without updating since last release)
Connection to knowledge	Indicates whether the computer can communicate with the Aether cloud to send monitored events and download security intelligence.	•  Connection OK •  One or more services are not accessible • Information not available
Last connection	Date when the Panda Endpoint Protection Plus status was last sent to the	Date

Field	Description	Values
	Panda Security cloud.	

Table 15.15: Fields in the Computer Protection Status 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	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Agent version	Internal version of the Panda agent module.	Character string
Installation date	Date when the Panda Endpoint Protection Plus software was successfully installed on the computer.	Date
Last update on	Date the agent was last updated.	Date

Field	Description	Values
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 the signature file was last updated.	Date
File antivirus Mail antivirus Web browsing antivirus Firewall Device control Web access control Anti-Theft	Status of the associated protection.	• **Not installed** • **Error**: If it is a known error, the cause of the error appears. If it is an unknown error, the error code appears instead. • **Enabled** • **Disabled** • **No license**
Error date	If an error occurred installing Panda Endpoint Protection Plus, date and time of the error.	Date

Field	Description	Values
Installation error	If an error occurred installing Panda Endpoint Protection Plus, error description.	Character string
Installation error code	Shows codes that identify the installation error occurred.	Codes are separated by ";": • Error code • Extended error code • Extended error subcode
Other security products	Name of any third-party antivirus product found on the computer at the time of installing Panda Endpoint Protection Plus.	Character string
Connection for web protection	Shows the status of the connection between the computer and the servers that store the dangerous URL database.	• OK • With problems
Connection for collective intelligence	Shows the status of the connection between the computer and the servers that store signature files and security intelligence.	• OK • With problems

Table 15.16: Fields in the Computer Protection Status exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Search computer	Computer name.	Character string
Last connection	Date when the Panda Endpoint Protection Plus status	• All

Field	Description	Values
	was last sent to the Panda Security cloud.	• Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
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
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Connection to knowledge servers	Indicates whether the computer can communicate with the Aether cloud to send monitored events and download security intelligence.	• **All** • **OK** • **With problems**: One or more services are not accessible

Field	Description	Values
Protection status	Status of the protection module installed on the computer.	• Installing... • Properly protected • Protection with errors • Disabled protection • No license • Install error
"RDP attack containment" mode	Status of the "RDP attack containment" mode.	• All • No • Yes

Table 15.17: Filters available in the Computer Protection Status list

Computer Details page

Click a row in the list to open the computer details page. For more information, see Computer details on page 236.

Threats detected by the antivirus

This list provides complete, consolidated information about all detections made on all supported platforms and for all 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 primary IP address.	Character string
Group	Group within the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string • 'All' group • Native group • Active Directory group
Threat type	Type of detected threat.	• Viruses and ransomware

Field	Description	Values
		• 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 Plus.	• Deleted • Disinfected • Quarantined • Blocked • Process ended • Allowed (audit mode)
Date	Date when the attack was detected.	Date

Table 15.18: Fields in the Threats Detected by the Antivirus 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 • Mobile device

Field	Description	Values
		• 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.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items • Dangerous actions blocked • Tracking cookies • Malware URLs • Other
Malware type	Threat subclass.	Character string
Action	Action taken by Panda Endpoint Protection Plus.	• Quarantined • Deleted • Blocked • Process ended • Allowed (audit mode)
Detected by	Engine that detected the threat.	• Device control • File protection • Firewall • Mail protection

Field	Description	Values
		• 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 to allow it to run.	Binary value
Date	Date when the attack was detected.	Date
Group	Group within the Panda Endpoint Protection Plus 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 the computer belongs to.	Character string
Description	Description assigned to the computer by the network administrator.	Character string

Table 15.19: 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**: Set a time period, from the current moment back. **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month • Last year
Computer type	Type of device.	• Workstation

Field	Description	Values
		• Laptop • Mobile device • Server
Threat type	Type of threat.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items • Dangerous actions blocked • Tracking cookies • Malware URLs • Other

Table 15.20: Filters available in the Threats Detected by the Antivirus list

Details page

This page shows detailed information about the detected virus.

Field	Description	Values
Threat	Threat name.	Character string
Action	Action taken by Panda Endpoint Protection Plus. See Restoring files from quarantine on page 545.	• Quarantined • Deleted • Blocked • Process ended • Allowed (audit mode)
Computer	Name of the computer where the threat was detected. It includes a link to the Computer Details page.	Character string

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
IP address	The computer primary IP address.	Character string
Logged-in user	Operating system user under which the threat was loaded and run.	Character string
Detection path	Location of the threat on the file system.	Character string
Name	Threat name.	Character string
Threat type	Type of threat.	Character string
Malware type	Type of malware.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items • Dangerous actions blocked • Tracking cookies • Malware URLs • Other
Detected by	Module that detected the item.	

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

Table 15.21: Details accessible from the Threats Detected by the Antivirus list

Blocked devices

This list provides details of the network computers that have restricted access to peripherals.

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	• Character string •  'All' group •  Native group •  Active Directory group
Name	Name assigned manually to the device by you to make identification easier.	Character string
Type	Type of device affected by the security settings.	• 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 and write access

Field	Description	Values
Date	Date and time when the action was taken.	Date

Table 15.22: Fields in the Blocked Devices 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 • Mobile device • Server
Computer	Computer name.	Character string
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by you.	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 operation was detected on the device.	Numeric value
Action	Action taken on the device.	• Block • Allow read

Field	Description	Values
		access • Allow read and write access
Detected by	Module that detected the disallowed operation.	Device control
Date	Date when the disallowed operation was detected.	Date
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by you.	Character string

Table 15.23: Fields in the Blocked Devices exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Search computer	Computer name.	Character string
Dates	• **Range**: Set a time period, from the current moment back. • **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month
Device type	Type of device affected by the security settings.	• Removable storage drives

Field	Description	Values
		• Imaging devices • CD/DVD drives • Bluetooth devices • Modems • Mobile devices
Name	Device name.	Character string

Table 15.24: Filters available in the Blocked Devices list

Details page

This page shows detailed information about the blocked device.

Field	Description	Values
Device	Name of the blocked device.	Character string
Action	Action taken by Panda Endpoint Protection Plus.	• Quarantined • Deleted • Blocked • Process ended
Computer	Name of the computer where the device was blocked.	Character string
Computer type	Type of computer.	• Workstation • Laptop • Server • Mobile device
IP address	The computer primary IP address.	Character string
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by you. To edit it, click the icon.	Character string

Field	Description	Values
Device 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
Blocked by	Module that detected the item.	Device control
Number of detections	Number of detected blocks.	Numeric value
Date	Date when the attack was detected.	Date

Table 15.25: Details accessible from the Blocked Devices list

Intrusion attempts blocked

This list shows the network attacks received by the computers on the network and blocked by the firewall.

Field	Description	Values
Computer	Name of the computer that received the network attack.	Character string
IP address	IP address of the primary network interface of the computer that received the network attack.	Character string
Group	Group within the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see Block intrusions on page 314.	• All intrusion attempts • ICMP Attack • UDP Port Scan

Field	Description	Values
		• Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Date	Date and time Panda Endpoint Protection Plus logged the attack on the computer.	Date

Table 15.26: 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.	Character string
Computer	Name of the computer that received the network attack.	Character string

Field	Description	Values
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see Block intrusions on page 314.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICM 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 launched the network attack.	Character string
Remote MAC address	Physical address of the computer that launched the network attack, provided it is on the same subnet as the computer that received the attack.	Character string
Local port	In TCP and UDP attacks, this section indicates the port where the intrusion attempt was received.	Numeric value
Remote port	In TCP and UDP attacks, this section indicates the port from which the intrusion attempt was launched.	Numeric value

Field	Description	Values
Number of detections	Number of intrusion attempts of the same type received.	Numeric value
Action	Action taken by the firewall according to its settings. For more information, see Firewall (Windows computers) on page 307.	Block
Detected by	Detection engine that detected the network attack.	Firewall
Date	Date the network attack was logged.	Date
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
IP address	IP address of the primary network interface of the computer that received the network attack.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by you.	Character string

Table 15.27: Fields in the Intrusion Attempts Blocked exported file

Filter tool

Field	Description	Values
Dates	• **Range**: Set a time period, from the current moment back. • **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see Block intrusions on page 314.	• All intrusion attempts

Field	Description	Values
		• 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.	• Workstation • Laptop • Mobile device • Server

Table 15.28: Filters available in the Intrusion Attempts Blocked list

Details page

This page shows detailed information about the network attack detected.

Field	Description	Values
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see Block intrusions on page 314.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood

Field	Description	Values
		• TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICM Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Action	Action taken by Panda Endpoint Protection Plus.	Blocked
Computer	Name of the computer where the threat was detected.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
IP address	The computer primary IP address.	Character string
Local IP address	IP address of the computer that received the network attack.	Character string
Remote IP address	IP address of the computer that launched the network attack.	Character string
Remote MAC address	Physical address of the computer that launched the network attack, provided it is on the same subnet as the computer that received the attack.	Character string

Field	Description	Values
Local port	In TCP and UDP attacks, this section indicates the port where the intrusion attempt was received.	Numeric value
Remote port	In TCP and UDP attacks, this section indicates the port from which the intrusion attempt was launched.	Numeric value
Detected by	Module that detected the item.	Firewall
Number of detections	Number of successive times the same type of attack occurred between the same source and target computers.	Numeric value
Date	Date when the attack was detected.	Date

Table 15.29: Details accessible from the Intrusion Attempts Blocked list

Web access by category

Field	Description	Values
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Allowed devices	Number of computers allowed to access pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value
Denied computers	Number of computers denied to access pages belonging to the category specified in the Category field.	Numeric value

Table 15.30: Fields in the Web Access by Category list

Fields displayed in the exported file

Field	Description	Values
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Allowed devices	Number of computers allowed to access pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value
Denied computers	Number of computers denied to access pages belonging to the category specified in the Category field.	Numeric value

Table 15.31: Fields in the Web Access by Category exported file

Filter tool

Field	Description	Values
Dates	• **Range**: Set a time period, from the current moment back. • **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month • Last year
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.

Table 15.32: Filters available in the Web Access by Category list

Web access by computer

This list shows all computers on the network and web page visits allowed or denied (sorted by category).

Field	Description	Values
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Group	Group within the Panda Endpoint Protection Plus group tree that the computer belongs to.	• Character string • 'All' group • Native group • Active Directory group
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value

Table 15.33: Fields in the Web Access by Computer 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 • Mobile device • Server
Computer	Computer name.	Character string
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.

Field	Description	Values
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value
Group	Group within the Panda Endpoint Protection Plus group tree that the computer belongs to.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by you.	Character string

Table 15.34: Fields in the Web Access by Category exported file

Filter tool

Field	Description	Values
Dates	• **Range**: Set a time period, from the current moment back. • **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Computer name.	Character string

Table 15.35: Filters available in the Web Access by Category list

Chapter 16

Risk assessment

The risk assessment feature enables you to monitor the overall status of the security risk for the computers you manage.

Panda Endpoint Protection Plus Individually monitors and assesses each configuration and each security module installed on the computers on the network. Each assessed feature is compared to an ideal configuration or status defined by Panda Security. When the ideal configuration and the configuration found on a user computer differ, a risk level is assigned to that specific feature.

When you configure the risk assessment feature, you can choose which security aspects you want to monitor on computers. If the assessed feature and the ideal configuration differ, Panda Security sets a specific risk level (Medium, High, or Critical). You can change this level afterward according to your needs.

Not all features you can assess are applicable to all operating systems installed across the network. Panda Security will add new checks with each new version of the product to gradually improve risk assessment.

For more information about the risk assessment feature, see: Accessing, controlling, and monitoring the management console on page 53: Information about how to manage user accounts and assign permissions. Managing lists on page 41: Information about how to manage lists.

Chapter contents

Chapter contents

Risk assessment settings

Required permissions

The risk assessment feature is visible to all users of the web console. However, you must have the Full Control role to configure it. For more information, see Managing roles and permissions on page 65. The risk assessment settings apply equally to all computers on the IT network.

Accessing the settings

From the top menu, select **Settings**. From the side menu, select **Risks**. The **Risks** page opens. This page is divided into two main areas: a list of risks and a series of drop-down menus to assign risk levels.

Risk list

Most risks have to do with the various types of settings implemented in Panda Endpoint Protection Plus. Other risks are related to the security software status information sent by computers to the Panda Security servers.

The risks you can assess vary based on the operating system installed on the computer.

Risk	Description
No protection	The computer has protection installation errors or does not have a license. See Protection status on page 446.
Out-of-date protection	The version of the protection engine installed on the computer is out of date. The computer is vulnerable to threats. See Details section (3) on page 248.
Out-of-date knowledge (more than 30 days)	The version of the signature file installed on the computer is out of date. The computer is vulnerable to threats. See Outdated protection on page 450.
No connectivity to knowledge servers	Communications between the computer and the Aether servers have failed. The computer is not completely protected. To verify the computer meets the connection requirements, see Product features and requirements on page 602.
No uninstallation protection	The computer is not password protected to prevent unauthorized protection uninstallation or tampering. See Configuring security against protection tampering on page 292.
Anti-tamper	The protection can be modified and tampered with. See Configuring security

Risk	Description
protection disabled	against protection tampering on page 292.
File antivirus disabled	The antivirus is disabled. See Antivirus on page 304 and Antivirus for web browsers on page 326 (Android).
Anti-phishing disabled	The computer is not protected against fraudulent emails and websites. See Threats to detect on page 306.
Web browsing antivirus disabled	The computer is not protected against threats hosted on certain web pages and URLs. See Antivirus on page 304 and Antivirus for web browsers on page 326.
Folder, file, and extension exclusions	There are files, folders, or extensions that are not scanned for malware. • For more information about how to configure items you do not want to be blocked, deleted, or disinfected, see Files and paths excluded from scans on page 302 • For more information about how to prevent certain programs from being blocked, see Authorized software and exclusions. • For more information about how to add folder-level, file, or file extension exclusions without impacting a computer risk level, see Managing exclusion impact.
Critical patches pending installation	The computer has Panda Patch Management installed and has reported the existence of critical patches that are pending installation. You can receive notification of this risk immediately or a specified number of days after the patches are published. By default, the number of days is 30, although you can edit this parameter when you enable this risk for evaluation. See Configuring the discovery of missing patches on page 351.

Table 16.1: Risk list

How risk assessment works

Panda Security sets a default risk level for each risk. This is the risk level when you first open the **Settings** > **Risks** page. You can change the default risk level to another risk level, based on your needs.

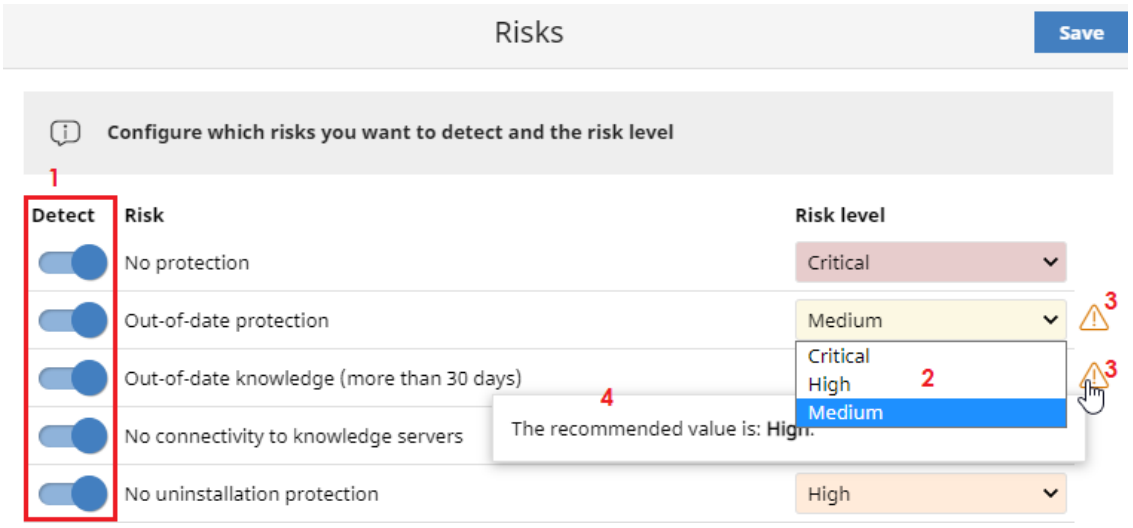


Figure 16.1: Configuring risk assessment

To configure risk assessment:

- From the list of risks **(1)**, enable the toggles for the risks you want to detect.
- From the **Risk level** drop-down menu **(2)**, select a level for each risk: **Critical**, **High**, **Medium**.

  If the recommended risk level is different from the level you select, the  icon **(3)** appears. Point to the icon. A message appears **(4)** that shows the risk level recommended by Panda Security.
- Click **Save**.

> *Risk update is asynchronous. There could be a delay between when you configure risks and when data shows in lists and widgets.*

Monitoring risk assessment

Risk assessment results appear in the relevant widgets and lists. For more information, see Risk assessment module lists and Risk assessment module panels/widgets.

Modification and recalculation of recommended values

When Panda Security releases a new version of Panda Endpoint Protection Plus, we might change the default risk level for risks. When you upgrade to a new version of Panda Endpoint Protection Plus:

- Risks that you did not modify the default risk level for automatically update to the new default value recommended by Panda Security.
- Panda Endpoint Protection Plus recalculates the overall risk level for all computers. The default configuration shows the new recommended risk levels.

Calculation of the overall risk level for a specific computer

The security software calculates the overall risk level for a specific computer when:

- You upgrade to a new version of Panda Endpoint Protection Plus.
- The computer settings change, the computer or device moves from one group to another, a new computer or device registers, or the license assigned to the computer changes, in some cases.

The overall risk level assigned to a computer matches the highest risk level of the risks detected on it.

For example:

- A computer has five risks. All of the them are active, one of which has a **High** risk level and the other four have a **Medium** risk level. The computer overall risk level is **High**.
- A computer has five risks. Four risks are active (One has a **High** risk level and three have a **Medium** risk level) and one is inactive (with a **Critical** risk level). The computer overall risk level is **High**.

Managing exclusion impact

The security software assigns a specific risk level to each risk detected on computers. On the **Manage exclusion impact** page, you can control whether folder-level, file, or file extension exclusions impact the overall security risk status for a computer.

Configure risk settings for exclusions

- From the top menu, select **Settings**. From the side menu, select **Risks**. The **Risks** page opens.
- From the list of risks **(1)**, enable the **Folder, file, and extension exclusions** toggle.
- Click **Manage exclusion impact**.

The **Manage exclusion impact** dialog box opens. This dialog box is divided into two areas:

- The left side shows all of the folder-level, file, or file extension exclusions added to all of the Workstations and Servers settings profiles created in the management console. These exclusions impact the security risk and are taken into account to calculate the risk level for your computers. See How risk assessment works and Calculation of the overall risk level for a specific computer.
- The right side shows the exclusions you have selected to not impact security risk status. These exclusions are not taken into account to calculate the overall risk level for your computers.

Click  to move the exclusions you do NOT want to impact security risk status to the right side of the dialog box. Click  to move exclusions back to the left side of the dialog box.

- Use the Control key to select multiple items at the same time. To select all items, click **Select all**.
- Click **Save**.

Viewing exclusions

The number of exclusions you have selected to not impact the risk level for your computers appears on the **Status** > **Risks** page. See Risk assessment module panels/widgets.

Risk assessment module lists

Accessing the lists

You can access the risk assessment lists in two ways:

- Select the **Status** menu at the top of the console.
- Select **Risks** from the side menu. Click the relevant widget.

  Or

- Select the **Status** menu at the top of the console.
- From the side panel, in the **My lists** section, click **Add**. The **Add list** window opens. This window shows all available lists.
- In the **General** section, select the risk list you want to use: **Risks by computer** or **Risks**. The list template opens. Edit and save it. The list is added to the **My lists** section in the side menu.

Risks by computer list

This list shows information about the risks detected on each computer or device as well as their risk level.

Field	Comment	Values
Computer	Computer name.	Character string
Group	Group to which the computer belongs.	Character string
Last connection	Date/time when the computer status was last sent to the Panda Security cloud.	Date/time
Risk level	Risk level for the computer or device. It is equal to the highest risk level for any risk detected on the computer.	• **No risk**: No risk was detected that had a critical, high, or medium risk level. • **Critical**: One or more risk detected have a critical risk level. • **High**: The highest risk level for any risk detected on the computer was high.

Field	Comment	Values
		• **Medium**: The highest risk level for any risk detected on the computer was medium.
Computer risks	Graph showing the risks detected on the computer or device during risk assessment.	• **Red**: Number of critical risks. • **Orange**: Number of high risks. • **Yellow**: Number of medium risks. • **Green**: Number of risks with no impact on security. • **Light gray**: Number of risks not compatible with the operating system installed on the computer or device. • **Dark gray**: Number of risks that were not evaluated because you did not enable them.

Table 16.2: Fields in the Risks by computer list

Click a row in the list to open the computer details page. See Computer details on page 236 and Details section (3) on page 248.

Fields displayed in the exported file

You can export the information in the list to a CSV file. Click the  icon. The exported file contains the following data:

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
Group	Folder in the Panda Endpoint Protection Plus group tree that	Character string

Field	Comment	Values
	the computer belongs to.	
Last connection	Date when the computer status was last sent to the Panda Security cloud.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android • iOS
Risk level	Overall risk level for the computer or device.	• No risk • Medium • High • Critical
Critical risks	Number of critical risks detected on the computer.	Numeric value
High risks	Number of high risks detected on the computer.	Numeric value
Medium risks	Number of medium risks detected on the computer.	Numeric value
No risk	Number of risks that have no impact on security.	Numeric value
Not applicable risks	Number of risks that do not apply to the computer based on the operating systems installed.	Numeric value
Not evaluated risks	Number of risks that you did not enable for evaluation.	Numeric value

Table 16.3: Fields in the Risks by computer exported file

Filter tool

To open the filter tool, click the **Filters** link next to the search box on the **Risks by computer** page. The filtering options are these:

Field	Comment	Values
Search computer	Filters computers by name.	Character string
Computer type	Filters computers according to type.	• Workstation • Laptop • Mobile device • Server
Last connection	Date when the computer risks were last sent to the Panda Security cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS • Android • iOS
Detected risk	The risk you enabled for evaluation.	• All • No protection • Out-of-date protection • Out-of-date knowledge (more than 30 days) • No connectivity to knowledge servers • No uninstallation protection

Field	Comment	Values
		• Anti-tamper protection disabled • File antivirus disabled • Anti-phishing protection disabled • Web browsing antivirus disabled • Folder, file, and extension exclusions • Critical patches pending installation
Risk level	Risk level assigned.	• Critical • High • Medium • No risk

Table 16.4: Filters available in the Risks by computer list

Risks list

The **Risks** list shows the risks you enabled for evaluation and the number of affected computers based on the risk level assigned to each risk. Click a row in the list to open the **Risks by computer** list.

The **Risks** list shows the following data:

Field	Comment	Values
Risk	Risk name.	Character string
Computers	Number of computers where the risk was detected.	Numeric value
Risk level	Risk level assigned.	• Critical • High • Medium • Risk of indicators of attack (see Risk

Field	Comment	Values
		assessment settings).
Risk by computers	Distribution graph that shows the number of computers where the risk was detected and the risk level assigned (Critical, High, Medium), and computers where there is no risk (the risk was selected for detection but was not detected).	• **Red**: Number of computers where the risk was detected and the risk level assigned is Critical. • **Orange**: Number of computers where the risk was detected and the risk level assigned is High. • **Yellow**: Number of computers where the risk was detected and the risk level assigned is Medium. • **Light gray**: Number of computers where the risk was not evaluated because it is not compatible with the operating system installed. • **Dark gray**: Number of computers where the risk was not evaluated because you did not enable it for detection.

Table 16.5: Fields in the Risks list

Fields in the exported file

You can export the information in the list to a CSV file. Click the  icon. The exported file contains the following data:

Field	Comment	Values
Client	Customer account the service belongs to.	Character

Field	Comment	Values
		string
Risk	Name of the risk you enabled for evaluation.	Character string
Risk level	Risk level assigned.	• Critical • High • Medium
Computers where the risk was detected	Number of computers where the risk was detected.	Numeric value
Critical	Number of computers in the account that have a Critical risk level.	Numeric value
High	Number of computers in the account that have a High risk level.	Numeric value
Medium	Number of computers in the account that have a Medium risk level.	Numeric value
Computers with no risk	Number of computers where the risk was not detected.	Numeric value
Computers the risk does not apply to	Number of computers where the risk was not evaluated because it is not compatible with the operating system installed.	Numeric value
Computers where the risk was not evaluated	Number of computers for which the risk was not enabled for detection.	Numeric value

Table 16.6: Fields in the Risks exported file

Filter tool

To open the filter tool, click the **Filters** link next to the search box on the **Risks** page. The filtering options are these:

Field	Comment	Values
Computer type	Filters computers according to type.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android • iOS

Table 16.7: Filters available in the Risks list

To schedule risk lists to be sent periodically, see *Scheduled sending of reports and lists on page 555*.

Risk assessment module panels/widgets

Accessing the dashboard

From the top menu, select **Status**. From the side menu, select **Risks**.

Company risk

This widget shows the number and percentage of computers on the network with an assigned risk level. The status of computers is indicated by a circle with various colors and associated counters.

At the bottom of the widget, a message appears that shows the number of exclusions that are not considered a risk, if any, based on the exclusion impact settings. When you click the message, the **Manage exclusion impact** dialog box opens. See Managing exclusion impact

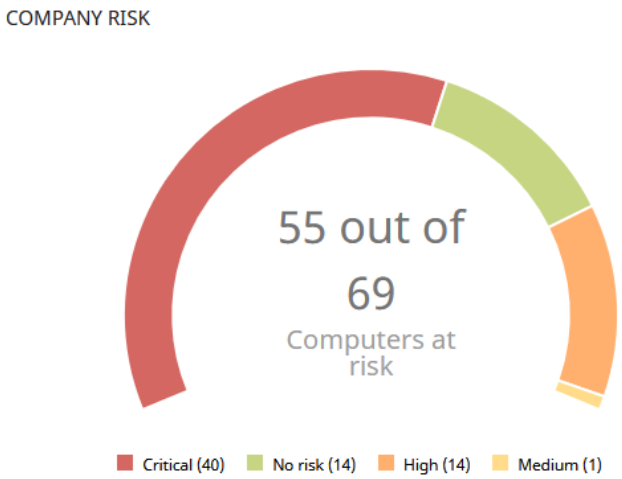


Figure 16.2: Company Risk panel

Meaning of the data displayed

Data	Description
Critical	Number of computers with a critical risk level.
High	Number of computers with a high risk level.
Medium	Number of computers with a medium risk level.
No risk	Number of computers that are not at risk.
Central area	Sum of all computers with an assigned risk level.

Table 16.8: Description of the data displayed in the Company Risk panel

Lists accessible from the panel

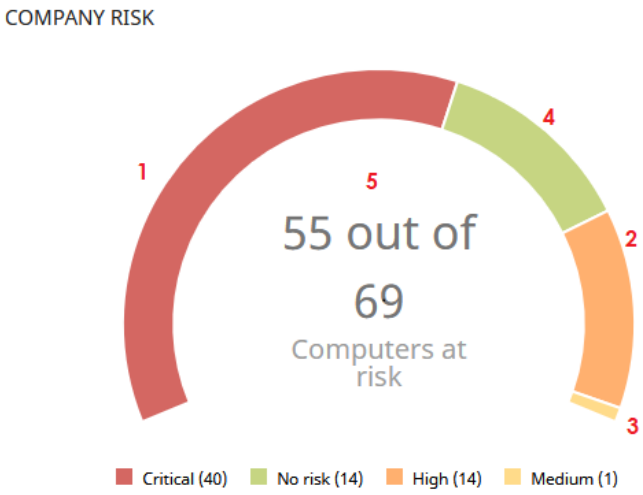


Figure 16.3: Hotspots in the Company Risk panel

Click the hotspots shown in **Hotspots in the Company Risk panel** to open the **Risks by computer** list with these predefined filters:

Hotspot	Filter
(1)	Risk = High
(2)	Risk = Critical
(3)	Risk = No risk
(4)	Risk = Medium
(5)	No filters

Table 16.9: Filters accessible from the Company Risk panel

Risks trend

This widget shows the number and types of risks that are detected over time.

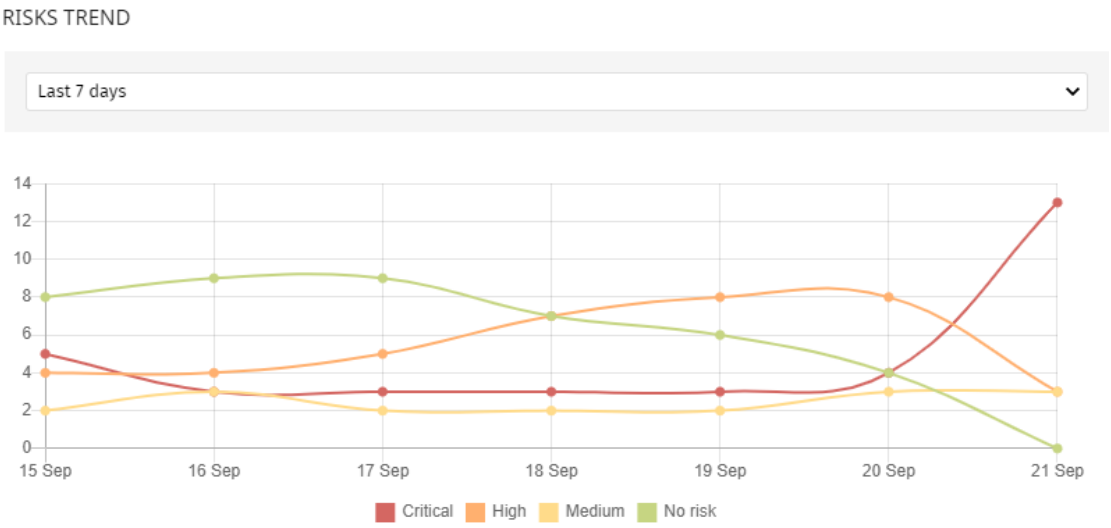


Figure 16.4: Risks Trend graph

Meaning of the data displayed

Data	Description
Critical risk	Trend of the number of computers with a critical risk level.
High risk	Trend of the number of computers with a high risk level.
Medium risk	Trend of the number of computers with a medium risk level.
No risk	Trend of the number of computers that have no risks.

Table 16.10: Description of the data displayed in the Risks Trend panel

Point the mouse to a node on the graph to show a label with this information:

- Date
- Risk level
- Number of affected computers

Lists accessible from the panel

Click the legend items under the graph to open the **Risks by computer** list filtered to show the selected item.

To open the **Risks by computer** full list with no filters applied, click an empty space on the graph.

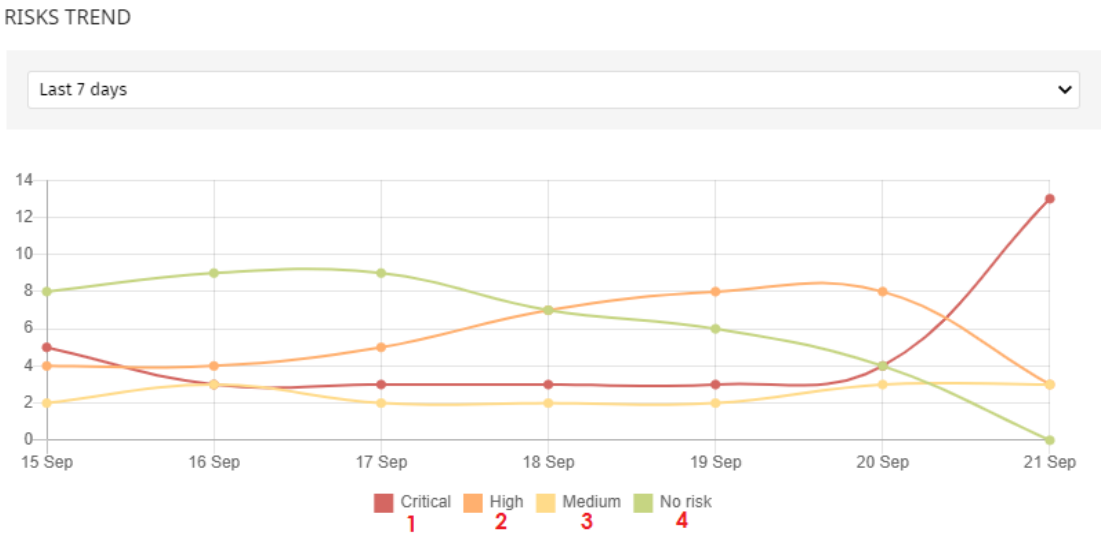


Figure 16.5: Hotspots in the Risks Trend graph

Hotspot	Filter
(1)	Risk = Critical
(2)	Risk = High
(3)	Risk = Medium
(4)	No risks

Table 16.11: Filters accessible from the Risks Trend panel

Detected risks

This widget shows the most commonly found risks on computers.

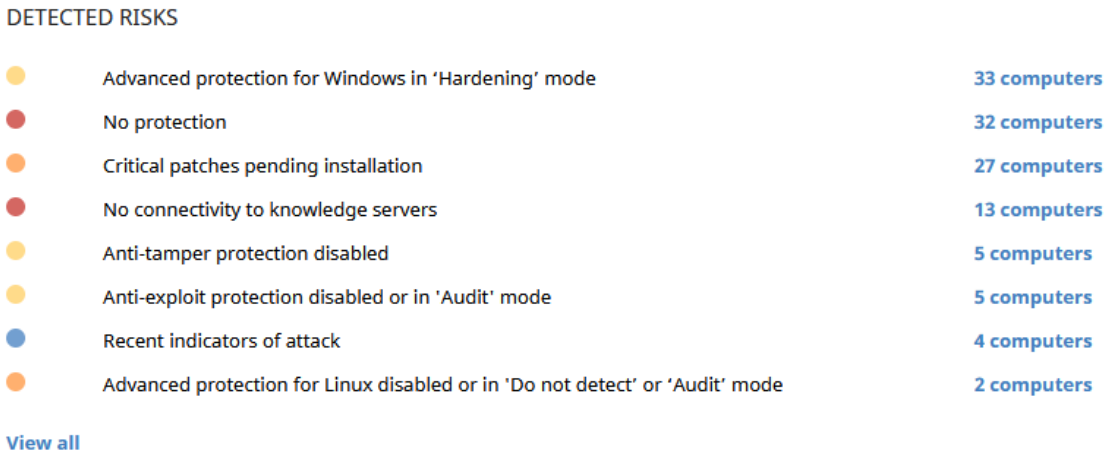


Figure 16.6: Detected Risks panel

Meaning of the data displayed

Data	Description
Icon	Risk level defined by you. • **Red**: Critical • **Orange**: High • **Yellow**: Medium • **Blue**: Custom
Name	Risk name.
Number	Number of computers where the risk was detected.
View all	Link to the full list of all of the risks detected.

Table 16.12: Description of the data displayed in the Detected Risks panel

Lists accessible from the panel

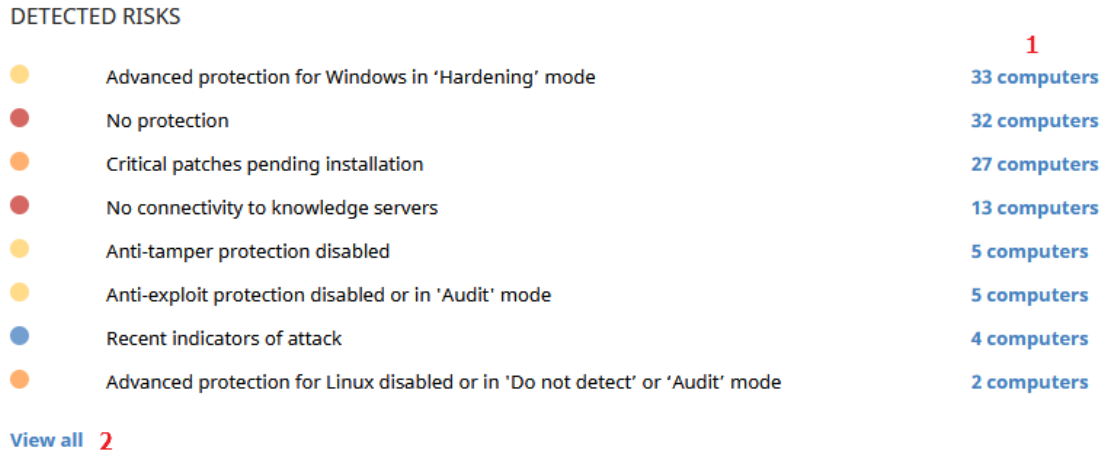


Figure 16.7: Hotspots in the Detected Risks panel

Click the hotspots shown in the figure to open these lists with these predefined filters:

Hotspot	List	Filter
(3)	Risks by computer	Detected risk = Risk selected on the widget
(4)	Risks	No filters

Table 16.13: Lists and filters accessible from the Detected Risks panel

Top 10 computers at risk

This widget shows the ten computers with the highest overall risk level.

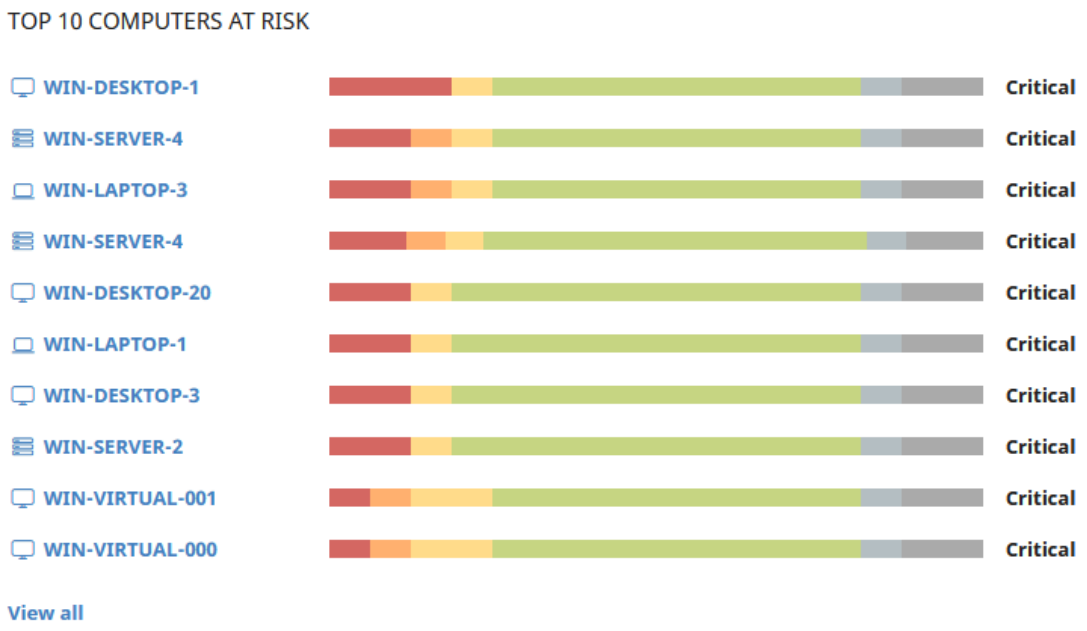


Figure 16.8: Top 10 Computers at Risk panel

A computer overall risk level is the highest risk level of the risk factors detected on the computer. For more information, see Calculation of the overall risk level for a specific computer.

Meaning of the data displayed

Data	Description
Name	Computer or device name and type.
Color bar	Type of risks found and the total number of risks.
Risk level	Overall risk level assigned to the computer.
View all link	Access to the Risks by Computer full list.

Table 16.14: Description of the data displayed in the Top 10 Computers at Risk panel

Lists accessible from the panel

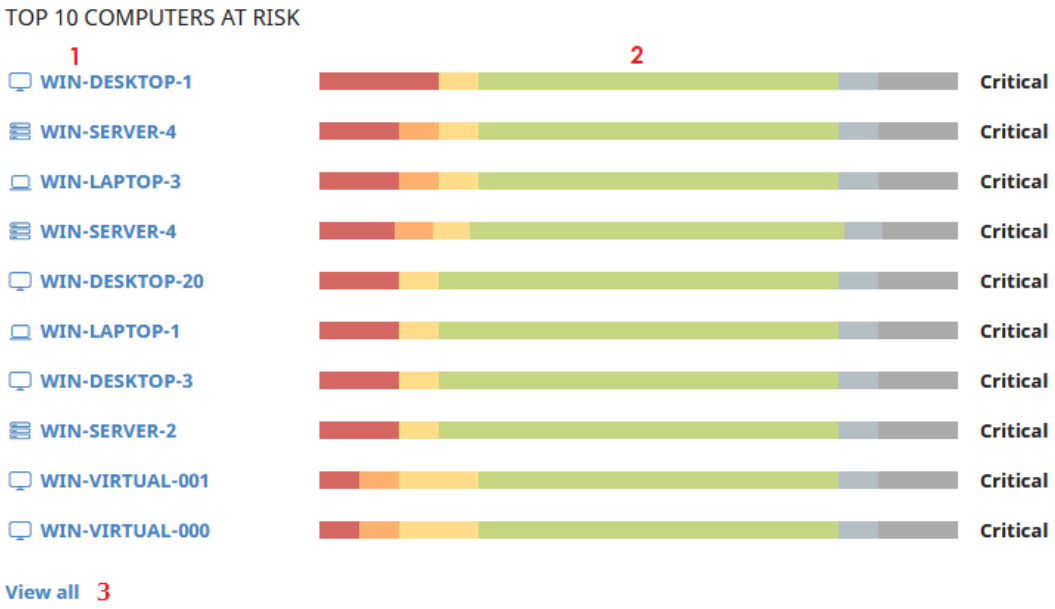


Figure 16.9: Hotspots in the Top 10 Computers at Risk panel

Click the hotspots shown in the figure to open these lists with these predefined filters:

Hotspot	List	Filter
(1)	Computer details	
(2)	Risks	Computer selected on the widget.
(3)	Risks by computer	No filters

Table 16.15: Lists and filters accessible from the Top 10 Computers at Risk panel

You can also review information on the status of the risks detected on a computer on the **Computer details** page. For more information, see Computer details on page 236.

Chapter 17

Vulnerability assessment

The vulnerability assessment module built on Aether platform finds computers on the network with known software vulnerabilities and reports on the availability of patches to mitigate vulnerability impact on computers.

Vulnerability assessment supports Windows, macOS, and Linux operating systems. It identifies third-party applications that have missing patches or have reached end of life (EOL), as well as the patches and updates released by Microsoft for all of its products (operating systems, databases, Office applications, etc.).

Vulnerability assessment does not install the identified patches on managed computers. You can install the required patches on your own or purchase the Patch Management module to install the patches centrally from the Panda Endpoint Protection Plus console.

For more information about the vulnerability assessment module, see:

Creating and managing settings profiles on page 267: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

Accessing, controlling, and monitoring the management console on page 53: Managing user accounts and assigning permissions.

Managing lists on page 41: Information about how to manage lists.

Chapter contents

Vulnerability assessment requirements

On 30 June 2025, our Windows and Mac protection for these OS versions will become End of Life (EOL): Windows XP, Vista, Server 2003, and Server 2008 (Windows 2008 R2 will continue to be supported) and macOS Yosemite, El Capitán, Sierra, High Sierra and Mojave. After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

Supported Windows operating systems

Workstations

- Windows 7 (32 and 64-bit)
- Windows 8 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 10 (32 and 64-bit)
- Windows 11 (64-bit)

Servers

- Windows 2008 (32 and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2, and 2016
- Windows Server 2022

Unsupported Windows computers

- The module does not install.
- Computers keep the vulnerability assessment settings profiles assigned to them, but they are not applied.
- The **Available patches by computers** list does not show information about these computers.

Supported macOS operating systems

- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura
- macOS Sonoma

Supported Linux operating systems

Supported 64-bit distributions:

- **Red Hat**: 7.0, 8.0
- **CentOS**: 7.0
- **SUSE Linux Enterprise**: 12, 15

Vulnerability assessment settings

Accessing the settings

- Select **Settings** from the top menu. Select **Vulnerability assessment** from the side menu.
- Click the **Add** button. The settings page opens.

Required permissions

Permission	Access type
Configure vulnerability assessment	Create, edit, delete, copy, or assign vulnerability assessment settings profiles.
View available patches	View vulnerability assessment settings profiles.

Table 17.1: Permissions required to access the vulnerability assessment settings

General options

To enable the solution to automatically search for available patches, enable **Automatically search for patches**. If this option is not enabled, the solution lists do not show missing patches, although you can use patch installation tasks to install missing patches on computers.

Network administrators can choose between installing patches manually or using a third-party tool. However, by purchasing the Panda Patch Management module, you can install patches centrally and automatically from the Panda Endpoint Protection Plus console.

Search frequency

Search for patches with the following frequency specifies how often vulnerability assessment searches the cloud-based patch databases to check for missing patches for your computers.

Patch criticality

Specifies the importance (or criticality) of the security patches that vulnerability assessment searches for.

Windows Service Packs are not applied to macOS or Linux computers or devices.

Software vendors define the importance of the security patches they make available to address vulnerabilities. Patch classifications are not universal and vary by vendor. To determine whether you want to install a patch, we recommend that you review its description, especially for patches that a vendor does not classify as Critical.

*Patches containing bug fixes and feature enhancements for macOS and Linux are included in the **Other patches (non-security related)** category.*

Vulnerability assessment module panels/widgets

Discover Patch Management

Panda Patch Management is a built-in module on Aether platform that finds computers on the network with known software vulnerabilities and updates them centrally and automatically.

For more information about Panda Patch Management, click the **Watch video** or **More information** links.

To close the informational message or not see it again, click the  icon.

Accessing the dashboard

To access the dashboard, select **Status** from the top menu. Select **Vulnerability assessment** from the side menu.

Required permissions

Permissions	Access to widgets
No permissions	• Vulnerability assessment status • Time since last check

Permissions	Access to widgets
View available patches	• End-of-Life programs • Available patches • Available patches trend • Most available patches for computers • Programs with most available patches

Table 17.2: Permissions required to access the vulnerability assessment widgets

Vulnerability assessment status

Shows computers where vulnerability assessment is working correctly and computers 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 shows the number and percentage of computers with the same status.

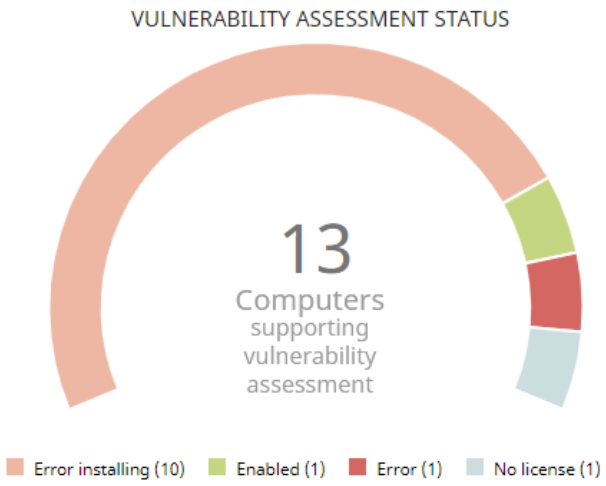


Figure 17.1: Vulnerability assessment status panel

Meaning of the data displayed

Data	Description
Enabled	Shows the percentage of computers where the vulnerability assessment module installed successfully, runs with no issues, and the assigned settings enable the module to search for patches automatically.
Disabled	Shows the percentage of computers where the vulnerability assessment module installed successfully, runs with no issues, but the assigned settings do not enable the module to search for patches automatically.

Data	Description
No license	Computers where the vulnerability assessment service does not work because no Panda Endpoint Protection Plus license is assigned to the computer or there are insufficient licenses.
Error installing	Computers where the module could not install.
No information	The computer has a license, but has not yet reported status to the server, or has an outdated agent installed.
Error	The vulnerability assessment module does not respond to requests sent from the server, or has settings that are different from those configured in the web console.
Central area	Shows the total number of computers compatible with the vulnerability assessment module.

Table 17.3: Description of the data displayed in the Vulnerability assessment status panel

Lists accessible from the panel

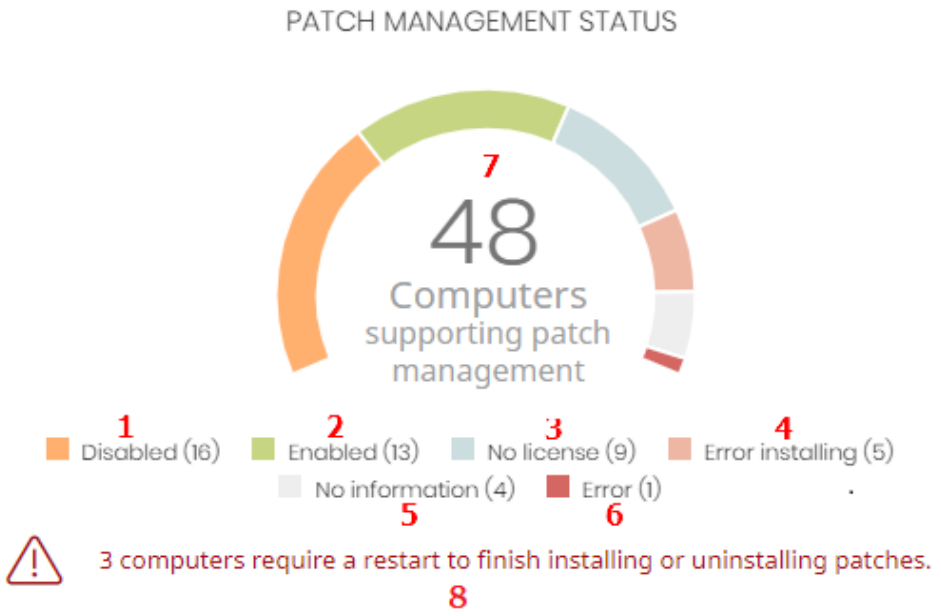


Figure 17.2: Hotspots in the Vulnerability assessment status panel

Click the hotspots shown in **Hotspots in the Vulnerability assessment status panel** to open the **Vulnerability assessment status** list with the following predefined filters:

Hotspot	Filter
(1)	Vulnerability assessment status = Disabled.
(2)	Vulnerability assessment status = Enabled.
(3)	Vulnerability assessment status = No license.
(4)	Vulnerability assessment status = Error installing.
(5)	Vulnerability assessment status = No information.
(6)	Vulnerability assessment status = Error.
(7)	No filters.

Table 17.4: Filters available for the Vulnerability assessment status list

Time since last check

Shows the number of computers that have not connected to the Panda Security cloud and reported patch status for more than 3, 7, and 30 days. Use this panel to identify computers that might be at risk and require your attention.

Figure 17.3: Time since last check panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported patch status in the last 72 hours.
7 days	Number of computers that have not reported patch status in the last 7 days.

Data	Description
30 days	Number of computers that have not reported patch status in the last 30 days.

Table 17.5: Description of the data displayed in the Time since last check panel

Lists accessible from the panel

Figure 17.4: Hotspots in the Time since last check panel

Click the hotspots shown in Figure 17.4: to open the **Vulnerability assessment status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago and Vulnerability assessment status = Enabled or Disabled or No information or Error.
(2)	Last connection = More than 7 days ago and Vulnerability assessment status = Enabled or Disabled or No information or Error.
(3)	Last connection = More than 30 days ago and Vulnerability assessment status = Enabled or Disabled or No information or Error.

Table 17.6: Filters available for the Vulnerability assessment status list

End-of-Life programs

Shows information about programs that have reached or are close to end of life, grouped by end-of-life date.

Figure 17.5: End-of-Life programs panel

Meaning of the data displayed

Data	Description
Currently in EOL	Programs that have reached end of life.
In EOL (currently or in 1 year)	Programs that have reached end of life or will in the next year.
With known EOL date	Programs that have a known end-of-life date more than one year in the future.

Table 17.7: Description of the data displayed in the End-of-Life programs panel

Lists accessible from the panel

Figure 17.6: Hotspots in the End-of-Life programs panel

Click the hotspots shown in Figure 17.6: to open 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 17.8: Filters available for the End-of-Life programs list

Available patches

Shows the number of patches of different types that are available for computers on the network. Numbers in this panel count the same patch multiple times if multiple computers do not have the patch installed.

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as Critical that are missing from computers.
Security patches - Important	Number of security patches classified as Important that are missing from computers..
Security patches - Low	Number of security patches classified as Low that are missing from computers.
Security patches - Unspecified	Number of security patches that do not have a severity classification and are missing from computers.
Other patches (non-security related)	Number of patches not related to security that are missing from computers.
Service Packs	Number of patch and hotfix bundles that are missing from computers. Not applicable for Linux or macOS computers.

Table 17.9: Description of the data displayed in the Available patches panel

Lists accessible from the panel

Click the hotspots shown in to open the **Available patches by computers** 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.

Hotspot	Filter
(7)	No filters.

Table 17.10: Filters available for the Available patches by computers list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation • Laptop • Server
Platform	• All • Windows • Linux • macOS
Patch type	• Operating system patches: Patches available for Windows, Linux, and macOS operating systems. • App patches: Patches available for apps.

Table 17.11: Filters available in the Available patches widget

Available patches trend

Shows the trend of the number of patches that are pending installation on the computers on the network, grouped by severity.

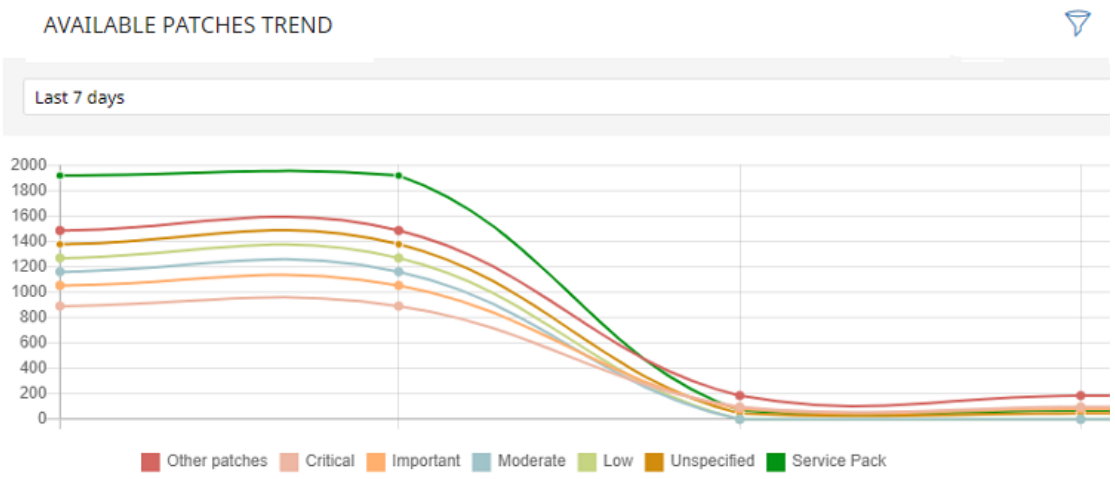


Figure 17.7: Available patches trend graph

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as Critical that are missing from computers.
Security patches - Important	Number of security patches classified as Important that are missing from computers..
Security patches - Low	Number of security patches classified as Low that are missing from computers.
Security patches - Unspecified	Number of security patches that do not have a severity classification and are missing from computers.
Other patches (non-security related)	Number of patches not related to security that are missing from computers.
Service Packs	Number of patch and hotfix bundles that are missing from computers. Not applicable for Linux or macOS computers.

Table 17.12: Description of the data displayed in the Available patches trend panel

Point to a node on the graph to show a tooltip with this information:

- Date
- Type
- Number of patches

Lists accessible from the panel

Click the legend items below the graph to open the Available patches by computers list filtered by the selected item. Click the graph to open the full Available patches by computers list with no filters applied.

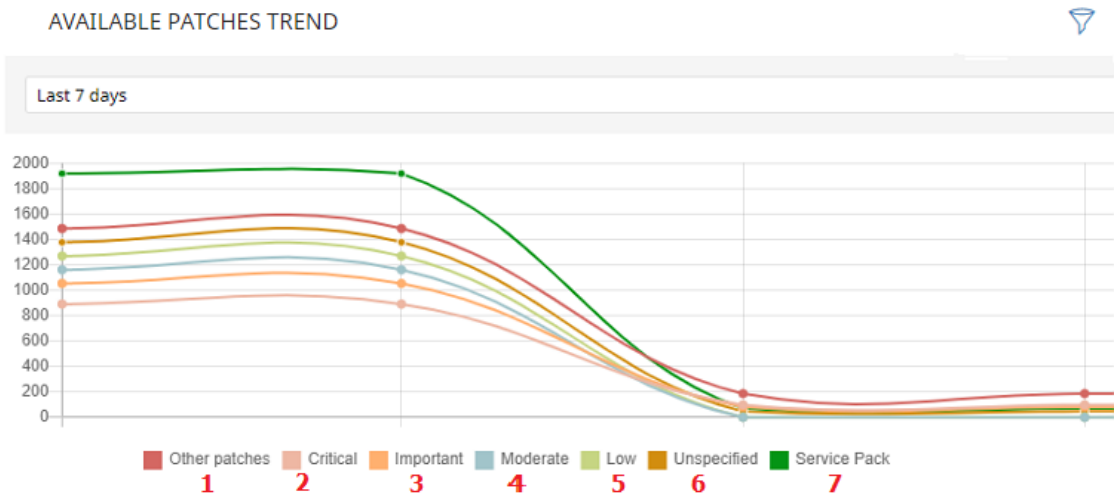


Figure 17.8: Data displayed in the Available patches trend graph

Hotspot	Filter
(1)	Criticality = Other patches (non-security-related).
(2)	Criticality = Critical (security-related).
(3)	Criticality = Important (security-related).
(4)	Criticality = Moderate (security-related).
(5)	Criticality = Low (security-related).
(6)	Criticality = Unspecified (security-related).
(9)	Criticality = Service Pack.

Table 17.13: Filters available for the Available patches by computers list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation

Filter	Definition
	• Laptop • Server
Platform	• All • Windows • Linux • macOS
Patch type	• Operating system patches: Patches available for Windows, Linux, and macOS operating systems. • App patches: Patches available for apps.

Table 17.14: Filters available in the Available patches trend widget

Most available patches for computers

Lists available patches (in **Pending** status) and the number of devices the patch is available for, in descending order from left to right.

Meaning of the data displayed

Data	Description
Name	Name of the available patch.
Number	Number of computers the patch is available for (the patch is in **Pending** status).
View all available patches link	Access to the Available patches by computers full list

Table 17.15: Description of the data displayed in the Most available patches for computers panel

Point to a box in the panel to see a summary of the patch, including:

- Patch name.
- Number of affected computers.
- Program (or operating system family).
- Criticality.

- Release date
- CVE (Common Vulnerabilities and Exposures) ID.

Lists accessible from the panel

Click a box in the panel to open the **Available patches by computers** list filtered to the selected patch.

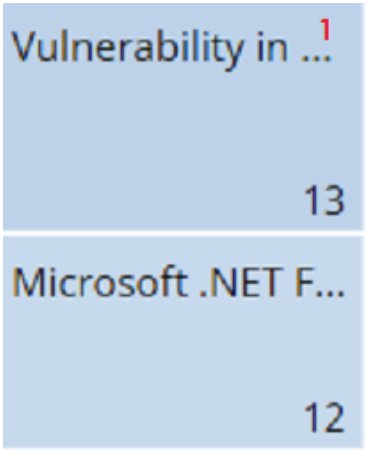


Figure 17.9: Hotspots in the Most available patches for computers panel

Hotspot	Filter
(1)	Patch = Name of the selected patch.

Table 17.16: Lists available from the Most available patches for computers panel

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop

Filter	Description	Values
		• Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Operating system patches

Table 17.17: Filters available in the Most available patches for computers panel

Programs with most available patches

Lists the programs that are missing patches, as well as the number of patches the program is missing, in descending order from left to right.

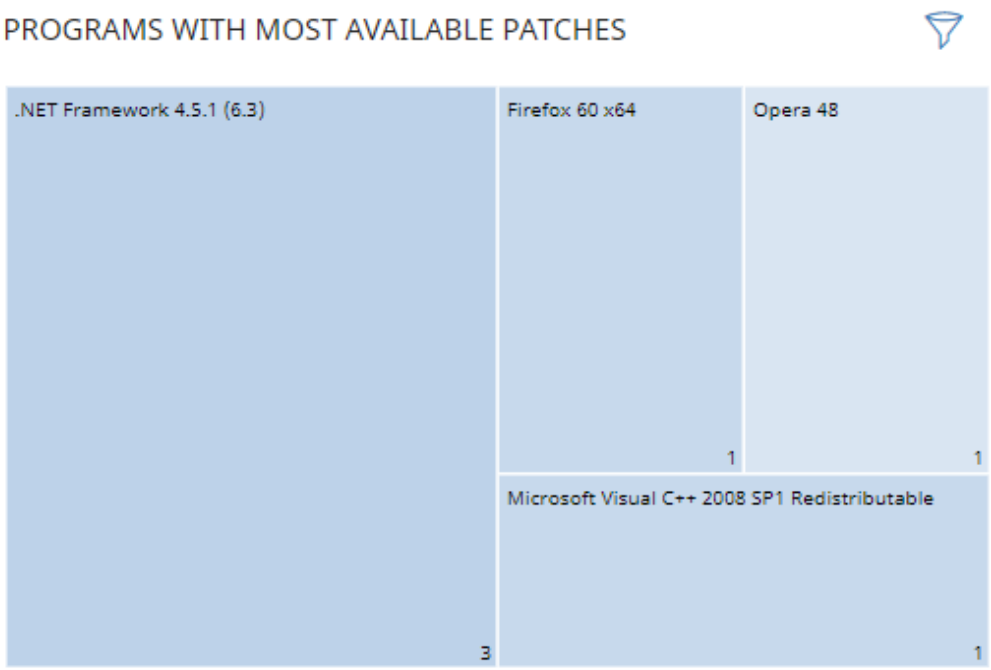


Figure 17.10: Programs with most available patches panel

Meaning of the data displayed

Data	Description
Name	Name of the program that is missing patches.

Data	Description
Number	Number of patches the program is missing.

Table 17.18: Description of the data displayed in the Programs with most available patches panel

Point to a box in the panel to see this information:

- Program name.
- Number of patches the program is missing.

Lists accessible from the panel

Click a box in the panel to open the **Available patches by computers** list filtered to the selected program.

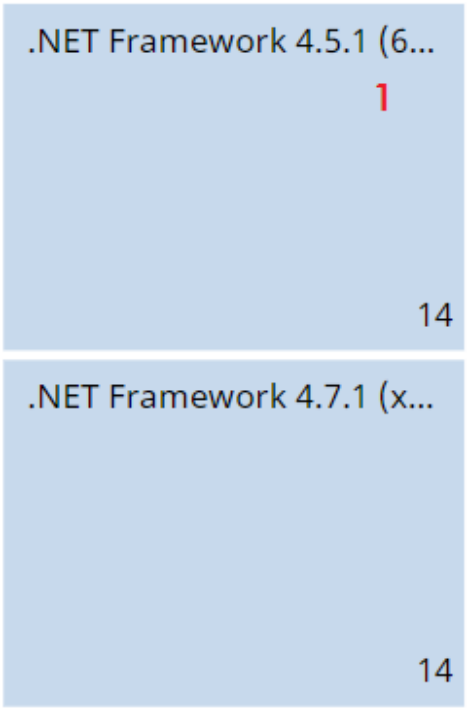


Figure 17.11: Hotspots in the Programs with most available patches panel

Hotspot	Filter
(1)	Program = Name of the selected program.

Table 17.19: Lists available from the Programs with most available patches panel

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Operating system patches

Table 17.20: Filters available in the Programs with most available patches panel

Vulnerability assessment module lists

Accessing the lists

There are two methods to access the lists:

- Select **Status** from the top menu. Select **Vulnerability assessment** from the side menu. Click the relevant widget.

  Or,

- Select **Status** from the top menu. Click the **Add** link from the side menu. A window opens with the available lists.

- Select a list from the **Vulnerability assessment** section to view the associated template. Edit the template and click **Save**. The list is added to the side menu.

Required permissions

Permissions	Access to lists
No permissions	• Vulnerability assessment status
View available patches	Read-only access to these lists: • Vulnerability assessment status • Available patches by computers • End-of-Life programs

Table 17.21: Permissions required to access the vulnerability assessment lists

Vulnerability assessment status

Shows all computers on the network that are compatible with vulnerability assessment (with filters that enable you to identify workstations and servers that are not using the service due to any of the reasons shown in the associated panel).

Field	Comment	Values
Computer	Name of the computer with out-of-date software.	Character string
Computer status	Agent reinstallation: • Reinstalling the agent. • Error reinstalling the agent. Protection reinstallation: • Reinstalling the protection. • Error reinstalling the protection. • Pending restart. Computer isolation status: • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated.	Icon

Field	Comment	Values
	"RDP attack containment" mode: • Computer in "RDP attack containment" mode. • Ending "RDP attack containment" mode.	
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Vulnerability assessment	Module status.	• Enabled • Disabled • Installation error (error reason) • No license • — No information • Error
Last checked	Date when vulnerability assessment last queried the cloud to check whether new patches had been published.	Date
Last connection	Date when the vulnerability assessment status was last sent to the Panda Security cloud.	Date

Table 17.22: Fields in the Vulnerability assessment status list

To view a graphical representation of the list data, access the Vulnerability assessment status widget.

Fields displayed in the exported file

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

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer with out-of-date software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Agent version		Character string
Installation date	Date when the 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
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether the protection module installed on the computer is updated to the latest version or not.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date the signature file was last updated.	Date

Field	Comment	Values
Vulnerability assessment status	Module status.	• Enabled • Disabled • Install error • No license • No information • Error
Last checked	Date when vulnerability assessment last queried the cloud to check whether new patches had been published.	Date
Installation error date	Date of the unsuccessful attempt to install the module.	Date
Installation error	Reason for the installation error.	• Download error • Execution error
Vulnerability assessment error	Error searching for available patches	Numeric value

Table 17.23: Fields in the Vulnerability assessment status exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Last checked	Date when vulnerability assessment last queried the cloud to check whether new patches had been published.	• All • More than 3

Field	Comment	Values
		days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the agent last connected to the Panda Security cloud.	Date
Vulnerability assessment status	Module status.	• Enabled • Disabled • Install error • No license • No information • Error

Table 17.24: Filters available in the Vulnerability assessment status list

Computer details page

Click any of the rows in the list to open the computer details page. See Computer details on page 236 for more information.

Available patches by computers

Shows all patches that are available for computers and information about patches in the process of installation.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Version	Version number of the out-of-date program.	Numeric value
Release date	Date when the patch was released for download and application.	Date

Field	Comment	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computers	Number of computers the patch is available for.	Numeric value

Table 17.25: Fields in the Available patches by computers list

To view a graphical representation of the list data, access the Available patches on page 361 widget.

Fields displayed in the exported file

Use the context menu to export the data. The export file can include all data in the list of available patches or a smaller version that shows information about the available patches in the last 7 days, the last month, or the last year.

Field	Comment	Values
Vendor	The company that created the out-of-date program.	Character string
Product family	Name of the product with patches pending installation or a reboot.	Character string
Program version	Version number of the out-of-date program.	Numeric value

Field	Comment	Values
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Version	Version number of the out-of-date program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Criticality	Update severity classification 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 the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date

Field	Comment	Values
Computers	Number of computers the patch is available for.	Numeric value
Platform	Operating system installed on the computer.	• Windows • Linux • macOS

Table 17.26: Fields in the Available patches by computers exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Patch type	Type of available patch.	• App patches • Operating system patches
Search computer	Computer name.	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Select a program	The search applies to the selected program, product	Character string

Field	Comment	Values
version, family, or vendor	family, or company.	
Criticality	Indicates the update severity classification 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 patches that cannot be downloaded directly because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.)	Boolean

Table 17.27: Filters available in the Available patches by computers list

Detected patch page

Click a row in the list. The **Detectedpatch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the computer.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Field	Comment	Values
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Program version	Version number of the out-of-date program. Not available for macOS or Linux patches.	Character string
Family	Name of the product with patches pending installation or a reboot. Not available for macOS or Linux patches.	Character string
Vendor	The company that created the out-of-date program. Not available for macOS or Linux patches.	Character string
Criticality	Indicates the update severity classification 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
Release date	Date when the patch was released for download and application.	Date

Field	Comment	Values
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and the patch requirements (if any). Not available for macOS or Linux patches.	Character string
Description	Information about the impact the vulnerability could have on computers. Not available for macOS or Linux patches.	Character string

Table 17.28: Fields on the Detected patch page

End-of-Life programs

Shows information about programs that have reached or are close to end of life. These programs are no longer supported by the software vendor and are particularly vulnerable to malware and cyberthreats.

Field	Comment	Values
Computer	Name of the computer with software that has reached end of life.	Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Program	Name of the program that has reached end of life.	Character string
Version	Version of the program that has reached end of life.	Character string
EOL	Date when the program reached end of life.	Date (in red if the program has reached end of life)

Table 17.29: Fields in the End-of-Life programs list

To view a graphical representation of the list data, access the End-of-Life programs on page 357.

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
IP address	The computer's primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Program	Name of the program that has reached end of life.	Character string
Version	Version of the program that has reached end of life.	Character string
EOL	Date when the program reached end of life.	Date
Last seen	Date when the computer was last discovered.	Date

Table 17.30: Fields in the End-of-Life programs exported file

Filter tool

Field	Comment	Values
Search computer	Computer name.	Character string

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
End-of-Life date	Date when the program will reach end of life.	• All • Currently in End of Life • In End of Life (currently or in 1 year)

Table 17.31: Filters available in the End-of-Life programs list

Program details page

Click a row in the list. The **Program details** page opens.

Field	Comment	Values
Program	Name of the program or Windows operating system version that received the patch.	Character string
Family	Bundle, suite, or program group the software belongs to.	Character string
Publisher/Company	Company that designed or published the program.	Character string
Version	Program version.	Character string
EOL	Date when the program reached end of life.	Date

Table 17.32: Fields on the Program details page

Chapter 18

Managing threats, items in the process of classification, and quarantine

Panda Endpoint Protection Plus provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This is achieved through tools that enable you to manage threat detection.

Chapter contents

Introduction to threat management tools

You can change the behavior of Panda Endpoint Protection Plus with regard to found threats using these tools:

- Allow the execution of programs classified as a virus.
- Do not detect a program classified as a virus again.
- Manage the backup/quarantine area.

Do not detect a program classified as a virus again

Administrators can allow software that Panda Endpoint Protection Plus classified as a threat. For example, a toolbar with extra search capabilities classified as a PUP. For more information, see Allowing blocked items to run.

Manage the backup/quarantine area

You have tools to restore items considered to be threats deleted from user computers.

Allowing blocked items to run

Restoring or stopping detecting programs classified as viruses

If users have to use certain features provided by a program whose signature file was classified as a threat, and you determine that the danger posed to the integrity of the managed IT network is low, you can allow the program to run.

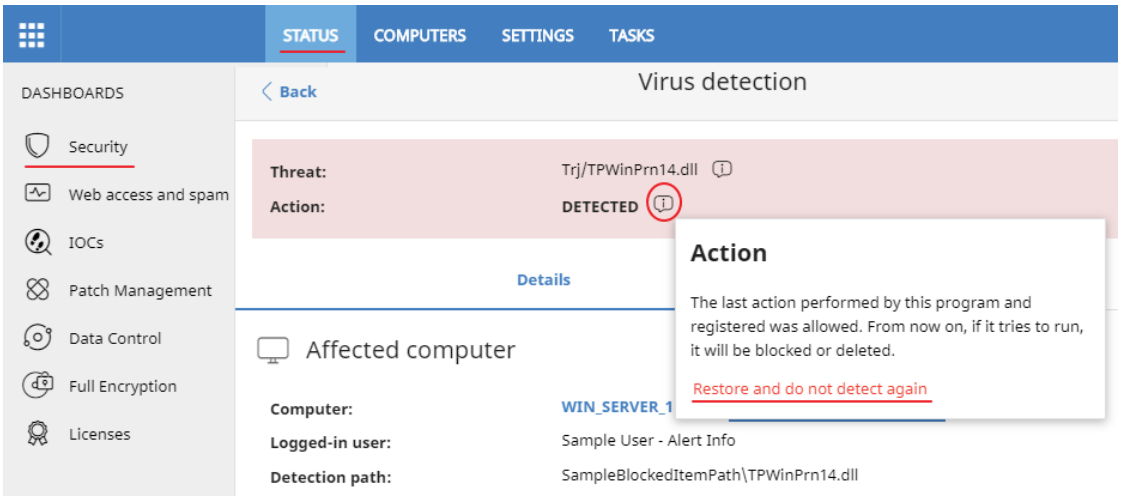


Figure 18.1: Restore and do not detect a threat again

To restore deleted programs from the quarantine or backup area and not detect them again:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Threats detected by the antivirus** panel and select the item that you want to allow to run.
- On the details page, click the  icon next to the action. A pop-up dialog box describes the action taken by Panda Endpoint Protection Plus.
- Click **Restore and do not detect again**. Panda Endpoint Protection Plus performs these actions:
  - Copies the item from quarantine or the backup area to its original location on the computers in the network.
  - Allows the item to run and does not generate any detections.
  - Adds the item to the **Programs allowed by the administrator** list.

Stopping allowing the execution of previously allowed items

To block a previously allowed item again:

- From the top menu, select **Status**. From the side panel, select **Security**.
- In the **Detected items allowed by the administrator** panel, select the type of item you want to stop allowing: **Malware**, **PUP**, **Exploit**, **Being classified**, or **Network attacks**.
- In the **Programs allowed by the administrator** panel, select the type of item you want to stop allowing: **Malware**, **PUP**, **Exploit**, **or Being classified**.
- In the **Programs allowed by the administrator** list, click the  icon to the right of the item that you want to stop allowing to run.

Panda Endpoint Protection Plus performs these actions:

- Removes the item from the **Programs allowed by the administrator** list.
- Adds an entry to the **History of programs allowed by the administrator** list. The **Action** column shows **Exclusion removed by the user**.
- If it is virus, the item reappears in the **Threats detected by the antivirus** list.
- Resumes generating incidents for the item.

Information about detected threats

You can get information about the programs classified as a threat by the signature file in the **Threats detected by the antivirus** panel and the list of the same name. See Security module panels/widgets on page 445.

List of allowed threats

You have multiple panels and lists available to get information about programs that you allow which Panda Endpoint Protection Plus initially prevented from running:

- The **Programs allowed by the administrator** panel.
- The **Programs allowed by the administrator** list.
- The **History of programs allowed by the administrator** list.

Programs allowed by the administrator

This panel shows programs the administrator allows which Panda Endpoint Protection Plus initially quarantined. These programs were considered as a threat because they were detected by the signature file.

Figure 18.2: Panel Programas permitidos por el administrador

Meaning of the data displayed

The panel shows the total number of items excluded from blocking, broken down by type:

- Malware
- PUPs
- Being classified
- Exploits

Lists accessible from the panel

Figure 18.3: Zonas activas del panel Programas permitidos por el administrador

Click the hotspots in Figure 18.3: to open the Programs allowed by the administrator list list with these predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Classification = Malware.
(3)	Classification = PUP.
(4)	Classification = Being classified (blocked and suspicious items).

Hotspot	Filter
(5)	Classification = Exploit.

Table 18.1: Filters available in the Programs Allowed by the Administrator list

Programs allowed by the administrator list

This list shows all items the administrator allows which Panda Endpoint Protection Plus considered a threat.

Field	Description	Values
Classification	Type of threat that is allowed to run.	• Malware • PUP • Goodware
Threat	Name of the item that is allowed to run.	Character string
Details	Name of the file that contains the threat.	Character string
Hash	String that identifies the file.	Character string
User name	Console user account that added the item exclusion.	Character string
Date allowed	Date the event took place.	Date
Delete	Removes the item exclusion.	

Table 18.2: Fields in the Programs Allowed by the Administrator list

Fields displayed in the exported file

Field	Description	Values
Details	Name of the file that contains the threat.	Character string
Current type	Current classification of the threat that is allowed to run.	• Malware • PUP • Goodware
Original type	Classification of the threat that is allowed to run when it was initially detected.	• Malware • PUP

Field	Description	Values
		• Goodware
Threat	Name of the item that is allowed to run.	Character string
Hash	String that identifies the file.	Character string
User name	User account which triggered the change to the allowed file.	Character string
Date allowed	Date the event was logged.	Date

Table 18.3: Fields in the Detected Items Allowed by the Administrator exported file

Filter tool

Field	Description	Values
Search	• **Details**: Details of the threat. • **Threat**: Name of the threat detected. • **User name**: Console user account that added the item exclusion. • **Hash**: String that identifies the file.	Enumeration

Table 18.4: Filters available in the Detected Items Allowed by the Administrator list

History of programs allowed by the administrator list

This list shows a history of all events related to threats that the administrator allowed to run. This list shows all classifications that a file has gone through, from the time it entered the **Programs allowed by the administrator** list until it left it, as well as all other classifications caused by Panda Endpoint Protection Plus or by you.

This list does not have a corresponding panel. You must access it through the **History** button in the upper-right corner of the **Programs allowed by the administrator** page.

Field	Description	Values
Classification	Type of threat that is allowed to run.	• Malware • PUP • Goodware

Field	Description	Values
Threat	Name of the item that is allowed to run.	Character string
Details	Name of the file that contains the threat.	Character string
Hash	String that identifies the file.	Character string
Action	Action taken on the allowed item. • **Exclusion removed by the user**: You allowed the item to be quarantined again. • **Exclusion added by the user**: You allowed the item to be removed from quarantine.	Enumeration
User name	User account which triggered the change to the allowed file.	Character string
Date allowed	Date the event was logged.	Date

Table 18.5: Fields in the History of Items Allowed by the Administrator list

Fields displayed in the exported file

Field	Description	Values
Details	Name of the file that contains the threat.	Character string
Current type	Current classification of the threat that is allowed to run.	• Malware • PUP
Original type	Classification of the threat that is allowed to run when it was initially detected.	• Malware • PUP
Threat	Name of the malware or PUP that is allowed to run.	Character string
Hash	String that identifies the file.	Character string
Action	Action taken on the allowed item. • **Exclusion removed by the user**: You allowed the item to be quarantined again. • **Exclusion added by the user**: You allowed the item to be	Enumeration

Field	Description	Values
	removed from quarantine.	
User name	Console user account that added the item exclusion.	Character string
Date allowed	Date the event took place.	Date

Table 18.6: Fields in the History of Programs Allowed by the Administrator exported file

Filter tool

Field	Description	Values
Search	• **Details**: Details of the threat. • **User name**: Console user account that added the item exclusion. • **Hash**: String that identifies the file.	Enumeration
Action	Action taken on the allowed item. • **Exclusion removed by the user**: You allowed the item to be blocked again. • **Exclusion removed after reclassification**: Panda Endpoint Protection Plus applied the action associated with the category after reclassification. • **Exclusion added by the user**: You allowed the item to be run. • **Exclusion kept after reclassification**: Panda Endpoint Protection Plus did not block the item after reclassification.	Enumeration

Table 18.7: Filters available in the History of Programs Allowed by the Administrator list

Managing the backup/quarantine area

The Panda Endpoint Protection Plus quarantine is a backup area that stores items that were deleted after being classified as a threat.

Quarantined items are stored on the user computer, in a `Quarantine` folder in the software installation directory. This folder is encrypted and cannot be accessed by any other process. It is therefore impossible to directly access or run the programs there.

The quarantine feature is only available on Windows, macOS, and Linux endpoints.

The classification and type of threat determines the actions that Panda Security takes on the detected file:

- **Malicious files for which disinfection is not possible**: The file is moved to quarantine permanently.
- **Malicious files for which disinfection is possible**: The file is disinfected and restored to its original location. A copy of the file is stored in quarantine for 30 days.
- **Non-malicious items**: Files determined to be goodware and incorrectly classified as malware (false positive), are automatically restored from quarantine to their original location. A copy of the file is stored in quarantine for seven days
- **Suspicious items**: Files are stored in quarantine for 30 days. If they a determined to be goodware, they are restored to their original location.

Panda Endpoint Protection Plus does not permanently delete files from user computers. All deleted files are sent to a backup folder.

Reviewing quarantined files

To review a list of quarantined items:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Threats detected by the antivirus** panel.
- Click **Filters**. In the **Action** area, select the **Quarantined** and **Deleted** checkboxes. Click **Filter**.

Restoring files from quarantine

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Threats detected by the antivirus** panel.
- Click **Filters**. In the **Action** area, select the **Quarantined** and **Disinfected** checkboxes.
- Next to the **Action**, click the icon. A pop-up describes why the item was moved to quarantine.
- Click **Restore and do not detect again**. The file is restored to its original location. The permissions, owner, and registry entries related to the file are also restored.

Chapter 19

Alerts

The alert system is a resource provided by Panda Endpoint Protection Plus to quickly notify administrators of situations that might affect the correct operation of the security service.

Namely, an alert is sent to the administrator every time one of these events occurs:

- The security software detects a malware specimen.
- The security software detects network attack activity.
- There is an attempt to use an unauthorized external device.
- The security software reclassifies an unknown item (malware or PUP).
- There is a license status change.
- There are installation errors or a computer is unprotected.

Chapter contents

Email alerts

Email alerts are messages generated and sent by Panda Endpoint Protection Plus to the configured recipients (typically the network administrator) when certain events occur.

Accessing the alert settings

From the top menu, select **Settings**. From the side menu, select **My alerts**. The **Email alerts** page opens, where you can configure the email alert settings.

Alert settings

The alert settings page is divided into three sections:

- **Send alerts in the following cases**: Select which events will trigger an alert. For more information, see Alert types .
- **Send the alerts to the following address**: Enter the email addresses of the alert recipients.
- **Send the alerts in the following language**: Choose the alert message language from those supported in the console:
  - German
  - Spanish
  - French
  - English
  - Italian
  - Japanese
  - Hungarian
  - Portuguese
  - Swedish

Alert export

If the console user has Total Control permissions, they can export the **My alerts** settings for all account users that have specified alert recipient email addresses. See Alert settings.

To export the settings, click the  icon in the upper-right corner of the **Email alerts** page.

Fields displayed in the exported file

Field	Description	Values
Customer	Customer account.	Character string
User	Panda Endpoint Protection Plus console user who configured **My alerts**.	Character string
Login email	Email address with which the user logs in to the Panda Endpoint Protection Plus console.	Character string
Blocked	Indicates whether the user can access the Panda Endpoint Protection Plus console. See Managing user accounts on page 55.	• Yes • No
Active cases to	Indicates whether the user has configured alerts to send in the	• Yes

Field	Description	Values
send	**My alerts** settings. See Alert settings.	• No
Destination address	Alert recipient email addresses specified by the user.	Character string

Table 19.1: Fields in the Alerts Destinations exported file

Access permissions and alerts

You define alerts for each web console user. The content of an alert email varies with the managed computers that are visible to the recipient.

Alert types

Type	Frequency	Condition	Information shown
Malware detections (real-time protection only)	The solution sends a maximum of two messages for each computer each day.	• Sends an alert for each malware detected in real time on a computer • Windows computers only.	• First or second message. • Name of the malicious program. • Computer name. • Group. • Date and time (UTC). • Path of the malicious program. • Hash. • Table with contextual telemetry associated with the attacking process at the time it is detected.

Type	Frequency	Condition	Information shown
			• List of computers where the malware was previously seen.
Malware URL blocked	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when a URL that points to malware is detected.	• Number of malware URLs detected within the time range. • Number of affected computers.
Phishing detections	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when a phishing attack is detected.	• Number of phishing attacks detected within the time range. • Number of affected computers.
Intrusion attempts blocked	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when the IDS module blocks an intrusion attempt. • Windows computers only.	• Number of intrusion attempts blocked within the time range. • Number of affected computers.
Blocked devices	The solution sends a message every 15 minutes with a summary of all	• Sends an alert when a user tries to access a device or peripheral that the administrator blocked. • Compatible with Windows, Linux, macOS, and Android devices.	• Number of device access attempts blocked. • Number of

Type	Frequency	Condition	Information shown
	detected threats.		affected computers.
Computers with protection errors	The solution sends an alert every time an error is found.	• Sends an alert when the solution finds an unprotected computer on the network. • Sends an alert when the solution finds a computer with a protection or installation error.	• Computer name. • Group. • Description. • Operating system. • IP address. • Active Directory path. • Domain. • Date and time (UTC). • **Failure reason**: Protection with errors or installation error.
Computers without a license	The solution sends an alert every time an error is found.	Sends an alert when the solution fails to assign a license to a computer when there is no free license.	• Computer name. • Description. • Operating system • IP address • Group • Active Directory path • Domain. • Date and time (UTC).

Type	Frequency	Condition	Information shown
			• Failure reason: Computer without a license.
Install errors	The solution sends an alert every time an error is found.	• Sends an alert when an event occurs that causes computer status to change (1) from protected to unprotected. • If the solution detects several events at the same time that could cause a computer status to change from protected to unprotected, it only generates one alert with a summary of all the events	• Computer name. • Protection status. • Reason for the status change.
Unmanaged computers discovered	The solution sends an alert every time an error is found.	• Sends an alert when a discovery computer finishes a discovery task. • Sends an alert when 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 19.2: Alert table

Status change alerts (1)

These computer statuses trigger an alert:

- **Protection with errors**: The status of the antivirus protection installed on a computer shows an error.
- **Installation error**: An installation error occurs that requires user intervention, such as insufficient disk space. Transient errors that can be resolved autonomously after a number of retries do not generate alerts.

- **No license**: A computer does not receive a license after registration because there are no free licenses

These computer statuses do not trigger an alert:

- **No license**: The administrator manually removes a computer license, or Panda Endpoint Protection Plus automatically removes a computer license because the number of purchased licenses has been reduced.
- **Installing**: It does not make sense to generate an alert every time the protection is installed on a computer on the network.
- **Protection disabled**: This status is the consequence of a voluntary change of settings.
- **Protection out-of-date**: This status does not necessarily mean the computer is unprotected, despite its protection is out of date.
- **Pending restart:** This status does not necessarily mean the computer is unprotected.
- **Knowledge out-of-date**: This status does not necessarily mean the computer is unprotected.

Opting out of email alerts

If an email recipient wants to opt out of the notifications, but does not have access to the Panda Endpoint Protection Plus console or appropriate permissions, the recipient can unsubscribe from the email message. To opt out of email alerts:

- At the bottom of the email alert, click the link **If you don't want to receive any more messages of this kind, click here.** In the window that opens, type the email address that you do not want to receive email alerts. The link is valid for 15 days after the alert is sent.
- If the email address you enter currently receives email alerts, a confirmation email is sent to the address.
- In the confirmation email, click the opt-out link to confirm that you want no longer want to receive emails at the specified email address. The link is valid for 24 hours after the alert is sent.

Chapter 20

Scheduled sending of reports and lists

Panda Endpoint Protection Plus sends, by email, all the security information from the computers it protects. This makes it easy to share information across departments in a company and keep a history of all the events that occurred on the platform, beyond the capacity limits of the web console. This feature enables you to closely monitor the security status of the network without having to access the web console, thus saving management time.

With automated email reports, stakeholders can stay up to speed on all generated security events, thanks to a tamper-proof system that enables them to accurately assess the security status of the network.

Chapter contents

Report features

Report period

There are two types of reports based on the time period covered by the report:

- **Consolidated reports**: These include, in a single document, all the information generated over a given period of time.
- **Instant reports**: These reflect the security status of the network at a specific moment in time.

Method of sending

Panda Endpoint Protection Plus enables you to send reports automatically based on the settings established in the task scheduler or manually on demand.

The automated sending of reports provides recipients with network activity information without having to go to the web console.

Format

Depending on the type of report, Panda Endpoint Protection Plus can deliver reports in PDF and/or CSV format.

Content

The content of reports can be configured depending on the type of report: include data from any number of Panda Endpoint Protection Plus modules or set filters to restrict the information displayed to computers that meet certain criteria.

Report types

Panda Endpoint Protection Plus enables you to generate three types of reports, each with its own features:

- List views
- Executive reports
- Lists of devices

Next is a summary of the features of each type of report:

Type	Period	Sent	Contents	Format
List views	Instant	Automatically	Configurable using searches	CSV
Executive reports	Consolidated	Automatically and on demand	Configurable by categories and groups	PDF, CSV, Excel, Word
Lists of devices	Instant	Automatically	Configurable using filters	CSV

Table 20.1: Summary of report types and their features

Requirements for generating reports

> *Users with the read-only role can preview executive reports but cannot schedule the sending of new reports.*

Next is a description of the tasks you must perform in order to use the feature for sending scheduled reports.

List views

First, create a view and configure the search tools so the list shows the information you consider relevant. After that, you can create the scheduled report task. See Creating a custom list on page 46 for more information about how to create list views with associated searches.

Executive reports

No prior tasks are required: The content of the report is determined at the time of configuring the schedule report task.

List of filtered devices

You must first create a filter or use one of the filters created in Panda Endpoint Protection Plus. See Filter tree on page 202 for more information about how to configure and use filters.

Accessing the sending of reports and lists

From the Scheduled reports section

To access the list of tasks for sending reports and lists, click **Status** in the top menu, then **Scheduled reports** from the side menu. A page opens with the tools required to search for previously created send tasks, edit them, delete them, or create new ones.

From a list view

List views are stored in the left panel of the **Status** page. You can schedule the sending of each of them following the steps below.

- **From the context menu**: Click the context menu of the list view. Click the option **Schedule report** . A window opens with the information required, which is explained in section Report and list settings.
- **From the list view**: Click the icon in the upper-right corner of the page. A window opens with the information required, which is explained in section Report and list settings.

After the scheduled report task has been created, a pop-up message appears in the upper-right corner of the page confirming the creation of the task.

From a filter

- Click the **Computers** menu at the top of the console. Click the tab to show the filter tree.
- When clicking a filter, the list of devices is refreshed to show the devices whose characteristics meet the conditions of the selected filter.
- Click the context menu icon ⋮ corresponding to the filter and click **Schedule report**. A window opens with the information required, which is explained in section Report and list settings.

After the scheduled report task has been created, a pop-up message appears in the upper-right or bottom-right corner of the page confirming the creation of the task. This message also includes a link to the list of scheduled report tasks. See Report and list settings.

Managing reports

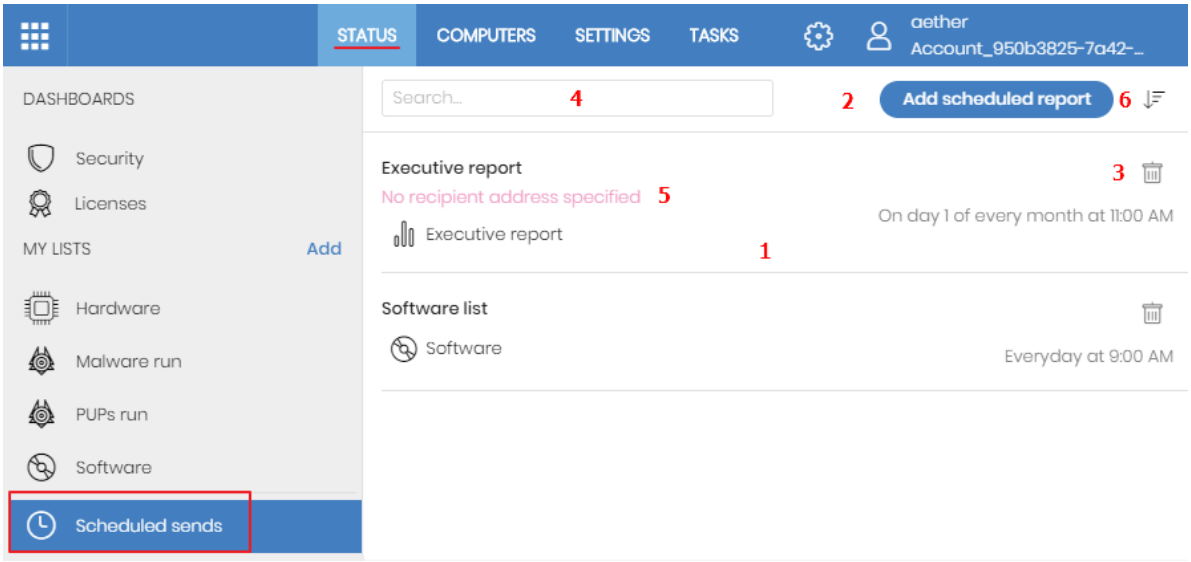


Figure 20.1: Page for managing scheduled sending of reports

To create, delete, edit, and list scheduled reports, click the **Status** menu at the top of the console. Then, click **Scheduled reports** from the side menu.

List of scheduled reports

The panel on the right shows the list of previously created scheduled report tasks.

All tasks include a name and below it a series of messages that indicate whether data is missing from the settings of the scheduled report task.

Creating scheduled reports

Click the **Add scheduled report** button **2** to show the settings window.

See Report and list settings for more information about the data administrators must provide to configure a scheduled report task.

Sorting scheduled reports

Click the  icon **(6)** to expand a context menu with the sort options:

- Sort by creation date
- Sort by name
- Ascending
- Descending

Deleting and editing scheduled reports

To delete or edit a scheduled report task, follow the steps below:

- To delete a scheduled report task, use the  icon **3**).
- To edit a scheduled report, click its name.

> *A list view or filtered list with a scheduled report task configured cannot be deleted until the corresponding task has been deleted.*
> *The lists sent by a scheduled report correspond to a specific list view or filtered list. If these are edited, the scheduled report will be updated accordingly.*

Report and list settings

Field	Description
Name	Name of the entry shown in the list of scheduled reports.
Send automatically	Frequency with which the report or list is sent: • **Every day**: It is sent every day at the scheduled time. • **Every week**: It is sent every week on the scheduled day and at the scheduled time • **Every month**: It is sent every month at the scheduled time on the scheduled date.
Report type	Type of report you want to send: • Executive report • List

Field	Description
	• Filter The report content varies depending on the type of report. For more information, see Contents of reports and lists.
Preview report	This option appears only when you select Executive Report. This link opens a new tab in your browser and enables you to see the contents of the report before you schedule it to be sent, download it, or print it. For lists and filters, the format is CSV and the preview option is not available.
Dates	Time period covered by the report. • Last month • Last 7 days • Last 24 hours In the case of lists and filters, the report is generated immediately. The information shown reflects the security status in the moment the report is generated. For more information, see Report features.
Computers	The computers from which data is extracted to generate the executive report: • **All computers**. • **Selected groups**: From the group tree, select individual groups using the checkboxes. This field appears only for executive reports.
To	Target email addresses separated by commas.
CC	Target email addresses (carbon copy recipients) separated by commas.
CCO	Target email addresses (blind copy recipients) separated by commas.
Subject	Summary description of the email message.
Format	• **For list views**: A CSV file is attached to the email message. • **For executive reports**: The report is attached to the email message in PDF, Excel, or Word format.

Field	Description
Language	Language of the report.
Content	Type of information included in the report: • **Table of contents**: List of the sections in the report. • **License status**: Information about the licenses contracted and used as well as their expiration dates. See Licenses on page 177. • **Security status**: The status of the Panda Endpoint Protection Plus software on the network computers on which it is installed. • **Detections**: The threats detected on the network. • **Risks:** The security risk levels assigned to computers on the network. See Risk assessment module panels/widgets on page 497 • **Web access**: User Internet activities. For more information, see Security module panels/widgets on page 445. • **Patch management**: The patch status of computers on your network. See Panda Patch Management widgets/panels on page 353. • **Vulnerability assessment status**: Shows computers on the network with known software vulnerabilities and reports on the availability of patches to mitigate vulnerability impact on computers. This appears only if the customer does not have Patch Management. For more information, see Vulnerability assessment module panels/widgets on page 508. • **Encryption**: The encryption status of the computers on the network. See Panda Full Encryption module panels/widgets on page 427. See Contents of reports and lists.

Table 20.2: Information to generate on-demand reports

Contents of reports and lists

Lists

The content of the lists sent is similar to the content generated by the **Export** or **Detailed export** button of a list view. If the list view supports detailed exports, when you configure the send task two options appear:

- **Summary report**: Corresponds to the **Export** option in the list.
- **Full report**: Corresponds to the **Detailed export** option in the list.

The lists that support detailed exports are:

- Software
- Patch installation history

For more information about the types of lists available in Panda Endpoint Protection Plus and their content, see Managing lists on page 41.

> *Lists include the computers visible to the user account that last edited the scheduled report. For this reason, a list edited by an account with less visibility than the account that initially created it contains information about a smaller number of computers than those shown when it was first created.*

Lists of devices

The content of the report sent corresponds to the basic exported list of devices filtered by certain criteria. For more information about the content of the CSV file sent, see Computers on page 216. For more information about how to manage and configure filters, see Filter tree on page 202.

Executive report

Depending on the settings defined in the **Contents** field, the executive report can include this data:

Overview

- **Created on**: Date when the report was created.
- **Period**: Time period covered by the report.
- **Included information**: Computers included in the report.

Table of contents

This section shows a list with links to the various sections of the executive report.

License status

- **Contracted licenses**: Number of licenses contracted by the customer.
- **Used licenses**: Number of licenses assigned to the network computers.
- **Expiration date**: Date when the license contract expires.

See Licenses on page 177.

Security status

Operation of the protection module on the network computers on which it is installed.

- **Protection status**: See Protection status on page 446.
- **Online computers**: See Offline computers on page 449.
- **Up-to-date protection**: See Outdated protection on page 450.
- **Up-to-date knowledge**: See Outdated protection on page 450.

Detections

The threats detected on the network.

- **Classification of all programs run and scanned**: See Security module panels/widgets on page 445.
- **Top 10 computers with most detections**: The top 10 computers with most detections by the antivirus module during the specified period:
    - **Computer**: Name of the computer.
    - **Group**: Group to which the computer belongs.
    - **Detections**: Number of detections during the specified period.
    - **First detection**: Date of first detection.
    - **Last detection**: Date of last detection.
- **Malware activity**: See Security module panels/widgets on page 445.
- **PUP activity**: See Security module panels/widgets on page 445.
- **Exploit activity**: See Security module panels/widgets on page 445.
- **Network attack activity**: See Security module panels/widgets on page 445.
- **Latest malware detections**: See Malware and PUP detection.
- **Latest PUP detections**: See Malware and PUP detection.
- **Latest exploit detections**: See Exploit detection.
- **Latest network attack detections**: See Security module lists on page 458.
- **Threats detected by the antivirus**: See Threats detected by the antivirus on page 451.

Risks

Overall status of the security risks assigned to computers. See Risk assessment module panels/widgets on page 497.

- **Company risk**: Number of computers on the network with an assigned risk level.
- **Risks trend**: Number and types of risks that are detected over time.
- **Detected risks**: The most commonly found risks and the number of computers where the risk was found.
- **Top 10 computers at risk**: Computers with the highest risk level.

Web access

Web activity of network users.

- **Web access**: See Web access on page 454.
- **Top 10 most accessed categories**: See Top 10 most accessed categories on page 454.
- **Top 10 most accessed categories by computer**: See Top 10 most accessed categories by computer on page 455.
- **Top 10 most blocked categories**: See Top 10 most blocked categories on page 456.
- **Top 10 most blocked categories by computer**: See Top 10 most blocked categories by computer on page 457.

Patch management

Patch status of computers on your network.

- **Patch management status**: See Patch management status on page 353.
- **Top 10 computers with most available patches**: List of the ten computers that are missing most patches, grouped by type: security patches, non-security patches, and Service Packs. See Computers with most available patches on page 366.
- **Top 10 most critical patches**: List of the ten most critical patches sorted by the number of computers affected.
- **Available patches trend**: Shows the trend of the number of patches that are pending installation on the computers on the network, grouped by severity. See Available patches trend on page 358.

Vulnerability assessment

- **Vulnerability assessment status**: Shows the status of the vulnerability assessment module on computers on your network: computers where vulnerability assessment did not install correctly, computers with no vulnerability assessment license, and other issues. See Vulnerability assessment status on page 509.

  Time since last check: Shows the number of computers that have not connected to the Panda Security cloud and reported patch status for more than 3, 7, and 30 days. See Time since last check on page 511.
- **Top 10 most critical patches**: List of the ten most critical patches sorted by the number of computers affected.
- **Top 10 programs with most available patches**: List of the ten programs with most missing patches available for installation.
- **Available patches trend**: Shows the trend of the number of patches that are pending installation on the computers on the network, grouped by severity. See Available patches trend on page 515.

Encryption

Encryption status of computers. It includes these widgets and lists:

- **Encryption status**: See Encryption status on page 427.
- **Computers supporting encryption**: See Computers supporting encryption on page 429.
- **Encrypted computers**: See Encrypted computers on page 431.
- **Authentication method applied**: See Authentication method applied on page 433.
- **Last encrypted computers**: Lists the ten computers that have been encrypted most recently by Panda Full Encryption, sorted by encryption date. Each line in the list contains the computer name, group, operating system, authentication method, and encryption date.

Chapter 21

Remediation tools

Panda Endpoint Protection Plus provides several remediation tools that help you resolve the issues found in the Protection, Detection, and Monitoring phases of the adaptive protection cycle. Some of these tools are automatic and do not require you to take any action. You can get access to other tools in the web console.

Chapter contents

Table Table 21.1: shows the tools available for each supported platform and their features.

Remediation tool	Platform	Type	Purpose
Automatic computer scanning and disinfection	Windows, macOS, Linux, Android	Automatic	Detects and disinfects malware when the solution detects 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, at specific time intervals, or after you create a remediation task.
On-demand restart	Windows	Manual	Forces a computer restart to apply updates, finish manual

Remediation tool	Platform	Type	Purpose
			disinfection tasks, and fix protection errors.
Ransomware removal and system restore	Windows, macOS, and Linux	Manual	Enables you to detect ransomware attacks and remove threats. On Windows systems, you can recover a clean copy of the encrypted files.

Table 21.1: Panda Endpoint Protection Plus remediation tools

Automatic computer scanning and disinfection

The Panda Endpoint Protection Plus protection module automatically detects and disinfects threats in these security areas:

*Automatic disinfection does not require administrator intervention. However, **File protection** must be enabled in the security settings assigned to the computers and devices. See Security settings for workstations and servers on page 299 for more information about the options available for the Panda Endpoint Protection Plus antivirus module.*

- **Web**: Malware downloaded to targeted computers through a web browser.
- **Email**: Malware that reaches email clients as a message attachment.
- **File system**: Malware detected when a file that contains a known or unknown threat in the computer storage system is run, moved, or copied.
- **Network**: Intrusion attempts from a host on the network or Internet, blocked by the firewall.

When Panda Endpoint Protection Plus detects a known threat, it automatically cleans the affected items when there is a disinfection method available. If not, the solution quarantines the items.

On-demand computer scanning and disinfection

To scan and disinfect user computers on demand, Panda Endpoint Protection Plus uses the task infrastructure.

Required permissions

The user account used to access the web console must have the **Launch scans and disinfect** permission assigned to its role. For more information about the permissions system, see Managing roles and permissions on page 65.

Types of on-demand scans

Immediate (Scan now option)

A task that starts immediately and which scans and disinfects the local file system (it does not scan network drives).

Panda Endpoint Protection Plus creates a task with these characteristics:

- **Maximum run time**: Unlimited.
- **Task start**:
    - If the target computer is turned on, the task starts as soon as it is launched.
    - If the target computer is turned off, the task is postponed until the computer becomes available within the next 7 days.
- The computer areas that are scanned are as follows:
    - **The entire computer:**
        - Memory.
        - Boot system.
        - Cookies.
        - Internal storage devices. Complete file system, all extensions.
        - Storage devices physically connected to the target computer (USB drives and others). Complete file system, all extensions.
    - **Critical areas**:
        - Memory.
        - Boot system.
        - Cookies.
        - %windir%\system32, %windir%\SysWow64. All extensions.
- The default action that is taken is:
    - **When detecting a disinfectable file**: The file is replaced with a clean version.
    - **When detecting a non-disinfectable file**: The file is deleted and a backup copy is moved to quarantine.

Scheduled (Scheduled scan option)

Create a task without settings. For more information about how to configure a scan task, see Configuring a scan task.

Accessing on-demand scan and disinfection tasks

From the computer tree

- Select **Computers** in the top menu. Select the **My organization** tab of the computer tree in the left panel.
- To launch an immediate scan on a group of computers, select the context menu of the group. Select **Scan now**  . The **Select the type of scan** window opens.
- Select the scan type: **The entire computer** or **Critical areas (Recommended)**. Click **OK**. The **New scan task created** message appears and the task is added to the list in the **Tasks** section.
- To schedule a scan on a group of computers, click the context menu of the group. Select **Schedule scan**  . A new scan task is created. For information about how to configure it, see Configuring a scan task.

From the computer tree list

- Select **Computers** in the top menu. Select the **My organization** tab of the computer tree in the left panel.
- Select the group of computers. Select the checkboxes of the computers you want to scan.
- To launch an immediate scan task, if you have selected a single computer, select the computer context menu. Select **Scan now.** If you have selected more than one, select **Scan now**  in the toolbar above. The **Select the type of scan** window opens.
- Select the scan type: **The entire computer** or **Critical areas (Recommended)**. Click **OK**. The **New scan task created** message appears and the task is added to the list in the **Tasks** section.
- To schedule a scan task, if you have selected a single computer, select the computer context menu. Select **Schedule scan**  . If you have selected more than one, select **Schedule scan**  in the toolbar above. A new scan task is created. For information about how to configure it, see Configuring a scan task.

Configuring a scan task

- Enter general details about the task in the **Name** and **Description** fields.
- If no recipients are defined, click the **No recipients selected** link in the **Recipients** section. A page opens where you can select the computers that will receive the configured task.

> *To access the computer selection page, you must first save the task. If you have not saved the task, a warning message is shown.*

- Select the types of computers that will receive the task: **Workstation**, **Laptop**, or **Server**.
- Click ⊕ to add individual computers or computer groups. Click 🗑 to remove them.
- Click the **View computers** button to view the computers that will receive the task.
- Schedule the task. You can configure these three parameters:

- **Starts:** Indicate the task start date/time.

Value	Description
As soon as possible (selected)	The task is 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 is launched on the date selected in the calendar. Specify whether the time on the computer or the Panda Endpoint Protection Plus server time should be considered.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task will not run. The task scheduler enables you to establish the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** Define a 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 solution waits indefinitely for the computer to be available to launch the task.

Table 21.2: Task launch parameters

- **Maximum run time**: Indicates the maximum time that the task can take to complete. After that time, the task is canceled returning an error.

- **Scan options:**

Value	Description

Scan type	• **The entire computer**: Runs an in-depth scan of the computer that includes all connected storage devices.
	• **Critical areas**: Runs a quick scan of these areas:
	  • `%WinDir%\system32`
	  • `%WinDir%\SysWow64`

Value	Description
	• Memory • Boot system • Cookies • **Specific items**: Specify the paths you want to scan on the mass storage devices. This option supports environment variables. The solution scans the specified path and every folder and file it contains.
Detect viruses	Detects programs that enter computers with malicious purposes. This option is always enabled.
Detect hacking tools and PUPs	Enable this toggle to detect potentially unwanted programs, as well as programs that hackers can use to carry out actions that cause problems for the user of the affected computer.
Detect suspicious files	Scheduled scans can scan computer software statically without the need to run the software. This reduces the likelihood that the scan detects some types of threats. Enable this toggle to use heuristic scan algorithms and improve detection rates. Only programs detected by the heuristic protection are considered suspicious programs.
Scan compressed files	Enable this toggle to decompress compressed files and scan their contents.
Exclude the following files from scans	• **Do not scan files excluded from the permanent protections**: Select this checkbox to not scan files that the administrator allowed to execute, as well as any file that is globally excluded in the console. • **Extensions**: Specify the extensions of the files you do not want to scan. Enter multiple file extensions separated by commas. • **Files**: Specify the names of the files you do not want to scan. Enter multiple file names separated by commas. • **Directories**: Specify the names of the folders you do not want to scan. Enter multiple folders separated by commas.

Table 21.3: Scan options

Lists generated by scan tasks

Scan tasks generate lists with results.

Accessing the lists

Follow these steps to access these lists:

- Go to the **Tasks** menu at the top of the console. Click **View results** in the scan task whose results you want to view. The **Task results** list opens.
- From the **Task results** list, click **View detections** to access the list of detected items.

Required permissions

Permissions	Access to lists
No permissions	**Scan task results** list.
View detections and threats	Access to the **View detections** list of a task.

Table 21.4: Permissions required to access scan task lists

Scan task results list

This list shows the malware items detected on the computers on your network:

Field	Description	Value
Computer	Name of the computer where the task ran.	Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Detections	Number of detections made on the computer.	Character string
Status	Status of the task.	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled

Field	Description	Value
		• Canceling • Canceled (maximum run time exceeded)
Start date	Task start date.	Date
End date	Task end date.	Date

Table 21.5: Fields in the Scan task results list

Filter tools

Field	Comment	Value
Status	Status of the task.	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Detections	Computers where detections were or were not made.	• All • With detections • No detections

Table 21.6: Filters available in the Scan task results list

View detections list

This list shows detailed information about each malware detection made by the scan task.

Field	Description	Value
Computer	Computer name.	Character string
Group	Folder in the Panda Endpoint Protection Plus folder tree that the computer belongs to.	Character string
Threat type	Malware category based on the actions the threat is designed to perform.	• Virus and ransomware • Spyware • Tracking cookies • Hacking tools and PUPs • Phishing • Dangerous actions blocked • Malware URLs • Other
Path	Threat location on the computer.	Character string
Action	Action taken on the computer.	• Quarantined • Deleted • Disinfected • Blocked • Process ended
Date	Date the action was taken.	Date

Table 21.7: Fields in the View detections list

Threat details page

Click any of the rows in the list to view the threat details page. See Computer details on page 236for more information.

Computer restart

If you need to restart a Windows computer to finish an update or to fix a protection problem, you can force the computer to restart:

- Go to the **Computers** menu at the top of the console. From the right panel, find the computer you want to restart:
  - **To restart a single computer**: Click the computer's context menu icon. Select **Restart** from the menu displayed.
  - **To restart multiple computers**: Use the checkboxes to select the computers you want to restart. Click the  icon on the action bar.

If the target computer is not available (offline), the restart command remains active for 7 days.

Reporting a problem

As with any technology, the Panda Endpoint Protection Plus software installed on your network computers might occasionally function incorrectly. Some symptoms could include:

- Errors reporting a computer status.
- Errors downloading knowledge or engine updates.
- Protection engine errors.

If Panda Endpoint Protection Plus functions incorrectly on a computer on the network, you can contact the Panda Security support department through the console and automatically send all the information required for diagnosis. From the top menu, select **Computers**. Click the context menu for the computer with errors. From the menu that opens, select **Report a problem**.

If Panda Endpoint Protection Plus functions incorrectly on a computer on the network, you can contact the Panda Security support department through the console and automatically send all the information required for diagnosis. From the top menu, select **Computers**. Click the context menu for the computer with errors. From the menu that opens, select **Report a problem**.

Allowing external access to the web console

If you find problems you cannot resolve, you can grant the Panda Security support team access to your console. Follow these steps:

- From the top menu, select **Settings**. From the side menu, select **Users.**.
- On the **Users** tab, enable **Allow the Panda Security S.L.U. team to access my console**.

Removing ransomware and restoring the system to a previous state

Ransomware threats encrypt the content of the files found on workstations and servers, demanding a ransom from the targeted company to get the recovery key that allows access to the encrypted information upon payment. These threats are extremely dangerous because of the impact they can have on business operations. Panda Endpoint Protection Plus implements multiple features to help organizations in both the attack detection and attack remediation phases.

Follow these steps if you detect a ransomware attack on your network:

Because the Shadow Copies feature makes a daily backup of computer files and keeps a maximum of seven copies, it is important that you recover a clean copy of the encrypted files within seven days after the attack takes place. Otherwise, all saved copies will be of encrypted files.

- Disconnect affected computers from the network to prevent the threat from spreading.
- Verify that the protection software is working on all computers:
    - To see the protection status of your computers, see the Protection status on page 446 widget.
    - Reinstall the security software on computers where the protection status is **Error**.
    - Find computers without security software installed. For more information about how to configure this feature, see Viewing discovered computers on page 114.
- Enable and configure the File antivirus, Mail antivirus, and Web browsing antivirus to detect all types of threats. For more information about how to configure this feature, see Antivirus on page 304.
- Configure anti-tamper protection. Set a password to prevent unauthorized uninstallation of the protection software. For more information about how to configure this feature, see Configuring security against protection tampering on page 292.
- Verify that the maximum space for Shadow Copies is between 10% and 20% to prevent copies from being deleted because of lack of space. For more information about how to configure this feature, see Configuring shadow copies on page 296.
- To remove ransomware, follow these steps:

    - Install at least the patches that fix the critical vulnerabilities detected. See Panda Patch Management (Updating vulnerable programs) on page 331.
    - Run an on-demand scan. See On-demand computer scanning and disinfection.
    - Restart affected computers to close any remote connection in progress. For more information about how to configure this feature, see Computer restart.
    - If, after the affected computers are restarted, the ransomware is still active, contact Panda Security tech support.
- Restore encrypted files on each computer using Shadow Copies or the data recovery procedure in place in your company.
- Restore the security settings changed at the beginning of this procedure to their usual values.

Chapter 22

Tasks

A task is a resource implemented in Panda Endpoint Protection Plus that enables you to associate a process with two variables: repetition interval and execution time.

- **Repetition interval**: You can configure tasks to be performed only once, or repeatedly through specified time intervals.
- **Execution time**: You can configure tasks to be run immediately after being set (immediate task), or at a later time (scheduled task).

Chapter contents

Introduction to the task system

Accessing the task system

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

- Top menu **Tasks**.
- Computer tree (accessible from the top menu **Computers**).
- Lists associated with the different supported modules.

The computer tree and the lists enable you to schedule and launch tasks quickly and easily, without having to go through the entire configuration and publishing process described in section Steps to launch a task. However, they provide less configuration flexibility.

Steps to launch a task

The primary resource for creating a task is the **Tasks** area accessible from the menu at the top of the console. This area enables you to create tasks from scratch, configuring every aspect of the process.

The process of launching a task consists of three steps:

- **Task creation and configuration**: Select the affected computers, the characteristics of the task, the date/time the task will be launched, the task frequency, and the way it will behave in the event of an error. Task settings depend on the type of task. For more information about how to create and configure a task, see Task types
- **Task publication**: The tasks you create must be entered in the Panda Endpoint Protection Plus task scheduler to be run on the scheduled day/time.
- **Task execution**: The task is run when the configured conditions are met.

Task types

Panda Endpoint Protection Plus enables you to launch the following tasks:

- Scan and disinfect files. See On-demand computer scanning and disinfection on page 568 for more information.
- Install patches and updates for the operating system and other programs installed on user computers. For more information, see Download and install patches on page 337.

Permissions associated with task management

For more information about the permission system implemented in Panda Endpoint Protection Plus, see Understanding permissions on page 67.

To create, edit, delete, or view tasks, you must use a user account that has the appropriate permission assigned to its role. Depending on the task, the required permissions are:

- **Launch scans and disinfect**: To create, delete, and edit **Scheduled scans** tasks.
- **Install, uninstall, and exclude patches**: To create, delete, and edit **Install patches** tasks.
- **View detections**: To view the results of **Scheduled scans** tasks.

Creating a task from the Tasks area

- From the top menu, select **Tasks**. A list opens and shows all created tasks and their status.
- Click the **Add task** button. From the drop-down menu, select a task type. A page opens for you to enter the task details. This page is divided into multiple areas:
  - **Overview (1)**: Task name and description.
  - **Recipients (2)**: Computers that receive the task.
  - **Schedule (3)**: Task schedule (day and time the task runs).
  - **Settings (4)**: Specify the actions the task must take. This section varies based on the task type and is described in the documentation associated with the related module.

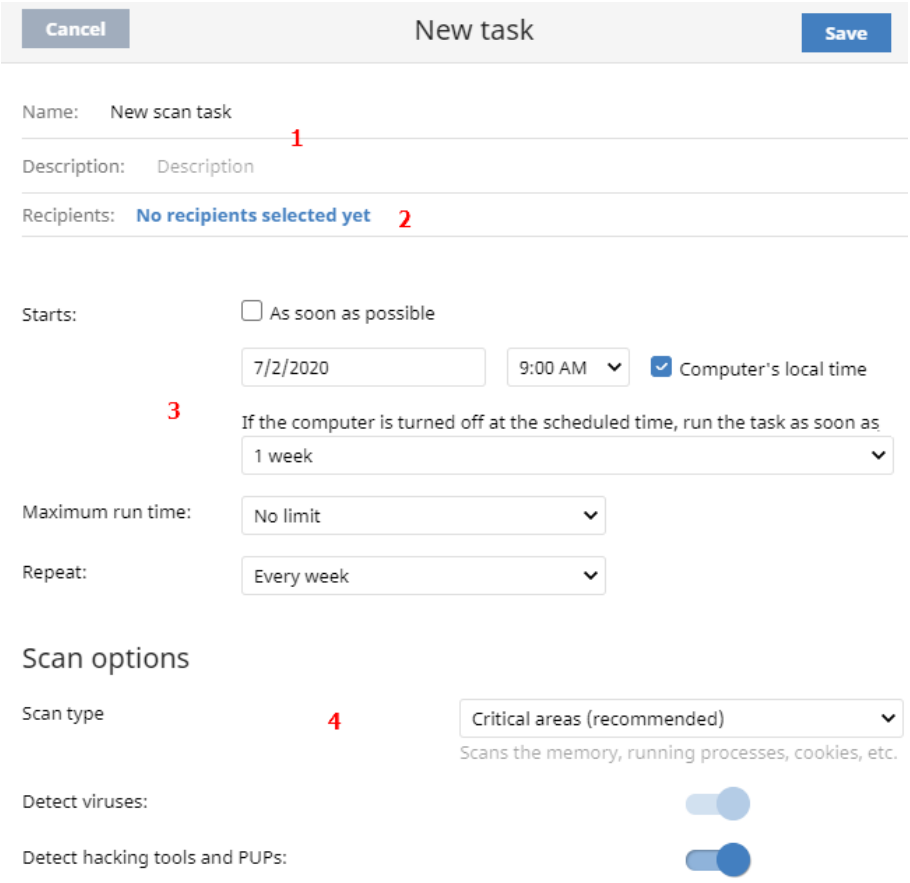


Figure 22.1: Overview of the New Task page for a scan task

Task recipients (2)

To access the computer selection page, you must first save the task. If you have not saved the task, a warning message is shown.

- In the **Recipients** section, click the **No recipients selected yet** link. A page opens where you can select the computers that you want to receive the configured task.
- Select the types of computers that will receive the task: **Workstation**, **Laptop**, **Server**, or **Mobile device**. The type of computer that can receive a task depends on the task to run.
- Click the ⊕ button to add individual computers or computer groups. Click the 🗑 button to remove them.

> *If you are configuring a patch installation task and want to send it to test computers only, enable the **Run the task only on test computers**toggle. This option is applicable only to service providers who have Panda Partner Center. For more information, see* *Panda Patch Management features on page 332*

- On the **Edit task** page, click the **View computers** button to view the computers that will receive the task.

Task schedule and frequency

You can configure these parameters:

- **Starts**: Indicates the task start date/time.

Value	Description
As soon as possible (selected)	The task runs 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 in the **If the computer is turned off** section
As soon as possible (cleared)	The task runs on the date selected in the calendar. Specify whether the time is based on the computer local time or the Panda Endpoint Protection Plus server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task does not run. The task scheduler enables you to establish the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** Define a time interval during which the task will run if the computer becomes available. • **Run when the computer is turned on:** There is no time limit. The system waits

Value	Description
	indefinitely for the computer to be available to run the task.

Table 22.1: Task execution parameters

- **Maximum run time**: Indicates the maximum time that the task can take to complete. After that time, the task is canceled returning an error.

Value	Description
No limit	There is no time limit for the task to complete.
1, 2, 8, or 24 hours	There is a time limit for the task to complete. After that time, if the task has not finished, it is canceled returning an error.

Table 22.2: Task duration parameters

- **Frequency**: Set a repeat interval (every day, week, month, or year) from the date specified in the **Starts:** field.

Value	Description
One time	The task runs only once at the time specified in the **Starts:** field.
Daily	The task runs every day at the time specified in the **Starts:** field.
Weekly	Use the checkboxes to select the days of the week on which the task must run, at the time specified in the **Starts:** field.
Monthly	Choose an option: • Run the task on a specific day of every month. If you select the 29th, 30th, or 31st of the month, and the month does not have that day, the task runs on the last day of the month. • Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 22.3: Task frequency parameters

Lower versions of the security software

If the recipient computers have a lower version of the security software installed, they might not correctly interpret frequency settings. Computers with lower versions of the security software interpret the task frequency settings as follows:

- **Daily tasks**: Unchanged.
- **Weekly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 7 days.
- **Monthly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 30 days.

Task publication

After you create and configure a task, it appears in the list of configured tasks. The status shows as **Unpublished** and it is not yet active.

To publish a task, click the **Publish** button. The task is added to the Panda Endpoint Protection Plus task scheduler, which runs it based on its settings.

Task list

Click **Tasks** in the top menu to view a list of all created tasks, their type, status, and other relevant information.

Field	Comment	Values
Icon	The task type.	• Patch installation or uninstallation task • On-demand scan task • Disinfection task
Name	The task name.	Character string
Schedule	Date the task is set to run.	Character string
Status	• **No recipients**: The task will not run because there are no	Character string

Field	Comment	Values
	recipients assigned to it. Assign one or more computers to the task. • **Unpublished**: The task will not run because it has not been added to the scheduler queue. Publish the task so it can be launched by the scheduler based on its settings. • **In progress**: The task is running. • **Canceled**: The task was manually canceled. This does not mean that all processes that were running on the target computers have stopped. • **Finished**: The task finished running on all affected computers, regardless of whether it failed or was performed successfully. This status only applies to one-time tasks.	

Table 22.4: Fields in the Tasks list

Filter tool

Field	Comment	Values
Type	The task type.	• Scan • Disinfection • Patch installation • Patch uninstallation • All
Search task	Enter the task name.	Character string
Schedule	The task repeat frequency.	• Scan • Immediate • Once • Scheduled
Status	Task status	• Scan • No recipients • Unpublished

Field	Comment	Values
		• In progress • Canceled • Finished
Sort list	Task list sort order.	• Sort by creation date • Sort by name • Ascending • Descending

Table 22.5: Filters available in the Tasks list

Task management

From the top menu, select **Tasks** to delete, copy, cancel, or view the results of created tasks.

Selecting the tasks to manage

- To manage a single task, select the checkbox next to the task name.
- To manage all tasks on the page, select the checkbox next to the search bar in the upper-left corner of the page. To select all tasks in the entire list, click the **Select all x rows in the list** link.

Modifying a published task

Click a task name to view its settings page. There you can modify some of the task parameters.

> *For published tasks, you can change the name and description only. To modify other fields in a published task, you must create a copy of the task.*

Canceling a published task

Select the checkboxes next to the tasks you want to cancel. In the toolbar, click the **Cancel** icon. This cancels the tasks, but does not delete them from the task window, which enables you to view the results. You can cancel only tasks whose status is **In progress**.

Deleting a task

Executed tasks are not automatically deleted. To delete a task, select it using the checkboxes and click the icon. You must cancel a task before you can delete it.

When you delete a task, you also delete the task results.

Copying a task

When you copy a task, you can copy all of its settings. If the task includes recipients, you can choose whether to copy them.

- From the top menu, select **Tasks**. Click the icon for the task you want to copy. From the drop-down menu, select the copy type.

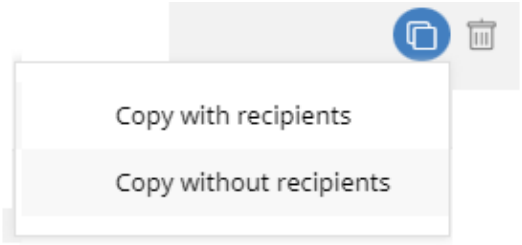


Figure 22.2: Copy task icon menu

- If you select **Copy without recipients**, the **Copy task** page opens.
  - To assign recipients, click the **No recipients selected yet** link. The **Recipients** page opens.
  - Select the task recipients. Click **Save** in the upper-right corner of the page.

*With patch installation tasks, if you want to send the task to test computers only, enable the **Run the task only on test computers** toggle. This option is applicable only to service providers who have Panda Partner Center. For more information, see Panda Patch Management features on page 332.*

If you select **Copy with recipients**, the **Copy task** page opens and shows the recipients configured in the original task.

Exporting tasks

Click the icon to export the list of tasks. A .CSV file is saved to the folder of your choice.

The downloaded file contains these columns:

Field	Definition
Task name	Task name

Field	Definition
Task type	The type of task: • IOC search • Patch uninstallation • Patch installation • Scan
Schedule	The pattern of recurrence for the task: • Inmediate • Once • Scheduled
Status	The status of the task: • No recipients • Unpublished • In progress • Canceled • Finished
Recipient group	The group that receives the task.
Workstation	• **Yes**: The task is assigned to computers of the Workstation type in the recipient group. • **No**: The task is not assigned to computers of the Workstation type in the recipient group.
Laptop	• **Yes**: The task is assigned to computers of the Laptop type in the recipient group. • **No**: The task is not assigned to computers of the Laptop type in the recipient group.
Server	• **Yes**: The task is assigned to computers of the Server type in the recipient group. • **No**: The task is not assigned to computers of the Server type in the recipient group.

Field	Definition
Mobile device	• **Yes**: The task is assigned to mobile devices in the recipient group. • **No**: The task is not assigned to mobile devices in the recipient group.
Recipient computer	The computer that receives the task.
Recipient computer group	Type of computer that receives the task: • Workstation • Laptop • Server • Mobile device

Table 22.6: Tasks exported list

Task results

Click the **View results** link of a published task to view its results up to that point and access a filter tool for finding specific computers among those that received the task.

Some of the fields in the results list are specific to certain tasks. Those fields are described in the documentation associated with the relevant module. Next is a description of the fields common to all results lists.

Field	Description	Values
Computer	Name of the computer where the task was run.	Character string
Group	Folder within the Panda Endpoint Protection Plus folder tree the computer belongs to.	Character string
Status	Status of the task process on the affected computer: • **Pending**: The task's next recurrence has not started because it is scheduled to run at a later time.. • **In progress**: The task is running on the computer.	Character string

Field	Description	Values
	• **Finished**: The task finished successfully. • **Failed**: The task failed and returned an error. • **Canceled (the task could not start at the scheduled time)**: The task could not start at the scheduled time because the target computer was turned off or in a state that prevented the task from running. • **Canceled**: The process was canceled on the computer. • **Canceling**: The task was canceled, but the target computer has not finished canceling the task process. • **Canceled (maximum run time exceeded)**: The task was automatically canceled because it exceeded its configured maximum run time.	
Start date	The task start date.	Date
End date	The task end date.	Date

Table 22.7: Common fields in task results lists

Task filter tool

Field	Description	Values
Date	Drop-down menu with the date the task became active based on the configured schedule. An active task can be launched immediately or wait until the target computer is available. This date is shown in the Date column.	Date
Status	• **Pending**: The task has not been launched as the execution window has not started yet. • **In progress**: The task is currently running. • **Finished**: The task finished successfully. • **Failed**: The task failed and returned an error. • **Canceled (the task could not start at the scheduled time)**: The target computer was not accessible at the time the task was set to start or during the selected time period. • **Canceled**: The task was manually canceled.	Enumeration

Field	Description	Values
	• **Canceled (maximum run time exceeded)**: The task was automatically canceled because it exceeded its configured maximum run time.	

Table 22.8: Search filters in task results

Automatic adjustment of task recipients

If the administrator selects a computer group as the recipient of a task, the computers that finally run the task may vary from those initially selected. This is because groups are dynamic entities that change over time.

That is, you can define a task at a specific time (T1) to be run on a specific group containing a series of computers. However, at the time the task is run (T2), the computers in that group may have changed.

When it comes to determining which computers will receive a configured task, there are three cases depending on the task:

- Immediate tasks.
- One-time scheduled tasks.
- Recurring scheduled tasks.

Immediate tasks

These tasks are created, published, and launched almost simultaneously and only once. The target group is evaluated at the time the administrator creates the task. The task status for the affected computers is **Pending**.

Adding computers to the target group

You cannot add new computers to the target group. Even if you add new computers to the target group, they will not receive the task.

Removing computers from the target group

You can remove computers from the target group. Move a computer to another group to cancel the task on that computer.

One-time scheduled tasks

There are two possible scenarios for changing the computers included in the target group:

Tasks which started running less than 24 hours ago

Within the first 24 hours after a task stars running, it is still possible to add or remove computers from its target groups. This 24-hour period is established to cover all time zones for multinational companies with a presence in several countries.

Tasks which started running more than 24 hours ago

24 hours after a task starts running, it is not possible to add new computers to it. Even if you add new computers to the target group, they will not receive the task. To cancel the task on a computer, move it outside the target group.

Recurring scheduled tasks

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

Unlike immediate tasks, the status of the task on each computer is not automatically set to **Pending**. The status of the task on each computer is shown gradually in the console as the Aether platform receives the relevant information from each computer.

Chapter 23

Product features and requirements

Chapter contents

Supported features by platform

General

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Web-based console	X	X	X	X	X
Information in dashboards	X	X	X	X	X
Filter-based computer organization	X	X	X	X	X
Group-based computer organization	X	X	X	X	X
Languages	11	11	11	16	10

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
supported in the security software					

Table 23.1: General features

Lists and reports

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Frequency that malware and PUPs activity are sent to the server	1 min	10 min	10 min	Immediately after scan completes	N/A
Frequency that other detections are sent to the server	15 min	15 min	15 min	Immediately after scan completes	15 min
List of detections	X	X	X	X	X
Executive reports	X	X	X	X	X
Scheduled executive reports	X	X	X	X	X

Table 23.2: List and report features

Protection

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Anti-phishing	X		X		X
Real-time permanent antivirus	X	X	X	X	

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
protection					
Contextual detections	X	X			
Risk evaluation	X	X	X	X	X
Shadow copies	X				
Decoy files	X				
Firewall	X				
Web access control	X		X		X
Device control	X				
Anti-theft				X	X

Table 23.3: Protection features

Hardware and software information

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Hardware information and list	X	X	X	X	X
Software information and list	X	X	X	X	X
Software change log	X	X	X	X	X
Information about installed OS patches	X				

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Vulnerability assessment	X	X	X		

Table 23.4: Hardware and software information features

Settings

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Security settings for workstations and servers	X	X	X	N/A	N/A
Anti-tamper protection	X	X			
Two-factor authentication	X	X			
Password to uninstall the protection and take actions locally	X	X			
Secure VPN connections	X		X	X	
Secure access to Wi-Fi network	X		X	X	
Ability to establish multiple proxies	X	X	X	N/A	N/A
Ability to work as a Panda proxy	X			N/A	N/A
Ability to access the	X	X	X	N/A	N/A

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Internet through a proxy					
Ability to work as a repository or cache	X			N/A	N/A
Ability to use the repository or cache	X			N/A	N/A
Discovery of unprotected computers	X				
Email alerts in the event of an infection	X	X	X	X	N/A
Email alerts when finding an unprotected computer	X	X	X	X	N/A

Table 23.5: Configuration features

Remote actions from the web console

Available fea-tures	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Real-time actions	X	X	X	X	X
On-demand scans	X	X	X	X	N/A
Scheduled scans	X	X	X	X	N/A
Remote installation of the Panda agent	X				
Remote	X	X	X		

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
uninstallation of the Panda agent					
Ability to reinstall the agent and protection	X				
Computer restart	X	X	X		
Ability to report incidents (PSInfo)	X			X	X
Ability to report problems	X	X	X	X	X

Table 23.6: Available remote actions

Security software updates and upgrades

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Signature updates	X	X	X	X	N/A
Protection upgrades	X	X	X	X	N/A
Ability to schedule protection upgrades	X	X	X	Google Play	App Store

Table 23.7: Security software update and upgrade features

Available modules

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	X	X	X		
Patch Management	X	X	X		
Panda Full Encryption	X	X	X		

Table 23.8: Available modules

(*) The feature works on Windows (Intel) and partially on Windows (ARM).

Product features and requirements

Chapter contents

Supported features by platform

General

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Web-based console	X	X	X	X	X
Information in dashboards	X	X	X	X	X
Filter-based computer organization	X	X	X	X	X
Group-based computer organization	X	X	X	X	X

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Languages supported in the security software	11	11	11	16	10

Table 23.9: General features

Lists and reports

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Frequency that malware and PUPs activity are sent to the server	1 min	10 min	10 min	Immediately after scan completes	N/A
Frequency that other detections are sent to the server	15 min	15 min	15 min	Immediately after scan completes	15 min
List of detections	X	X	X	X	X
Executive reports	X	X	X	X	X
Scheduled executive reports	X	X	X	X	X

Table 23.10: List and report features

Protection

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Anti-phishing	X		X		X
Real-time	X	X	X	X	

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
permanent antivirus protection					
Contextual detections	X	X			
Risk evaluation	X	X	X	X	X
Shadow copies	X				
Decoy files	X				
Firewall	X				
Web access control	X		X		X
Device control	X				
Anti-theft				X	X

Table 23.11: Protection features

Hardware and software information

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Hardware information and list	X	X	X	X	X
Software information and list	X	X	X	X	X
Software change log	X	X	X	X	X
Information about installed OS	X				

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
patches					
Vulnerability assessment	X	X	X		

Table 23.12: Hardware and software information features

Settings

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Security settings for workstations and servers	X	X	X	N/A	N/A
Anti-tamper protection	X	X			
Two-factor authentication	X	X			
Password to uninstall the protection and take actions locally	X	X			
Secure VPN connections	X		X	X	
Secure access to Wi-Fi network	X		X	X	
Ability to establish multiple proxies	X	X	X	N/A	N/A
Ability to work as a Panda proxy	X			N/A	N/A

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Ability to access the Internet through a proxy	X	X	X	N/A	N/A
Ability to work as a repository or cache	X			N/A	N/A
Ability to use the repository or cache	X			N/A	N/A
Discovery of unprotected computers	X				
Email alerts in the event of an infection	X	X	X	X	N/A
Email alerts when finding an unprotected computer	X	X	X	X	N/A

Table 23.13: Configuration features

Remote actions from the web console

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Real-time actions	X	X	X	X	X
On-demand scans	X	X	X	X	N/A
Scheduled scans	X	X	X	X	N/A
Remote installation of the Panda agent	X				

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Remote uninstallation of the Panda agent	X	X	X		
Ability to reinstall the agent and protection	X				
Computer restart	X	X	X		
Ability to report incidents (PSInfo)	X			X	X
Ability to report problems	X	X	X	X	X

Table 23.14: Available remote actions

Security software updates and upgrades

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Signature updates	X	X	X	X	N/A
Protection upgrades	X	X	X	X	N/A
Ability to schedule protection upgrades	X	X	X	Google Play	App Store

Table 23.15: Security software update and upgrade features

Available modules

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	X	X	X		
Patch Management	X	X	X		
Panda Full Encryption	X	X	X		

Table 23.16: Available modules

(*) The feature works on Windows (Intel) and partially on Windows (ARM).

Requirements for Windows platforms

Supported operating systems

On 30 June 2025, our Windows protection for these OS versions will become End of Life (EOL): Windows XP, Vista, Server 2003, and Server 2008 (Windows 2008 R2 will continue to be supported). After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

Workstations with an x86 or x64 microprocessor

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 11 (64-bit)

Computers with an ARM microprocessor

- Windows 10 and Pro
- Windows 11 and Pro
- Windows Server 2025 Standard, Datacenter

Servers with an x86 or x64 microprocessor

- Windows 2003 (32-bit, 64-bit) and R2 SP2
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 and Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025 Standard, Datacenter
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016, 2019, and 2022

IoT and Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64-bit)
- Windows Embedded Standard 2009, 7, 7 (64-bit), 8, 8 (64-bit)
- Windows Embedded Pro 8, 8 (64-bit)
- Windows Embedded Industry 8, 8 (64-bit), 8.1, 8.1 (64-bit)
- Windows IoT Core 10, 10 (64-bit)
- Windows IoT Enterprise 10, 10 (64-bit), 11
- Windows Server IoT 2019

Windows Embedded systems allow custom installations that could impact Panda Endpoint Protection Plus. After you install Panda Endpoint Protection Plus, we recommend that you confirm it works as expected.

Hardware requirements

- **Processor**: x86- or x64-compatible CPU with at least SSE2 support.
- **RAM**: 1 GB.
- **Available hard disk space for installation**: The minimum space required to install the security software varies depending on the operating system version installed on the computer. On average, the security software requires 650 MB of available space for installation.

Other requirements

Ports

Panda Endpoint Protection Plus requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443.

The Panda Endpoint Protection Plus agent requires port 33000 for communication between protected computers and with the Firebox or Access Point devices (see Endpoint Access Enforcement settings and Network Access Enforcement on page 290

Root certificates

It is necessary to keep the root certificates of workstations and servers up to date. Also, the computers must be able to access these URLs:

http://*.globalsign.com

http://*.digicert.com

http://*.sectigo.com

Windows computers update root certificates automatically through Windows Update. Nevertheless, incorrectly installed updates might cause problems.

If root certificates are not up to date, some features such as the ability for agents to establish real-time communications with the management console, or the Patch Management module, might not work.

To identify and update root certificates, use the tool available at https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/troubleshooting/psinfotool/psinfo-check-cert.html?Highlight=psinfo.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection Plus be synchronized. This synchronization is normally achieved using an NTP server.

If a computer is not synchronized, several security issues could arise:

- Lack of stability in communications between the computer and the Panda Security servers.
- Errors checking certificates, which appear as valid or expired based on the computer system date, not the real date.
- Date errors in alerts generated by protections, which show the computer system date, not the real date.
- Scan and patch installation tasks show the computer system date, not the real date.
- The installer expiration date is not respected.
- The time periods defined in the web access control feature are not adhered to.
- Some scheduled actions might not run correctly, such as computer restarts and problem notifications.

Support for SHA-256 driver signing

To keep security software up to date, the workstation or server must support SHA-256 driver signing. Some versions of Windows do not include this feature by default and you must update them:

Windows platform	Updates required	URL
Windows Vista x86/Vista x64	SP2 and KB4474419	KB4474419 SP2
Windows Server 2008 x86/Server 2008 x64	SP2 and KB4474419	KB4474419 SP2
Windows 7 x86/Windows 7 x64	SP1 and KB4474419	KB4474419 SP1
Windows 2008 R2 x64	KB4474419	KB4474419

Table 23.17: Updates required to support SHA-256 signed drivers

Computers that do not support SHA-256 driver signing will not have their protection software updated beyond protection version 9.00.00. These computers are not shown in the Outdated protection on page 450 widget as candidates to be updated. These computers are shown with the warning **Cannot upgrade this computer's protection to the latest version**. For more information about computer alerts and how to display them, see Computer details on page 236.

To find computers that do not support SHA-256 driver signing, create a filter in the filter tree with the parameters described in Filter computers not compatible with SHA-256 signed drivers on page 209. For more information about the filter tree, see Filter tree on page 202.

> *We recommend that you update all computers to make sure they are protected with the latest available version of the security software.*

After you install the patches indicated, the latest available version of the security software downloads within four hours. You must restart the computer to complete the update.

Communication with the Panda Endpoint Protection Plus server through TLS 1.2

To enable the security software to communicate with the Panda Endpoint Protection Plus server through the TLS 1.2 protocol, ciphers TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 are required. For more information, see Manage SSL/TLS protocols and cipher suites for AD FS.

Windows 2008 R2 does not support TLS 1.2 natively. It requires that you install a patch available for certain WinHTTP protocols. For more information, see Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows.

Requirements for macOS platforms

> *On 30 June 2025, our Mac protection for these OS versions will become End of Life (EOL): macOS Yosemite, El Capitan, Sierra, High Sierra, or Mojave. After the EOL date, the product license will be automatically removed from all computers that run these OS versions, and you will not be able allocate licenses to affected computers. Computers without a license will have all protections disabled, lose access to Collective Intelligence, stop receiving signature file updates, and cease to run assigned tasks. See https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.*

Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur

- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma
- macOS 15 Sequoia

Hardware requirements

- **Processor**: Intel® Core 2 Duo.
- **RAM**: 2 GB.
- **Available hard disk space for installation**: The minimum space required to install the security software varies depending on the operating system version installed on the computer. On average, the security software requires 400 MB of available space for installation.
- **Ports**: Ports 3127, 3128, 3129, and 8310 must be accessible for the web filtering and malware web detection to work. The Panda Endpoint Protection Plus agent requires port 33000 for communication between computers.

IP addresses required for product activation

To install the security software, make sure the corporate firewall allows traffic to these IP address ranges:

- 17.248.128.0/18
- 17.250.64.0/18
- 17.248.192.0/19

Required permissions

For the security software to operate correctly, you must enable:

- Network extensions.
- System extensions.
- Full disk access.
- Background execution.

Complete the appropriate procedure for your macOS version:

For macOS Catalina or higher

To enable system extensions:

- Open the Panda Endpoint Protection Plus agent on the user computer. Click **Open Security Preferences**.
- The **Security & Privacy** dialog box opens. In the lower-left corner, click the lock icon.

- Enter the administrator **User Name** and **Password**. Click **Unlock**.
- Click **Allow**. System extensions are enabled.

To enable Full Disk Access:

- Open the Panda Endpoint Protection Plus agent on the user computer. Click **Open hard disk access preferences**.
- The **Security & Privacy** dialog box opens. In the lower-left corner, click the lock icon.
- Enter the administrator **User Name** and **Password**. Click **Unlock**.
- Select **Protection Agent**.
- Click **Quit & Reopen**. Full Disk Access is enabled.

For macOS Mojave 10.14 or lower

When your Panda Endpoint Protection Plus software for macOS starts, macOS might block the kernel extensions necessary for it to work.

The reason for this is that macOS 10.14 and lower contain a security feature that requires user approval before it can load new third-party kernel extensions.

For more information, see https://developer.apple.com/library/archive/technotes/tn2459/_index.html#//apple_ref/doc/uid/DTS40017658.

When a request is made to load a kernel extension that the user has not yet approved, the load request is denied. You might receive these notifications:

- System Extension Blocked message.
- Your Computer Is Not Protected message.

To manually approve the kernel extension:

- When you receive the **System Extension Blocked** message, click **OK**. Or, click **Open System Preferences** when you receive the **Your Computer Is Not Protected** message. The **System Preferences** dialog box opens.
- Click **Security & Privacy**.
- In the lower-left corner, click the lock icon.
- In the **Security & Privacy** dialog box, click **Allow**.

For macOS Ventura 13

The security software might stop working on computers if the agent is not allowed to run in the background. For this reason, you must allow the **Background execution** permission on the computer.

Requirements for Linux platforms

Panda Endpoint Protection Plus can be installed on Linux workstations and servers. On computers with no graphical environment, the URL filtering and web detection features are disabled. To manage the security software on computers with no graphical environment, use the `/usr/ local/protection-agent/pa_cmd` tool.

Supported distributions

64-bit distributions

- **Ubuntu**: 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 17.10, 18.04 LTS, 18.10, 19.04, 19.10, 20.04 LTS, 20.10, 21.04, 21.10, 22.04 LTS, 22.10, 23.04, 23.10, 24.04, and 24.10.
- **Fedora**: 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40 and 41.
- **Debian**: 8, 9, 10, 11, and 12.
- **RedHat**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 and 9.6.
- **CentOS**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, and 8.5.
- **CentOS Stream**: 8 and 9.
- **Rocky Linux**: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 and 9.6.
- **AlmaLinux**: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 and 9.6.
- **Linux Mint**: 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2, 19.3, 20, 20.1, 20.2, 20.3, 21, 21.1, 21.2, 21.3 22 and 22.1.
- **SUSE Linux Enterprise**: 11 SP2, 11 SP3, 11 SP4, 12, 12 SP1, 12 SP2, 12 SP3, 12 SP4, 12 SP5, 15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 15 SP6 and 15 SP7.
- **Oracle Linux:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 and 9.6.
- **openSUSE**: 15.3, 15.4, 15.5, and 15.6.
- **Amazon Linux:** 2

32-bit distributions

- **Red Hat**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.
- **CentOS**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.

Supported kernel versions

For more information about the supported Linux distributions and kernels, see https://www.pandasecurity.com/enterprise/downloads/docs/product/help/adaptivedefense360/v16/es/Content/28_linux_kernels.htm.

Panda Endpoint Protection Plus is not supported on special or modified versions of the Linux kernel.

Supported file managers

- Nautilus
- PCManFM
- Dolphin

Hardware requirements

- **Processor**: x86 or x64-compatible CPU with at least SSE2 support.
- **RAM**: 1.5 GB.
- **Available hard disk space for installation**: The minimum space required to install the security software varies depending on the operating system version installed on the computer. On average, the security software requires 500 MB of available space for installation.
- **Ports**: Ports 3127, 3128, 3129, and 8310 must be accessible for the web filtering and malware web detection to work. The Panda Endpoint Protection Plus agent requires port 33000 for communication between computers.

Installation script checks

When you run it, the installation script performs a number of checks that require installation of one of these packages or binaries:

- wget
- curl
- semanage (if you need to integrate the security software using SELinux policies)

If none of these packages are installed, the installation process fails returning an error.

Installation package dependencies

The Linux agent uses the distribution package manager to download all dependencies that are not satisfied. Generally, the packages required are:

- **Libcurl**: For Debian-based distributions, see Libcurl libraries
- **OpenSSL**
- **GCC and compilation utilities**: make and makeconfig only on Fedora.

The installation process on Fedora includes compilation of the modules required by the Panda Endpoint Protection Plus agent to work correctly.

To show the agent dependencies, run these commands on a terminal based on the target distribution:

- For Debian-based distributions: `dpkg --info package.deb`
- For Fedora-based distributions: `rpm --qRp package.rpm`

Libcurl libraries

The protection module requires the installation of the 32-bit `libcurl3` or 32-bit `libcurl4` library. If you already have one of these libraries installed (for 64-bit systems), make sure the package manager downloads the same library (`libcurl3` or `libcurl4`) with the same version for 32-bit systems. Otherwise, Panda Endpoint Protection Plus does not run correctly on the computer and you must manually install the appropriate library.

For example, if your computer has the `libcurl3 x.y.z` library (for 64-bit systems), the package manager must download the `libcurl3 x.y.z` library (for 32-bit systems), and not `libcurl4 x.y.z` (for 32-bit systems).

Supported kernels

Last updated: Tuesday, July 1, 2025

For more information about the supported Linux distributions and kernels, see Supported kernels.

Requirements for Android platforms

Supported operating systems

- Android Marshmallow 6.0
- Android Nougat 7.0 - 7.1
- Android Oreo 8.0
- Android Pie 9.0
- Android 10
- Android 11
- Android 12
- Android 13
- Android 14
- Android 15

Hardware requirements

The minimum space required to install the security software varies depending on the operating system version installed on the device. On average, the security software requires 10 MB of available space for installation.

Network requirements

For push notifications to work, open ports 5228, 5229, and 5230 to all IP addresses contained in the IP blocks listed in Google's ASN 15169.

Permissions required on the device

To use all of the Panda Endpoint Protection Plus features, the user of the device must allow these permissions:

- Camera access
- Read phone state
- Make calls
- Get location
- Device location services
- Draw over other apps
- Act as device administrator
- Access external storage
- Background location access

On mobile devices that run Android 12, these permissions are also required:

- Disable app hibernation
- Ignore battery optimizations

On mobile devices that run Android 13, this permission is also required:

- Send notifications

Requirements for iOS platforms

Supported operating systems

- iOS 13 / iPadOS 13
- iOS 14 / iPadOS 14

- iOS 15 / iPadOS 15
- iOS 16 / iPadOS 16
- iOS 17 / iPadOS 17

Hardware requirements

The minimum space required to install the security software varies depending on the operating system version installed on the device. On average, the security software requires 12 MB of available space for installation.

Network requirements

The application installed on the mobile device uses the Apple Push Notification service to communicate with Panda Endpoint Protection Plus. If the device is connected to the network by 2G, 3G, or 4G, there are no specific network requirements.

If the device is connected to the network by Wi-Fi, Access Point (AP), or other method, it connects to specific servers. Make sure these ports are available:

- TCP 5223 to communicate with the Apple Push Notification service.
- TCP 443 or 2197 to send notifications.

Servers that make up the Apple Push Notification service use load balancing. The device will not always connect to the same IP address. We recommend that you configure your firewall to allow connections to the entire 17.0.0.0/8 range assigned to Apple. If this is not possible, allow connections to these IP ranges:

For IPv4:

- 17.249.0.0/16
- 17.252.0.0/16
- 17.57.144.0/22
- 17.188.128.0/18
- 17.188.20.0/23

For IPv6:

- 2620:149:a44::/48
- 2403:300:a42::/48
- 2403:300:a51::/48
- 2a01:b740:a42::/48

For more information, see https://support.apple.com/en-us/HT203609.

Permissions required on the device

To use all of the Panda Endpoint Protection Plus features, the user of the device must allow these permissions:

- Get location
- Device location services
- Background location access
- Filter network content
- Receive push notifications
- Send notifications
- Allow background app refresh

Local ports and URL access

Local ports

To implement certain features, the security software installed on the computers on the network uses these listening ports:

Windows

- **TCP port 18226**: Used by computers with the cache role on all network interfaces. See Cache role on page 282.
- **TCP port 21226**: Used by computers with the cache role to request the files to download on all network interfaces. See Cache role on page 282.
- **TCP port 3128**: Used by computers with the proxy role on all network interfaces. See Panda proxy role on page 280.
- **UDP port 21226**: Used by computers with the discovery computer role on all network interfaces. See Discovery computer role on page 284
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces, and for communication between computers. See Network Access Enforcement on page 290 and Network Access Enforcement settings.
- **UDP port 35621**: Used by the protection module on the localhost interface.

Linux

- **UDP port 21226**: Used by computers with the discovery computer role on all network interfaces. See Discovery computer role on page 284
- **TCP port 4575**: Used by the protection module on the localhost interface.

- **TCP port 8310**: Used by the protection module on the localhost interface.
- **TCP port 5560**: Internal process communication on the localhost interface.
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces, and for communication between computers. See Network Access Enforcement on page 290 and Network Access Enforcement settings.

macOS

- **UDP port 21226**: Used by computers with the discovery computer role on all network interfaces. See Discovery computer role on page 284
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces. See Network Access Enforcement on page 290.
- **TCP port 4575**: Used by the protection module on the localhost interface.
- **TCP port 8310**: Used by the protection module on the localhost interface.
- **TCP port 5560**: Internal process communication on the localhost interface.
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces, and for communication between computers. See Network Access Enforcement on page 290 and Network Access Enforcement settings.

Access to the web console

You can access the management console with the latest version of these browsers:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Access to service URLs

For Panda Endpoint Protection Plus to work correctly, the protected computers must be able to access these URLs.

Product name	URLs

Panda Endpoint Protection Plus	• https://*.pandasecurity.com
	  • Downloading of installers, the generic uninstaller, and policies.
	  • Agent communications (registration, configuration, tasks, actions, status, real-time communications).
	  • Communications between the protection and Collective Intelligence.

Product name	URLs
	• Downloading of signature files on Android systems. • http://*.pandasecurity.com • Downloading of signature files (on all systems except Android). • https://*.windows.net URLs to send unknown files: • cmg-fusmb.pandasecurity.com • cmp-fusmb.pandasecurity.com • cpg-fusmb.pandasecurity.com • cpp-fusmb.pandasecurity.com • cppi-fusmb.pandasecurity.com • cppl-fusmb.pandasecurity.com • cppe-fusmb.pandasecurity.com • rpuws.pandasecurity.com
Root certificates	• http://*.globalsign.com • http://*.digicert.com • http://*.sectigo.com
Web filtering	• https://rp.cloud.threatseeker.com • https://wg.cloud.threatseeker.com
Panda Patch Management	• https://content.ivanti.com • https://application.ivanti.com • https://stlicense.ivanti.com • https://help.ivanti.com • https://license.shavlik.com
Activity testing	For Windows protection versions higher than 8.00.16. • http://proinfo.pandasoftware.com/connectiontest.html For connectivity tests: • http://*.pandasoftware.com

Product name	URLs
Network attack protection	• https://cpg-nap.pandasecurity.com/nap/buffer • https://cpp-nap.pandasecurity.com/nap/buffer

Table 23.18: Service access URLs

Access to URLs for patch and update downloads (Panda Patch Management)

For a complete list of the URLs that must be accessible to the network computers that receive patches or have the cache/repository role, see this support article: https://www.pandasecurity.com/uk/support/card?id=700044.

Glossary

A

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 in network environments.

Adware

Program that automatically runs, displays, or downloads advertising to the computer.

Alert

See Incident.

Anti-spam

Technology that searches for unwanted email based on its contents.

Anti-Tamper protection

A set of technologies aimed at preventing tampering of the Panda Endpoint Protection Plus 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 Plus and designed to locate lost or stolen mobile devices and minimize data exposure in the case of theft.

Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, contextual analysis, etc.), to detect and remove computer viruses and other threats.

ARP (Address Resolution Protocol)

A telecommunication protocol used for resolution of Internet layer addresses into link layer addresses. On IP networks, this protocol translates IP addresses into physical MAC addresses.

ASLR (Address Space Layout Randomization)

Address Space Layout Randomization (ASLR) is a security technique used in operating systems to prevent buffer overflow-driven exploits. 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.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

A set of resources developed by the MITRE Corporation to describe and categorize dangerous actions of cybercriminals based on observations from around the world. ATT&CK is a structured list of the known behaviors of attackers, broken down into tactics and techniques, and expressed as a matrix. As this list is a comprehensive representation of the behaviors that hackers use when they infiltrate networks, it is a useful resource to develop defensive, preventive, and remedial strategies for organizations. See MITRE Corporation.

Automatic assignment of settings

See Inheritance.

B

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 do not go through routers and use different addressing methodology to differentiate them from unicast packets.

Buffer overflow

Anomaly affecting the management of the input buffers of a process. 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.

C

Cache/Repository (role)

Computers that automatically download and store all files required so that other computers with Panda Endpoint Protection Plus installed can update their signature file, agent, and protection engine without having to access the Internet. This saves bandwidth as it is not necessary for each computer to separately download the updates it needs. All updates are downloaded centrally for all computers on the network.

CKC (Cyber Kill Chain)

In 2011, Lockheed-Martin drafted a framework or model for defending computer networks, which stated that cyberattacks occur in phases and each of them can be interrupted through certain controls. Since then, the Cyber Kill Chain (CKC) has been adopted by IT security organizations to define the phases of cyberattacks. These phases range from remote reconnaissance of the target's assets to data exfiltration.

Cloud (Cloud computing)

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

Computers without a license

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers are not protected, but are shown in the web management console.

CVE (Common Vulnerabilities and Exposures)

List of publicly known cybersecurity vulnerabilities defined and maintained by The MITRE Corporation. Each entry on the list has a unique identifier, enabling CVE to offer a common naming scheme that security tools and human operators can use to exchange information about vulnerabilities with each other.

D

DEP (Data Execution Prevention)

A feature implemented in operating systems to prevent the execution of code from memory pages marked as non-executable. This feature was developed to prevent buffer-overflow exploits.

Device control

Module that enables organizations to define the way protected computers must behave when connecting a removable or mass storage device to them.

DHCP

Service that assigns an IP address to each computer on a network

Dialer

Program that redirects users who 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 Plus 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.

DNS (Domain Name System)

Service that translates domain names into different types of information, generally IP addresses.

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).

E

Entity

Predicate or complement included in the action tables of the forensic analysis module.

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.

EOL (End of Life)

A term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life. After a product reaches its EOL stage, it stops receiving updates or fixes from the relevant vendor, leaving it vulnerable to hacking attacks.

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.

F

Filter

A dynamic-type computer container that automatically groups together items that meet the conditions defined by the administrator. Filters simplify the assignment of security settings and facilitate management of all computers on the network.

Filter tree

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

Firewall

Technology that blocks the network traffic that matches certain patterns defined in rules established by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

Folder tree

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

FQDN (Fully Qualified Domain Name)

A fully qualified domain name (FQDN) is a domain name that specifies the exact location of a host within the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone.

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.

G

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.

H

Hacking tool

Programs used by hackers to perform actions that cause problems for the user of the affected computer (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 enables attackers to insert and later run arbitrary code in the target system's heap memory space. This technique is widely used to exploit vulnerabilities in web browsers and web browser plug-ins.

Heuristic scanning

Static scanning that employs a set of techniques to statically inspect potentially dangerous files. It examines hundreds of characteristics of a file to determine the likelihood that it may take malicious or harmful actions when run on a user's computer.

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

I

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.

Incident

Message relating to the Panda Endpoint Protection Plus advanced protection that may require administrator intervention. Incidents are reported to the administrator through the management console or email (alerts), and to users through pop-up messages generated by the agent and displayed locally on the protected device.

Indicator of attack (IOA)

This is an indicator with a high probability of representing a cyberattack. These are generally attacks in early stages or in exploit phase. These attacks do not generally use malware, as attackers commonly take advantage of legitimate operating system tools to perform the attack and hide their activity. See Indicator.

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 (Internet Protocol)

Principal Internet communications protocol for sending and receiving datagrams generated at the underlying link level.

IP address

Number that identifies a device interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

J

Joke

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

L

Linux distribution

Set of software packets and libraries that make up an operating system based on the Linux kernel.

M

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, a Trojan, a 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.

Malware lifecycle

Breakdown of all the actions unleashed by a malicious program from the time it is first seen on a customer's computer until it is classified as malware and disinfected.

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) an underlying protocol can transmit.

N

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.

O

OU (Organizational Unit)

Hierarchical method for classifying and grouping objects stored in directories.

P

Panda agent

One of the modules included in the Panda Endpoint Protection Plus client software. It manages communications between computers on the network and the Panda cloud-based servers, in addition to managing local processes.

Panda Endpoint Protection Plus client software

Program installed on the computers to protect. It consists of two modules: the Panda agent and the protection.

Panda Full Encryption service

A module compatible with Panda Endpoint Protection Plus 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.

Partner

A company that offers Panda 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.

Patch Management service

A module compatible with Panda Endpoint Protection Plus 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.

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.).

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Phishing

A technique for obtaining confidential information from users fraudulently. The targeted information includes passwords, credit card numbers, and bank account details.

PIN (Personal Identification Number)

The PIN (Personal Identification Number) is a sequence of 8 to 20 numbers that serves as a simple password and is necessary to start a

computer with an encrypted drive. Without the PIN, the boot sequence is not completed and it is impossible to access the computer.

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 Plus software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the 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.

Q

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Quarantine

See Backup.

R

Recovery key

If an anomalous situation is detected on a computer protected with Panda Endpoint Protection Plus, or you forget the unlock key, the system will request a 48-digit recovery key. This password is managed from the management console and must be entered in order to complete the startup process. Each encrypted volume has its own unique recovery key.

RIR (Regional Internet Registry)

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

Role

Specific permission configuration applied to one or more user accounts and which authorizes users to view and edit certain resources of the console.

Rootkit

A program designed to hide objects such as processes, files, or Windows registry entries (often including its own). This type of software is used by attackers to hide evidence and utilities on previously compromised systems.

RWD (Responsive Web Design)

A set of techniques that enable the development of web pages that automatically adapt to the size and resolution of the device being used to view them.

S

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.

SIEM (Security Information and Event Management)

Software that provides storage and real-time analysis of the alerts generated by network devices.

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.

Spam

This term refers to unsolicited email messages that usually contain advertising and are generally sent out massively. Spam can have a range of negative effects on the recipient.

Spyware

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and collects personal data.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

Suspicious item

A program with a high probability of being malware and classified by our heuristic scanner. This type of technology is only used in the scheduled and on-demand scans launched from the Tasks module, never in real-time scans. Heuristic scanning is used to compensate for the lower detection capability of scheduled scan tasks, in which program code is scanned statically, without running the program. See Heuristic scanning.

SYN

Flag in the TOS (Type Of Service) field of TCP packets that identifies them as connection start packets.

System partition

Area of the hard disk that remains unencrypted and which is necessary for computers with Panda Full Encryption enabled to start up properly.

T

Tactic

In ATT&CK terminology, tactics represent the ultimate motive or goal of a technique. It is the adversary's tactical objective: the reason for taking an action. See ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

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.

Technique

In ATT&CK terminology, the techniques represent the way (or the strategy) that an adversary achieves a tactical objective. In other words, 'how'. For example, an adversary, in order to achieve the objective of

accessing credentials (tactic), executes a dump of the data (technique). See ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

TLS (Transport Layer Security)

New version of protocol SSL 3.0.

TPM (Trusted Platform Module)

The TPM is a chip that is part of the motherboard of 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.

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.

U

UDP (User Datagram Protocol)

A transport-layer protocol which is unreliable and unsuited for connections for exchanging IP packets.

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 Plus to regulate administrator access to the web console and establish the actions that administrators can take on the computers on the network.

User (network)

A company's worker using computing devices to do their job.

User account

See User (console).

V

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 enter computers and 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.

W

Web access control

Technology that enables 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 Plus, accessible anywhere, anytime through a supported Internet browser. The web console enables 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. The Panda Endpoint Protection Plus 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

Windows network architecture where shared resources, permissions, and users are managed independently on each computer.