



 Panda Endpoint Protection

Panda Endpoint Protection Administration Guide

Author: Panda Security

Version: 9.10.00

Date: 10/10/2023

Legal notice.

Neither the documents nor the programs that you may access may be copied, reproduced, translated, or transferred to any electronic or readable media without prior written permission from Panda Security, Santiago de Compostela, 12, 48003 Bilbao (Bizkaia), SPAIN.

Registered trademarks.

Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names may be registered trademarks of their respective owners.

© Panda Security 2023. All rights reserved.

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 Administration Guide

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

<https://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONoAP-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/endpointprotection/latest/en/index.htm>

Release notes

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

<https://info.pandasecurity.com/aether/?product=EP&lang=en>

Technical support

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

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

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

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

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

Panda Endpoint Protection 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/feedbackEPGuideEN>

Table of contents

Table of contents	4
Preface	15
Who is this Administration Guide for?	15
What is Panda Endpoint Protection?	15
Icons	16
Panda Endpoint Protection overview	17
Panda Endpoint Protection benefits	17
Panda Endpoint Protection features	18
Aether platform features	19
Key benefits of Aether	19
Aether architecture	21
Aether on users' computers	21
Key components	23
Product user profile	25
Supported devices and languages	25
Panda Endpoint Protection features	27
New security needs	27
Permanent antivirus protection and Collective Intelligence	28
Protection with context-based detections	29
Email and web protection	29
Firewall and intrusion detection system (IDS)	29
Device control	30
Vulnerability patching (Panda Patch Management)	30
Network status visibility	30
Disinfection techniques	30
The adaptation phase	31
The management console	33

Benefits of the web console	34
Web console requirements	34
IDP-based federation	35
General structure of the web console	35
Top menu (1)	36
Side menu (2)	39
Center panel (3)	40
Basic elements of the web console	40
Status area overview	43
Managing lists	45
Templates, settings, and views	45
List sections	48
Operations with lists	50
Predefined lists	53
Controlling and monitoring the management console	55
About user accounts	56
User account structure	56
Two-factor authentication	56
About roles	58
Structure of a role	58
Why are roles necessary?	58
Full Control role	59
Read-Only role	59
About permissions	59
Understanding permissions	59
Accessing the user account and role settings	65
Creating and configuring user accounts	65
Creating, editing, and deleting users	65
Exporting users	65
Listing created users	66
Creating and configuring roles	67
User account activity log	67
Session log	68

User actions log	69
System events	80
Installing the client software	83
Installation on Windows systems	85
Protection deployment overview	85
Installation requirements	88
Generating the installation package and manual deployment	89
Installing the downloaded package	91
Integrating computers based on their IP address	91
Installation with centralized tools	92
Installation from a gold image	95
Remote installation of the client software	102
Remote installation on discovered computers	102
Computer discovery	103
Deleting and hiding computers	105
Viewing discovered computers	106
Discovered computer details	110
Installation on Linux systems	114
Protection deployment overview	114
Installation requirements	115
Network requirements	115
Other requirements	115
Generating the installation package and manual deployment	116
Installation on Linux platforms	117
Installation on macOS systems	120
Protection deployment overview	120
Installation requirements	121
Network requirements	121
Other requirements	122
Manually deploying the macOS agent	122
Installing the downloaded package	123
Installation on Android systems	124
Protection deployment overview	124

Installation requirements	125
Manually deploying and installing the Android agent	125
Deploying the Android agent using an MDM/EMM solution	127
Installation on iOS systems	128
Protection deployment overview	128
Basic concepts	129
Installation requirements	131
Deploying and installing the iOS agent	131
Deploying and installing the agent on supervised devices	137
Configuring an iOS device in supervised mode without loss of data	145
Managing the Apple ID and digital certificates	148
Checking deployment	152
Uninstalling the software	155
Manual uninstallation	155
Remote uninstallation	157
Remote reinstallation	157
Licenses	161
Definitions and basic concepts	162
License contracts	162
Computer status	162
License status and groups	163
Types of licenses	163
Assigning licenses	163
Releasing licenses	164
Processes associated with license assignment	164
Case 1: Computers with assigned licenses and excluded computers	164
Case 2: Computers without an assigned license	165
Licenses module panels/widgets	166
Licenses module lists	168
Expired licenses	172
Expiration notifications	172
Withdrawal of expired licenses	172
Adding trial licenses to commercial licenses	172

Computer search based on license status	173
Product updates and upgrades	175
Updatable modules in the client software	175
Protection engine updates	176
Updates	176
Communications agent updates	178
Knowledge updates	178
Windows, Linux, and macOS devices	178
Android devices	178
Management console update	179
Considerations prior to updating the console version	179
Managing computers and devices	181
The Computers area	182
The Computer tree panel	183
Filter tree	184
About filters	184
Predefined filters	184
Creating and organizing filters	186
Configuring filters	187
Example filters	189
Group tree	191
Creating and organizing groups	193
Moving computers from one group to another	195
Filtering results by groups	196
Filtering groups	197
Scan and disinfection tasks	197
Available lists for managing computers	198
The Computer list panel	198
My lists panel	208
Computer details	217
General section (1)	218
General section for mobile devices	218
Computer notifications section (2)	220

Details section (3)	229
Detections section (4) for Windows, Linux, and macOS computers	234
Detections section (4) for Android and iOS devices	234
Hardware section (5)	235
Software section (6)	236
Settings section (7)	238
Action bar (8)	238
Hidden icons (9)	239
Managing settings	241
Strategies for creating settings profiles	241
Overview of assigning settings profiles to computers	242
Introduction to the various types of settings profiles	243
Modular vs. monolithic settings profiles	245
Creating and managing settings profiles	247
Manual and automatic assignment of settings profiles	249
Manual/direct assignment of settings profiles	249
Indirect assignment of settings profiles: the two rules of inheritance	251
Inheritance limits	252
Overwriting settings	253
Moving groups and computers	255
Exceptions to indirect inheritance	256
Settings received from a partner	256
Features of the settings sent by partners	257
Requirements	257
Viewing assigned settings profiles	257
Configuring the agent remotely	259
Configuring the Panda agent role	260
Proxy role	260
Cache/repository role	261
Discovery computer role	263
Configuring proxies lists for Internet access	264
Configuring downloads from cache computers	266
Requirements for using a cache computer	267

Configuring real-time communication	268
Configuring the agent language	269
Configuring the agent visibility	269
Configuring Secure VPN	270
Requirements	270
Requirements checking	271
Accessing the Secure VPN settings	271
Configuring the anti-tamper protection and password	272
Anti-tamper protection	272
Password-protection of the agent	272
Configuring Shadow Copies	273
Accessing the Shadow Copies feature	274
Security settings for workstations and servers	277
Accessing the settings and required permissions	278
Introduction to the security settings	278
General settings	279
Local alerts	279
Updates	280
Uninstall other security products	280
Files and paths excluded from scans	280
Antivirus	281
Threats to detect	282
File types	283
Firewall (Windows computers)	283
Operating mode	284
Network types	284
Program rules	286
Connection rules	288
Block intrusions	290
Device control (Windows computers)	292
Allowed devices	293
Security settings for mobile devices	295
Security settings for Android devices	296

Updates	296
Antivirus	296
Anti-theft	297
Accessing the anti-theft feature	297
Anti-theft protection settings	297
Security settings for iOS devices	298
Antivirus for web browsers	298
Exclusions	299
Anti-theft	299
Accessing the anti-theft protection	299
Panda Patch Management (Updating vulnerable programs)	301
Panda Patch Management features	302
General workflow	303
Make sure that Panda Patch Management works correctly	303
Make sure that all published patches are installed	304
Download and install the patches	304
Download patches manually	309
Uninstall problematic patches	312
Check the result of patch installation/uninstallation tasks	313
Exclude patches for all or certain computers	313
Make sure the programs installed are not in EOL (End-Of-Life) stage	314
Check the history of patch and update installations	314
Check the patch status of computers with incidents	315
Configuring the discovery of missing patches	315
General options	316
Search frequency	316
Patch criticality	316
Panda Patch Management widgets/panels	317
Panda Patch Management module lists	329
Panda Full Encryption (Device encryption)	363
Introduction to encryption concepts	364
Panda Full Encryption service overview	366
General features of Panda Full Encryption	367

Panda Full Encryption minimum requirements	368
Management of computers according to their prior encryption status	368
Encryption and decryption	369
Panda Full Encryption response to errors	374
Getting a recovery key	375
Getting the recovery key ID for an encrypted drive	375
Getting a recovery key	377
Finding a recovery key	377
Managing computers encrypted by the user	378
Panda Full Encryption module panels/widgets	378
Panda Full Encryption lists	385
Encryption settings	392
Panda Full Encryption settings	392
Available filters	394
MDR service settings	395
MDR service settings	395
MDR setting options	396
Malware and network visibility	399
Security module panels/widgets	399
Security module lists	408
Managing threats, items in the process of classification, and quar- antine	433
Introduction to threat management tools	433
Allowing and preventing items to run	434
List of allowed threats	435
Managing the backup/quarantine area	439
Alerts	441
Email alerts	441
Scheduled sending of reports and lists	447
Report features	447
Report types	448
Requirements for generating reports	449

Accessing the sending of reports and lists	449
Managing reports	451
Configuring reports and lists	452
Contents of the reports and lists	454
Lists	454
Lists of devices	454
Executive report	455
Remediation tools	457
Automatic computer scanning and disinfection	458
On-demand computer scanning and disinfection	458
Creating a task from the computer tree	459
Creating a task from the Computers list	460
Scan options	462
Lists generated by scan tasks	463
Scan task results list	463
View detections list	465
Computer restart	466
Reporting a problem	466
Allowing external access to the web console	467
Removing ransomware and restoring the system to a previous state	467
Tasks	469
Introduction to the task system	469
Creating a task from the Tasks area	471
Task publication	474
Task list	474
Task management	475
Task results	476
Automatic adjustment of task recipients	478
Hardware, software, and network requirements	481
Supported features by platform	481
Requirements for Windows platforms	486
Supported operating systems	486

Hardware requirements	487
Other requirements	488
Requirements for macOS platforms	490
Requirements for Linux platforms	491
Requirements for Android platforms	493
Requirements for iOS platforms	494
Local ports	495
Access to the web console	496
Access to service URLs	496
The Panda Account	499
Creating a Panda Account for Panda Security users	499
Activating the Panda Account	500
Creating and linking a Panda Account to WatchGuard	501
Glossary	503

Chapter 1

Preface

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

Chapter contents

Who is this Administration Guide for?	15
What is Panda Endpoint Protection?	15
Icons	16

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?

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

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

- Panda Endpoint Protection
- Aether platform

Panda Endpoint Protection

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

Aether platform

Aether is the ecosystem where Panda Endpoint Protection is run. It is a scalable and efficient platform for the centralized management of the Panda Security security solutions, addressing the needs of key accounts and MSPs. Aether delivers all the information generated by Panda Endpoint Protection about processes, the programs run by users, and the 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.

Panda Endpoint Protection overview

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

Chapter contents

Panda Endpoint Protection benefits	17
Panda Endpoint Protection features	18
Aether platform features	19
Key benefits of Aether	19
Aether architecture	21
Aether on users' computers	21
Key components	23
Product user profile	25
Supported devices and languages	25

Panda Endpoint Protection benefits

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

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

Panda Endpoint Protection features

Panda Endpoint Protection is a product that 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. This means the malware database has been moved from the user's 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 users' computers.

Cross-platform security

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 systems, Linux, macOS, Android, and virtual environments (VMware, Virtual PC, MS Hyper-V, Citrix). Management of licenses belonging to both persistent and non-persistent virtualization infrastructure (VDI)..

Easy to manage

- Easy-to-manage solution which does not require maintenance or additional infrastructure on the customer's 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 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 competitors' products to facilitate rapid migration from third-party solutions.
- **Smooth learning curve:** Intuitive, simple web-based management interface, with most-frequently used options one click away.

Aether platform features

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

The Aether platform manages communications with the agents deployed across the network. Its management console presents the data gathered by Panda Endpoint Protection 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.

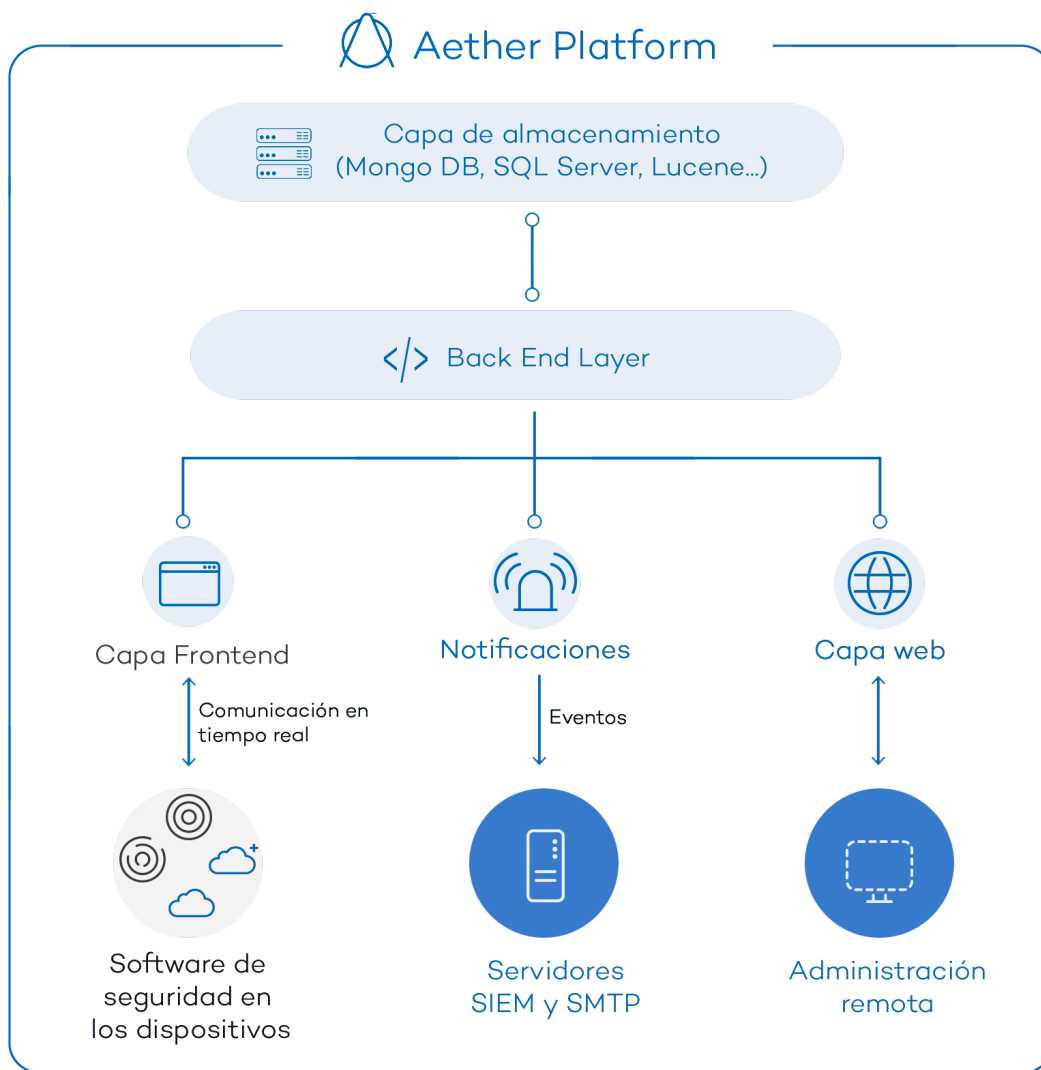


Figure 2.1: Logical structure of Aether

Aether on users' computers

Network computers protected by Panda Endpoint Protection 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 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 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.

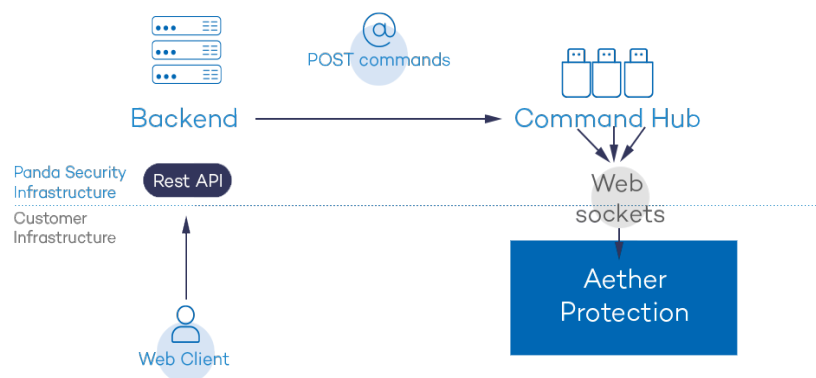


Figure 2.2: Flowchart of the commands entered through the management console

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 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 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 and its components:

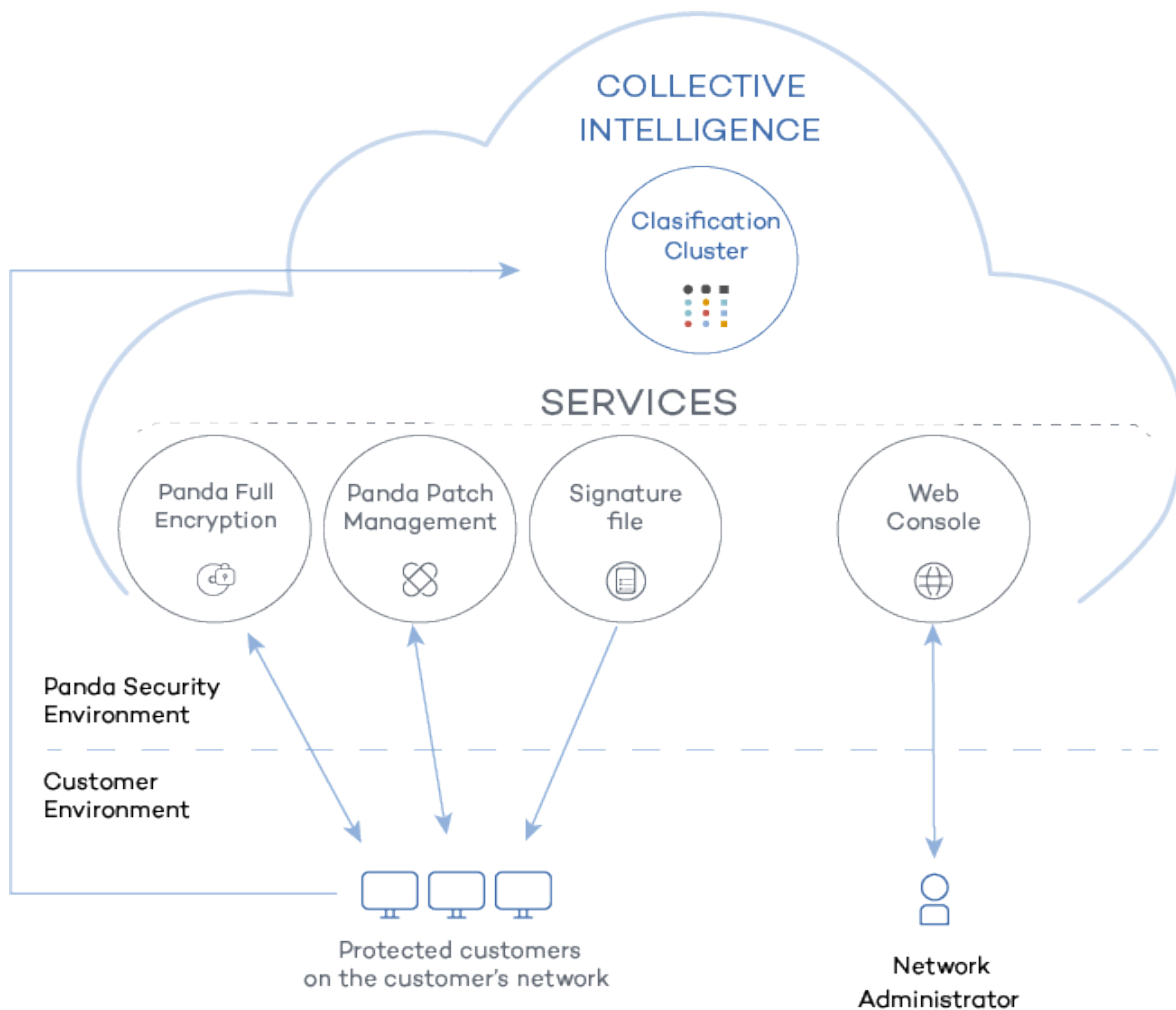


Figure 2.3: Panda Endpoint Protection general structure

- **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.
- **Panda Data Control service (optional):** A service for finding, listing, and monitoring the personal information stored in PII files.

- **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).
- 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 protection installed on computers queries Collective Intelligence only when required, ensuring maximum detection power without negatively affecting resource consumption.

Signature file servers

These are the cloud-based resources that Panda Security makes available to users to download the signature files required by Panda Endpoint Protection to perform detection tasks. 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 496.

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

Computers protected with Panda Endpoint Protection

Panda Endpoint Protection requires the installation of a small software component on all computers on the network susceptible of having security problems. This component is made up of two

modules: the Panda communications agent and the Panda Endpoint Protection protection module.



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

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

Product user profile

Even though Panda Endpoint Protection 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 [Hardware, software, and network requirements](#) on page 481.

Supported operating systems

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

Supported web browsers

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

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

Languages supported in the web console

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

Panda Endpoint Protection features

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

Chapter contents

New security needs	27
Permanent antivirus protection and Collective Intelligence	28
Protection with context-based detections	29
Email and web protection	29
Firewall and intrusion detection system (IDS)	29
Device control	30
Vulnerability patching (Panda Patch Management)	30
Network status visibility	30
Disinfection techniques	30
The adaptation phase	31

New security needs

In recent years, the use of the Internet and all types of mobile devices has become universal in all fields. Laptops, servers, smartphones, tablets, removable storage drives, and numerous other devices are now widely used in corporate environments. The business world has benefited

enormously from these changes, increasing productivity and efficiency and also improving internal and external communication.

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

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

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

Permanent antivirus protection and Collective Intelligence

The permanent antivirus protection is the traditional security module used to defend organizations against the infection vectors most commonly used by hackers. This module leverages the signature file published by Panda Security for local download as well as real-time queries to Collective Intelligence.

In the current context of ever-increasing amounts of malware, cloud-hosted services have proven much more effective than traditional, locally-stored signature files. That is why the Panda Endpoint Protection antivirus protection is primarily based on Collective Intelligence, a cloud-based knowledge platform that exponentially increases detection capabilities.

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

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

Panda Endpoint Protection leverages Collective Intelligence to increase its detection capabilities without negatively impacting on customers' system performance. All knowledge is in the cloud and all users can benefit from it.



For more information about the Panda Endpoint Protection antivirus service on Windows, Linux, and macOS platforms, see [Security settings for workstations and servers](#) on page 277. For more information about the Panda Endpoint Protection antivirus service on mobile platforms, see [Security settings for mobile devices](#) on page 295.

Protection with context-based detections

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

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

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

Email and web protection

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

Firewall and intrusion detection system (IDS)

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

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

Device control

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

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

Vulnerability patching (Panda Patch Management)

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

To tackle this threat, Panda Patch Management enables administrators to create real-time and scheduled patching tasks and push them out to the computers in their organization, thereby reducing the attack surface of workstations and servers.

Network status visibility

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

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



For more information, see [Malware and network visibility](#).

Disinfection techniques

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



For more information, see [Remediation tools](#).

The adaptation phase

You can use Panda Endpoint Protection to strengthen the security of workstations and servers in a number of ways:

Changing the antivirus protection settings

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

Decoy Files

When you enable the Decoy Files feature, Panda Endpoint Protection generates bait files on user computers that it permanently monitors. When a process modifies any of those files, the Decoy Files feature generates an alert, blocks the process, and classifies it as ransomware. To avoid classifying legitimate programs as ransomware, you can create exclusions.

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

Another commonly-used infection vector is the USB drives and modems that users use. Limiting or totally blocking access to these devices blocks malware infections through these means.

Restricting communications (firewall and IDS)

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

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

Changing the Panda Patch Management settings

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

Additionally, uninstalling or updating the programs that are in EOL (End of Life) status minimizes the attack surface of your computers, as all software that does not receive updates is removed. This software is more likely to have unpatched vulnerabilities that could be exploited by malware.

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

This minimizes the exposure of the data stored on the company's computers in the event of loss or theft, and prevents access to confidential data with recovery tools for retrieving files from removed drives. Additionally, we recommend that you use the TPM module included on computer motherboards or update their hardware to support this tool. The TPM enables you to prevent hard

disks from being used on computers other than those used to encrypt them, and detect changes to a computer's boot sequence.

Recovering information using Shadow Copies

Create a daily backup of hard disks, both internal and USB-connected disks, and NTFS disks. This feature enables you to recover information lost due to a ransomware attack or files encrypted by attackers.

VPN security reinforcement

Security for VPN connections provides an additional layer of protection for VPN connections between the corporate network and remote computers. The agent installed on the protected computer collects and sends information to check whether it meets the security requirements for connecting to the VPN. If it does not meet those requirements, the connection is rejected. For more information, see [Configuring Secure VPN](#) on page 270.

The management console

Panda Endpoint Protection 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	34
Web console requirements	34
IDP-based federation	35
General structure of the web console	35
Top menu (1)	36
Side menu (2)	39
Center panel (3)	40
Basic elements of the web console	40
Status area overview	43
Managing lists	45
Templates, settings, and views	45

List sections	48
Operations with lists	50
Predefined lists	53

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 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.

Web console requirements

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

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

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

- Go to <https://www.watchguard.com/>. Click the **Log In** button in the upper-right corner of the page.
- Enter your WatchGuard credentials. The **Support Center** page opens.
- Click the **My Watchguard** menu at the top of the page. A drop-down menu appears.

- Click the **Manage Panda Products** option. The Panda Cloud page opens with all contracted services.
- Click the Panda Endpoint Protection tile. The management console opens.

The following requirements must be met to access the web console:

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



For more information about how to create a Panda Account to access the web console, see [The Panda Account](#) on page 499.

- You must use a supported browser.
- Check the computer has an Internet connection and verify that communication through port 443 is not blocked by a firewall.

IDP-based federation

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

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

General structure of the web console

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

The aim is to deliver a simple yet flexible and powerful tool that 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.

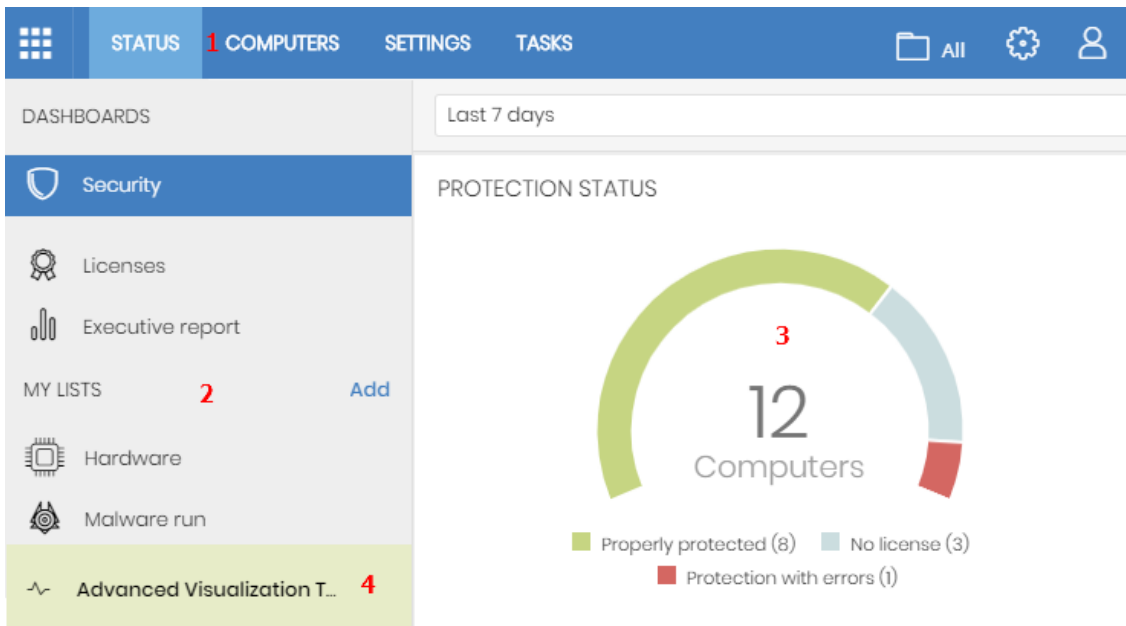



Figure 4.1: Panda Endpoint Protection management console overview

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 [182](#) for more information.

Settings menu

Define the behavior of Panda Endpoint Protection 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 [241](#) for more information about how to create settings profiles in Panda Endpoint Protection.

Tasks menu

Schedule security tasks to be run on the day and time you specify. See [Tasks](#) on page [469](#).

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 [196](#) 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 update](#) on page [179](#).

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 Administration Guide	Provides access to the Panda Endpoint Protection Administration Guide.
Technical Support	Takes you to the technical support website for Panda Endpoint Protection.
Suggestion Box	Launches the mail client installed on the computer to send an email to 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 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. <ul style="list-style-type: none"> • Version: product version.

Option	Description
	<ul style="list-style-type: none"> • Protection version: internal version of the protection module installed on computers. • Agent version: internal version of the communications module installed on computers.

Table 4.1: General options menu

User account icon

Displays a drop-down menu with the following options:


Option	Description
Account	Name of the account used to access the console.
Customer ID	This is the number used by Panda to identify the customer. It 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	Change the information of the product's main account. Users who access the Panda Endpoint Protection console from WGPortal do not see this option as their account is configured from the WatchGuard website.
Change account	Lists all the accounts that are accessible to the administrator and 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 4.2: 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 4.1:** 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 399.

Basic elements of the web console

Tab menu

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

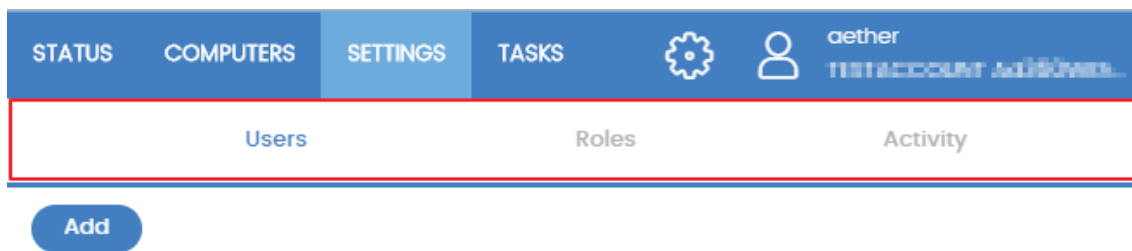


Figure 4.2: Tab menu

Action bar



Figure 4.3: 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 administrators 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.

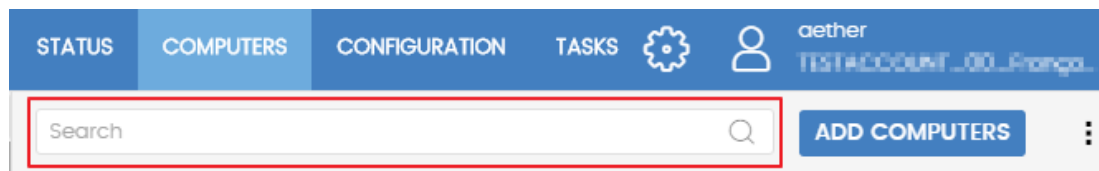


Figure 4.4: Filter tool

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.

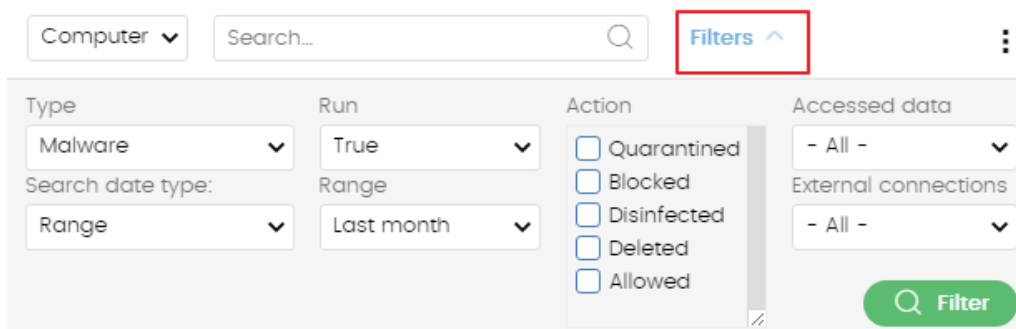
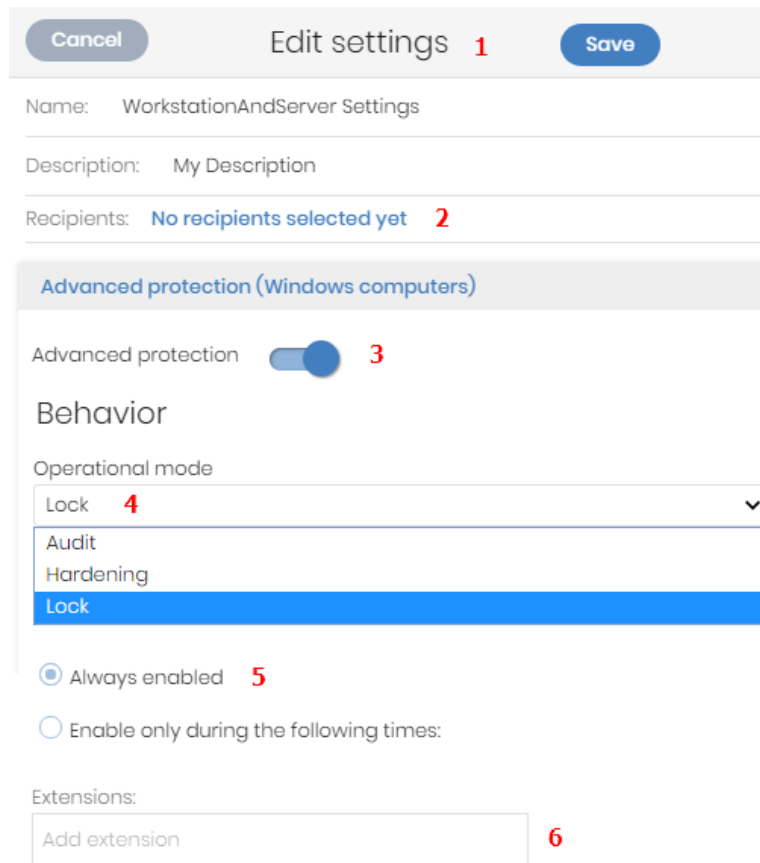


Figure 4.5: Data filter tool in lists

Other interface elements

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

- Buttons. **(1)**
- Links. **(2)**
- Checkboxes. **(3)**
- Drop-down menus. **(4)**
- Combo boxes. **(5)**
- Text fields. **(6)**



Cancel Edit settings 1 Save

Name: WorkstationAndServer Settings

Description: My Description

Recipients: No recipients selected yet 2

Advanced protection (Windows computers)

Advanced protection 3

Behavior

Operational mode

Lock 4

Audit

Hardening

Lock

Always enabled 5


Enable only during the following times:

Extensions:

Add extension 6


Figure 4.6: Controls for using the management console

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 are displayed when you click the  icon. They show options related to the area they are in.

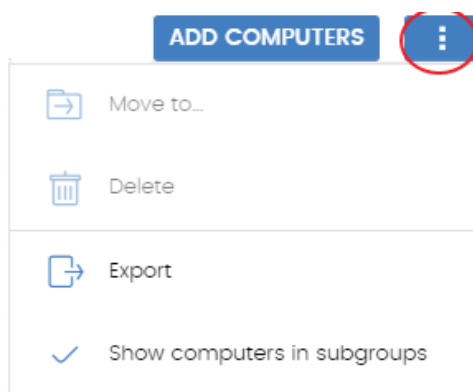


Figure 4.7: Context menus

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.

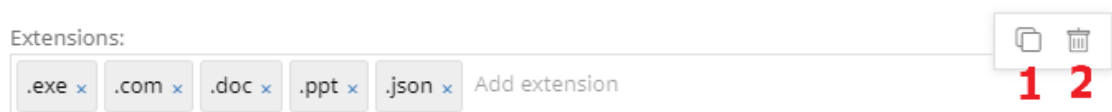


Figure 4.8: Copy and Delete buttons

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

Status area overview

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

Access to dashboards (1)

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

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

Time period selector (2)

The dashboard shows information for the time period selected by the administrator in the drop-down menu at the top of the **Status** page. You can select the following time periods:

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



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

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 399.
- **Patch Management:** Information about updates of the operating system and third-party software installed on computers. For more information about the available widgets, see [Security module panels/widgets](#) on page 399.
- **Panda Full Encryption:** Information about the encryption status of your computers' internal storage devices. For more information about the available widgets, see [Security module panels/widgets](#) on page 399.
- **Licenses:** Information about the status of the Panda Endpoint Protection licenses assigned to the computers on your network. See [Licenses](#) for more information about license management.
- **Scheduled reports:** See [Scheduled sending of reports and lists](#) on page 447 for more information about how to configure and generate reports.

My lists (4)

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

Information panels/widgets (5)

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

The information in the 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 uses several types of graphs to display information in the most practical way based on the type of data shown:

- Pie charts.
- Histograms.
- Line charts.

Managing lists

Panda Endpoint Protection structures the information collected at two levels: a first level that presents the data graphically 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 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.

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.

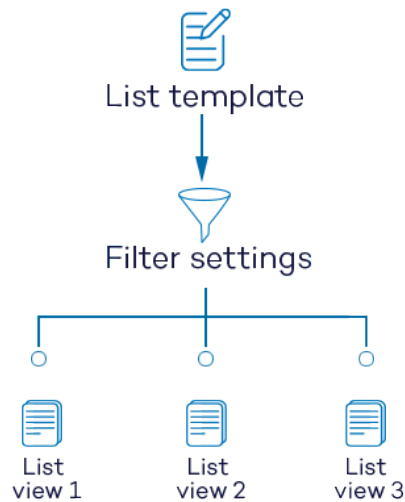


Figure 4.9: Generating three lists from a single template/data source

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 168 for more information.
	Unmanaged computers discovered	Shows all Windows computers on your network that do not have the Panda Endpoint Protection software installed. See Computer discovery on page 103 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 213 for more information.
	Software	Shows the software installed on the computers on your network. See Software on page 211 for more information.

Group	List	Description
	Hardware	Shows the hardware installed on the computers on your network. See Hardware on page 208 for more information.
Security	Computer protection status	Shows details of the protection status of the computers on your network. See Computer protection status on page 409 for 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 415 for more information.
	Intrusion attempts blocked	Shows the intrusion attempts blocked by the computer's firewall. See Intrusion attempts blocked on page 425 for more information.
	Blocked devices	Shows details of all computers on your network with limitations regarding access to peripherals. See Blocked devices on page 421 for more information.
	Blocked connections	Shows the connections blocked by the local firewall. See Intrusion attempts blocked on page 425 for 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 330 for more information.
	Available	Shows a list of all missing patches on the computers

Group	List	Description
	patches	on your network and published by Panda Security. See Available patches on page 323 for more information.
	Installation history	Shows the patches that Panda Endpoint Protection tried to install and the computers that received them during the selected time period. See Installation history on page 345 for 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 343 for more information.
	Excluded patches	Shows the computer-patch pairs excluded from installation tasks. See Excluded patches on page 352 for more information.
Data protection	Encryption status	Shows information about the computers on your network compatible with the encryption feature. See Encryption status on page 385 for more information.

Table 4.3: Templates available in Panda Endpoint Protection

Additionally, there are other templates you can directly access from the context menu of certain lists or from certain widgets on the 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.

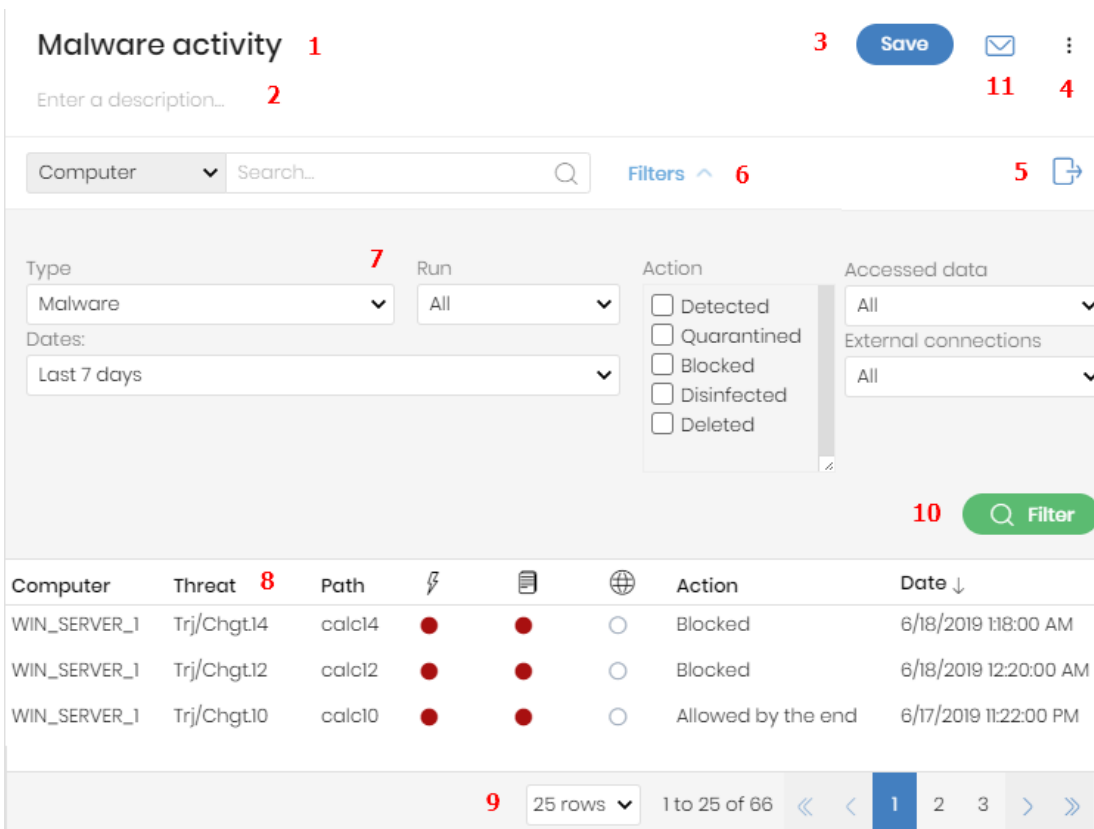





Figure 4.10: List page elements

- **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](#) on page 50 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.

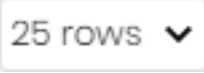
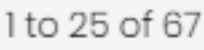





Icon	Description
	Rows per page selector.
	Range of rows displayed out of the total number of rows.
	First page link.
	Previous page link.
	Numbered links to access pages directly.
	Next page link.
	Last page link.

Table 4.4: Pagination controls

- **Scheduled report (11):** Panda Endpoint Protection enables you to send a CSV file with the contents of the list by email. See [Scheduled sending of reports and lists](#) on page 447 for more information.

Operations with lists

Click the **Status** menu at the top of the console. Click **My lists** from the side menu to view all lists created by the administrator as well as a number of predefined lists that Panda Endpoint Protection includes by default. See [Predefined lists](#) for more information.

Creating a custom list

You can create a new custom list/view in various 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)** and then clicking **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 of the list you want to copy.
 - Click **Make a copy**. A new template view is created with the name "Copy of...".

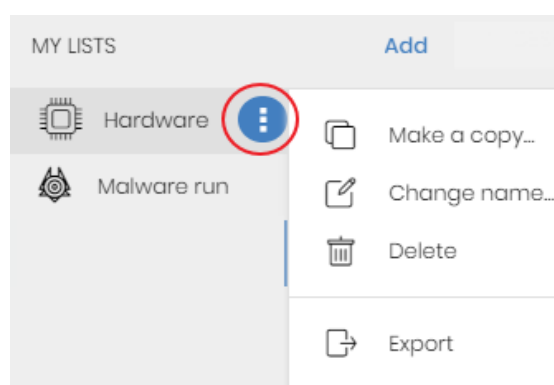




Figure 4.11: Context menu of the lists accessible from the My lists panel



Deleting a list

You can delete a list in various ways:

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




Copying a list

You can copy a list in various ways:

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



Exporting a list

You can export lists to CSV format to get more information than is displayed 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 various 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's context menu **(4)**.
 - Click the  **Export** icon from the drop-down menu displayed. A CSV file is downloaded with the list data.

Exporting a list's details


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

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

Configuring a custom list

- Assign a new name to the list **(1)**. By default, the console creates new names for lists by adding the text “New” to the type of list, or “Copy 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 and is accessible 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 of the list to be sent and select the **Schedule report** option.
 - A window opens where you can enter the necessary information to automatically send the list.
- **From the list**
 - Click the  **(11)** icon. A window opens where you can enter the necessary information to automatically send the list.



See [Scheduled sending of reports and lists](#) on page [447](#) for more information.

Available actions for computers in lists

Some lists, such as **Licenses** or **Computer protection status**, incorporate checkboxes that enable you to select computers. Select one or more computers to display an action bar at the top of the page. This bar makes it easier to manage the selected workstations and servers.

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 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](#) 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 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 [409](#) for more information.

Software

Shows a list of the programs installed across your network. See [Software](#) on page [211](#) for more information.

Hardware

Shows a list of the hardware components installed across your network. See [Hardware](#) on page [208](#) for more information.

Chapter 5

Controlling and monitoring the management console

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

These resources are as follows:

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

Chapter contents

About user accounts	56
User account structure	56
Two-factor authentication	56
About roles	58
Structure of a role	58
Why are roles necessary?	58
Full Control role	59
Read-Only role	59
About permissions	59
Understanding permissions	59
Accessing the user account and role settings	65
Creating and configuring user accounts	65
Creating, editing, and deleting users	65
Exporting users	65

Listing created users	66
Creating and configuring roles	67
User account activity log	67
Session log	68
User actions log	69
System events	80

About user accounts

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

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



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

User account structure

A user account consists of the following items:

- **Account login email:** This is assigned when the account is created. Its aim is to identify the administrator accessing the account.
- **Account password:** This is assigned after the account is created and is designed to control access to the account.
- **Assigned role:** This is assigned after the user account is created. It determines which computers the account user can manage and the actions they can take.

Two-factor authentication

Panda Endpoint Protection 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 the network administrator tries to access the web console, they are prompted to enter an additional authentication item: a code that only the account owner has. This is a randomly generated code that is sent to a specific device, normally the Panda Endpoint Protection administrator's personal smartphone or tablet.

Requirements for enabling 2FA

Access to a personal smartphone or tablet with a built-in camera.

Google Authenticator or an equivalent app must be installed on the personal device. Google Authenticator can be downloaded for free from

<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl>

Enabling 2FA

In the top menu, click the user account and select the **Set up my profile** option. The **Panda Account** page opens.



Figure 5.1: Shortcut to your Panda Account

Click **Login** from the side menu. Click the **Enable** link in section **Two-step verification**. A window opens for you to configure Google Authenticator or the equivalent app installed on your mobile device.

Scan the QR code displayed in the window using Google Authenticator or your equivalent app and enter the generated code in section **Enter the code provided by your app**. Click the **Verify** button. From this moment on, your device is linked to the Panda Endpoint Protection service and will generate short-lived random passcodes.

Accessing the console using an account with 2FA enabled

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

Forcing all console users to use 2FA

To force all console users to enable and use 2FA, the user account from which the use of 2FA is enforced must have the **Manage users and roles** permission and access to all computers on the network. See [Manage users and roles](#) for a description of this permission. See [Structure of a role](#) for more information about how to configure the groups that a role has permissions on.

- Click **Settings** from the menu at the top of the console. Click **Users** in the side menu. Click the **Security** tab.
- Select the option **Require users to have two-factor authentication enabled to access this account**.
- If the user account that forces all console users to have 2FA enabled does not have 2FA enabled for itself, a warning message is displayed prompting you to access your **Panda Account** and enable the feature. See [Enabling 2FA](#)

About roles

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

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

Structure of a role

A role consists of the following:

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

Why are roles necessary?

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

The number of computers to manage

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

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

The purpose of the specific computer

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

The knowledge or expertise of the technician

Depending on the profile of the technician or their role within the IT department, they can be assigned simply monitoring or validation (read-only) permissions or more advanced access, such as permission to edit the security settings of computers. For example, it is not uncommon in large

companies to find a certain group of technicians dedicated solely to deploying software on the network.

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

Full Control role

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

The **Full Control** role cannot be deleted or edited. Neither is it possible to access its details. Any user account can be assigned this role through the web console.

Read-Only role

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

The **Read-Only** role cannot be deleted or edited. Neither is it possible to access its details. Any user account can be assigned this role through the web console.

About permissions

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

Understanding permissions

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

Modify computer tree

- **Enabled:** The account user has full access to the group tree, and can create and delete groups, as well as moving computers to already-created groups.
- **Enabled with permission conflict:** Because of the inheritance mechanism that applies to the computer tree, any changes made to the tree structure 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 249
- **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 distribute the installer to the computers on the network and integrate them into the console. They can also delete computers from the console and configure all aspects related to the discovery of unmanaged computers: assign and revoke the discovery computer role, edit discovery settings, launch an immediate discovery task, and install the Panda agent remotely from the list of discovered computers.
- **Disabled:** The account user cannot download the installer, nor distribute it to the computers on the network. Neither can they delete computers from the console or access the computer discovery feature.

Modify network settings (proxies and cache)

- **Enabled:** The account user can create new **Network settings 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 they 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 they 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 software on Windows computers.
- **Disabled:** The account user cannot restart computers or remotely reinstall the Panda Endpoint Protection 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 is shown.

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 a computer.

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 is shown. 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 a specific mobile device.

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 for sending anti-theft tasks to mobile devices.
- **Disabled:** The account user cannot view the geolocation map nor use the action panel for sending anti-theft tasks to mobile devices.

View detections and threats

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



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

Launch scans and disinfect

- **Enabled:** The account user can create, edit, and delete scan and disinfection tasks.
- **Disabled:** The account user cannot create new scan and disinfection tasks, nor edit or delete existing ones. They 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 workstations and servers.
- **Disabled:** The account user cannot create, edit, delete, or assign patch management settings profiles to Windows workstations and servers.

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

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 the following lists: **Available patches**, **End-of-Life programs**, **Installation history**,

and **Excluded patches**.

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

View available patches



*This permission is 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 the following lists: **Patch management status**, **Available patches**, **End-Of-Life programs**, and **Installation history**.

Configure computer encryption

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

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 a computer or group.
- **Disabled:** The account user cannot view the encryption settings profiles created, nor access the encryption settings profiles assigned to each computer.

Access recovery keys for encrypted drives

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

Accessing the user account and role settings




From the **Settings** menu at the top of the console, click **Users** in the side menu. There are two sections associated with the management of roles and user accounts:

- **Users:** Create new user accounts and assign a role to them.
- **Roles:** Create and edit settings profiles for accessing Panda Endpoint Protection resources.

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

Creating and configuring user accounts


Creating, editing, and deleting users

- Select the **Settings** menu at the top of the console. Click **Users** from the side menu.
- Click the **Users** tab. There, you can take all necessary actions to create and edit user accounts:
 - **Add a new user account:** Click **Add** to add a new user, set the email account for accessing the console, the role to which it belongs, and a description of the account. After this is completed, the system sends an email to the account to generate the login password.
 - **Edit a user account:** Click the name of the user. A page opens with all the account details that can be edited.
 - **Delete or disable a user account:** Click the  icon of a user account to delete it. Click a user account and click the **Block this user** button to temporarily block access to the web console from the account. If the account is currently logged in, it is logged out immediately. Also, email alerts are no longer sent to the email addresses configured in the account's settings.
 - **Organize and search in the list of users:** Click the  icon to arrange the list of users in ascending/descending order, by name or by date of creation. To search for a user, type in the search box and click .

Exporting users

Follow these steps to export the list of users:

- Select the **Settings** menu at the top of the console. A list appears with all created settings profiles.

- Select **Users** from the side menu. A list appears with all created users.
- Click the  icon. A CSV file is downloaded with the list data.

Fields displayed in the exported file

Field	Definition	Values
Client	Customer account the service belongs to	Character string
Name	User profile name	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-step verification	This indicates whether or not two-step verification is enabled	Boolean
Blocked	Indicates whether the user account is activated or blocked	Boolean

Fields in the User list exported file

Listing created users



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

Field	Description
Account name	User account name.
Role	Role assigned to the user account.
Email account	Email account assigned to the user.

Field	Description
Padlock	Indicates whether the account has Two-Factor Authentication (2FA) enabled.
Status	Indicates whether the user account is activated or blocked.

Table 5.1: User list

Creating and configuring roles

- From the **Settings** menu at the top of the console, click **Users** from the side menu.
- Click the **Roles** tab. There, you can take all necessary actions to create and edit roles:
 - **Add a new role:** Click **Add** to add a new role. Enter the name of the role, a description (optional), the groups the role will grant permissions on, and configure specific permission settings.
 - **Edit a role:** Click the name of a role. A page opens with all the settings that can be edited.
 - **Copy a role:** Click the  icon. A page opens with a new role with exactly the same settings as the original one.
 - **Delete a role:** Click the  icon of a role to delete it. If the role you are trying to delete has user accounts assigned, the delete action is canceled.

Limitations when creating users and roles

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

- A user account can 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 are 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.

User account activity log

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

on which object.

To access the activity log, click the **Settings** menu at the top of the console. 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.	<ul style="list-style-type: none"> • Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 5.2: Fields in the Sessions list

Fields displayed in the exported file

Field	Description	Values
Date	Date and time that the access took place.	Date
User	User account that accessed the console.	Character string
Activity	Action taken by the account	<ul style="list-style-type: none"> • Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 5.3: Fields in the Sessions exported file

Filter tool

Field	Description	Values
From	Set the start point of the	Date

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

Table 5.4: Filters available in the Sessions list

User actions log

The **User actions** section shows a list of 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 Actions list

Field	Description	Values
Date	The date and time when the action occurred.	Date
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 console object the action was performed on.	See table Item types and actions

Table 5.5: Fields in the Actions log

Fields displayed in the exported file

Field	Description	Values
Date	The date and time when the action occurred.	Date
User	The user account that performed the action.	Character string
Action	The user action completed.	See table Item types and actions

Field	Description	Values
		actions
Item type	The type of console object the action was performed on.	See table Item types and actions
Item	The console object the action was performed on.	See table Item types and actions

Table 5.6: Fields in the Actions log 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
Users	User name.	List of all user accounts created in the management console.

Table 5.7: Filters available in the Actions log

Item types and actions

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

Item type	Action	Item
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.
Apple push certificate	Upload	Name of the certificate imported into the console
Settings - Remote control	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.

Item type	Action	Item
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.
	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 - 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.
Settings - VDI environments	Edit	Name of the settings profile the action was performed on.
Settings - Trusted network	Edit	Name of the settings profile the action was performed on.
Preference for VDI environments	Edit	
Device	Edit name	Name of the device the action was performed on.

Item type	Action	Item
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 'Network settings'	Name of the device the action was performed on.
	Inherit 'Network settings'	Name of the device the action was performed on.
	Assign 'Proxy and language' settings	Name of the device the action was performed on.
	Inherit 'Proxy and language' settings	Name of the device the action was performed on.
	Assign 'Per-computer settings'	Name of the device the action was performed on.
	Inherit 'Per-computer settings'	Name of the device the action was performed on.

Item type	Action	Item
	Assign 'Workstations and servers' settings	Name of the device the action was performed on.
	Inherit 'Workstations and servers' settings	Name of the device the action was performed on.
	Assign 'Android devices' settings	Name of the device the action was performed on.
	Inherit 'Android devices' settings	Name of the device the action was performed on.
	Assign license	Name of the device the action was performed on.
	Unassign license	Name of the device the action was performed on.
	Restart	Name of the device the action was performed on.
	Lock	Name of the device the action was performed on.
	Wipe data	Name of the device the action was performed on.
	Snap the thief	Name of the device the action was performed on.
	Remote alarm	Name of the device the action was performed on.
	Locate	Name of the device the action was performed on.
	Designate as Panda proxy	Name of the computer the action was performed on.

Item type	Action	Item
	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.
	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.

Item type	Action	Item
	Make visible	Name of the unmanaged computer the action was performed on.
	Delete	Name of the unmanaged computer the action was performed on.
	Edit description	Name of the unmanaged computer the action was performed on.
	Install	Name of the unmanaged computer the action was performed on.
Filter	Create	Name of the filter the action was performed on.
	Edit	Name of the filter the action was performed on.
	Delete	Name of the filter the action was performed on.
Group	Create	Name of the group the action was performed on.
	Edit	Name of the group the action was performed on.
	Delete	Name of the group the action was performed on.
	Change parent group	Name of the group the action was performed on.
	Assign 'Network settings'	Name of the group the action was performed on.
	Inherit 'Network settings'	Name of the group the action was performed on.

Item type	Action	Item
	Assign 'Per-computer settings'	Name of the group the action was performed on.
	Inherit 'Per-computer settings'	Name of the group the action was performed on.
	Assign 'Workstations and servers' settings	Name of the group the action was performed on.
	Inherit 'Workstations and servers' settings	Name of the group the action was performed on.
	Assign 'Android devices' settings	Name of the group the action was performed on.
	Inherit 'Android devices' settings	Name of the group the action was performed on.
	Sync group	Name of the group the action was performed on.
	Move computers to their Active Directory path	Name of the group the action was performed on.
Advanced reports	Access	
List	Create	Name of the list the action was performed on.
	Edit	Name of the list the action was performed on.
	Delete	Name of the list the action was performed on.
Patch	Exclude for a specific computer	Name of the patch the action was performed on.
	Exclude for all	Name of the patch the action was

Item type	Action	Item
	computers	performed on.
	Stop excluding for a specific computer	Name of the patch the action was performed on.
	Stop excluding for all computers	Name of the patch the action was performed on.
	Mark as 'Manually downloaded'	Name of the patch the action was performed on.
	Mark as 'Requires manual download'	Name of the patch the action was performed on.
Action to take when a threat is reclassified	Edit	
Email sending option	Edit	
Access permission for the Panda Security team	Edit	
Access permission for resellers	Edit	
Email sending option (reseller)	Edit	
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.

Item type	Action	Item
Task - Security scan	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.
	Task - Patch installation	Create
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.

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

Table 5.8: Item types and actions

System events

This section lists all events that occurred in Panda Endpoint Protection and were not originated by a user account, but by the system itself as a response to the actions listed in [Table 1.4](#).

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	See Table 1.4 :

Field	Description	Values
Type	Type of object the action was performed on.	See Table 1.4 :
Item	Console object the action was performed on.	See Table 1.4 :

Table 5.9: Fields in the System events list

Fields displayed in the exported file

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

Table 5.10: Fields in the System events 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

Table 5.11: Filters available in the System events list

Item types and actions

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

Item type	Action	Item
Computer	Register on server after agent reinstallation	Name of the computer the action was performed on.
Computer	Uninstall agent	Name of the computer the action was performed on.
Scheduled report	Disable automatically	Name of the scheduled report the action was performed on.

Table 5.12: Item types and actions

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 console displays the device to administrators, who can run any necessary actions on it.

Chapter contents

Installation on Windows systems	85
Protection deployment overview	85
Installation requirements	88
Generating the installation package and manual deployment	89
Installing the downloaded package	91
Integrating computers based on their IP address	91
Installation with centralized tools	92
Installation from a gold image	95
Remote installation of the client software	102
Remote installation on discovered computers	102
Computer discovery	103
Deleting and hiding computers	105

Viewing discovered computers	106
Discovered computer details	110
Installation on Linux systems	114
Protection deployment overview	114
Installation requirements	115
Network requirements	115
Other requirements	115
Generating the installation package and manual deployment	116
Installation on Linux platforms	117
Installation on macOS systems	120
Protection deployment overview	120
Installation requirements	121
Network requirements	121
Other requirements	122
Manually deploying the macOS agent	122
Installing the downloaded package	123
Installation on Android systems	124
Protection deployment overview	124
Installation requirements	125
Manually deploying and installing the Android agent	125
Deploying the Android agent using an MDM/EMM solution	127
Installation on iOS systems	128
Protection deployment overview	128
Basic concepts	129
Installation requirements	131
Deploying and installing the iOS agent	131
Deploying and installing the agent on supervised devices	137
Configuring an iOS device in supervised mode without loss of data	145
Managing the Apple ID and digital certificates	148
Checking deployment	152
Uninstalling the software	155
Manual uninstallation	155
Remote uninstallation	157
Remote reinstallation	157

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.

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. On large networks, this task can be sped up using discovery features (see [Computer discovery](#)).
- Verify that you have purchased enough licenses for the unprotected devices (see [Licenses](#) on page 161).



Panda Endpoint Protection 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 277. To assign a settings profile to the computers on your network, see [Manual and automatic assignment of settings profiles](#) on page 249.

The Panda Endpoint Protection 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 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. 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 280). While looking for updates, Panda Endpoint Protection checks the assigned settings profiles once a day. For a list of the third-party security products that Panda Endpoint Protection uninstalls automatically, see <https://www.pandasecurity.com/es/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 version that you want to install:

Trial versions

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

Commercial versions

By default, it is not possible to install a commercial version of Panda Endpoint Protection on a computer with a solution from another vendor other than Panda Security. If there is an uninstaller available for the other vendor's product, it is uninstalled and Panda Endpoint Protection 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 6.1: summarizes how the computer behaves to complete the installation of Panda Endpoint Protection.

Previous product	Panda End-point Protection	Restart
None	Trial or commercial version	NO
Panda Endpoint Protection Legacy, Panda Endpoint Protection Plus Legacy	Commercial version	LIKELY (only if a protection upgrade is required)
Third-party antivirus	Trial	NO (by default, both products will coexist)
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 6.1: 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 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 241.

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 [Remote installation of the client software](#).
- Remote deployment from the management console. See [Remote installation of the client](#)

software.

- Installation using gold image generation. See [Installation from a gold image](#).

Installation requirements



For a complete description of the requirements for each platform, see [Hardware, software, and network requirements](#) on page [481](#).

Requirements by platform

Windows

- **Workstations:** Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 10, and Windows 11.
- **Servers:** Windows 2003 SP2, Windows 2008, Windows Server Core 2008, Windows Small Business Server 2011, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022.
- **Versions with an ARM processor:** Windows 10 Home and Pro. Windows 11 Home and Pro.
- **Free space for installation:** 650 MB.
- **Updated root certificates** to use the Panda Patch Management module and establish real-time communications with the management console. See [Update root certificates](#) on page [488](#).
- **Support for SHA-256 signed drivers:** To keep security software up to date, the workstation or server must support SHA-256 driver signing. For more information about affected operating systems and how to update them, see [Support for SHA-256 driver signing](#) on page [489](#). To find computers that do not support SHA-256 driver signing, see [Filter computers not compatible with SHA-256 signed drivers](#) on page [190](#).

IoT and Windows Embedded Industry

Compatible with Windows XP Embedded and higher.



Windows Embedded systems allow custom installations that could possibly impact the installation and working of Panda Endpoint Protection and some of its modules. After you install Panda Endpoint Protection, we recommend that you verify the different protection modules work correctly.

Network requirements

Panda Endpoint Protection 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 requires access to, see [Access to service URLs](#) on page 496.

Other requirements

Update root certificates

For the product to operate correctly, the root certificates on all protected computers must be kept up to date. If root certificates are not updated, some product features might cease to operate. See [Update root certificates](#) on page 488.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection be synchronized. This synchronization is normally achieved using an NTP server. See [Time synchronization of computers \(NTP\)](#) on page 488.

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.
- Click the Windows icon, both for devices with an x86 or ARM processor. The **Windows** window opens.

The screenshot shows a configuration window titled "Windows" with a close button (X) in the top right. The window contains the following elements:

- A "Back" button in the top left.
- A section "Add computers to this group:" with a radio button selected and a dropdown menu showing "All". A red number "1" is next to the radio button.
- A section "Add computers to their Active Directory path:" with an unselected radio button. A red number "2" is next to the radio button.
- A section "Select the network settings to apply to the computers:" with a radio button selected and a button labeled "Default settings". A red number "3" is next to the radio button.
- A section "Select the network settings to apply to the computers:" with an empty text input field. A red number "4" is next to the input field.
- Two buttons at the bottom: "Send URL by email" and "Download installer". A red number "6" is above the "Send URL by email" button, and a red number "5" is above the "Download installer" button.

Figure 6.1: 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 191):
 - 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 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 259.
 - **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 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 193.

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

- If you select **Select the group based on the computer's IP**, Panda Endpoint Protection 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, it is advisable to install the client software for Windows computers centrally using third-party tools.

Using the command line to install the installation package

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

- **GROUPPATH="group1\group2"**: Path in the group tree where the computer will reside. The 'All' root node is not specified. If the group does not exist, the computer is integrated into the 'All' root node.
- **PRX_SERVER**: Name or IP address of the corporate proxy server.
- **PRX_PORT**: Port of the corporate proxy server.
- **PRX_USER**: User of the corporate proxy server.
- **PRX_PASS**: Password of the corporate proxy server.

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

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="London\AccountingDept"  
PRX_SERVER="CorporateProxy" 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 for Windows, macOS, and Linux automatically using the following components:

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

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

Component features and requirements

These components do not have any specific requirements besides those indicated for Panda Systems Management and Panda Endpoint Protection.

Component size:

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

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

Steps for preparing the installation GPO (Group Policy Object)

1. Download the Panda Endpoint Protection package and share the installer on the network.
 - Place the Panda Endpoint Protection installer in a shared folder accessible to all the computers that are to receive the software.
2. Create a new OU (Organizational Unit) called "Aether deployment".
 - Open the MMC and add the Group Policy Management snap-in.
 - Right-click the domain node. Click **New** and **Organizational Unit** to create a new Organizational Unit called "Aether deployment".
 - Right-click the newly created Organizational Unit and select **Block Inheritance**.

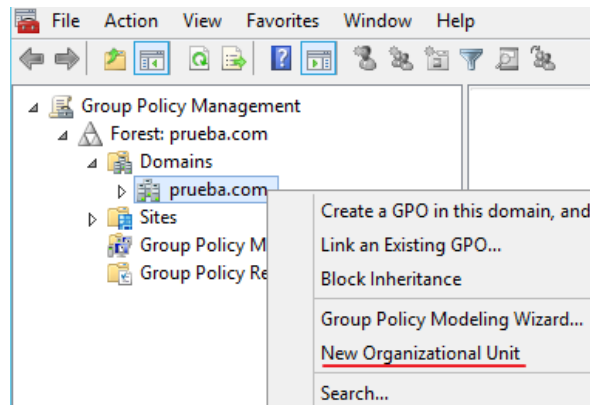


Figure 6.2: New Organizational Unit

3. Create a new GPO with the installation package.

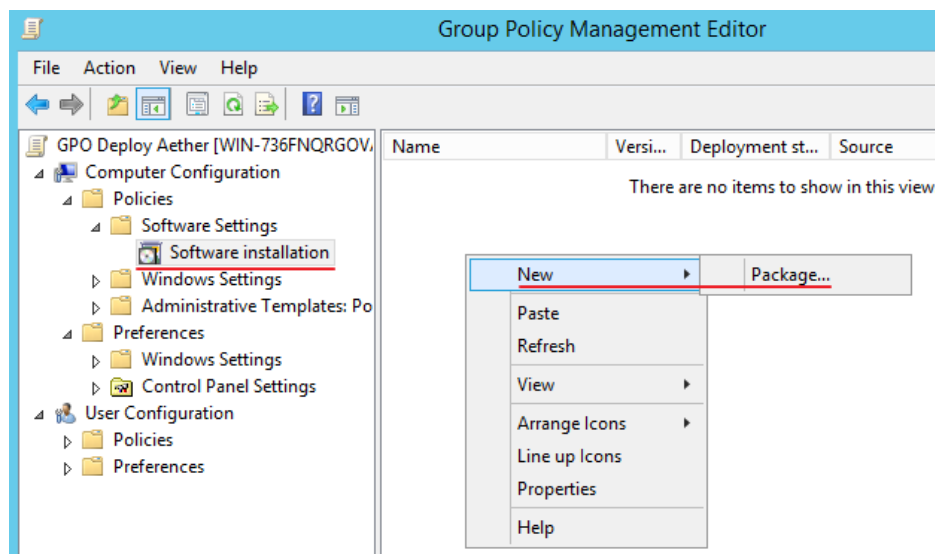


Figure 6.3: New installation package

- Right-click the newly created Organizational Unit. Select the option **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 software to the branch. Click **Computer configuration, Policies, Software Settings, Software installation**.
 - Right-click **Software installation**, and select **New, Package**.
 - Add the Panda Endpoint Protection .msi installation file.
4. Edit the package properties

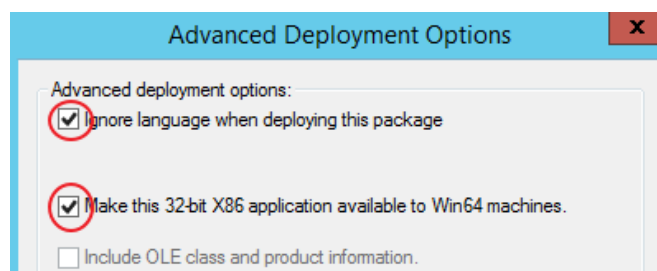


Figure 6.4: Configuring the deployment options

- Right-click the package you have 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 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 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 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 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 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 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 updates to the computer you want to clone.

- To enable or disable agent updates, see [Communications agent updates](#) on page 178.
- To enable or disable protection updates, see [Protection engine updates](#) on page 176.
- To assign settings profiles to computers, see [Managing settings](#) on page 241.
- For more information about groups in Panda Endpoint Protection, see [Group tree](#) on page 191

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 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 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 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 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/es-ES/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 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 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 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 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.

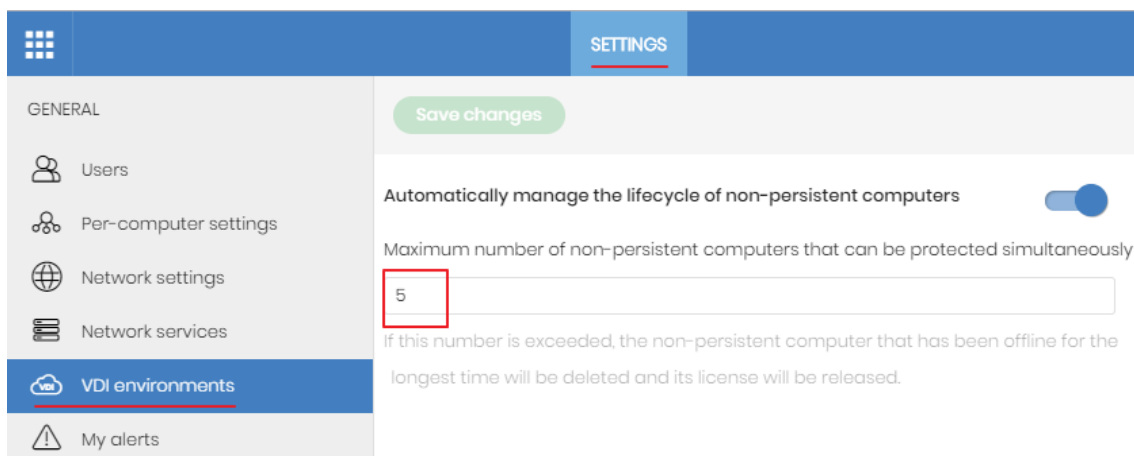


Figure 6.5: Configuring the number of licenses assigned to non-persistent VDI computers

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/es-ES/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 is fully up to date.
- Preload the Panda Endpoint Protection 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 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 a 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 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 console.
- Verify that all persistent computers are included in the list.

Verify the status of Panda Endpoint Protection 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.

Remote installation of the client software

All products based on Aether Platform include tools to find unmanaged computers and devices on the network and to open a remote installation session from the management console.



Remote installation is only compatible with Windows platforms.

Operating system and network requirements

To install Panda Endpoint Protection remotely, the target computers must 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 queries must be allowed.
- 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.



Turn on network discovery and file and printer sharing. Go to Control Panel > Network and Internet > Network and Sharing Center > Change advanced sharing settings and select Turn on network discovery and Turn on file and printer sharing.

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

Remote installation on discovered computers

To remotely install the Panda Endpoint Protection software on one or more unmanaged computers:

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 link **xx computers have been discovered that are not being managed by Panda Endpoint Protection**.
 - Go to the **Computers** menu at the top of the console. Click **Add computers**. Select **Discovery and remote installation**. A wizard opens. Click the **View unmanaged computers discovered** link.
- From 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.

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](#).

Computer discovery

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

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

Assigning the role of discovery computer to a computer on your network

- Make sure the computer that you want to designate as the discovery computer has Panda Endpoint Protection 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:

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

Table 6.2: Information displayed for each discovery computer

Limiting the discovery scope



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

To restrict the scope of the discovery of network computers:

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select a discovery computer and click **Configure**.
- Select one of the following options in the **Discovery scope** section:
 - **Search across the entire network**: The discovery computer uses the network mask configured on the interface to scan its subnet for unmanaged computers. The search is performed only on ranges of private IP addresses.
 - **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.

Scheduling computer discovery tasks

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

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select a discovery computer and 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 Panda Endpoint Protection server time.
- Click **Save**. The discovery computer shows a summary of the scheduled task in its description.

Discovering computers on demand

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

Deleting and hiding computers

Deleting computers

Panda Endpoint Protection does not remove computers that are no longer accessible because they were removed from the network from the **Unmanaged computers discovered** list.

You must manually delete them from the list:

- In **Unmanaged computers discovered**, 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, click the general context menu above the table, and select **Delete**.
 - To delete a single computer, click the computer's context menu at the end of the computer row, and select **Delete**.



If you delete an unmanaged computer in the console and do not uninstall the Panda Endpoint Protection software or remove it physically from the network, it appears again 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, you can hide computers from the installation:

- In **Unmanaged computers discovered**, 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, click the general context menu above the table, and select **Hide and do not discover again**.
- To hide a single computer, click the computer's context menu and select **Hide and do not discover again**.



Viewing discovered 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 dashboard. Find 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**. 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 installed, and those computers where the protection is not working adequately, 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.	<ul style="list-style-type: none"> — 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. See Computer notifications section (2) on page 220 for a description of error messages. If the cause of the error is unknown, the associated error code is displayed.
IP address	The computer's primary IP address.	Character string
NIC manufacturer	Manufacturer of the discovery computer network interface card.	Character string
Last discovery computer	Name of the discovery computer that last found the unmanaged workstation or server.	Character string
Last seen	Date when the	Date

Field	Description	Values
	computer was last discovered.	

Table 6.3: Fields in the Unmanaged computers discovered list

If the **Status** field shows the text **Installation error** and the cause of the error is known, a text string is added with a description of the error. For a list of the installation errors reported by Panda Endpoint Protection, see [Computer notifications section \(2\)](#) on page 220.

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
First seen	Date when the computer was first discovered.	Character string
First seen by	Name of the discovery computer that first found the workstation/server.	Character string

Field	Description	Values
Last seen	Date when the computer was last discovered.	Date
Last seen by	Name of the discovery computer that last found the user's computer.	Character string
Description	Description of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	<ul style="list-style-type: none"> • 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. See Computer notifications section (2) on page 220 for a description of error messages.
Error	Error description.	See Computer notifications section (2) on page 220 .
Installation error date	Date and time when the error took place.	Date

Table 6.4: Fields in the Unmanaged computers list exported file

Filter tool

Field	Description	Values
Search	Search by computer name, IP address, NIC manufacturer, or discovery computer.	Character string
Status	Panda Endpoint Protection	<ul style="list-style-type: none"> • Unmanaged: The computer is eligible

Field	Description	Values
	installation status.	<p>for installation, but the installation process has not started yet.</p> <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Last 24 hours • Last 7 days • Last month

Table 6.5: 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. See [Computer details](#) on page 217.

Discovered computer details

From 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 computers that last found the computer.

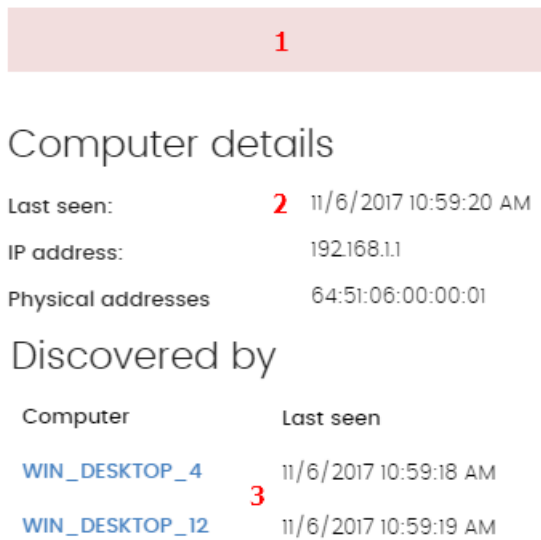


Figure 6.6: Discovered computer details

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.

Status	Type	Recommended action
	Unable to register the agent	Make sure the computer is turned on and meets the remote installation requirements.
Error installing the Panda Endpoint Protection protection	This message indicates the reason for the protection installation failure.	
	Insufficient disk space to perform the installation	See Hardware requirements on page 487 to see the free space required for installing Panda Endpoint Protection.
	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	See Supported uninstallers for a list of the third-party solutions that Panda Security can uninstall.
	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 no longer appears 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 and meets the	

Status	Type	Recommended action
		requirements specified in Hardware, software, and network requirements on page 481

Table 6.6: Information in the Computer alerts section

Computer details (2)

Field	Description
Computer name	Name of the discovered computer.
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.
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 6.7: 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.

Table 6.8: Last discovery computer

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

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. Verify that you have purchased enough licenses for the unprotected computers. See [Licenses](#) on page 161.



Panda Endpoint Protection 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.

Determine computer default settings

When the software is installed on the computer or device, Panda Endpoint Protection 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 241.

Installation requirements



For a complete description of the requirements for each platform, see [Hardware, software, and network requirements](#) on page 481.

- **64-bit operating systems:** Ubuntu 14.04 LTS and higher, Fedora 23 and higher, Debian 8 and higher, Red Hat 6.0 and higher, CentOS 6.0 and higher, Linux Mint 18 and higher, SUSE Linux Enterprise 11.2 and higher, Oracle Linux 6 and higher. No window manager required. Use the `/usr/local/protection-agent/bin/pa_cmd` tool from the command line.
- **32-bit operating systems:** Red Hat 6.0 to Red Hat 6.10 and CentOS 6.0 to CentOS 6.10.



For information about the last Linux kernel version supported, see <https://www.pandasecurity.com/spain/support/card?id=700009>.

- **Free space for installation:** 500 MB.
- **Ports:** 3127, 3128, 3129, and 8310 must be open for the web malware detection feature to work. On computers with no graphical environment installed, the web detection feature is disabled.

To install Panda Endpoint Protection on Linux platforms, the target computer must remain connected to the Internet during the installation process. The installer connects to the appropriate repositories based on the system (RPM or DEB), and the packages required to finish the installation successfully download. To install Panda Endpoint Protection on Linux platforms isolated from the network, see [Installation on Linux platforms without an Internet connection \(without dependencies\)](#).

Network requirements

Panda Endpoint Protection 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 requires access to, see [Access to service URLs](#) on page 496.

Other requirements

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection be synchronized. This synchronization is normally achieved using an NTP server. See [Time synchronization of computers \(NTP\)](#) on page 488.

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

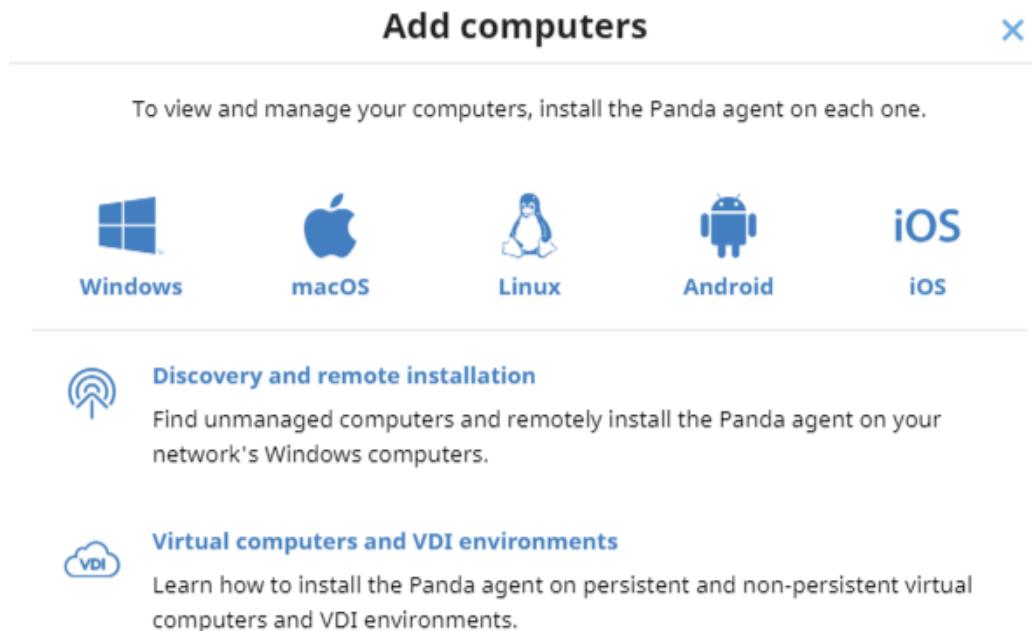


Figure 6.7: Window for selecting a platform supported by Panda Endpoint Protection

- 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 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 259.
- 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 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**.

Installation on Linux platforms

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

- Installation on Linux platforms with an Internet connection
- Installation on Linux platforms with Secure Boot
- Installation on Linux platforms without an Internet connection (without dependencies)

Installation on Linux platforms with an Internet connection

Make sure you have administrator permissions on the device and that the downloaded package has execute permissions. The installer searches the target computer for the libraries it needs. If it cannot find the libraries there, 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-- --no-deps"
```

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

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

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

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

- Make sure this directory was created:

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

Installation on Linux platforms with Secure Boot

Some Linux distributions detect when a computer has Secure Boot enabled. With Secure Boot enabled, the protection 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. `openssl`, `keyutils`, `mokutil`, `pesign`, `kernel-uek-devel-$(uname -r)` packages.

Enabling the protection software on computers with Secure Boot enabled

To enable the protection software, follow this procedure directly on the computer in order to interact with its boot system:

- Check the state of Secure Boot:

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

If Secure Boot is enabled on the computer, the message `Secure Boot enabled` is displayed.

- Verify that the protection driver is not loaded:

```
$ lsmod | grep prot
```

- Update the protection repository:

```
$ sudo /usr/local/management-agent/repositories/pa/install  
--addrepo=https://repository.pandasecurity.com/aether/installers/  
protection/linux/3.01.00.0001
```

- Upgrade the protection driver. For distributions other than SUSE, use this command:

```
$ sudo /usr/local/management-agent/repositories/pa/install --install  
--kernel-only
```

- Upgrade the protection driver. For SUSE, use this command:

```
$ sudo zypper up protection-agent-kmp-default
```

- 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 8-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 the Panda Security protection. Select **Continue** to continue the registration process.
 - When prompted to **Enroll the key**, select **Yes**.
 - Enter the password created previously. 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, complete these steps after you complete the steps to register the certificate:

- Run this command:

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

This 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 already signed  
Kernel module successfully loaded
```

Installation on Linux platforms without an Internet connection (without dependencies)

Workstations and servers without direct access to the Internet or access through a Panda Security or corporate proxy and with out-of-date Linux distributions installed must use the Panda Endpoint Protection full installation package. This package includes all the libraries required for the agent to work. This installation method is recommended only when the target computer is truly isolated from the Internet, because if security failures are detected in the third-party libraries included in the installation package, they are not automatically updated.

The full installer is compatible with these distributions:

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

The full 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 full 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 previous repository settings are kept.

To install the Panda Endpoint Protection 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

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. Verify that you have purchased enough licenses for the unprotected devices. See [Licenses](#) on page 161.



Panda Endpoint Protection 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.

Determine device default settings

When the software is installed on the computer or device, Panda Endpoint Protection 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 241.

Installation requirements



For a complete description of the requirements for each platform, see [Hardware, software, and network requirements](#) on page 481

- **Operating systems:** macOS 10.10 Yosemite and higher.
- **Free space for installation:** 400 MB.
- **Ports:** 3127, 3128, 3129, and 8310 must be accessible for the web anti-malware to work.

Network requirements

Panda Endpoint Protection 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 requires access

to, see [Access to service URLs](#) on page 496.

Other requirements

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Panda Endpoint Protection be synchronized. This synchronization is normally achieved using an NTP server. See [Time synchronization of computers \(NTP\)](#) on page 488.

Required permissions

For the protection to operate correctly, you must:

- Enable network extensions.
- Enable system extensions.
- Enable full disk access.

For more information, see [Requirements for macOS platforms](#) on page 490.

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

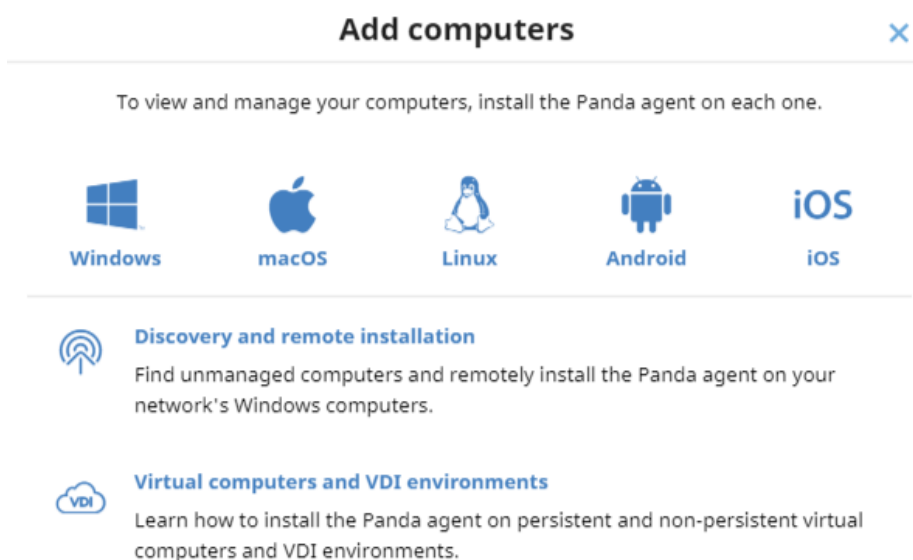


Figure 6.8: Window for selecting a platform supported by Panda Endpoint Protection

- 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 259.
- 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-gent.app/Contents /*/Library/  
ApplicationSupport/ManagementAgent/
```



To install the product agent on devices with macOS Catalina, you must assign specific permissions. For more information, see:

<https://www.pandasecurity.com/es/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 (Mobile 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.
- Determine device default settings. See [Managing settings](#) on page [241](#).
- 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. Verify that you have purchased enough licenses for the unprotected devices. See [Licenses](#) on page [161](#).



Panda Endpoint Protection 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 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 241.

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](#) on page 125.
- Deployment using a third-party MDM/EMM solution. See [Deploying the Android agent using an MDM/EMM solution](#) on page 127.

Installation requirements

Supported devices

- **Operating systems:** Android 5.0 or higher.
- **Free space for installation:** 10 MB (based on the device model, it is possible that more free space is required).

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

For all Panda Endpoint Protection features to work correctly on the smartphone, the device user must grant all permissions requested by the app. For a complete list of the required permissions, see [Permissions required on the device](#) on page 494.

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

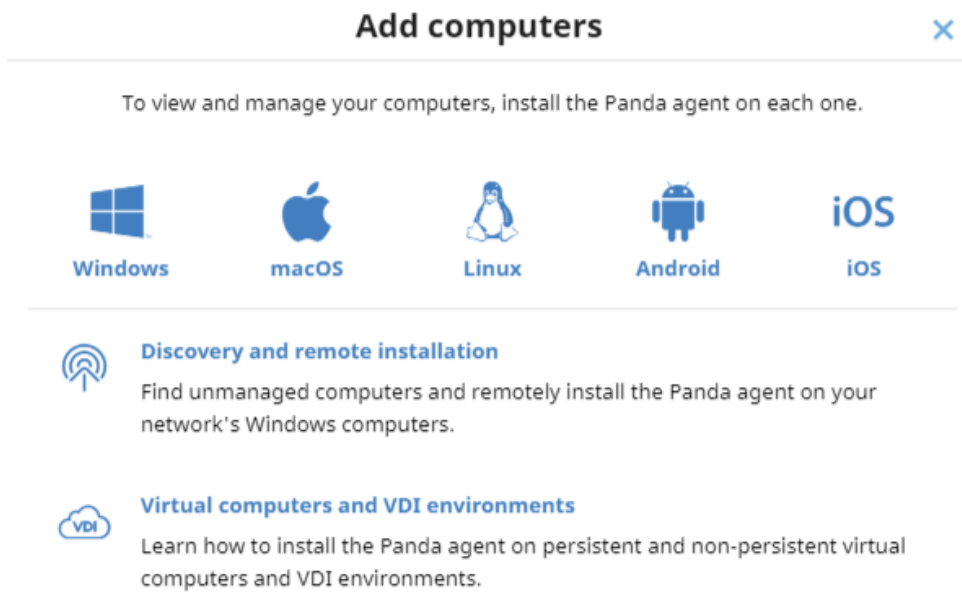


Figure 6.9: Window for selecting a platform supported by Panda Endpoint Protection

- 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 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 494.
- Regardless of whether the permissions are granted or not, the installation process completes and the device appears in the Panda Endpoint Protection 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.
- 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/EMM solution, enter the integration URL and the name with which the integrated device will be displayed in the Panda Endpoint Protection console.
 - **Automatic name:** Panda Endpoint Protection assigns the name it will use to identify the device in the console.
 - **Manual name:** The MDM/EMM solution administrator chooses the name that will be used to identify the device in the Panda Endpoint Protection console. Use wildcards and other special characters based on the specifications of the MDM/EMM solution you use.
 - **Undefined:** The device user assigns the device name the first time they run the app.
- The first time the app is launched on the mobile device, the **Enter alias** screen opens.
- If the device name has not been previously specified, enter the name that will be used to identify the device in the Panda Endpoint Protection console. 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 494.
- Regardless of whether the permissions are granted or not, the installation process completes and the device appears in the Panda Endpoint Protection 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.
- 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 [Determine device default settings](#).

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. Verify that you have purchased enough licenses for the unprotected devices. See [Licenses](#) on page 161.



Panda Endpoint Protection 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 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 241.

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 iOS agent](#).
- 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, 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 (Mobile Device 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.

Panda MDM

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 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.



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](#).

Enrollment types supported by Panda Endpoint Protection

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

Enrollment type	Features available in the Panda Endpoint Protection console
<p>Installation on iOS devices enrolled into the Panda (recommended if you did not already use an MDM solution)</p>	<ul style="list-style-type: none"> • Hardware inventory • Software inventory • Web protection * • Web filtering * • Geolocation • Remote alarm • Wipe data • Lock
<p>Installation on iOS devices enrolled into a third-party MDM solution (recommended if you already used an MDM solution)</p>	<ul style="list-style-type: none"> • Hardware inventory • Web protection * • Web filtering * • Geolocation • Remote alarm
<p>Installation on iOS devices not enrolled into an MDM solution</p>	<ul style="list-style-type: none"> • Hardware inventory • Geolocation • Remote alarm

Enrollment types supported by Panda Endpoint Protection

* 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 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

Supported iOS versions

- iOS 13 / iPadOS 13
- iOS 14 / iPadOS 14
- iOS 15 / iPadOS 15

Hardware requirements

At least 12 MB of internal memory is required on the target device.

Network requirements

The app installed on the mobile device uses the Apple Push Notification Service (APNs) to communicate with Panda Endpoint Protection. In normal conditions, if the target device is connected to the cellular network (2G/3G/4G or higher), it is not necessary to meet any specific network requirements. For other scenarios, see [Requirements for iOS platforms](#).

Permissions required on the device

For all Panda Endpoint Protection features to work correctly on the smartphone, the device user must grant all permissions requested by the app. For a complete list of the required permissions, see [Permissions required on the device](#).

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.

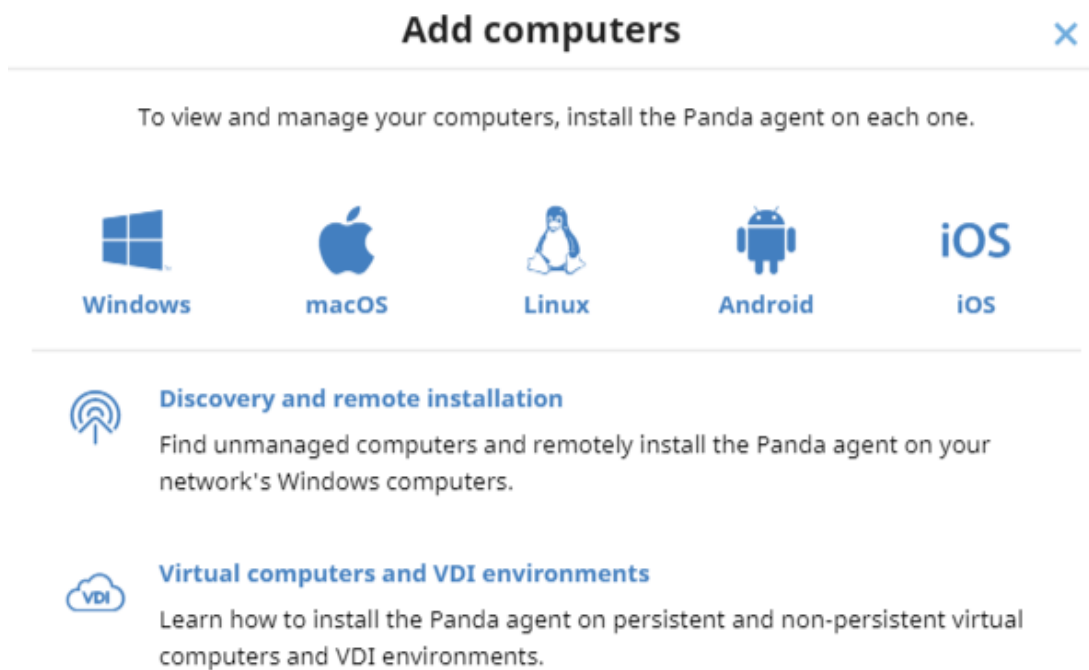


Figure 6.10: Window for selecting a platform supported by Panda Endpoint Protection

- 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.
 - 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 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 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 management console. To generate a certificate, see [Creating and importing the digital certificate into the Panda Endpoint Protection 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](#).
- Select the **Computers** menu at the top of the Panda Endpoint Protection management console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection.
- Click the **iOS** icon. A window opens with information about the previously uploaded certificate.

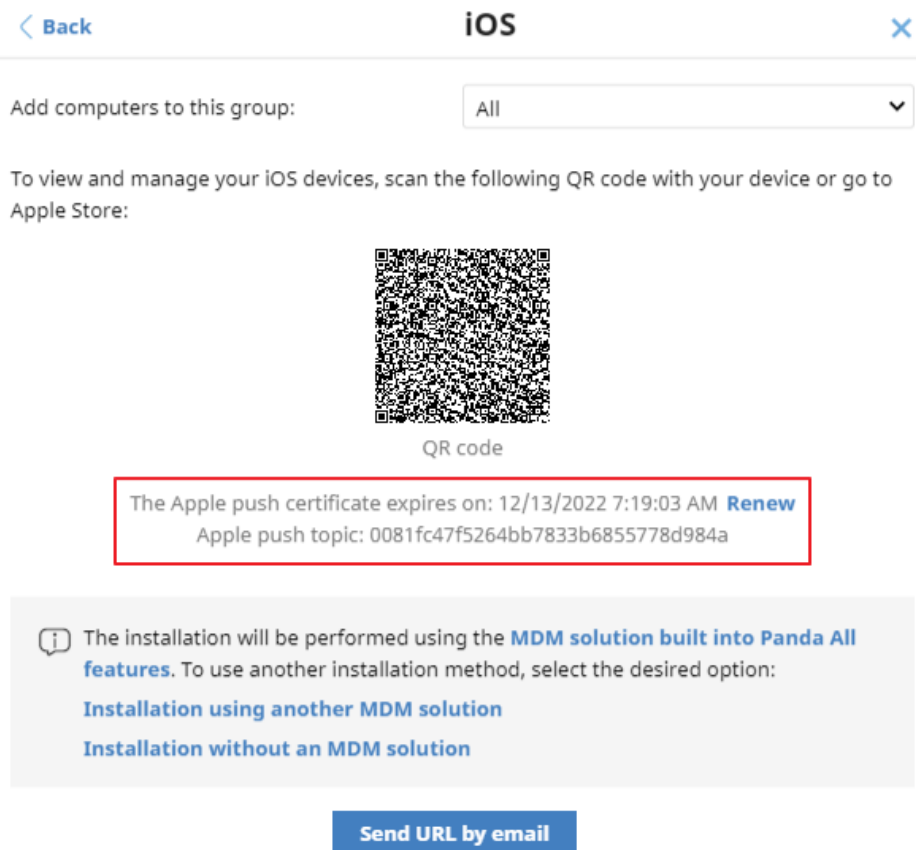


Figure 6.11: Window with the uploaded Apple digital certificate

- 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 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 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.
- 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.

[← Back](#) **iOS - Another MDM solution** [×](#)

Add computers to this group: ▼

To install and manage iOS devices, download, distribute, and install the following profile to enable web access control on your devices (works only on supervised devices). [Download](#)

Next, find our app in your MDM solution:

iTunes Store Id:	1606209387
Bundle Id:	com.watchguard.corporate
App Name:	WatchGuard Mobile Security

Enter the following attributes in your MDM solution:

x_wg_device_name:	Device name variable in your MDM solution
x_wg_is_supervised:	Optional. A variable in your MDM solution that indicates the device is supervised. ⓘ
x_wg_integration_url:	https://b67ur.app.goo.gl/?link=https%3a%2f%2faetherdev.pandasecurity.com%2fapi%2fv1%2faccounts%2f1e296166-ce3b-43db-936e-c03ed2c6fc35%2fsites%2f5a7e34c5-38d1-4b11-aebc-27a74479f058%2finstallerdownload%3finstallerType%3d2%26platform%3d5%26customGroupId%3d659dfb5f-f5eb-4b8e-837f-cd6e624b4cdc%26sToken%3dbe586b1a7bb04b613a8cbf67a0d1c07d37898a25b24d517b9e1435e500af72db&ibi=com.watchguard.corporate&ipbi=com.watchguard.corporate&isi=1606209387&ius=customscheme&efr=1

Figure 6.12: 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 6.12](#), 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 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 administrator. Copy the content of the **x_wg_integration_url**

attribute shown in the Panda Endpoint Protection 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 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 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 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.



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/es/app/apple-configurator-2/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 MDM solution enrollment URL

- Verify you have a valid Apple certificate uploaded to the Panda Endpoint Protection management console. To generate a certificate, see [Creating and importing the digital certificate into the Panda Endpoint Protection 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](#) on page 129 and [Enrollment types supported by Panda Endpoint Protection](#) on page 130.
- Select the **Computers** menu at the top of the Panda Endpoint Protection management console. Click the **Add computers** button. A window opens with the platforms supported by Panda Endpoint Protection.
- Click the **iOS** icon. The **iOS** window opens with information about the previously uploaded certificate.

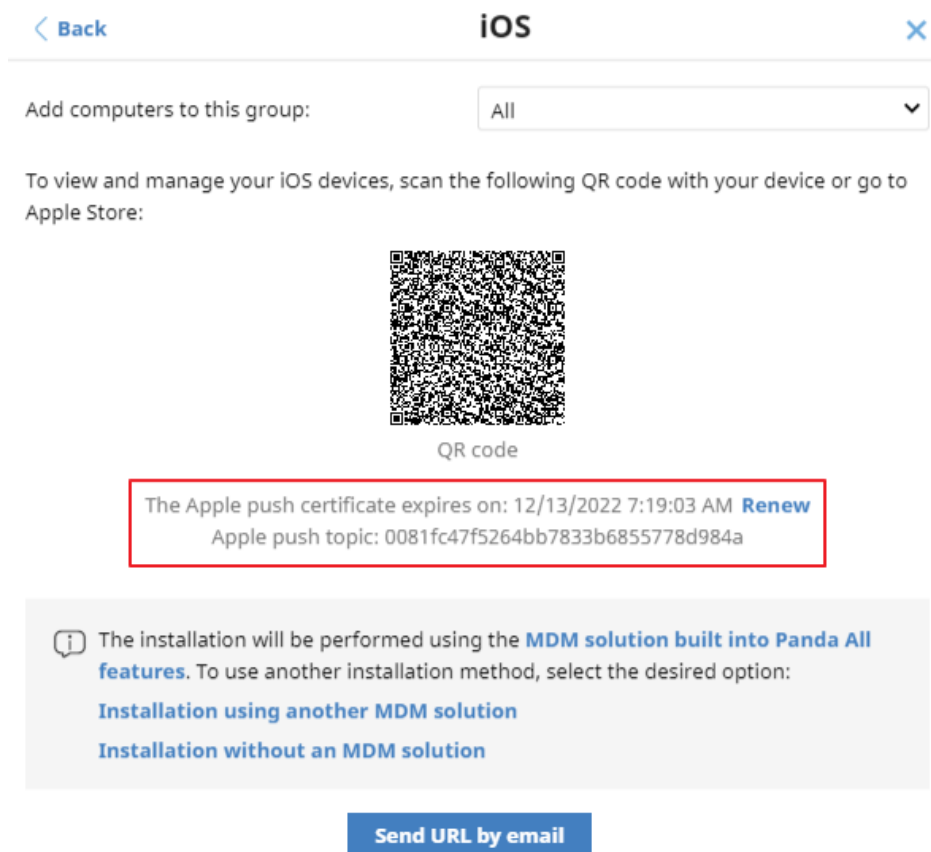


Figure 6.13: Window with the uploaded Apple digital certificate

- 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 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 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 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.
- 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.

[Back](#) **iOS - Another MDM solution** ✕

Add computers to this group:

To install and manage iOS devices, download, distribute, and install the following profile to enable web access control on your devices (works only on supervised devices). [Download](#)

Next, find our app in your MDM solution:

iTunes Store Id:	1606209387
Bundle Id:	com.watchguard.corporate
App Name:	WatchGuard Mobile Security

Enter the following attributes in your MDM solution:

x_wg_device_name:	Device name variable in your MDM solution
x_wg_is_supervised:	Optional. A variable in your MDM solution that indicates the device is supervised. ⓘ
x_wg_integration_url:	https://b67ur.app.goo.gl/?link=https%3a%2f%2faetherdev.pandasecurity.com%2fapi%2fv1%2faccounts%2f1e296166-ce3b-43db-936e-c03ed2c6fc35%2fsites%2f5a7e34c5-38d1-4b11-aebc-27a74479f058%2finstallerdownload%3finstallerType%3d2%26platform%3d5%26customGroupId%3d659dfb5f-f5eb-4b8e-837f-cd6e624b4cdc%26sToken%3dbe586b1a7bb04b613a8cbf67a0d1c07d37898a25b24d517b9e1435e500af72db&ibi=com.watchguard.corporate&ipbi=com.watchguard.corporate&isi=1606209387&ius=customscheme&efr=1

Figure 6.14: 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 6.14](#), 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 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 administrator. Copy the content of the **x_wg_integration_url** attribute shown in the Panda Endpoint Protection 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 console.

- Push the **WatchGuard Mobile Security** app from the MDM solution to the devices that you want to protect. After a few minutes, 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 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 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 console

To integrate iOS devices into Panda Endpoint Protection 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.
- Click the **iOS** icon. If no certificate has been previously imported, a window opens with the procedure for creating a valid certificate.

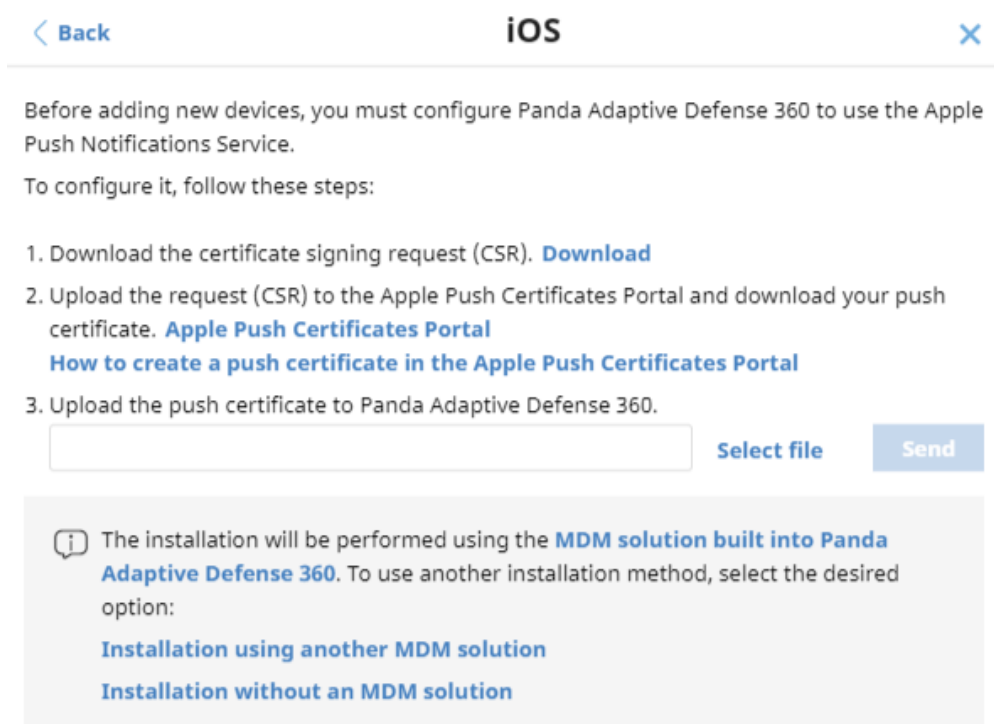


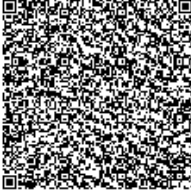
Figure 6.15: Window detailing the procedure for creating and importing an Apple digital certificate

- 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 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 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.

< Back iOS X

Add computers to this group:

To view and manage your iOS devices, scan the following QR code with your device or go to Apple Store:



QR code

The Apple push certificate expires on: 12/13/2022 7:19:03 AM [Renew](#)
 Apple push topic: 0081fc47f5264bb7833b6855778d984a

i The installation will be performed using the **MDM solution built into Panda All features**. To use another installation method, select the desired option:
[Installation using another MDM solution](#)
[Installation without an MDM solution](#)

[Send URL by email](#)

Figure 6.16: 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 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 6.17: 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 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 management console. Click the **Add computers** button. A window opens with all platforms supported by Panda Endpoint Protection.
- 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 management console. See [Creating and importing the digital certificate into the Panda Endpoint Protection 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.
- 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.

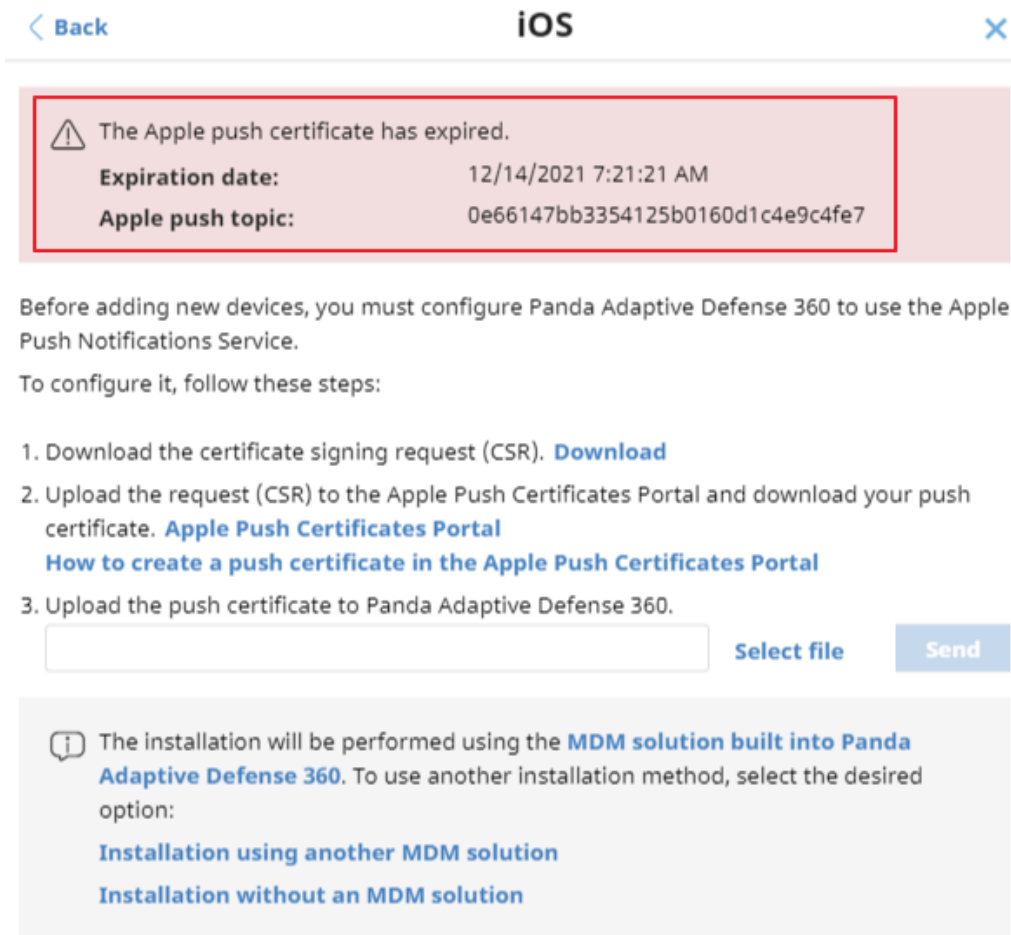


Figure 6.18: Window with information about an expired digital certificate

Checking deployment

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

- Using the **Protection status** widget. See [Protection status](#) on page [400](#) for more information.
- Using the **Computer protection status** list. See [Computer protection status](#) on page [409](#) 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 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	Warning	Uninstallation (4)	401

Message	Level	Category	ID
parameters %parameters%			
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 6.9: Agent installation result codes in the Event Viewer

Uninstalling the software

You can uninstall the Panda Endpoint Protection software manually from the control panel of the operating system on each computer, or remotely from the **Computers** menu or from the **Computer protection status** and **Licenses** lists.

Manual uninstallation

End users can manually uninstall the solution, if the administrator has not configured an uninstallation password in the security settings profile applied to their 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 [Password-protection of the agent](#) on page 272.

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

- **Windows and macOS computers:** Agent and protection.
- **Linux computers:** Agent, protection, and kernel module.
- **Android devices:** Protection.
- **iOS devices:** Protection and MDM profile if the device is managed by an MDM solution.

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

On Windows 8 or higher:

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

On Windows Vista, Windows 7, Windows Server 2003, and higher

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

On Windows XP

- Control Panel > Add or remove programs.

On a macOS device

- Open the Command Menu from: 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 checkbox. Tap Disable > OK.
- In Settings, tap Apps. Tap Panda Endpoint Protection > Uninstall > OK.

On an iOS device not enrolled into an MDM solution

- Tap and hold the WatchGuard Mobile Security app on the Home screen. All the apps on the device start jiggling and the icon "-" appears on all of them.
- Tap the "-" icon in the upper-left corner of 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 uninstalled from the mobile device.

On an iOS device enrolled into the Panda MDM solution

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

On an iOS device enrolled into a third-party MDM solution

Unlike with devices enrolled into the Panda MDM solution, in this case we recommend that you uninstall the WatchGuard Mobile Security app using the third-party MDM solution from which it is managed. If you delete the management profile manually from the smartphone, all the software that was installed using the MDM solution is also lost, and the device can no longer be centrally managed from the MDM solution.

On Linux

Open a command line. Enter these commands:

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

Manual uninstallation result

When you uninstall the Panda Endpoint Protection software (Panda agent and protection) from a computer, all data associated with the computer disappears from the management console: all counters, entries in reports, and details of the computer's activity.

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

Remote uninstallation

To remotely uninstall the Panda Endpoint Protection software on a Windows computer:

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



Remote uninstallation is only supported on Windows platforms. On Linux and macOS platforms, the affected computer is removed from the management console and all of its counters, but it reappears in the next discovery task.

Remote reinstallation

To resolve a situation when Panda Endpoint Protection 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.

- Local admin or domain admin account credentials.

Accessing the feature

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

- [Computer protection status](#) on page [409](#).
- [Patch management status](#) on page [330](#).
- [Encryption status](#) on page [385](#).
- [Licenses module lists](#) on page [168](#).
- [Hardware](#) on page [208](#).

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





The **Reinstall protection (requires restart)** and **Reinstall agent** options are only displayed for computers supporting this feature.



Identifying computers whose software needs reinstalling

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's context menu, click **Reinstall protection (requires restart)**  or **Reinstall agent** . A window opens where you can configure the reinstallation options. See [Reinstall protection selection window](#) and [Reinstall agent selection window](#).

Reinstalling the software on multiple computers

- Use the checkboxes to select the computers that need to have the protection or the agent reinstalled.
- From the toolbar, click **Reinstall protection (requires restart)**  or **Reinstall agent** . A window opens where you can configure the reinstallation options. See [Reinstall protection selection window](#) and [Reinstall agent selection window](#).

Reinstall protection selection window

When you choose to reinstall a computer's protection, a window is displayed with the following 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 waiting period expires, the protection is uninstalled, and the computer restarts automatically in order to reinstall the protection.

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

Reinstall agent selection window

When you choose to reinstall a computer's agent, a window is displayed prompting you to enter the following 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 the following actions:

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

Error codes

To get a list of the error messages and corrective actions, see [Protection software reinstallation errors](#) on page [224](#).

Chapter 7

Licenses

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

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

Chapter contents

Definitions and basic concepts	162
License contracts	162
Computer status	162
License status and groups	163
Types of licenses	163
Assigning licenses	163
Releasing licenses	164
Processes associated with license assignment	164
Case 1: Computers with assigned licenses and excluded computers	164
Case 2: Computers without an assigned license	165
Licenses module panels/widgets	166
Licenses module lists	168
Expired licenses	172
Expiration notifications	172
Withdrawal of expired licenses	172
Adding trial licenses to commercial licenses	172
Computer search based on license status	173

Definitions and basic concepts

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



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

License contracts

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

- **Product type**: Panda Endpoint Protection, Panda Full Encryption, 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:

- **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, 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 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.




See [Managing computers and devices](#) on page **181** for more information about the search tool, the folder tree, and the filter tree.

Automatic assignment of licenses

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

Manual assignment of licenses

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

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

Releasing licenses

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


Automatic release

- When the Panda Endpoint Protection software is uninstalled from a computer on the network, the system automatically recovers a license and returns it to the group of licenses available for use.
- Similarly, when a license contract expires, licenses are automatically released from computers in accordance with the process explained in section [Withdrawal of expired licenses](#).

Manual release

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

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

- Go to the **Computers** menu at the top of the console. Find the device whose license you want to release. You can use the folder tree, the filter tree, or the search tool.
- Click the computer to open its details page.
- Go to the **Details** tab. The **Licenses** section displays 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 integrated into the Aether platform is assigned a Panda Endpoint Protection product license automatically, and as such acquires the status of **Computer with an**

assigned license. 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

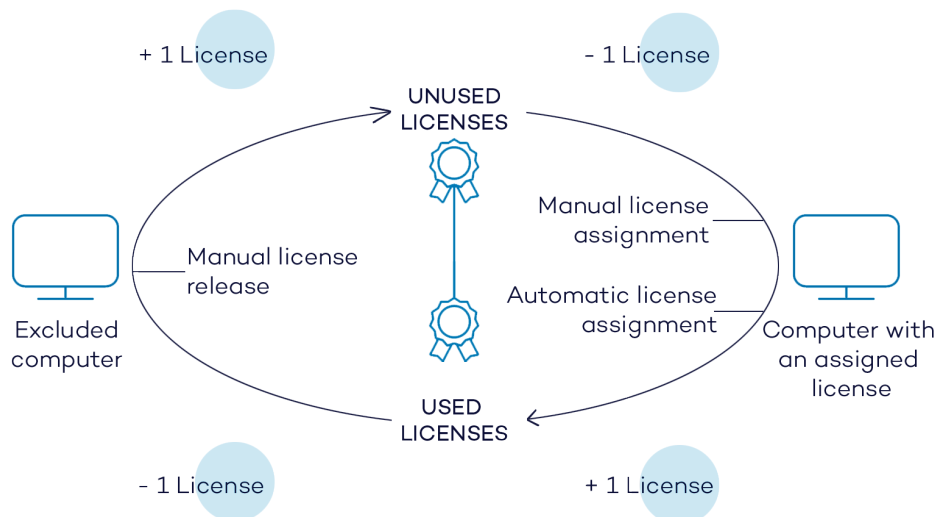


Figure 7.1: Modification of license groups with computers with licenses assigned and excluded computers

Case 2: Computers without an assigned license

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

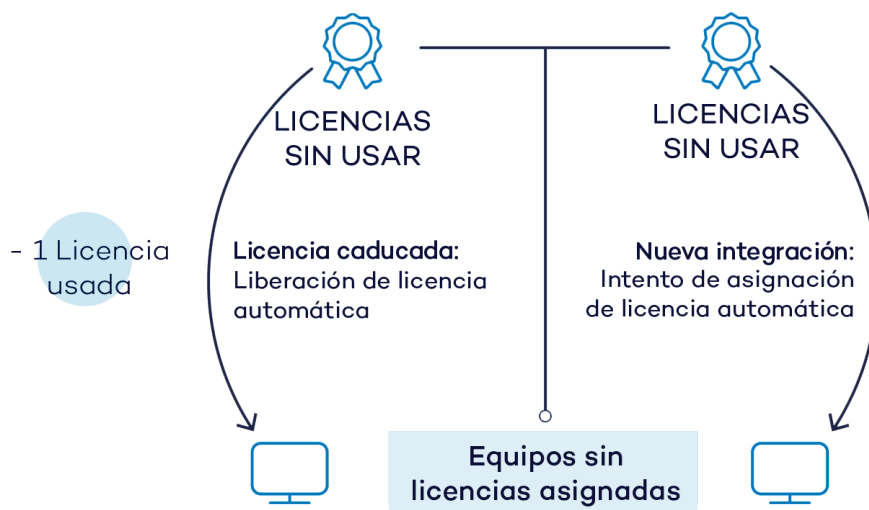


Figure 7.2: Computers without an assigned license due to expiration of the license contract and because the group of unused licenses was empty at the time of integration

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

Licenses module panels/widgets

Accessing the dashboard

To access the dashboard, click the **Status** menu at the top of the console. 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.

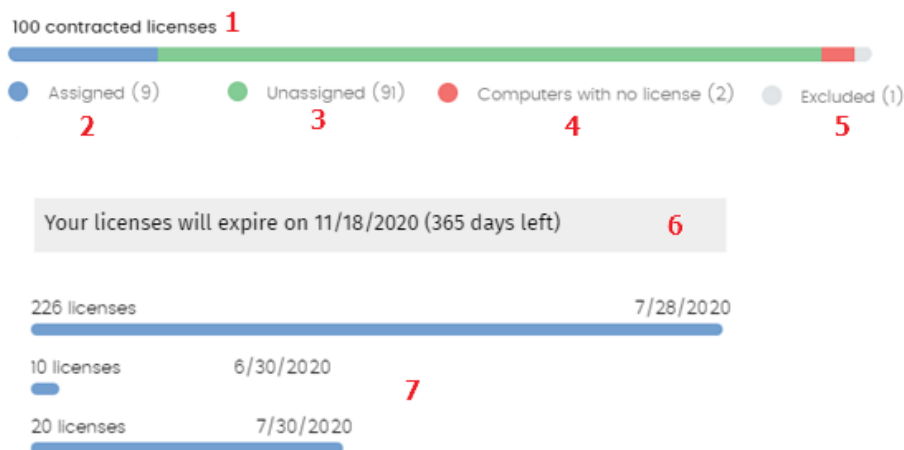


Figure 7.3: License panel with three license contracts

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	Number of computers protected with an assigned license.

Hotspot	Description
assigned licenses (2)	
Number of unassigned licenses (3)	Number of licenses contracted that have not been assigned to any computer and are therefore not being used.
Number of computers without a license (4)	Computers that are not protected as there are insufficient licenses. Licenses 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 7.1: Description of the data displayed in the Licenses panel

Lists accessible from the panel

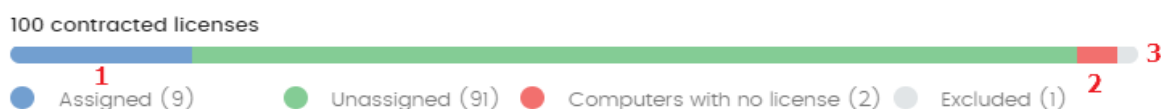


Figure 7.4: Hotspots in the Contracted licenses panel

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

Filter field	Value
(1) License status	Assigned

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

Table 7.2: 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 folder tree the computer belongs to.	Character string
License status	The computer's license status.	<ul style="list-style-type: none"> •  Assigned •  Computer without a license


Field	Description	Values
		<ul style="list-style-type: none">  Excluded
Last connection	Date when the computer status was last sent to the Panda Security cloud.	Date

Table 7.3: Fields in the Licenses list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account that the product belongs to.	Character string
Computer type	Purpose of the computer within the organization's network	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Windows Linux macOS Android
Active Directory	Path to the computer in the company's Active Directory.	Character string
Virtual machine	Indicates whether the computer is physical or virtual.	Boolean
Agent version	Internal version of the agent component that is part of the Panda Endpoint Protection client software.	Character string
Protection	Internal version of the protection component that is	Character string

Field	Description	Values
version	part of the Panda Endpoint Protection client software.	
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last connection date	Date when the computer status was last sent to the Panda Security cloud.	Date
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 7.4: 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	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device

Field	Description	Values
Platform	Operating system installed on the computer.	<ul style="list-style-type: none"> • All • Windows • Linux • macOS • Android
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	<ul style="list-style-type: none"> • 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
License status	The computer's license status.	<ul style="list-style-type: none"> • Assigned • No license • Excluded

Table 7.5: 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 217 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.

Expiration notifications

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

In addition to this, you are notified of the license contracts that have expired during the last thirty days.



If all products and license contracts have expired, you no longer have access to the management console.

Withdrawal of expired licenses

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

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

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



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

Adding trial licenses to commercial licenses

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

- A new trial license contract 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 is, by default, enabled on all computers in Audit mode. If you do not want to enable Panda Endpoint Protection on all computers or you want to set a different protection mode, this can be configured accordingly.



See [Manual and automatic assignment of settings profiles](#) on page 249 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 filter tree enables you search for computers based on the status of their licenses.



See [Creating and organizing filters](#) on page 186 for more information about how to create filters in Panda Endpoint Protection.

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 license assigned.
		Not assigned	Lists computers that do not have a Panda Endpoint Protection license assigned.

Category	Property	Value	Description
		Unassigned manually	Lists computers whose Panda Endpoint Protection license was manually released by the network administrator.
		Unassigned automatically	Lists computers whose Panda Endpoint Protection license was automatically released by the system.

Table 7.6: Fields in the License filter

Product updates and upgrades

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

Chapter contents

Updatable modules in the client software	175
Protection engine updates	176
Updates	176
Communications agent updates	178
Knowledge updates	178
Windows, Linux, and macOS devices	178
Android devices	178
Management console update	179
Considerations prior to updating the console version	179

Updatable modules in the client software

The components installed on users' computers are the following:

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

The update procedure and options vary depending on the operating system of the device to update, as indicated in [Table 8.1](#):

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

Table 8.1: Update procedures based on the client software component

- **On demand:** You can launch the update 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, go to the **Settings** menu at the top of the console and select **Per-computer settings** from the left menu.

Updates

To enable automatic updates of the Panda Endpoint Protection protection module, click the **Automatically update Panda Endpoint Protection 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 the following parameters for computers to run updates at specific time intervals:

- Start time
- End time

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

Running updates on specific days

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

- **Any day**: The updates will run when they are available. This option does not link Panda Endpoint Protection updates to specific days.
- **Days of the week**: Use the checkboxes to select the days of the week on which the Panda Endpoint Protection updates will run. If an update is available, it will run on the first day of the week that matches your selection.
- **Days of the month**: Use the drop-down menus to set a range of days of the month for the Panda Endpoint Protection updates to take place. If an update is available, it will run on the first day of the month that matches your selection.
- **On the following days**: Use the drop-down menus to set a specific date range for the Panda Endpoint Protection 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 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 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.

Knowledge updates

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

Windows, Linux, and macOS devices

Go to **Settings** at the top of the console. Select **Workstations and servers** from the left menu.

Go to **General**. The following 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's work.

Android devices

Go to **Settings** at the top of the console. Select **Mobile devices** from the left menu.

Panda Endpoint Protection 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 update

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

Considerations prior to updating the console version

Although this is a process that takes place entirely on the Panda Security servers, upgrading the console version can push new versions of the security software to the customer's computers. This can result in high traffic loads and the need to restart the computers on the network in some cases. To reduce the traffic during updates, see [Configuring downloads from cache computers](#) on page 266.

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

Starting the management console update


- Click the **Web notifications** icon  on the upper-right side of the top menu. The unread notifications appear.
- If there is a console upgrade available, a message entitled **New management console version** is shown, along with the **New features and improvements** link, the version to which the console will be updated, 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 37.



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

- After the button is clicked, the update 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 update process, it is not possible to log in to the management console.
- After some time, which depends on the number of managed computers and the data stored on the console, the update process will finish.

Canceling the update

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

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, 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	182
The Computer tree panel	183
Filter tree	184
About filters	184
Predefined filters	184
Creating and organizing filters	186
Configuring filters	187
Example filters	189
Group tree	191
Creating and organizing groups	193
Moving computers from one group to another	195
Filtering results by groups	196
Filtering groups	197
Scan and disinfection tasks	197
Available lists for managing computers	198
The Computer list panel	198
My lists panel	208
Computer details	217

General section (1)	218
General section for mobile devices	218
Computer notifications section (2)	220
Details section (3)	229
Detections section (4) for Windows, Linux, and macOS computers	234
Detections section (4) for Android and iOS devices	234
Hardware section (5)	235
Software section (6)	236
Settings section (7)	238
Action bar (8)	238
Hidden icons (9)	239

The Computers area

The **Computers** area in the web console enables you to manage all devices integrated into Panda Endpoint Protection.

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.

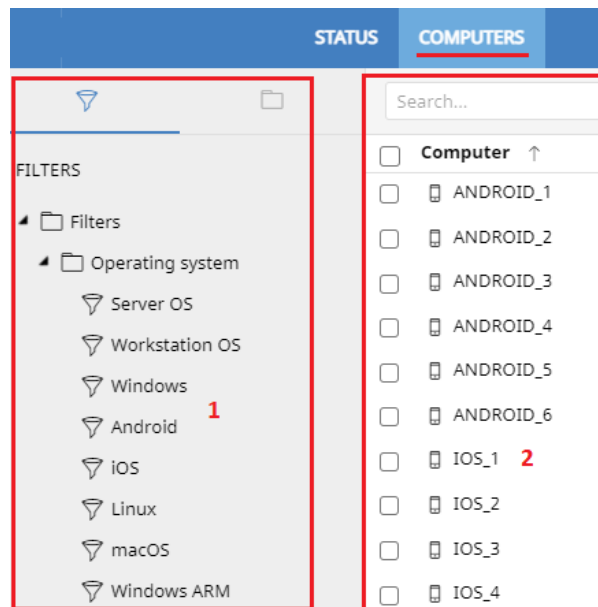


Figure 9.1: General view of the panels in the Computers area

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

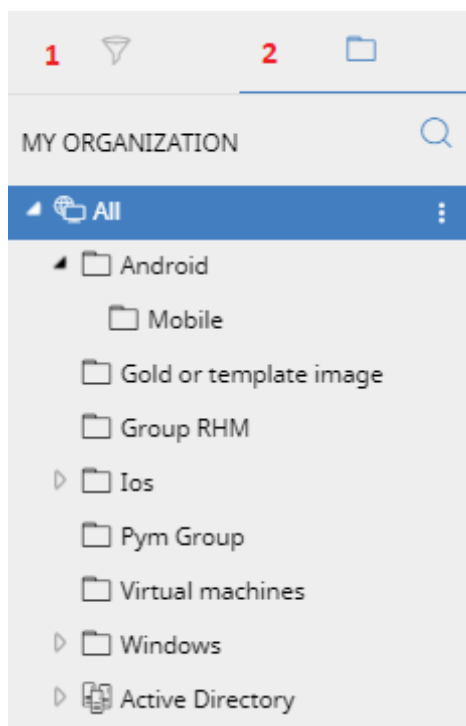


Figure 9.2: The Computer tree panel

- **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 399. For information about how to assign security settings profiles, see [Manual and automatic assignment of settings profiles](#) on page 249. For more information about how to take remediation actions, see [Remediation tools](#) on page 457.

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 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.

Name	Group	Description
Adobe Acrobat Reader	Software	Lists all computers with Acrobat Reader installed.
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.
Exchange servers	Software	Lists all computers with Microsoft Exchange Server installed.

Table 9.1: Predefined filter list

Creating and organizing filters

To create and organize filters, click the context menu icon next to a branch of your choice in the filter tree. A pop-up menu 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.

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:

Edit filter

Name: 1

Contains computers that meet the following conditions

Computer Name Is equal to Desktop-Luci + -

AND 3

Hardware CPU - Manufacturer Contains Intel + -

OR

Software Installation date Before 9/17/2018 + -

Group + New condition

OK Cancel

Figure 9.3: 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 301 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 the Panda Security cloud:

- **Category:** Security
- **Property:** Connection for collective intelligence
- **Condition:** Is equal to
- **Value:** With problems
- **Rule:**
 - **Category:** Security
 - **Property:** Connection for collective intelligence
 - **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)

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	These are Panda Endpoint Protection groups, some of which are predefined.







Group type	Description
groups 	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 9.2: Group types in Panda Endpoint Protection

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 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.

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. Panda Endpoint Protection automatically updates Active Directory groups within one hour when you make changes to your Active Directory structure.

In Panda Endpoint Protection, 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.

For information on how to reestablish the synchronization relationship between Active Directory and Panda Endpoint Protection, see [Returning multiple computers to their Active Directory group](#) on page 196.

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 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 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 All 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 interprets all specified paths as part of the selected group.
- If the groups indicated in the file do not already exist, Panda Endpoint Protection 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, 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](#) on page 194

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. To do this, you must move the computer in Active Directory and then wait up to one hour for Panda Endpoint Protection 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.

Scan and disinfection tasks

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



For more information about the various types of scans, see [Scan options](#) on page 462.

Immediate scans

Click the **Scan now** option to launch an immediate scan of all computers in a group and its subgroups. A dialog box opens for you to select the scan type: **The entire computer** or **Critical areas**.

Scheduled scans

Click the **Schedule scan** option to schedule a scan for a computer or group.

Available lists for managing computers

The Computer list panel

Accessing the list

- Select the **Computers** menu at the top of the console. The panel on the left shows the computer or folder tree, whereas the panel on the right shows all managed computers on the network.
- Click an item from the group tree or filter tree on the left. The panel on the right is updated with the content of the selected item.

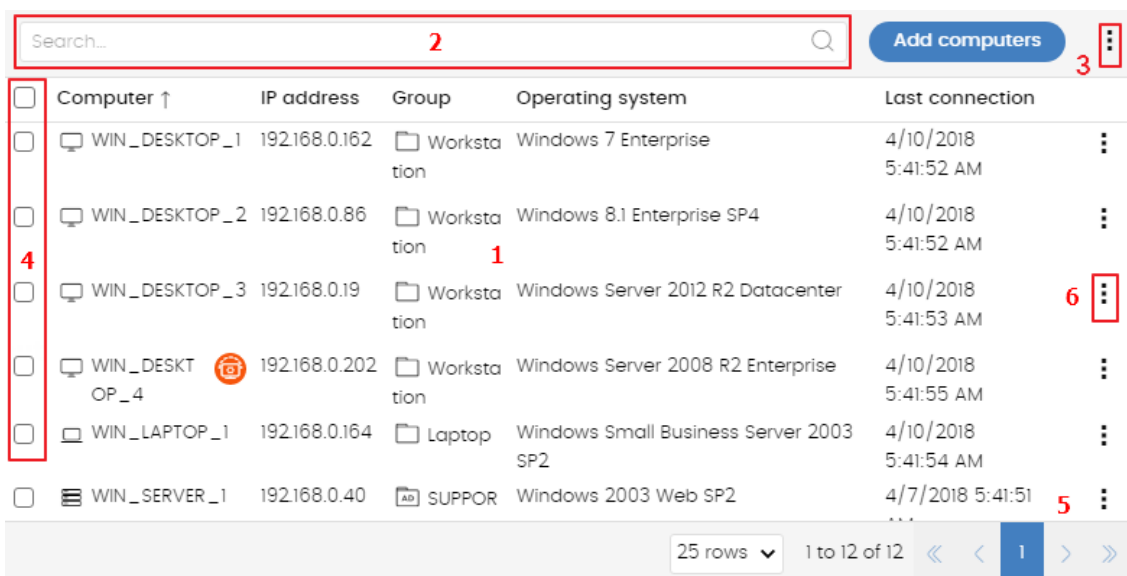


Figure 9.4: The Computer list panel

Required permissions

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

Computers



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

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










- **(1)** List of computers belonging to the selected branch.
- **(2)** Search tool: Enables you to find computers by their name, description, IP address, or last logged-in user. It supports partial matches and is not case sensitive.
- **(3)** General context menu: Enables you to apply an action to multiple computers.










- **(4)** Computer selection checkboxes.
- **(5)** Pagination controls at the bottom of the panel.
- **(6)** Context menu for each computer.

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

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

You can see this detailed information for each computer:

Field	Description	Values
<p>Computer</p>	<p>Computer name and type.</p>	<p>Character string:</p> <ul style="list-style-type: none"> •  Workstation or server •  Laptop •  Mobile device (Android smartphone or tablet)
<p>Computer status</p>	<p>Agent reinstallation:</p> <ul style="list-style-type: none"> •  Reinstalling the agent. •  Agent reinstallation error. <p>Protection reinstallation:</p> <ul style="list-style-type: none"> •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. <p>Computer isolation status:</p> <ul style="list-style-type: none"> •  Computer in the process of being isolated. 	<p>Icon</p>

Field	Description	Values
	<ul style="list-style-type: none"> •  Isolated computer. •  Computer in the process of stopping being isolated. <p>“RDP attack containment” mode:</p> <ul style="list-style-type: none"> •  Computer in “RDP attack containment” mode. •  Ending “RDP attack containment” mode. 	
IP address	The computer's primary IP address.	IP address
Description	Description assigned to the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory path	Path to the computer in the company's Active Directory.	Character string
IP address	The computer's primary IP address.	IP address
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs, and its type.	Character string: <ul style="list-style-type: none"> •  Group •  IP-based group •  Active Directory AD or root domain •  Organizational unit •  Group tree root
Operating system	Name and version of the operating system installed on the computer.	Character string
Last	Date when the computer status was last sent to	Date

Field	Description	Values
connection	the Panda Security cloud.	
Last logged-in user	Names of the user accounts that have an active session on the computer.	Character string

Table 9.3: 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.	<ul style="list-style-type: none"> • 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
Physical addresses (MAC)	Comma-separated list of the physical addresses of all cards installed on the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory	Path to the computer in the company's Active Directory.	Character string
Group	Folder within the Panda Endpoint Protection group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string

Field	Description	Values
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last connection	Last time the computer connected to the cloud.	Date
Platform	Type of operating system installed.	<ul style="list-style-type: none"> • 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 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.	Boolean
Protection version	Internal version of the protection module installed on the computer.	Character string
Last update on	Date when the protection was last updated.	Date
Licenses	Licensed product.	Panda Endpoint Protection
Network settings	Name of the network settings 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

Field	Description	Values
Settings inherited from	Name of the folder from which the device inherited its 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 its 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 its 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 its settings profile.	Character string
Data Control	Name of the personal data monitoring (Panda Data Control) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited its 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	Character string

Field	Description	Values
from	inherited the encryption settings profile.	
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
Indicators of attack (IOA)	Name of the Indicators of attack (IOA) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the Indicators of attack (IOA) settings profile.	Character string
Isolation status	Shows the isolation status of the computer.	<ul style="list-style-type: none"> • Isolated • Isolating • Stopping isolation • Not isolated
"RDP attack containment" mode	Status of the "RDP attack containment" mode.	Boolean
Description	Description assigned to the computer.	Character string
Last logged-in user	Names of the user accounts, separated by commas, that have an interactive session active on the Windows computer.	Character string
Requested action	Requested action that is pending execution or is in progress.	<ul style="list-style-type: none"> • Restart • Protection reinstallation • Agent reinstallation
Requested action failed	Type of error reported by the requested action.	<ul style="list-style-type: none"> • Wrong credentials • Discovery computer not

Field	Description	Values
		<ul style="list-style-type: none"> available • Unable to connect to the computer • Operating system not supported • Unable to download the agent installer • Unable to copy the agent installer • Unable to uninstall the agent • Unable to install the agent • Unable to register the agent • Action requires input from the user
Last proxy used	<p>Access method used by Panda Endpoint Protection 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.</p>	Character string
Shadow Copies	<p>Shows the feature status:</p> <ul style="list-style-type: none"> • Enabled • Disabled • Error 2010: The Shadow Copies service could not be enabled. 	Enumeration

Field	Description	Values
	<ul style="list-style-type: none"> Error 2011: An error occurred creating the last Shadow Copy. 	
Last copy	Date and time the last copy was made.	Date

Table 9.4: Fields in the Computer list exported file

Filter tools

Field	Description	Values
Computer	Computer name.	Character string.

Table 9.5: Filters available in the Computer list

Management tools

When you select one or more computers using their checkboxes **(4)**, the search tool **(2)** hides and the action bar **(7)** is displayed instead.

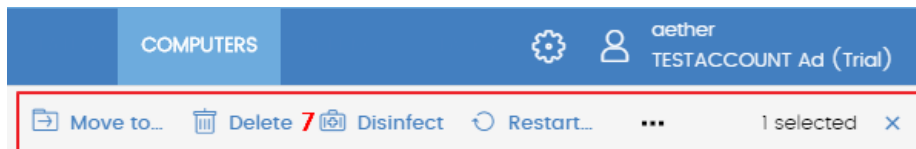



Figure 9.5: Action bar

Click the checkbox in the table header **(4)** to select all computers on the current page of the list. The **Select all xx rows in the list** option appears, which enables you to select all computers on the list regardless of the page you are on.

Action	Description
 Refresh computer information	Forces the agent installed on the computer to take the following actions: <ul style="list-style-type: none"> • Check for pending actions. • Check for pending tasks. • Check for applied settings profiles. • Send status information. This icon is shown only for computers with the Real-time communication feature enabled. See Configuring real-time communication on page 268 for more information.











Action	Description
 Move to	Opens a window showing the group tree. Choose the group to move the computer to. The computer inherits the settings profiles assigned to the target group. See Creating and managing settings profiles on page 247 for more information.
 Move to Active Directory path	Moves the selected computers to the group that corresponds to their organizational unit in the organization's Active Directory.
 Delete	Deletes the computer from the console and uninstalls the Panda Endpoint Protection client software from it. See Uninstalling the software on page 155 for more information.
 Scan now	See Scan and disinfection tasks for an introduction to scan tasks or Tasks on page 469 for a complete description.
 Schedule scan	See Scan and disinfection tasks for an introduction to scan tasks or Tasks on page 469 for a complete description.
 Restart	Restarts the computer. See Computer restart on page 466 for more information.
 Schedule patch installation	See Panda Patch Management (Updating vulnerable programs) for more information about how to patch Windows computers.
 Reinstall protection (requires restart)	Reinstalls the protection if a malfunction occurs. See Remote reinstallation on page 157 for more information.
 Selected	Undoes the current selection.


Table 9.6: Computer management tools

My lists panel

Accessing the My lists panel

- Go to top menu **Status**. 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 45 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: <ul style="list-style-type: none"> •  Workstation or server. •  Laptop. •  Mobile device (Android smartphone or tablet).
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string

Field	Description	Values
CPU	Make and model of the microprocessor installed on the computer. The number of installed cores is shown in brackets.	Character string
Memory	Total amount of RAM memory installed.	Character string
Disk capacity	Sum of the capacity of all the internal hard disks connected to the computer.	Character string
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	Date
Context menu	Management tools. See Management tools for more information.	

Table 9.7: Fields in the Hardware list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • 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

Field	Description	Values
Group	Folder in the Panda Endpoint Protection 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 status was last sent to the Panda Security cloud.	Date
Platform	Type of operating system installed.	<ul style="list-style-type: none"> • 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 of cores	Number of cores in CPU number N.	Numeric value
CPU-N Number of logical processors	Number of logical cores reported to the operating system by the Hyper-Threading/SMT (simultaneous multithreading) system.	Numeric value
Memory	Sum of all the RAM memory banks installed on the computer.	Character string
Disk-N Capacity	Total space on internal storage device number N.	Character string
Disk-N Partitions	Number of partitions on internal storage device number N reported to the operating system.	Numeric value
TPM spec version	Versions of the APIs compatible with the TPM chip.	Character string

Field	Description	Values
BIOS - Serial number	The computer's BIOS serial number.	Character string

Table 9.8: Fields in the Hardware exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	<ul style="list-style-type: none"> • Windows • Android

Table 9.9: 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 9.10: 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 9.11: 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.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
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 group tree that the computer belongs to.	Character string

Field	Description	Values
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 9.12: Fields in the detailed export file

Filter tool

Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	<ul style="list-style-type: none"> • Windows • Linux • macOS • Android

Table 9.13: 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 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 agent.



Deleting computers from the **Computers with duplicate name** list without uninstalling the Panda Endpoint Protection agent removes them from the Panda Endpoint Protection console. However, those computers reappear in the Panda Endpoint Protection 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: <ul style="list-style-type: none"> • 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 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
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	Date

Table 9.14: Fields in the Computers with duplicate name list

Fields displayed in the exported file

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

Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder in the Panda Endpoint Protection 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 software was successfully installed on the computer.	Date
Last connection date	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	Date
Platform	Type of operating system installed.	<ul style="list-style-type: none"> • Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string

Field	Description	Values
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 9.15: Fields in the Computers with duplicate name exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	<ul style="list-style-type: none"> • All • Windows • Linux • macOS • Android
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	<ul style="list-style-type: none"> • All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3

Field	Description	Values
		days ago • More than 7 days ago • More than 30 days ago

Table 9.16: Filters available in the Computers with duplicate name list

Computer details 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 is displayed with details of the hardware and software installed, as well as the security settings profile assigned to it.

The details page is divided into the following sections:



Figure 9.6: Computer details overview

- **General (1):** Information to help you identify the computer.
- **Notifications (2):** Details of any potential problems.
- **Details (3):** A summary of the hardware, software, and security settings of the computer.
- **Detections (4):** The security status of the computer.
- **Hardware (5):** Hardware installed on the computer, its components and peripherals, as well as resource consumption and use.

- **Software (6):** Software packages installed on the computer, as well as versions and changes.
- **Settings (7):** 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 window and the number of actions, some of the actions are available from an options menu.

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 connection	Date when the client software last connected to the Panda Endpoint Protection cloud.

Table 9.17: 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 start remote actions on a managed device.

 In the case of iOS devices, the actions you can take vary depending on whether the mobile device is enrolled into an MDM solution or not. See [Installation on iOS systems](#) on page 128.

 See [Anti-theft](#) on page 297 for more information about how to enable the anti-theft feature for mobile devices and configure the private mode.

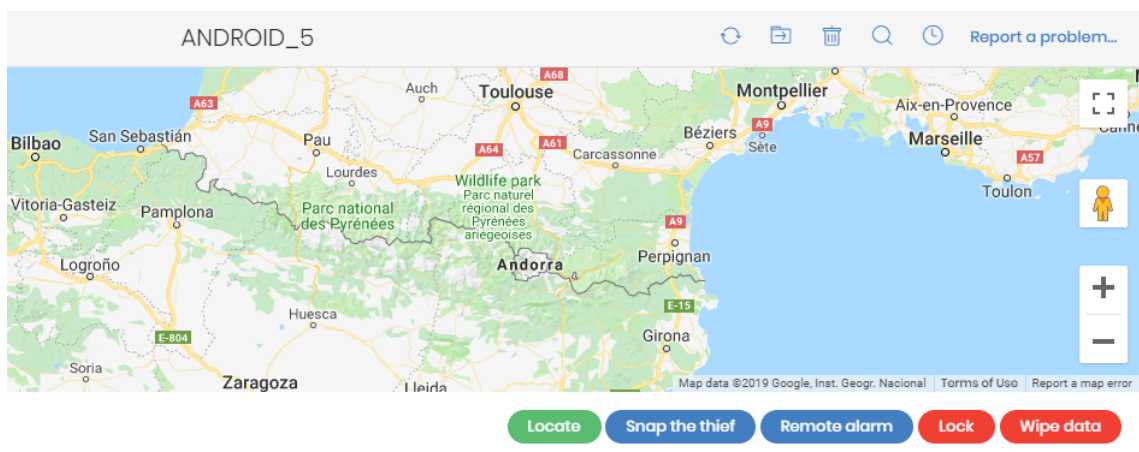


Figure 9.7: Anti-theft dashboard for mobile devices

The available actions are:

Action	Description
Locate	<ul style="list-style-type: none"> With private mode enabled: The console displays a window prompting you to enter the code entered by the device user when enabling private mode. When you enter the correct code, Panda Endpoint Protection gets the device coordinates and shows the device location on the map. With private mode disabled: The Panda Endpoint Protection server gets the device coordinates directly and shows the device location on the map.
Snap the thief	<p>This option is not available for iOS devices.</p> <p>When anti-theft is enabled, you can take a photo of the person using the device. The feature displays 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:</p> <ul style="list-style-type: none"> Now: The Panda Endpoint Protection agent immediately takes a photo from the device and sends it to the specified address.

Action	Description
	<ul style="list-style-type: none"> • When the screen is touched: The Panda Endpoint Protection agent takes a photo and sends it to the specified address when the user or potential thief touches the device screen.
Remote alarm	Displays 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 displays the message and phone number you specify. To not play an alarm sound, select the Don't play any sound checkbox.
Lock	<p>Locks the phone, preventing it from being used when it is lost or stolen. This feature behaves differently depending on the operating system version installed on the device:</p> <p>Android</p> <ul style="list-style-type: none"> • Lower than 7: The console prompts the user to set a PIN, which is used to lock the phone. • 7 through 11 (inclusive): If a PIN exists that was previously set by the user, it is used to lock the phone. If a PIN has never been set previously, the console prompts the user to set one and uses it to lock the phone. • Higher than 11: The console never prompts the user to set a PIN. If a PIN exists that was previously set by the user, it is used to lock the phone. If a PIN has never been set previously, the screen is turned off. <p>iOS:</p> <p>13 or higher: If a PIN exists that was previously set by the user, it is used to lock the phone. If a PIN has never been set previously, the screen is turned off.</p>
Wipe data	This option deletes all content and applications from the device. The device returns to factory settings.

Table 9.18: Actions supported by the anti-theft module for mobile devices

Computer notifications section (2)

These notifications describe any problems encountered on computers with regard to the operation of Panda Endpoint Protection and provide instructions for resolving them.

Occasionally, notifications **(1)** are accompanied by codes **(2)**.

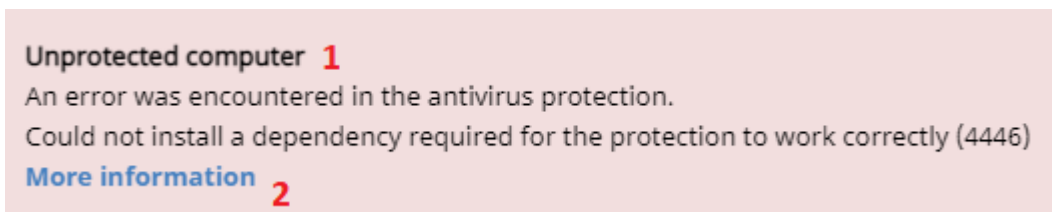


Figure 9.8: Unprotected computer notification and associated code

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/es/support/card?id=700031>.

These tables list the types of notifications generated and recommended actions.

Computers in containment mode

Notification	Description	Reference
Computer in "RDP attack containment" mode	The computer has received a high number of failed RDP connection attempts, and all RDP connections have been blocked to contain the attack.	See Detection and protection against RDP attacks
We're trying to end the "RDP attack containment" mode on this computer.	The administrator has manually ended the "RDP attack containment" mode on the computer, but the operation is not yet complete. This could be because the computer is turned off, offline, pending restart, or the action is in progress.	See Detection and protection against RDP attacks .

Table 9.19: Notifications related to the attack containment feature


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 licenses.	See Releasing licenses on page 164 for more information.
	There are free licenses but none of them have been assigned to this computer.	See Assigning licenses on page 163 for more

Notification	Description	Reference
		information.

Table 9.20: 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. See table [Table 1.2](#): on page 1 for more information.


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.	See Hardware, software, and network requirements on page 481 for more information.
	A reboot is required to complete the installation due to a previous uninstallation.	See Computer restart on page 466 for more information.
Error installing Data Control	There was an error during installation of Panda Data Control on the computer.	See Panda Data Control requirements for more information.
Error installing the protection and Data Control	There was an error during installation of the protection and the module on the computer.	See Hardware, software, and network requirements on page 481 and Panda Data Control requirements for more information.
Error installing the patch manager	There was an error during installation of the patch	See Make sure that Panda Patch Management works correctly on

Notification	Description	Reference
	management module.	page 303 for more information.
Error installing the encryption module	There was an error during installation of the encryption module.	See Panda Full Encryption minimum requirements on page 368 for more information.
Error installing the Panda agent	Wrong credentials.	See Offline computers on page 403 for more information.
	The discovery computer is not available.	See Security module panels/widgets on page 399 , and Assigning the role of discovery computer to a computer on your network on page 104 for more information.
	Unable to connect to the target computer because it is turned off or does not comply with the hardware or network requirements.	See Security module panels/widgets on page 399 for more information. See Hardware, software, and network requirements on page 481 for more information.
	The computer operating system is not supported.	See Hardware, software, and network requirements on page 481 for more information.
	Unable to download the agent installer due to a network error.	See Hardware, software, and network requirements on page 481 for more information.
	Unable to copy the agent installer due to low free disk space on the computer.	See Hardware, software, and network requirements on page 481 for more information.
	Unable to copy the agent installer because the target computer is turned off or does not meet the remote installation requirements.	See Offline computers on page 403 and Hardware, software, and network requirements on page 481 for more information.

Notification	Description	Reference
	Unable to register the agent.	See Offline computers on page 403 and Hardware, software, and network requirements on page 481 for more information.
Error communicating with servers	The computer cannot connect to one or more servers in the Panda cloud.	See Hardware, software, and network requirements on page 481 for more information.

Table 9.21: Notifications related to the installation of the Panda Endpoint Protection software

Protection software reinstallation 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. See table [Table 1.2](#): on page [1](#) for more information.

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 403 and Remote reinstallation requirements on page 157 .
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 403 and Remote reinstallation requirements on page 157 .
Error installing the Panda agent	Wrong credentials.	See Offline computers on page 403 for more information.
	The discovery computer is not available.	See Offline computers on page 403 .

Notification	Description	Reference
	Unable to connect to the computer. It is off or offline, or does not meet remote installation requirements.	See Offline computers on page 403 and Remote reinstallation requirements on page 157 .
	The operating system is not supported. It does not meet remote installation requirements.	See Remote reinstallation requirements on page 157 .
	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 403 and Remote reinstallation requirements on page 157 .
	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 403 and Remote reinstallation requirements on page 157 .
	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 403 and Remote reinstallation requirements on page 157 .
	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 403 and Remote reinstallation requirements on page 157 .
	Unable to register the agent because the computer is turned off or does not meet remote installation requirements.	See Offline computers on page 403 and Remote reinstallation requirements on page 157 .

Notification	Description	Reference
		157.
	Action requires input from the user.	See Offline computers on page 403 and Remote installation requirements on page 157.

Table 9.22: Notifications related to the reinstallation of the Panda Endpoint Protection agent

Panda Endpoint Protection 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 466.
Error encrypting the computer	Unable to encrypt the computer due to an error.	See Computer restart on page 466.

Table 9.23: Notifications related to Panda Endpoint Protection 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 Computer restart on page 466. See Encryption and decryption on page 369
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 403.
Reinstalling the protection.	The administrator has requested that the computer protection be reinstalled but the	See Remote installation on page

Notification	Description	Reference
	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.	157
Unprotected computer	The antivirus protection is disabled. Enable the protection.	See Manual and automatic assignment of settings profiles on page 249 , Creating and managing settings profiles on page 247 , and Antivirus on page 281 .
Computer offline for N days	The computer is turned off or does not meet the network access requirements.	See Hardware, software, and network requirements on page 481 .
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 Hardware, software, and network requirements on page 481 .
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	The new versions of the protection require	See Support for SHA-256 driver signing on page

Notification	Description	Reference
this computer's protection to the latest version	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	489.

Table 9.24: 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.	See Computer restart on page 466 for more information.
	An error occurred during the update process. Make sure the computer meets the hardware and network requirements.	See Hardware, software, and network requirements on page 481 and the amount of available disk space in the Hardware section (5) .
	Updates are disabled for the computer. Assign the computer a settings profile with updates enabled.	See Protection engine updates on page 176 .
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 178 .

Table 9.25: Notifications related to out-of-date Panda Endpoint Protection 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

Notification	Description	Reference
iOS or Android device with permission problems	The device user has not granted permissions required by Panda Endpoint Protection, affecting its performance.	See Requirements for iOS platforms on page 494 and Requirements for Android platforms on page 493

Table 9.26: 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 protection modules.
- **Data protection** (Windows only): The status of the modules responsible for protecting the content of the data stored on computers.

Computer

Field	Description
Name	Computer name.
Description	Descriptive text provided by the administrator.
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.

Field	Description
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 161 for more information.
Agent version	Internal version of the Panda agent installed on the computer.
Last bootup date	Date when the computer was last booted.
Installation date	Date when the computer's operating system was last installed.
Last proxy used	Access method used by Panda Endpoint Protection 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 last connected to the Panda Security cloud checking for changes to the settings.
Shadow Copies	Shows the feature status: <ul style="list-style-type: none"> • Enabled • Disabled • Error code
Last copy	Shows the date and time of the last copy made.

Field	Description
Last logged-in user	Names of the user accounts that have an active session on the computer.

Table 9.27: Fields in the Computer section

Security

This section shows the status (Enabled, Disabled, Error) of the Panda Endpoint Protection technologies that protect the computer against malware.

Field	Description
File antivirus	Protection for the file system.
Anti-theft	<p>Actions for mitigating data exposure in the event of theft of a mobile device.</p> <p>This feature is not available for iOS devices not installed with an MDM solution. See Installation on iOS systems on page 128.</p>
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 128.
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).
Patch management	Installation of patches and updates for Windows operating systems and third-party applications. Detection of the patch status of the computers on the network and removal of problematic patches.
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.

Field	Description
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.
Connection to knowledge servers	Status of the connection between the computer and the Panda Security servers. In case of errors, links are shown to support pages with information about the requirements that must be met.

Table 9.28: Fields in the Security section

Data protection

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

Field	Description
Hard disk encryption	<p>Encryption module status:</p> <ul style="list-style-type: none"> • 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 Full Encryption license assigned. <p>Get recovery key: Opens a window showing the IDs of the computer's encrypted storage media. Click any of them to display the relevant recovery key. See Getting a recovery key on page 375 for more</p>

Field	Description
	information.
	<p>Encryption process status:</p> <ul style="list-style-type: none"> • Unknown: There are drives whose status is unknown. • Unencrypted disks: Some of the drives compatible with the encryption technology are neither encrypted nor in the process of being encrypted. • Encrypted disks: All drives compatible with the encryption technology are encrypted. • Encrypting: At least one of the computer drives is being encrypted. • Decrypting: At least one of the computer drives is being decrypted. • Encrypted by the user: All storage media are encrypted by the user. • Encrypted by the user (partially): Some storage media are encrypted by the user.
Authentication method	<ul style="list-style-type: none"> • Unknown: The authentication method is not compatible with those supported by Panda Patch Management. • Security processor (TPM). • Security processor (TPM) + Password • Password: Authentication method based on a PIN, extended PIN, or passphrase. • USB drive: Authentication method based on a USB drive. • Not encrypted: None of the drives compatible with the encryption technology is encrypted or in the process of being encrypted.
Encryption date	Date when the computer was fully encrypted for the first time.
Removable storage drive encryption	<p>Encryption module status:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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 Full Encryption license assigned. <p>View encrypted devices on this computer: Opens a window showing the IDs of the computer's encrypted external storage media. Click any of them to display the relevant recovery key. See Getting a recovery key on page 375 for more information.</p>

Table 9.29: 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 405.
Available patches	See Available patches on page 323.
End-of-Life programs	See End-of-Life programs on page 321.

Table 9.30: 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 405.

List of widgets available in the Detections section

Hardware section (5)

Contains information about the hardware resources installed on the computer:

Field	Description	Values
CPU	Information about the computer's microprocessor, along with a line chart showing CPU consumption at different time intervals based on your selection.	<ul style="list-style-type: none"> • 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Memory	Information about the memory chips installed, along with a line chart with memory consumption at different time intervals based on your selection.	<ul style="list-style-type: none"> • 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Disk	Information about the mass storage system, along with a pie chart with the current percentage of free/used space.	<ul style="list-style-type: none"> • Device ID • Size • Type • Partitions • Firmware revision • Serial number • Name
BIOS	Information about the BIOS installed on the computer.	<ul style="list-style-type: none"> • Version • Manufacture date • Serial number

Field	Description	Values
		<ul style="list-style-type: none"> Name Manufacturer
TPM	Information about the security chip located on the computer's motherboard. To be used by Panda Endpoint Protection, the TPM must be enabled, activated, and owned.	<ul style="list-style-type: none"> Manufacturer version: Internal version of the chip. Spec version: Supported API versions. Version Manufacturer Activated: The TPM is ready to receive commands. This is used on systems with multiple TPMs. Enabled: The TPM is ready to work as it has been enabled in the BIOS. Owner: The operating system can interact with the TPM.

Table 9.31: Fields in the Hardware section of a computer's details

Software section (6)

Provides information about the software installed on the computer, the Windows operating system updates, and a history of software installations and uninstallations.

Filter tool

Type a software name or publisher in the **Search** text box and press Enter to perform a search. The following information is displayed for each program found:

Field	Description
Name	Name of the installed program.



Field	Description
Publisher	Company that developed the program.
Installation date	<p>Date when the program was last installed.</p> <p>With iOS devices enrolled into an MDM solution, this field indicates the date when the installed app was first seen on the device. See Deploying and installing the iOS agent on page 131.</p> <p>This information is not available for iOS devices not enrolled into an MDM solution.</p> <p>Devices enrolled into the Panda MDM solution send the server a daily report that includes the third-party apps they have installed.</p>
Size	Program size.
Version	Internal version of the program.

Table 9.32: Fields in the Software section of a computer's 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

- Click the **Installations and uninstallations** link to show a history of all changes made to the computer:

Field	Description
Event	<ul style="list-style-type: none"> •  Software uninstallation. •  Software installation.
Name	Name of the installed program.
Publisher	Company that developed the program.

Field	Description
Date	Date the program was installed or uninstalled.
Version	Internal version of the program.

Table 9.33: Fields in the Installations and uninstalls section

Settings section (7)

Shows the various settings profiles assigned to the computer and enables you to edit and manage them:

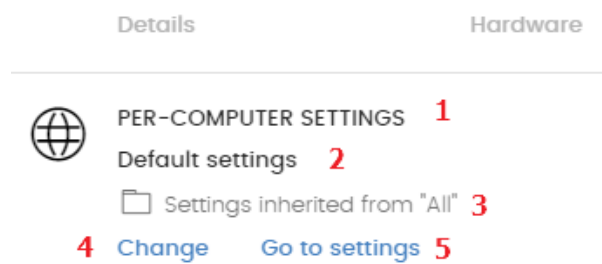



Figure 9.9: Example of inherited and manually assigned settings profiles

- **(1) Settings type:** Indicates the type of settings profile assigned to the computer. See [Introduction to the various types of settings profiles](#) on page 243 for information on the types of settings available in Panda Endpoint Protection.
- **(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 options.**



See [Creating and managing settings profiles](#) on page 247 for more information about how to create and edit settings profiles.

Action bar (8)

This resource groups multiple actions that can be taken on the managed computers on your network:

Action	Description
 Move to	Moves the computer to a standard group.
 Move to Active Directory path	Moves the computer to its original Active Directory group.
 Delete	Releases the Panda Endpoint Protection license and deletes the computer from the web console.
 Scan now	Enables you to run a scan task immediately. See On-demand computer scanning and disinfection on page 458 for more information.
 Schedule scan	Enables you to schedule a scan task. See On-demand computer scanning and disinfection on page 458 for more information.
 Schedule patch installation	Creates a task that installs all released patches missing from the target computer. See Download and install the patches on page 304 for more information.
 Restart	Restarts the computer immediately. See Computer restart on page 466 for more information.
 Reinstall protection (requires restart)	Reinstalls the protection if a malfunction occurs. See Remote reinstallation on page 157 for more information.
Report a problem	Opens a support ticket for the Panda Security support department. See Reporting a problem on page 466 for more information.

Table 9.34: Actions available from a computer's details page

Hidden icons (9)

Depending on the size of the page and the number of icons to display, some of them may be hidden under the **...** icon. Click it to show all remaining icons.

Chapter 10

Managing settings

Settings, also called "settings profiles" or simply "profiles", offer administrators a simple way of establishing security and connectivity parameters for the computers managed through Panda Endpoint Protection.

Chapter contents

Strategies for creating settings profiles	241
Overview of assigning settings profiles to computers	242
Introduction to the various types of settings profiles	243
Modular vs. monolithic settings profiles	245
Creating and managing settings profiles	247
Manual and automatic assignment of settings profiles	249
Manual/direct assignment of settings profiles	249
Indirect assignment of settings profiles: the two rules of inheritance	251
Inheritance limits	252
Overwriting settings	253
Moving groups and computers	255
Exceptions to indirect inheritance	256
Settings received from a partner	256
Features of the settings sent by partners	257
Requirements	257
Viewing assigned settings profiles	257

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 183.

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 268.

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 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 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.

The following is an introduction to the different types of settings profiles supported by Panda Endpoint Protection:

Panda Endpoint Protection enables you to configure the following 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 Controlling and monitoring the management console on page 55.
Per-computer settings	Create settings profiles to specify how often to update the Panda Endpoint Protection security software installed on workstations and servers. You can also define settings to prevent tampering and unauthorized uninstallation of the software. For more information, see Configuring the agent remotely on page 259.
Network settings	Create settings profiles to specify the language of the Panda Endpoint Protection software 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 259.
Network services	Specify how Panda Endpoint Protection communicates with computers on the network: <ul style="list-style-type: none"> • Proxy: Define computers that act as a proxy to enable isolated computers with Panda Endpoint Protection installed to access the cloud. For more information, see Proxy role on page 260. • Cache: Define computers that act as a cache for signature files, security patches, and other components used to update the Panda Endpoint Protection software installed on other computers and devices on the network. For more information, see Cache/repository role on page 261. • Discovery: Define computers that discover unprotected computers on the network. For more information, see Discovery computer role on page 263.
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 .
Workstations and servers	Configure security settings profiles to define how Panda Endpoint Protection protects the computers on your network against threats and malware. For more information, see Security settings for workstations and servers .

Settings	Description
	servers on page 277 .
Mobile devices	Create settings profiles to protect tablets and smartphones against threats, malware, and theft. For more information, see Security settings for mobile devices on page 295 .
Patch management	Create settings profiles to specify the discovery of new security patches published by vendors for the Windows operating systems and third-party software installed across the network. For more information, see Panda Patch Management (Updating vulnerable programs) on page 301 .
Encryption	Create settings profiles to encrypt the content of your computers' internal storage devices. For more information, see Panda Full Encryption (Device encryption) on page 363 .

Table 10.1: Description of the types of settings profiles available in Panda Endpoint Protection

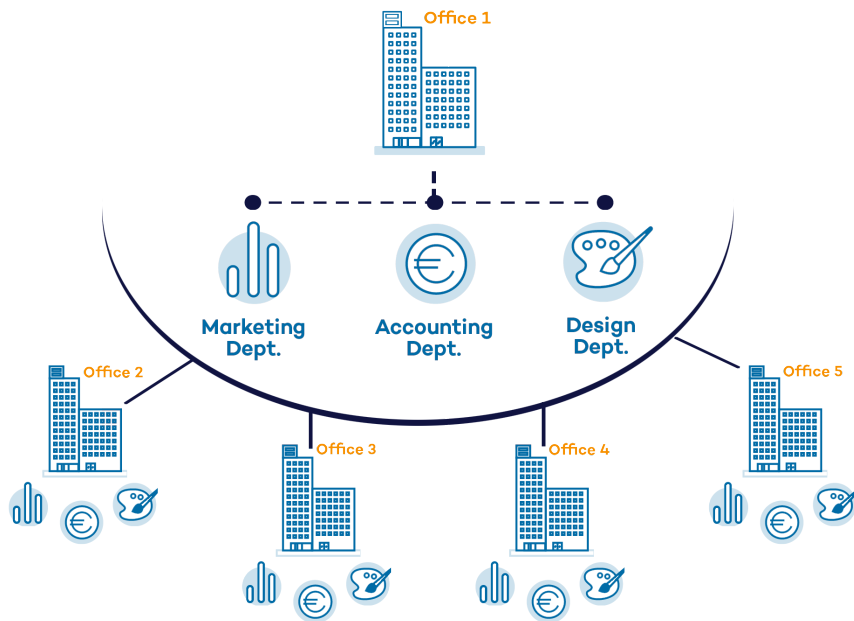
Modular vs. monolithic settings profiles

By supporting different types of profiles, Panda Endpoint Protection uses a modular approach for creating and deploying the settings to apply to managed computers. The reason for using this modular approach and not just a single, monolithic profile that covers all the settings is to reduce the number of profiles created in the management console. This in turn 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

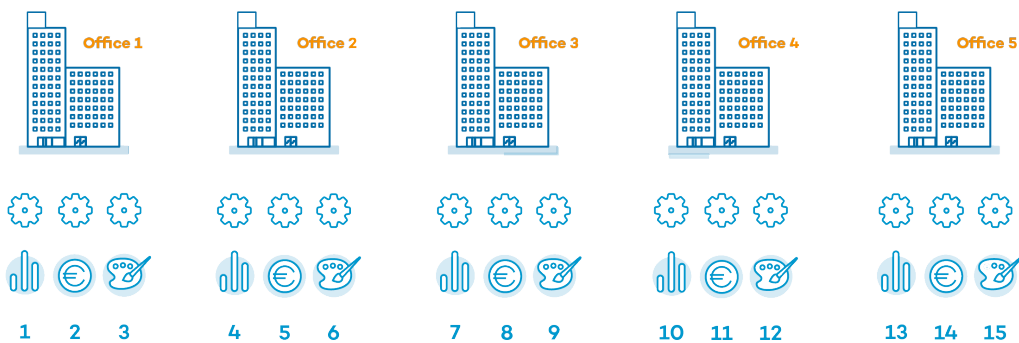
The following example uses a company with five offices, each with a different communications infrastructure and therefore different proxy settings. Also, each office requires three different security settings profiles: one for the Design department, another for the Accounting department, and the other for Marketing.

Network of a company with several offices



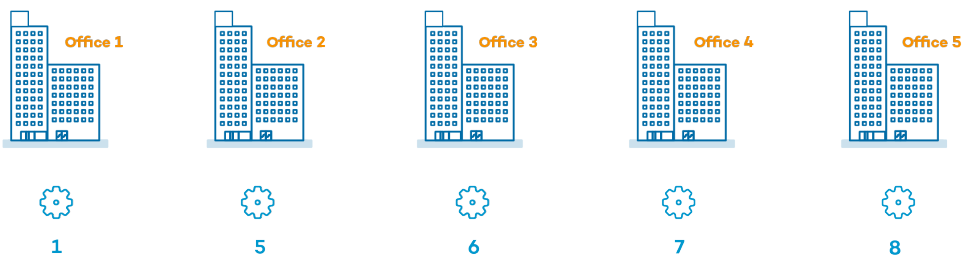
Using monolithic profiles, the company would require 15 different settings profiles (5 offices x 3 security settings profiles in each office = 15) to adapt to the needs of all three departments in the company's offices.

Monolithic profile

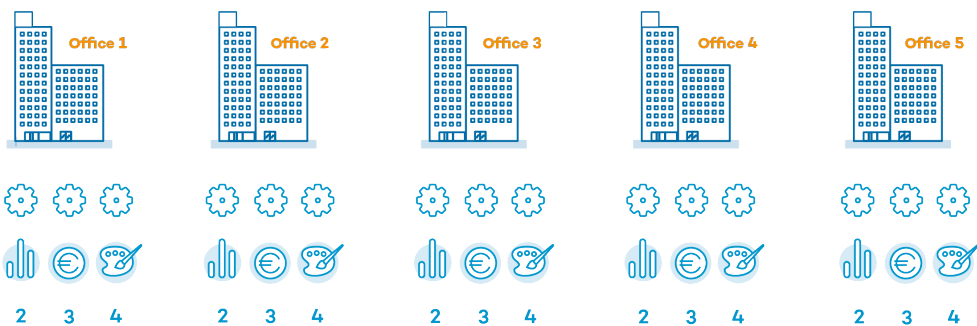


However, because Panda Endpoint Protection separates the proxy settings from the security settings, the number of profiles needed is reduced (5 proxy profiles + 3 department profiles = 8) as the security profiles for each department in one of the offices can be reused and combined with the proxy profiles in other offices.

Proxy and Language modular profile



Security modular profile



Creating and managing settings profiles

Click Settings in the menu bar at the top of the page to create, copy, and delete settings profiles. The panel on the left contains different sections corresponding to the various types of settings profiles that can be configured (1). In the right panel, you can see the profiles of the selected category that have already been created (2), and the buttons for adding (3), copying (4), and deleting profiles (5). To search for a settings profile, type the name in the Search box (6).

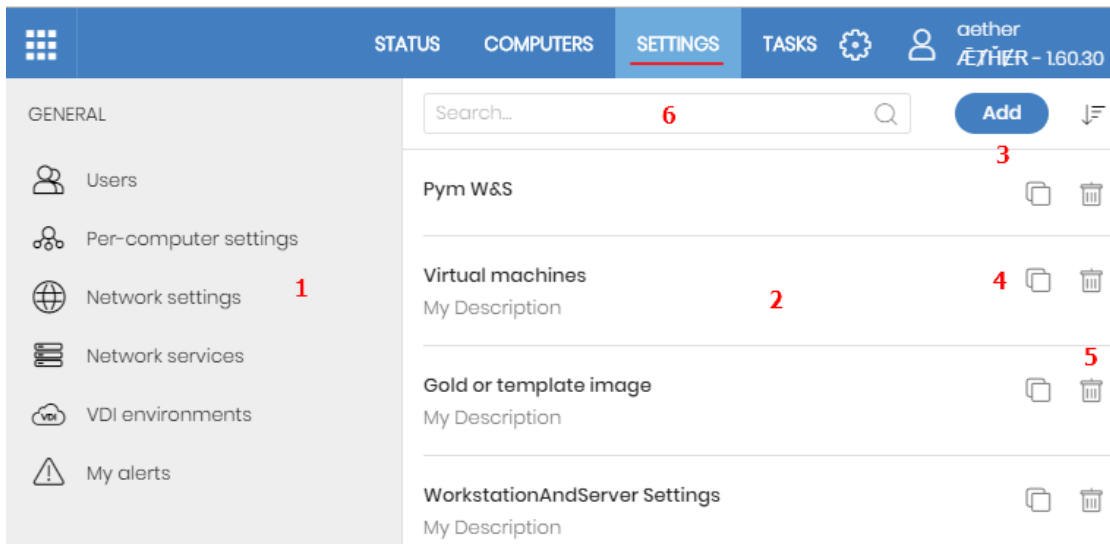



Figure 10.1: Page for creating and managing settings profiles

 The settings profiles created from Panda Partner Center are displayed with the Panda Partner Center. Point the mouse to the label to show the following message: "These settings are managed from Panda Partner Center". The settings profiles created from Panda Partner Center are read only and enable you to change only their recipients. For more information, see section [Settings management for Panda-based products in the Panda Partner Center Administration Guide](#).

Creating settings profiles

Click **Add** to open the create settings profile page. All profiles have a name and a description, which are displayed in the list of settings profiles.

Sorting settings

Click the  icon (7) to expand a context menu with the available sort options:

- Sort by creation date
- Sort by name
- Ascending
- Descending

Copying, deleting, and editing settings profiles

- To copy and delete a settings profile, use the (4) and (5) icons. You cannot delete a settings profile that is assigned to a device or computer.
- To edit a settings profile, click its name.



Before editing a profile, make sure the new settings are correct. Please note that if the profile is already assigned to any computers on the network, any changes you make will be applied automatically and immediately.

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 191.

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.

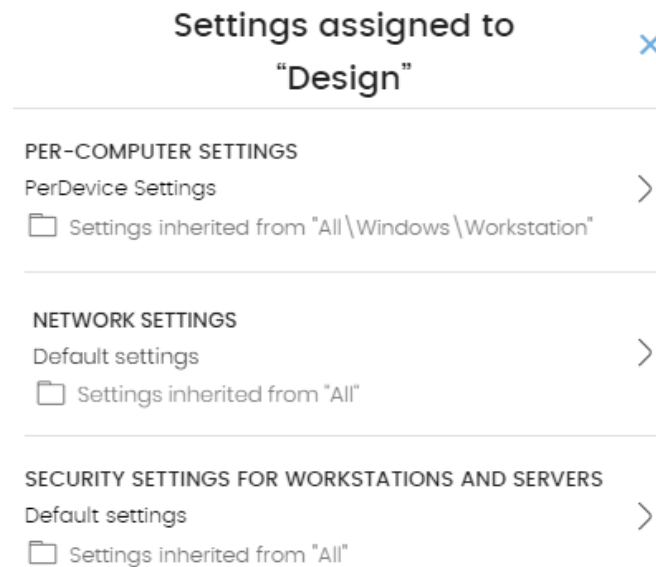


Figure 10.2: Example of inherited and manually assigned settings profiles

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).

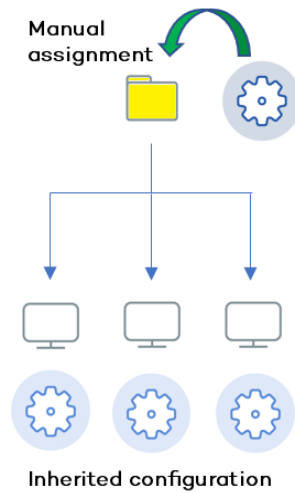


Figure 10.3: Inheritance/indirect assignment

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.

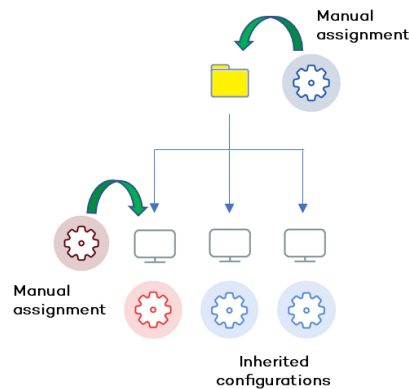


Figure 10.4: Precedence of manually assigned settings over inherited settings

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.

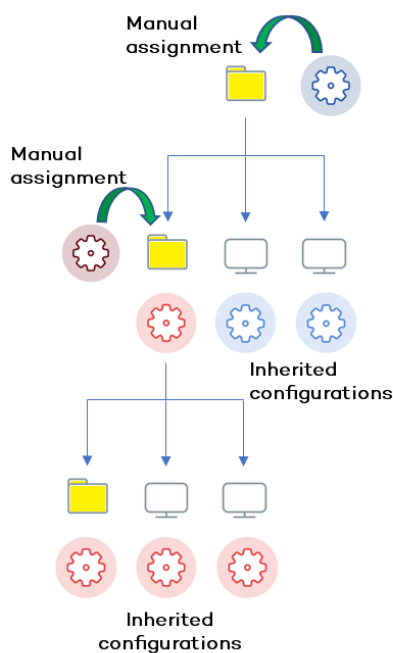


Figure 10.5: Inheritance limits

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.

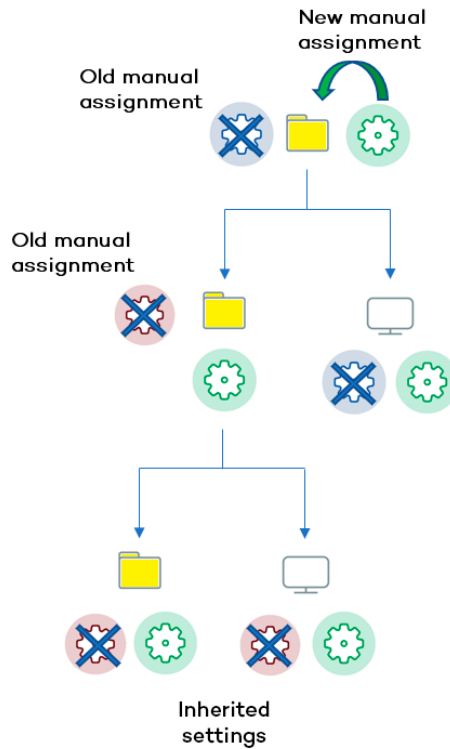


Figure 10.6: Overwriting manual settings

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 choosing this option as this action is irreversible! When you select this option, all groups and computers inherit the new settings. Panda Endpoint Protection overwrites all manual settings

and removes all manually assigned settings below the group.

Keep all settings

When you select this option, new settings apply only to groups and computers that do not have manually assigned settings.

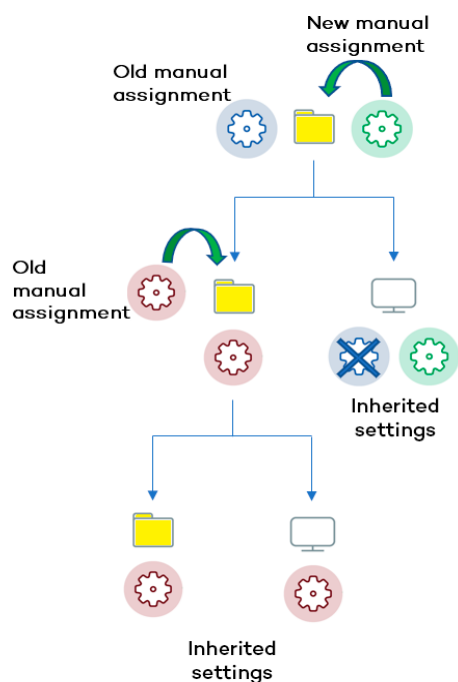


Figure 10.7: Keeping manual settings

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 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, 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 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 console because of a group change in Active Directory, you must manually assign network settings.

Settings received 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 security software remotely, partners send setting to their customers. These settings are shown in the management console with the label Panda Partner Center.

Features of the settings sent by partners

By default, settings sent by partners cannot be edited or deleted from 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 the partner](#) on page 280 and [Software authorized by a partner](#).

Requirements

To receive settings sent by a partner, follow these steps:

- Select **Settings (1)** from the top menu. Select **Users (2)** from the left panel.
- Select the **Users** tab. Select **Allow my reseller to access my console(3)**.

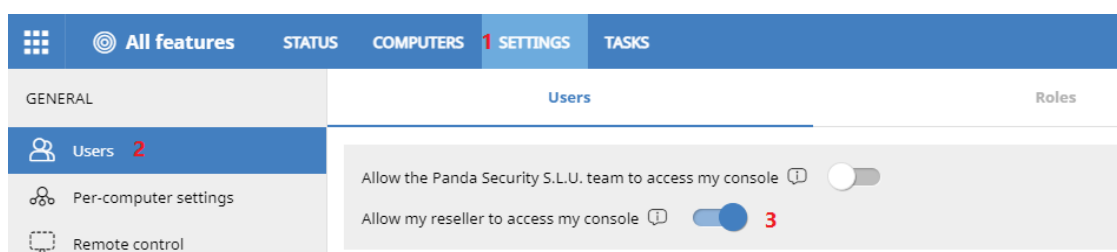



Figure 10.8: Option **Allow my reseller to access my console**

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 201 for more information.

Chapter 11

Configuring the agent remotely

Administrators can configure various aspects of the Panda agent installed on the computers on their network from the web console:

- Define a computer's role towards the other protected workstations and servers.
- Protect the Panda Endpoint Protection client software from unauthorized tampering by hackers and advanced threats (APTs).
- Define the visibility of the agent on the workstation or server, and 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	260
Proxy role	260
Cache/repository role	261
Discovery computer role	263
Configuring proxies lists for Internet access	264
Configuring downloads from cache computers	266
Requirements for using a cache computer	267
Configuring real-time communication	268
Configuring the agent language	269
Configuring the agent visibility	269
Configuring Secure VPN	270

Requirements	270
Requirements checking	271
Accessing the Secure VPN settings	271
Configuring the anti-tamper protection and password	272
Anti-tamper protection	272
Password-protection of the agent	272
Configuring Shadow Copies	273
Accessing the Shadow Copies feature	274

Configuring the Panda agent role

The Panda agent installed on the Windows computers on your network can have three roles:

- Proxy
- Discovery computer
- Cache

To assign a role to a computer with the Panda agent installed, click the **Settings** menu at the top of the console. Then, select **Network services** from the menu on the left. Three tabs appear: **Panda Proxy**, **Cache**, and **Discovery**.



Only computers that use the Windows operating system can take on the Proxy, Cache, or Discovery Computer roles.

Proxy role

Panda Endpoint Protection enables you to use the proxy installed on the organization's network to access the Panda cloud. We recommend that you use a computer with the Panda Endpoint Protection proxy role assigned only for isolated computers which do not have access to a corporate proxy.



Proxy computers cannot download patches or updates through the Panda Patch Management module. Only computers with direct access to the Panda Security cloud or with indirect access through a corporate proxy can download patches.

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.


Requirements for designating a computer as a proxy

- Windows operating system and Panda Endpoint Protection 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](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 open for inbound and outbound connections.
- The proxy computer name must be resolved from the computer that uses it.

Designating a computer as a proxy

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Proxy** tab. A list appears with all computers that have been designated as a proxy.
- Click **Add proxy server**. A window opens with all computers managed by Panda Endpoint Protection 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 proxy

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Proxy** tab. A list appears with 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/repository role

Panda Endpoint Protection 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 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.

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 node 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 downloads all necessary files to keep its repository automatically synchronized. All other computers on the same subnet contact the cache computer for 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.

Next to the computer you want to remove from the list, click .

Specifying the storage drive

You can configure the Panda Endpoint Protection 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.

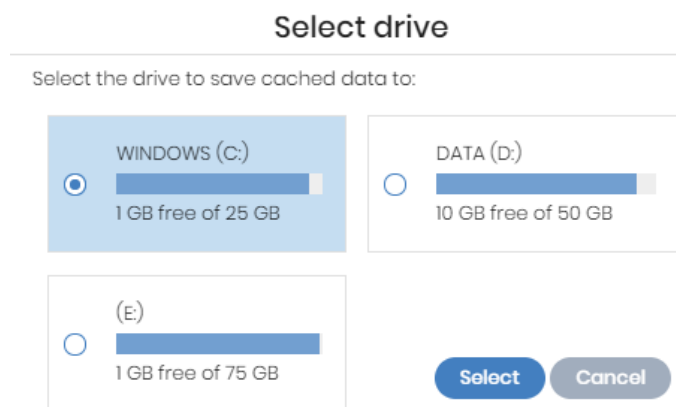


Figure 11.1: Volume selection window for a cache computer

- To view the space on a drive, point the mouse at the tile. 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 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 server. If the drive has not reported its status, the drive that stores the Panda Endpoint Protection 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 across a customer's network.



See [Computer discovery](#) on page 103 for more information about the Panda Endpoint Protection discovery and installation processes.

Configuring proxies lists for Internet access

Panda Endpoint Protection 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.

To this end, Panda Endpoint Protection supports various Internet access methods which can be configured by the administrator and which the solution turns to when it needs to connect to the Panda Security cloud. After being selected, the access method continues to be used until it becomes unavailable, at which point Panda Endpoint Protection moves on to the next method in the list until it finds one that is valid. After it gets to the end of the list, it goes back to the beginning until all connection methods have been tried at least once.

The connection types supported by Panda Endpoint Protection are as follows:

Proxy type	Description
Do not use proxy	Direct access to the Internet. Computers access the Panda Security cloud directly to download updates and report their status. If you select this option, the Panda Endpoint Protection software communicates with the Internet using the computer settings.
Corporate proxy	Access to the Internet through a proxy installed on the company's network. <ul style="list-style-type: none"> • 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.
Panda Endpoint Protection proxy	Access through the Panda Endpoint Protection agent installed on a computer on the network. This option centralizes all network communications through a computer with the Panda agent installed. To configure a computer to access the Internet through a Panda Endpoint Protection proxy, click the Select computer link. A window

Proxy type	Description
	opens with a list of all available computers on the network with the proxy role. Select one of the computers and click the Add button.






Table 11.1: Types of Internet access methods supported by Panda Endpoint Protection



You can configure an access list consisting of multiple computers with the proxy role. To do this, first assign the Panda Endpoint Protection proxy role to one or more computers on the network with Panda Endpoint Protection installed, using the steps described in [Designating a computer as a proxy](#).

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 ([Table 1.1:](#)) 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 mechanism

If a Panda agent is unable to connect to the Aether platform despite having tried all connection methods in its configured access list, it will use the following fallback mechanism to restore the connection by other means:

- Direct connection: Panda Endpoint Protection tries to connect directly to the Panda Security cloud, if this option was not previously configured in the access list.
- Internet Explorer: Panda Endpoint Protection tries to retrieve the computer's Internet Explorer proxy settings with the profile of the user currently logged in to the computer.

- If the proxy requires explicit credentials, this method cannot be used.
- If Internet Explorer is configured to use a PAC (Proxy Auto-Config) file, the agent will use the URL in the configuration file, provided the resource access protocol is HTTP or HTTPS.
- WinHTTP: Panda Endpoint Protection reads the default proxy settings.
- WPAD: The solution queries the network using DNS or DHCP to retrieve the discovery URL that points to the PAC configuration file, if this option was not previously configured in the access list.

The computer will try to exit the fallback mechanism multiple times per day, checking the access list configured by the administrator. This way, it checks to see whether the connection mechanisms defined for the computer are available again.

Configuring downloads from cache computers



Access to computers designated as a cache to speed up updates and patch downloads is only available for Windows computers.

There are two ways to use computers with the cache role:

- **Automatic mode:** In this mode, a computer that starts a download uses cache computers found on the network that meet the requirements specified in section **Automatic mode**. 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 nodes differ from automatically selected ones in the following aspects:
 - When a computer has multiple cache nodes 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 cache computer

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 and redirect their update requests to it.
- In addition to being on the same subnet, 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 nodes

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 nodes receive the notification and connect to the cache computer. If there is more than one designated cache node on a network segment, computers on the subnet connect to the most appropriate node based on the amount of free resources it has.

Occasionally, computers on the network set to automatically detect cache nodes check whether there are new nodes with the cache role.

Configuring the assignment method for cache nodes

- 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 nodes 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 nodes. Computers that receive these settings connect to the cache nodes specified in the list.

Configuring real-time communication

Panda Endpoint Protection 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 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 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 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 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.

Configuring Secure VPN

Secure VPN provides an additional layer of protection for VPN connections between remote computers and corporate networks.

A computer trying to connect to a VPN network must meet a series of requirements for the Firebox to allow the connection. If it does not meet those requirements, the connection is rejected.

The Panda agent installed on the computer collects and sends the information that the Firebox needs to perform the necessary checks.

UUID validation and generation mechanism

A UUID (Universal Unique Identifier) is a character string used to uniquely identify a device.

The mechanism the Firebox uses to validate VPN connections is a UUID + password. This means you must configure the same UUID-password pair in the Firebox and in the Panda Endpoint Protection console.

If you have not configured a UUID in your Firebox yet, you must generate a new one. Because this is an open format, there are many UUID generators available for free online. For example: <https://www.uuidgenerator.net/>

Use a long password that includes upper case, numeric, and special characters.



For more information about the Firebox and its VPN connection settings, see https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/services/tdr/tdr_host_sensor_enforcement_configure.html

Requirements

To use Secure VPN with the Firebox, the computer from which the VPN connection is to be established must meet the following requirements:

- Have protection installed and running.
- You must configure a valid UUID and authentication key in both the Firebox and the Panda Endpoint Protection console.
- Operating system: Windows 8.1 or higher.
- Ports: For Secure VPN to work, the Panda agent installed on the computer must be able to communicate with the Firebox over port 33000.

- Valid protection settings: Panda Endpoint Protection antivirus protection enabled and running.



Secure VPN is not compatible with Linux or macOS. If you enable this feature, computers with these operating systems or versions lower than Windows 8.1 cannot connect to a VPN.

Requirements checking

When a computer tries to connect to a corporate VPN network, the Firebox takes the following actions:

- Requests information about the status of the protection installed on the computer.
- Verifies that the account UUID and the authentication key are valid. Both are available in the Firebox settings used to connect to the VPN.
- Verifies that the computer operating system is valid, by comparing it to the operating systems in its settings.

If all checks turn out positive, the Firebox allows access from the computer to the corporate VPN network. Otherwise, it rejects the connection.



By default, all computers are forced to comply with the security requirements for establishing a VPN connection through the Firebox.

Accessing the Secure VPN settings

To enable Secure VPN, follow these steps:

- From the side menu, select **Network services**.
- From the tab menu, select **Secure VPN**.
- To enable the protection, click the toggle.
- Enter the account UUID and the authentication key.
- Click **Save changes**.

Configuring the anti-tamper protection and password

Anti-tamper protection

Many advanced threats use techniques for disabling the security software installed on computers. The anti-tamper protection prevents unauthorized modification of the way the protection works, protecting the software from being stopped, paused, or removed, with a password.

The Panda Endpoint Protection anti-tamper protection works as follows:

- The default **Per-computer settings** profile provided by the solution include a unique, predefined password for each customer. This password cannot be changed as all default settings profiles are read-only.
- The **Per-computer settings** profiles generated by users allow the anti-tamper protection to be enabled or disabled according to the organization's needs.

The passwords set when creating security settings profiles must be between 6 and 15 characters long.

Enabling/disabling the anti-tamper protection

- 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.
- Expand the **Security against unauthorized protection tampering** section:
 - **Enable Anti-Tamper protection**: Prevents users and certain types of malware from stopping the protections. Enabling this option requires setting up a password which will be required if, for example, the administrator or a support team member needs to temporarily disable the protection from a computer's local console to diagnose a problem. Use the toggle at the right to enable and disable this feature in the settings profiles you create.



*If you disable the **Enable Anti-Tamper protection** or **Request password to uninstall the protection from computers** toggles, a security warning is shown when saving the settings. We do not recommend disabling these security options.*

Password-protection of the agent

Administrators can set up a local password to prevent users from changing the protection features or completely uninstalling the Panda Endpoint Protection software from their computers.

Setting up the local password

- 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.
- Expand the **Security against unauthorized protection tampering** section:
 - **Request password to uninstall Aether from computers:** Prevents users from uninstalling the Panda Endpoint Protection software, protecting it with a password.
 - **Allow the protections to be temporarily enabled/disabled from a computer's local console:** Enables administrators to manage a computer's security parameters from its local console. Enabling this option requires setting up a password.



If a computer loses its license because it is manually removed or because it expires or is canceled, the anti-tamper protection and password-based uninstallation protection are disabled.

Configuring Shadow Copies

Shadow Copies is a technology included in Microsoft Windows that enables you to transparently create backup copies of the files stored on a user computer.

From the Panda Endpoint Protection console, you can centrally and remotely interact with the 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

Panda Endpoint Protection complements the Shadow Copies service included in Microsoft Windows with additional features to protect user data from threats:

- Configure and manage a backup (snapshot) repository separately from other repositories the user might have created.
- Protect 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 from being deleted.
- Specify the percentage of hard disk space you want to use for backup copies (this is 10% by default).
- Make a backup copy of the files every 24 hours. The first copy is made when you enable the feature (it is disabled by default).

- Save up to seven copies of each file, 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 and higher.
 - Windows 2003 Server and 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

- Select the **Settings** menu at the top of the console. Select **Per-computer settings** from the side menu. A list appears with all created settings profiles.
- Click an existing 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 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 disk space set in the management console has priority over other settings established by the network administrator.

Using filters to find computers with Shadow Copies enabled

- Select the **Computers** menu at the top of the console.
- From 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** window 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 187

Chapter 12

Security settings for workstations and servers

Configure security settings profiles for workstations and servers to define how Panda Endpoint Protection 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 **247**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

[Controlling and monitoring the management console](#) on page **55**: 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	278
Introduction to the security settings	278
General settings	279
Antivirus	281
Firewall (Windows computers)	283
Device control (Windows computers)	292

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 12.1: Permissions required to access the Workstations and servers settings

Introduction to the security settings

The parameters for configuring the security of workstations and servers are divided into various sections. 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.

Table 12.2: Available modules in Panda Endpoint Protection

Not all features are available for all supported platforms. This table provides a summary of the features in Panda Endpoint Protection 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	X
Device control	X		

Table 12.3: Supported security features by platform

(1) Mail filtering for Microsoft Exchange servers is only available for customers who purchased Panda Endpoint Protection version 3.72.00 or earlier.

General settings

The general settings enable you to configure how Panda Endpoint Protection behaves with respect to updates, the removal of competitor products, and file and folder exclusions from scans.

Local alerts

Field	Description
Show malware, firewall, and device control alerts	In the text box, type a custom message to include in the alert. The Panda Endpoint Protection agent shows a pop-up window with the configured text.
Show an alert every time the web access control feature blocks a page	A pop-up window displays on the workstation or server every time Panda Endpoint Protection blocks a web page.

Table 12.4: Fields in the Local alerts section

Updates



See [Product updates and upgrades](#) on page 175 for more information about how to update the agent, the protection, and the signature file of the client software installed on users' computers.

Uninstall other security products



See [Protection deployment overview](#) for more information about how to configure the action to take if another security product is already installed on users' computers.

See [Supported uninstallers](#) for a complete list of the competitor products that Panda Endpoint Protection uninstalls automatically from users' computers.

Files and paths excluded from scans

Configure items on your computers that will not be deleted or disinfected when scanning for malware.



Exclusions disable antivirus protection for the specified files and file paths. Because this setting can cause potential security holes, we recommend that you only exclude files and paths to resolve performance problems.

Exclusions set by the partner

By default, administrators cannot edit or delete the **Workstations and servers** settings sent by the partner. However, the partner can establish settings as editable, which appear with the tag **Editable Exclusions**. In this case, administrators can add exclusions but they cannot delete or edit the list of exclusions defined by the partner.

If the partner changes the status of the settings sent from editable to non-editable, the exclusions added by users cease to apply, and only those sent by the partner apply. If the partner changes the status once again to editable, the exclusions added by the administrator are restored and applied again.

Exclude the following disk files

Specify the files on the hard disk of your protected computers that will not be deleted or disinfected by Panda Endpoint Protection.

Field	Description
Extensions	Specify the extensions of files that will not be scanned.
Folders	Specify folders whose content will not be scanned. You can use system variables to exclude folders from scans. You cannot exclude folders by using user-created variables.
Files	Specify files that will not be scanned. You can use wildcard characters ? and *. If you do not specify the path to a file, 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. You cannot use wildcards when specifying the full path to a file.
Recommended exclusions for Exchange servers	Click Add to automatically load a series of Microsoft-recommended exclusions to optimize the performance of the product on Exchange servers.

Table 12.5: Disk files that will not be scanned by Panda Endpoint Protection

Exclude the following email attachments

Specify the file extensions of email attachments that will not be scanned.

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.
Mail protection	Enable or disable the antivirus protection for the mail client installed on users' computers. Panda Endpoint Protection detects threats received over the POP3 protocol and encrypted variants.

Field	Description
Web browsing antivirus	Enable or disable the antivirus protection for the web browser installed on users' computers. Panda Endpoint Protection detects threats received over the HTTP protocol and encrypted variants.

Table 12.6: Antivirus protection modules available in Panda Endpoint Protection

When Panda Endpoint Protection detects malware or the Panda Security anti-malware laboratory identifies a suspicious file, Panda Endpoint Protection 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.

Threats to detect

Configure the types of threats that Panda Endpoint Protection 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.

Field	Description
Create Decoy Files to help detect ransomware	Creates bait files on user computers that are permanently monitored by Panda Endpoint Protection. If they are modified, these files identify the process that modified them as ransomware, ending it to prevent mass encryption of the file system.

Table 12.7: Malware types detected by the Panda Endpoint Protection antivirus protection

File types

Specify the types of files to be scanned by Panda Endpoint Protection:

Field	Description
Scan compressed files on disk	Decompresses compressed files and scans their contents for malware.
Scan compressed files in emails	Decompresses email attachments and scans their contents for malware.
Scan all files regardless of their extension when they are created or modified (Not recommended)	Many types of data files do not pose a threat to the security of computer networks. When you enable this option, the solution scans all files when they are created or modified. For best performance, we recommend that you do not enable this option.

Table 12.8: File types scanned by the Panda Endpoint Protection antivirus protection

Firewall (Windows computers)

Panda Endpoint Protection monitors the communications sent and received by each computer on the network, blocking all traffic that matches the rules defined by 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 select the most appropriate network type.

Network type	Description
Public network	Networks in public places such as airports, Internet cafés, and universities. 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 12.9: Network types supported by the firewall

Panda Endpoint Protection 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 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 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 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.
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 12.10: Types of default actions supported by the firewall for the programs installed on computers

2. **Enable or disable Panda 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 12.1: 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.
Deny all connections	The program cannot connect to the local network or Internet.

Table 12.11: Communication modes for allowed programs

- **Advanced permissions:** Specify parameters of the traffic you want to allow or deny.

Field	Description
Action	<p>Defines the action that Panda Endpoint Protection takes when the examined traffic matches the rule.</p> <ul style="list-style-type: none"> • Allow: Allows the traffic. • Deny: Blocks the traffic. It drops the connection.
Direction	<p>Sets the traffic direction for connection protocols such as TCP.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

Field	Description
Protocol	<p>Establish the layer 3 protocol for the traffic generated by the program you want to control:</p> <ul style="list-style-type: none"> • All • TCP • UDP
IP	<ul style="list-style-type: none"> • 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 12.12: Advanced communication options for allowed programs

Connection rules

Connection rules define traditional TCP/IP traffic filtering. Panda Endpoint Protection 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	<p>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.</p>

Action	Description
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 12.13: Types of default actions supported by the firewall for the programs installed on users' computers

2. **Enable or disable Panda 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 12.2: 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	Select the direction of the traffic to match for connection protocols such as TCP. <ul style="list-style-type: none"> • 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.

Field	Description
Protocol	<p>Select the traffic protocol. The options vary for the protocol you select:</p> <ul style="list-style-type: none"> • TCP, UDP, TCP/UDP: Define TCP and/or UDP rules, including local and remote ports. <ul style="list-style-type: none"> • 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, indicating their type and subtype. • IP Types: Select the higher-level protocols you want to apply the rule to.
IP addresses	<p>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 (-).</p> <p>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.</p>
MAC addresses	<p>Specify the source or target MAC address of the traffic to control.</p>

Table 12.14: 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.
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	<ul style="list-style-type: none"> • 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	Protects the system against UDP port scanning attacks.

Field	Description
Scan	
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	<ul style="list-style-type: none"> • 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.
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 12.15: 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)

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



The device control feature enables you to control the behavior of protected Windows computers when they connect to a removable or mass storage device. You can select the device or devices you want to authorize or block, and specify their usage.

Enabling device control

- Enable the **Enable device control** toggle.
- For each type of device, specify the authorized use.
 - In the case of USB flash drives and CD/DVD drives, you can choose among **Block**, **Allow read access**, or **Allow read & write access**.
 - The options available for Bluetooth and imaging devices, USB modems, and smartphones are **Allow and Block**.

Allowed devices

This section 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 those devices you want to exclude from your previously 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 displays 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 display 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's devices by Panda Endpoint Protection can sometimes lead to confusion or prevent you from correctly identifying them. To resolve this issue, you can assign custom names to devices:

- From the **Allowed devices** section, select the device you want to rename.
- Click the  icon. A window appears requesting you to enter a new name for the device.
- Click **OK**. The **Allowed devices** list is updated with the new name.

Chapter 13

Security settings for mobile devices

The **Settings** menu at the top of the Panda Endpoint Protection console provides the parameters required to configure the security of the smartphones and tablets in the organization. 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 247: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

Controlling and monitoring the management console on page 55: Managing user accounts and assigning permissions.

Chapter contents

Security settings for Android devices	296
Security settings for iOS devices	298

Security settings for Android devices

Accessing the settings

- Select the **Settings** menu at the top of the console.
- Select **Mobile devices** from the side menu.
- 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 13.1: 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 175.

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, click 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's 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

- Select the **Settings** menu at the top of the console. Select **Mobile devices** from the side menu.
- Select the **Android devices** tab. A list appears with 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, see [General section for mobile devices](#) on page 218

Anti-theft protection settings

Field	Description
Report the device's location	The device sends its GPS coordinates to the Panda Endpoint Protection server. Use the toggle to enable or disable this option.
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. Use the toggle to enable or disable this option.

Field	Description
Privacy	Enables users to enable private mode. Private mode disables geolocation tracking. Use the toggle to enable or disable this option.

Table 13.2: Anti-theft features for Android devices

Security settings for iOS devices

Accessing the settings

- Select the **Settings** menu at the top of the console.
- Select **Mobile devices** from the side menu.
- 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 13.3: 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, click the toggles.



This feature is not available for iOS devices not enrolled into an MDM solution. See [Installation on iOS systems](#) on page 128.

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

- Select the **Settings** menu at the top of the console. Select **Mobile devices** from the side menu.
- Select the **iOS devices** tab. A list appears with 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**.



See [General section for mobile devices](#) on page 218 for more information about the anti-theft actions available in Panda Endpoint Protection.

Anti-theft protection settings

Field	Description
Behavior	The device sends its GPS coordinates to the Panda Endpoint Protection server. Use the toggle to enable or disable this option.
Privacy	Enables users to enable private mode. Private mode disables geolocation tracking. Use the toggle to enable or disable this option.

Table 13.4: Anti-theft features for iOS devices

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, preventing malware from taking advantage of the software flaws that may affect the organization's workstations and servers in order to infect them.

Panda Patch Management supports Windows operating systems. It detects both third-party applications with missing patches or in EOL (End-Of-Life) stage, as well as all patches and updates published by Microsoft for all of its products (operating systems, databases, Office applications, etc.).



Windows XP SP3 and Windows Server 2003 SP2 computers require a computer with the cache/repository role on the same subnet in order to detect and install missing patches. Windows XP SP3 and Windows Server 2003 SP2 computers cannot download patches even if they have the cache/repository role assigned.

Panda Patch Management is not compatible with Windows ARM systems.

For more information about the Panda Patch Management module, see:



Creating and managing settings profiles on page 247: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

Controlling and monitoring the management console on page 55: Managing user accounts and assigning permissions.

Managing lists on page 45: Information about how to manage lists.

Chapter contents

Panda Patch Management features	302
General workflow	303
Configuring the discovery of missing patches	315
Panda Patch Management widgets/panels	317
Panda Patch Management module lists	329

Panda Patch Management features

You can access the features provided by Panda Patch Management from the following sections in the management console:

- **To configure the discovery of missing patches:** Go to the **Patch management** settings section (top menu **Settings**, side panel). See [Configuring the discovery of missing patches](#) for more information.
- **To configure patch exclusions:** Go to the **Available patches** list. See [Exclude patches for all or certain computers](#) for more information.
- **To have visibility into the update status of the entire IT network:** Go to the **Patch Management** dashboard (top menu **Status**, side panel). See [Patch management status](#) for more information.
- **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**). See [End-of-Life programs](#) for more information.
- **To view a history of all installed patches:** Check the **Installation history** list (top menu **Status**, side panel **My lists - Add**). See [Installation history](#) for more information.
- **To patch computers:** From the **Tasks** 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 and from **Computer details**. See [Download and install the patches](#) for more information.

- **To uninstall patches:** Select one of the following options:
 - From the **Last patch installation tasks** widget, click the **View installation history** link. See [Last patch installation tasks](#) for more information.
 - Go to the **Status** menu at the top of the console. Click **My lists - Add** and select the **Installation history** list. See [Installation history](#) for more information.
 - Go to the **Tasks** menu at the top of the console. 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 with the patch details and the **Uninstall** button if the patch supports this option. See [Uninstalling a patch](#) for more information.

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 to manage the service correctly. See [General options](#) for more information.

Make sure that all published patches are installed

As software vendors discover flaws in their products, they publish updates and patches that must be installed on the affected systems in order to fix them. These patches have a criticality level and type associated to them:

- To view missing patches by type and criticality level, use the [Patch criticality](#) widget.
- To view details of the patches that are missing on a computer or computer group:
 - Go to the computer tree (top menu **Computers**, **Folder** tab in the side panel). Click the context menu of a computer group containing Windows computers. 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 the patches

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



The patches released by Microsoft will not be installed successfully if the Windows Update service is stopped on the target workstation or server. However, to prevent Panda Patch Management from overlapping with Windows Update, it is recommended that Windows Update be set to be inactive on the computer. See [General options](#) on page 316.

Patches and updates are installed through quick tasks and scheduled tasks. Quick tasks install patches in real time but do not restart the target computer, even though this may be required in order to complete the installation process. Scheduled tasks enable you to configure all parameters related to the patch installation operation. See [Tasks](#) on page 469 for more information about tasks in Panda Endpoint Protection.

Patch download and bandwidth savings

Prior to installing a patch, it must be downloaded from the software vendor's servers. This download takes place in the background and separately on each computer when the installation task is launched. To minimize bandwidth usage, the module leverages the cache/repository node infrastructure implemented on the customer's network.



Proxy nodes cannot download patches or updates. See [Configuring the Panda agent role](#) on page 260 for more information about roles in Panda Endpoint Protection.

Nodes with the cache/repository role store patches for a maximum of 30 days; After then, the patches are deleted. If a computer requests a patch from a cache node, but the node does not have the patch in its repository, the computer waits for the cache node to download it. The wait time depends on the size of the patch to download. If the node cannot download the patch, the computer tries to download it directly instead.

After a patch has been applied to a target computer, it is deleted from the storage media where it resides.

Installation task sequence

Patch installation tasks may require downloading patches from the vendor's servers if the nodes on the network with the cache/repository role do not already have the relevant patches. In this scenario, please note that quick tasks start downloading the necessary patches as soon as they are created. This could result in high bandwidth usage if those tasks affect many computers or there is a large amount of data to download.

In contrast, scheduled patch installation tasks start downloading the necessary patches when configured in the settings. However, if the start time of multiple tasks coincides, the module

introduces a short random delay of up to 2 minutes to prevent downloads from overlapping and minimize bandwidth usage to a certain extent.

Interrupting patch installation tasks

You can interrupt patch installation tasks if the installation process has not started yet on the target computers. If the installation process has already begun, however, you cannot cancel the task as doing so could cause errors on computers.

Patch download strategies

The management console is a very flexible tool that enables you to install patches in multiple ways. Generally, you can apply the following strategies:

- To install one or more specific patches, use the **Available patches** list and configure the filter tool.
- To install all patches of a certain type or with a specific criticality level, use a quick or scheduled task.
- To install patches on a specific computer or computer group, use the group tree.

Next is a description of all possible combinations of patches and targets, along with the steps to take to complete the patch operation in each case.

Target/Patch	One or multiple specific patches	One, multiple, or all types of patches
One or multiple computers	Case 1: From the Available patches list	Case 2: From the computer tree
A group	Case 3: From the Available patches list	Case 4: From the computer tree
Multiple or all groups	Case 5: From the Available patches list	Case 6: From the Tasks top menu

Table 14.1: Patch installation based on the target and the patches to install

Case 1: From the Available patches list

Follow these steps to install one or multiple specific patches on one or multiple computers:

- Go to **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 checkboxes besides the computers-patches you want to install. Select **Install** from the action bar to create a quick task, or **Schedule installation** to create a scheduled task.

Case 2: From the computer tree

Follow these steps to install one, multiple, or all types of patches on one or multiple computers:

- Go to **Computers** in the top menu. Click the **Folders** tab in the computer tree (left panel). Select the group that the target computers belong to. If the target computers belong to multiple groups, click the All root group.
- Click the checkboxes besides the computers that the patches will be applied to.
- From the action bar, click **Schedule patch installation**.
- Configure the task, click the **Save** button, and publish it.

Case 3: From the Available patches list

Follow these steps to install a specific patch on a computer group:

- Go to **Computers** in the top menu. Click the **Folders** tab in the computer tree (left panel). Click the target group's context menu.
- Click the **View available patches** option. The **Available patches** list opens, filtered by the relevant group.
- Use the **Patch** field in the filter tool to list only the patch you want to install.
- Select all computers in the list by clicking the relevant checkboxes.
- Click **Install** from the action bar to create a quick task, or **Schedule installation** to create a scheduled task.

To install multiple specific patches on a group of computers, repeat these steps as many times as patches you want to install.

Case 4: From the computer tree

Follow these steps to install one, multiple, or all types of patches on a computer group:

- Go to **Computers** in the top menu. Click the **Folders** tab in the computer tree (left panel). Click the target group's context menu.
- Click the **Schedule patch installation** option. The task settings page opens.
- Configure the task, indicating the type or types of patches that will be installed on the group. Click the **Save** button and publish it.

Case 5: From the Available patches list

Follow these steps to install a specific patch on multiple computer groups:

- Go to **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 find the patch to install.

- Click the checkbox besides the patch you want to install. Click **Schedule installation** to create a task.
- Go to top menu **Tasks**. Edit the task you have just created.
- In the **Recipients** field, add the groups that the patch will be applied to (use the **Computer groups** section to do this). Remove any additional computer that may appear in the **Additional computers** section.
- Click **Back**. Finish configuring the task. Click **Save**.
- Publish the task.

To install multiple specific patches on multiple computer groups, repeat these steps for all the patches you want to install.

Case 6: From the Tasks top menu



To manage **Install patches** tasks, the user account used to access the web console must have the **Install, uninstall, and exclude patches** permission assigned to its role. For more information about the permission system in Panda Endpoint Protection, see [Understanding permissions](#) on page 59.

Follow these steps to install one, multiple, or all types of patches on multiple or all computer groups:

- Go to **Tasks** in the top menu. Click **Add task**. Select **Install patches**.
- Set the **Recipients** field, indicating the computers and groups that the patches will be applied to.
- Schedule the task. See [Task schedule and frequency](#) on page 472 for more information.
- Specify the criticality level of the patches you want to install.
- Specify which products are to receive patches by selecting the relevant checkboxes in the product tree. Because the product tree is a dynamic resource that changes over time, keep the following rules in mind when selecting items from the tree:
 - Selecting a node also selects all of its child nodes and all items dependent on them. For example, selecting Adobe also selects 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. In addition to this, if, later, Panda Patch Management adds a new program or family to the Adobe group, that program or family is selected as well. In contrast to this, if you manually select a number of child nodes from the Adobe group, and later Panda Patch Management

adds a new child node to the group, this is not automatically selected.

- The programs to patch are evaluated at the time when tasks are run, not at the time when they are created or configured. For example, if Panda Patch Management adds an entry to the tree after the administrator has created a patch task, and that entry is selected automatically in accordance with the rule in the previous point, the task installs the patches associated with that new program when run.
- Set the restart options in case the target workstations or servers need to be restarted to finish installing the patch.
 - **Do not restart automatically:** Upon completing the patch installation task, a window is displayed to the user with the options **Restart now** and **Remind me later**. If the latter is selected, a reminder is displayed 24 hours later.
 - **Automatically restart workstations only:** Upon completing the patch installation task, a window is displayed to the user with the **Restart now** option, a **Minimize** button, and a **4-hour countdown timer**. This window is maximized every 30 minutes as a reminder to the user. Less than one hour before the restart, the minimize button is disabled. 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** and publish the task.

Download patches manually

In some cases, Panda Endpoint Protection 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 Endpoint Protection shows a link that you can use as a reference to find and download the patch. If the link is not helpful, contact the vendor of the software to patch. For more information, see <https://www.pandasecurity.com/en/support/card?id=700111>.

For these patches, you can download the patch manually and add it to the patch repository so other computers can install it.

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

- Select the **Status** menu at the top of the console. Click **Add** from the **My lists** side panel. A list is shown with all available lists.
- Click the **Available patches** list. Configure the following 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 **Available patches** 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 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 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. See [Specifying the storage drive](#) for more information.

- 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, you can **mark the patch as manually downloaded** from the **Available patches** list.
- 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. See [Download and install the patches](#) for more information.




Panda Patch Management does not check if 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 the following 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 is removed 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.

Requirements for uninstalling an installed patch

- You must have the **Install/Uninstall patches** permission enabled. See [Install, uninstall, and exclude patches](#) for more information.
- The patch must have been successfully installed.
- The patch must support the rollback feature. Not all patches support this feature.

Uninstalling a patch

- Go to the patch uninstallation 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](#) on page [322](#) 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

- Go to the **Settings** menu at the top of the console. Select **Patch management** from the side menu.
- 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 the Patch management settings profiles.

Table 14.2: Permissions required to access the Patch management settings

General options

- Click **Disable Windows Update on computers** for Panda Patch Management to manage updates exclusively and without interfering with the local Windows Update settings.
- Click the **Automatically search for patches** toggle to enable the patch search functionality. If the toggle is disabled, the lists in the module do not display missing patches, although you can still apply them through the patch installation tasks.

Search frequency

Search for patches with the following frequency indicates how frequently Panda Patch Management checks for missing patches on your computers using its cloud-hosted patch database.

Patch criticality

Sets the criticality of the patches that Panda Patch Management looks for in the databases of available patches.



The criticality level of patches is defined by the vendor of the software affected by the vulnerability. The classification criteria are not universal. We recommend that, prior to installing a patch, you check its description, especially for those patches not classified as 'critical'. This way, you can choose to install the patch or not depending on whether you are suffering the symptoms described.

Panda Patch Management widgets/panels

Accessing the dashboard

To access the dashboard, click 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	<ul style="list-style-type: none"> Patch management status Time since last check
Install, uninstall, and exclude patches	<ul style="list-style-type: none"> End-of-Life programs Available patches Last patch installation tasks
View available patches	<ul style="list-style-type: none"> End-of-Life programs Available patches Last patch installation tasks

Table 14.3: Permissions required to access the Patch management widgets

Patch management status

Shows 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.

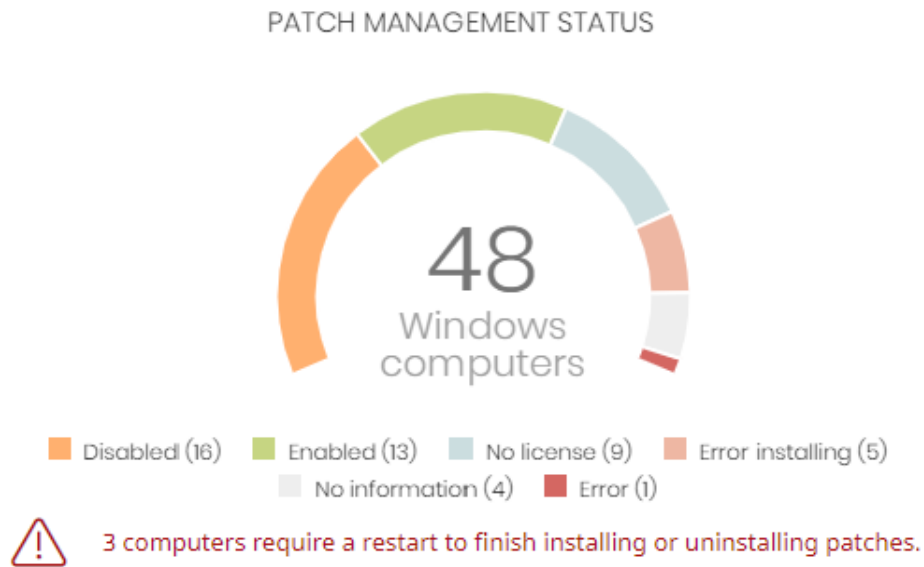


Figure 14.1: Patch management status panel

Meaning of the data displayed

Data	Description
Enabled	Shows the percentage of computers where Panda Patch Management was installed successfully, is running correctly, and the assigned settings profile enables the module to search for patches automatically.
Disabled	Shows the percentage of computers where Panda Patch Management was installed successfully, is running correctly, but the assigned settings profile prevents the module from searching for patches automatically.
No license	Computers where the patch management service is not working because there are insufficient licenses or because an available license has not been assigned to the computer.
Error installing	Shows computers where the module could not be installed.
No information	Computers that have just received a license and have not reported their status to the server yet, and computers with an outdated agent.
Error	Computers where the Panda Patch Management module does not respond to the requests sent from the server, or its settings are different from those defined in the web console.
Central area	Shows the total number of computers compatible with the Panda Patch

Data	Description
	Management module.
Pending restart	Shows the number of computers that require a restart to finish installing or uninstalling patches.

Table 14.4: Description of the data displayed in the Patch management status panel

Lists accessible from the panel

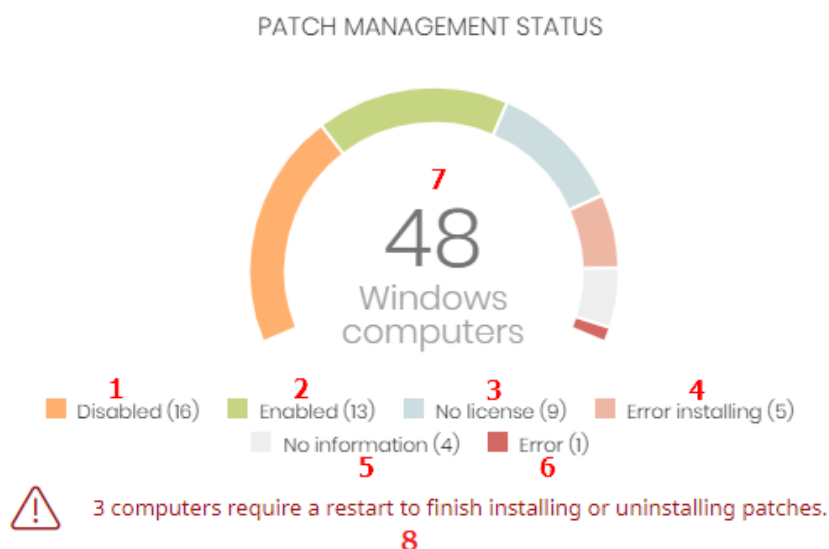


Figure 14.2: Hotspots in the Patch management status panel

Click the hotspots shown in **Figure 14.2:** to access the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Patch management status = Disabled.
(2)	Patch management status = Enabled.
(3)	Patch management status = No license.
(4)	Patch management status = Error installing.
(5)	Patch management status = No information.
(6)	Patch management status = Error.

Hotspot	Filter
(7)	No filter.
(8)	Patch management status = Pending restart.

Table 14.5: Filters available in the Patch management status list

Time since last check

Shows computers that have not connected to the Panda Security cloud to report their patch status for a certain amount of time. These computers are susceptible to security problems and require special attention from you.

TIME SINCE LAST CHECK



Figure 14.3: Time since last check panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported their patch status in the last 72 hours.
7 days	Number of computers that have not reported their patch status in the last 7 days.
30 days	Number of computers that have not reported their patch status in the last 30 days.

Table 14.6: Description of the data displayed in the Time since last check panel

Lists accessible from the panel

TIME SINCE LAST CHECK



Figure 14.4: Hotspots in the Time since last check panel

Click the hotspots shown in [Figure 14.4](#): 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 = Enabled or Disabled or No information or Error.

Table 14.7: Filters available in the Patch management status list

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.

END-OF-LIFE PROGRAMS



Figure 14.5: End-of-Life programs panel

Meaning of the data displayed

Data	Description
Currently in EOL	Programs on the network that have reached their EOL.
In EOL (currently or in 1 year)	Programs on the network that have reached their EOL or will reach it in a year.
With known EOL date	Programs on the network with a known EOL date.

Table 14.8: Description of the data displayed in the End-of-Life programs panel

Lists accessible from the panel

END-OF-LIFE PROGRAMS




Figure 14.6: Hotspots in the End-of-Life programs panel

Click the hotspots shown in [Figure 14.6](#): to access the **End-of-Life programs** list with the following predefined filters:

Hotspot	Filter
(1)	End-of-Life date = Currently in EOL.
(2)	End-of-Life date = In EOL (currently or in 1 year).
(3)	End-of-Life date = All.

Table 14.9: Filters available in the End-of-Life programs list

Last patch installation tasks



See [Task management](#) on page [475](#) for more information about how to edit an existing task.

Shows a list of the last patch installation tasks created. This widget displays multiple links through which you can manage the patch installation tasks:

LAST PATCH INSTALLATION TASKS

-  [Install .NET Framework 4.5.1 \(6.3\) patch on 6 computers](#) In progress
-  [New task \(Install patches\): Install patches with the following criticality](#) In progress

[View all](#) [View installation history](#)

Figure 14.7: Last patch installation tasks panel

- Click a task to edit its settings.
- Click the **View all** link to access the top menu **Tasks**. There you can see all the patch installation tasks that have been created.
- Click the **View installation history** link to access the **Installation history** list. There you can see the patch installation tasks that have finished successfully or with errors.
- Click the context menu associated with a task to display a drop-down menu with the following options:
 - **Cancel**: Interrupts the task before starting to install patches on the target computer.
 - **View results**: Shows the task results.

Available patches

Shows the number of computer-missing patch pairs on the network, sorted by patch type. Each missing patch is counted as many times as there are computers that do not have it installed.

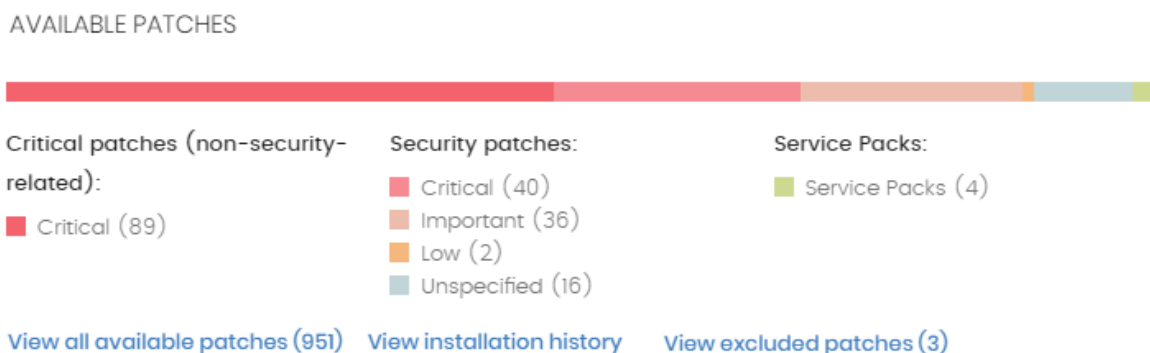


Figure 14.8: Available patches panel

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches rated 'Critical' and pending application.
Security patches - Important	Number of security patches rated 'Important' and pending application.
Security patches - Low	Number of security patches rated 'Low' and pending application.
Security patches - Unspecified	Number of security patches that do not have a severity rating and are pending application.
Other patches (non-	Number of non-security patches that are pending application.

Data	Description
security related)	
Service Packs	Number of patch and hotfix bundles that are pending application.
View all available patches	Number of patches of any severity, related or not to system security, and which are pending application.
View excluded patches	Number of patches excluded from installation.

Table 14.10: Description of the data displayed in the Available patches panel

Lists accessible from the panel

AVAILABLE PATCHES

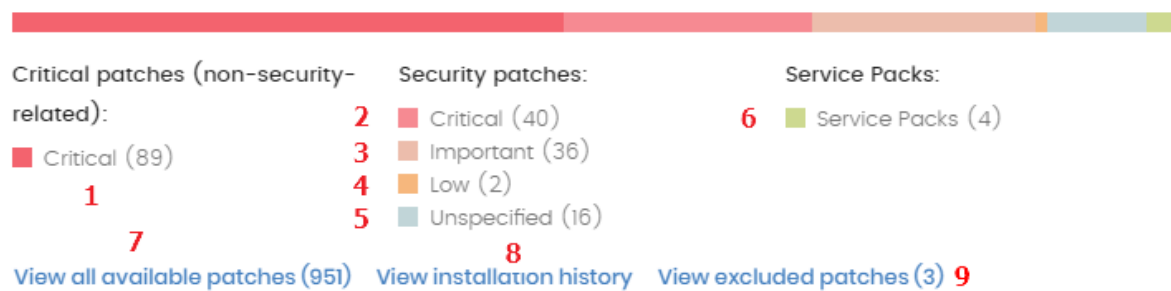


Figure 14.9: Hotspots in the Available patches panel

Click the hotspots shown in [Table 1.8](#): 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).
(5)	Available patches	Criticality = Other patches (non-security-related).
(6)	Available patches	Criticality = Service Pack.

Hotspot	List	Filter
(7)	Available patches	No filter.
(8)	Installation history	No filter.
(9)	Excluded patches	No filter.

Table 14.11: Filters available in the Available patches list

Most available patches for computers

Shows the patches (in **Pending** or **Pending restart** status) available for the largest number of computers.

MOST AVAILABLE PATCHES FOR COMPUTERS



The .NET Framework...	Cumulative Sec...	SQL Se...	Vulne...	Notep...	Java 8...	Micro...	Notep...
18	16	10	9	9	9	9	9
Microsoft .NET Fram...	Microsoft .NET F...	Network I...	Micro...	Secur...	Java 8...	Sec...	Tim...
18	14	8	7	7	7	6	6
Microsoft security a...	Microsoft .NET F...	Security O...	Securit...	Securit...	Sec...	Q...	S...
16	14	8	6	4	4	3	3
Cumulative Security ...	Vulnerability in ...	Firefox 61....	Securit...	Securit...	Octo...	Se...	Hy...
16	13	7	5	4	3	3	3
Google Chrome 67.0...	Firefox 61.0 x64	Compatibi...	Update...	Updat...	Cum...	Se...	Vul...
16	12	7	5	4	3	3	3
		Java 8 Upd...	Securit...	Stop er...	Secur...		
		7	5	4	3	2	2

Figure 14.10: Most available patches for computers panel

Meaning of the data displayed

Microsoft .NET Fram... 1	Google Chrome... 16
2 18	
The .NET Framework... 18	Microsoft .NET F... 14

Figure 14.11: Hotspots in the Most available patches for computers panel

Data	Description
Patch name (1)	Name of the available patch.
Number of computers (2)	Number of computers that have the patch available (in Pending or Pending restart status).

Table 14.12: Description of the data displayed in the Most available patches for computers panel

Click any of the files in the panel to open the **Available patches** list.

Point the mouse to a file in the panel to display a tooltip with the following information:

- Patch name.
- Number of computers that have the patch available.
- Program (or operating system family).
- Criticality.
- Release date.
- CVE (Common Vulnerabilities and Exposures) ID.

Lists accessible from the panel

Click the  icon to open the available filters.

Field	Description	Values
Criticality	Update severity rating and type.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related)

Field	Description	Values
		<ul style="list-style-type: none"> Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack
Computer type	The device type the patch is applied to.	<ul style="list-style-type: none"> Workstation Laptop Server
Patch type	Software type the patch is applied to.	<ul style="list-style-type: none"> App patches Operating system patches

Table 14.13: Filters available in the Most available patches for computers panel

Computers with most available patches

COMPUTERS WITH MOST AVAILABLE PATCHES



WIN_LAPTOP_2	WIN_SERVER_7	WIN_DE...	WIN_LA...	WIN_DE...	WIN_D...	WIN_D...
25	20					
WIN_DESKTOP_10	WIN_SERVER_7	17	16	16	15	14
23	20	WIN_DESKTOP...	WIN_S...	WIN_S...	WIN_...	WIN_...
WIN_LAPTOP_4	WIN_DESKTOP_16	13				
21	19	WIN_DESKTOP...	12	12	12	11
WIN_DESKTOP_14	WIN_SERVER_8	13	WIN_SER...	WIN_DESKTO...	WIN...	
20	18	WIN_DESKTOP...	10	10	7	
	WIN_VIRTUAL_003	12	WIN_VIRT...	WIN_VIRTUAL...	8	WIN...
	18	WIN_SERVER_4	10	WIN_DESKTO...	8	6

Figure 14.12: Computers with most available patches panel

Meaning of the data displayed



Figure 14.13: Hotspots in the Computers with most available patches panel

Data	Description
Computer name (1)	Name of the computer with patches available.
Number of patches available for the computer (2)	Number of patches available for the computer

Table 14.14: Description of the data displayed in the Computers with most available patches panel

Lists accessible from the panel

Click the  icon to open the available filters.

Field	Description	Values
Criticality	Update severity rating and type.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	The device type the patch is	<ul style="list-style-type: none"> • Workstation

Field	Description	Values
	applied to.	<ul style="list-style-type: none"> Laptop Server
Patch type	Software type the patch is applied to.	<ul style="list-style-type: none"> App patches Windows operating system patches

Table 14.15: Filters available in the Computers with most available patches panel

Panda Patch Management module lists

Accessing the lists

There are two ways to access the lists:

- Go to the **Status** menu at the top of the console. Select **Patch Management** from the side menu. Click the relevant widget.
- Or,
- Go 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 a list from the **Patch management** section 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 **Tasks** menu at the top of the console by clicking **View results** in a patch installation or uninstallation task.

Required permissions






Permissions	Access to lists
No permissions	<ul style="list-style-type: none"> Patch management status
Install, uninstall, and exclude patches	<ul style="list-style-type: none"> Access to lists and context menus to install and uninstall patches: Available patches

Permissions	Access to lists
	<ul style="list-style-type: none"> • Installation history • End-of-Life programs • Excluded patches • Patch installation/uninstallation task results • View installed/uninstalled patches
View available patches	<ul style="list-style-type: none"> • Read-only access to lists: • Available patches • Installation history • End-of-Life programs • Excluded patches • Patch installation/uninstallation task results • View installed/uninstalled patches

Table 14.16: Permissions required to access the Patch management lists

Patch management status

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 one of the reasons displayed in the associated panel).

Field	Comment	Values
Computer	Name of the computer with outdated software.	Character string
Computer status	Agent reinstallation: <ul style="list-style-type: none"> •  Reinstalling the agent. •  Agent reinstallation error. Protection reinstallation: <ul style="list-style-type: none"> •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart 	Icon












Field	Comment	Values
	<p>Computer isolation status:</p> <ul style="list-style-type: none">  Computer in the process of being isolated.  Isolated computer.  Computer in the process of stopping being isolated. <p>"RDP attack containment" mode:</p> <ul style="list-style-type: none">  Computer in "RDP attack containment" mode.  Ending "RDP attack containment" mode. 	
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Patch management	Module status.	<ul style="list-style-type: none">  Enabled  Disabled  Installation error (failure reason)  No license  No information  Error
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	Date

Table 14.17: Fields in the Patch management status list



To view a graphical representation of the list data, access the [Patch management status](#) widget.

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Agent version		Character string
Installation date	Date when the Panda Patch Management module was successfully installed on the computer.	Date
Last connection date	Date when the agent last connected to the Panda Security cloud.	Date
Platform	Operating system installed on the computer.	<ul style="list-style-type: none"> • Windows • Linux • macOS • Android

Field	Comment	Values
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.	<ul style="list-style-type: none"> • Enabled • Disabled • Install error • No license • No information • Error
Requires restart	The computer requires a reboot to finish installing 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.	<ul style="list-style-type: none"> • Download error • Execution error

Table 14.18: Fields in the Patch management status exported file

Filter tool

Field	Comment	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	<ul style="list-style-type: none"> • All • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the agent last connected to the Panda Security cloud.	Date
Pending restart to complete patch installation	The computer requires a reboot to finish installing one or more downloaded patches.	Boolean
Patch management status	Module status.	<ul style="list-style-type: none"> • Enabled • Disabled • Install error • No license • No information • Error

Table 14.19: Filters available in the Patch management status list

Computer details page

Click any of the rows in the list to open the computer details page. See [Computer details](#) on page 217 for more information.

Available patches

Shows a list of 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 combination.

Field	Comment	Values
Computer	Name of the computer with outdated software.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the outdated program or Windows operating system 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.	<ul style="list-style-type: none"> • 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:	

Field	Comment	Values
	<ul style="list-style-type: none"> • Pending: The patch is available for the computer but has not been installed yet. • Requires manual download: The patch must be manually downloaded and copied to a cache computer by the administrator. See Download patches manually for more information. • Pending (manually downloaded): The patch has been manually downloaded and is already included in the patch repository. See Download patches manually for more information. • Pending restart: The patch has been installed but the computer has not been restarted. Some patches might not be applied until the computer is restarted. 	
Context menu	<p>Displays an actions menu:</p> <ul style="list-style-type: none"> • 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. • View all available patches for the computer: Displays all available patches for the computer that have not been installed yet. • View which computers have the patch available: Displays all computers that have the patch available for installation. 	

Table 14.20: Fields in the Available patches list



To view a graphical representation of the list data, access the [Available patches](#) widget.

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
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 Windows 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

Field	Comment	Values
Criticality	Update severity rating and type.	<ul style="list-style-type: none"> • 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
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 have access to it.	Boolean

Field	Comment	Values
Download size (KB)	Patch size in compressed format. Applying the patch or update might require more space on the target computer's storage media than indicated in this field.	Numeric value
Status	Indicates the patch installation status: <ul style="list-style-type: none"> • Pending: The patch is available for the computer but has not been installed yet. • Pending (manually downloaded): The patch has been manually downloaded and is already included in the patch repository. See Download patches manually for more information. • Requires manual download: The patch must be manually downloaded and copied to a cache computer by the administrator. See Download patches manually for more information. 	Character string
File name	Name of the file that contains the patch.	Character string
Download URL	HTTP resource for downloading the patch in the software vendor's infrastructure.	Character string

Table 14.21: Fields in the Available patches exported file

Filter tool

Field	Comment	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server
Patch type	Type of patch	<ul style="list-style-type: none"> • App patches • Operating system patches
Search computer	Computer name.	Character string

Field	Comment	Values
Computer	Name of the computer with outdated software.	Character string
Program	Name of the outdated program or Windows 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
Program, family, or vendor	The search applies to the selected program, product family, or company.	Character string
Criticality	Indicates the update severity rating and type.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Displays patches that are in the process of installation, filtering them by the installation stage they are in.	<ul style="list-style-type: none"> • Pending • Requires manual download • Pending (manually downloaded)

Field	Comment	Values
		<ul style="list-style-type: none"> 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 14.22: Filters available in the Available patches list

Patch detected page

Click any of the rows in the list to open the **Patch detected** page. This page can provide the following content:

- Information about the available patch and the **Install patch** button.
- Information about the patch in the process of installation. The text **Pending restart** appears next to the **Install patch** button.

Click the **Install patch** button. A pop-up window appears for you to select the recipients of the patch installation task:

- 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 displayed. 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 Windows 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	Character string

Field	Comment	Values
	installation or a reboot.	
Vendor	The company that created the outdated program.	Character string
Criticality	Indicates the update severity rating and type.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer	Name of the computer with outdated software.	Character string
Installation status	Indicates 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.	<ul style="list-style-type: none"> • 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's storage media than indicated in this field.	Numeric value

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).	Character string
Download URL	URL for downloading the patch individually.	Character string
File name	Name of the file that contains the patch.	Character string

Table 14.23: Fields on the Patch detected page

End-of-Life programs

Shows programs that are no longer supported by the relevant vendor. These programs are particularly vulnerable to malware and cyberthreats.

Field	Comment	Values
Computer	Name of the computer with EOL software.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program reached its end of life.	Date (in red if the program has reached its end of life)

Table 14.24: 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 321 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.	<ul style="list-style-type: none"> • Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program reached its end of life.	Date
Last seen	Date when the computer was last discovered.	Date

Table 14.25: Fields in the End-of-Life programs exported file

Filter tool

Field	Comment	Values
Search computer	Computer name.	Character string
End-of-Life date	Date when the program will reach its EOL.	<ul style="list-style-type: none"> • All • Currently in End of Life • In End of Life (currently or in 1 year)

Table 14.26: Filters available in the End-of-Life programs list

Program details page

Click any of the programs in the list to open the **Program details** page.

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 its end of life.	Date

Table 14.27: Fields on the Program details page

Installation history

Shows the patches that Panda Patch Management tried to install and the computers that received them in a given time interval.

Field	Comment	Values
Date	Date when the patch or update was installed.	Date
Computer	Name of the computer that received the patch or update.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the program or Windows operating system version that received the patch.	Character string
Version	Version of the program or	Character string

Field	Comment	Values
	operating system that received the patch.	
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the patch.	<ul style="list-style-type: none"> • Other patches • Critical • Important • Moderate • Low • Unspecified • Service Pack
Installation	Installation status of the patch or update.	<ul style="list-style-type: none"> • Installed • Requires restart • Error • Uninstalled • The patch is no longer required
Context menu ⋮	Displays a drop-down menu with options.	<ul style="list-style-type: none"> • View task: Shows the settings of the patch installation or uninstallation task. • 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 14.28: Fields in the Installation history list



To view a graphical representation of the list data, see [Last patch installation tasks](#).

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Date	Date of the installation attempt.	Date
Program	Name of the program or Windows operating system version that received the patch.	Character string
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the patch.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related)

Field	Comment	Values
		<ul style="list-style-type: none"> 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
Installation	Installation status of the patch or update.	<ul style="list-style-type: none"> Installed Requires restart Error The patch is no longer required Uninstalled
Installation error	The Panda Patch Management module did not install correctly.	<ul style="list-style-type: none"> Unable to download: Installer not available Unable to download: The file is corrupted Not enough

Field	Comment	Values
		disk space
Download URL	URL for downloading the patch individually.	Character string
Result code	Code indicating the result of the patch installation task. Success or reason for failure. See the vendor's documentation to interpret the result code.	Numeric value

Table 14.29: Fields in the Installation history exported file

Filter tool

Field	Comment	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server
Search computer	Computer name.	Character string
Date	Time period in which the patches were installed.	<ul style="list-style-type: none"> • Last 24 hours • Last 7 days • Last month • Custom range
Criticality	Severity rating of the patch.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related)

Field	Comment	Values
		<ul style="list-style-type: none"> Low (security-related) Unspecified (security-related) Service Pack
Installation	Installation status of the patch or update.	<ul style="list-style-type: none"> Installed Requires restart Error The patch is no longer required Uninstalled
Program	Name of the outdated program installed or Windows operating system version.	Character string
Patch	Name of the installed patch.	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string

Table 14.30: Filters available in the Installation history list

Patch installed page

Click any of the rows in the list to open the Patch installed page. This page provides detailed information about the patch.

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 Windows operating system version with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	<ul style="list-style-type: none"> Other patches



Field	Comment	Values
		(non-security related) <ul style="list-style-type: none"> • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Installation date	Date the patch was successfully installed on the computer.	Date
Result	Installation status of the patch or update.	<ul style="list-style-type: none"> • Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Release date	Date when the patch was released for download and application.	Date

Field	Comment	Values
Download size	Patch size in compressed format. Applying the patch or update might require more space on the target computer's storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and 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 14.31: Fields on the Excluded patch page

Excluded patches

Shows patches that the administrator has marked as excluded, preventing them from being installed on the computers on the organization's network. The list displays a line for each computer-excluded patch pair, except for patches excluded for all computers on the network, for which a single line is displayed.

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 displays the computer name.  If the patch was excluded for all computers in the account, the text "(All)" is displayed.	Character string
Group	Folder in the Panda Endpoint Protection 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

Field	Comment	Values
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the patch.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.32: Fields in the Excluded patches list



To view a graphical representation of the list data, access the [Available patches](#) on page [323](#) widget.

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop

Field	Comment	Values
		<ul style="list-style-type: none"> Server
Computer	<p>The content of this field varies depending on the target of the exclusion:</p> <p>If the patch was excluded for a single computer, the field displays the computer name.</p> <p>If the patch was excluded for all computers in the account, the text "{All}" is displayed.</p>	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	The computer's description assigned by the network administrator.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the patch.	<ul style="list-style-type: none"> Other patches (non-security related) Critical (security-related) Important (security-related) Moderate (security-

Field	Comment	Values
		<ul style="list-style-type: none"> 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
Download size (KB)	Patch size in compressed format. Applying the patch or update might require more space on the target computer's storage media than indicated in this field.	Numeric value
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.33: Fields in the Excluded patches exported file

Filter tool

Field	Comment	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server

Field	Comment	Values
Computer	Name of the computer for which patches have been excluded.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Show non-downloadable patches	Shows 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 describing the vulnerability associated with the patch.	Character string
Criticality	Severity rating of the patch.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.34: Filters available in the Excluded patches list

Excluded patch page

Click any of the rows in the list to open the **Excluded patch** page. This page provides detailed information about the patch excluded from installation tasks.

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 Windows operating system version with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	<ul style="list-style-type: none"> • Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Release date	Date when the patch was released for download and application.	Date

Field	Comment	Values
Download size	Patch size in compressed format. Applying the patch or update might require more space on the target computer's storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and 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 14.35: Fields on the Excluded patch page


Patch installation/uninstallation task results

Shows the results of the patch installation or uninstallation tasks performed on the computers on your network.

Field	Description	Values
Name	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Panda Endpoint Protection group the computer belongs to.	Character string
Status	Task status.	<ul style="list-style-type: none"> • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run

Field	Description	Values
		time exceeded)
Patches installed/uninstalled	Number of patches installed/uninstalled.	Character string.
Start date	Date the installation task started.	Date
End date	Date the installation task ended.	Date

Table 14.36: Fields on the Installation/uninstallation task results page


To view a graphical representation of the list data, see [Last patch installation tasks](#).

Filter tools

Field	Description	Values
Status	Installation/uninstallation task status.	<ul style="list-style-type: none"> • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)

Field	Description	Values
Applied/Uninstalled patches	Computers on which patches have been installed/uninstalled.	<ul style="list-style-type: none"> All No patches installed/uninstalled With patches installed/uninstalled

Table 14.37: Filters available in the Patch installation/uninstallation task results list

View installed/uninstalled patches

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 group the computer belongs to.	Character string
Program	Patched program.	Character string
Version	Program version.	Character string
Patch	Installed/uninstalled patch.	Character string
Criticality	Relevance of the installed/uninstalled patch.	<ul style="list-style-type: none"> Other patches (non-security related) Critical (security-related) Important (security-related) Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack

Field	Description	Values
Result	Indicates whether the task was completed successfully or failed.	<ul style="list-style-type: none">• Installed• Requires restart• Error• The patch is no longer required• Uninstalled
Date	Date the task was run.	Date

Table 14.38: Fields in the View installed/uninstalled patches list



To view a graphical representation of the list data, see [Last patch installation tasks](#).

Chapter 15

Panda Full Encryption (Device encryption)

Panda Full Encryption is a built-in module on Aether platform that encrypts the content of the data storage media connected to the computers managed by Panda Endpoint Protection. By doing this, it minimizes the exposure of corporate data in the event of data loss or theft as well as when storage devices are removed without having deleted the data.

Panda Full Encryption is compatible with certain versions of Windows 7 and later operating systems (see section [Supported operating system versions](#)), and 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, 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 [247](#): Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

[Controlling and monitoring the management console](#) on page [55](#): Managing user accounts and assigning permissions.

[Managing lists](#) on page [45](#): Information about how to manage lists.

Chapter contents

Introduction to encryption concepts	364
Panda Full Encryption service overview	366
General features of Panda Full Encryption	367

Panda Full Encryption minimum requirements	368
Management of computers according to their prior encryption status	368
Encryption and decryption	369
Panda Full Encryption response to errors	374
Getting a recovery key	375
Panda Full Encryption module panels/widgets	378
Panda Full Encryption lists	385
Encryption settings	392
Available filters	394

Introduction to encryption concepts

Panda Full Encryption uses the tools integrated in Windows operating systems to manage encryption on network computers protected with Panda Endpoint Protection.

In order to understand the processes involved in the encryption and decryption of information, we will first present some concepts related to the encryption technology used.

TPM

TPM (Trusted Platform Module) is a chip included in the motherboard of some desktops, laptops, and servers. Its main aim is to protect users' sensitive data, storing passwords and other information used in login processes.

The TPM is also responsible for detecting changes in the chain of startup events on a computer, for example preventing access to a hard drive from a computer other than the one used for its encryption.

The minimum TPM version supported by Panda Full Encryption is 1.2. Panda Security recommends it be used along with other supported authentication systems. In some scenarios, the TPM may be disabled in the computer BIOS and it may be necessary to enable it manually.

Supported password types

PIN

The PIN (Personal Identification Number) is a sequence of numbers that serves as a simple password and is necessary to start a computer with an encrypted drive. Without the PIN, the boot sequence is not completed and it is impossible to access the computer.

Extended PIN

If the hardware is compatible, Panda Full Encryption uses an extended or enhanced PIN combining letters and numbers to increase the complexity of the password.

Because the extended PIN is requested in the computer startup process prior to loading the operating system, BIOS limitations may 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 entering the extended PIN. For this reason, Panda Full Encryption checks that the characters entered by users belong to an EN-US keyboard layout, before setting the extended PIN for the computer encryption process.

Passphrase

A passphrase is similar to a password, but is typically longer. It consists of alphanumeric characters and is equivalent to the extended PIN.

Panda Full Encryption prompts users for a different type of password based on the following circumstances:

- Passphrase: If the computer has a TPM installed.
- Extended PIN: If the computer operating system and hardware support it.
- PIN: If the other options are not valid.

USB key

Enables you to store the encryption key on a USB device formatted with the NTFS, FAT, or FAT32 file system. 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.



Some older PCs cannot access USB drives during the startup process. Check whether the computers in your organization have access to USB drives from the BIOS.

Recovery key

If an anomalous situation is detected on a computer protected with Panda Full Encryption, or you forget the unlock key, the system requests a 48-digit recovery key. This key is managed from the management console and must be entered in order to complete the startup process. Each encrypted drive has its own unique recovery key.



Panda Full Encryption stores the recovery keys only for the computers it manages. The management console does not display the keys for computers encrypted by users or those not managed by Panda Security.

The recovery key is requested in the following scenarios:

- When the PIN or passphrase is entered incorrectly repeatedly in the startup process.
- When a computer protected with TPM detects a change to the startup sequence (hard disk protected with TPM and connected to another computer).

- When the motherboard has been changed and consequently the TPM.
- On disabling or clearing the TPM.
- On changing the computer's startup settings.
- When the startup process is changed:
 - BIOS update.
 - Firmware update.
 - UEFI update.
 - Changes to the boot sector.
 - Changes to the master boot record.
 - Changes to the boot manager.
 - Changes to the firmware (Option ROM) in certain components that are part of the boot process (video cards, disk controllers, etc).
 - Changes to other components that take part in the initial startup phases.

BitLocker

This is the software installed on some versions of Windows 7 and later operating systems and which is responsible for encrypting and decrypting the data stored on the computer drives. Panda Full Encryption installs BitLocker automatically on those server versions that do not have it but are compatible with it.

System partition

This is a small area of the hard disk -approximately 1.5 gigabytes- which is unencrypted and is required for the computer to correctly complete the startup process. Panda Full Encryption automatically creates this system partition if it does not already exist.

Encryption algorithm

The encryption algorithm in Panda Full Encryption is AES-256, though computers with drives encrypted by users with other algorithms are also compatible.

Panda Full Encryption service overview

The general encryption process covers several areas that administrators must be aware of in order 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's computer:** Depending on whether BitLocker was used before on the user's computer, the process of integration in Panda Full Encryption may 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. See [Encryption of previously unencrypted drives](#) for more information.
- **Viewing the encryption status of the network:** Through the widgets/panels accessible through the **Status** menu, **Panda Full Encryption** side panel. See [Panda Full Encryption module panels/widgets](#) for a complete description of the widgets included in Panda Full Encryption. Filters are also supported to find computers in the lists according to their status. See [Available filters](#) for more information.
- **Restriction of encryption permissions to security administrators:** The role system described in [Understanding permissions](#) on page 59 covers the encryption feature and the ability to view the encryption status of network computers.
- **Access to the recovery key:** Where users forget the PIN/passphrase or when the TPM has detected an irregular situation, the network administrator can centrally obtain the recovery key and send it to the user. See [Getting a recovery key](#) for more information.

General features of Panda Full Encryption

Supported authentication types

Depending on whether there is a TPM and on the operating system version, Panda Full Encryption allows different combinations of authentication methods. These are as follows, in the order that they are recommended by Panda Security:

- **TPM + PIN:** Compatible with all supported versions of Windows. The TPM chip must be enabled in the BIOS and a PIN must be established.
- **Only TPM:** Compatible with all supported versions of Windows. The TPM chip must be enabled in the BIOS except in Windows 10, where it is automatically enabled.
- **USB drive:** Requires a USB drive. The computer must be able to access USB devices during startup. Required on Windows 7 computers without TPM.
- **Passphrase:** Only available on computers with Windows 8 and later without TPM.

By default, Panda Full Encryption uses an encryption method that includes TPM usage if available. If you choose an authentication routine not included in the above list, the management console displays a warning indicating that the computer will not be encrypted.

Supported storage devices

Panda Full Encryption encrypts all internal mass storage devices:

- Fixed storage drives on the computer (system and data).
- Virtual hard disks (VHD), though only used space, regardless of what appears in the management console.
- Removable hard drives.
- USB drives.

The following are not encrypted:

- Dynamic hard disks.
- Very small partitions.
- Other external storage devices.

Panda Full Encryption minimum requirements

The minimum requirements are split into:

- Supported Windows operating system families.
- Hardware requirements.

Supported operating system versions

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows 11 (Pro, Enterprise, Education)
- Windows Server 2008 R2 and higher (including Server Core editions)

Hardware requirements

- TPM 1.2 and higher if this authentication method is used.
- USB key and computer that supports reading USB devices from the BIOS on Windows 7 systems without TPM.

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 agent

Regardless of whether a computer is managed by Panda Full Encryption or not, if its drives are encrypted, when uninstalling Panda Endpoint Protection 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, the last stored recovery key is displayed.

Encryption and decryption

Encryption of previously unencrypted drives

The encryption process starts when the Panda Endpoint Protection agent installed on the user's computer downloads an encryption settings profile. At that moment, a window is shown that guides the user through the entire process.

The total number of steps involved varies depending on the type of authentication chosen by the administrator and the previous status of the computer. If any of the steps ends in an error, the agent reports it to the management console and the process stops.



It is not permitted to encrypt computers from a remote desktop session as it is necessary to restart the computer and enter a password before loading the operating system, actions that are not possible with a standard remote desktop tool.

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.

Next we describe the entire encryption process and whether feedback is displayed to the computer user and if a restart is required:

Step	Process on the computer	User interaction
1	The agent receives a settings profile from the encryption module, which asks for the content of the storage drives installed to be encrypted.	None
2	If the computer is a server and does not have BitLocker tools installed, they are downloaded and installed.	A window is shown requesting permission to restart the computer and complete installation of BitLocker or to postpone the process. If 'postpone' is selected, the process stops and the user is asked again during the next login. Requires restart.
3	If the computer was not previously encrypted, a system partition is created.	A window appears asking for permission to restart the computer and complete the creation of the system partition or postpone it. If 'postpone' is selected, the process stops and the user is asked again during the next login. Requires restart.
4	If there is a group policy previously established by the administrator and which conflicts with those set by Panda Full Encryption, an error message appears and the process stops. The group policies configured by Panda Full Encryption are: In the Local Group Policy Editor, follow this path: Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives. Select Not Set for the specified policies to avoid this error.	If the administrator has not defined global group policies that conflict with the local ones defined by Panda Full Encryption, no message appears.

Step	Process on the computer	User interaction
5	Preparing the TPM if it exists, and if the authentication method selected requires this component and was not previously enabled from the BIOS.	<p>This requires confirming a restart so that the user can enter the BIOS on the computer to enable the TPM.</p> <p>On Windows 10 systems, there is no need to change the BIOS settings but the restart is required.</p> <p>The restart in step 3, if required, combines with this one.</p>
6	Preparing the USB device if the authentication method selected requires this component.	This requires users to plug in a USB device to store the password for starting the computer.
7	Storing the PIN if the authentication method selected requires this component.	The user is required to enter the PIN. If alphanumeric characters are used and the hardware is not compatible with those characters, error -2144272180 is shown. In that case, a numerical PIN must be entered.
8	Storing the passphrase if the authentication method selected requires this component.	The user is required to enter the passphrase.
9	The recovery key is generated and sent to the Panda Security cloud. After it has been received, the process continues on the user's computer.	None.
10	Checking that the hardware on the computer is compatible with the encryption technology. The encryption process begins.	<p>Confirmation of a restart is required in order to check the hardware used in the various authentication methods.</p> <p>Requires restart.</p>
11	Encryption of drives.	The encryption process begins and runs in the background, without interfering with the user. The length of the process

Step	Process on the computer	User interaction
		<p>depends on the drive being encrypted. On average, the encryption time is about 2-3 hours.</p> <p>Users can use and shut down computers normally. In the latter case, the process continues whenever the computer is restarted.</p>
12	The encryption process takes place silently and from then on is completely invisible to the user.	Depending on the authentication method selected, the user may need to enter a USB key, a PIN, a passphrase, or nothing at all when the computer restarts.

Table 15.1: Steps for encrypting previously unencrypted drives

Encryption of previously encrypted drives

If any drive on the computer is already encrypted, Panda Full Encryption modifies certain parameters so that it can be centrally managed. The action taken is as follows:

- If the authentication method chosen by the user does not coincide with the one specified in the settings profile, the latter changes, and the user is asked for the necessary passwords or hardware resources. If it is not possible to assign an authentication method compatible with the platform and the settings profile specified by the administrator, the computer continues to use the user's encryption and is not managed by Panda Full Encryption.
- If the encryption algorithm used is not supported (not AES-256), no change takes place to avoid full decryption and encryption of the drive, but the computer is managed by Panda Full Encryption.
- If there are both encrypted and unencrypted drives, all drives are encrypted with the same authentication method.
- If the previous authentication method required a password to be entered and is compatible with the methods supported by Panda Full Encryption, the user is asked for the password in order to unify the authentication method in all drives.
- If the user chose encryption settings different from those set by the administrator (encryption solely of the occupied sectors, not the whole drive), no changes are made in order to minimize the encryption process.
- At the end of the process, the device is managed by Panda Full Encryption. A recovery key is generated and sent to the Panda Security cloud.

Encryption of new drives

If a user creates a new drive after the encryption process is complete, Panda Full Encryption encrypts it immediately, respecting the encryption settings profile assigned by the network administrator.

Decrypting drives

There are three scenarios:

- If Panda Full Encryption encrypts a computer, from that moment the administrator can assign a settings profile to decrypt it.
- If a computer was already encrypted by the user prior to the installation of Panda Full Encryption and is assigned an encryption settings profile, it is considered encrypted by Panda Full Encryption and can be decrypted by assigning a settings profile from the management console.
- If a computer was already encrypted by the user prior to the installation of Panda Full Encryption and has never been assigned an encryption settings profile, it is not considered encrypted by Panda Full Encryption and cannot be decrypted by assigning a settings profile from the management console.

Local editing of BitLocker settings

The computer user has access to the local BitLocker settings from the Windows tools, but the changes made are immediately reverted to the settings established by the network administrator through the management console. The way that Panda Full Encryption responds to a change of this type is 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 keys

As users can connect and disconnect external storage devices from their computers at any time, the way Panda Full Encryption works with these devices is as follows:

- If the workstation or server does not have BitLocker installed and running, the agent does not download the required packages and the device is not encrypted. Nor are any messages displayed to the user.

- If the computer has BitLocker installed and running, a pop-up message is displayed to the user prompting them to encrypt the device in the following situations:
 - Every time they connect an unencrypted USB storage device.
 - If there is an unencrypted device connected to the computer at the time the administrator enables the encryption settings profile from the web console.
- The encryption message is displayed to the user for 5 minutes, after which it disappears. 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. See [Write to removable storage drives](#) for more information.
- Encrypting a USB device does not require creating a system partition.
- If the external storage device is already encrypted by a solution other than Panda Full Encryption, and the user connects it to their computer, the encryption message is not displayed and the device can be used normally. Panda Full Encryption does not send the recovery keys to the web console.
- Writing to the USB device is not allowed if the option **Write to removable storage drives** in Panda Data Control is enabled and the device has not been encrypted by BitLocker or by Panda Full Encryption. See [Write to removable storage drives](#) for more information.
- To decrypt a device encrypted by Panda Full Encryption, the user can use BitLocker manually.
- Only the space used is encrypted.
- All partitions on the device are encrypted with the same key.



Removing a USB device when the encryption process is not complete might corrupt its contents.

Panda Full Encryption response to errors

- **Errors in the hardware test:** The hardware test runs every time the computer is started up until it is passed, at which time the computer 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.

Getting a recovery key

In cases where a user makes repeated attempts to enter an incorrect PIN or password while the device boots up, or a Trusted Platform Module (TPM) chip detects a change in the boot sequence, the user is prompted to enter a BitLocker recovery key.

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 the Recovery Key ID: a unique 40-digit string associated with each encrypted drive.

Required permissions

Permission	Access type
Access recovery keys for encrypted drives	To find and obtain the recovery key for an encrypted drive.

Table 15.2: Permissions required to obtain a recovery key

Getting the recovery key ID for an encrypted drive

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:

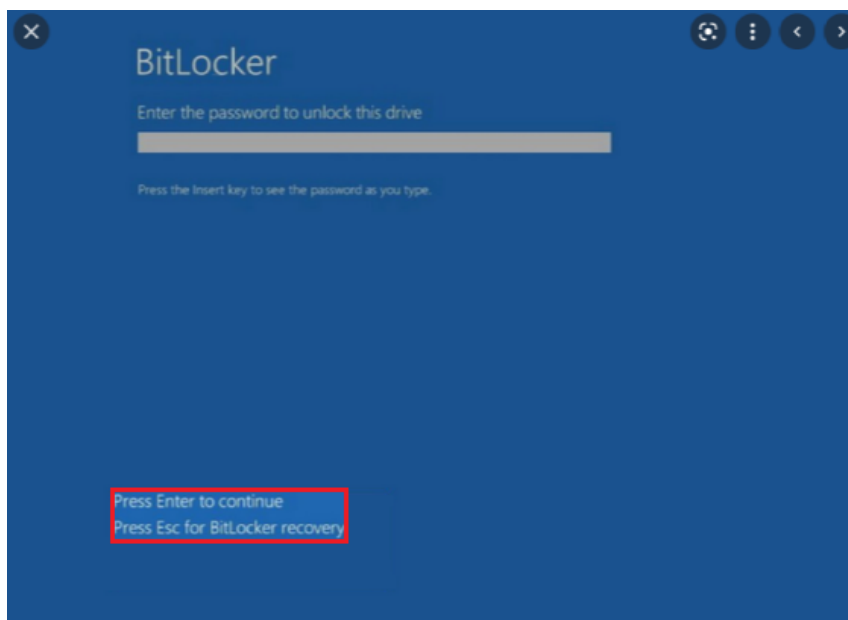


Figure 15.1: Accessing the recovery key ID for an encrypted drive

Press **Esc** to access the window displaying the recovery key ID for the encrypted drive:



Figure 15.2: Recovery key ID for an encrypted drive

In the case of partitions of encrypted disks, the window displayed to the user when accessing the partition is different, and only the first eight digits of the recovery key ID are visible:

BitLocker (E:)

Enter the 48-digit recovery key to unlock this drive.

(Key ID: 2A[blurred]22)

[Load key from USB drive](#)

Unlock

Figure 15.3: Recovery key ID for an encrypted partition



For more information about the encryption of drives on computers, see section [Encryption and decryption](#) on page 369.

Getting a recovery key

- Select the **Computers** menu at the top of the console. Click the computer for which you want to obtain the key.
- On the **Details** tab, **Data protection** section, click the **Get recovery key** link (to obtain a removable drive recovery key, click the link **View encrypted devices on this computer**).

A dialog box opens and shows the recovery key IDs of the encrypted drives on the computer.

- Click the recovery key ID of the key to recover. A window with the recovery key opens.
- Copy the key and send it to the user.

Finding a recovery key

If the user has visibility of all the computers in the account, the search results also include the IDs of drives on computers that have been deleted.

Finding a recovery key from the Encrypted computers widget

- Click the **Recovery key search** link.
- Enter the encrypted drive recovery key ID provided by the user. The recovery key that the user can use to access the computer is displayed.
- 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 displayed.



It is possible that the first eight digits are the same for more than one recovery key, in which case all corresponding keys are displayed in the search results.

Finding a recovery key from the Computer details

- Select the **Computers** menu at the top of the console. Click the computer for which you want to obtain the key.
- On the **Details** tab, **Data protection** section, click the **Get recovery key** link (to obtain a removable drive recovery key, click the link **View encrypted devices on this computer**).

A dialog box opens and shows the recovery key IDs of the encrypted drives on the computer.

- Click the **Find another key** link and enter the recovery key ID of the key to recover.

Managing computers encrypted by the user

Computers that are partially or entirely encrypted by users using BitLocker are not integrated into Panda Full Encryption. Neither their encryption nor their recovery keys can be managed.

If the user enables Panda Full Encryption, the authentication methods assigned on configuring the encryption of the computers are replaced by those of Panda Full Encryption.

Panda Full Encryption module panels/widgets

Accessing the dashboard

To access the dashboard, select the **Status** menu at the top of the console. Select Panda Full Encryption from the side menu.

Required permissions

No additional permissions are required to access the widgets associated with **Panda Full Encryption**.

Encryption status

Shows the computers that support Panda Full Encryption and their encryption status.

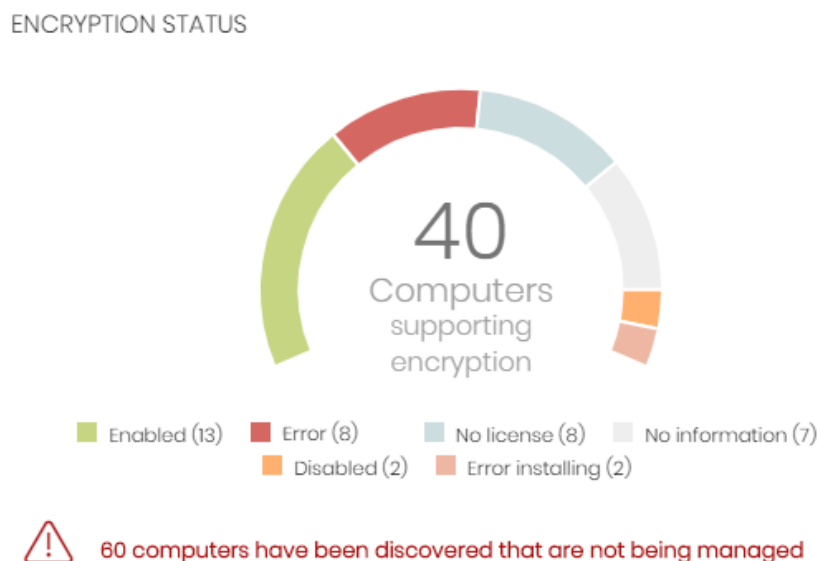


Figure 15.4: Encryption status panel

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.

Data	Description
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 are compatible with Panda Full Encryption, but do not have an assigned license.
No information	Computers with a recently assigned license that have not reported their status to the server, or computers with an expired agent.

Table 15.3: Description of the data displayed in the Encryption status panel

Lists accessible from the panel

ENCRYPTION STATUS

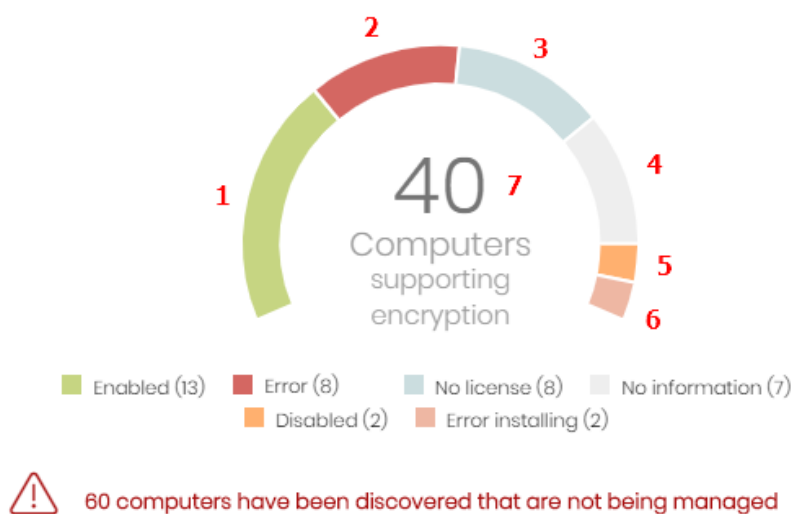


Figure 15.5: Hotspots in the Encryption status panel

Click the hotspots shown in **Figure 15.5**: to open the **Encryption status** list with the following predefined filters:

Hotspot	Filter
(1)	Encryption status = Enabled.

Hotspot	Filter
(2)	Encryption status = Error.
(3)	Encryption status = No license.
(4)	Encryption status = No information.
(5)	Encryption status = Disabled.
(6)	Encryption status = Error installing.
(7)	No filter.

Table 15.4: Lists accessible from the Encryption status panel

Computers supporting encryption

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.

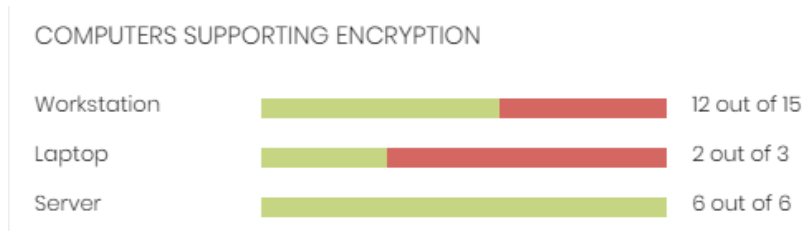


Figure 15.6: Computers supporting encryption panel

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.

Data	Description
Server - red	Servers that do not support encryption.

Table 15.5: Description of the data displayed in the Computers supporting encryption panel

Lists accessible from the panel

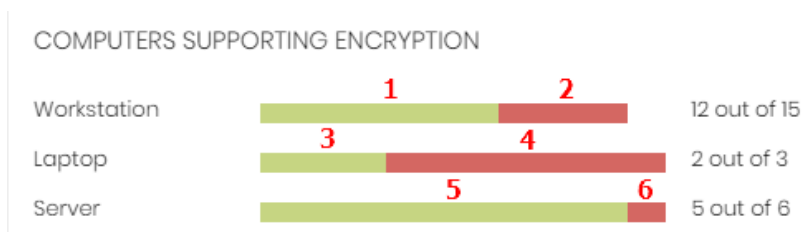


Figure 15.7: Hotspots in the Encryption status panel


Click the hotspots shown in **Figure 15.7:** to open the **Encryption status** list with the following predefined filters:

Hotspot	Filter
(1)	Computer type = Workstation.
(2)	Computer list filtered by Encryption not supported.
(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 15.6: Lists accessible from the Encryption status panel

Encrypted computers

Shows the encryption status of computers that support Panda Full Encryption.


For more details on searching for recovery keys, see section [Getting a recovery key](#)

ENCRYPTED COMPUTERS



■ Encrypted disks (9) ■ Encrypted by the user (1)
■ Encrypted by the user (partially) (4) ■ Encrypted (partially) (4)
■ Encrypting (1) ■ Unencrypted disks (1)



9 computers require user action to be encrypted or apply changes to encryption.

[Recovery key search](#)

Figure 15.8: 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.
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 15.7: Description of the data displayed in the Encrypted computers panel

Lists accessible from the panel

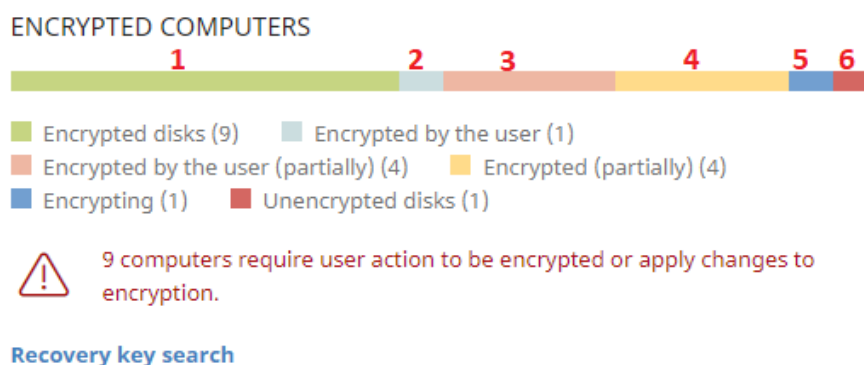


Figure 15.9: Hotspots in the Encrypted computers panel

Click the hotspots shown in [Figure 15.9](#): to open the **Encryption status** list with the following predefined filters:

Hotspot	Filter
(1)	Disk encryption = Encrypted disks.
(2)	Disk encryption = Encrypted by the user.
(3)	Disk encryption = Encrypted by the user (partially).
(4)	Disk encryption = Encrypted (partially).
(5)	Disk encryption = Encrypting.
(6)	Disk encryption = Unencrypted disks.
(7)	Disk encryption = Decrypting.
(8)	Disk encryption = Unknown.

Table 15.8: Lists accessible from the Encryption status panel

Authentication method applied

Shows encrypted computers and the type of encryption used.

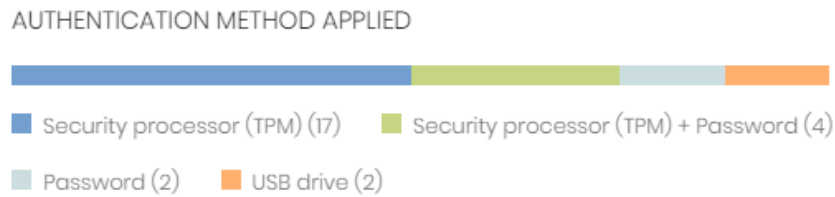


Figure 15.10: Authentication methods panel

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 and PIN or password for authentication.
Password	While booting, the computer requests a PIN or password for authentication.
USB drive	While booting, the computer uses a USB key for authentication.
Unencrypted	The computer has no encrypted disks.

Table 15.9: Description of the data displayed in the Authentication method applied panel

Lists accessible from the panel

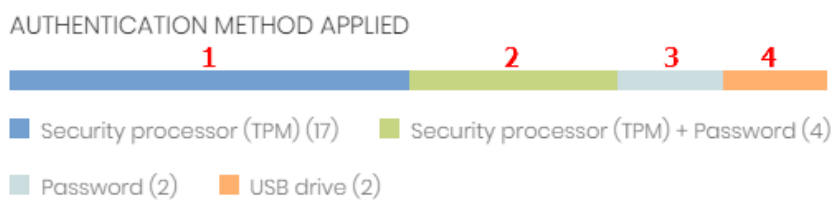


Figure 15.11: Hotspots in the Authentication method applied panel

Click the hotspots shown in **Figure 15.11**: to open the **Encryption status** list with the following predefined filters:

Hotspot	Filter
(1)	Authentication method = Security processor (TPM)
(2)	Authentication method = Security processor (TPM) + Password
(3)	Authentication method = Password
(4)	Authentication method = USB drive
(5)	Authentication method = Unknown
(6)	Authentication method = Unencrypted

Table 15.10: Description of the list filters

Panda Full Encryption lists

Accessing the lists

You can access the lists in two ways:

- Click the **Status** menu at the top of the console. Select **Panda Full Encryption** from the side menu and click the relevant widget.
- Or,
- Click the **Status** menu at the top of the console. Click the **Add** link in the side menu. A window opens with the available lists.
- Select a list from the **Data protection** section 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


Shows all computers on the network managed by Panda Endpoint Protection 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	Character string

Field	Comment	Values
	encryption technology.	
Computer status	<p>Agent reinstallation:</p> <ul style="list-style-type: none">  Reinstalling the agent.  Agent reinstallation error <p>Protection reinstallation:</p> <ul style="list-style-type: none">  Reinstalling the protection.  Protection reinstallation error.  Pending restart <p>Computer isolation status:</p> <ul style="list-style-type: none">  Computer in the process of being isolated.  Isolated computer.  Computer in the process of stopping being isolated. <p>"RDP attack containment" mode:</p> <ul style="list-style-type: none">  Computer in "RDP attack containment" mode.  Ending "RDP attack containment" mode. 	Icon
Group	Folder within the Panda Endpoint Protection 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.	<ul style="list-style-type: none"> No information Enabled Disabled Error

Field	Comment	Values
		<ul style="list-style-type: none"> • Install error • No license
Disk status	Status of the computer's internal storage media with regard to encryption.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted
Last connection	Date when the agent last connected to the Panda Security cloud.	Date

Table 15.11: 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.	<ul style="list-style-type: none"> • Workstation • Laptop • Server
Computer	Name of the computer compatible with the encryption technology.	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
Group	Folder within the Panda Endpoint Protection 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 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

Field	Comment	Values
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Boolean
Last update	Date the signature file was last updated.	Date
Hard disk encryption	Panda Full Encryption module status.	<ul style="list-style-type: none"> • No information • Enabled • Disabled • Error • Install error • No license
Disk status	Status of the computer's internal storage media with regard to encryption.	<ul style="list-style-type: none"> • Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Encryption pending user action	User actions (entering data or restarting) are pending to complete the encryption process.	Boolean
Authentication method	Authentication method selected to encrypt disks.	<ul style="list-style-type: none"> • All • Unknown • Security processor (TPM) • Security

Field	Comment	Values
		processor (TPM) + Password <ul style="list-style-type: none"> • Password • USB drive • Not encrypted
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 15.12: 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
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop

Field	Comment	Values
		<ul style="list-style-type: none"> • Server
Disk status	Status of the computer's internal storage media with regard to encryption.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • No information • Enabled • Disabled • Error • Install error • No license
Authentication method	Authentication method selected to encrypt disks.	<ul style="list-style-type: none"> • All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted

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

Table 15.13: Filters available in the list

Computer details page

Click any of the rows in the list to open the computer details page. See [Computer details](#) on page 217 for more information.

Encryption settings

Accessing the settings

- Click the **Settings** menu at the top of the console. Select **Encryption** from the side menu.
- 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 15.14: 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 acts 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, but not with Panda Full Encryption, and you disable **Encrypt all hard disks on computers**, there are no changes.

- If a computer is encrypted, but not with Panda Full Encryption, and you enable **Encrypt all hard disks on computers**, the internal encryption settings are adjusted to coincide with the encryption methods supported by Panda Full Encryption, thereby avoiding re-encrypting the drive. See [Encryption of previously encrypted drives](#) for more information.
- If a computer is not encrypted and you enable **Encrypt all hard disks on computers**, all the drives on the computer are encrypted as described in section [Encryption of previously unencrypted drives](#).

Ask for password to access the computer

Enable password authentication on starting up the computer. Depending on the platform and whether there is TPM hardware, two types of passwords are permitted:

- **Computers with TPM:** A PIN-type password is requested.
- **Computers without TPM:** A passphrase is requested.



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

To prevent the use of USB devices supported by Panda Full Encryption in authentication, you can disable their use.



Only Windows 7 computers without TPM can use USB authentication. If you disable the use of USB devices, these computers are not encrypted.

Encrypt used disk space only

You can minimize the encryption time by restricting the feature to the sectors of the hard disk that are actually being used. The sectors released after deleting a file will remain encrypted, but the space that was free prior to the encryption of the hard disk will remain unencrypted and will be accessible to third parties using tools for recovering deleted files.

Prompt for removable storage drive encryption

Displays a window prompting the user to encrypt the external mass storage devices and USB keys connected to the computer. See [Encrypting and decrypting external hard drives and USB keys](#) for more information about the behavior and requirements for this setting.

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 [184](#). 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.

MDR service settings



The MDR service settings page appears in the Panda Endpoint Protection console only if the customer has purchased this service from a partner. Before you fill in this form, contact your partner.

WatchGuard MDR (Managed Detection and Response) is a 24/7 cybersecurity service that enables partners to provide a managed detection and response service to customers with minimum investment in a SOC (Security Operations Center). The service monitors the security of computers in the organization, searching for threats, detecting attacks, investigating, and providing guided recommendations about how to restore affected assets and improve customer security.

The MDR service leverages innovative technologies that use artificial intelligence algorithms. Additionally, the service is fully managed by a team of cybersecurity experts, which improves customer security and cyber resilience overall and minimizes detection and response times.



For more information about the MDR module, see:

[Creating and managing settings profiles](#) on page 247: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.

[Controlling and monitoring the management console](#) on page 55: Managing user accounts and assigning permissions.

Chapter contents

MDR service settings	395
MDR setting options	396

MDR service settings

Accessing the settings

In the top menu, select **Settings**. In the side menu, select **MDR**. The service allows only one settings profile, which you establish at account level and applies to all computers on the managed IT network.

Required permissions

Permission	Access type
Configure MDR	Create, edit, and delete MDR settings profiles.
View MDR settings	View MDR settings profiles.

Table 15.15: Permissions required to access the MDR settings

MDR setting options

MDR settings enable customers to send partners up-to-date information about the IT network they manage. With that information, the partner can determine the cybersecurity resources they need to correctly provide the detection, protection, and response service.

To create or edit an MDR settings profile when you modify your IT infrastructure, enter the relevant information in these fields.

General

Field	Description
Customer business vertical	Specify the industry or vertical your business belongs to.
Number of business locations	Specify the number of branch offices your business has.
Number of employees	Specify the number of employees who have one or more managed devices.
Includes remote employees	Specify the number of people who have one or more managed devices and work outside the business office.

Table 15.16: MDR general settings

Technology

Field	Description
Operating systems	Specify the operating systems in use in the network. Include computers that are not protected by Panda Security products.

Field	Description
Hardware devices	Specify the vendor name and types of hardware devices in the network for early identification of possible existing vulnerabilities. Include devices not protected by Panda Security products.
Critical computers	Specify computers that provide a critical service for your business. You can add individual computers or computer groups.

Table 15.17: Network technology settings

Response plan

Field	Description
Allow WG Security Operations Center to isolate computers on the customer network	Specify whether Panda Security is authorized to use the computer isolation feature to respond to a compromised system. For more information about how to isolate computers, see Computer isolation .
Exceptions	Specify computers for which Panda Security cannot use the computer isolation feature to respond to a compromised system. For more information about how to isolate computers, see Computer isolation .

Table 15.18: Response plan settings

Reports

Specify email addresses to receive weekly and monthly executive reports. Separate email addresses with commas. The maximum number of email addresses you can specify for each type of report is three.

Chapter 16

Malware and network visibility

Panda Endpoint Protection 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 447.


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	399
Security module lists	408

Security module panels/widgets

Panda Endpoint Protection shows the security status of the entire IT network or specific computers through widgets:

- **IT network:** Select **Status** in the menu at the top of the console. Click **Security**  from the side menu. A page opens with counters showing the security status of the computers that are visible to the administrator. See [Structure of a role](#) on page 58 for information about how to set the computer groups that will be visible to the account used to access the management console. See [Filter by group icon](#) on page 37 for information about how to restrict the visibility of the groups defined in the role.
- **Computer:** Select **Computers** in the menu at the top of the console. Choose a computer from the network. Click the **Detections** tab. A page opens with counters showing the security status of the selected computer. See [Detections section \(4\) for Windows, Linux, and macOS computers](#) on page 234.

The following is a description of the different widgets implemented on the Panda Endpoint Protection dashboard, their areas and hotspots, as well as their tooltips and what they mean.

Protection status

Shows computers where Panda Endpoint Protection works correctly and where it does not, and computers with installation errors or problems. The status of the network computers is represented with a circle with different colors and associated counters.



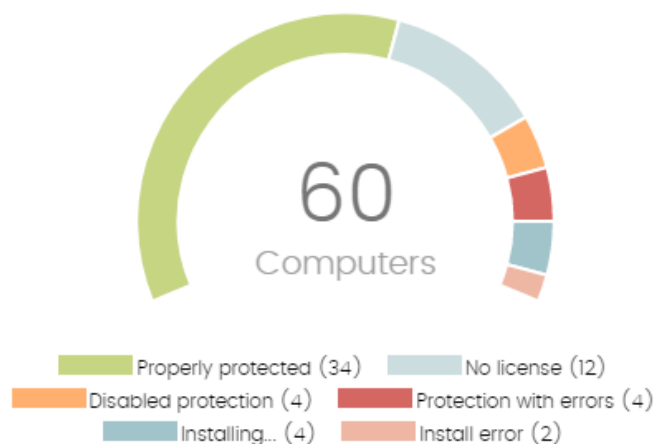
The sum of all percentages can be greater than 100% as the status types are not mutually exclusive. A computer can have different statuses at the same time.

The panel provides a graphical representation and percentage of computers with the same status.



iOS devices are added to the total number of computers and devices at the center of the widget. However, no other information about them is included in the widget, because iOS devices do not have advanced or antivirus protection. For more information, see [Security settings for iOS devices](#) on page 298.

PROTECTION STATUS



40 computers have been discovered that are not being managed by Panda All features.

Figure 16.1: Protection status panel

Meaning of the data displayed

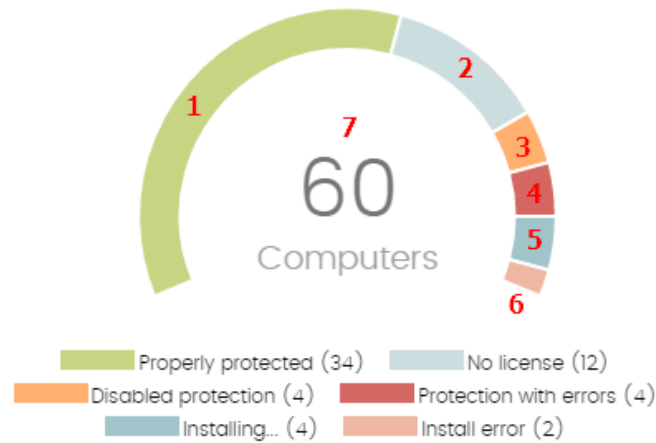
Data	Description
Properly protected	Percentage of computers where Panda Endpoint Protection installed without errors and is working correctly.
Installing...	Percentage of computers on which Panda Endpoint Protection is currently being installed.
No license	Computers that are unprotected because there are insufficient licenses or because an available license has not been assigned to the computer.
Disabled protection	Computers where the antivirus protection is not enabled.
Protection with errors	Computers with Panda Endpoint Protection installed, but whose protection module does not respond to the requests sent from the Panda Security servers.
Install error	Computers on which the installation process could not be completed.

Data	Description
Central area	Number of computers with a Panda agent installed.

Table 16.1: Description of the data displayed in the Protection status panel

Lists accessible from the panel

PROTECTION STATUS



40 computers have been discovered that are not being managed by Panda All features.

Figure 16.2: Hotspots in the Protection status panel

Click the hotspots shown in [Figure 16.2](#): to open the **Computer protection status** list with the following predefined filters:

Hotspot	Filter
(1)	Protection status = Properly protected.
(2)	Protection status = Installing...
(3)	Protection status = Disabled protection.
(4)	Protection status = Protection with errors.
(5)	Protection status = No license.
(6)	Protection status = Install error.

Hotspot	Filter
(7)	No filter.

Table 16.2: Filters available in the Computer protection status list

Offline computers

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.

OFFLINE COMPUTERS



Figure 16.3: Offline computers panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported their status in the last 72 hours.
7 days	Number of computers that have not reported their status in the last 7 days.
30 days	Number of computers that have not reported their status in the last 30 days.

Table 16.3: Description of the data displayed in the Offline computers panel

Lists accessible from the panel



Figure 16.4: Hotspots in the Offline computers panel

Click the hotspots shown in [Figure 16.4](#): to open the **Offline computers** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 16.4: Filters available in the Offline computers list

Outdated protection

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.

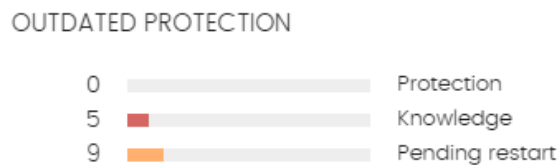


Figure 16.5: Outdated protection panel

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	For at least seven days, the computer has had a version of the antivirus engine older than the latest released engine.
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 16.5: Description of the data displayed in the Outdated protection panel

Lists accessible from the panel

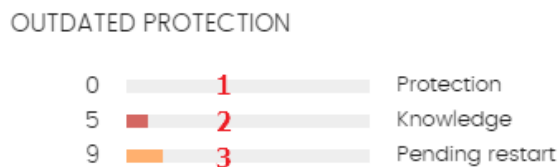


Figure 16.6: Hotspots in the Outdated protection panel

Click the hotspots shown in [Figure 16.6](#): to open the **Computer protection status** list with the following predefined filters:

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

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

Threats detected by the antivirus

Shows all intrusion attempts that Panda Endpoint Protection detected in the selected time period.

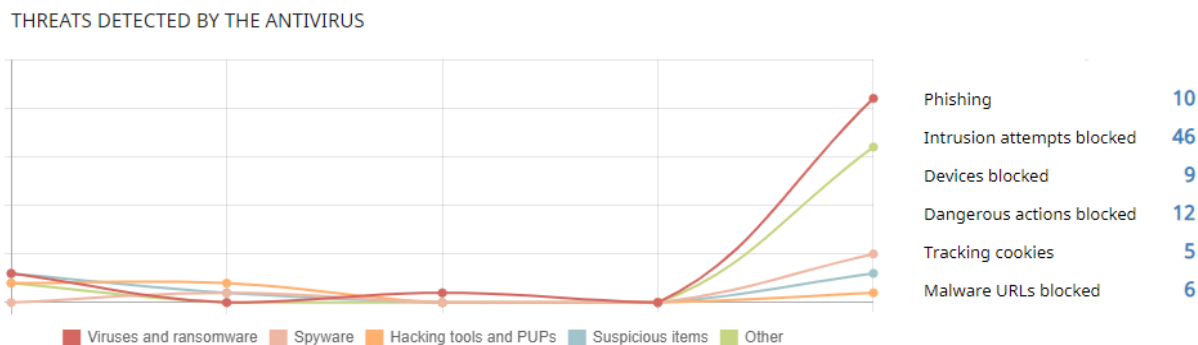


Figure 16.7: Threats detected by the antivirus panel

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 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 16.7: Description of the data displayed in the Threats detected by the antivirus panel

The list to the right of the chart shows events that the administrator may want to monitor in order 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's attempt to use a device whose access is restricted according to the settings established by the network administrator in the Device Control module.

Data	Description
Tracking cookies	Detection of cookies used to track users' web activity.
Malware URLs blocked	Web addresses that point to pages containing malware.

Table 16.8: Description of the data displayed in the Threats detected by the antivirus panel

Lists accessible from the panel

THREATS DETECTED BY THE ANTIVIRUS

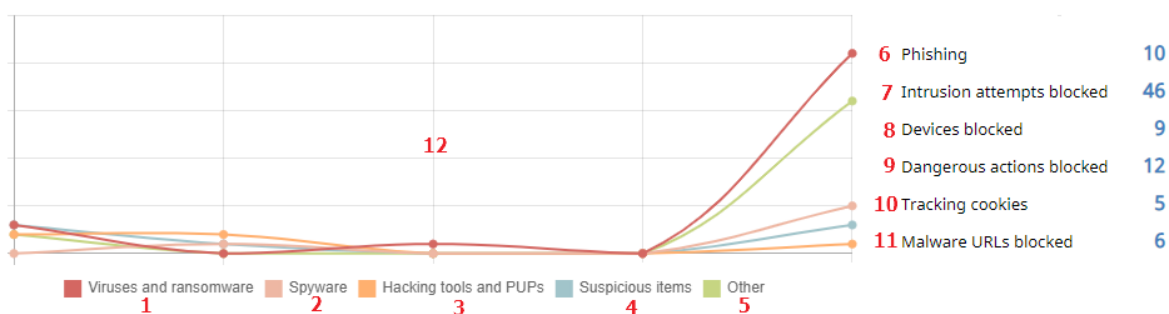


Figure 16.8: Hotspots in the Threats detected by the antivirus panel

Click the hotspots shown in [Figure 16.8](#): to access the following list with the following 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.

Hotspot	List	Filter
(6)	Threats detected by the antivirus	Threat type = Phishing.
(7)	Intrusion attempts blocked	No filter.
(8)	Devices blocked	No filter.
(9)	Threats detected by the antivirus	Threat type = Dangerous actions blocked.
(10)	Threats detected by the antivirus	Threat type = Tracking cookies.
(11)	Threats detected by the antivirus	Threat type = Malware URLs.
(12)	Threats detected by the antivirus	No filter.

Table 16.9: Filters available in the Threats detected by the antivirus list

Security module lists

The security lists display the information collected by Panda Endpoint Protection in connection with computer protection activities. They provide highly detailed information as they contain the raw data used to generate the widgets.

There are two ways to access the security lists:

- Go to the **Status** menu at the top of the console. Select **Security** from the side panel. Click any of the available widgets to access its associated list. Depending on the item you click on the widget, you will access different lists with predefined filters.

Or

- Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** side panel. A window opens that shows all lists available in Panda Endpoint Protection.
- Click any of the lists in the **Security** section. The list opens with no filters applied.














Click any of the entries on the list to open a new page with more details about that particular item.

Computer protection status

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 protection, the computers on the network must communicate with the Panda Security cloud. See the list of URLs that must be accessible from computers in section [Access to service URLs](#) on page 496.

Field	Description	Values
Computer	Computer name.	Character string
Computer status	<p>Agent reinstallation:</p> <ul style="list-style-type: none">  Reinstalling the agent.  Agent reinstallation error. <p>Protection reinstallation:</p> <ul style="list-style-type: none">  Reinstalling the protection.  Protection reinstallation error.  Pending restart. <p>Computer isolation status:</p> <ul style="list-style-type: none">  Computer in the process of being isolated.  Isolated computer.  Computer in the process of stopping being isolated. <p>"RDP attack containment" mode:</p> <ul style="list-style-type: none">  Computer in "RDP attack containment" mode.  Ending "RDP attack containment" mode. 	Icon

Field	Description	Values
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string <ul style="list-style-type: none"> •  'All' group •  Native group •  Active Directory group
Antivirus	Antivirus protection status.	<ul style="list-style-type: none"> •  Installing •  Error. If it is a known error, the cause of the error is shown. If it is an unknown error, the error code is shown 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.	<ul style="list-style-type: none"> •  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.	<ul style="list-style-type: none"> •  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.	<ul style="list-style-type: none"> •  Connection OK •  One or more services are

Field	Description	Values
		not accessible <ul style="list-style-type: none"> Information not available
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	Date

Table 16.10: 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.	<ul style="list-style-type: none"> Workstation Laptop Server Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Agent version	Internal version of the Panda agent module.	Character string

Field	Description	Values
Installation date	Date when the Panda Endpoint Protection software was successfully installed on the computer.	Date
Last update on	Date the agent was last updated.	Date
Platform	Operating system installed on the computer.	<ul style="list-style-type: none"> • 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 Web browsing antivirus Firewall Device control Anti-Theft	Status of the associated protection.	<ul style="list-style-type: none"> • Not installed • Error: If it is a known error, the cause of the error is shown. If it is an unknown error, the error code is shown instead • Enabled • Disabled • No license

Field	Description	Values
Error date	If an error occurred installing Panda Endpoint Protection, date and time of the error.	Date
Installation error	If an error occurred installing Panda Endpoint Protection, error description.	Character string
Installation error code	Displays codes that identify the installation error occurred.	Codes are separated by “;”: <ul style="list-style-type: none"> • 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.	Character string
Connection for collective intelligence	Shows the status of the connection between the computer and the servers that store signature files and security intelligence.	<ul style="list-style-type: none"> • OK • With problems

Table 16.11: Fields in the Computer protection status exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
Search computer	Computer name.	Character string
Last connection	Date when the Panda Endpoint Protection status was last sent to the Panda Security cloud.	<ul style="list-style-type: none"> • All • Less than 24 hours ago

Field	Description	Values
		<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • All • Yes • No • Pending restart
Platform	Operating system installed on the computer.	<ul style="list-style-type: none"> • All • Windows • Linux • macOS • Android
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Connection to knowledge servers	Indicates whether the computer can communicate with the Aether cloud to send monitored events and download security intelligence.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> Installing... Properly protected Protection with errors Disabled protection No license Install error
"RDP attack containment" mode	Status of the "RDP attack containment" mode.	<ul style="list-style-type: none"> All No Yes

Table 16.12: Filters available in the Computer protection status list

Computer details page

Click any of the rows in the list to open the computer details page. See [Computer details](#) on page 217 for more information.

Filter tool

Details page

Shows detailed information about the program blocked by the advanced security policies. See [Exploit detection](#).

Threats detected by the antivirus

Provides complete and consolidated information about all the detections made on all supported platforms and for all the infection vectors used by hackers to infect computers on the network.

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
IP address	The computer's primary IP address.	Character string
Group	Group within the Panda Endpoint Protection group	Character string




Field	Description	Values
	tree that the computer belongs to.	<ul style="list-style-type: none"> •  'All' group •  Native group •  Active Directory group
Threat type	Type of detected threat.	<ul style="list-style-type: none"> • Viruses and ransomware • 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.	<ul style="list-style-type: none"> • Deleted • Disinfected • Quarantined • Blocked • Process ended
Date	Date when the attack was detected.	Date

Table 16.13: Fields in the Threats detected by the antivirus list

Fields displayed in the exported file

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

Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Mobile device • Server
Computer	Name of the computer where the threat was detected.	Character string
Malware name	Name of the detected threat.	Character string
Threat type	Type of detected threat.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Quarantined • Deleted • Blocked • Process ended
Detected by	Engine that detected the threat.	<ul style="list-style-type: none"> • Device control • File protection • Firewall

Field	Description	Values
		<ul style="list-style-type: none"> • Mail protection • On-demand scan • Web protection
Detection path	Location of the threat on the file system.	Character string
Excluded	The threat was excluded from the scans by the administrator to allow it to run.	Binary value
Date	Date when the attack was detected.	Date
Group	Group within the Panda Endpoint Protection group tree that the computer belongs to.	Character string
IP address	Primary IP address of the computer where the detection was made.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the network administrator.	Character string

Table 16.14: Fields in the Threats detected by the antivirus exported file

Filter tool

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
Dates	<p>Range: Set a time period, from the current moment back.</p> <p>Custom range: Choose specific dates from a calendar.</p>	<ul style="list-style-type: none"> • Last 24 hours • Last 7 days • Last month • Last year
Computer	Type of device.	<ul style="list-style-type: none"> • Workstation

Field	Description	Values
type		<ul style="list-style-type: none"> Laptop Mobile device Server
Threat type	Type of threat.	<ul style="list-style-type: none"> Viruses and ransomware Spyware Hacking tools and PUPs Phishing Suspicious items Dangerous actions blocked Tracking cookies Malware URLs Other

Table 16.15: Filters available in the Threats detected by the antivirus list

Details page

Shows detailed information about the detected virus.

Field	Description	Values
Threat	Threat name.	Character string
Action	Action taken by Panda Endpoint Protection	Quarantined Deleted Blocked Process ended
Computer	Name of the computer where the threat was detected. It includes a link to the Computer details page.	Character string
Computer	Type of device.	<ul style="list-style-type: none"> Workstation

Field	Description	Values
type		<ul style="list-style-type: none"> Laptop Server Mobile device
IP address	The computer's primary IP address.	Character string
Logged-in user	Operating system user under which the threat was loaded and run.	Character string
Detection path	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.	<ul style="list-style-type: none"> 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.	
Date	Date when the attack was detected.	Date

Table 16.16: Details accessible from the Threats detected by the antivirus list

Blocked devices

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 folder tree that the computer belongs to.	<ul style="list-style-type: none"> • Character string •  'All' group •  Native group •  Active Directory group
Name	Name manually assigned to the device by the administrator to make identification easier.	Character string
Type	Type of device affected by the security settings.	<ul style="list-style-type: none"> • Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices • Modems • Mobile devices
Action	Action taken on the device.	<ul style="list-style-type: none"> • Block • Allow read access • Allow read and write access
Date	Date and time when the action was taken.	Date

Table 16.17: Fields in the Blocked devices list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • 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 the administrator.	Character string
Type	Type of device.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Block • Allow read access • Allow read and write access

Field	Description	Values
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 folder tree that the computer belongs to.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 16.18: Fields in the Blocked devices exported file

Filter tool


Field	Description	Values
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Mobile device • Server
Search computer	Computer name.	Character string
Dates	<ul style="list-style-type: none"> • Range: Set a time period, from the current moment back. • Custom range: Choose specific dates from a calendar. 	<ul style="list-style-type: none"> • Last 24 hours • Last 7 days • Last month
Device type	Type of device affected by the security settings.	<ul style="list-style-type: none"> • Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices

Field	Description	Values
		<ul style="list-style-type: none"> • Modems • Mobile devices
Name	Device name.	Character string

Table 16.19: Filters available in the Blocked devices list

Details 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	<ul style="list-style-type: none"> • Quarantined • Deleted • Blocked • Process ended
Computer	Name of the computer where the device was blocked.	Character string
Computer type	Type of computer.	<ul style="list-style-type: none"> • Workstation • Laptop • Server • Mobile device
IP address	The computer's primary IP address.	Character string
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by the administrator. You can edit it by clicking the icon. 	Character string
Device type	Type of device.	<ul style="list-style-type: none"> • Removable storage drives • Imaging devices

Field	Description	Values
		<ul style="list-style-type: none"> • 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 device was blocked.	Date

Table 16.20: Details accessible from the Blocked devices list

Intrusion attempts blocked

Shows the network attacks received by the computers on the network and blocked by the firewall.

Field	Description	Values
Computer	Name of the computer that received the network attack.	Character string
IP address	IP address of the primary network interface of the computer that received the network attack.	Character string
Group	Folder in the Panda Endpoint Protection group tree that the computer belongs to.	Character string
Intrusion type	Indicates the type of intrusion detected. See Block intrusions on page 290 for more information about each type of network attack.	<ul style="list-style-type: none"> • All intrusion attempts • ICMP Attack • UDP Port Scan • Header

Field	Description	Values
		Lengths <ul style="list-style-type: none"> • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Date	Date and time Panda Endpoint Protection logged the attack on the computer.	Date

Table 16.21: Fields in the Intrusion attempts blocked list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	Character string
Computer	Name of the computer that received the network attack.	Character string
Intrusion type	Indicates the type of intrusion detected. See Block intrusions on page 290 for more information about each type of network attack.	<ul style="list-style-type: none"> • ICMP Attack • UDP Port

Field	Description	Values
		Scan <ul style="list-style-type: none"> • 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. See Firewall (Windows computers) on page 283 for more information.	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 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 the administrator.	Character string

Table 16.22: Fields in the Intrusion attempts blocked exported file

Filter tool

Field	Description	Values
Dates	<ul style="list-style-type: none"> • Range: Set a time period, from the current moment back. • Custom range: Choose specific dates from a calendar. 	<ul style="list-style-type: none"> • Last 24 hours • Last 7 days • Last month
Intrusion type	Indicates the type of intrusion detected. See Block intrusions on page 290 for more information about each type of network attack.	<ul style="list-style-type: none"> • All intrusion attempts • ICMP Attack • UDP Port Scan • Header Lengths

Field	Description	Values
		<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Workstation • Laptop • Mobile device • Server

Table 16.23: Filters available in the Intrusion attempts blocked list

Details page

Shows detailed information about the network attack detected.

Field	Description	Values
Intrusion type	Indicates the type of intrusion detected. See Block intrusions on page 290 for more information about each type of network attack.	<ul style="list-style-type: none"> • ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check

Field	Description	Values
		<ul style="list-style-type: none"> • 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	Blocked
Computer	Name of the computer where the threat was detected.	Character string
Computer type	Type of device.	<ul style="list-style-type: none"> • Workstation • Laptop • Mobile device • Server
IP address	The computer's primary IP address.	Character string
Local IP address	IP address of the computer that received the network attack.	Character string
Remote IP address	IP address of the computer that 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	Numeric value

Field	Description	Values
	where the intrusion attempt was received.	
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 16.24: Details accessible from the Intrusion attempts blocked list

Chapter 17

Managing threats, items in the process of classification, and quarantine

Panda Endpoint Protection provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This balance is achieved through tools that enable you to manage the detection of found threats.

Chapter contents

Introduction to threat management tools	433
Allowing and preventing items to run	434
List of allowed threats	435
Managing the backup/quarantine area	439

Introduction to threat management tools

Network administrators can change the behavior of Panda Endpoint Protection with regard to found threats using the following tools:

- Allow/stop allowing the execution of programs classified as viruses.
- Detect/stop detecting programs classified as viruses.
- Manage the backup/quarantine area.

Detect/stop detecting programs classified as viruses

Administrators can allow the execution of software that implements features valued by users but which has been classified as a threat. This is the case of PUPs, for example. These are often toolbars which provide search capabilities but also collect users' private data and confidential corporate information for advertising purposes. See [Allowing and preventing items to run](#) for more information.

Manage the backup/quarantine area

Administrators can retrieve items considered threats and therefore deleted from users' computers.

Allowing and preventing items to run

Restoring/Stopping detecting programs classified as viruses

If users need to use certain features provided by a program classified as a threat by the signature file, and the administrator considers that the danger posed to the integrity of the managed IT network is low, the administrator can allow the program to run.

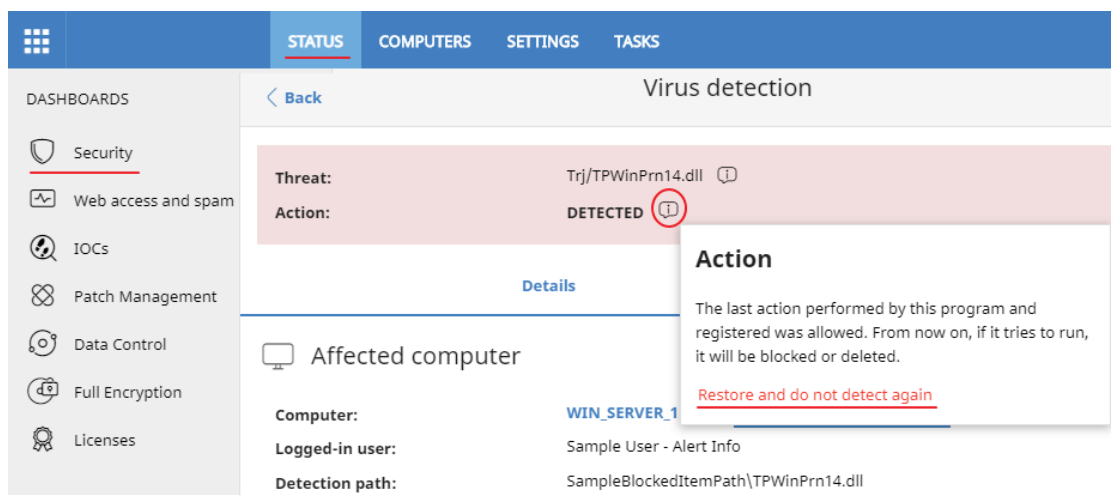



Figure 17.1: Restore and do not detect a threat again


To restore deleted programs from the quarantine/backup area and not detect them again:

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel.
- Click the **Threats detected by the antivirus** panel and select the item that you want to allow to run.
- Click the  icon in the **Action** field. A window opens explaining the action taken by Panda Endpoint Protection.
- Click the **Restore and do not detect again** link. Panda Endpoint Protection performs the following actions:
 - The item is copied from the quarantine/backup area to its original location on the computers on the IT network.

- The item is allowed to run and will not generate any detections.
- The program is added to the **Programs allowed by the administrator** list.

Stopping allowing the execution of previously allowed items

To block a previously allowed item again:

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel.
- In the **Programs allowed by the administrator** panel, click the type of item that you want to stop allowing to run: **Malware**, **PUP**, **Exploit**, or **Being classified**.
- In the **Programs allowed by the administrator** panel, click the type of item that you want to stop allowing to run: **Malware** or **PUP**.
- In the **Programs allowed by the administrator** list, click the  icon to the right of the item that you want to stop allowing to run.

After you click the  icon, Panda Endpoint Protection performs the following actions:

- The item is removed from the **Programs allowed by the administrator** list.
- An entry is added to the **History of programs allowed by the administrator** list, with the **Action** column showing **Exclusion removed by the user** as its value.
- If the item is classified as a virus, it reappears in the **Threats detected by the antivirus** list.
- If the item is classified as a virus, it generates incidents again.

List of allowed threats

Network administrators have multiple panels and lists available to get information about programs that were initially blocked by Panda Endpoint Protection and then allowed to run:

- The **Programs allowed by the administrator** panel.
- The **Programs allowed by the administrator** list.
- The **History of programs allowed by the administrator** list.

Programs allowed by the administrator

Shows programs allowed by the administrator which initially were quarantined by Panda Endpoint Protection because they were identified as a virus by the signature file.



Figure 17.2: Programs allowed by the administrator panel

Meaning of the data displayed

The panel shows the total number of items excluded from blocking by the administrator, broken down by type:

- Malware
- PUP

Lists accessible from the panel



Figure 17.3: Hotspots in the Programs allowed by the administrator panel

Click the hotspots shown in [Figure 17.3](#): to open the **Programs allowed by the administrator** list with the following predefined filters:

Hotspot	Filter
(1)	No filter.
(2)	Classification = Malware.
(3)	Classification = PUP.

Table 17.1: Filters available in the Programs allowed by the administrator list

History of programs allowed by the administrator list

Shows a history of all events that have occurred over time regarding threats and unknown files in the process of classification which the administrator allowed to run. This list shows all the classifications that a file has gone through, from the time it entered the **Programs allowed by the administrator** list until it left it, as well as all other classifications caused by Panda Endpoint Protection or the administrator.

This list does not have a corresponding panel. To access the list, click the **History** link in the upper-right corner of the **Software allowed by the administrator** list.

Field	Description	Values
Program	Name of the file with malicious code that was allowed to run.	Character string
Classification	Type of threat that was allowed to run.	<ul style="list-style-type: none"> • Malware • PUP • Goodware
Threat	Name of the malware or PUP that was allowed to run. If it has not been identified, the column shows the file's name instead. If it is an exploit, the exploit technique used is shown.	Character string
Hash	String identifying the file. This is empty if it is an exploit.	Character string
Action	Action taken on the allowed item. <ul style="list-style-type: none"> • Exclusion removed by the user: The administrator allowed the item to be quarantined again. • Exclusion added by the user: The administrator allowed the item to be removed from quarantine. 	Enumeration
User	User account which triggered the change to the allowed file.	Character string
Date	Date the event took place.	Date

Table 17.2: Fields in the History of programs allowed by the administrator list

Fields displayed in the exported file

Field	Description	Values
Program	Name and path of the file with malicious code that was allowed to run.	Character string
Current type	Last classification of the threat allowed to run.	<ul style="list-style-type: none"> • Malware • PUP

Field	Description	Values
Original type	Original classification of the file when it was allowed to run.	<ul style="list-style-type: none"> Malware PUP
Threat	Name of the malware or PUP that was allowed to run. If it has not been identified, the column shows the file's name instead.	Character string
Hash	String identifying the file.	Character string
Action	Action taken on the allowed item. <ul style="list-style-type: none"> Exclusion removed by the user: The administrator allowed the item to be quarantined again. Exclusion added by the user: The administrator allowed the item to be removed from quarantine. 	Enumeration
User	User account which triggered the change to the allowed file.	Character string
Date	Date the event took place.	Date

Table 17.3: Fields in the History of programs allowed by the administrator exported file

Filter tool

Field	Description	Values
Search	<ul style="list-style-type: none"> User: User account which triggered the change to the allowed file. Program: Name of the file containing the threat. Hash: String identifying the file. 	Enumeration
Action	Action taken on the allowed item. <ul style="list-style-type: none"> Exclusion removed by the user: The administrator allowed the item to be blocked again. Exclusion removed after reclassification: Panda Endpoint Protection applied the action associated with the category after reclassification. 	Enumeration

Field	Description	Values
	<ul style="list-style-type: none"> • Exclusion added by the user: The administrator allowed the item to be run. • Exclusion kept after reclassification: Panda Endpoint Protection did not block the item after reclassification. 	

Table 17.4: Filters available in the History of programs allowed by the administrator list

Managing the backup/quarantine area

The Panda Endpoint Protection quarantine is a backup area that stores items which have been deleted after being classified as a threat.

Quarantined items are stored on each user's computer, in the `Quarantine` folder located in the software installation directory. This folder is encrypted and cannot be accessed by any other process. It is therefore not possible to directly access or run the programs there, unless it is through the web console.



The quarantine feature supports Windows, macOS, and Linux platforms.

The Panda Labs department at Panda Security determines the action to take in accordance with the classification and type of each item detected. As such, the following situations can occur:

- **Malicious items for which disinfection is possible:** These are disinfected and restored to their original location.
- **Malicious items for which disinfection is not possible:** These are moved to quarantine and remain there for seven days.
- **Non-malicious items:** If goodware is incorrectly classified as malware (false positive), it is automatically restored from quarantine to its original location.
- **Suspicious items:** These are stored in quarantine for 30 days. If they finally turn out to be goodware, they are automatically restored to their original location.




Panda Endpoint Protection does not permanently delete files from users' computers. All deleted files are sent to the backup area.

Viewing quarantined items

To get a list of the items sent to quarantine:

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel.
- Click the **Threats detected by the antivirus** panel.
- From the list filters, select the **Moved to quarantine** and **Deleted** checkboxes in the **Action** field. Click **Filter**.

Restoring items from quarantine

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel.
- Click the **Threats detected by the antivirus** panel.
- From the list, select a threat whose **Action** field is **Moved to quarantine** or **Disinfected**.
- Click the  icon in the **Action** field. A window opens explaining why the item was moved to quarantine.
- Click the **Restore and do not detect again** link. The item is moved to its original location. The permissions, owner, and registry entries related to the file are also restored.

Chapter 18

Alerts

The alert system is a resource provided by Panda Endpoint Protection to quickly notify administrators of situations that might affect the correct operation of the security service.

Namely, an alert is sent to the administrator every time one of the following events occur:

- A malware specimen is detected.
- A network attack is detected.
- There is an attempt to use an unauthorized external device.
- An unknown item, malware, or PUP is reclassified.
- There is a license status change.
- There are installation errors or a computer is unprotected.

Chapter contents

Email alerts	441
---------------------------	------------

Email alerts

Email alerts are messages generated and sent by Panda Endpoint Protection to the configured recipients (typically the network administrator) when certain events occur.

Accessing the alert settings

Click the **Settings** menu at the top of the console. Click **My alerts** from the side menu. You will access the **Email alerts** page, 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. See [Table 1.1](#): for more information.
- **Send the alerts to the following address:** Enter the email addresses of the alert recipients.
- **Send the alerts in the following language:** Choose the alert message language from those supported in the console:
 - German
 - Spanish
 - French
 - English
 - Italian
 - Japanese
 - Hungarian
 - Portuguese
 - Russian
 - Swedish

Access permissions and alerts

Alerts are defined independently for each user of the web console. The contents displayed in an alert vary depending on the managed computers that are visible to the recipient's role.

Alert types

Type	Frequency	Condition	Information displayed
Malware detections (real-time protection only)	A maximum of two messages per computer-malware-day.	<ul style="list-style-type: none"> • Every time malware is detected in real time on a computer. • On Windows computers only. 	<ul style="list-style-type: none"> • First or second message. • Name of the malicious program. • Computer name. • Group. • Date and time (UTC). • Path of the malicious

Type	Frequency	Condition	Information displayed
			<p>program.</p> <ul style="list-style-type: none"> • Hash. • Action table for the program. • List of computers where the malware was previously seen.
Malware URL blocked	Every 15 minutes	<ul style="list-style-type: none"> • When a URL pointing to malware is detected. 	<ul style="list-style-type: none"> • Number of malware URLs detected within the time range. • Number of affected computers.
Phishing detections	Every 15 minutes	<ul style="list-style-type: none"> • When a phishing attack is detected. 	<ul style="list-style-type: none"> • Number of phishing attacks detected within the time range. • Number of affected computers.
Intrusion attempts blocked	Every 15 minutes	<ul style="list-style-type: none"> • When an intrusion attempt is blocked by the IDS module. • Compatible with Windows computers. 	<ul style="list-style-type: none"> • Number of intrusion attempts blocked within the time range. • Number of affected computers.
Blocked devices	Every 15 minutes	<ul style="list-style-type: none"> • A user tries to access a device or peripheral blocked 	<ul style="list-style-type: none"> • Number of device access

Type	Frequency	Condition	Information displayed
		<p>by the administrator.</p> <ul style="list-style-type: none"> Compatible with Windows, Linux, macOS, and Android devices. 	<ul style="list-style-type: none"> attempts blocked. Number of affected computers.
Computers with protection errors	Every time the relevant event is detected	<ul style="list-style-type: none"> An unprotected computer is found on the network. A computer with a protection status error or protection installation error is found. 	<ul style="list-style-type: none"> 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	Every time the relevant event is detected	The solution fails to assign a license to a computer due to lack of sufficient free licenses.	<ul style="list-style-type: none"> Computer name. Description. Operating system IP address Group Active Directory path Domain.

Type	Frequency	Condition	Information displayed
			<ul style="list-style-type: none"> Date and time (UTC). Failure reason: Computer without a license.
Installation error	Every time the relevant event is detected	<ul style="list-style-type: none"> An event occurs that causes a computer's status to change (1) from protected to unprotected. If several circumstances are detected at the same time that may cause a computer's status to change from protected to unprotected, only one alert is generated with a summary of all those circumstances. 	<ul style="list-style-type: none"> Computer name. Protection status. Reason for the status change.
Unmanaged computers discovered	Every time the relevant event is detected	<ul style="list-style-type: none"> Every time a discovery computer finishes a discovery task. A discovery task finds a never-seen-before computer on the network. 	<ul style="list-style-type: none"> Name of the discovery computer. Number of discovered computers. Link to the list of unmanaged computers discovered.

Table 18.1: Alert table

Status changes (1)

The following computer statuses will trigger an alert:

- **Protection with errors:** If the status of the antivirus protection installed on a computer shows an error, an alert is generated.
- **Installation error:** If an installation error occurs that requires user intervention (e.g. insufficient disk space), an alert is generated. Transient errors that can be resolved autonomously after a number of retries do not generate alerts.
- **No license:** If a computer does not receive a license after registration because there are no free licenses, an alert is generated.

Finally, the following computer statuses will not trigger an alert:

- **No license:** No alert is generated if the administrator manually removes a computer's license or if Panda Endpoint Protection automatically removes a computer's license because the number of purchased licenses has been reduced.
- **Installing:** It 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, so no alert is generated.
- **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

In cases where the email alert recipient wants to opt out of the notifications but cannot access the Panda Endpoint Protection console or does not have enough permissions to modify the settings, the steps below must be taken:

- Click the link at the bottom of the message: **"If you don't want to receive any more messages of this kind, click here."** A window opens prompting for the email address at which the notifications are being received. The link is valid for 15 days.
- If an email address is entered that appears in any of the settings configured in Panda Endpoint Protection, an email is sent to that address for the user to confirm that they want to opt out of the notifications sent for that account.
- Click the link in the email received to delete the email address from all the settings in which it appears. The link is valid for 24 hours.

Chapter 19

Scheduled sending of reports and lists

Panda Endpoint Protection 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	447
Report types	448
Requirements for generating reports	449
Accessing the sending of reports and lists	449
Managing reports	451
Configuring reports and lists	452
Contents of the reports and lists	454

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 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 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 modules or set filters to restrict the information displayed to computers that meet certain criteria.

Report types

Panda Endpoint Protection enables you to generate three types of reports, each with its own features:

- List views
- Executive reports
- Lists of devices

Next is a summary of the features of each type of report:

Type	Period	Sent	Contents	Format
List views	Instant	Automatically	Configurable using searches	CSV
Executive reports	Consolidated	Automatically and on demand	Configurable by categories and groups	PDF, CSV, Excel, Word
Lists of devices	Instant	Automatically	Configurable using filters	CSV

Table 19.1: Summary of report types and their features

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 [50](#) 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. See [Filter free](#) on page [184](#) 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.

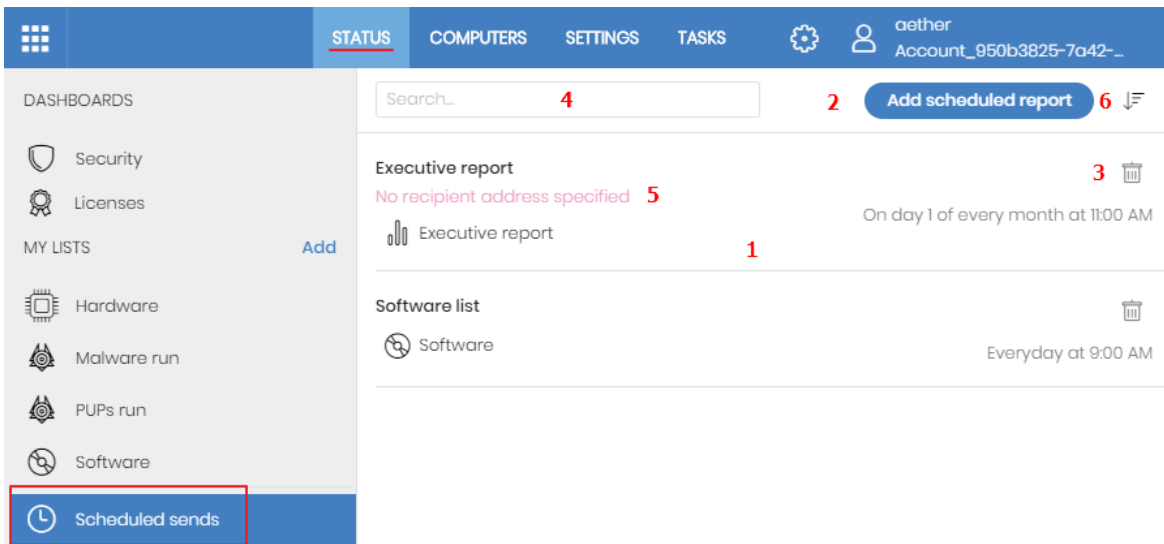


Figure 19.1: Page for managing scheduled sending of reports

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 [Configuring reports and lists](#)
- **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 [Configuring reports and lists](#)

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 [Configuring reports and lists](#)

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 [List of scheduled reports](#).

Managing reports

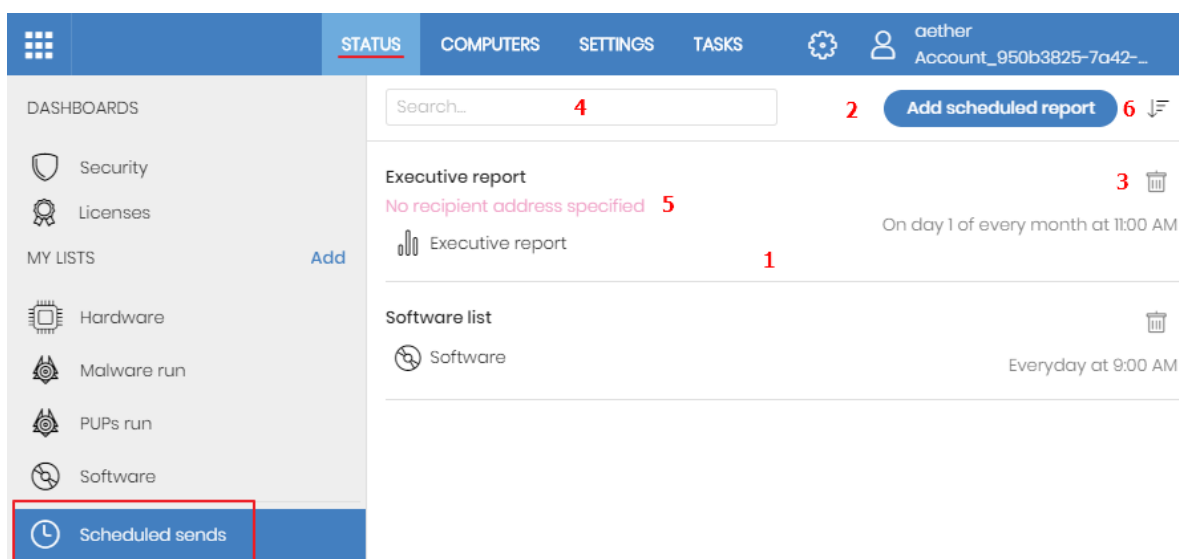


Figure 19.2: Page for managing scheduled sending of reports

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 ([Figure 19.1](#)).

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 ([Figure 19.1: 5](#))

Creating scheduled reports

Click the **Add scheduled report** button ([Figure 19.1: 2](#)) to show the settings window.

See [Configuring reports and lists](#) 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 ([Figure 19.1: 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.

Configuring reports and lists

Field	Description
Name	Name of the entry shown in the list of scheduled reports.
Send automatically	<p>Frequency with which the report or list will be sent:</p> <ul style="list-style-type: none"> • Every day: It will be sent every day at the scheduled time. • Every week: It will be sent every week on the scheduled day and at the scheduled time • Every month: It will be sent every month at the scheduled time on the scheduled date.
Report type	<p>Type of report to send:</p> <ul style="list-style-type: none"> • Executive report • List • Filter <p>See Contents of the reports and lists.</p>
Preview report	<p>This link is only displayed when the report type chosen is Executive Report. Click the link to open a new tab in the browser showing the contents of the report so it can be reviewed before scheduling it, downloading it, or printing it using the top toolbar.</p> <p>For lists, the format is CSV and the preview option is therefore not available.</p>
Dates	Time period covered by the report.

Field	Description
	<ul style="list-style-type: none"> • Last month • Last 7 days • Last 24 hours <p>This field is only displayed for executive reports. The lists contain data relevant to the moment they are created.</p>
Computers	<p>The computers from which data will be extracted to generate the executive report:</p> <ul style="list-style-type: none"> • All computers. • Selected groups: Shows the group tree from which individual groups can be selected using the checkboxes. <p>This field is only displayed for executive reports.</p>
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.
Format	<ul style="list-style-type: none"> • For list views: A CSV file is attached to the email. • For executive reports: A PDF, Excel, or Word file containing the report is attached to the email.
Language	Language of the report.
Contents	<p>Type of information included in the report:</p> <ul style="list-style-type: none"> • Table of contents: List of the sections in the report. • License status: Shows information about the licenses contracted and used as well as their expiration dates. See Licenses on page 161. • Security status: The status of the Panda Endpoint Protection software on the network computers on which it is installed. • Detections: Shows the threats detected on the network. • Patch management: Shows the status of computers regarding patches.

Field	Description
	<p>See “Panda Patch Management widgets/panels on page 317.</p> <ul style="list-style-type: none"> • Encryption: Shows the encryption status of the computers on the network. See Panda Full Encryption module panels/widgets on page 378. <p>See Contents of the reports and lists.</p>

Table 19.2: Information for generating on-demand reports

Contents of the reports and lists

Lists

The content of the lists sent is similar to that generated when clicking the **Export** or **Detailed export** button of a list view. If the list view supports detailed exports, when configuring the send task two options are shown:

- **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

See [Managing lists](#) on page [45](#) for more information about the types of lists available in Panda Endpoint Protection and their content.



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 for a smaller number of computers than those displayed when it was first created.

Lists of devices

The content of the report sent corresponds to the basic exported list of devices filtered by certain criteria. See [The Computers area](#) on page [182](#) for more information about the contents of the CSV file sent. See [Filter tree](#) on page [184](#) for information about how to manage and configure filters.

Executive report

Depending on the settings defined in the **Contents** field, the executive report can have the following data:

Overview

- **Created on:** Date the report was created.
- **Period:** Time period covered by the report.
- **Included information:** Computers included in the report.

Table of contents

Shows a list with links to 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 the license contract expires.

See "[Licenses](#) on page 161".

Network security status

Operation of the protection module on the network computers on which it is installed.

- **Protection status:** See [Protection status](#) on page 400.
- **Online computers:** See [Offline computers](#) on page 403.
- **Up-to-date protection:** See [Outdated protection](#) on page 404.
- **Up-to-date knowledge:** See [Outdated protection](#) on page 404.

Detections

The threats detected on the network.

- **Top 10 computers with most detections:** The top 10 computers with most detections by the antivirus module during the specified period:
 - **Computer:** Name of the computer.
 - **Group:** Group to which the computer belongs.
 - **Detections:** Number of detections during the specified period.
 - **First detection:** Date of first detection.
 - **Last detection:** Date of last detection.
- **Threats detected by the antivirus:** See [Threats detected by the antivirus](#) on page 405.

Patch management

Status of computers regarding patches.

- **Patch management status:** See [Patch management status](#) on page [317](#).
- **Top 10 computers with most available patches:** List of the ten computers with most patches available but not installed, grouped by type: security patches, non-security patches, and Service Packs. See [Available patches](#) on page [323](#).
- **Top 10 most critical patches:** List of the ten most critical patches sorted by the number of computers affected. See [Available patches](#) on page [323](#).

Encryption

Encryption status of computers. It includes the following widgets and lists:

- **Encryption status:** See [Encryption status](#) on page [378](#).
- **Computers supporting encryption:** See [Computers supporting encryption](#) on page [380](#).
- **Encrypted computers:** See [Encrypted computers](#) on page [381](#).
- **Authentication method applied:** See [Authentication method applied](#) on page [383](#).
- **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.

Remediation tools

Panda Endpoint Protection 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

Automatic computer scanning and disinfection	458
On-demand computer scanning and disinfection	458
Computer restart	466
Reporting a problem	466
Allowing external access to the web console	467
Removing ransomware and restoring the system to a previous state	467

Table **Table 1.1:** 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.

Remediation tool	Platform	Type	Purpose
On-demand restart	Windows	Manual	Forces a computer restart to apply updates, finish manual disinfection tasks, and fix protection errors.

Table 20.1: Panda Endpoint Protection remediation tools

Automatic computer scanning and disinfection

The Panda Endpoint Protection 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 277 for more information about the options available for the Panda Endpoint Protection 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 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

Permissions required to manage Scheduled scan tasks

To manage **Scheduled scan** tasks, the user account used to access the web console must have the **Launch scans and disinfect** permission assigned to its role.




For more information about the permission system implemented in Panda Endpoint Protection, see [Understanding permissions](#) on page 59. For more information about how to manage the tasks run on workstations and servers, view their results, and edit their settings, see [Tasks](#) on page 469.

There are two ways to scan and disinfect computers on demand:

- Create a scheduled scan task.
- Run an immediate scan.

Creating a task from the computer tree

The computer tree enables you to define scan tasks for all computers in a computer group very quickly.

- Go to the **Computers** menu at the top of the console. From the panel on the side, click the  icon to display the computer tree's folder view.
- From the computer tree, click the context menu icon of the group whose computers you want to scan and disinfect. The context menu of the relevant branch opens.
- Click one of the following two options:
 - **Scan now**: Create a scan task and run it immediately on all computers in the group.
 - **Schedule scan**: Opens the **Tasks** area where you can create a recurring and/or scheduled task. The task template is partially populated: The **Recipients** field shows the group selected in the computer tree. Configure the remaining parameters as explained in section [Creating a task from the Tasks area](#) on page 471.

Immediate tasks

Immediate tasks (launched through the **Scan now** option in the context menu) have the following characteristics:

- You can select the scan type (**The entire computer** or **Critical areas**). See section [Task schedule and frequency](#) on page 472 for more information.
- They scan the computer's local file system; network drives are ignored.
- **You do not need to specify an execution time or repetition interval**: They are one-time tasks which start right after being configured.
- **You do not need to publish them**: They are automatically published by Panda Endpoint Protection.

- The management console displays a pop-up message informing of the success or failure of the task creation operation.

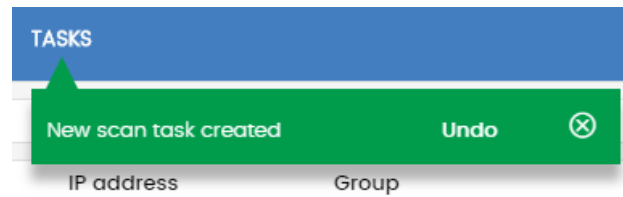


Figure 20.1: Scan task created message

Scheduled tasks

Scheduled tasks (launched through the **Schedule scan** option in the context menu) are identical to the tasks created from the **Tasks** area and discussed in section [Creating a task from the Tasks area](#) on page 471. The only difference is that the **Recipients** field is populated with the group selected in the computer tree. Therefore, you must specify the task's execution time and repetition interval, and publish it for activation.

Creating a task from the Computers list

The **Computers** area enables you to create tasks in a similar way to the computer tree or the **Tasks** area. However, in this case you can individually select computers belonging to the same group or subgroup.

Use one of the following resources depending on the number of computers you want to receive the task:

- **Context menu:** If you want to apply the task to one computer only.
- **Checkboxes and action bar:** If you want to apply the task to one or more computers belonging to a group or subgroup.

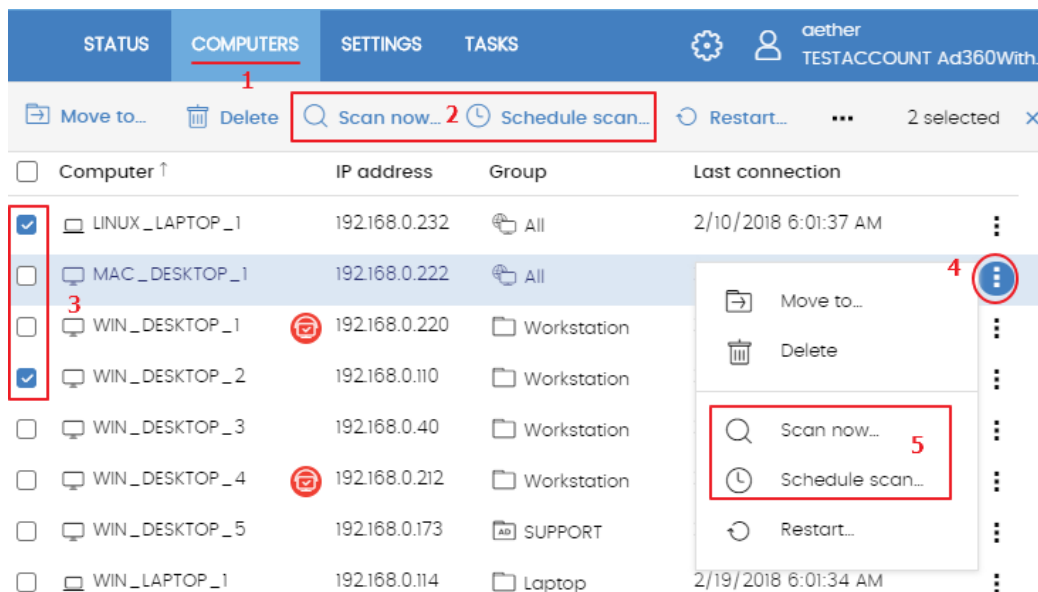




Figure 20.2: Context menus and action bar for quick task creation

Context menu associated with a single computer

- Click the **Computers(1)** menu at the top of the console. From the computer tree, select the group that the computer you want to scan belongs to.
- From the computer list, click the context menu icon of the computer you want to scan. **(4)**
- From the context menu **(5)**, click one of the following two options:
 - **Scan now:** Create a scan task that is run immediately on the selected computer.
 - **Schedule scan:** Opens the **Tasks** area. The task template is partially populated: The Recipients field shows the selected computer. Configure the remaining parameters as explained in section [Creating a task from the Tasks area](#) on page 471.

Checkboxes and action bar

- Click the **Computers (1)** menu at the top of the console. From the computer tree, select the group that the computers you want to scan belong to.
- Use the checkboxes **(3)** to select the computers you want to scan. An action bar **(2)** appears at the top of the page.
- Click one of the following icons:
 - **Scan now** : Create a scan task that is run immediately on the selected computers.
 - **Schedule scan** : Opens the **Tasks** area. The task template is partially populated: The Recipients field shows the computers selected in the **Computer tree**. Configure the remaining parameters as explained in section [Creating a task from the Tasks area](#) on page 471.

Scan options

The scan options enable you to configure the antivirus engine parameters in order to scan your computers' file systems.

Value	Description
Scan type	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • %WinDir%\system32 • %WinDir%\SysWow64 • Memory • Boot system • Cookies • Specific items: Runs a scan of a selected storage device. This option supports environment variables. The solution scans the specified path and every folder and file it contains.
Detect viruses	Enable this toggle to detect programs that enter computers with malicious purposes. This toggle 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	<ul style="list-style-type: none"> • 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.

Value	Description
	<p>Enter multiple file extensions separated by commas.</p> <ul style="list-style-type: none"> • 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 20.2: 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 20.3: 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 folder tree that the computer belongs to.	Character string

Field	Description	Value
Detections	Number of detections made on the computer.	Character string
Status	Status of the task.	<ul style="list-style-type: none"> • All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Start date	Task start date.	Date
End date	Task end date.	Date

Table 20.4: Fields in the Scan task results list

Filter tools

Field	Comment	Values
Status	Status of the task.	<ul style="list-style-type: none"> • All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling

Field	Comment	Values
		<ul style="list-style-type: none"> • Canceled (maximum run time exceeded)
Detections	Computers where detections were or were not made.	<ul style="list-style-type: none"> • All • With detections • No detections

Table 20.5: 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	Values
Computer	Computer name.	Character string
Group	Folder in the Panda Endpoint Protection folder tree that the computer belongs to.	Character string
Threat type	Malware category based on the actions the threat is designed to perform.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Quarantined • Deleted

Field	Description	Values
		<ul style="list-style-type: none"> Disinfected Blocked Process ended
Date	Date the action was taken.	Date


Table 20.6: 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 217 for 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 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 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. To do this, click the **Computers** menu at the top of the console. Select the computer with errors and click its context menu. Select **Report a problem** from the menu displayed.

Allowing external access to the web console

If you find problems you cannot resolve, you can grant the Panda Security support team access to your console. Follow these steps:

- Click the **Settings** menu at the top of the console. Select **Users** from the side menu.
- 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 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 **400** 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 **Computer discovery** on page **103**.

- 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 [281](#).
- 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 the anti-tamper protection and password](#) on page [272](#).
- 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 [273](#).
- 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 [301](#).
 - 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.

Tasks

A task is a resource implemented in Panda Endpoint Protection 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	469
Creating a task from the Tasks area	471
Task publication	474
Task list	474
Task management	475
Task results	476
Automatic adjustment of task recipients	478

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 publication:** The tasks you create must be entered in the Panda Endpoint Protection 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 enables you to launch the following tasks:

- Scan and disinfect files. See [On-demand computer scanning and disinfection](#) on page [458](#) for more information.
- Install patches and updates for the operating system and other programs installed on users' computers. See [Panda Patch Management \(Updating vulnerable programs\)](#) on page [301](#) for more information.

Permissions associated with task management



For more information about the permission system implemented in Panda Endpoint Protection, see [Understanding permissions](#) on page [59](#).

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

- Select **Tasks** in the top menu. A list of all created tasks and their status opens.
- Click the **Add task** button and select a task type from the drop-down menu. 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 will receive the task.
 - **Schedule (3)**: Task schedule (day and time the task will be launched).
 - **Settings (4)**: Specify the actions to be taken by the task. This section varies based on the task type and is described in the documentation associated with the related module.



The screenshot shows the 'New task' configuration page for a scan task. At the top, there are 'Cancel', 'New task', and 'Save' buttons. The form is organized into several sections:

- Overview (1)**: Contains 'Name: New scan task', 'Description: Description', and 'Recipients: No recipients selected yet'.
- Schedule (3)**: Includes 'Starts:' with options for 'As soon as possible', a date field (7/2/2020), a time dropdown (9:00 AM), and a checked checkbox for 'Computer's local time'. Below this is a section for 'If the computer is turned off at the scheduled time, run the task as soon as' with a dropdown menu set to '1 week'.
- Settings (4)**: Includes 'Maximum run time: No limit' and 'Repeat: Every week'.
- Scan options**: Includes 'Scan type: Critical areas (recommended)', 'Detect viruses: [checked]', and 'Detect hacking tools and PUPs: [checked]'.

Figure 21.1: Overview of the New task page for a scan task

Task recipients (2)

- Click the **No recipients selected yet** link in the **Recipients** section. A page opens where you can select the computers that will 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.



To access the computer selection page, you must first save the task. If you have not saved the task, a warning message is displayed.

- Click the **View computers** button to view the computers that will receive the task.

Task schedule and frequency

You can configure the following three parameters:

Starts: Indicates the task start 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 computer's local time or the Panda Endpoint Protection server time should be considered.
If the computer is turned off	<p>If the computer is turned off or cannot be accessed, the task will not run. The task scheduler enables you to establish the task's expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available).</p> <ul style="list-style-type: none"> • 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 system waits indefinitely for the computer to be available to launch the task.

Table 21.1: Task launch parameters

Maximum run time: Indicates the maximum time that the task can take to complete. After that time, the task 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 21.2: Task duration parameters

- **Frequency:** Set a repeat interval (every day, week, month, or year) from the date specified in the **Starts:** field.

Value	Description
One time	The task is run only once at the time specified in the Starts: field.
Daily	The task is run every day at the time specified in the Starts: field.
Weekly	Use the checkboxes to select the days of the week on which the task must be run, at the time specified in the Starts: field.
Monthly	Choose an option: <ul style="list-style-type: none"> • 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 is run on the last day of the month. • Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 21.3: Configuring the frequency of a task

Lower versions of the security software

If the recipient computers have a lower version of the security software, 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 is added to the list of configured tasks. However, it displays 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 task scheduler, which will launch 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.	<ul style="list-style-type: none"> •  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	<ul style="list-style-type: none"> • No recipients: The task will not run because there are no 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. 	Character string

Field	Comment	Values
	<ul style="list-style-type: none"> • 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 21.4: Fields in the Tasks list

Filter tool


Field	Comment	Values
Type	The task type.	<ul style="list-style-type: none"> • Scan • Disinfection • Patch installation • Patch uninstallation • All
Search task	Enter the task name.	Character string
Schedule	The task repeat frequency.	<ul style="list-style-type: none"> • All • Immediate • Once • Scheduled
Sort list 	Task list sort order.	<ul style="list-style-type: none"> • Sort by creation date • Sort by name • Ascending • Descending

Table 21.5: Filters available in the Tasks list

Task management

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

Modifying published tasks

Click a task's name to view its settings page. There you can modify some of the task's parameters.




You can change only the name and description of published tasks. To modify other parameters of a published task, you must copy it first.

Canceling published tasks

Select the checkboxes to the left of the tasks to cancel. Click the **Cancel**  icon from the toolbar.

The tasks are canceled, but they do not disappear from the Tasks page so you can still view their results. Only tasks whose status is **In progress** can be canceled.


Deleting tasks

Executed tasks are not automatically deleted. To delete a task, select it using the checkboxes and click the  icon. A published task can only be deleted if it is previously canceled.



Deleting a task also deletes its results.

Copying tasks

To create a new task with the same settings as an existing task, click the  icon.

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 folder tree the computer belongs to.	Character string

Field	Description	Values
Status	<p>Status of the task process on the affected computer:</p> <ul style="list-style-type: none"> • Pending: The task was published successfully, but the target computer has not yet received it or has received it but the task has not yet run because it is scheduled to run at a later time. • In progress: The task is running on the computer. • Finished: The task finished successfully. • Failed: The task failed and returned an error. • Canceled (the task could not start at the scheduled time): The task could not start at the scheduled time because the target computer was turned off or in a state that prevented the task from running. • Canceled: The process was canceled on the computer. • 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. 	Character string
Start date	The task start date.	Date
End date	The task end date.	Date

Table 21.6: Common fields in task results lists

Task filter tool

Field	Description	Values
Date	Drop-down menu with the date the task became active based on the configured schedule. An active task can be launched immediately or wait until the target computer is available. This date is shown in the Date column.	Date
Status	<ul style="list-style-type: none"> • Pending: The task has not been launched as the execution window has not started yet. • In progress: The task is currently running. 	Enumeration

Field	Description	Values
	<ul style="list-style-type: none"> • 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. • Canceled (maximum run time exceeded): The task was automatically canceled because it exceeded its configured maximum run time. 	

Table 21.7: Search filters in task results

Automatic adjustment of task recipients

If the administrator selects a computer group as the recipient of a task, the computers that finally run the task may vary from those initially selected. This is because groups are dynamic entities that change over time.

That is, you can define a task at a specific time (T1) to be run on a specific group containing a series of computers. However, at the time the task is run (T2), the computers in that group may have changed.

When it comes to determining which computers will receive a configured task, there are three cases depending on the task:

- Immediate tasks.
- One-time scheduled tasks.
- Recurring scheduled tasks.

Immediate tasks

These tasks are created, published, and launched almost simultaneously and only once. The target group is evaluated at the time the administrator creates the task. The task status for the affected computers 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 starts 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 22

Hardware, software, and network requirements

Most of the security intelligence that Panda Endpoint Protection generates and uses is generated in the cloud. This intelligence is downloaded and leveraged by the security software installed on users' computers. To make sure the security software works correctly, the customer's IT infrastructure must meet the requirements specified in the next sections.

Chapter contents

Supported features by platform	481
Requirements for Windows platforms	486
Requirements for macOS platforms	490
Requirements for Linux platforms	491
Requirements for Android platforms	493
Requirements for iOS platforms	494
Local ports	495
Access to the web console	496
Access to service URLs	496

Supported features by platform

Available features		Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
General	Web console	X	X	X	X	X

Available features		Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	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 supported by the agent	11	11	11	16	10
Lists and reports	Frequency of sending malware, PUP, and exploit activity data and blocked programs to the server	1 min	10 mins	10 mins	After a scan is completed	N/A
	Frequency of sending other detections to the server	15 min	15 min	15 min	After a scan is completed	15 min
	List of detections	X	X	X	X	X
	Executive report	X	X	X	X	X
	Scheduled executive report	X	X	X	X	X

Available features		Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Protections						
	Contextual detections	X	X			
	Real-time permanent antivirus protection	X	X	X	X	
	Anti-tamper protection	X				
	Anti-Phishing	X		X		X
	Firewall	X				
	Device control	X				
Hardware and software information	Hardware information and list	X	X		X	X
	Software information and list	X	X	X	X	X
	Software change log	X	X	X	X	X
	Information about the OS patches installed	X				
Settings	Security for	X	X	X	N/A	N/A

Available features		Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	workstations and servers					
	Password for uninstalling the protection and taking actions locally	X				
	Security for VPN connections	X				
	Assign multiple proxies	X			N/A	N/A
	Act as Panda proxy	X			N/A	N/A
	Use Panda proxy	X	X	X	N/A	N/A
	Act as a repository/cac he	X			N/A	N/A
	Use repository/cac he	X			N/A	N/A
	Discover unprotected computers	X				
	Email alerts in the event of an infection	X	X	X	X	N/A

Available features		Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	Email alerts when finding unprotected computers	X	X	X	X	N/A
Remote actions from the web console	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				
	Reinstall the protection agent	X				
	Restart	X	X	X		
	Report incidents (PSInfo)	X			X	
Updates	Signature updates	X	X	X	X	N/A
	Protection upgrades	X	X	X	X	N/A

Available features		Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	Schedule protection upgrades	X	X	X	Google Play	App Store
Modules						
	Panda Patch Management	X				
	Panda Full Encryption	X				

Table 22.1: Supported features by platform

(*) Only available for Intel microprocessors and partially on Windows (ARM)

Requirements for Windows platforms

Supported operating systems

Workstations with an x86 or x64 microprocessor

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 11 (64bits)

Computers with an ARM microprocessor

- Windows 10 Pro
- Windows 10 Home
- Windows 11 Pro
- Windows 11 Home

Servers with an x86 or x64 microprocessor

- Windows 2003 (32-bit, 64-bit, and R2) SP2 and later
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016 and 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016, and 2019
- Windows Server 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)



Embedded systems can be installed in a customized way, and so the way Panda Endpoint Protection and some of its modules work on such systems can vary greatly depending on the installation. Install Panda Endpoint Protection and check the various protections work correctly.

Hardware requirements

- **Processor:** x86 or x64-compatible CPU with at least SSE2 support.
- **RAM:** 1 GB
- **Available hard disk space for installation:** 650 MB

Other requirements

Update root certificates

For the product to operate correctly, the root certificates on all protected computers must be kept 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 stop working.



To identify and update root certificates, use the tool available at <https://www.pandasecurity.com/resources/tools/wescertcheck.zip>

Time synchronization of computers (NTP)

Although not an essential requirement, it is advisable that the clocks on computers protected by Panda Endpoint Protection be synchronized. This synchronization is normally achieved using an NTP server.

If a computer is not synchronized, several security issues could arise:

- A lack of stability in the communications between the computer and the Panda Security servers.
- Errors checking certificates, which will appear as valid or expired based on the computer system date, not the real date.
- Date errors in the alerts generated by the protections, which will display the computer system date, not the real date.
- The scan and patch installation tasks will display the computer system date, not the real date.
- The installer expiration date will not be respected.
- 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	Link to KB4474419 Link to SP2
Windows Server 2008 x86/Server 2008 x64	SP2 and KB4474419	Link to KB4474419 Link to SP2
Windows 7 x86/Windows 7 x64	SP1 and KB4474419	Link to KB4474419 Link to SP1
Windows 2008 R2 x64	KB4474419	Link to KB4474419

Table 22.2: 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 404 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 217.

To find computers that do not support SHA-256 driver signing, create a filter in the filter tree with the parameters shown in [Filter computers not compatible with SHA-256 signed drivers](#) on page 190. For more information about the filter tree, see [Filter tree](#) on page 184.



We recommend that you update all computers to make sure they are protected with the latest available version of the protection software.

After you install the patches indicated, the latest available version of the protection software downloads within four hours. You must restart the computer to complete the update.

Requirements for macOS platforms

Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey

Hardware requirements

- **Processor:** Intel® Core 2 Duo
- **RAM:** 2 GB
- **Free space for installation:** 400 MB
- **Ports:** 3127, 3128, 3129, and 8310 must be accessible for the web anti-malware to work.

Required permissions

For the protection to function correctly, you must assign permissions to enable the security software in the macOS. Enable network extensions, system extensions, and Full Disk Access.

Complete these instructions for your macOS version:

Instructions for macOS Catalina or higher

To enable system extensions:

- Open the Panda Endpoint Protection agent on the user computer. Click **Open Security Preferences panel**.
- 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 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.

Instructions for macOS Mojave 10.14 or lower

When Panda Endpoint Protection starts, the operating systems could block the kernel extensions required for the protection to function correctly.

This is because these macOS versions include a security feature that requires user approval before loading 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 and macOS presents two alerts:

- System Extension Blocked message.
- Your Computer is Unprotected message.

To resolve it, follow these steps:

- In the System Extension Blocked message, click **OK**. You can also click the **Open System Preferences** button in the Your Computer is Unprotected message. The **System Preferences** window opens.
- Click **Security & Privacy**.
- In the lower-left corner, click the lock icon.
- In the **Security & Privacy** dialog box, click **Allow**. System extensions are enabled.

Requirements for Linux platforms

Panda Endpoint Protection can be installed on both Linux workstations and servers. On computers with no graphical environment installed, the URL filtering and web detection features are disabled. To manage protection on computers with no graphical environment, use the `/usr/local/protection-agent/pa_cmd` tool.

To install Panda Endpoint Protection on Linux platforms, the target computer must remain connected to the Internet during the installation process.

Supported 64-bit distributions

- **Ubuntu:** 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04 and 21.10
- **Fedora:** 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, and 34.
- **Debian:** 8, 9, 10, and 11.
- **Red Hat:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4 and 8.5
- **CentOS:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4 and 8.5
- **Linux Mint:** 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2, 19.3, 20, 20.1, 20.2, 20.3.
- **SUSE Linux Enterprise:** 11.2, 11.3, 11.4, 12, 12.1, 12.2, 12.3, 12.4, 12.5, 15, 15.1, 15.2, and 15.3.
- **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, 8.0, 8.1, 8.2, 8.3, 8.4 and 8.5.

Supported 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/en/support/card?id=700009#show2>.

Panda Endpoint Protection is not supported on special or modified versions of the Linux kernel.

Supported file managers

- Nautilus
- PCManFM
- Dolphin

Hardware requirements

- **Processor:** x86 or x64-compatible CPU with at least SSE2 support.
- **RAM:** 1.5 GB.
- **Free space for installation:** 100 MB.
- **Ports:** 3127, 3128, 3129, and 8310 must be open for the web malware detection feature to work.

Installation package dependencies

During installation, the Linux agent downloads all packages required to satisfy dependencies. In general, the packages the system requires to operate correctly are:

- Libcurl
- OpenSSL
- GCC and Fedora's build tools (make, makeconfig, etc.)



The installation process on Fedora includes building of the modules required by the Panda Endpoint Protection agent to operate correctly.

To display 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`

Requirements for Android platforms

Supported operating systems

- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0
- Pie 9.0
- Android 10
- Android 11

Hardware requirements

At least 10 MB of internal memory is required on the target device. Based on the device model, it is possible that more free space is required.

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 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

Requirements for iOS platforms

Supported operating systems

- iOS 13/iPadOS 13
- iOS 14/iPadOS 14
- iOS 15/iPadOS 15

Network requirements

The app installed on the mobile device uses the Apple Push Notification service (APNs) to communicate with Panda Endpoint Protection. In normal conditions, if the target device is connected to the cellular network (2G/3G/4G or higher), it is not necessary to meet any specific network requirements.

If the device is connected to a Wi-Fi network, access point (AP), or uses an alternate method to connect to the Internet, it must be able to connect to specific servers through these ports:

- TCP port 5223 to communicate with APNs.
- TCP port 443 or 2197 to send notifications to APNs.

The servers in APNs use load balancing. Therefore, the target device will not always connect to the same IP addresses. If possible, allow connections to the entire 17.0.0.0/8 range used by Apple on the firewall. Otherwise, allow connections to these IP address ranges:

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

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 features, the user of the device must allow these permissions:

- Get location
- Device location services
- Background location access
- Filter network content
- Receive push notifications

Local ports

To implement certain features, the security software installed on the computers on the network uses the following listening ports:

- **TCP port 18226**: Used by computers with the cache/repository role to serve files. See [Cache/repository role](#) on page 261.
- **TCP port 21226**: Used by computers with the cache/repository role to request the files to download. See [Cache/repository role](#) on page 261.
- **TCP port 3128**: Used by computers with the proxy role. See [Proxy role](#) on page 260.

- **UDP port 21226**: Used by computers with the discovery computer role. See [Discovery computer role](#) on page 263
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox. See [Configuring Secure VPN](#) on page 270

Access to the web console

The management console is accessible with the latest version of these browsers:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

Access to service URLs

For Panda Endpoint Protection to work correctly, the protected computers must be able to access the following URLs.

Product name	URLs
Panda Endpoint Protection	<ul style="list-style-type: none"> • https://*.pandasecurity.com <ul style="list-style-type: none"> • Downloading of installers, the generic uninstaller, and policies. • Agent communications (registration, configuration, tasks, actions, status, real-time communications). • Communications between the protection and Collective Intelligence. • Downloading of signature files on Android systems. • http://*.pandasecurity.com <ul style="list-style-type: none"> • Downloading of signature files (on all systems except Android). • https://*.windows.net <ul style="list-style-type: none"> • Performance counters (CPU, memory, disk, etc.) • Notifications every 15 minutes if there is no real-time communication.
Root certificates	<ul style="list-style-type: none"> • http://*.globalsign.com

Product name	URLs
	<ul style="list-style-type: none"> • http://*.digicert.com • http://*.sectigo.com
Panda Patch Management	<p>All URLs in the following resource: https://forums.ivanti.com/s/article/URL-Exception-List-for-Ivanti-Patch-for-SCCM</p> <p>https://content.ivanti.com</p>
Activity testing	<ul style="list-style-type: none"> • http://proinfo.pandasoftware.com/connectiontest.html <p>For Windows protection versions higher than 8.00.16.</p> <ul style="list-style-type: none"> • http://*.pandasoftware.com <p>For connectivity tests.</p>

Table 22.3: Service access URLs

Ports

- Port 80 (HTTP)
- Port 443 (HTTPS, WebSocket)
- Port 8080 (access from Orion)

Patch and update downloads (Panda Patch Management)

See the following support article <https://www.pandasecurity.com/uk/support/card?id=700044> for a full list of the URLs that must be accessible from the network computers that will receive patches, or from the network computers with the cache/repository role.

Chapter 23

The Panda Account

The Panda Account provides administrators with a safer mechanism to self-manage login credentials and access the Panda Security services purchased by their organization than the standard method of receiving credentials by email.

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



Users with access to the Panda Account are those who were initially registered in Panda Security, regardless of whether they have later been migrated to the WatchGuard provider or not. Users belonging to the WatchGuard security provider from the start do not have access to the Panda Account.

Chapter contents

Creating a Panda Account for Panda Security users	499
Activating the Panda Account	500
Creating and linking a Panda Account to WatchGuard	501

Creating a Panda Account for Panda Security users

To create a new Panda Account, follow the steps below:

Receive the email

- When purchasing Panda Endpoint Protection, you will receive an email from Panda Security.
- Click the link in the message to access the website from which you can create your Panda Account.

Fill out the form

- Enter your details in the form shown.
- Use the drop-down menu located in the lower-right corner if you want to view the page in a different language.
- Access the License Agreement and the Privacy Policy by clicking the relevant links.
- Click **Create** to finish and receive an email at the address indicated in the form. Use that message to activate your account.

Activating the Panda Account

After it is created, you need to activate your Panda Account. To do this, you must use the message received at the email address you specified when creating your Panda Account.

- Find the message in your inbox.
- Click the activation button. By doing this, the address provided when creating your Panda Account will be confirmed as valid. If the button does not work, copy and paste the URL included in the message into your browser.
- The first time you access your Panda account, you will be asked to confirm your password. Do it and click the **Activate account** button.
- Enter the required information and click **Save data**. If you prefer to provide your data at another time, use the **Not now** option.
- Accept the License Agreement and click **OK**.

After your Panda Account has been successfully activated, you are taken to the Panda Cloud site home page. From there, you can access the Panda Endpoint Protection web console. To do this, click the solution's tile you will find in the **My Services** section.

Editing the Panda Account

If your associated security provider is Panda Security, click the **Edit account** option in Panda Cloud.



Figure 23.1: Editing the user account

If your associated security provider is WatchGuard, go to <https://watchguard.com/>

Creating and linking a Panda Account to WatchGuard



For more information about how to activate and link a Panda Account when activating a commercial license, see <https://www.pandasecurity.com/es/support/card?id=300003>.

To manage Aether products, WatchGuard users must meet the following requirements:

- They must have a WatchGuard user account.
- They must have a Panda Endpoint Protection user account.
- They must link both accounts.

Users belonging to the WatchGuard security provider from the start automatically create a Panda account when activating a commercial license for a Panda Security product for the first time.

Users belonging to the WatchGuard security provider but who initially belonged to Panda Security already have a Panda Account. All they have to do is link that account to their WatchGuard Account.

Creating a Panda Account automatically when assigning a commercial license for a Panda Security product

- Go to <https://watchguard.com/activate> and enter the license key for the Panda Security product.

- Click **I need a Panda account**. A page opens with the account name and ID. We recommend that you save this information. You may need to provide it if you contact Support.
- Click **Submit** and **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.
- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Panda Endpoint Protection.
- To access Panda Endpoint Protection, click **Manage Your Panda Product**. Next, click **Accept and continue** to accept the End User License Agreement.

Linking a Panda Account to a WatchGuard Account when assigning a commercial license for a Panda Security product

- Go to <https://watchguard.com/activate> and enter the license key for the Panda Security product.
- Click **Link my Panda account**. The Panda Cloud page opens. Enter your Panda Endpoint Protection login credentials. These were sent to you in the welcome email.
- Click the **Log in** button. A page opens indicating that both accounts are linked.
- Click **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.
- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Panda Endpoint Protection.
- To access Panda Endpoint Protection, click **Manage Your Panda Product**. Next, click **Accept and continue** to accept the End User License Agreement.

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-Tamper protection

A set of technologies aimed at preventing tampering of the Panda Endpoint Protection processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

Anti-Theft

Set of technologies incorporated into Panda Endpoint Protection and designed to locate lost or stolen mobile devices and minimize data exposure in the case of theft.

Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, contextual analysis, etc.), to detect and remove computer viruses and other threats.

ARP (Address Resolution Protocol)

A telecommunication protocol used for resolution of Internet layer addresses into link layer addresses. On IP networks, this protocol translates IP addresses into physical MAC addresses.

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 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 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.

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 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 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 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 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 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 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, 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

Settings

See Settings profile.

Settings profile

Specific settings governing the protection or any other aspect of the managed computer. Profiles are assigned to a group or groups

and then applied to all computers that make up the group.

Signature file

File that contains the patterns used by the antivirus to detect threats.

SMTP server

Server that uses SMTP (Simple Mail Transfer Protocol) to exchange email messages between computers.

Spyware

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and collects personal data.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

Suspicious item

A program with a high probability of being malware and classified by our heuristic scanner. This type of technology is only used in the scheduled and on-demand scans launched from the Tasks module, never in real-time scans. Heuristic scanning is used to compensate for the lower detection capability of scheduled scan tasks, in which program code is scanned statically, without running the program. 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 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 console

Tool to manage the advanced security service Panda Endpoint Protection, 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 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.

