Panda Adaptive Defense 360

Panda Adaptive Defense 360 on Aether Administration Guide

Version: 3.40.00-00a

Author: Panda Security

Date: 8/27/2018

Contents

1. Preface

1.1. Introduction

This guide contains basic information and procedures for making the most out of **Panda Adaptive Defense 360 on Aether**.

1.2. Who is this guide aimed at?

This documentation is aimed at network administrators in charge of managing corporate IT security.

To get the most out of **Panda Adaptive Defense 360 on Aether**, certain technical knowledge of the Windows environment is required with respect to processes, the file system and the registry, as well as understanding the most commonly-used network protocols. This way, network administrators can accurately interpret the information in the management console and draw conclusions that help to bolster corporate security.

1.3. What is Panda Adaptive Defense 360 on Aether?

Panda Adaptive Defense 360 on Aether is a managed service that allows organizations to protect their IT assets, find out the extent of any security problem detected, and develop prevention and response plans against unknown and advanced persistent threats (APTs).

Panda Adaptive Defense 360 on Aether is divided into two clearly defined functional areas:

- Panda Adaptive Defense 360
- Aether Platform

Panda Adaptive Defense 360

This is the module 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

This is a scalable and efficient platform for the centralized management of Panda Security's solutions. **Aether** facilitates the real-time presentation of the information generated by **Panda Adaptive Defense 360** about processes, the programs run by users and the devices installed, in an organized and highly detailed manner.

Aether is perfectly suited to address the needs of key accounts and MSPs.

1.4. Icons

The following icons are used in this guide:

ⓘ	Additional information, such as an alternative way of performing a certain task
💡	Suggestions and recommendations
⚠	Important advice regarding the use of features in **Panda Adaptive Defense 360**
🔍	Additional information available in other chapters or sections of the guide

2. Introduction

2.1. Introduction

Panda Adaptive Defense 360 on Aether is a solution based on multiple protection technologies which allows organizations to replace the traditional antivirus solution installed on their network with a complete, managed security service.

It allows the execution of legitimate software only

Panda Adaptive Defense 360 monitors and classifies all processes run on the customer's IT network based on their behavior and nature. The service protects workstations and servers by allowing only those programs classified as trusted to run.

It adapts to the organization's environment

Unlike traditional antivirus solutions, **Panda Adaptive Defense 360 on Aether** leverages a new security approach that allows it to accurately adapt to the environment of any given company, monitoring the running of all applications and learning continuously from the actions taken by each process.

After a brief learning period, **Panda Adaptive Defense 360 on Aether** is able to offer a far greater level of security than traditional antivirus solutions.

Assessment and remediation of security problems

The solution's security offering is completed with monitoring, forensic analysis and remediation tools that enable administrators to determine the scope of the incidents detected and resolve them.

Continuous monitoring provides valuable information about the context in which the security problems took place. This information allows administrators to assess the impact of incidents and take the necessary measures to prevent them from occurring again.

Cross-platform service

Panda Adaptive Defense 360 on Aether is a cloud-based cross-platform service compatible with Windows, macOS, Linux and Android devices. It provides administrators with a single tool to ensure the security of all computers in the organization, without the need to install new management infrastructure and thereby reducing the total cost of ownership (TCO).

2.2. Panda Adaptive Defense 360 on Aether: key features

Panda Adaptive Defense 360 is a managed service that offers guaranteed security for companies against advanced threats and targeted attacks. It is based on four pillars:

- **Visibility**: tracks every action taken by running applications.
- **Detection**: constant monitoring of running processes, and real-time blocking of zero-day and targeted attacks, as well as other advanced threats designed to bypass traditional antivirus solutions.

- **Response:** forensic information for in-depth analysis of every attempted attack, as well as remediation tools.
- **Prevention**: prevent future attacks by editting the settings of the different protection modules and patching the vulnerabilities found in the operating systems and applications installed.

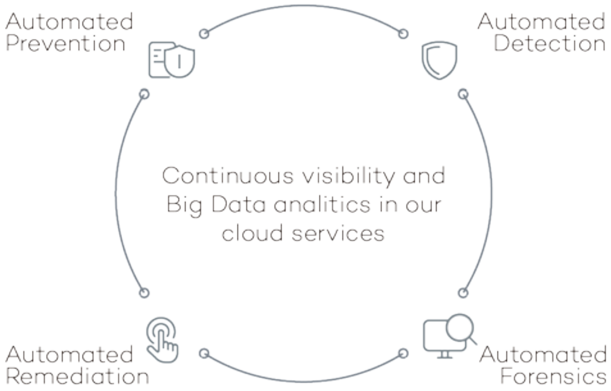


*Figure 1: the four pillars of **Panda Adaptive Defense 360**'s advanced protection*

2.3. Aether Platform: key features

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

Aether Platform manages communication with the agents deployed across the network. Plus, it management console presents the data gathered by **Panda Adaptive Defense 360** in the simplest and easiest to understand way for later analysis by the network administrator.

Panda Adaptive Defense 360, in turn, has been developed to get the most out of the services delivered by Aether Platform, focusing all efforts on improving customers' security.

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. **Panda Adaptive Defense 360** has been developed to get the most out of the services delivered by the **Aether** platform, focusing all efforts on improving customers' security. **Aether**, in turn, manages communication with the agents deployed and the administrator of the solution via the management console, and the presentation and processing of the information collected by **Panda Adaptive Defense 360** to be analyzed.

2.3.1 Key benefits of Aether

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

- **Cloud management platform**

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

- It does not require management servers to host the management console on the customer's premises: as it operates from the cloud, it can be accessed directly by all devices subscribed to the service, from anywhere and at any time, regardless of whether they are office-based or on-the-road.
- Network administrators can access the management console at any moment and from anywhere, using any compatible Internet browser from a laptop, desktop or even mobile devices such as tablets or smartphones.
- It is a high-availability platform, operating 99.99% of the time. Network administrators don't need to design and deploy expensive systems with redundancy to host the management tools.

- **Real-time communication with the platform**

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

- **Multi-product and cross-platform**

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

- **Minimize 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 between products**: all products report through the same console and on a single platform: 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 into a single format.
- **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, macOS, Linux and Android.

- **Flexible and granular settings**

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

- **Complete and customized information**

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

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

2.3.2 Aether architecture

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

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

Figure 2 shows a high-level diagram of **Aether Platform**.

2.3.3 Aether on users' computers

Network computers protected by **Panda Adaptive Defense 360 on Aether** have a software program installed, made up of two independent yet related modules, which provide all the protection and management functionality:

- **Panda communications agent module**: this acts as a bridge between the protection module and the cloud, managing communications, events and the security settings implemented by the administrator from the management console.
- **Panda Adaptive Defense 360 protection module**: this is responsible for providing effective protection for the user's computer. To do this, it uses a communications agent to receive the configurations and send statistics and detection information and details of the items scanned.

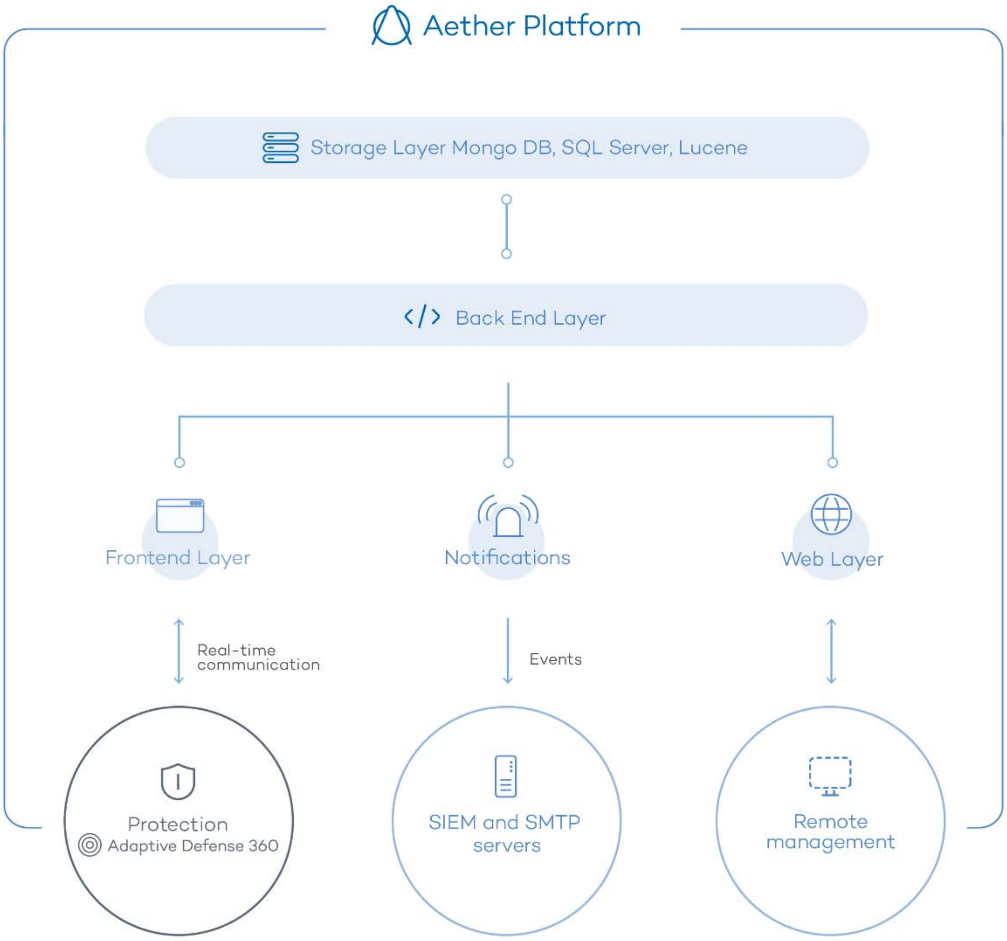


*Figure 2: logical structure of **Aether Platform***

- **Panda real-time communications agent**

The Panda agent handles communication between managed computers and the **Panda Adaptive Defense 360** server. It also establishes a dialog among the computers that belong to the same network in the customer's infrastructure**.**

This module, besides managing local processes, also gathers the configuration changes made by the administrator through the Web console, and applies them to the **Panda Adaptive Defense 360** protection module.

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

The settings configured by the network administrator via the **Panda Adaptive Defense 360** management console are sent to the backend through a REST API. The backend in turn forwards them to the Command Hub, generating a POST command which pushes the information to all managed devices. This information is transmitted instantly provided the communication lines are not congested and every intermediate element is working properly.

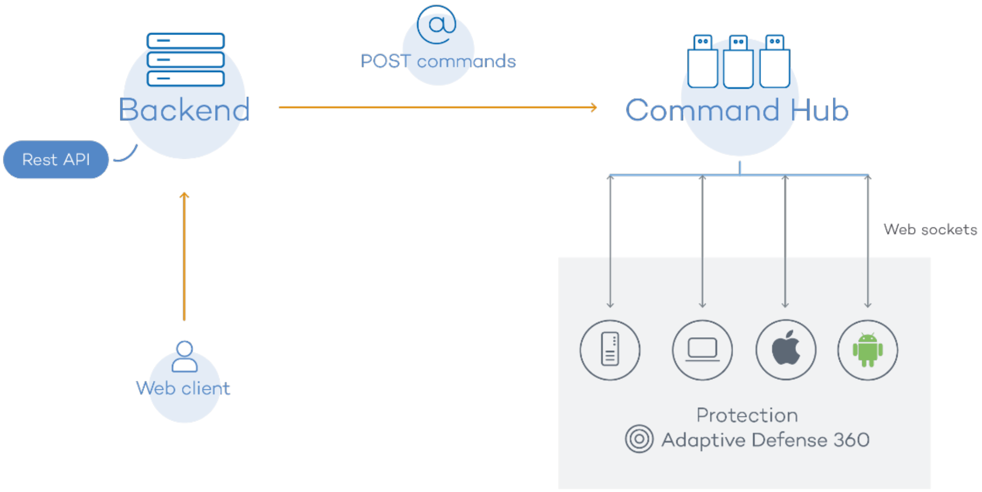


Figure 3: flowchart of the commands entered via the management console

2.4. Panda Adaptive Defense 360 architecture: key components

Panda Adaptive Defense 360 is an advanced security service that analyzes the behavior of all processes run in the customer's IT infrastructure. This analysis is performed using machine learning techniques in Big Data environments hosted in the cloud.

Figure 4 shows the general structure of **Panda Adaptive Defense 360** and its components:

Panda Adaptive Defense 360 is made up of the following components:

- **Big Data analytics infrastructure**: made up of non-relational databases, services that correlate the events monitored in real time, and a classification cluster for the monitored processes.
- **100% Attestation service**: classifies all processes run accurately and without creating false positives or false negatives.
- **Threat Hunting service**: uses a horizontal correlation approach to analyze the telemetry gathered from the execution of processes on customers' systems in order to detect advanced threats.
- **Panda SIEMFeeder** (optional): integrates **Panda Adaptive Defense 360** with third-party SIEM tools.
- **Panda Data Control service** (optional): a service for finding and monitoring the personal information stored in PII files.
- **Advanced Reporting Tool service**(optional)**:** reporting service for generating advanced security intelligence.

- **Panda Patch Management service**(optional): a service for patching Windows operating systems and third-party applications.
- **Web console**: management console server.
- Corporate **SIEM server** (optional)
- Computers protected with the installed software (**Panda Adaptive Defense 360**).
- Computer of the network administrator that accesses the Web console.

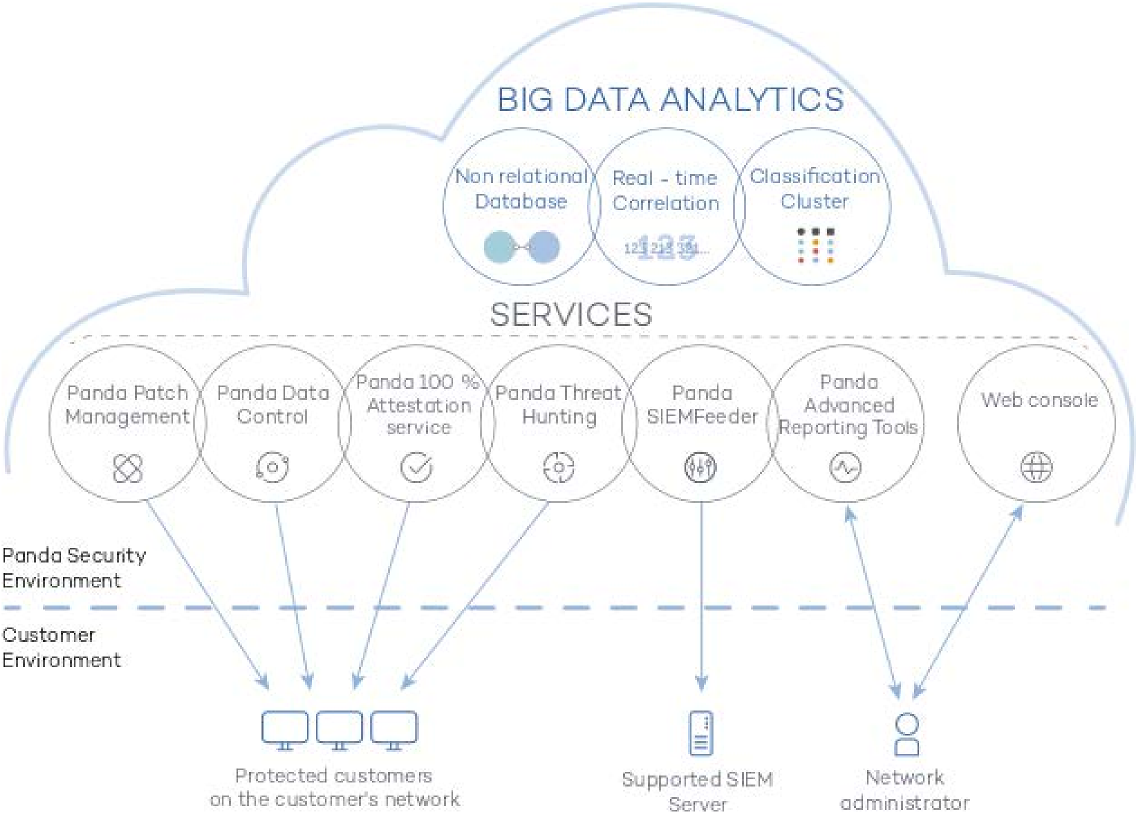


*Figure 4: **Panda Adaptive Defense 360** general structure*

Below we describe the roles of each of these components.

2.4.1 Big Data analytics infrastructure

The cloud server cluster receives the actions taken by the user's programs and monitored by the protection module installed on the customer’s computers. Using artificial intelligence techniques, the **Panda Adaptive Defense 360** server farm analyzes the behavior of those programs and classifies each running process. This classification is returned to the protection module installed on each computer, and is taken as the basis to run the actions required to keep the computer protected.

The **Panda Adaptive Defense 360** cluster is made up of a server farm hosted in the cloud and constituting a Big Data exploitation environment. It is in this environment where we continuously apply a mixture of technologies based on Machine Learning algorithms. These algorithms classify all running programs by examining their static attributes, execution context information and the actions performed by the monitored processes run on users' computers.

The advantages provided by this cloud-based model in comparison to the methodology used by traditional antiviruses, which send samples to the antivirus vendor for manual analysis, are multiple:

- Every process run on the computers protected by **Panda Adaptive Defense 360** is monitored and analyzed. This eliminates the uncertainty that characterizes traditional antivirus solutions, which can recognize malware items but cannot identify any other application.
- The delay in classifying processes seen for the first time (the malware window of opportunity) is minimal, as **Panda Adaptive Defense 360** sends the actions triggered by each process in real time to our servers. Our cloud servers are constantly working on the actions collected by our sensors, significantly reducing any delay in issuing a classification and the time that computers are exposed to threats.
- The continuous monitoring of every process allows **Panda Adaptive Defense 360** to classify as malware items which initially behaved as goodware. This is typical of targeted attacks and other advanced threats designed to operate under the radar.
- Cloud-based scanning frees customers from having to install and maintain a dedicated hardware and software infrastructure, or stay up to date with license payments and manage warranties, notably reducing the TCO.

2.4.2 Management console Web server

Panda Adaptive Defense 360 is managed entirely through the Web console accessible to administrators from https://www.pandacloudsecurity.com/PandaLogin/

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

Refer to Chapter 4 The management console, to check whether your Internet browser is compatible with the service.

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

2.4.3 Computers protected by Panda Adaptive Defense 360

Panda Adaptive Defense 360 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 Adaptive Defense 360** protection module.

The **Panda Adaptive Defense 360** protection module contains the technologies designed to protect customers' computers. **Panda Adaptive Defense 360** provides, in a single product, everything necessary to detect targeted and next-generation malware (APTs), as well as remediation tools to disinfect compromised computers and assess the impact of intrusion attempts.

> *Panda Adaptive Defense 360 can be installed without problems on computers with competitors' security products installed.*

2.5. Panda Adaptive Defense 360 services

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

2.5.1 100% Attestation service

This service is included in the product by default and is designed to allow the execution of only those programs certified by Panda Security. To do that, it uses a combination of local technologies on the user's computer and cloud-hosted technologies in a Big Data infrastructure. These technologies are capable of automatically classifying 99.08 percent of all running processes. The remaining percentage is manually classified by malware experts. This approach allows us to classify 100 percent of all binaries run on customers' computers without creating false positives or false negatives.

All executable files found on users' computers that are unknown to **Panda Adaptive Defense 360** are sent to Panda Security's Big Data analytics infrastructure for analysis.

> *Unknown files are sent to Panda Security only once for all customers using Panda Adaptive Defense 360, which reduces the impact on customers' networks to almost zero. Additionally, bandwidth management mechanisms are implemented, as well as per-computer and per-hour bandwidth limits.*

2.5.2 Panda Threat Hunting service

This service is included in the product by default and is designed to detect malwareless/fileless attacks as well as the lateral movements performed by advanced threats prior to taking harmful actions against corporate security.

Thanks to its continuous monitoring of the computers on the network, Panda Threat Hunting is capable of detecting attacks that don't use known malware and even the actions of malicious insiders.

2.5.3 Panda Advanced Reporting Tool service (optional)

Panda Adaptive Defense allows all the information collected from customers' computers to be automatically and seamlessly sent to **Panda Advanced Reporting Tool**, a service designed to store and exploit the knowledge generated on the customer's network.

All actions triggered by the processes run across the IT network are sent to **Panda Advanced Reporting Tool**, where they are correlated and analyzed in order to extract security intelligence. This will provide administrator with additional information on threats and the way users are using corporate computers. This information is delivered in the most flexible and visual way to make it easier to understand.

Panda Advanced Reporting Tool is directly accessible from the **Panda Adaptive Defense** Web console dashboard.

Refer to the Advanced Reporting Tool User Guide (accessible from the product's Web page) for more information about how to configure and make the most out of this service.

2.5.4 Panda SIEMFeeder service (optional)

Panda Adaptive Defense 360 integrates seamlessly with the third-party SIEM solutions installed by customers on their IT infrastructure. The activities performed by the applications run on their network are delivered to the SIEM server, ready for use and enriched with the knowledge provided by **Panda Adaptive Defense 360**.

The SIEM systems compatible with **Panda Adaptive Defense 360** are:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora

Refer to the SIEMFeeder User Guide for a detailed description of the information collected by Panda Adaptive Defense 360 and sent to the customer's SIEM system.

2.5.5 Panda Data Control service (optional)

This is a new security module integrated in the **Panda Adaptive Defense** platform, and designed to help organizations comply with the data protection regulations governing the storage and processing of personally identifiable information (PII).

Panda Data Control discovers, audits and monitors the entire lifecycle of PII files in real time: from data at rest to data in use (the operations taken on personal data) and data in motion (data exfiltration).

Refer to the Panda Data Control Administrator's Guide for more information about the service.

2.5.6 Panda Patch Management service (optional)

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

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

2.6. Panda Adaptive Defense 360 on Aether: user profile

Even though **Panda Adaptive Defense 360** is a managed service that offers security without intervention by the network administrator, it also provides clear and detailed information about the activity of the processes run by all users on the 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.

2.7. Panda Adaptive Defense 360 on Aether: supported devices and languages

Refer to Appendix 1: Panda Adaptive Defense 360 requirements, for a full description of the platforms supported by Panda Adaptive Defense 360 on Aether and its requirements.

Panda Adaptive Defense 360 supports the following operating systems:

- Windows Workstation
- Windows Server
- Linux
- macOS
- Android smartphones and tablets

Additionally, the management console supports the following Web browsers:

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

Finally, the following languages are supported in the management console:

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

2.8. Available resources and documentation

Below is a list of the available resources for **Panda Adaptive Defense 360 on Aether**.

Panda Adaptive Defense 360 Administration Guide

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADAPTIVEDEFENSE360oAP-guide-3.40.0-EN.pdf

Panda Advanced Reporting Tool Administration Guide

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-Guide-EN.pdf

Panda Data Control Administration Guide

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-

Guide-EN.pdf

Product Support Page

http://www.pandasecurity.com/uk/support/adaptive-defense-360-aether.htm

Product Page

http://www.pandasecurity.com//intelligence-platform/solutions.htm

3. The adaptive protection full cycle

The adaptive protection cycle
Complete protection of the IT network
Detection and monitoring
Remediation and response
Adaptation / Prevention

3.1. Introduction

This chapter provides an overview of the general strategy adopted by **Panda Adaptive Defense 360** to manage the security of a company's network.

Over 200,000 new viruses are created every day, and a great majority of those new malware specimens are designed to run on users' computers in the background for long periods of time, concealing their presence on compromised systems.

For this reason, the traditional approach of protecting systems using locally stored or cloud-based signature files has become gradually ineffective: the huge growth in the amount of malware in circulation has increased the window of opportunity for malware, that is, the time lapse between the appearance of a new virus and the release of the antidote by security companies.

Consequently, every security strategy must be based on minimizing malware dwell time, presently estimated at 259 days for the increasingly common targeted attacks, whose main objectives are industrial espionage and data theft.

In view of this dramatic change in the malware landscape, **Panda Adaptive Defense 360 on Aether** proposes a new security strategy based on an adaptive protection cycle: a set of protection, detection, monitoring, forensic analysis and remediation services integrated and centralized within a single Web management console.

This new approach aims to prevent or minimize security breaches, drastically reducing productivity losses and the risk of theft of confidential corporate information. Administrators are freed from the complex task of determining what is dangerous and why, dedicating their time and resources to managing and monitoring the security status of the network.

This new approach enables IT Departments to quickly adapt corporate IT security policies to the changing patterns of advanced malware.

3.2. The adaptive protection cycle

The aim of **Panda Adaptive Defense 360** is to enable IT Department to create a space where they can define and establish corporate security policies that respond rapidly and adequately to the new types of threats that are continuously emerging. This space is partly the product of the removal of responsibilities from the company’s technical team of deciding which files are safe and which are dangerous, and for what reason. With **Panda Adaptive Defense 360**, a company’s technical department will receive unambiguous classification of absolutely all programs run on its IT resources.

On the other hand, the IT Department will also receive a set of tools for viewing the security status, resolving problems related to advanced malware, and performing forensic analyses, which will enable the detailed study of the behavior of APTs and other threats.

With all this information and tools, administrators can completely close the corporate security cycle: monitoring the status of the network, resetting the system to the situation prior to any potential security breach, and being aware of its scope in order to implement appropriate contingency measures. This entire cycle is also in a continuous process of refinement and improvement, resulting in a secure, flexible and productive environment for all the company's users.

The adaptive protection cycle implemented by companies with the help of **Panda Adaptive Defense 360** is illustrated in the Figure 5.

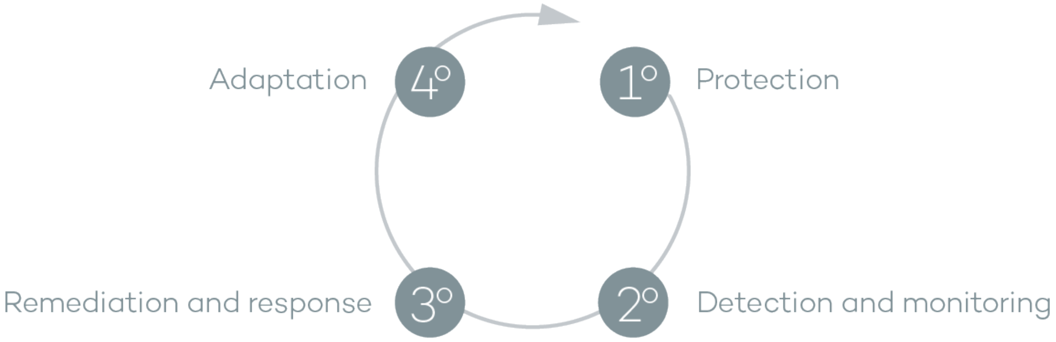


Figure 5: adaptive protection cycle

3.3. Phase 1: Complete protection of the IT network

The first phase in the adaptive protection cycle involves the necessary tools to effectively protect and defend the IT network against attacks and infection attempts.

3.3.1 Permanent antivirus protection and Collective Intelligence

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

In the current context of ever-increasing amounts of malware, cloud-hosted services have proved much more efficient than traditional signature files to successfully combat the enormous amount of threats in circulation. That's why **Panda Adaptive Defense 360**'s antivirus protection is primarily based on Collective Intelligence, a cloud-based knowledge platform that exponentially increases detection capabilities.

Collective Intelligence has servers that automatically classify and process all the information provided by the user community about the detections made on their systems. **Panda Adaptive Defense 360** queries Collective Intelligence only when required, ensuring maximum detection power without negatively affecting resource consumption.

Whenever a new malware specimen is detected on a computer in the user community, **Panda Adaptive Defense 360** sends the relevant information to our **Collective Intelligence** servers in the cloud, automatically and anonymously. This information is processed by our servers, delivering the solution to all users in the community in real time.

In short, **Panda Adaptive Defense 360** leverages Collective Intelligence to increase its detection capabilities without negatively impacting system performance. Now, all knowledge is in the cloud, and thanks to **Panda Adaptive Defense 360**, all users can benefit from it.

Refer to chapters 10 and 11 for more information about Panda Adaptive Defense 360's antivirus service for the different supported platforms

3.3.2 Protection against advanced stealth techniques and macro viruses

In addition to the traditional detection strategy based on comparing the payload of scanned files to its signature files, **Panda Adaptive Defense 360** uses several detection engines that scan the behavior of processes locally.

This allows the solution to detect strange behavior in the main scripting engines (Visual Basic Script, JavaScript and Powershell) incorporated into all current Windows systems and used as an extension of the command line. It also allows **Panda Adaptive Defense 360** to detect malicious macros embedded in Office files (Word, Excel, PowerPoint, etc.).

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

3.3.3 Email and Web protection

Panda Adaptive Defense 360 goes beyond the traditional email and Web security approach based on plug-ins that add protection features to certain email clients and Web browsers. Instead, it works by intercepting at low level every communication that uses common protocols such as HTTP, HTTPS or POP3. This way, the solution is able to provide permanent, homogeneous protection for all email and Web applications past, present and future, without the need for specific configurations or updates every time an email or Web service provider releases a new product incompatible with the previous plug-ins.

3.3.4 Firewall and intrusion detection systems (IDS)

Panda Adaptive Defense 360 provides three basic tools to filter the network traffic that protected computers send and receive:

- **Protection using system rules**: these rules describe communication characteristics (ports, IP addresses, protocols etc.) in order to allow or deny the data flows that match the configured rules.

- **Program protection**: rules that allow or prevent the programs installed on users' computers from communicating.
- **Intrusion detection system**: detects and rejects malformed traffic patterns that may affect the security or performance of protected computers.

3.3.5 Device Control

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

Panda Adaptive Defense 360 allows administrators to restrict the use of those devices on protected computers, blocking access to them or allowing complete or partial use only (read-only access).

3.3.6 Spam, virus and content filtering for Exchange servers

Panda Adaptive Defense 360 scans Exchange servers for viruses, hacking tools and suspicious/potentially unwanted programs directed to users' mailboxes.

Apart from that, eliminating junk mail (spam) is a time-consuming task. And not only that, spam is also a frequent source of scams. To tackle this, **Panda Adaptive Defense 360** provides anti-spam protection for Exchange servers. This feature helps companies improve user productivity and increase the security of network computers.

Panda Adaptive Defense 360 protects Exchange email servers by using two different technologies:

- **Mailbox protection**

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

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

Additionally, the mailbox protection allows administrators to scan Exchange server users' folders in the background, making the most of server idle times. This protection uses smart scans to avoid re-scanning already scanned items, as opposed to the typical scenario where both the mailboxes and the quarantine folder are scanned every time a new signature file is published.

- **Transport protection**

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

This protection does not allow manipulation of the items contained in the body of scanned messages. That is, the body of dangerous messages is treated as a single component, and every action taken by **Panda Adaptive Defense 360** affects the entire message: delete the message, quarantine it, let it through without taking any action, etc.

3.3.7 Web access control

Panda Adaptive Defense 360 divides websites into 64 categories, enabling network administrators to restrict access to them and to any manually entered URL. This protection helps organizations optimize network bandwidth usage and employee productivity, restricting access to non-business related Web resources.

Additionally, **Panda Adaptive Defense 360** allows administrators to set time restrictions to limit access to certain Web page categories and blacklisted sites during working hours, or authorize it during non-business hours or weekends.

3.4. Phase 2: Detection and monitoring

The second phase in the adaptive protection cycle assumes that the malware or targeted attack managed to bypass the barriers placed in the Protection Phase, and infected one or several computers on the network, going unnoticed by users.

In this phase, **Panda Adaptive Defense 360** implements a number of innovative technologies that allow the network administrator to pinpoint the problem.

3.4.1 Advanced permanent protection

Panda Adaptive Defense 360's advanced protection is a new, ground-breaking technology that continuously monitors every process run on the customer's Windows computers. **Panda Adaptive Defense 360** collects every action taken by the processes run on users' computers and sends them to a server, where they are analyzed applying automatic Machine Learning techniques in Big Data environments. The service returns a classification (goodware or malware) with 99.9991 accuracy (less than 1 error for every100,000 files analyzed), preventing false positives.

For the most complicated cases, Panda Security has a laboratory manned by malware specialists, whose aim is to classify all executable files within the shortest possible time from the time they are first seen on the customer's network.

Panda Adaptive Defense 360 implements three operational modes for unknown (not yet classified) processes and processes classified as malware:

- **Audit**

In Audit mode, **Panda Adaptive Defense 360** gives information about the threats it detects but doesn't block or disinfect the malware found. This mode is useful for testing the security solution or checking that installing the product doesn't have a negative effect on computer performance.

- **Hardening**

In those environments where there are constant changes to the software installed on computers, or where many unknown programs are run, for example proprietary software, it may not be viable to wait for **Panda Adaptive Defense 360** to learn about them in order to classify them.

Hardening mode aims to keep a balance between the infection risk for computers and user productivity. In this mode, blocking of unknown programs is limited to those initially considered dangerous. Four scenarios are defined:

- Files classified by **Panda Adaptive Defense 360** as goodware: they are allowed to run.
- Files classified by **Panda Adaptive Defense 360** as malware: they are sent to quarantine or disinfected.
- Unclassified files coming from external sources (Internet, email and USB devices): they are prevented from running until a classification is returned. Once a classification is returned, they are allowed to run (goodware) or quarantined (malware).

> ***This classification is almost immediate in most cases. That is, a program downloaded from the Internet and unknown to Panda Adaptive Defense 360 may be initially blocked, but then allowed to run within minutes if it turns out to be goodware.***

- Unclassified files that were installed on the user's computer before the implementation of **Panda Adaptive Defense 360**: they are allowed to run although their actions are monitored and sent to the server for analysis. Once classified, they will be allowed to run (goodware) or sent to quarantine (malware).

- **Lock**

In environments where security is the top priority, and in order to offer maximum security guarantees, **Panda Adaptive Defense 360** should be configured in Lock mode. In this mode, all software that is in the process of classification or is already classified as malware is prevented from running. Only legitimate software is allowed to run.

Just as in Hardening mode, programs classified as malicious are sent to quarantine, whereas unknown programs are prevented from running until they are classified as goodware or malware.

More than 99% of programs found on users' computers are already classified by Panda Adaptive Defense 360. Only a small minority of programs will be prevented from running. Refer to chapter 9 for more information about Panda Adaptive Defense 360's operational modes

3.4.2 Anti-exploit protection

Panda Adaptive Defense 360 implements technologies to protect network computers against threats capable of leveraging vulnerabilities in installed software. These vulnerabilities can be exploited to cause anomalous behaviors in applications, leading to security failures on customers' networks.

Exploit threats leverage both known and unknown (zero-day) vulnerabilities, triggering a chain of events (CKC, Cyber Kill Chain) that they must follow to compromise systems. **Panda Adaptive Defense 360** blocks this chain of events effectively and in real time, neutralizing exploit attacks and rendering them harmless.

In order to achieve these high levels of protection and immediate response, **Panda Adaptive Defense 360** implements new hooks in the operating system, using them to locally and continually monitor all actions taken by the processes run on users' computers.

This strategy allows **Panda Adaptive Defense 360** to detect the exploit techniques used by hackers, going beyond the traditional approach used by other security products and consisting of searching for patterns and statically detecting CVE-payload pairs through signature files.

In short, **Panda Adaptive Defense 360** leverages constantly evolving algorithms and the work of Panda Security's cyber-security experts to provide global anti-exploit protection against vulnerability exploit techniques such as Heap Spraying, ROP, DEP and ASLR bypassing techniques, etc.

3.4.3 Fileless/malwareless threat detection

Some advanced threats manage to evade signature-based detection strategies by not dropping files onto the infected computer's hard disk These threats, which are run in the target computer's RAM memory only, are extremely difficult to detect. Not only that, the impact of their actions is extremely hard to determine with standard forensic analysis procedures.

The advanced protection provided by **Panda Adaptive Defense 360** can neutralize these attacks by continuously monitoring all running processes and analyzing their behavior. All processes that perform a sequence of actions considered dangerous will be classified as malware, regardless of the number of files that are dropped onto the storage media of the targeted workstation or server. Also, since all actions taken by these processes are logged in Panda Security's cloud, it is possible to conduct complete forensic analyses.

3.4.4 Monitoring data files (Panda Data Control)

Panda Adaptive Defense 360 monitors every access to users' data files by the processes run on computers. This way, if a malicious item manages to infect the computer, it will be possible to accurately determine which files were modified and when. It will also be possible to determine if those files were sent out over the Internet, the destination IP addresses, and other information that may be useful for the subsequent forensic analysis or remediation actions. Below we list the types of data files that are monitored:

- Office documents.
- PDF documents.
- CAD documents.
- Desktop databases.
- Browser password stores.
- Mail client password stores.
- FTP client password stores.
- Active Directory password stores.
- Certificate stores and user certificates.
- Digital Wallet stores.
- Browser settings.
- Firewall settings.
- GPO settings.

3.4.5 Vulnerability patching (Panda Patch Management)

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

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

3.4.6 Network status visibility

Panda Adaptive Defense 360 provides a number of resources that allow administrators to assess the security status of their corporate network at a glance, using the activity panels displayed in the solution's dashboard.

Some of these tools, like the reports, are already known, however, the important thing is not only to be able to determine whether the customer's network has been attacked and the extent of the attack, but to have the necessary information to determine the likelihood of an infection.

The **Panda Adaptive Defense 360** dashboard provides key information for this purpose:

- Information on which processes found on the network are unknown to **Panda Adaptive Defense 360** and are being classified by Panda Security, along with a preliminary assessment of their danger level.
- Detailed activity information by means of lists of the actions performed by the unknown programs which finally turned out to be malware.
- Detections made for each infection vector.

This module provides administrators with global visibility into the processes run on the network: known malware trying to enter the network and neutralized by the Protection module, and unknown malware designed to go unnoticed by traditional detection technologies and which managed to bypass the detection systems in place.

Finally, administrators will have the option to enhance the security of their network by preventing all unknown software to run, or adjust the block level to allow certain unknown programs to run.

Refer to 16 Malware and network visibility for more information about how to view and monitor computers and processes

3.5. Phase 3: Remediation and response

In the event of a security breach, administrators must be able to work in two lines of action: quickly restore affected computers to their original state, and assess the impact of the infection, that is, find out whether there was a data leak, the extent of the attack, which computers were compromised, etc. The Remediation and Response phase provides tools for these two scenarios.

- **Response**

The forensic analysis tool provides administrators with visibility into all actions taken by malware on infected computers, as well as with essential information for assessing the risk level of threats: infection vector (how the malware entered the organization's network), propagation patterns, whether the malware accessed the infected computer's hard drive in order to extract confidential information, etc.

Panda Adaptive Defense 360 generates a safe environment for administrators to perform forensic analyses, isolating compromised computers from the rest of the network. Isolating a computer prevents it from communicating with other computers outside of the network, preventing data leaks. However, isolated computers will be allowed to communicate with Panda Security's cloud in order to allow administrators to remotely investigate incidents without having to physically access the affected computer.

Additionally, **Panda Advanced Reporting Tool** and **Panda Data Control** complement and help interpret the data gathered by **Panda Adaptive Defense 360**. They give administrators access to graphical information representing all processes run by users, not only those classified as malware. They also identify files with personally identifiable information (PII) and any process that accesses them and sends them outside the corporate network.

- **Remediation**

Panda Adaptive Defense 360 provides the traditional disinfection tools typical of antivirus solutions, along with a quarantine to store suspicious and deleted items.

Refer to chapter 19 Remediation tools for more information

3.6. Phase 4: Adaptation / Prevention

After the attack has been analyzed with the aforementioned remediation and response tools, and once the cause of the infection has been identified, the administrator will have to adjust the company's security policies to prevent any such situation from occurring again.

The Adaptation phase may result in a large number of initiatives depending on the results obtained through the forensic analysis: from employee training courses on appropriate Internet use, to reconfiguration of corporate routers or user permissions on personal computers.

Panda Adaptive Defense 360 can be used to strengthen endpoint security in a number of ways:

- **Changing the advanced protection settings**

If the company's users tend to always use the same software, but there are users who install programs from dubious sources, a possible solution to reduce the risk posed by those users is to enable the Lock mode provided by the advanced protection. This will minimize malware exposure on top risk computers, preventing installation of illegitimate programs.

- **Changing the antivirus protection settings**

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

- **Restricting access to certain websites by category**

Reconfiguring the categories of website content accessible to users will reduce the number of dubious sites, ad-ridden pages, and innocent-looking but dangerous download portals (ebooks, pirated software, etc.) that may infect users' computers.

- **Filtering out spam and phishing messages**

Email is an infection vector commonly used by phishing attacks. Adjusting the settings of the content filtering and anti-spam features will reduce the number of unsolicited messages received at users' mailboxes, reducing the attack surface.

- **Partially or completely preventing access to pen drives and other external devices**

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

- **Using the firewall and the intrusion detection system (IDS) to restrict communications from and to installed programs**

The 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 for malware to enter the network. If malware is detected that has infected the network via a chat or P2P application, configuring the firewall rules correctly can prevent those programs from communicating with the exterior world.

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

- **Changing the Panda Patch Management settings**

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

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

4. The management console

General characteristics of the console

General structure of the Web management console

4.1. Introduction

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

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

The Web management console lets administrators deploy the **Panda Adaptive Defense 360** software to all computers on the network, configure their security settings, monitor the protection status of the network, and benefit from remediation and forensic analysis tools to resolve problems. All these functions are available from a single console, facilitating integration of different tools and minimizing the complexity of using products from different vendors.

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

The Web console is hosted in the cloud so it is not necessary to install new infrastructure on customers' premises, configure VPNs or change router settings. Neither is it necessary to invest in hardware, operating system licenses or databases, nor to manage licenses and warranties to ensure the operativity of the service.

- **Service management from anywhere at anytime**

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

4.1.1 Web console requirements

The Web console can be accessed from the following link:

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

The following requirements are necessary to access the Web management console:

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

> ***Refer to Appendix 2: creating and managing a Panda Account for more information about how to create a Panda account for accessing the Web console.***

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

4.1.2 IDP federation

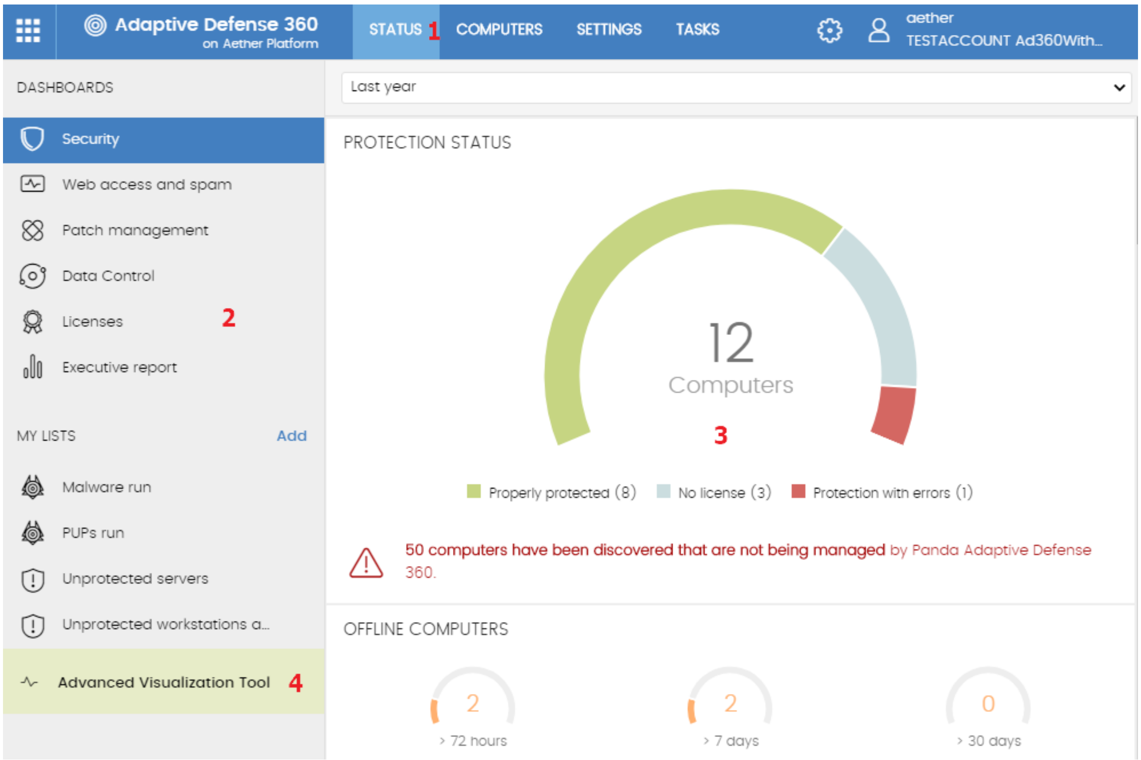
Panda Adaptive Defense 360 delegates credential management to an identity provider (IDP), a centralized application responsible for managing user identity.

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

4.2. General characteristics of the console

Panda Adaptive Defense 360's management console allows administrators to interact with the service, and provides the following benefits:

- **Responsive/adaptive design**: the Web console adapts to the size of the screen or Web browser the administrator is viewing it with, dynamically hiding and showing items as required.
- **Prevents page reloads**: the console uses Ajax technologies for easy navigation through lists, avoiding full page reloads.
- **Flexibility**: its interface adapts easily to the administrator's needs, allowing them to save settings for subsequent accesses.
- **Homogeneity**: the resources implemented in the management console follow clearly-defined usability patterns to lower the administrator's learning curve.
- **List export tools**: all lists can be exported to CSV format with extended fields for later consultation.



50 computers have been discovered that are not being managed by Panda Adaptive Defense 360.

Figure 6: overview of the ***Panda Adaptive Defense 360*** *management console*

4.3. General structure of the Web management console

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

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

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

4.3.1 Top menu (1)

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

- Panda Cloud button
- Status
- Computers
- Settings
- Tasks
- General settings
- User account

Panda Cloud button

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

Status menu

The **Status** menu at the top of the console displays the dashboard, which provides administrators with an overview of the security status of the network through widgets and a number of lists accessible through the side menu.

Refer to chapter 7 Managing computers and devices for more information.

Computers menu

The **Computers** menu provides the basic tools for network administrators to define the computer structure that best adapts to the security needs of their IT network.

Choosing the right device structure is essential in order to assign security settings quickly and easily.

Refer to chapter 8 Managing settings for more information.

Settings menu

Lets you define different types of settings:

- **Users**: lets you manage the users that will be able to access the management console, and the actions they can take.

Refer to chapter 22 Controlling and monitoring the management console for more information.

- **Per-computer settings**: lets you configure the **Panda Adaptive Defense 360** software updates and its administration password.
- **Proxy and language**: lets you configure the way computers connect to the Internet and the language of the **Panda Adaptive Defense 360** software.
- **Workstations and servers**: lets you create the configuration profiles to assign to the devices displayed in the **Computers** menu.

Refer to chapter 10 for more information.

- **Android devices**: lets you create the configuration profiles to assign to the Android smartphones and tablets displayed in the **Computers** menu.

Refer to chapter 11 Android security settings for more information.

- **Alerts**: lets you configure the alerts to be sent to the administrator's mailbox.

Refer to chapter 20 Alerts for more information.

Tasks menu

Lets you schedule security tasks to be run on the day and time specified by the administrator.

Refer to chapter 15 Tasks for more information.

General Settings menu

Displays a drop-down menu that allows the administrator to change the console language and access the following resources:

- **Panda Adaptive Defense 360 Administration Guide**
- **Panda Advanced Reporting Tool Administration Guide**
- **Panda Data Control Administration Guide**
- **Technical Support**: takes you to the Technical Support Web page for **Panda Adaptive Defense 360 on Aether.**
- **Suggestion box**: launches the mail client installed on the computer to send an email to Panda Security's technical support department.
- **License Agreement**: displays the product's EULA (End User License Agreement).
- **Language**: lets you change the language of the console.
- **About...:** displays the version of the different elements that make up **Panda Adaptive Defense 360.**
  - **Version**: product version.
  - **Protection version:** internal version of the protection module installed on computers.
  - **Agent version:** internal version of the communications module installed on computers.

User Account menu

Displays a drop-down menu with the following setting options:

- **Set up my profile**: lets you change the information of the product's main account.
- **Change account**: lists all the accounts that are accessible to the administrator and lets you select an account to work with.
- **Log out**: lets you log out of the management console and takes you back to the IDP screen.

4.3.2 Side menu (2)

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

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

4.3.3 Widgets (3)

The widgets are graphical representations of data. They allow administrators to view at a glance the available information regarding a certain aspect of network security. Hover the widgets to display tooltips with additional information. Click the widgets to show additional details.

Refer to chapter 16 Malware and network visibility for more information.

4.3.4 Access to Advanced Visualization Tool (4)

Advanced Visualization Tool gives access to the management console for the **Panda Data Control** and **Panda Advanced Reporting Tool** modules. Both modules share a console specifically designed to generate advanced charts and tables with relevant information about the activity of all processes run on your organization's workstations and servers.

4.3.5 Tab menu

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

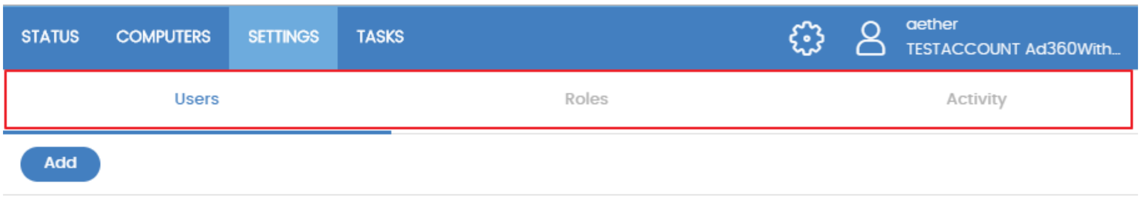


Figure 7: tab menu

4.3.6 Action bar

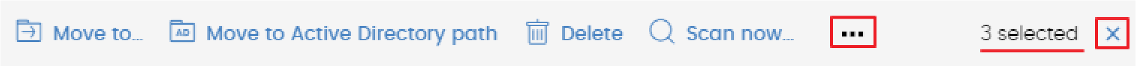


Figure 8: action bar

To facilitate navigating the console and performing some common operations on your managed workstations and servers, an action bar has been added at the top of every list that contains checkboxes to select computers.

The number of buttons on the action bar will vary depending on the size of the window. Click the ••• icon at the right end of the action bar to view those buttons that don't fit within the allocated space.

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

4.3.7 Filtering and search tools

The filtering and search tools allow administrators to filter and display information of special interest.

Some filtering tools are generic and apply to the entire screen, for example in the **Status** and **Computers** menus.

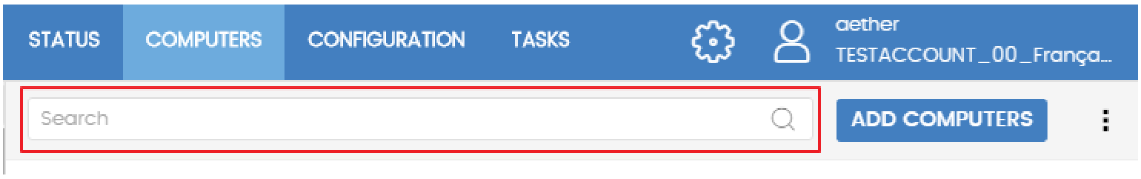
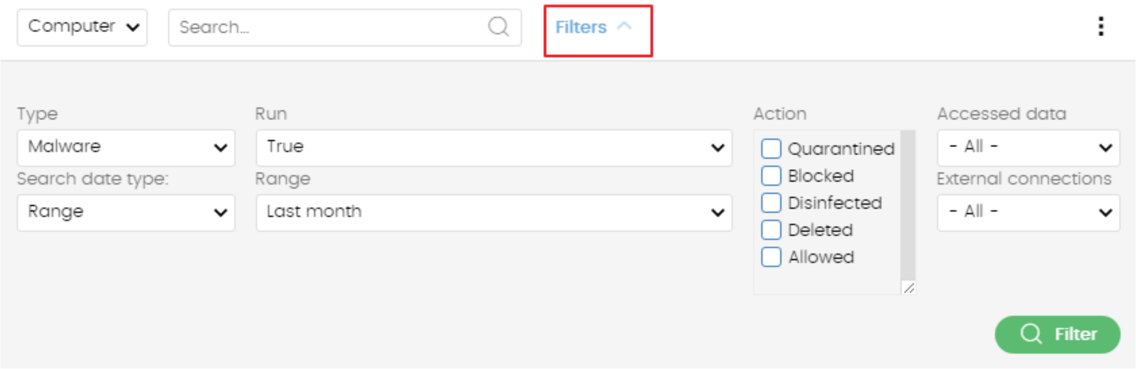


Figure 9: search tool

However, there are other more complete tools accessible through the **Filters** button, which allow you to refine your searches according to categories, ranges and other parameters based on the information displayed.



Type: Malware
Run: True
Search date type: Range
Range: Last month
Action: □ Quarantined □ Blocked □ Disinfected □ Deleted □ Allowed
Accessed data: - All -
External connections: - All -

Figure 10: filtering tool for data lists

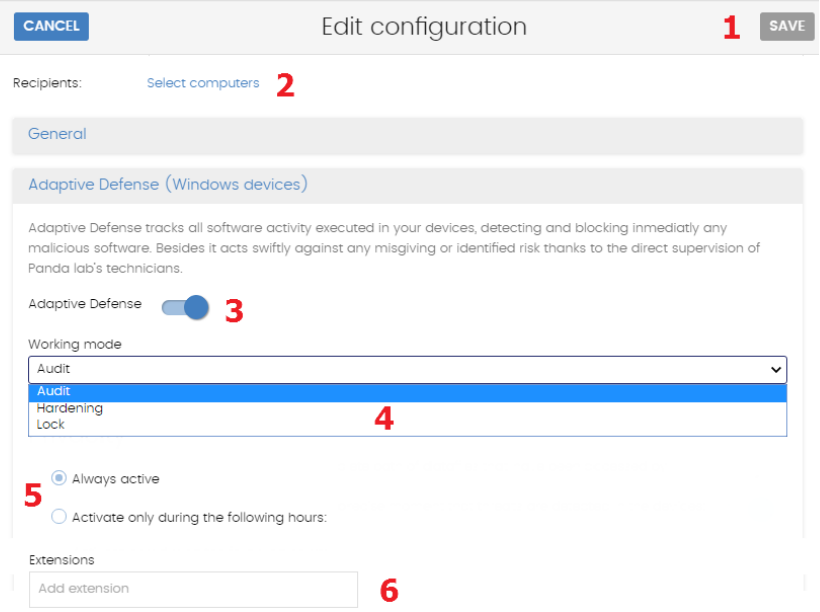
4.3.8 Back button

To help with navigation, there is a **Back** button that takes you to the last-viewed screen. The button label may change if the last-viewed screen belongs to an area other than the current area. In that case, the label will display the name of the area you have just abandoned instead of **Back**.

4.3.9 Settings elements (8)

The **Panda Adaptive Defense 360** Web console uses standard settings elements, such as:

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



Recipients: Select computers

General

Adaptive Defense (Windows devices)

Adaptive Defense tracks all software activity executed in your devices, detecting and blocking inmediatly any malicious software. Besides it acts swiftly against any misgiving or identified risk thanks to the direct supervision of Panda lab's technicians.

Adaptive Defense ●

Working mode: Audit

Audit
Hardening
Lock

● Always active
○ Activate only during the following hours:

Extensions: Add extension

Figure 11: controls for using the management console

4.3.10 Context menus

These are drop-down menus that appear when the user clicks the ⋮ icon. They display options relevant to the area they are in.

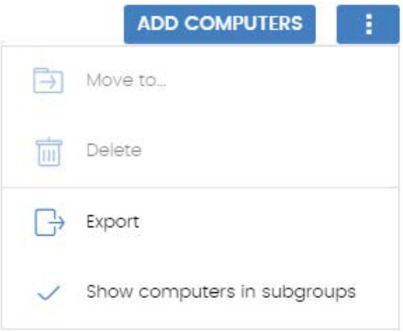


Figure 12: context menu

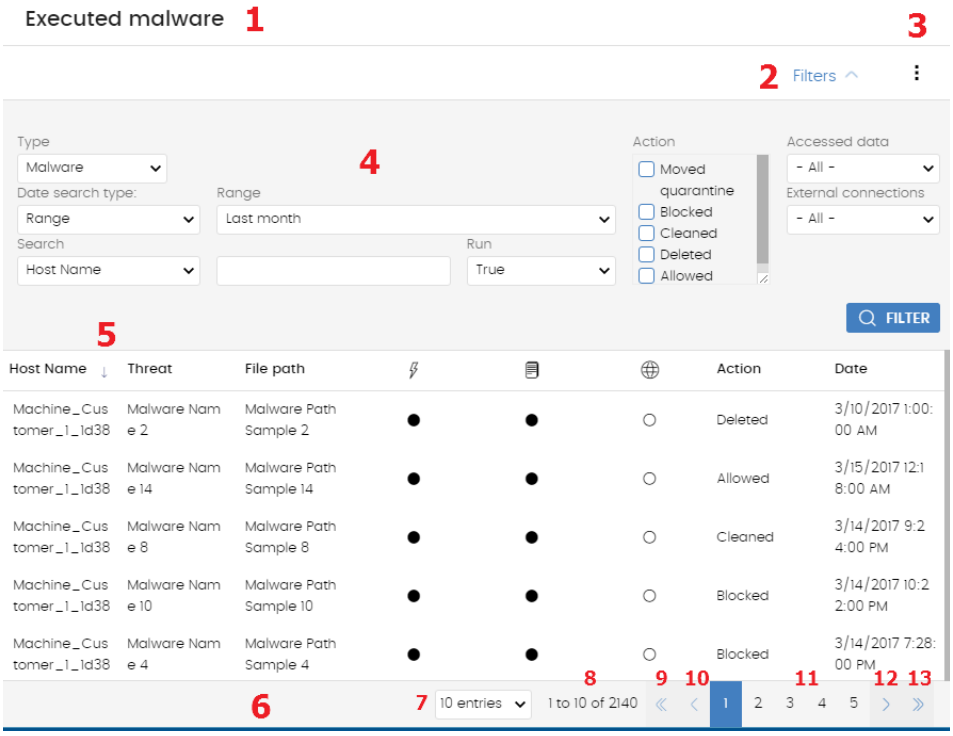
4.3.11 Lists

The lists display information in tables along with tools to help with navigation.

- **List name (1)**: lets you identify the information on the list.
- **Filtering and search tool link (2)**: click it to display a panel with search and filtering controls.
- **Context menu (3):** displays a drop-down menu with export options.
- **Filtering and search parameters (4):** let you refine the data displayed on the list.
- **Sort order (5)**: you can change the sort order of the list by clicking the column headers at the top of the list view. Click the same header a second time to switch between ascending

and descending order. This is indicated with arrows (↑ for ascending and ↓ for descending).

- **Pagination (6)**: at the bottom of the table there are pagination tools to help you navigate easier and faster.
  - Rows per page selector **(7)**
  - Number of pages/rows displayed out of the total number of pages/rows **(8)**
  - First page link **(9)**
  - Previous page link **(10)**
  - Links to the next 5 pages **(11)**
  - Next page link **(12)**
  - Last page link **(13)**



Executed malware

Type: Malware

Date search type: Range

Range: Last month

Search: Host Name

Run: True

Action: ☐ Moved quarantine ☐ Blocked ☐ Cleaned ☐ Deleted ☐ Allowed

Accessed data: - All -

External connections: - All -

Host Name ↓	Threat	File path				Action	Date
Machine_Customer_1_Id38	Malware Name 2	Malware Path Sample 2	●	●	○	Deleted	3/10/2017 1:00:00 AM
Machine_Customer_1_Id38	Malware Name 14	Malware Path Sample 14	●	●	○	Allowed	3/15/2017 12:18:00 AM
Machine_Customer_1_Id38	Malware Name 8	Malware Path Sample 8	●	●	○	Cleaned	3/14/2017 9:24:00 PM
Machine_Customer_1_Id38	Malware Name 10	Malware Path Sample 10	●	●	○	Blocked	3/14/2017 10:22:00 PM
Machine_Customer_1_Id38	Malware Name 4	Malware Path Sample 4	●	●	○	Blocked	3/14/2017 7:28:00 PM

10 entries | 1 to 10 of 2140 | 1 2 3 4 5

Figure 13: items in lists

5. Licenses

5.1. Introduction

To benefit from **Panda Adaptive Defense 360**'s advanced security services you need to purchase licenses of the product and assign them to the computers to protect, according to your organization's security needs**.**

This chapter explains how to manage your **Panda Adaptive Defense 360** licenses, as well as how to assign them to your computers, release them and check their status.

To start using the **Panda Adaptive Defense 360** service, you must purchase a number of licenses equal to or greater than the number of computers to protect. Each **Panda Adaptive Defense 360** license is assigned to a single computer (workstation, server or mobile device).

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

5.2. Definitions and key concepts for managing licenses

The following is a description of terms required to understand the graphs and data provided by **Panda Adaptive Defense 360** to show the status of computer licenses.

5.2.1 License contracts

Licenses are grouped into license contracts. A license contract is a group of licenses with certain similar characteristics, as follows:

- **Product type**: Panda Adaptive Defense 360, Panda Adaptive Defense 360 with Advanced Reporting Tool, Panda Adaptive Defense 360 with Panda Data Control, Panda Adaptive Defense 360 with Advanced Reporting Tool and Panda Data Control, Patch Management.
- **Contracted licenses**: number of licenses contracted in the license contract.
- **License type**: NFR, Trial, Commercial, Subscription.
- **Expiry**: license expiry date and the computers that will cease to be protected.

5.2.2 Computer status

Panda Adaptive Defense 360 makes a distinction between three different license statuses on network computers:

- **Computers with a license**: the computer has a valid license in use.
- **Computers without a license**: the computer doesn’t have a valid license in use, but is eligible to have one.
- **Excluded**: computers for which it has been decided not to assign a license. These computers won’t be protected by **Panda Adaptive Defense 360**, although they will be

displayed in the console and some management features will be valid for them. To exclude a computer, you have to release the 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).

5.2.3 License status and groups

There are two possible status types 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.

Licenses are separated into two groups according to their status:

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

5.2.4 Types of licenses

- **Commercial licenses**: these are the standard **Panda Adaptive Defense 360** 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 that has a trial license assigned has temporary access to all product features.
- **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 expiry date. This is a "pay-as-you-go" type service.

5.2.5 License management

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

Automatic assignment of licenses

Once you install **Panda Adaptive Defense 360** on a computer on the network, and provided there are unused **Panda Adaptive Defense 360** licenses, the system will assign a free license to the computer automatically.

Manual assignment of licenses

Follow the steps below to manually assign a **Panda Adaptive Defense 360** license to a network computer.

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

5.2.6 License release

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

Automatic release

When the **Panda Adaptive Defense 360** software is uninstalled from a network computer, the system automatically recovers a license and returns it to the group of licenses available for use.

Similarly, when a license contract expires, licenses will automatically be unassigned from computers in accordance with the expired license process explained later in this chapter.

Manual release

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

Follow the steps below to manually release a **Panda Adaptive Defense 360** license:

- Go to the **Computers** menu at the top of the console. Find the device whose license you want to release. You can use the folder tree, the filter tree or the search tool.
- Click the computer to access its details screen.
- Go to the **Details** tab. The **Licenses** section will display the **status 'Panda Adaptive Defense 360'**. Click the ⊗ icon to release the license and send it back to your pool of unused licenses.

5.2.7 Processes for assigning and releasing licenses

Case 1: excluded computers and those with assigned licenses

By default, each new computer on the **Aether** platform is assigned a **Panda Adaptive Defense 360** product license automatically, and as such acquires the status of a computer with an assigned license. This process continues until the number of available licenses reaches zero.

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

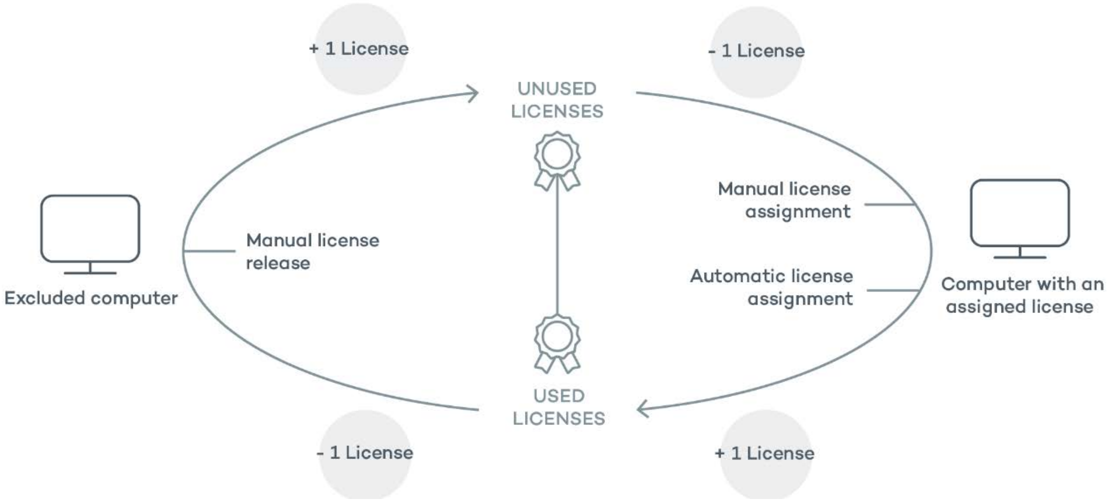


Figure 14: modification of license groups with excluded computers and those with licenses assigned

Case 2: computers without an assigned license

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

Similarly, when an assigned license expires, the computer will have the 'without license' status in accordance with the expired license process explained later in this chapter.

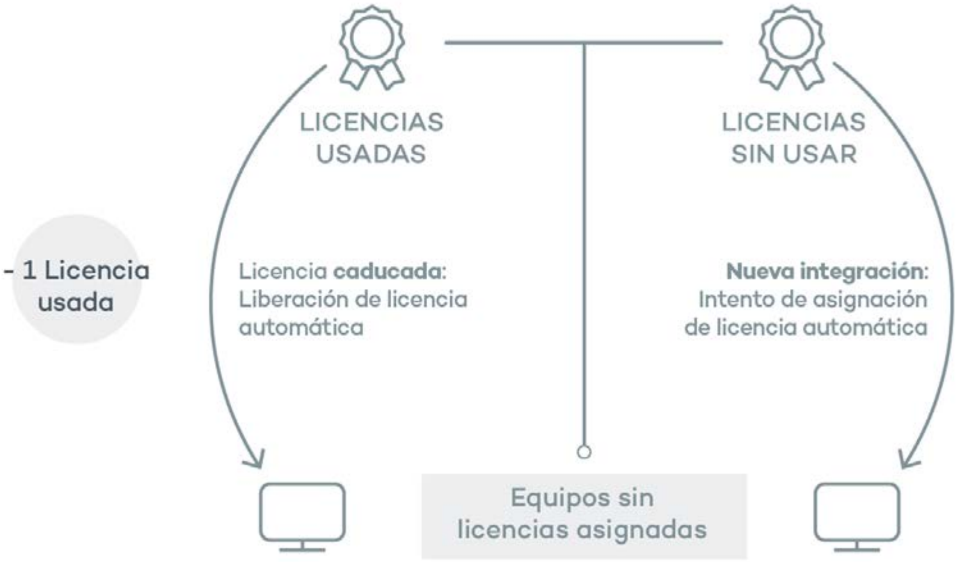

LICENCIAS USADAS
LICENCIAS SIN USAR
- 1 Licencia usada
Licencia caducada: Liberación de licencia automática
Nueva integración: Intento de asignación de licencia automática
Equipos sin licencias asignadas

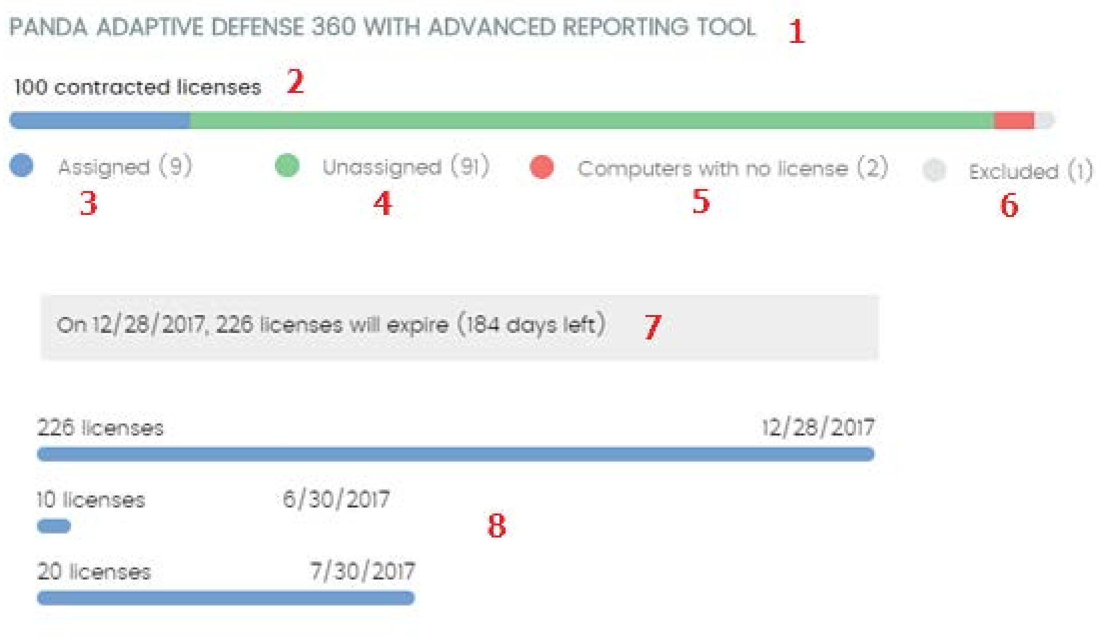
Figure 15: computers without an assigned license due to expiry of the license contract and because the group of unused licenses is empty.

5.3. Contracted licenses

To see details of contracted licenses click the **Status** menu and then **Licenses** in the side menu. You will see a window with two graphs: **contracted licenses** and **License expiry.**

5.3.1 Widget

The panel shows how the contracted product licenses are distributed.



PANDA ADAPTIVE DEFENSE 360 WITH ADVANCED REPORTING TOOL

100 contracted licenses

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

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

226 licenses	12/28/2017
10 licenses	6/30/2017
20 licenses	7/30/2017

Figure 16: license panel with three license contracts

- **Name of the contracted product (1)**
- **Total number of licenses contracted (2)**
- **Number of licenses assigned (3)**
- **Number of licenses not assigned (4)**
- **Number of computers without license (5)**
- **Number of excluded computers (6)**
- **License expiry (7)**
- **License contract expiry (8)**

Name of the contracted product (1)

This specifies the products and services contracted. Each different product is shown separately. If the same product has been contracted several times (several license contracts of one product) they will be shown together, indicating the different expiry dates of the licenses in a horizontal bar chart.

Total number of contracted licenses (2)

This represents the maximum number of computers that can be protected if all the contracted licenses are assigned.

Assigned (3)

This is the number of computers protected with an assigned license.

Unassigned (4)

This is the number of licenses contracted that haven't been assigned to a computer and are therefore not being used.

Computers without a license (5)

Computers that are not protected as there are insufficient licenses. Licenses will be assigned automatically once they are bought.

Excluded computers (6)

Computers without a license assigned and that are not eligible to have a license.

License expiry (7)

If there is only one license contract, all licenses expire at the same time, on the specified date.

License contract expiry (8)

If one product has been contracted several times over a period of time, a horizontal bar chart is displayed with the licenses associated to each contract/license contract and the separate expiry dates.

5.3.2 'Licenses' list

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

Field	Comments	Values
Computer	Computer name	Character string
Group	Folder in the Panda Adaptive Defense 360 group tree to which the computer belongs	Character string
License status		'Assigned Computers with no license Excluded computers
Last connection	Date that the computer status was last sent to the Panda Security cloud	Date

Table 1: 'Licenses' list fields

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the product belongs to	Character string
Computer type		Workstation Laptop Mobile device Server
Computer	Computer name	Character string
Last connection date	Date that the computer status was last sent to the Panda Security cloud	Date
Platform	Operating system installed on the computer.	Windows Linux macOS Android
Active Directory	Path in the company's Active Directory tree where the computer is found	Character string
License status		Assigned Unassigned Excluded
Agent version		Character string
Protection version		Character string
System boot date		Date
Installation date	Date that the Panda Adaptive Defense 360 software was successfully installed.	Date
Operating system	Operating system installed, internal version and patch status.	Character string
Exchange server	Version of the mail sever installed.	Character string
Virtual machine	Indicates whether the computer is physical or virtual	Boolean
Group	Folder within the Panda Adaptive Defense 360 group tree to which the computer belongs	Character string
IP address	Primary IP address of the computer.	Character string
Domain	Windows domain that the computer belongs to	Character string
Description		Character string

Table 2: fields in the 'Licenses' exported file

Filter tool

Field	Comments	Values
Find computer	Computer name	Character string
Computer type		Workstation Laptop Mobile device Server
Last connection	Date that the computer status was last sent to the Panda Security cloud	All More than 72 hours More than 7 days More than 30 days
Platform	Operating system installed.	All Windows Linux macOS Android
License status		Assigned No license Excluded

Table 3: filters available in the 'Licenses' list

Lists accessible from the panel

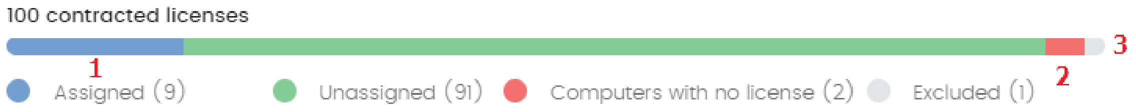


Figure 17: hotspots in the Contracted licenses panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1)** Filter by **License status** = Assigned
- **(2)** Filter by **License status** = Unassigned
- **(3)** Filter by **License status** = Excluded

5.4. Expired licenses

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

5.4.1 Expiry notifications

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

In addition, a message is displayed for each expired license contract, with 30 days warning of the number of licenses that will no longer be valid.

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

5.4.2 Withdrawal of expired licenses

Panda Adaptive Defense 360 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 group of available licenses, which are then distributed among the computers on the network.

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

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

This logic for withdrawing expired licenses affects all compatible devices with Panda Adaptive Defense 360 and with licenses assigned.

5.5. Adding Trial licenses to Commercial licenses

Where a customer has commercial licenses of **Endpoint Protection**, **Endpoint Protection Plus** or **Fusion** on the Aether platform and they get a trial license of **Panda Adaptive Defense 360**, there will be a series of changes, both to the management console and to the software installed on network computers:

- A new trial license contract is created for the trial period and with the same amount of licenses as previously available and the licenses contracted for the trial.
- Commercial license contracts appear temporarily disabled during the trial period, though the expiry and renewal cycle is unaffected.
- The corresponding product functionality is enabled for the trial with no need to update the computers.

- **Panda Adaptive Defense 360** will, by default, be enabled in Audit mode. If you do not want to enable **Panda Adaptive Defense 360** on all computers or you want to set a different protection mode, this can be configured accordingly.

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

5.6. Searching for computers based on the status of their licenses

Panda Adaptive Defense 360's filter tree lets you search for computers based on the status of their licenses.

Refer to chapter 7 Managing computers and devices for more information about how to create a Panda Adaptive Defense 360 filter.

The properties of the **License** category are as follows:

- **Property – License status**: you can create filters based on the following license status:
  - **Assigned**: lists those computers with a **Panda Adaptive Defense 360** license assigned.
  - **Not assigned**: lists those computers that don't have a **Panda Adaptive Defense 360** license assigned.
  - **Unassigned manually**: lists those computers whose **Panda Adaptive Defense 360** license was released by the network administrator.
  - **Unassigned automatically**: lists those computers whose **Panda Adaptive Defense 360** license was automatically released by the system.
- **Property - License name**: finds every computer with a **Panda Adaptive Defense 360** license assigned.
- **Property – Type**: lists those computers with a specific type of **Panda Adaptive Defense 360** license.
  - **Release**: lists computers with **commercial licenses** of **Panda Adaptive Defense 360.**
  - **Trial**: lists computers with **trial licenses** of **Panda Adaptive Defense 360.**

6. Installing the Panda Adaptive Defense 360 software

Protection deployment overview
Installation requirements
Manual installation
Discovery and remote installation
Installation with centralized tools
Software uninstall

6.1. Introduction

The installation process deploys **Panda Adaptive Defense 360** to all computers on the customer's network. All the software required to enable the advanced protection service and monitor the security status of the network is found in the installation package: there is no need to install any other program on the customer's network.

It is important to install the **Panda Adaptive Defense 360** software on every computer on the network to prevent security breaches that may be later exploited by attackers through malware designed to attack vulnerable systems.

Panda Adaptive Defense 360 provides several tools to help administrators install the protection. These tools are discussed later in this chapter.

6.2. Protection deployment overview

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

Identify the unprotected devices on the network

The administrator must find those computers on the network without protection installed or with a third-party security product that needs replacing or complementing with **Panda Adaptive Defense 360**.

Once identified, the administrator must check to see if they have purchased enough licenses.

Panda Adaptive Defense 360 allows you to install the solution's software even if you don't have enough licenses. These computers will be shown in the management console along with their characteristics (installed software, hardware, etc.), but won't be protected against next-gen malware.

Check if the minimum requirements for the target platform are met

The minimum requirements for each operating system are described later in this chapter.

Select the installation procedure

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

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

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

Computers with no protection installed won't need to be rebooted to install the protection services provided by **Panda Adaptive Defense 360**.

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

If you want to install **Panda Adaptive Defense 360** on a computer that already has an antivirus solution from another vendor, you can choose between installing the solution without uninstalling the current protection so that both products coexist on the computer, or uninstall the other solution and work exclusively with **Panda Adaptive Defense 360**.

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

The default behavior will vary depending on the **Panda Adaptive Defense 360** version to install.

- **Trial versions**

By default, you can install a trial version of **Panda Adaptive Defense 360** without removing any other pre-existing third-party solution. This allows organizations to evaluate **Panda Adaptive Defense 360** and see for themselves how it detects advanced threats that their traditional antivirus cannot detect.

- **Commercial versions**

By default, it is not possible to install a commercial version of **Panda Adaptive Defense 360** on a computer with a solution from another vendor. If **Panda Adaptive Defense 360** has the uninstaller to uninstall the other vendor's product, it will uninstall it and then install **Panda Adaptive Defense 360**. Otherwise, the installation process will stop.

> *Refer to Appendix 3: list of uninstallers for a list of the antivirus solutions that Panda Adaptive Defense 360 uninstalls automatically. If the solution that needs to be removed is not on the list, it will have to be removed manually.*

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

Refer to chapter 10 for more information about how to define a security configuration. Refer to chapter 8 Managing settings for more information about how to assign settings to computers

- **Panda Security antivirus products**

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

If the computer is already protected with AdminSecure (Panda Security for Business), the behavior will be the same as with a competitor antivirus.

Table 4 summarizes the necessary conditions for a computer restart.

Previous product	Panda Adaptive Defense 360 on Aether	Restart
None	Trial or commercial version	NO
Endpoint Protection Legacy, Endpoint Protection Plus Legacy, Panda Adaptive Defense 360 Legacy, Adaptive Defense Legacy, Panda Fusion Legacy	Commercial version	LIKELY (Only if a protection upgrade is required)
Third-party antivirus and AdminSecure	Trial version	NO (By default, both products will coexist)
Third-party antivirus and AdminSecure	Commercial version	LIKELY (A restart may be necessary to finish uninstalling the third-party product)
Citrix systems	Trial or commercial version	LIKELY (with older versions)

Table 4: probability of a restart when installing Panda Adaptive Defense 360 on Aether

Determine whether it will be necessary to install the protection during non-working hours

In addition to the restart considerations covered before, installing **Panda Adaptive Defense 360** causes a micro-interruption (less than 4 seconds) in the connections established by the programs running on the computer. Any applications that do not incorporate security mechanisms to detect connection interruptions will need a restart. If a restart is not possible and there is the possibility that some applications may not work properly after the micro-interruption, it is advisable to install the **Panda Adaptive Defense 360** software outside office hours.

Determine the computers' default settings

So that **Panda Adaptive Defense 360** can protect the computers on the network from the outset, it forces administrators to select both the target group that the computers to protect will integrate into, and the relevant proxy and language settings. This must be selected upon generating the installer. Refer to section **Downloading the Panda Adaptive Defense 360 software** for more information.

Once the software has been installed on a computer, **Panda Adaptive Defense 360** will apply to it the settings configured for the group that the computer is integrated into. If the proxy and language settings for the selected group are different from those specified when generating the installer, the installer settings will prevail.

6.3. Installation requirements

> *For a full description of the necessary requirements for each platform, refer to Appendix 1: Panda Adaptive Defense 360 requirements.*

6.3.1 Requirements for each supported platform

Windows platforms

- **Workstations**: Windows XP SP3 and later, Windows Vista, Windows 7, Windows 8 and later, and Windows 10.
- **Servers**: Windows 2003 SP2 and later, Windows 2008, Windows Small Business Server 2011 and later, Windows Server 2012 R2, Windows Server 2016, Windows Server Core 2008 and later.
- **Exchange servers**: from 2003 to 2016.
- **Free space for installation**: 650 MB.

MacOS platforms

- **Operating systems**: macOS 10.10 Yosemite and later.
- **Free space for installation**: 400 MB.
- **Ports:** port 3128 must be accessible for the Web anti-malware and URL filtering to work.

Linux platforms

- **64-bit operating systems**: Ubuntu 14.04 LTS and later, Fedora 23 and later.
- **Supported kernel**: up to version 4.10 (64-bit).
- **Free space for installation**: 100 MB.

- **Ports:** ports 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware and URL filtering to work

> *Refer to our support website for more information about the last Linux kernel version supported by Panda Adaptive Defense 360. Any later version won't be supported.*

Android platforms

- **Operating systems**: Android 4.0 and later.
- **Free space for installation**: 10 MB (depending on the model, it is possible that the required space be larger).

6.3.2 Network requirements

Panda Adaptive Defense 360 accesses multiple Internet-hosted resources. In general, it requires access to ports 80 and 443. For a complete list of all the URLs that computers with the **Panda Adaptive Defense 360** software installed need to access, refer to Appendix 1: Panda Adaptive Defense 360 requirements.

6.4. Manually downloading and installing the Panda Adaptive Defense 360 software

6.4.1 Downloading the installation package from the Web console

> *Refer to chapter 7 for more information about the different types of groups. Refer to chapter 8 for information about how to assign settings to computers and tree branches, and refer to chapter 9 to learn about how to create new proxy and language settings.*

This consists of downloading the installation package directly from the management console. To do this, follow the steps below:

- Go to the **Computers** menu, click **Add computers**, and select the platform to protect: Windows, Linux, Android or macOS (Figure 18).
- Select the group that the computer will integrate into (Figure 19**Error! Reference source not found.**):
  - To integrate the computer into a native group, click **Add computers to this group (1)** and select a destination in the folder tree displayed.
  - To integrate the computer into an Active Directory group, click **Add computers to their Active Directory** path **(2)**.
- Next, you must select the proxy and language settings **(3)** to apply to the computer. If the computer is to be integrated into a native group, it will automatically inherit the settings of

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

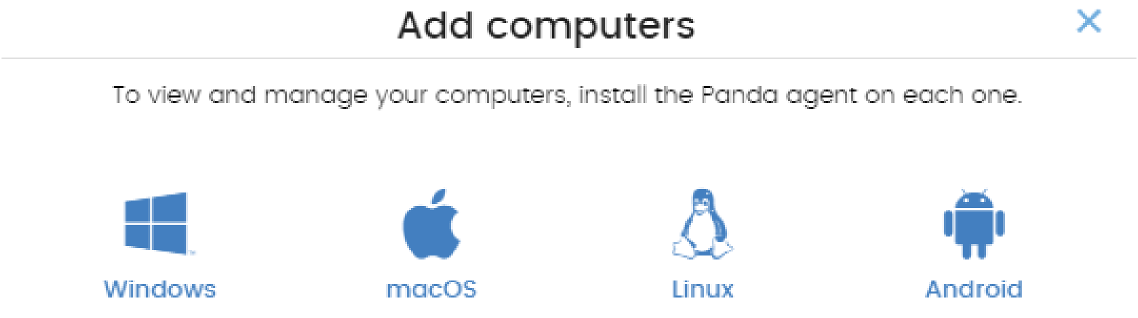

Add computers
To view and manage your computers, install the Panda agent on each one.
Windows
macOS
Linux
Android

Figure 18: platform selection window

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

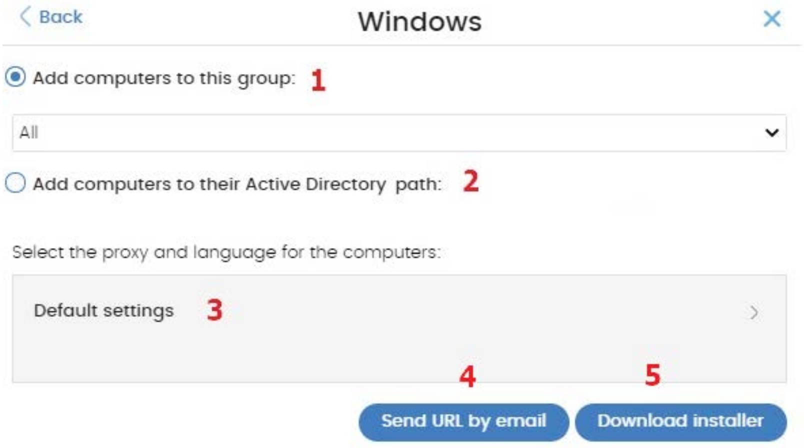

Back
Windows
Add computers to this group: 1
All
Add computers to their Active Directory path: 2
Select the proxy and language for the computers:
Default settings 3
4
5
Send URL by email
Download installer

Figure 19: configuring the download package

6.4.2 Generating a download URL

This option allows you to generate a download URL and send it to the targeted users to launch the installation manually from each computer.

The method used to send users the download URL is via email. To do this, click the **Send URL by email (3)** button.

Just as when downloading the installer from the Web console, you'll have to select the group in the group tree that the computer to protect will integrate into, as well as its proxy and language settings. These settings will take precedence over the group settings.

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

6.4.3 Manually installing the Panda Adaptive Defense 360 software

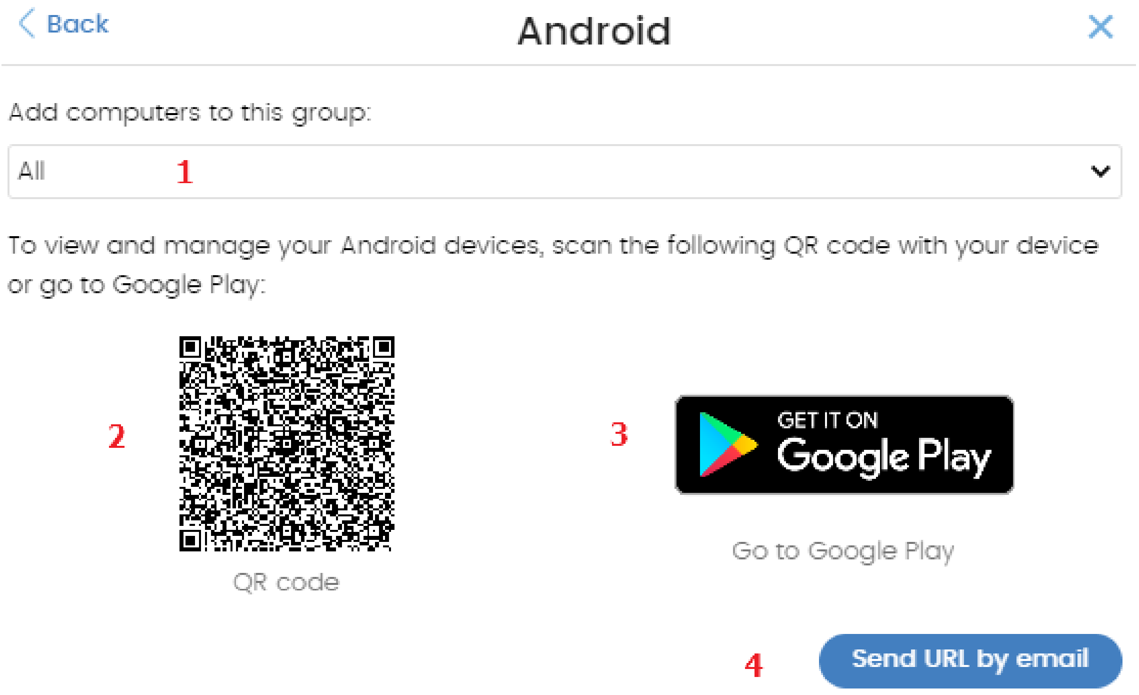
Administrator permission is required to install the Panda Adaptive Defense 360 software on users' computers

Installing Panda Adaptive Defense 360 on Windows, Linux and macOS platforms

Run the downloaded installer and follow the installation wizard. The product will then verify that it has the latest version of the signature file and the protection engine. If it does not, it will update automatically.

Installing Panda Adaptive Defense 360 on Android platforms

Click **Add computer** in the **Computers** menu and select the Android icon to display the information below:



Add computers to this group:

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

Figure 20: platform selection screen

Add computers to this group (1): this lets you specify the group within the folder tree to which the device will be added once the **Panda Adaptive Defense 360** software is installed.

- **QR code (2):** the QR code that contains the link to download the software from Google Play.

- **Go to Google Play (3)**: a direct link to download the **Panda Adaptive Defense 360** software from Google Play.
- **Send URL by email (4):** an email message with the download link ready to send to the user of the device that will be protected by **Panda Adaptive Defense 360.**

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

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

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

  - **Via email**: click the **Send URL by email** link to generate an email with the link for the user. The user will have to click the link that points to the app download in Google Play.
  - **Via the management console**: if you have accessed the management console from the device, click the **Go to Google Play** link and download the app.
- Once the app is installed, the user will be prompted to accept the granting of administrator permissions for the app. Depending on the version of Android (6.0 and later), these permissions will be presented progressively as required or, on the contrary, a single window will be displayed the first time the app is run, requesting all the necessary permissions just once.

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

6.5. Automatic computer discovery and remote installation

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

> *Remote installation is only compatible with Windows platforms.*

6.5.1 Requirements for installing Panda Adaptive Defense 360

For you to be able to install Panda Adaptive Defense 360 remotely, the target computers must meet the following requirements:

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

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

6.5.2 Computer discovery

Computers are discovered by means of another computer with the role of '*Discovery computer'*. All computers that meet the aforementioned requirements are susceptible to appear on the list of discovered computers, regardless of whether their operating system or device type supports the installation of Panda Adaptive Defense 360.

Requirements for finding unprotected computers on your network

The list of discovered computers displays all workstations and servers that meet the following requirements:

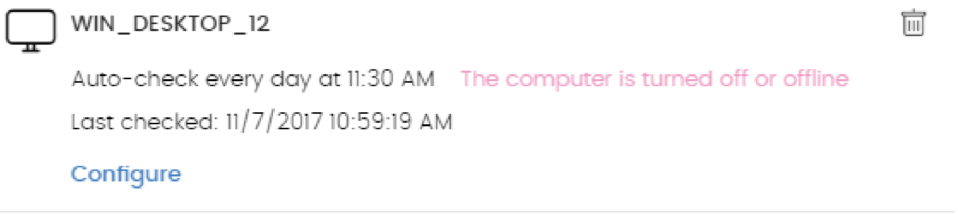
- Have not been hidden by the administrator
- Are not currently managed by **Panda Adaptive Defense 360 on Aether Platform**
- Are located on the same subnet segment as the discovery computer

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

- Make sure the discovery computer has **Panda Adaptive Defense 360** installed.
- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Discovery** tab.
- Click the **Add discovery computer** button, and select the computer(s) that you want to perform discovery tasks across the network.

Characteristics of a discovery computer

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



WIN_DESKTOP_12

Auto-check every day at 11:30 AM The computer is turned off or offline

Last checked: 11/7/2017 10:59:19 AM

Configure

Figure 21: information displayed for each discovery computer

Computer name

- **Discovery task settings:** settings of the automatic discovery task scheduled to find unmanaged computers on the network, if there is one.
- **Last checked**: time and date when the last discovery task was launched.
- **The computer is turned off or offline: Panda Adaptive Defense 360** cannot connect to the discovery computer.
- **Configure**: lets you define the task scope and type (automatic or manual). If the task is automatic, it will be performed once a day.

6.5.3 Discovery scope

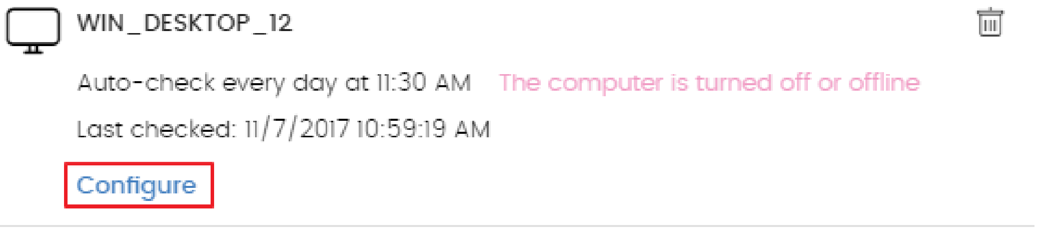
Follow the steps below to limit the scope of a discovery task:

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

6.5.4 Scheduling computer discovery tasks

Scheduling a task

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



WIN_DESKTOP_12

Auto-check every day at 11:30 AM The computer is turned off or offline

Last checked: 11/7/2017 10:59:19 AM

Configure

Figure 22: access to the discovery task settings window

- **Automatic execution of discovery tasks**

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Discovery** tab. Select a discovery computer and click **Configure**.
- From the **Run automatically** drop-down menu, select **Every day**.
- Select the start time of the scheduled task.
- Select whether to take the discovery computer's local time or the **Panda Adaptive Defense 360** server time as reference.
- Click **OK**. The discovery computer will show a summary of the scheduled task in its description.

- **Manual execution of discovery tasks**

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

6.5.5 List of discovered computers

Displays the unmanaged devices found by **Panda Adaptive Defense 360**.

There are two ways to access this list:

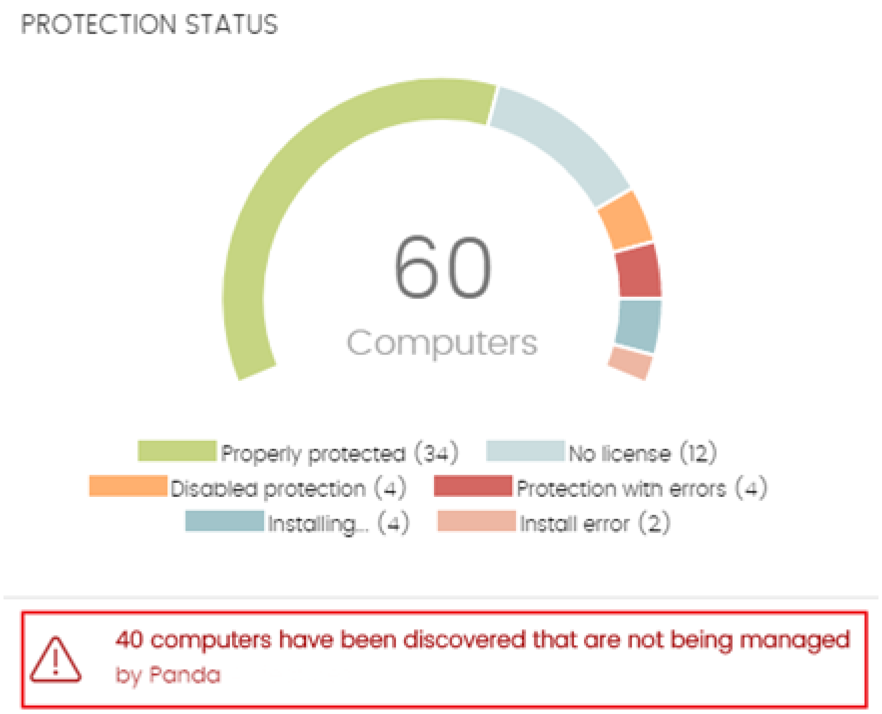
- From the **Protection status** widget
- From **My lists**

- **Protection status widget**

Go to the **Status** menu at the top of the console. You'll see the **Protection status** widget on the **Panda Adaptive Defense 360** dashboard. At the bottom of the widget you'll see the following text: **xX computers have been discovered that are not being managed by Panda Adaptive Defense 360**.

- **My lists**

Go to **My lists** on the left-hand side menu and click the **Add** link. From the drop-down menu, select the list **Unmanaged computers discovered**.



40 computers have been discovered that are not being managed by Panda

*Figure 23: access to the list of discovered computers from the **Protection status** widget*

Description of the list of discovered computers

Field	Comments	Values
Computer	Name of the discovered computer	Character string
Status	Indicates the computer status with regard to the installation process	— **Discovered**: the computer is eligible for installation, but the installation process has not started yet ☁ **Installing**: the installation process is in progress **Installation error:** displays a message specifying the type of error. See later for a description of all possible errors
IP address	The computer's primary IP address	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card	Character string
Discovered by	Name of the discovery computer	Character string
Last seen	Date when the computer was last discovered	Date

Table 5: fields in the list of discovered computers

Next is a description of the possible error messages:

- **Wrong credentials.** The entered credentials don't have sufficient privileges to perform the installation.
- **Discovery computer not available**:
  - The discovery computer that found the unmanaged workstation or server has been deleted and the installation cannot be run.
- **Unable to connect to the computer**:
  - The computer is turned off.
  - The firewall is preventing the connection.
  - The computer's operating system is not supported.
- **Unable to download the agent installer**:
  - The downloaded package is corrupt.
  - There is no installation package for the operating system of the workstation/server.
  - There is not enough free space on the computer to download the agent package.
  - The agent package download was very slow and has been canceled.
- **Unable to copy the agent**.
  - There is not enough free space on the computer to copy the agent package.
- **Unable to install the agent**.
  - There is not enough free space on the computer to install the agent.
  - An agent is already installed on the computer. If both agents are the same version, the installation will be launched in repair mode.
- **Unable to register the agent**.
  - The computer must be restarted before the agent can be uninstalled.
  - **Panda Endpoint Protection** is installed on the remote computer.

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer	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's network interface card	Character string
Domain	Windows domain the computer belongs to	Character string
First seen	Date when the computer was first discovered	Character string
First seen by	Name of the discovery computer that first saw the workstation/server	Character string

Field	Comments	Values
Last seen	Date when the computer was last discovered	Date
Last seen by	Name of the discovery computer that last saw the workstation/server	Character string

Table 6: fields in the 'List of discovered computers' exported file

Filter tool

Field	Comments	Values
Search	Search by computer name, IP address, NIC manufacturer or discovery computer	Character string
Status	Panda Adaptive Defense 360 installation status	**Discovered**: the computer is eligible for installation, but the installation process has not started yet **Installing**: the installation process is in progress **Installation error**
Last seen	Date when the computer was last discovered	Last 24 hours Last 7 days Last month

Table 7: filters available in the list of discovered computers

Hidden computers

To avoid generating too long lists of discovered computers that may contain computers not eligible for **Panda Adaptive Defense 360** installation, it is possible to hide computers selectively by following the steps below:

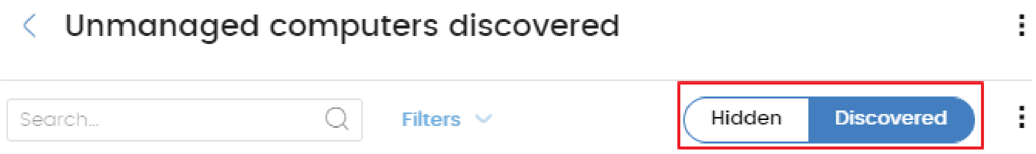


Figure 24: discovered/Hidden computer list selector

- From the list of discovered computers, select **Discovered (1)** and click **Filter**.
- Select the checkboxes that correspond to the computers that you want to hide **(2).**
- To hide multiple computers simultaneously, click the general context menu and select **Hide and do not discover again (3).**
- To hide a single computer, click the computer's context menu and select **Hide and do not discover again (4).**

Deleted computers

Panda Adaptive Defense 360 doesn't remove, from the list of discovered computers, those discovered computers that are no longer accessible because they have been withdrawn from the network due to inspection, malfunction, theft or for any other reason.

To manually remove those computers that are no longer accessible follow the steps below:

- From the list of discovered computers, select **Discovered** or **Hidden** depending on the status of the relevant computers **(1).**
- Select the checkboxes that correspond to the computers that you want to delete **(2).**
- To delete multiple computers simultaneously, click the general context menu and select **Delete (3).**
- To delete a single computer, click the computer's context menu and select **Delete (4).**

> ***Any computer that is deleted by you from the console without uninstalling the Panda Adaptive Defense 360 software and without being physically withdrawn from the network will appear again in the next discovery task. Only delete those computers that you are sure will never be accessible again.***

6.5.6 Details of a discovered computer

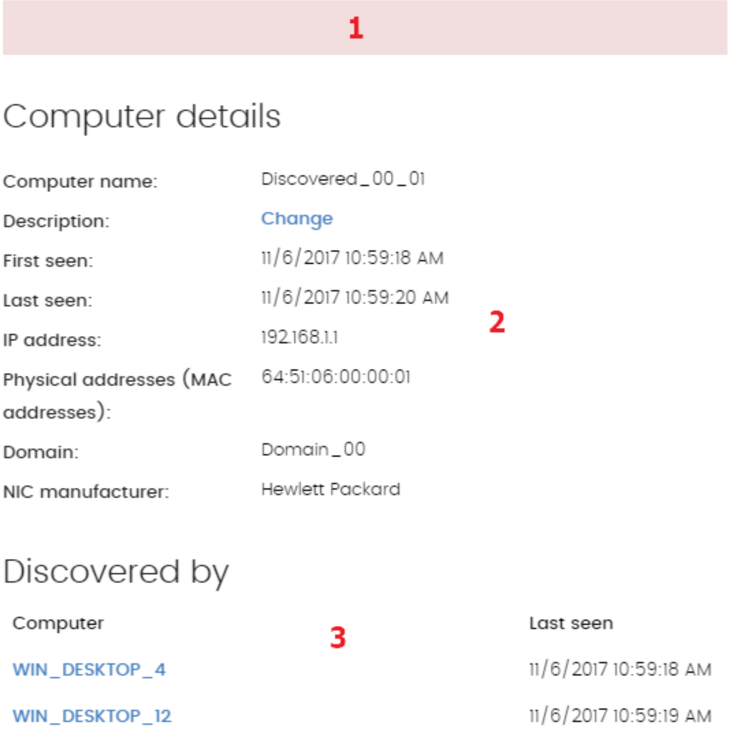
Click a discovered computer to view its details window. This window is divided into 3 sections:

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

Computer alerts

- **Error installing the Panda agent**: this message specifies the reason why the agent installation failed.
  - Wrong credentials. Launch the installation again using credentials with sufficient privileges to perform the installation.
  - Discovery computer not available.
  - Unable to connect to the computer. Make sure the computer is turned on and meets the remote installation requirements.
  - Unable to download the agent installer. Make sure the computer is turned on and meets the remote installation requirements.
  - Unable to copy the agent installer. Make sure the computer is turned on and meets the remote installation requirements.
  - Unable to install the agent. Make sure the computer is turned on and meets the remote installation requirements.
  - Unable to register the agent. Make sure the computer is turned on and meets the remote installation requirements.

- **Error installing the Panda Adaptive Defense 360 protection**: this message indicates the reason for the protection installation error.
  - Insufficient disk space to perform the installation.
  - Windows Installer is not operational.
  - Removal of the third-party protection installed was canceled by the user.
  - Another installation is in progress.
  - Error automatically uninstalling the third-party protection installed.
  - There is no uninstaller available to remove the third-party protection installed.
- **Installing Panda agent**: once the installation process is complete, the computer will no longer appear on the list of discovered computers.
- **Hidden computer.**
- **Unmanaged computer**: the computer doesn't have the Panda agent installed.



Computer details

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

Discovered by

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

Figure 25: details of a discovered computer

Computer details

- **Computer name.**
- **Description:** lets you assign a description to the computer, even though it is currently not managed.
- **First seen:** date/time when the computer was first discovered.
- **Last seen:** date/time when the computer was last discovered.
- **IP address.**
- **Physical addresses (MAC).**

- **Domain:** Windows domain the computer belongs to.
- **NIC manufacturer:** manufacturer of the computer's network interface card.

Last discovery computer

- **Computer**: name of the discovery computer that last found the unmanaged computer.
- **Last seen**: date/time when the computer was last discovered.

6.5.7 Installing the protection on computers

To remotely install the **Panda Adaptive Defense 360** software on one or more computers on your network follow the steps below:

From the list of discovered computers

- Go to the list of discovered computers. There are three ways to do this:
  - Go to **My lists** on the left-hand side menu and click the **Add** link. From the drop-down menu, select the **Unmanaged computers discovered** list.
  - 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 Adaptive Defense 360**.
  - Go to the **Computers** menu at the top of the console. Click **Add computers** and select **Discovery and remote installation.** A wizard will be displayed. Click the link **View unmanaged computers discovered.**
- From the list of discovered computers, select **Discovered** or **Hidden** depending on the status of the relevant computers **(1).**
- Select the checkboxes that correspond to the computers that you want to install the software on.
- To install it on multiple computers simultaneously, click the general context menu and select **Install Panda agent**.
- To install it on a single computer, click the computer's context menu and then click **Install Panda agent**.
- Configure the installation by following the steps described in section 6.4.3.
- You can enter one or multiple installation credentials. Use the local administrator account of the target computer or the domain that it belongs to in order to install the software successfully.

From the computer details window

Click a discovered computer to display its details window. At the top of the screen you'll see the button **Install Panda agent**. Follow the steps detailed in section 6.4.3 Manually installing the Panda Adaptive Defense 360 software.

6.6. Installation with centralized tools

6.6.1 Using the command line to install the installation package

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

- **IGNORE_LEGACY_AGENT=[TRUE|FALSE]**: keeps the **Panda Endpoint Protection/Plus** agent of the traditional platform (legacy) product if already installed. The default value is FALSE; if the legacy product's agent is already installed on the computer the installation process is interrupted.
- **GROUPPATH="group1\group2"**: path in the group tree where the computer will reside. The 'All' root node is not specified. If the group doesn't exist, the computer will be integrated into the 'All' root node.
- **PRX_SERVER**: name or IP address of the corporate proxy server.
- **PRX_PORT**: port of the corporate proxy server.
- **PRX_USER**: user of the corporate proxy server.
- **PRX_PASS**: password of the corporate proxy server.

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

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

6.6.2 Deploying Panda Adaptive Defense 360 from Panda Systems Management

Panda Systems Management customers can deploy **Panda Adaptive Defense 360** for Windows, macOS and Linux automatically using the following components:

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

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

Component features and requirements

These components don't have any specific requirements besides those indicated for **Panda Systems Management** and **Panda Adaptive Defense 360 on Aether**.

Component size:

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

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

6.6.3 Deploying Panda Adaptive Defense 360 with Microsoft Active Directory

There are third-party tools that can help you install the **Panda Adaptive Defense 360** software centrally on Windows devices across medium-sized and large networks. Below we have listed the steps to take to deploy the **Panda Adaptive Defense 360** software to Windows computers on a network with Active Directory using GPO (Group Policy Object).

1 Download and share the Panda Adaptive Defense 360 installer

- Move the **Panda Adaptive Defense 360** installer to a shared folder which is accessible to all the computers that are to receive the software.

2 Create a new OU (Organizational Unit) called "Adaptive Defense"

- Open the "Active Directory Users and Computers" applet in the network's Active Directory.

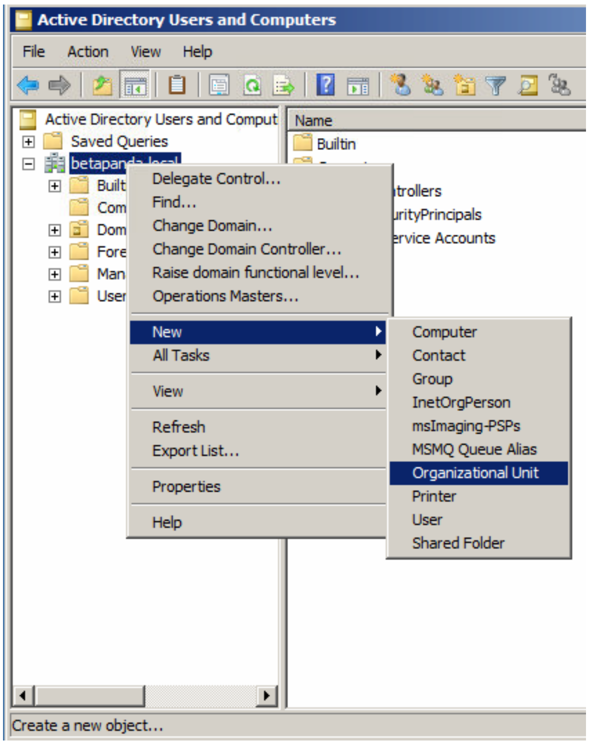


Figure 26: create an Organizational Unit

- Open the Group Policy Management snap-in and, in Domains, select the newly created OU to block inheritance.

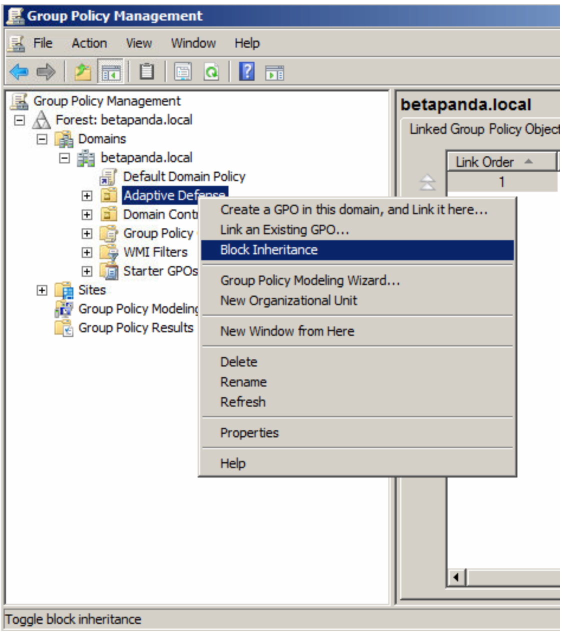
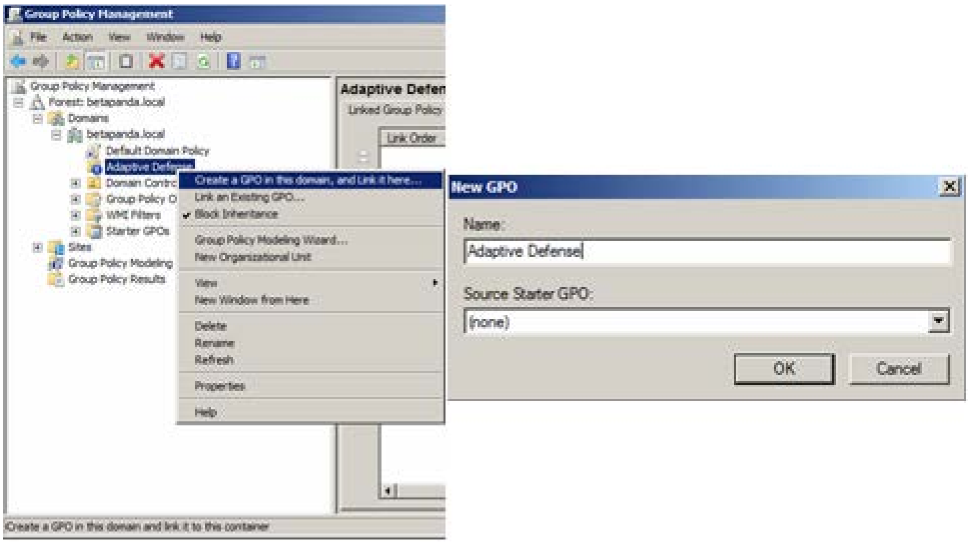


Figure 27: block inheritance

- Create a new GPO in the "Adaptive Defense" OU.



Name: Adaptive Defense

Source Starter GPO: (none)

Figure 28: create a GPO

3 Add a new installation package to the newly created GPO

- Edit the GPO.

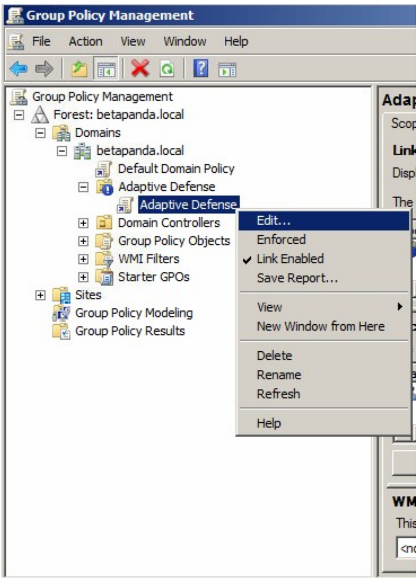


Figure 29: edit the newly created GPO

- Add a new installation package which contains the **Panda Adaptive Defense 360** software. To do this, you will be asked to add the installer to the GPO.

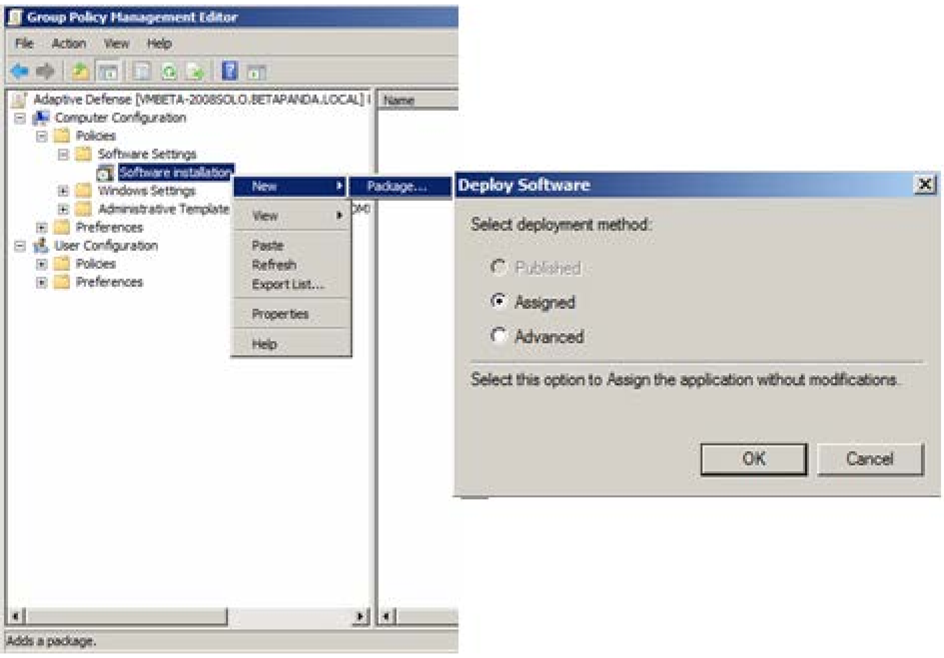
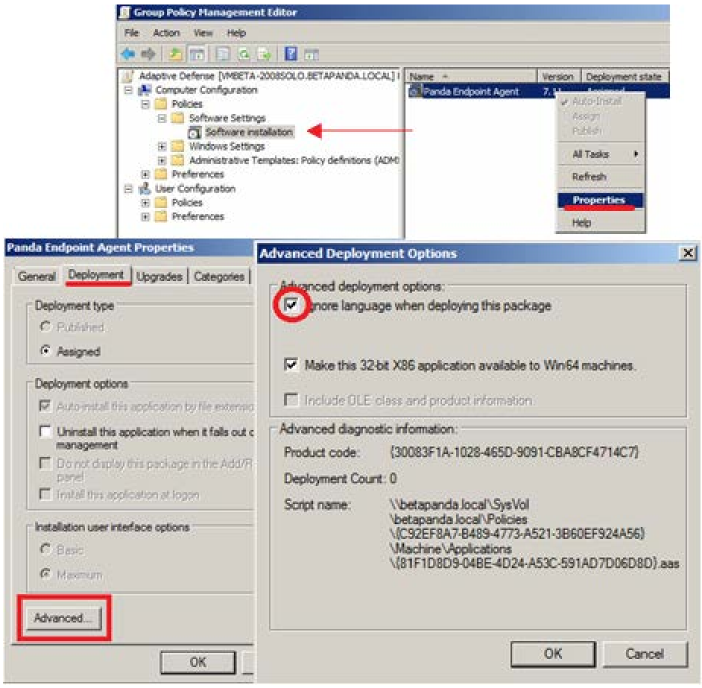


Figure 30: assign a new deployment package

4 Edit the deployment properties

- Go to Properties, Deployment, Advanced, and select the checkbox to avoid checking the target operating system against the one defined in the installer.



Deployment type
○ Published
● Assigned

Deployment options
☑ Auto-install this application by file extensio
□ Uninstall this application when it falls out o management
□ Do not display this package in the Add/R panel
□ Install this application at logon

Installation user interface options
○ Basic
● Maximum

Advanced deployment options:
☑ Ignore language when deploying this package
☑ Make this 32-bit X86 application available to Win64 machines.
□ Include OLE class and product information

Advanced diagnostic information:
Product code: {30083F1A-1028-465D-9091-CBA8CF4714C7}
Deployment Count: 0
Script name: \\betapanda.local\SysVol\betapanda.local\Policies\{C92EF8A7-B489-4773-A521-3B60EF924A56}\Machine\Applications\{81F1D8D9-04BE-4D24-A53C-591AD7D06D8D}.aas

Figure 31: configure the deployment package

- Finally, in the Adaptive Defense OU you created in “Active Directory Users and Computers”, add all the network computers to which the software will be sent.

6.7. Uninstalling the software

You can uninstall the **Panda Adaptive Defense 360** software manually from the operating system’s control panel, or remotely from the **Computers** area or from the **Computer protection status and Licenses lists**.

6.7.1 Manual uninstallation

The **Panda Adaptive Defense 360** software can be manually uninstalled by end users themselves, provided the administrator has not set an uninstallation password when configuring the security profile for the computer in question. If an uninstallation password has been set, the end user will need authorization or the necessary credentials to uninstall the protection.

Installing **Panda Adaptive Defense 360** actually installs multiple independent programs depending on the target platform:

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

To completely uninstall **Panda Adaptive Defense 360**, all modules must be removed. If only the protection module is uninstalled, the agent will install it again after some time.

On Windows 8 and later:

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

On Windows Vista, Windows 7, Windows Server 2003 and later:

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

On Windows XP:

- Control Panel > Add or remove programs.

On macOS:

- Finder > Applications > Drag the icon of the protection to uninstall to the recycle bin, or run the following command `sudo sh /Applications/Protection-Agent.app/Contents/uninstall.sh`.
- Dragging the icon to the recycle bin doesn't uninstall the agent. To remove it, you have to run the following command `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`

On Android devices:

- Go to Settings. Security > Device administrators.
- Clear the Panda Adaptive Defense 360 checkbox. Then, tap Disable > OK.
- Back in the Settings window, tap Apps. Click Panda Adaptive Defense 360 > Uninstall > OK.

On Linux:

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

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

We recommend using the command line to uninstall the product:

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

6.7.2 Manual uninstallation results

Uninstalling the Panda Adaptive Defense 360 software (Panda agent and protection) from a computer will cause it to disappear completely from the management console along with its associated information (counters, reports, computer activity and process activity information, etc.).

If, later, the computer is reintegrated into the management console by reinstalling the Panda Adaptive Defense 360 software, all previously-deleted information will be immediately retrieved.

6.7.3 Remote uninstallation

Follow these steps to remotely uninstall the Panda Adaptive Defense 360 software from a Windows computer:

- Access the **Computers** area (or the **Licenses or Computer protection status** lists), and select the checkboxes of the computers whose protection you want to uninstall.
- From the action bar, click the **Delete** button. A confirmation window will be displayed.
- In the confirmation window, select the **Uninstall the Panda agent from the selected computers** checkbox to completely remove the Panda Adaptive Defense 360 software.

Once uninstalled, all data associated with the computers will disappear from the management console and its different counters (malware detected, URLs blocked, emails filtered, devices blocked, etc.). However, all that information will be retrieved as soon as you reinstall the **Panda Adaptive Defense 360** software.

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

7. Managing computers and devices

The Computers area
The computers list panel
The computer tree panel
The Filters tree
The Groups tree
Computer details

7.1. Introduction

The management console lets you display the computers managed in an organized and flexible way, enabling administrators to rapidly locate devices.

7.1.1 Requirements for managing computers from the management console

In order for a network device to be managed through the management console, the Panda agent must be installed on the device.

As with other Panda Security products based on **Aether, Panda Adaptive Defense 360** delivers the Panda agent in the installation package for all compatible platforms.

Devices without a **Panda Adaptive Defense 360** license but with the Panda agent installed will appear in the management console, although the protection will be uninstalled and it won't be possible to run scans or perform other **Panda Adaptive Defense 360** tasks on them**.**

Computers with expired licenses will still be scanned for threats, but the signature file won't be updated and the advanced protection won't be applied. In this condition, Panda Adaptive Defense 360 won't be an effective solution to combat threats, and Panda Security strongly recommends renewing the contracted services in order to keep the network protected.

7.2. The Computers area

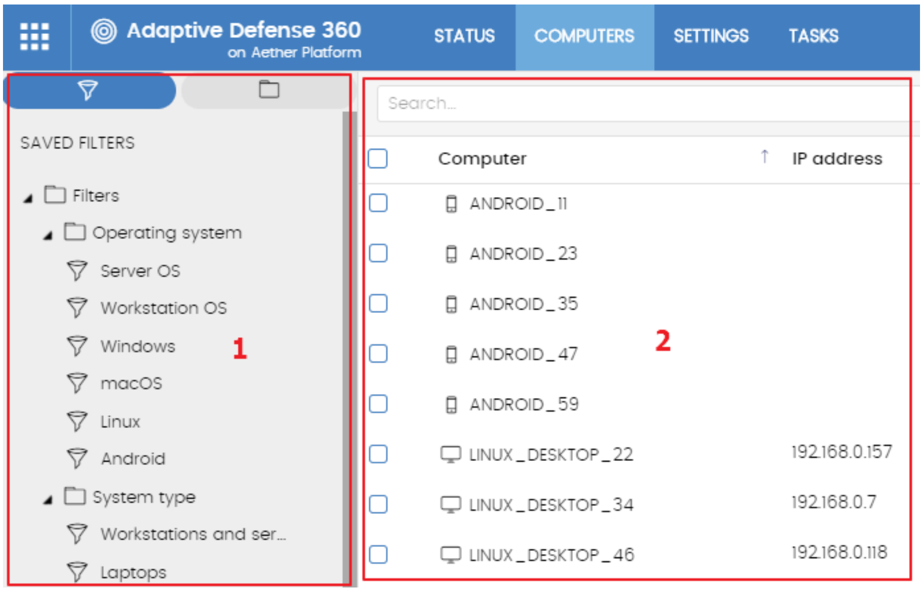


Figure 32: general view of the panels in the Computers area

To access the area for managing devices, click the **Computers** menu**.** Two different areas are displayed: the side panel with the **Computers** tree **(1)** and the main panel with the **List of computers (2)**. Both panels work together and this chapter explains how they operate.

When you select an item from the **Computers** tree, the **Computers list** is updated with all the devices assigned to the selected section of the tree.

Display computers in subgroups

It is possible to restrict the list of devices by displaying only those that belong to the selected branch of the tree, or alternatively by displaying all devices in the selected branch and its corresponding sub-branches. To do this, click the context menu and select **Show computers in subgroups**.

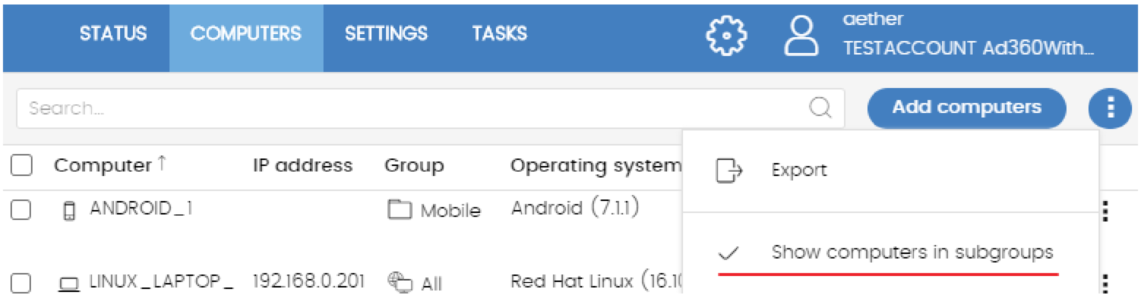


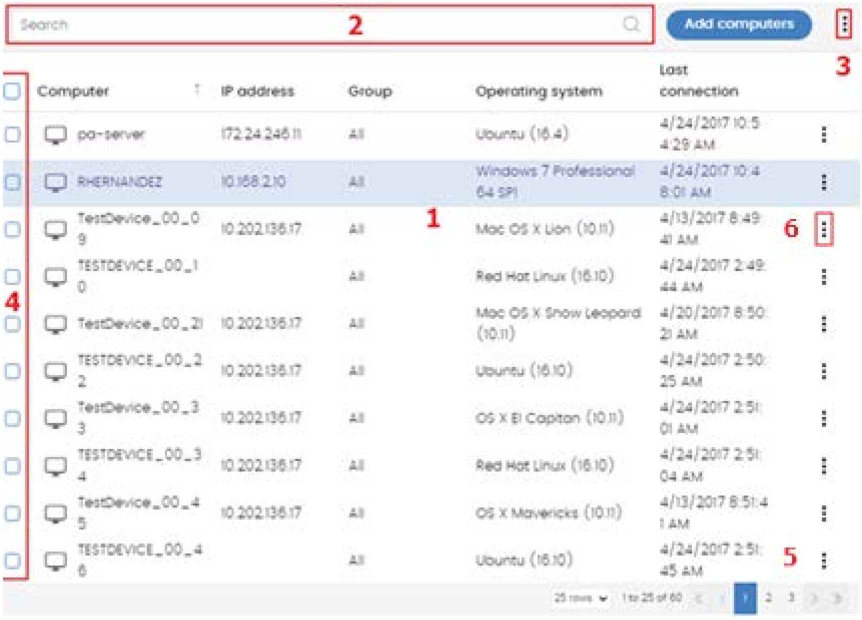
Figure 33: show computers in subgroups

7.3. The Computers list panel

The Computers screen 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 figure below shows all items that make up the Computer screen:

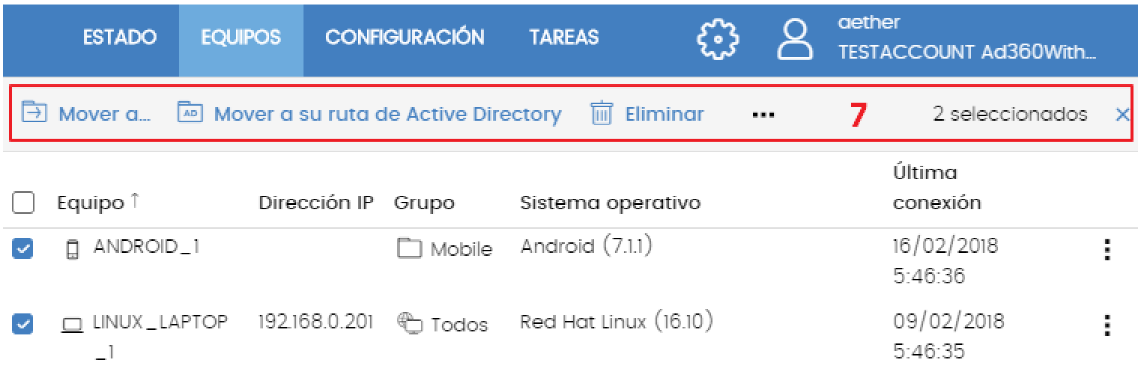
- **(1)** List of computers belonging to the selected branch.
- **(2)** Search tool. The search tool lets you find computers by their name. It supports partial matches and doesn't differentiate between uppercase and lowercase letters.
- **(3)** Context menu: lets you apply an action on multiple computers.
- **(4)** Selection checkboxes.
- **(5)** There is a pager at the bottom of the screen to ease navigation.
- **(6)** Context menu



□	Computer ↑	IP address	Group	Operating system	Last connection
□	pa-server	172.24.246.11	All	Ubuntu (16.4)	4/24/2017 10:5 4:29 AM
□	RHERNANDEZ	10.168.2.10	All	Windows 7 Professional 64 SP1	4/24/2017 10:4 8:01 AM
□	TestDevice_00_09	10.202.136.17	All	Mac OS X Lion (10.11)	4/13/2017 8:49: 41 AM
□	TESTDEVICE_00_10		All	Red Hat Linux (16.10)	4/24/2017 2:49: 44 AM
□	TestDevice_00_21	10.202.136.17	All	Mac OS X Snow Leopard (10.11)	4/20/2017 8:50: 21 AM
□	TESTDEVICE_00_22	10.202.136.17	All	Ubuntu (16.10)	4/24/2017 2:50: 25 AM
□	TestDevice_00_33	10.202.136.17	All	OS X El Capitan (10.11)	4/24/2017 2:51: 01 AM
□	TESTDEVICE_00_34	10.202.136.17	All	Red Hat Linux (16.10)	4/24/2017 2:51: 04 AM
□	TestDevice_00_45	10.202.136.17	All	OS X Mavericks (10.11)	4/13/2017 8:51:4 1 AM
□	TESTDEVICE_00_46		All	Ubuntu (16.10)	4/24/2017 2:51: 45 AM

Figure 34: the computers list panel

Select one or more computers using their checkboxes **(4)**. The search tool **(2)** will be hidden and the action bar **(7)** will be displayed instead.



□	Equipo ↑	Dirección IP	Grupo	Sistema operativo	Última conexión
☑	ANDROID_1		Mobile	Android (7.1.1)	16/02/2018 5:46:36
☑	LINUX_LAPTOP_1	192.168.0.201	Todos	Red Hat Linux (16.10)	09/02/2018 5:46:35

Figure 35: action bar

7.3.1 Computers list

You will see the following details for each computer:

Field	Comments	Values
Computer	Computer name and type	Character string 🖥 Desktop computer (Windows, Linux or macOS workstation or server) 💻 Laptop computer 📱 Mobile device (Android smartphone or tablet)

Field	Comments	Values
IP address	The computer's primary IP address	Character string 🖥 Computer in the process of being isolated 🖥 Isolated computer 🖥 Computer in the process of stopping being isolated
Group	Folder in the Panda Adaptive Defense 360 Groups tree to which the computer belongs, and its type	Character string 📁 Group 🖥 Active Directory domain or root group AD Organizational Unit 📁 Groups tree root
Operating system		Character string
Last connection	Date when the computer status was last sent to Panda Security's cloud	Date

Table 8: fields in the Computers list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Computer name	Character string
IP addresses	List of the IP addresses of the cards installed on the computer	Character string
Physical addresses (MAC)	List of the physical addresses of the cards installed on the computer	Character string
Domain	Windows domain to which the computer belongs	Character string
Active Directory	Path in the company's Active Directory tree where the computer is found	Character string
Group	Folder in the Panda Adaptive Defense 360 Groups tree to which the computer belongs	Character string
Agent version		Character string

Field	Comments	Values
System boot date		Date
Installation date	Date when the Panda Adaptive Defense 360 software was successfully installed on the computer	Date
Last connection date	Last time the computer connected to the cloud	Date
Platform	Type of operating system installed	Windows Linux macOS Android
Operating system	Operating system installed on the computer, internal version and patches applied	Character string
Virtual machine	Indicates whether the computer is physical or virtual	Boolean
Exchange Server	Version of the mail server installed	Character string
Protection version		Character string
Last update on	Date the protection was last updated	Date
Licenses	Licensed product	Panda Adaptive Defense 360
Proxy and language settings	Name of the proxy and language settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer has inherited the proxy and language settings	Character string
Security settings for workstations and servers	Name of the security settings applied to the workstation or server	Character string
Settings inherited from	Name of the folder from which the computer has inherited its settings	Character string
Security settings for Android devices	Name of the security settings applied to the mobile device	Character string
Settings inherited from	Name of the folder from which the device has inherited its settings	Character string
Per-computer settings	Name of the settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer has inherited its settings	
Personal data monitoring settings	Name of the personal data monitoring (Panda Data Control) settings applied to the computer	Character string

Field	Comments	Values
Settings inherited from	Name of the folder from which the computer has inherited its personal data monitoring settings	Character string
Description		Character string

Table 9: fields in the 'Computers list' exported file

Filter tools

Field	Comments	Values
Computer	Computer name	Character string

Table 10: filters available on the Computers list screen

7.3.2 Management tools

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

- **Move to**: opens a window showing the group tree. Choose the group to move the computer to. The computer will inherit the settings assigned to the target group. Refer to Chapter 8 for more information about how to define settings.
- **Move to Active Directory path**: moves the selected computer to the group that corresponds to its organizational unit in the organization's Active Directory.
- **Delete**: deletes the computer from the console and uninstalls the Panda Adaptive Defense 360 software from it. Refer to chapter 6 Installing the Panda Adaptive Defense 360 software for more information about how to uninstall the Panda Adaptive Defense 360 software.
- **Scan now**: see later in this chapter for an introduction to scan tasks, or see chapter 14 Tasks for more information about immediate scan tasks.
- **Schedule scan**: see later in this chapter for an introduction to scan tasks, or see chapter 14 Tasks for more information about scheduled tasks.
- **Restart**: refer to chapter 18 Remediation tools for more information about remote computer restart.
- **Isolate computer**: refer to chapter 18 Remediation tools for more information about computer isolation and its implications.
- **Stop isolating the computer**: refer to chapter 18 Remediation tools for more information about computer isolation and its implications.
- **Schedule patch installation**: refer to chapter 13 Panda Patch Management (Updating vulnerable programs) for more information on how to install patches on Windows computers.
- **X selected**: to undo the current selection, click the **X selected** button from the action bar.

7.4. The Computers tree panel

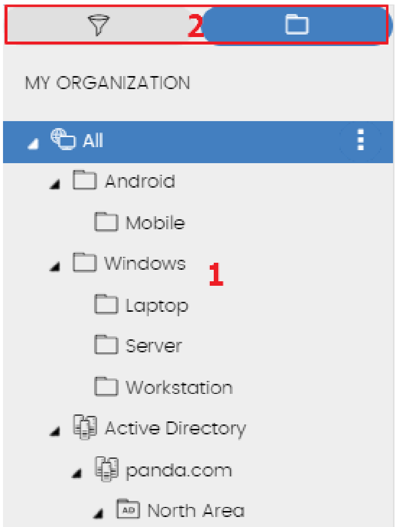


Figure 36: the Computers tree panel

Panda Adaptive Defense 360 displays your computers through the Computers tree **(2)**, which offers two independent views or trees **(1)**:

- **Filters tree** : this lets you manage network computers using dynamic groups. Computers are automatically assigned to these types of groups.
- **Groups tree** : this lets you manage network devices through static groups. Computers are manually assigned to these types of groups.

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

- Locate computers that fulfill certain criteria in terms of hardware, software or security.
- Easily assign security settings profiles.
- Take troubleshooting action on groups of computers.

To locate unprotected computers or those with certain security criteria or protection status, see Chapter 16 Malware and network visibility. To assign security settings profiles, see Chapter 8 Managing settings. To run troubleshooting tasks, see chapter 19 Remediation tools.

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

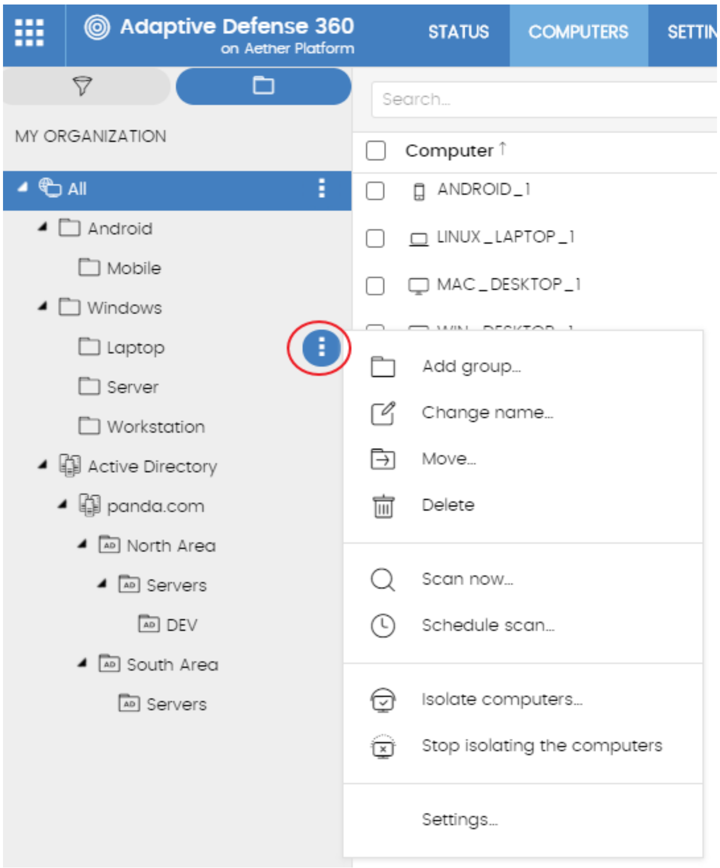


Figure 37: pop-up menu with all available operations for the selected branch

7.5. Filters tree

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

The Filters tree can be accessed from the left-hand panel, by clicking the filter icon.

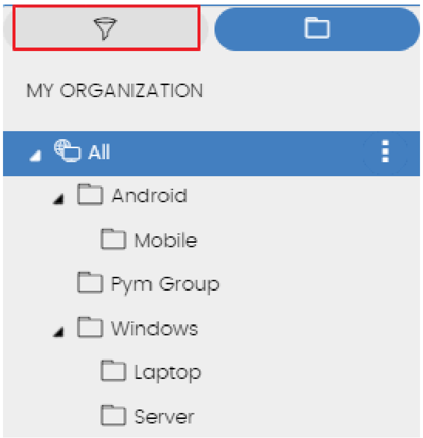


Figure 38: access to the Filters tree

Clicking different items in the tree will update the right-hand panel, presenting all the computers that meet the criteria established in the filter.

7.5.1 What is a filter?

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

A computer can belong to more than one filter.

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

7.5.2 Groups of filters

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

7.5.3 Predefined filters

Panda Adaptive Defense 360 includes a series of commonly used filters that administrators can use to organize and locate network computers. Predefined filters can also be edited or deleted.

A predefined filter that has been deleted cannot be recovered.

Name	Group	Description
Workstations and servers	Type of device	List of physical workstations or servers
Smartphones and tablets	Type of device	List of smartphones and tablets
Virtual machines	Type of device	List of virtual machines
Server operating systems	Operating system	List of computers with a server operating system installed
Workstation operating systems	Operating system	List of computers with a workstation operating system installed
Windows	Operating system	List of all computers with a Windows operating system installed

Name	Group	Description
macOS	Operating system	List of all computers with a Mac OS installed
Android	Operating system	List of all computers with an Android operating system installed
Java	Software	List of all computers with the Java JRE SDK installed
Adobe Acrobat Reader	Software	List of all computers with Acrobat Reader installed
Adobe Flash Player	Software	List of all computers with Flash player installed
Google Chrome	Software	List of all computers with Chrome browser installed
Mozilla Firefox	Software	List of all computers with Firefox browser installed
Exchange server	Software	List of all computers with Microsoft Exchange Server installed

Table 11: list of predefined filters

7.5.4 Creating and organizing filters

The actions you can take on filters are available through the pop-up menu displayed when clicking the context menu for the relevant branch in the Filters tree.

Creating filters

To create a filter, follow the steps below:

- Click the context menu of the folder where the filter will be created.

> ***Filters cannot be nested if they are not in folders. If you select a filter in the tree, the newly created filter will be at the same level, in the same folder.***

- Click **Add filter**.
- Specify the name of the filter. It does not have to be a unique name. The configuration of the filter is described later in this chapter.

Creating folders

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

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

Deleting filters and folders

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

You cannot delete the 'Filters' root node.

Moving and copying filters and folders

To move or copy a filter or folder, follow the steps below:

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

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

Renaming filters and folders

To rename a filter or folder, follow the steps below:

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

It is not possible to rename the 'Filters' root folder. Also, to rename a filter you have to edit it.

7.5.5 Filter settings

To access the filter settings window, create a new filter or edit an existing one.

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

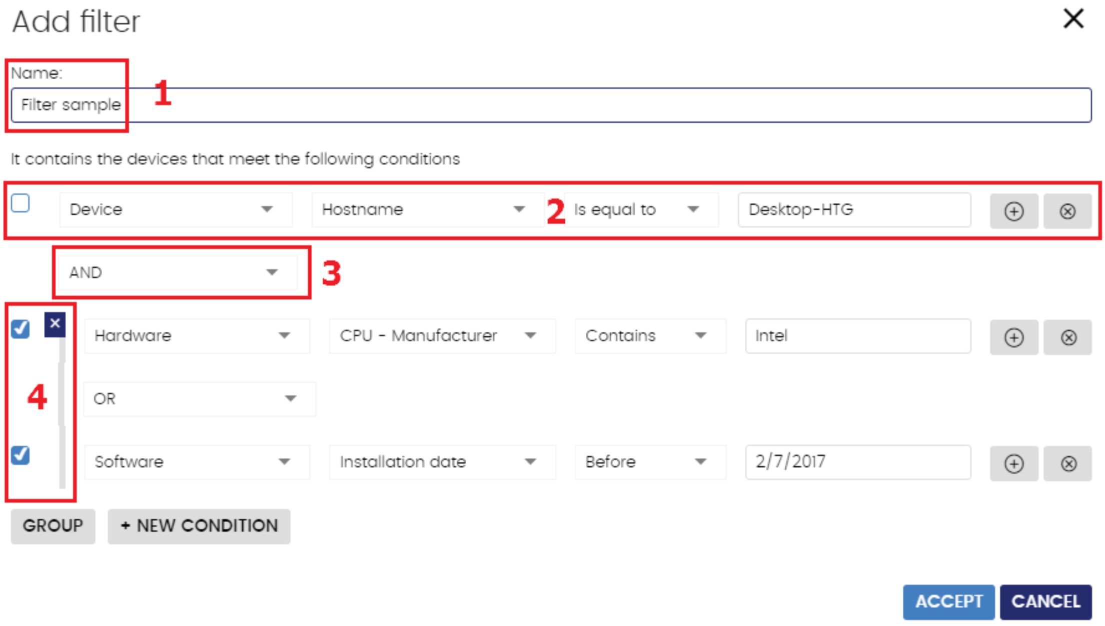
A filter has four sections:

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

7.5.6 Filter rules

A filter rule comprises the items described below:

- **Category (1)**: this groups the properties in sections to make it easy to find them.
- **Property (2)**: the characteristic of a computer that determines whether it belongs to a filter.
- **Operation (3)**: this determines the way in which the computer's characteristics are compared to the values set in the filter.



Add filter

Name: Filter sample

It contains the devices that meet the following conditions

☐ Device | Hostname | Is equal to | Desktop-HTG

AND

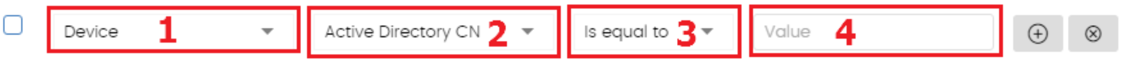
☑ Hardware | CPU - Manufacturer | Contains | Intel

OR

☑ Software | Installation date | Before | 2/7/2017

Figure 39: general view of the filter settings

- **Value (4)**: the content of the property. Depending on the type of property, the value field will change to reflect entries such as 'date', etc.



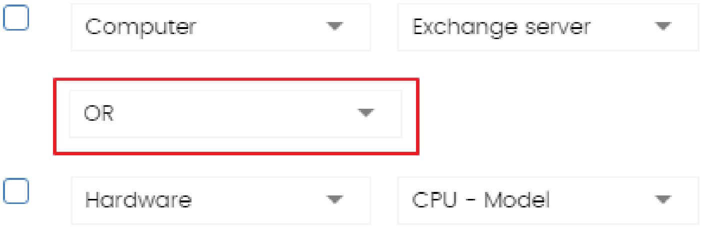
☐ Device | Active Directory CN | Is equal to | Value

Figure 40: components of a filter rule

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

7.5.7 Logical operators

To combine two rules in the same filter, use the logical operators **AND** or **OR**. This way, you can inter-relate several rules. The options **AND/OR** will automatically appear to condition the relation between the rules.



□ Computer ▾ Exchange server ▾

OR ▾

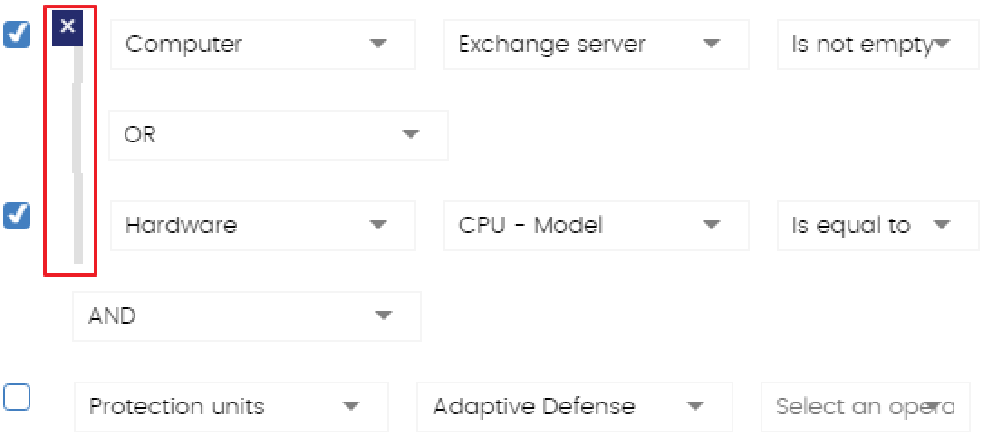
□ Hardware ▾ CPU - Model ▾

Figure 41: logical operator OR

7.5.8 Groups of filter rules

A group involves the use of parentheses in a logical expression. In a logical expression, parentheses are used to alter the order of the operators, in this case, the filter rules.

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



☑ ✕ Computer ▾ Exchange server ▾ Is not empty ▾

OR ▾

☑ Hardware ▾ CPU - Model ▾ Is equal to ▾

AND ▾

□ Protection units ▾ Adaptive Defense ▾ Select an opera

Figure 42: group of filter rules equivalent to (Rule 1 OR Rule 2) AND Rule 3

Groups with several levels can be defined in the same way that you can nest groups of logical operators by using parentheses.

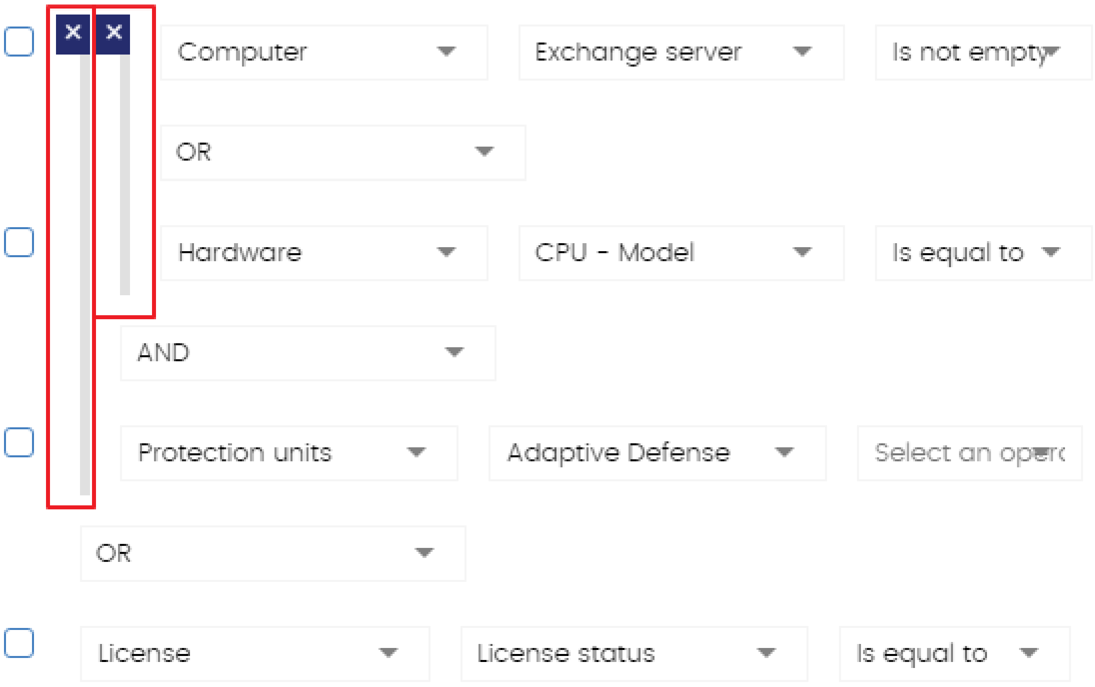


Figure 43: nested group equivalent to ((Rule 1 AND Rule 2) AND Rule 3) OR Rule 4

7.6. Groups tree

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

The Groups tree is accessible from the left panel by clicking the folder icon.

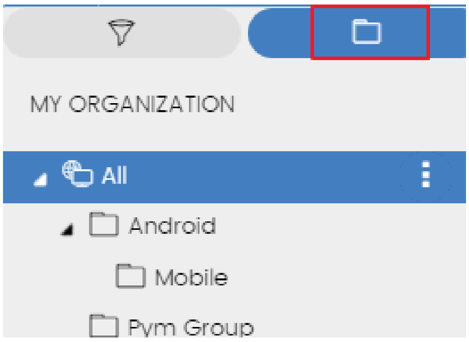


Figure 44: access to the Groups tree

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.

7.6.1 What is a group?

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

The maximum number of levels in a group is 10.

7.6.2 Group types

- **Root group** : this is the parent group from which all other folders derive.
- **Native groups** : these are the **Panda Adaptive Defense 360** standard groups. They support all operations (move, rename, delete, etc.) and contain other standard groups and computers.
- **Active Directory groups** : these groups replicate the Active Directory structure that already exists in your organization. Some operations cannot be performed on these groups. They contain other Active Directory groups and computers.
- **Active Directory root group** : contains all of the Active Directory domains configured on the organization's network. It contains Active Directory domain groups.
- **Active Directory domain group** : Active Directory branches representing domains. They contain other Active Directory domain groups, Active Directory groups and computers.

7.6.3 Group structure

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

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

7.6.4 Active Directory groups

For those organizations that have an Active Directory server installed on their network, **Panda Adaptive Defense 360** can automatically obtain the configured Active Directory structure and replicate it in the Groups tree. This way, the branch will show a computer distribution familiar to the administrator, helping them find and manage their computers faster.

To automatically replicate the Active Directory structure existing in the organization, the Panda agents report the Active Directory group they belong to the Web console and, as agents are deployed, the tree is populated with the various organizational units.

The Active Directory tree cannot be modified from the **Panda Adaptive Defense 360** console, it will only change when the underlying Active Directory structure is also changed. These changes are replicated in the **Panda Adaptive Defense 360** Web console within 15 minutes.

7.6.5 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 Groups tree.

Creating groups

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

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

Deleting groups

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

The All root node cannot be deleted

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

Moving groups

To move a group, follow the steps below:

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

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

Renaming groups

To rename a group, follow the steps below:

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

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

7.6.6 Moving computers from one group to another

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

Moving groups of computers to groups

To move several computers to a group at the same time, follow the steps below:

- Select the group **All** in order to list all the managed computers or use the search tool to locate the computers to move.
- Use the checkboxes to select the computers in the panel listing the computers.
- Click the ⋮ icon at the right of the search bar. A drop-down menu will appear with the option **Move to.** Click here to show the target groups tree.
- Select the target Groups tree.

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 assigning groups of computers, but simply select a single computer.
- Use the checkbox to select the computer in the list and click the ⋮ menu icon to the right.
- From the window with the details of the computer:
    - In the panel with the list of computers, click the computer you want to move in order to display the details.
    - In the **Group** field click **Change**. This will display a window with the target groups tree.
    - Select the target group and click **OK**.

Moving computers from an Active Directory group

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

Moving computers to an Active Directory group

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

Returning multiple computers to their Active Directory group

To return multiple computers to their original Active Directory group, click the context menu of the group where they are and select **Move computers to their Active Directory path**. All computers that belong to a group in the company's Active Directory and which have been moved by the administrator to other groups in the **Panda Adaptive Defense 360** console will be restored to their original Active Directory location.

7.6.7 Scan tasks

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

Immediate scans

Click the **Scan now** option to launch an immediate scan of all computers belonging to a group or any of its subgroups. A window will be displayed for you to select the scan type to run: **The entire computer** or **Critical areas**. Refer to chapter 15 Tasks for more information about the scan types available in **Panda Adaptive Defense 360**.

Scheduled scans

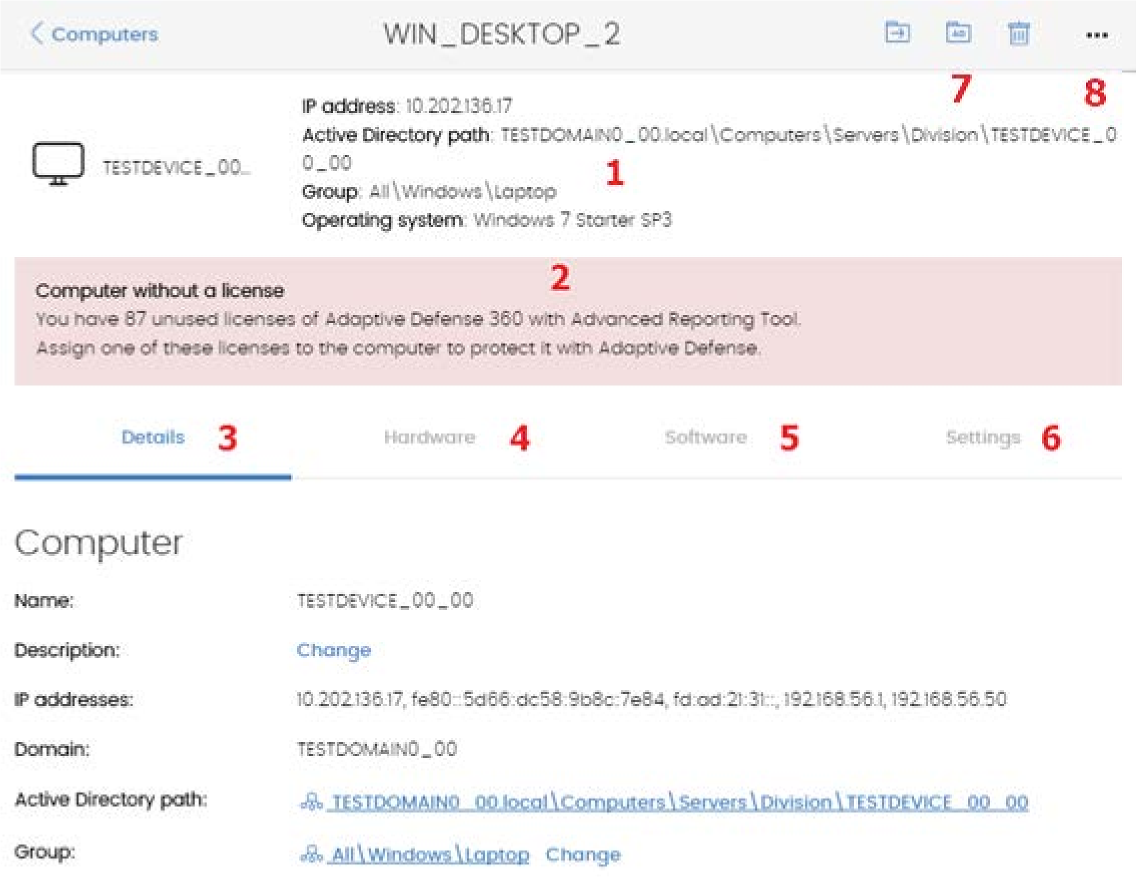
Click the **Schedule scan** option to create a scheduled scan task. Refer to chapter 15 Tasks for more information about how to configure a scheduled task.

7.7. Computer details

When you select a computer from the list of computers, a window is displayed with details of the hardware and software installed, as well as the security settings assigned to it.

The details window is divided into six sections:

- **General (1)**: this displays information to help identify the computer.
- **Notifications (2)**: details of any potential problems.
- **Details (3)**: this gives a summary of the hardware, software and security settings of the computer.
- **Hardware (4)**: here you can see the hardware installed on the computer, its components and peripherals, as well as resource consumption and use.
- **Software (5)**: here you can see the software packages installed on the computer, as well as versions and changes.
- **Settings (6)**: this shows the security settings and other settings assigned to the computer.



TESTDEVICE_00...

IP address: 10.202.136.17
Active Directory path: TESTDOMAIN0_00.local\Computers\Servers\Division\TESTDEVICE_00_00
Group: All\Windows\Laptop
Operating system: Windows 7 Starter SP3

Computer without a license
You have 87 unused licenses of Adaptive Defense 360 with Advanced Reporting Tool.
Assign one of these licenses to the computer to protect it with Adaptive Defense.

Computer

Name:	TESTDEVICE_00_00
Description:	Change
IP addresses:	10.202.136.17, fe80::5d66:dc58:9b8c:7e84, fd:ad:21:31::, 192.168.56.1, 192.168.56.50
Domain:	TESTDOMAIN0_00
Active Directory path:	TESTDOMAIN0_00.local\Computers\Servers\Division\TESTDEVICE_00_00
Group:	All\Windows\Laptop Change

Figure 45: general view of a computer's details

7.7.1 General section (1)

This contains the following information:

- **Name of the computer and icon** indicating the type of computer.
- **IP address**: IP address of the computer.
- **Active Directory path**: full path to the computer in the company's Active Directory.
- **Group**: the folder in the Groups tree to which the computer belongs.
- **Operating system**: full version of the operating system installed on the computer.
- **Computer role**: indicates if the computer has any of the following roles assigned to it: discovery computer, cache or proxy.

7.7.2 Computer notifications section (2)

These notifications describe any problems encountered on the computers with regard to the operation of **Panda Adaptive Defense 360**, as well as providing indications for resolving them. The following is a summary of the types of notifications generated and the recommended actions.

Unprotected computer:

- **Protection disabled**: a message is displayed stating that the antivirus protection, Adaptive Defense (advanced) protection, or Exchange protection is disabled. You are advised to assign protection settings to the computer with the protection enabled. See Chapter 8 for assigning security settings and Chapter 10 for creating security settings.

- **Protection with errors**: a message is displayed stating that the antivirus protection, Adaptive Defense (advanced) protection, or Exchange protection has an error. Restart the computer or reinstall the software. See Chapter 6 to install the software on the computer and Chapter 19 to restart the computer.
- **Error installing the patch manager**: an error occurred while installing the patch manager (**Panda Patch Management** on the computer.
  - **Unable to download**: installer not available.
  - **Unable to download**: the file is corrupted.
  - **Not enough disk space**.
- **Installation error**: the computer is unprotected because there was an error during installation. See Chapter 6 to reinstall the software on the computer.
- **Installation in progress**: the computer is unprotected because the installation of **Panda Adaptive Defense 360** is incomplete. Wait a few minutes until the installation is complete.

Out-of-date computer:

- **Computer pending restart**: the update for the security engine has been downloaded but the computer needs to be restarted for it to be applied. See Chapter 19 to restart the computer remotely.
- **Protection updates disabled**: the software won't receive any improvements. This will jeopardize the security of the computer in the future. See Chapter 14 to create and assign 'Per-computer settings' that allow the software to be updated.
- **Knowledge updates disabled:** the software won't receive any updates to the signature file. This will jeopardize the security of the computer in the short-term. See Chapters 10 and 11 to create security settings that allow the signature file to be updated.
- **Knowledge update error**: the download of the signature file failed. There is an explanation in this chapter of how to check the free space on your hard disk. See Chapter 19 to restart the computer. See Chapter 6 to reinstall software on the computer.

Blocked files

The computer contains unknown files that are in the process of classification and cannot be run. See the **Currently blocked programs being classified** panel in the dashboard to check the file and add an exclusion if necessary. See Chapter 17 to manage items that are in the process of classification.

Offline since…

The computer has not connected to the Panda Security cloud in several days. Check the connectivity of the computer and the firewall settings. See chapter 17 Managing threats, quarantined items and items being classified to check whether the connectivity requirements are fulfilled. See Chapter 6 to reinstall the software.

Pending restart

- The administrator has requested a restart which has not yet been applied.
- Patches have been installed that require a restart.

7.7.3 Details section (3)

The information on this tab is divided into two sections: Computer (with information about the device settings provided by the Panda agent), and Security (with the status of the Panda Adaptive Defense 360 protection).

- **Computer**
  - **Name:** computer name
  - **Description**: descriptive text provided by the administrator
  - **Physical addresses (MAC)**: physical addresses of the network interface cards installed
  - **IP addresses**: list of all the IP addresses (main and alias)
  - **Domain**: Windows domain that the computer belongs to. This is empty if it does not belong to a domain.
  - **Active Directory path**: the path of the computer in the company's Active Directory tree.
  - **Group**: the group in the Groups tree to which the computer belongs. To change the computer's group, click **Change**.
  - **Operating system**
  - **Mail server**: version of Microsoft Exchange server installed on the computer.
  - **Virtual machine**: this indicates whether the computer is physical or virtual.
  - **Licenses**: the Panda Security product licenses installed on the computer. For more information, see Chapter 5.
  - **Agent version**
  - **System boot date**
  - **Installation date**
  - **Last connection** of the agent to the Panda Security infrastructure. The communications agent will connect at least every four hours.
- **Security:** this section indicates the status (Enabled, Disabled, Error) of the **Panda Adaptive Defense 360** technologies.
  - **Advanced protection**
  - **File antivirus**
  - **Mail antivirus**
  - **Web browsing antivirus**
  - **Firewall protection**
  - **Device control**
  - **Web access control**
  - **Patch management**
  - **Protection version**
  - **Knowledge update date:** date when the signature file was last updated
- **Data Control:** this section indicates the status and the installed version of the Panda Data Control service.
- **Personal data monitoring.**

- **Allow data searches on this computer:** indicates if the computer has a settings profile assigned that allows it to receive file searches and report their results**.**
- **Indexing status:** provided that file searches by content are allowed, Panda Data Control must parse all files contained in the supported storage media to retrieve their content and generate a database**.**
- **Version:** internal version of the indexing engine**.**

For more information about the security details of the protected computers, see chapter 16 Malware and network visibility

7.7.4 Hardware section (4)

This contains the following information:

- **CPU**: information about the processor on the computer, and a line chart with CPU consumption at different time intervals based on your selection:
  - 5 minute intervals over the last hour.
  - 10 minute intervals over the last 3 hours.
  - 40 minute intervals over the last 24 hours.
- **Memory**: information about the memory chips installed, and a chart with memory consumption at different time intervals based on your selection:
  - 5 minute intervals over the last hour.
  - 10 minute intervals over the last 3 hours.
  - 40 minute intervals over the last 24 hours
- **Disk**: information about the mass storage system, and a pie chart with the percentage of free/used space at that moment.

7.7.5 Software section (5)

This contains a list of the programs installed on the computer and all updates of the Windows operating system and other Microsoft programs. The information displayed is as follows:

- **Name:** program name
- **Publisher:** program developer
- **Installation date**
- **Size**
- **Version**

Search tool

The tool that enables you to locate software packages using partial or complete matches in all the fields shown previously.

The drop-down menu lets you restrict the search to only updates, installed software or both.

Change log

The change log lists all the software installation and uninstallation events that take place within the configured date range. For each event, the following information is displayed:

- **Event**: installation 🖫 or uninstallation 🗑
- **Name**: name of the software package responsible for the event
- **Publisher:** the program developer
- **Version**
- **Date**

7.7.6 Settings section (6)

The **Settings** section displays the different types of settings assigned to the computer, and allows you to edit and manage them:

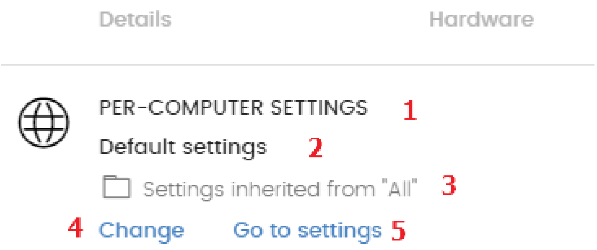


Figure 46: editing and managing the assigned settings

- **(1)** Settings type: per-computer settings, Proxy and language settings, Settings for workstations and servers, Settings for Android devices.
- **(2)** Settings name.
- **(3)** Method used to assign the settings: assigned directly to the computer or inherited from a parent group.
- **(4)** Button to change the settings assigned to the computer.
- **(5)** Button to edit the settings options.

> *Refer to chapter 8 Managing settings for more information about how to create, edit and assign settings.*

7.7.7 Action bar (7)

Shows the different actions you can take on the computer:

- **Move to**: moves the computer to a standard group.
- **Move to Active Directory group**: moves the computer to its original Active Directory group.

- **Delete**: frees up the **Panda Adaptive Defense 360** license and deletes the computer from the Web console.
- **Scan now**: lets you run a scan task immediately. Refer to chapter 19 Remediation tools for more information.
- **Schedule scan:** lets you schedule a scan task. Refer to chapter 15 Tasks for more information.
- **Isolate computer**: prevents the computer from establishing external communications in order to help administrators perform remote forensic analysis tasks on compromised computers. Refer to chapter 19 for more information.
- **Stop isolating the computer**: restores communications with other computers. Refer to chapter 19 Remediation tools for more information about computer isolation and its implications.
- **Schedule patch installation:** creates a task that installs all released patches missing from the target computer. See chapter 13 Panda Patch Management (Updating vulnerable programs) for more information.
- **Restart**: restarts the computer immediately. Refer to chapter for more information.
- **Report a problem**: opens a support ticket for Panda Security's support department. Refer to chapter 19 for more information.

7.7.8 Hidden icons (8)

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

8. Managing settings

8.1. Introduction

This chapter looks at the resources implemented in **Panda Adaptive Defense 360** for managing the settings of network computers.

8.2. What are settings?

Settings, also called "settings profiles" or simply "profiles", offer administrators a simple way of establishing the security, productivity and connectivity parameters on the computers managed through **Panda Adaptive Defense 360**.

Administrators can create as many profiles and variations of settings as they deem necessary. The need for new settings may arise from the varied nature of computers on the network:

- Computers used by people with different levels of IT knowledge require different levels of permissiveness with respect to the running of software, access to the Internet or to peripherals.
- Users with different tasks to perform and therefore with different needs require settings that allow access to different resources.
- Users that handle confidential or sensitive information require greater protection against threats and attempts to steal the organization's intellectual property.
- Computers in different offices require settings that allow them to connect to the Internet using a variety of communication infrastructures.
- Critical servers require specific security settings.

8.3. Overview of assigning settings to computers

In general, assigning settings to computers is a four-step process:

1 **Creation of groups of similar computers or with identical connectivity and security requirements**

2 **Assigning computers to a corresponding group**

3 **Assigning settings to groups**

4 **Immediate and automatic pushing out of settings to network computers**

All these operations are performed from the Groups tree, which can be accessed from the **Computers** menu**.** The Groups tree is the main tool for assigning settings quickly and to large groups of computers.

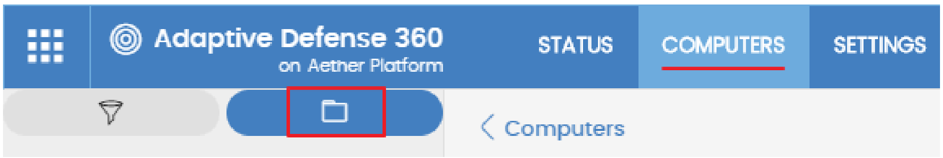


Figure 47: access to the Groups tree

Administrators therefore have to put similar computers in the same group and create as many groups as there are different types of computers on the network.

For more information about working with the Groups tree and assigning computers to groups, see chapter 7.

8.3.1 Immediate deployment of settings

Once settings are assigned to a group, they will be applied to the computers in the group immediately and automatically, in accordance with the inheritance rules described later in this chapter. The settings are applied to the computers in just a few seconds.

To disable the immediate deployment of settings, refer to chapter 9

8.3.2 Multi-level trees

In medium-sized and large organizations, there could be a wide range of settings. To facilitate the management of large networks, **Panda Adaptive Defense 360** lets you create group trees with various levels.

8.3.3 Inheritance

In large networks, it is highly likely that administrators will want to reuse existing settings on groups within the hierarchical structure of the tree. The inheritance feature lets you assign settings to a group and then, in order to save time, automatically to all the groups below this group in the tree.

8.3.4 Manual settings

To prevent settings being applied to all inferior levels in the Groups tree, or to assign different settings to a certain computer in part of the tree, it is possible to manually assign settings to groups or individual computers.

8.3.5 Default settings

Initially, all computers in the Groups tree inherit the settings established in the **All** root node.

The **All** root node has the following settings set by default:

- **Per-computer settings**: default settings.
- **Proxy and language**: default settings.
- **Security settings for workstations and servers**: default settings.
- **Security settings for Android devices:** default settings.
- **Personal data monitoring:** default settings.
- **Patch management**: default settings
- **Sensitive data**: default settings.

This means that all computers are protected from the outset, even before administrators have accessed the console to establish security settings.

8.4. Modular vs monolithic settings profiles

Panda Adaptive Defense 360 uses a modular format for creating and distributing settings to computers. As such, there are six independent profiles covering six settings areas.

The six types of profiles are as follows:

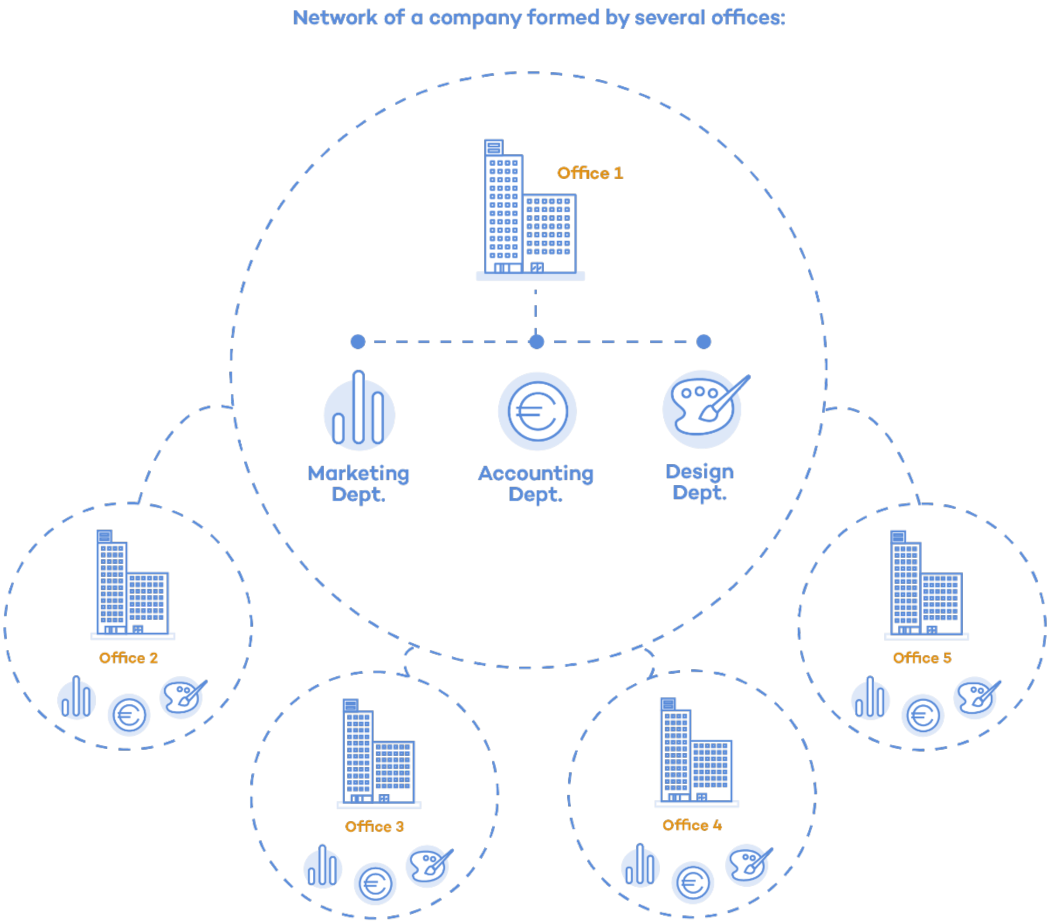
- Per-computer settings.
- Proxy and language settings.
- Security settings for workstations and servers.
- Security settings for Android devices.
- Patch management.
- Personal data monitoring.

The reason for using this modular format and not just a single, monolithic profile that covers all the settings is to reduce the number of profiles created in the management console. The modular format means that the settings are lighter than monolithic configurations that result in numerous large and redundant profiles with little differences between each other. This in turn reduces the time that administrators have to spend managing the profiles created.

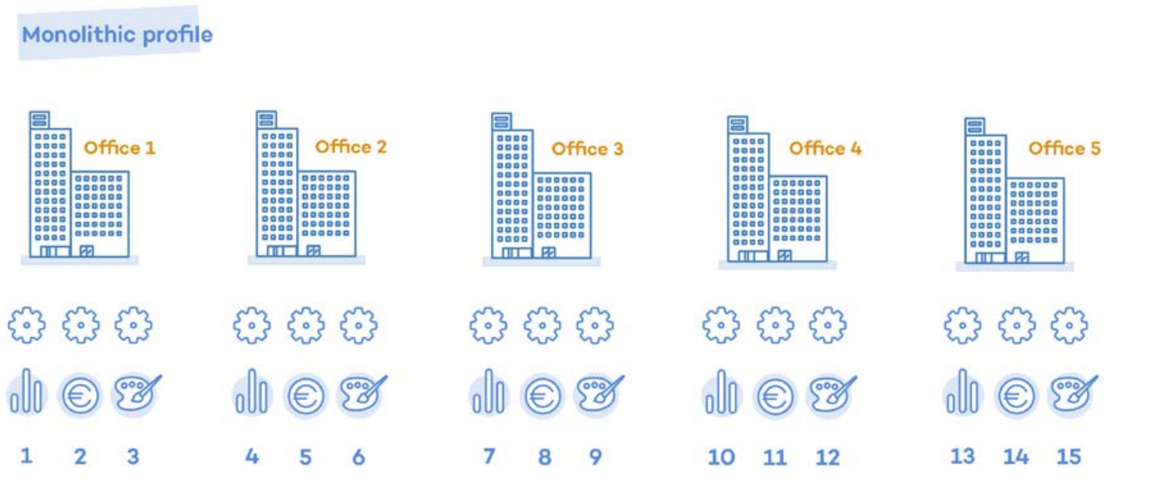
This modular format means it is possible to combine several settings that adapt to the needs of the user, with a minimal number of different profiles.

Case study: creating settings for several offices

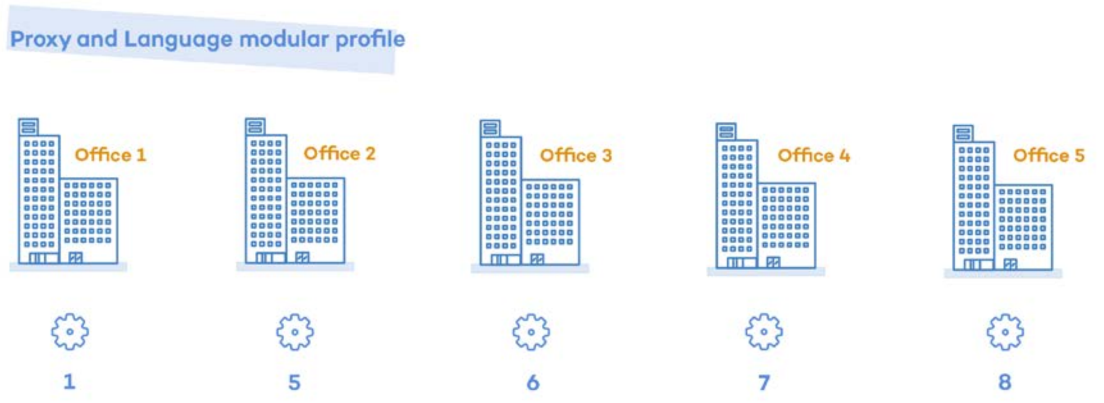
In this example, there is a company with five offices, each with a different communications infrastructure and therefore different proxy settings. Also, each office requires three different security settings, one for the Design department, another for the Accounts department and the other for Marketing.

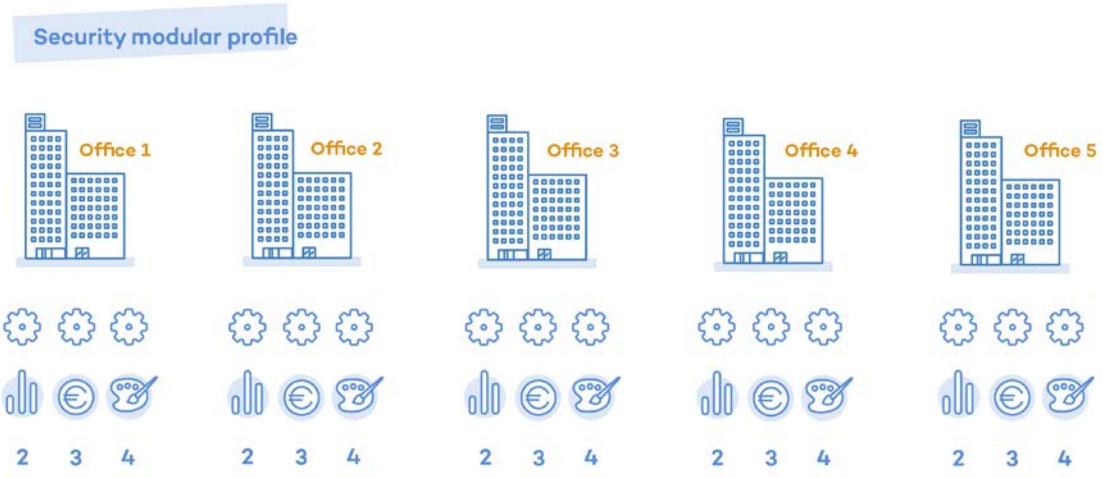


If **Panda Adaptive Defense 360** implemented all the configuration parameters in a single monolithic profile, the company would require 15 different settings profiles (5 x 3 =15) to adapt to the needs of all three departments in the company's offices.



However, as **Panda Adaptive Defense 360** 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.





8.5. Overview of the settings

Refer to chapters 9, 10 and 11 for more information about the Panda agent settings and the protections compatible with each supported platform

Proxy and language settings

These settings let you define the language of the agent installed on end users' computers and the proxy server used to connect to the Internet.

Per-computer settings

Let you define several settings pertaining to the Panda agent:

- Update frequency of the **Panda Adaptive Defense 360** software installed on computers. Refer to chapter 14 Software updates for more information.
- Password required to install the agent on end users' computers.
- Anti-Tamper protection.

Workstation and server

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

Android devices

This type of profile defines the security settings of Android devices (tablets and smartphones).

Sensitive data

These settings control how the **Panda Data Control** service will behave with respect to the detection and monitoring of the personally identifiable information (PII) stored in the unstructured data files found across the organization.

8.6. Creating and managing settings

Creating, copying and deleting settings is carried out by clicking **Settings** in the menu bar at the top of the screen. In the panel on the left there are five sections corresponding to the five types of available settings profiles **(1)**, **(2)**, **(3)** **(4)** **(5)** and **(6)**. In the right-hand panel, you can see the settings profiles of the selected category that have already been created **(9),** and the buttons for adding **(7)**, copying **(8)** and deleting profiles **(10).**

Creating settings

Click **Add** to display the window for creating settings. All profiles have a main name and a description, which are displayed in the list of settings.

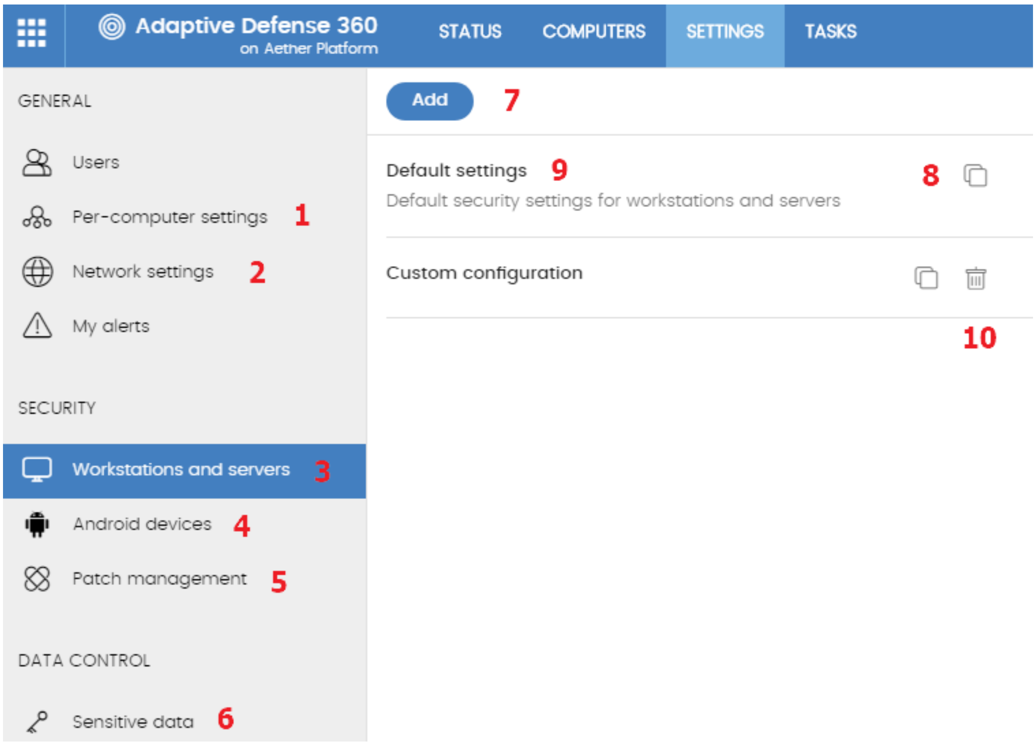


Figure 48: screen for creating and managing settings profiles

Copying and deleting settings

Use the icons **(8)** and **(10)** to copy and delete a settings profile, although if it has been assigned to one or more computers, you won't be able to delete it until it has been freed up. Click the settings profile in order to edit it.

Before editing a profile, check that the new settings are correct, as if the profile has already been assigned to your computers on the network, the changes will be applied automatically and immediately.

8.7. Manual and automatic assigning of settings to groups of computers

Once settings profiles have been created, they can be assigned to computers in two different ways:

- Manually (direct)
- Automatically through inheritance (indirectly)

These strategies complement each other and it is highly advisable that administrators understand the advantages and limitations of each one in order to define the most simple and flexible structure possible, in order to minimize the workload of daily maintenance tasks.

8.7.1 Assigning settings directly/manually

Manually assigning settings involves the administrator directly assigning profiles to computers or groups.

Once settings profiles have been created, there are three ways of assigning them:

- From the **Computers** option in the menu at the top of the screen, through the Groups tree shown in the panel on the left.
- From the computer details in the list of computers, also accessible from the **Computers** menu.
- From the profile itself when it is created or edited.

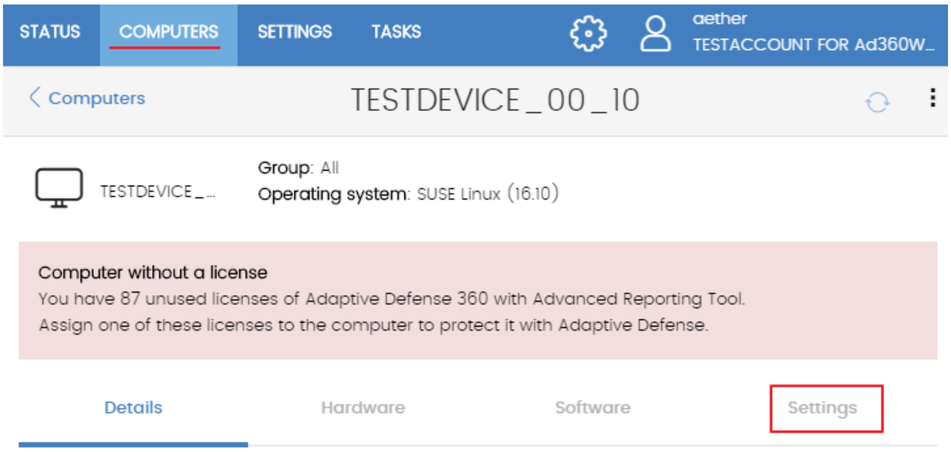
For more information about the Groups tree, see Chapter 7.

From the Groups tree

To assign a settings profile to the computers in a group, click the **Computers** menu at the top of the console, and select a group from the left-hand Groups tree. Then, follow the steps below:

- Click the group's context menu.
- Click **Settings**. A window will open with the profiles already assigned to the selected group and the type of assignment:
  - **Manual/Direct assignment:** the text will read **Directly assigned to this group.**
  - **Inherited/Indirect assignment**: the text will read **Settings inherited from**, followed by the name and full path of the group the settings were inherited from.
- Select the new settings and click **OK** to assign the settings to the group.
- The settings will immediately be deployed to all members of the group and sub-groups.
- The changes will immediately apply to all corresponding computers.

From the computer list panel



Group: All
Operating system: SUSE Linux (16.10)

Computer without a license
You have 87 unused licenses of Adaptive Defense 360 with Advanced Reporting Tool.
Assign one of these licenses to the computer to protect it with Adaptive Defense.

Figure 49: access to settings from the Computer details tab.

To assign a settings profile to a specific computer, follow the steps below:

- In the **Computers** menu, click the group or filter containing the computer to which you want to assign the settings. Click the computer in the list of computers in the right-hand panel to see the computer details screen.
- Click the **Settings** tab. This will display the profiles assigned to the computer and the type of assignment:
  - **Manual/Direct assignment:** the text will read **Directly assigned to this group.**
  - **Inherited/Indirect assignment**: the text will read **Settings inherited from**, followed by the name and full path of the group the settings were inherited from.
- Select the new settings. They will be applied automatically to the computer.

From the settings profile itself

The quickest way to assign a settings profile to several computers belonging to different groups is via the settings profile itself.

Follow the steps below to assign a settings profile to multiple computers or computer groups:

- Go to the **Settings** menu at the top of the console and select the type of settings that you want to assign from the left-hand side menu.
- Select a specific settings profile from those available, and click **Recipients**. A window will be displayed divided into two sections: **Computer groups** and **Additional computers**.
- Click the ⊕ button to add computers or computer groups to the settings profile.
- Click the **Add** button. The profile will be assigned to the selected computers and the new settings will be immediately applied.

> ***Removing a computer from the list of computers that will receive a settings profile will cause it to re-inherit the settings assigned to the group it belongs to. A warning message will be displayed before the computer is removed.***

8.7.2 Indirect assigning of settings: the two rules of inheritance

Indirect assigning of settings is applied through inheritance, which allows automatic deployment of a settings profile to all computers in the node to which the settings have been applied.

The rules that govern the relation between the two forms of assigning profiles (manual/direct and automatic/inheritance) are displayed below in order of priority:

1 **Automatic inheritance rule: a group or computers automatically inherits the settings of the parent group or one above it in the hierarchy.**

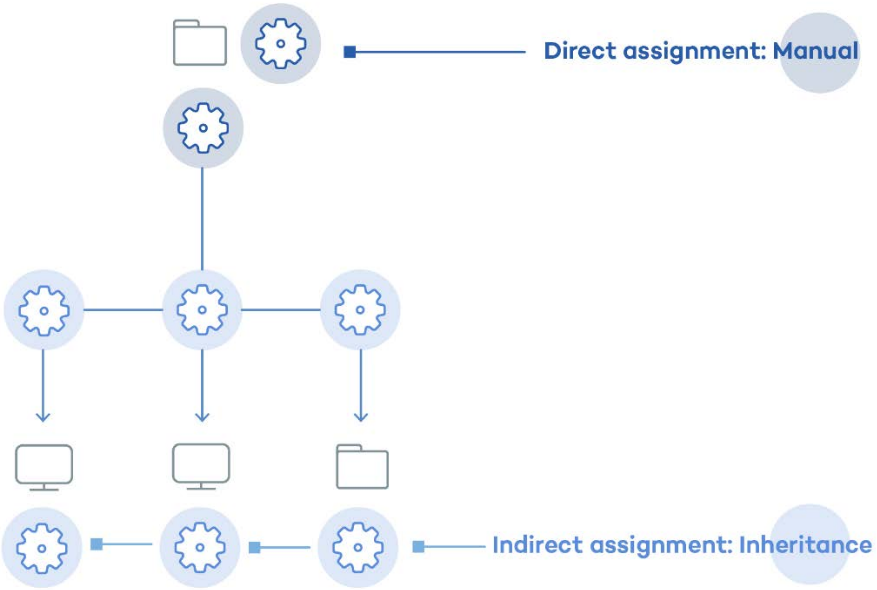


Figure 50: example of inheritance/indirect assigning. The parent group receives the settings that are then pushed out to the child nodes.

2 Manual priority rule: manually assigned profiles have priority over inherited ones.

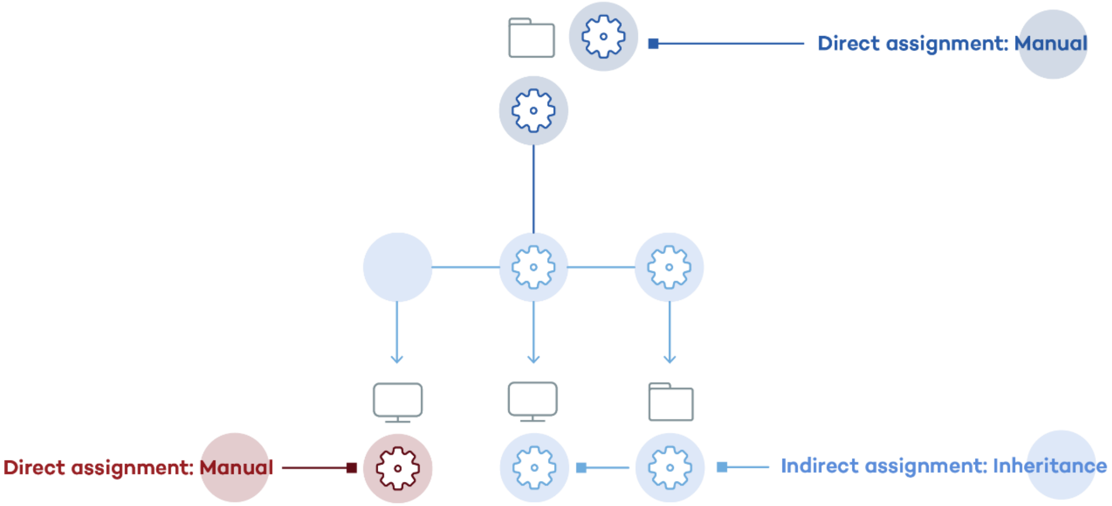

Direct assignment: Manual
Direct assignment: Manual
Indirect assignment: Inheritance

Figure 51: example of the priority of direct assigning over indirect. The inherited settings are overwritten with the manually assigned ones

8.7.3 Inheritance limits

The settings assigned to a group (manual or inherited) are applied to all branches of the tree, until manually assigned settings are found.

8.7.4 Overwriting settings

As illustrated in the previous point, rule 2 (manual priority) dictates that manually applied settings have preference over inherited settings. This is the case in a typical scenario where initially inherited settings are applied to the whole tree, and then some items have special manual settings applied.

However, it is often the case that once the inherited and manual settings have been applied, there may be a change to the inherited settings in a higher level node that affects the manual settings of items lower down.

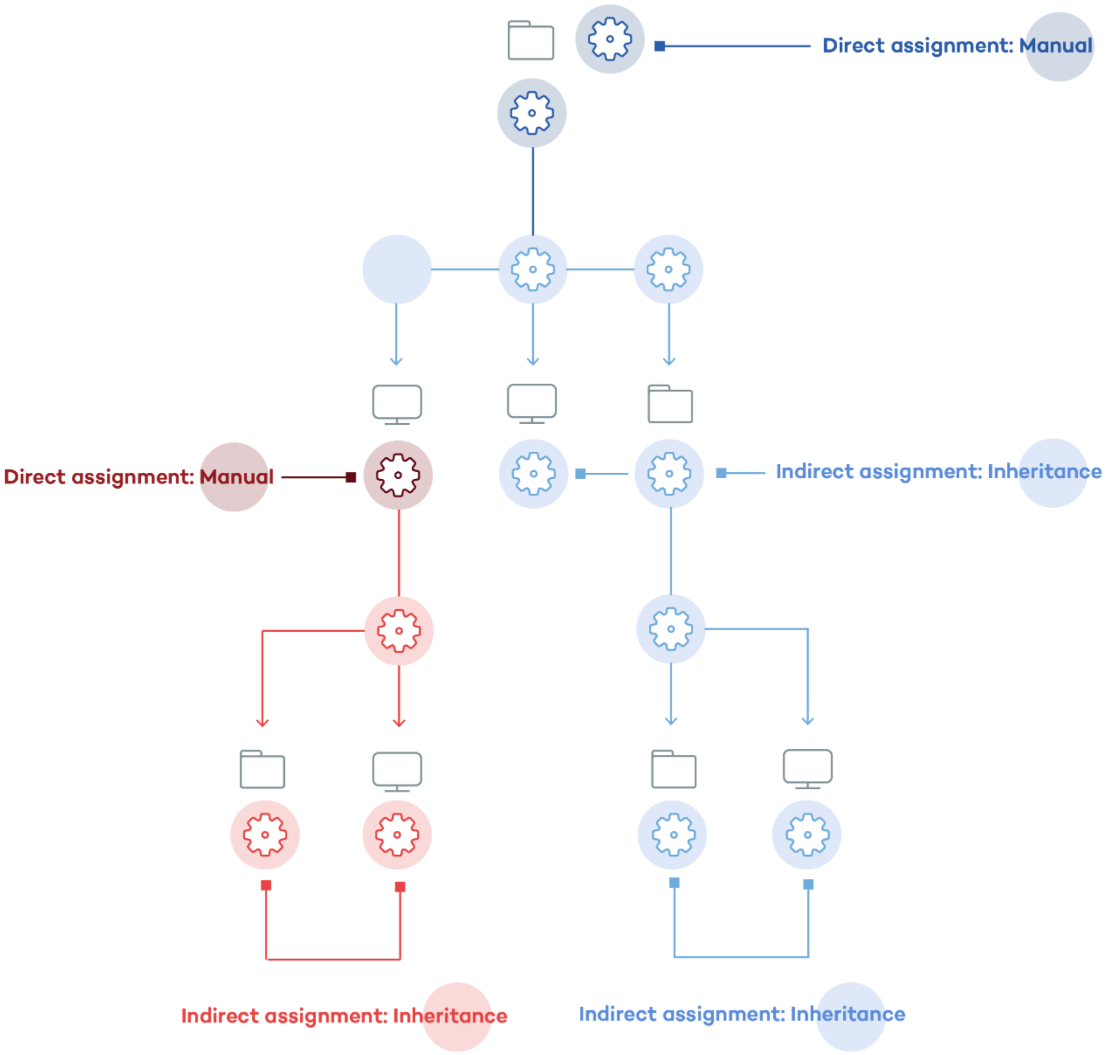

Direct assignment: Manual
Direct assignment: Manual
Indirect assignment: Inheritance
Indirect assignment: Inheritance
Indirect assignment: Inheritance

Figure 52: example of inheritance restricted by manual/direct assignment of settings. The parent node settings are passed on to the dependent branches of the tree but stop once manually assigned settings are found.

In this case, **Panda Adaptive Defense 360** asks the administrator if the previously set manual settings are to be kept or overwritten with the inheritance:

- If the inherited settings have priority, the new settings will be inherited by all subordinate items, regardless of whether there are manually assigned settings or not and deleting any manual settings.
- If the manual settings have priority, the new settings are only inherited in those groups where no manual settings have previously been assigned, and any manual settings are maintained.

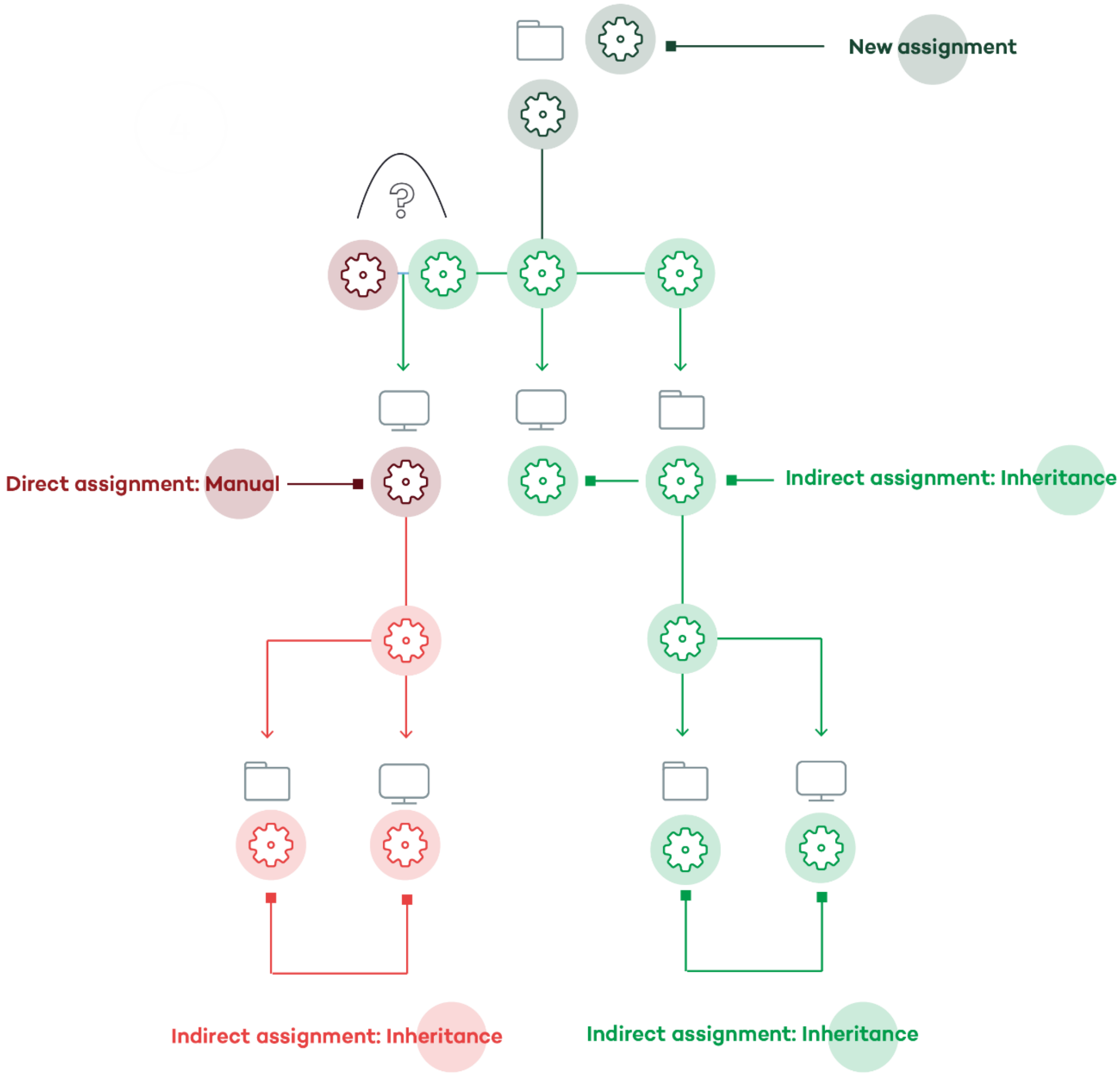
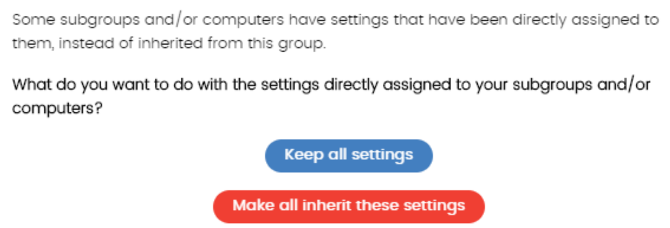

New assignment
Direct assignment: Manual
Indirect assignment: Inheritance
Indirect assignment: Inheritance
Indirect assignment: Inheritance

Figure 53: change to the inherited settings in a node that affects the manually applied settings of items lower down

This way, when the system detects a change to the settings that has to be applied to subordinate nodes, and one or more of them have manually assigned settings (regardless of the level), a screen appears asking the administrator which option to apply: **make all inherit these settings** or **Keep all settings**.



Some subgroups and/or computers have settings that have been directly assigned to them, instead of inherited from this group.

What do you want to do with the settings directly assigned to your subgroups and/or computers?

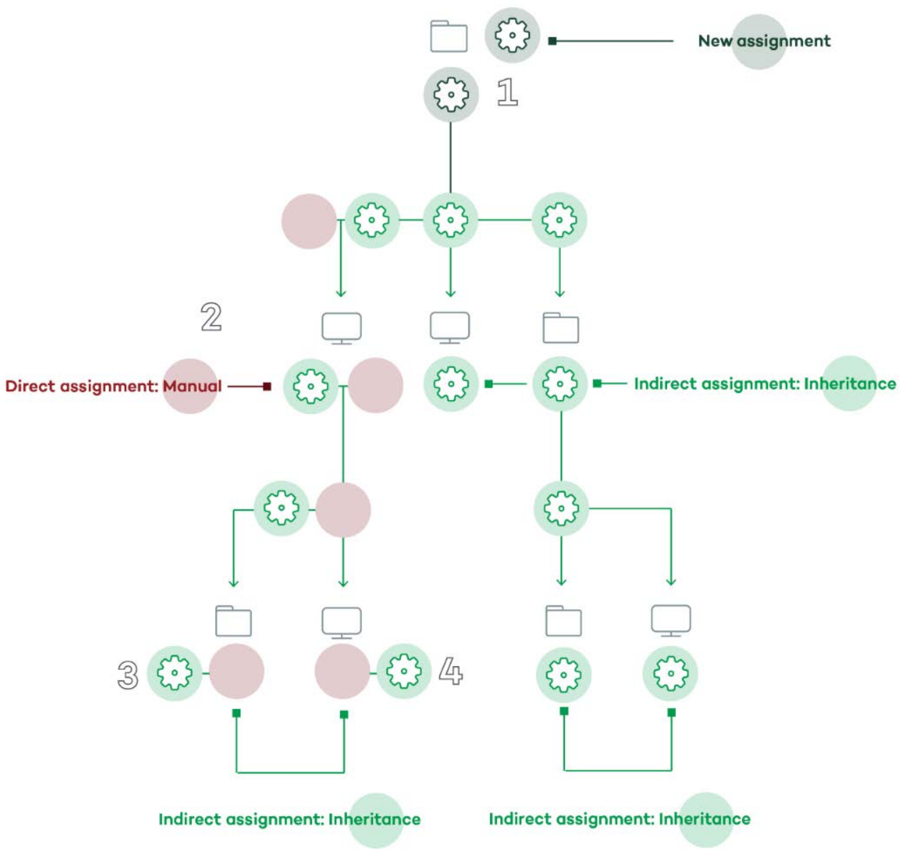
Figure 54: window for selecting the way that settings changes are applied to a branch containing groups configured manually

Make all inherit these settings

> ⚠ ***Be careful when choosing this option as it is not reversible! All manually applied settings below the node will be lost, and the inherited settings will be applied immediately to the computers. This could change the way Panda Adaptive Defense 360 works on many computers.***

The new manual settings **(1)** will be inherited by all nodes in the tree, overwriting any previous manual settings **(2)** all the way down to the lowest level children nodes: **(3)** and **(4)**.

Keep all settings



New assignment
1
2
Direct assignment: Manual
Indirect assignment: Inheritance
3
4
Indirect assignment: Inheritance
Indirect assignment: Inheritance

Figure 55: the manual settings are deleted and the settings inherited from the parent node are applied

If the administrator chooses **Keep all settings**, the new settings will only be applied to the subordinate nodes that don't have manually applied settings.

If you choose to keep the manually assigned settings, the propagation of the new inherited settings will stop at the first manually configured node. Although nodes subordinate to a manually configured node inherit its settings, implementation of the new settings stops at the first node in the tree that has the manual settings. In the figure, the implementation of the settings in **(1)** stops in node **(2)**, so that nodes **(3)** and **(4)** don't receive the new settings, even though inheritance is being used.

8.7.5 Deleting manually assigned settings and restoring inheritance

To delete manually assigned settings to a folder, and restore the settings inherited from a parent node, follow the steps below:

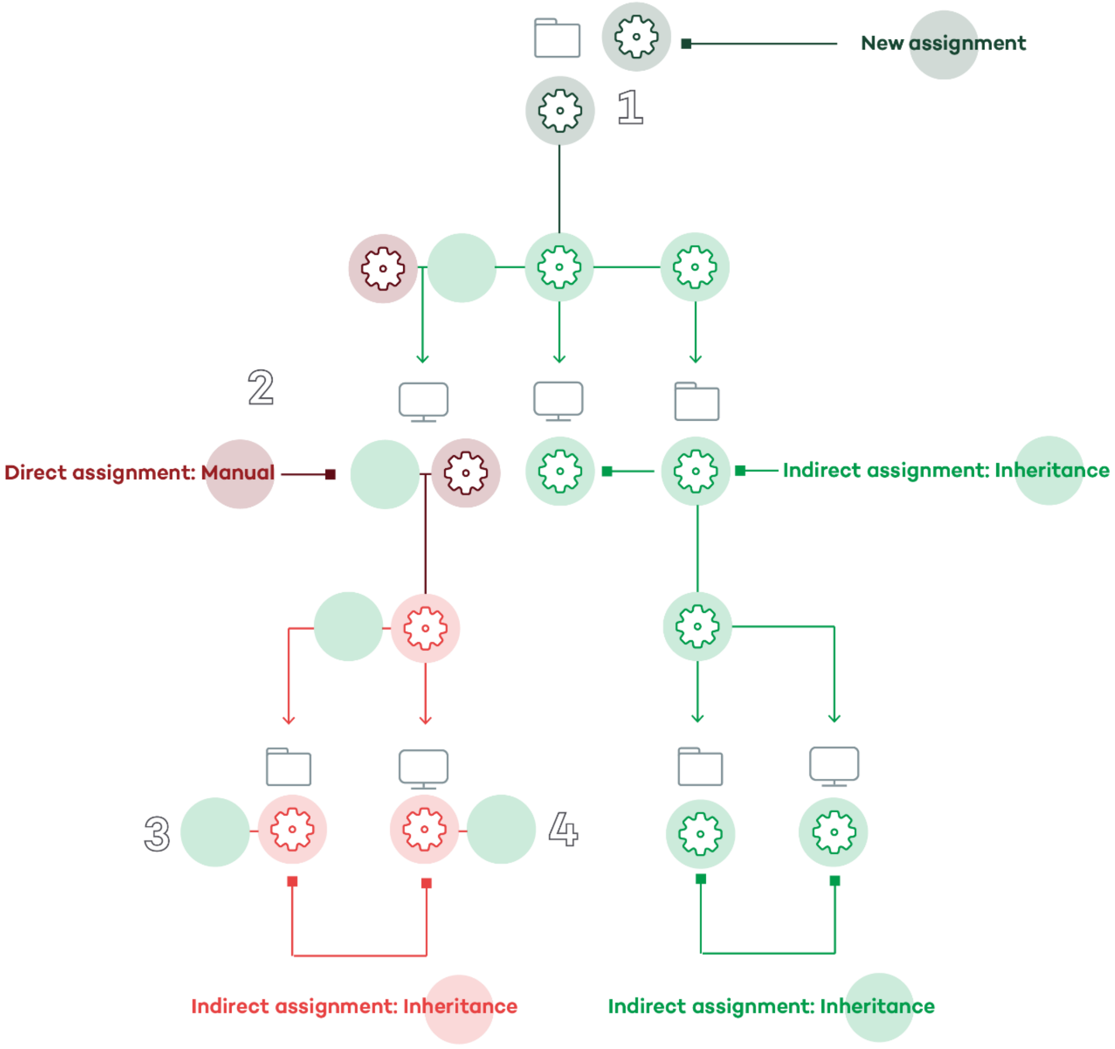

New assignment
1
2
Direct assignment: Manual
Indirect assignment: Inheritance
3
4
Indirect assignment: Inheritance
Indirect assignment: Inheritance

Figure 56: manually applied settings are maintained

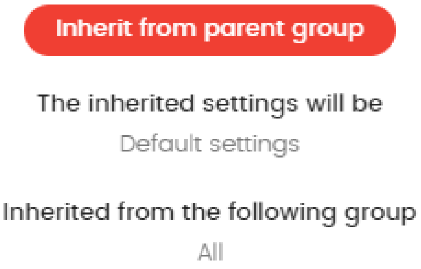
- In the **Computers** menu, click the group with the manually assigned settings to delete in the Groups tree in the panel on the left.
- Click the context menu icon and select **Settings**. A pop-up window will appear with the profiles assigned. Select the manually assigned profile you want to delete.
- A list will appear with all the available profiles that can be assigned manually. At the end of the list you will see the button **Inherit from parent group** along with the settings that will be inherited if you click the button, and the group from which they will be inherited.

8.7.6 Moving groups and computers

When you move a group or computer to another branch of the tree, the way **Panda Adaptive Defense 360** operates with respect to the settings to apply will vary depending on whether the items moved are complete groups or individual computers.

Moving individual computers

In the case of moving individual computers, **Panda Adaptive Defense 360** respects the manual settings that are established on the devices moved, and automatically overwrites the inherited settings with the settings established in the new parent group.



Inherit from parent group

The inherited settings will be

Default settings

Inherited from the following group

All

Figure 57: button for deleting manual settings and re-establishing inheritance

Moving groups

In the case of moving groups, Panda Adaptive Defense 360 displays a window with the question "Do you want the settings inherited by this computer to be replaced by those in the new group?".

- If you answer **YES**, the process will be the same as with moving computers: the manual settings will be respected and the inherited settings overwritten with those established in the parent node.
- If the answer is **NO**, the manual settings will also be respected but the original inherited settings of the moved group will have priority and as such will become manual settings.

8.8. Viewing the assigned settings

The management console offers four methods of displaying the settings profiles assigned to a group or computer:

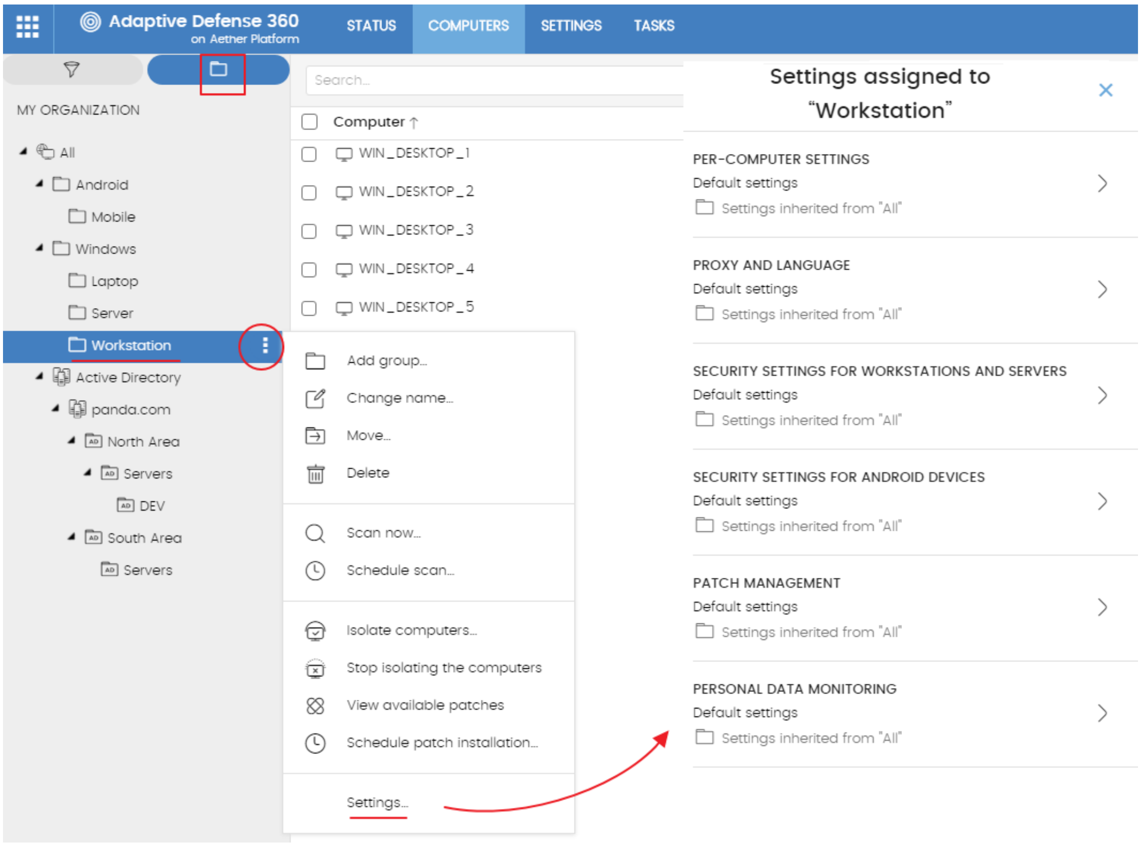
- From the Groups tree
- From the Settings lists
- From the computer's **Settings** tab
- From the exported list of computers

From the groups tree

To view the settings assigned to a group, click the context menu of the relevant branch in the Groups tree, and select **Settings** in the pop-up menu displayed.

Below is a description of the information displayed in this window:

- **Type of settings**:
  - Proxy and language settings
  - Per-computer settings
  - Security settings for workstations and servers
  - Security settings for Android devices
  - Personal data monitoring settings



Settings assigned to "Workstation"

PER-COMPUTER SETTINGS
Default settings
Settings inherited from "All"

PROXY AND LANGUAGE
Default settings
Settings inherited from "All"

SECURITY SETTINGS FOR WORKSTATIONS AND SERVERS
Default settings
Settings inherited from "All"

SECURITY SETTINGS FOR ANDROID DEVICES
Default settings
Settings inherited from "All"

PATCH MANAGEMENT
Default settings
Settings inherited from "All"

PERSONAL DATA MONITORING
Default settings
Settings inherited from "All"

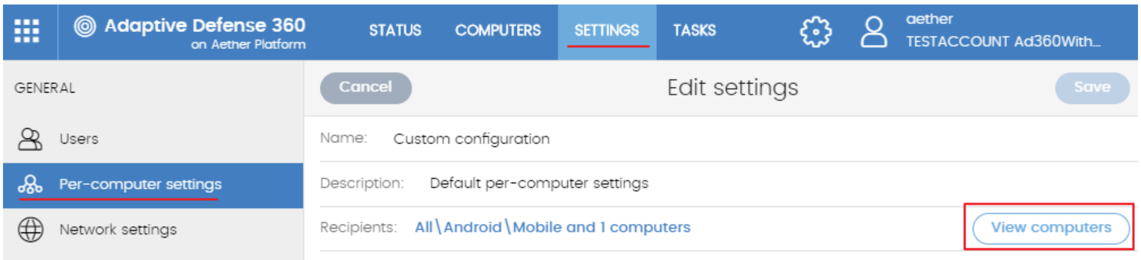
Figure 58: settings assigned from the Groups tree

- **Name of the settings**: name given by the administrator when creating the settings.
- **Inheritance type**
  - **Settings inherited from…:** 🗀 The settings were assigned to the specified parent folder. Every computer on the branch inherits them.
  - **Directly assigned to this group**: → The settings applied to the computers are those that the administrator assigned to the folder manually.

From the Settings menu

To view the computers and computer groups assigned to a specific settings profile, follow the steps below:

- Go to the **Settings** menu at the top of the console and select the relevant type of settings from the left-hand side menu.
- Select the relevant settings profile from those available.
- If the settings profile has been assigned to one or more computers or groups, the **View computers** button will be displayed.



Name: Custom configuration

Description: Default per-computer settings

Recipients: All \ Android \ Mobile and 1 computers

Figure 59: viewing the list of computers assigned to a settings profile

From the computer's Settings tab

In the **Computers** menu, when you select a computer from the panel on the right, you will see the details screen. The **Settings** tab will display the list of profiles assigned to the computer.

Exporting the list of computers

From the Computers tree (Groups tree or Filters tree), you can export the list of computers to CSV format by clicking the context menu and selecting **Export**.

Refer to chapter 7 for a full description of all fields included in the exported CSV file.

9. Agent and local protection settings

Agent roles
Internet access via proxy server
Real-time communication
Languages
Anti-Tamper protection and password

9.1. Introduction

Administrators can configure several aspects of the Panda agent installed on the computers on their network:

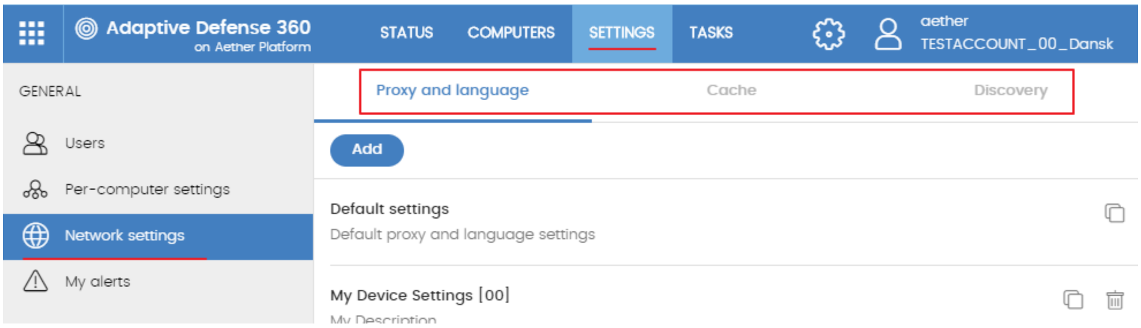
- Define a computer's role towards the other protected workstations and servers.
- Protect the **Panda Adaptive Defense 360** software from unauthorized tampering by hackers and advanced threats (APTs).
- Configure the communication established between the computers on the network and the Panda Security cloud.

9.2. Configuring the Panda agent role

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

- Proxy
- Discovery computer
- Cache

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



Default settings
Default proxy and language settings

My Device Settings [00]
My Description

Figure 60: access to the role settings window

9.2.1 Proxy role

Panda Adaptive Defense 360 allows computers without direct Internet access to use the proxy server installed on the network. If no proxy is accessible, you can assign the proxy role to a computer with **Panda Adaptive Defense 360** installed.

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

Configuring a computer as a proxy server

- Click the **Proxy and language** tab. Select an existing **Proxy and language** settings profile or create a new one.
- Expand the **Proxy** section and select **Panda Adaptive Defense 360 proxy.**
- Click **Select computer...**
- In the computer selection window, click **Add proxy server**. A list will be displayed with all managed computers that haven't been designated as proxy server yet.
- Select the computers that will act as a proxy server for all other workstations and servers protected by **Panda Adaptive Defense 360.**

Revoking the proxy role

- Click the **Proxy and language** tab. Select an existing **Proxy and language** settings profile or create a new one.
- Expand the **Proxy** section and select **Panda Adaptive Defense 360 proxy.**
- Click **Select computer...**
- Click the 🗑 icon of the computer that you want to stop acting as a proxy.

9.2.2 Cache/repository role

Panda Adaptive Defense 360 lets you assign the cache role to one or more computers on your network. These computers will automatically download and store all files required so that other computers with **Panda Adaptive Defense 360** installed can update their signature file, agent and protection engine without having to access the Internet. This saves bandwidth as it won't be necessary for each computer to separately download the updates they need. All updates are downloaded centrally for all computers on the network.

Configuring a computer as a cache

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the menu on the left and select the **Cache** tab.
- Click **Add cache computer**.
- Use the search tool at the top of the screen to quickly find those computers you want to designate as cache.
- Select one of more computers from the list and click **OK**.

From then on, the selected computer will have the cache role and will start downloading all necessary files, keeping its repository automatically synchronized. All other computers on the same subnet will contact the cache computer for updates.

Revoking the cache role

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Cache** tab.
- Click the 🗑 icon of the computer that you want to stop acting as a cache.

Requirements and limitations of computers with the cache role

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

It is advisable to designate a computer with the cache role in each network segment on the corporate network

- All other computers will automatically discover the presence of the cache node and will redirect their update requests to it.
- A protection license has to be assigned to the cache node in order for it to operate.
- The firewall must be configured to allow incoming and outgoing UPnP/SSDP traffic on UDP port 21226 and TCP port 3128.

Discovery of cache nodes

Computers designated with the cache role broadcast their status to the network segments to which their interfaces connect. All other computers will receive the relevant notification and will connect to the most appropriate node based on the amount of free resources should there be more than one designated cache node on the same network segment.

In addition, network computers will occasionally ask if there is any node with the cache role.

Cache node capacity

The capacity of a cache node is determined by the number of simultaneous connections it can accommodate in high load conditions and by the type of traffic managed (signature file downloads, installer downloads, etc.). Approximately, a computer with the cache role assigned can serve around 1,000 computers simultaneously.

9.2.3 Discovery computer role

The **Discovery** tab is directly related to the installation and deployment of **Panda Adaptive Defense 360** across the customer's network. Refer to chapter 6 Installing the Panda Adaptive Defense 360 software **Error! Reference source not found.**for more information about the **Panda Adaptive Defense 360** discovery and installation processes**.**

9.3. Configuring Internet access via a proxy server

Configuring proxy usage

To configure the way one or more computers connect to the Internet via a proxy server, you must create a **Proxy and language** settings profile. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Proxy and language** tab.
- Select an existing **Proxy and language** settings profile or create a new one.
- In the **Proxy** section, choose the type of proxy to use.
  - **Do not use proxy**: direct access to the Internet.
  - **Corporate proxy**: access to the Internet via a proxy installed on the company's network.
  - **Panda Adaptive Defense 360 proxy:** access via the **Panda Adaptive Defense 360** agent installed on a computer on the network.

- **Do not use proxy**

Computers without a proxy configured directly access the Panda Security cloud to download updates and send status reports. The **Panda Adaptive Defense 360** software communicates with the Internet using the computer settings.

- **Corporate proxy**

- **Address**: IP address of the proxy server.
- **Port**: proxy server port.
- **Proxy requires authentication**: enable it if the proxy requires a user name and password.
- **User name**
- **Password**

- **Panda Adaptive Defense 360 proxy**

This lets you centralize all network communications through a computer with the Panda agent installed.

To configure the sending of data via a **Panda Adaptive Defense 360** proxy, click the link **Select computer** to display a list of the available computers that have the proxy role on the network.

UDP port 21226 and TCP port 3128 on computers designated as a Panda Adaptive Defense 360 proxy cannot be used by other applications. Additionally, the computer's firewall must be configured to allow incoming and outgoing traffic on both ports.

Fallback mechanism

When a Panda agent cannot connect to the **Aether** platform, the following fallback logic is applied to restore the connection via other means:

- If the Internet connection is configured via corporate proxy or **Panda Adaptive Defense 360** proxy and there is no response, an attempt is made to connect directly.
- Internet Explorer: the Panda agent tries to recover the Internet Explorer proxy settings with the profile of the user logged in to the computer.
  - If the configuration of the proxy credentials is defined explicitly, this method can't be used.
  - If the Internet Explorer proxy settings use PAC (Proxy Auto-Config) the URL is obtained from the settings file, provided that the protocol is HTTP or HTTPS
- WinHTTP / WinInet: the default proxy settings are read.
- WPAD (Web Proxy Auto-discovery Protocol): a request is sent to the network via DNS or DHCP to get the URL that points to the PAC settings file.

9.4. Configuring real-time communication

Real-time communication between your protected computers and the **Panda Adaptive Defense 360** server requires that each computer have an open connection at all times. However, in those organizations where the number of open connections may have a negative impact on the performance of the installed proxy, it may be advisable to disable real-time communication. The same applies to those organizations where the traffic generated when simultaneously deploying configuration changes to a large number of computers may impact bandwidth usage.

Isolated workstations and servers cannot communicate in real time with the Panda Security cloud via a computer with the Panda Adaptive Defense 360 proxy role assigned. These communications will be established through the ordinary procedure. This limitation doesn't affect computers using a corporate proxy to access the Internet.

Disabling real-time communication

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Proxy and language** tab.
- Select an existing **Proxy and language** settings profile or create a new one.
- In the **Proxy** section, click the **Advanced options** link.
- Clear the **Enable real-time communication** checkbox.

If you disable real-time communication, your computers will communicate with the **Panda Adaptive Defense 360** server every 15 minutes.

9.5. Configuring the agent language

To set up the language of the Panda agent for one or more computers, create a **Proxy and language** settings profile. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Proxy and language** tab.
- Select an existing **Proxy and language** settings profile or create a new one.
- Select a language from the list:
    - English
    - Spanish
    - Swedish
    - French
    - Italian
    - German
    - Portuguese
    - Hungarian
    - Russian
    - Japanese
    - Finnish (local console)

If the language is changed while the Panda Adaptive Defense 360 local console is open, the system will prompt the user to restart the console. This process does not affect the security of the computer.

9.6. Configuring the Anti-Tamper protection and password

9.6.1 Anti-Tamper protection

Many advanced threats and hackers take advantage of sophisticated techniques to disable the security software installed on computers and bypass protection features. To stop that, **Panda Adaptive Defense 360** incorporates anti-tamper technologies that prevent unauthorized tampering of the solution.

Enabling the Anti-Tamper protection

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Expand section **Security against unauthorized protection tampering:**
  - **Enable Anti-Tamper protection (prevents users and certain types of malware from stopping the protections).** Enabling this option requires setting up a password, which will be required if, for example, the administrator or a support team member needs to temporary disable the protection from the local computer in order to diagnose a problem.

9.6.2 Password-protection of the agent

Administrators can set up a password to prevent users from changing the protection features or completely uninstalling the **Panda Adaptive Defense 360** software from their computer.

Setting up the password

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Expand section **Security against unauthorized protection tampering:**
  - **Request password to uninstall Aether from computers**: this is to prevent users from uninstalling the **Panda Adaptive Defense 360** software.
  - **Allow the protections to be temporarily enabled/disabled from the computers' local console**: this allows administrators to manage a computer’s security from its local console. Enabling this option requires setting up a password.

10. Security settings for workstations and servers

10.1. Introduction

Panda Adaptive Defense 360's **Settings** menu provides access to the parameters required to configure the security settings for workstations and servers. Click the **Workstations and servers** section from the left-hand menu to display a list of the security configurations already created.

This chapter describes the available parameters to configure the security settings for workstations and servers. It also includes practical recommendations on how to protect all computers on your network, without negatively impacting users' activities.

10.2. Introduction to the security settings for workstations and servers

The parameters for configuring the security of workstations and servers are divided into nine sections. Clicking each section displays a drop-down panel with the associated options. Below we offer a brief explanation of each section:

Feature	Windows	macOS	Linux	Windows Exchange
Advanced Protection	X			
Anti-Exploit Protection	X			
Antivirus	X	X	X	X
Firewall & IDS	X			
Email Protection	X			
Web Protection	X	X	X	
Device Control	X			
Web Access Control	X	X	X	
Anti-Spam				X
Content Filtering				X

Table 12: security features per platform

- **General**: lets you configure the updates, the removal of competitor products, and file exclusions from scans.
- **Advanced protection (Windows devices):** lets you configure the behavior of the advanced protection and the anti-exploit protection against APTs, targeted attacks, and advanced malware capable of leveraging known and zero-day exploits.
- **Antivirus**: lets you configure the general parameters that control the traditional anti-malware protection against viruses and threats.
- **Firewall (Windows devices):** lets you configure the general parameters that control the firewall and IDS against network attacks.

- **Device Control (Windows devices):** lets you configure the general parameters that control user access to the peripheral devices connected to their computers.
- **Web Access Control**: lets you restrict access to certain Web content categories.
- **Antivirus for Exchange servers**: scans the inbound and outbound email that goes through your Exchange mail servers, searching for threats.
- **Anti-Spam for Exchange servers**: scans the inbound and outbound email that goes through your Exchange mail servers, searching for unwanted email.
- **Content Filtering for Exchange servers**: restricts the content types that can reach your Exchange servers.

10.3. General settings

The general settings let you configure how **Panda Adaptive Defense 360** behaves regarding updates, the removal of competitor products, and file and folder exclusions from the scans performed by the traditional antivirus.

10.3.1 Updates

Refer to chapter 14 Software updates for more information about how to update the agent, the protection, and the software signature file installed on users' computers.

10.3.2 Uninstall other security products

Refer to chapter 6 Installing the Panda Adaptive Defense 360 software for more information about what to do with competitor products when installing **Panda Adaptive Defense 360**.

> ***Refer to Appendix 3: list of uninstallers for a list of the competitor products that Panda Adaptive Defense 360 can automatically uninstall from users' computers.***

10.3.3 Exclusions

> ***These settings affect both the antivirus protection and the advanced protection.***

The **Exclusions** section lets you select items that won't be scanned for malware. Excluding a file with an .EXE or .COM extension will allow the execution of both the program and its libraries and binary files on all computers (unless they are known threats). Nevertheless, these programs and libraries will continue to be monitored by **Panda Adaptive Defense 360** in order to determine whether they are malware or goodware.

Disk files

Lets you select the files on the hard disk of protected computers that won't be scanned by **Panda Adaptive Defense 360.**

- **Extensions**: lets you specify file extensions that won't be scanned.
- **Folders**: lets you specify folders whose content won't be scanned.
- **Files**: lets you indicate specific files that won't be scanned.
- **Recommended exclusions for Exchange servers**: click **Add** to automatically load a series of Microsoft-recommended exclusions to optimize the performance of **Panda Adaptive Defense 360** on Exchange servers.

Exclude the following email attachments:

Lets you specify the extensions of email file attachments that **Panda Adaptive Defense 360** won't scan.

10.4. Advanced protection (Windows computers)

10.4.1 Behavior

This section lets you choose from different operational modes to block unknown malware and protect your network against APTs and advanced threats.

- **Advanced protection**: lets you enable/disable the protection engine against advanced threats, specific of **Panda Adaptive Defense 360.**
- **Operational mode**:
  - **Audit**: in audit mode, **Panda Adaptive Defense 360** only reports on detected threats but doesn’t block or disinfect the malware detected.
  - **Hardening**: allows the execution of the unknown programs already installed on users' computers. However, unknown programs coming from external sources (Internet, email, etc.) will be blocked until they are classified. Programs classified as malware will be disinfected or deleted.
  - **Lock**: prevents the execution of all programs classified as malware as well as all unknown programs that are pending classification.

10.4.2 Anti-exploit

The anti-exploit protection blocks, automatically and without user intervention in most cases, all attempts to exploit the vulnerabilities found in the processes running on users' computers.

How does the anti-exploit protection work?

Network computers may contain processes with programming bugs. These processes are known as 'vulnerable processes' and, despite being completely legitimate, sometimes they don't correctly interpret certain data sequences received from external sources.

When a vulnerable process receives inputs maliciously crafted by hackers, there can be an internal malfunction that allows the attacker to inject fragments of malicious code into the memory areas managed by the vulnerable process. This process becomes then 'compromised'.

The injected code can cause the compromised process to execute actions that it wasn't programmed for, and which compromise the computer security. **Panda Adaptive Defense 360**'s anti-exploit protection detects all attempts to inject malicious code into the vulnerable processes run by users.

Panda Adaptive Defense 360 neutralizes exploits in two different ways depending on the exploit detected:

- **Automatic exploit blocking**

In this case, **Panda Adaptive Defense 360** detects the injection attempt while it is still in progress. The injection process hasn't been completed yet, therefore, the target process is not yet compromised and there is no risk for the computer. The exploit is neutralized without the need to end the affected process or restart the computer. There are no data leaks from the affected process.

The user of the target computer will receive a notification depending on the settings established by the administrator.

- **Exploit detection**

In this case, **Panda Adaptive Defense 360** detects the code injection when it has already taken place. Since the malicious code is already inside the vulnerable process, it is necessary to end it before it performs actions that may put the computer's security at risk.

Regardless of the time elapsed between when the exploit was detected and when the compromised process is ended, **Panda Adaptive Defense 360** will indicate that the computer was at risk, although, obviously, the risk will actually depend on the time that passed until the process was stopped and on the malware itself.

Panda Adaptive Defense 360 can end a compromised process automatically to minimize the negative effects of an attack, or ask the user for permission to do so in order to remove it from memory. This will allow the user to, for example, save their work or critical information before the compromised process is terminated or their computer is restarted.

In those cases where it is not possible to end a compromised process, the user will be asked for permission to restart their computer.

Anti-exploit protection settings

- **Anti-exploit:** enables the anti-exploit protection
  - **Audit**: select this option if you want **Panda Adaptive Defense 360** to report exploit detections in the Web console, without taking any action against them or displaying any information to the computer user upon detection. These notifications will be emailed to the administrator as well, based on the email alert settings configured in the console.
  - **Block**: select this option if you want **Panda Adaptive Defense 360** to block exploit attacks. In some cases it may be necessary to end the compromised process or restart the computer.
    - **Report blocking to the computer user:** the user will receive a notification, and the compromised process will be automatically ended if required.
    - **Ask the user for permission to end a compromised process**: the user will be asked for permission to end the compromised process should it be necessary. This will allow the user to, for example, save their work or critical information before the compromised process is stopped. Additionally, every time a computer needs to be restarted, the user will be asked for confirmation, regardless of whether the option **Ask the user for permission to end a compromised process** is selected or not.

Given that many exploits continue to run malicious code while in memory, an exploit won't appear as resolved in the Malicious programs and exploits panel of the Web console until the relevant process is ended

10.4.3 Privacy

Panda Adaptive Defense 360 can display the full name and path of the files sent to the cloud for analysis in its reports and forensic analysis tools. If you don't want this information to be sent to Panda Security's cloud, clear the relevant checkbox in the **Privacy** tab.

Additionally, **Panda Adaptive Defense 360** can also show the user that was logged in on the computer where a detection took place. If you don't want this information to be sent to Panda Security's cloud, clear the relevant checkbox in the **Privacy** tab.

10.4.4 Network usage

Every executable file found on users' computers that is unknown to **Panda Adaptive Defense 360** will be sent to Panda Security's cloud for analysis. This behavior is configured so that it has no impact on the performance of the customer's network (the maximum number of MB that can be transferred in an hour per agent is set by default to 50). Unknown files are sent only once for all customers using **Panda Adaptive Defense 360**. Additionally, bandwidth management mechanisms have been implemented in order to minimize the impact on the customer's network.

To configure the maximum number of MB that an agent can send per hour, enter the relevant value and click **OK**. To establish unlimited transfers, set the value to 0.

10.5. Antivirus

This section lets you configure the general behavior of the signature-based antivirus engine.

- **File protection**: enable/disable the antivirus protection for the file system.
- **Email protection:** enable/disable the antivirus protection for the mail client installed on users' computers.
- **Web browsing protection** Enable/disable the antivirus protection for the Web client installed on users' computers.

The action taken by **Panda Adaptive Defense 360** when finding a malware or suspicious file is defined by Panda Security's anti-malware laboratory, and is based on the following criteria:

- **Files identified as malware if disinfection is possible**: they are disinfected. The original file is deleted and replaced with a harmless, disinfected copy.
- **Files identified as malware when disinfection is not possible**: if disinfection is not possible, the solution makes a backup copy of the infected file and the original file is deleted.

10.5.1 Threats to detect

Lets you configure the types of threats that **Panda Adaptive Defense 360** will search for and remove from the file system, mail client and Web client installed on users' computers.

- **Detect viruses**
- **Detect hacking tools and PUPs**
- **Block malicious actions**: enables a set of anti-exploit technologies that scan the behavior of local processes, looking for suspicious activity.
- **Detect phishing**

10.5.2 File types

This section lets you specify the types of files to be scanned by **Panda Adaptive Defense 360**:

- **Scan compressed files on disk**
- **Scan compressed files in emails**
- **Scan all files regardless of their extension when they are created or modified (Not recommended):** to enhance efficiency and performance, we recommend that you don't scan all types of files as many types of data files actually don't pose a threat to the security of the network.

10.6. Firewall (Windows devices)

Panda Adaptive Defense 360 provides three basic tools to filter the network traffic that protected computers send and receive:

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

10.6.1 Operational mode

There are two operational modes for the firewall, which can be defined through the **Let computer users configure the firewall** option:

- **Enabled** (user-mode or self-managed firewall): this option allows end users to manage the firewall protection from the local console installed on their computers.
- **Disabled** (administrator-mode firewall): the administrator configures the firewall protection of every computer on the network through configuration profiles.

10.6.2 Network type

Laptops and mobile devices can connect to networks with different security levels, from public Wi-Fi networks, such as those in Internet cafés, to managed and limited-access networks, such as those found in companies. To set the firewall's default behavior, the network administrator must select the type of network that the computers in the configured profile usually connect to.

- **Public network**: these are the networks found in Internet cafés, airports, etc. They have limitations on the way protected computers are used and accessed, especially with regard to file, resource and directory sharing.
- **Trusted network**: these are office and home networks. Your computer is perfectly visible to the other computers on the network. Additionally, there are no limitations on sharing files, resources or directories.

Panda Adaptive Defense 360 will behave differently and will apply different predetermined rules depending on the type of network. You can view these predetermined rules **(Panda rules)** in the **Program rules** and **Connection rules** sections.

10.6.3 Program rules

This section lets you configure which programs can communicate with the local network/Internet, and which cannot.

To build an effective protection strategy it is necessary to follow the steps below in the order listed:

1 Set the default action

- **Allow:** implements a permissive strategy based on always accepting connections for all programs for which you haven't configured a specific rule in step 3. This is the default, basic mode.

- **Deny**: implements a restrictive strategy based on always denying connections for all programs for which you haven't configured a specific rule in step 3. This is an advanced mode, as it requires adding rules for every frequently used program. Otherwise, those programs will not be allowed to communicate, affecting their performance.

2 Enable Panda's rules

Enables Panda Security's predefined rules for the selected network type.

3 Add rules to define the specific behavior of your applications

Change the order of the program rules, add, edit or remove them by using the Up **(1)**, Down **(2)**, Add **(3)**, Edit **(4)** and Delete **(5)** buttons on the right. The checkboxes **(6)** will let you select the rules to apply each action to.

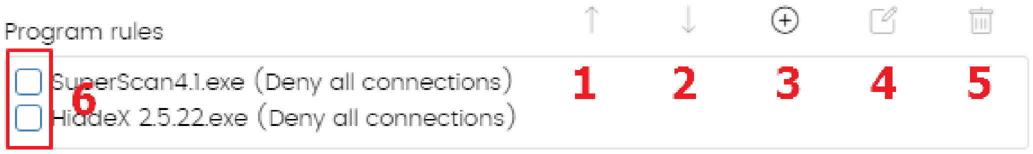

Program rules
□ SuperScan4.1.exe (Deny all connections)
□ HiddeX 2.5.22.exe (Deny all connections)
1
2
3
4
5
6

Figure 61: edit controls for program rules

The following fields are mandatory when you are creating a rule:

- **Description**
- **Program**: lets you select the program whose behavior you want to control.
- **Connections allowed for this program:**
  - **Allow inbound and outbound connections**: the program can connect to the Internet/local network and allows other programs or users to connect to it. There are certain types of programs that need these permissions to work correctly: file sharing programs, chat applications, Internet browsers, etc.
  - **Allow outbound connections**: the program can connect to the Internet/local network, but won't accept inbound connections from other users or applications.
  - **Allow inbound connections**: the program accepts connections from programs or users from the Internet/local network, but won't be allowed to establish outbound connections.
  - **Deny all connections**: the program cannot connect to the Internet or local networks.
  - **Advanced permissions**:
    - **Action**: defines the action that **Panda Adaptive Defense 360** will take if the examined traffic matches the rule.
      - **Allow**: allows the traffic.
      - **Deny**: blocks the traffic. It drops the connection.
    - **Direction**: sets the traffic direction for connection protocols such as TCP.
      - **Outbound**: traffic from the user's computer to another computer on the network.

  - **Inbound**: traffic to the user's computer from another computer on the network.
- **Zone**
- **Protocol**: Lets you establish the layer 3 protocol for the traffic generated by the program you want to control.
  - **All**
  - **TCP**
  - **UDP**
- **IPs**:
  - **All**: the rule doesn't take into account the connection's source and destination IP addresses.
  - **Custom**: lets you specify the source and destination IP addresses of the traffic to control. You can enter multiple addresses separated by commas (,). To specify a range, use a hyphen (-).
- **Ports**: lets you specify the communication port. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).

10.6.4 Connection rules

This section lets you define traditional TCP/IP traffic filtering rules. **Panda Adaptive Defense 360** compares the value of certain fields in the headers of each packet sent and received by the protected computers, and checks it against the rules entered by the administrator. If the traffic matches any of the rules, the associated action is taken.

Connection rules affect the entire system (regardless of the process that manages them). They have priority over the program rules that govern the connection of your programs to the Internet/local network.

To build an effective strategy to protect the network against dangerous and unwanted traffic, it is necessary to follow the steps below in the order listed:

1 Specify the firewall's default action in the Program rules section

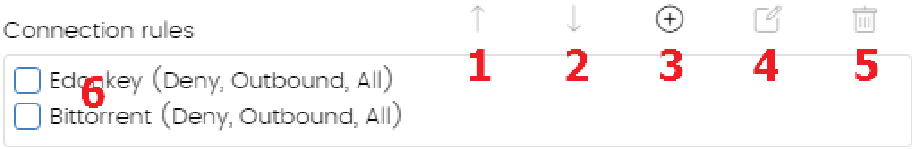
- **Allow:** implements a permissive strategy based on always accepting all connections for which you haven't configured a specific rule in step 3.
  This is the default, basic mode: all connections for which there is not an existing rule will be automatically accepted.
- **Deny**: implements a restrictive strategy based on always denying all connections for which you haven't configured a specific rule in step 3. This is an advanced mode: all connections for which there is not an existing rule will be automatically denied.

2 Enable Panda's rules

Enables Panda Security's predefined rules for the selected network type.

3 Add rules that describe specific connections along with the associated action

Change the order of the connection rules, add, edit or remove them by using the Up **(1)**, Down **(2)**, Add **(3)**, Edit **(4)** and Delete **(5)** buttons on the right. The checkboxes **(6)** will let you select the rules to apply each action to.



Connection rules

□ Edonkey (Deny, Outbound, All)
□ Bittorrent (Deny, Outbound, All)

Figure 62: edit controls for connection rules

The order of the rules on the list is important. They are applied in descending order, therefore, if you change the position of a rule, you will also change its priority.

Next, we describe the fields found in a connection rule:

- **Name**
- **Description**
- **Action**: indicates the action that **Panda Adaptive Defense 360** will take if the examined traffic matches the rule.
  - **Allow**: allows the traffic.
  - **Deny**: blocks the traffic. It drops the connection.
- **Direction**: specifies the direction of the traffic for connection protocols such as TCP.
  - **Outbound**: outbound traffic.
  - **Inbound**: inbound traffic.
- **Zone**
- **Protocol**: lets you specify the rule protocol. The options displayed will vary depending on the option you select:
  - **TCP, UPD, TCP/UDP: l**ets you define TCP and/or UDP rules, including local and remote ports.
    - **Local ports: l**ets you specify the connection port used on the user's computer. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).
    - **Remote ports: l**ets you specify the connection port used on the remote computer. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).
  - **ICMP: l**ets you create rules that describe ICMP messages, along with their type and subtype.
  - **IP Types**: **l**ets you create rules for the IP protocol and other higher-level protocols.
- **IP addresses:** lets you specify the traffic's source and destination IP addresses.
- **MAC addresses**: lets you specify the traffic's source and destination MAC addresses.

The source and destination MAC addresses are overwritten every time the traffic goes through a proxy, router, etc. Therefore, the data packets will reach their destination with the MAC address of the last device that handled traffic.

10.6.5 Block intrusions

The intrusion detection system (IDS) allows administrators to detect and reject malformed traffic specially crafted to impact the security and performance of the computers to protect. This traffic type may cause malfunction of user programs and lead to serious security issues, allowing remote execution of user applications by hackers, data theft, etc.

Panda Adaptive Defense 360 provides protection against 15 types of generic patterns. This protection can be enabled and disabled by selecting and clearing the relevant checkboxes. Next is a description of the types of malformed traffic supported and the protection provided:

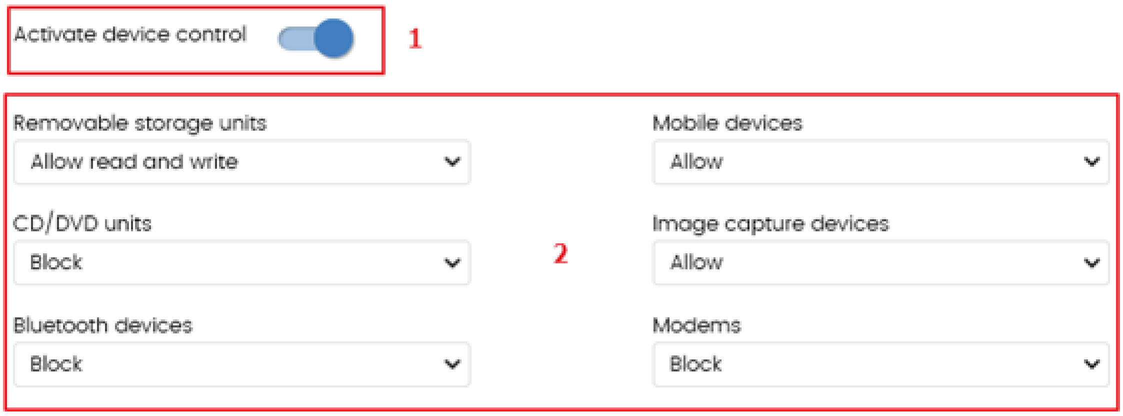
- **IP Explicit Path**: rejects IP packets that contain an explicit source route field. These packets are not routed based on their target IP address, but the routing information is defined beforehand.
- **Land Attack**: stops denial-of-service attacks that use TCP/IP stack loops by detecting packets with identical source and target addresses.
- **SYN Flood**: this attack launches TCP connection attempts massively to force the targeted computer to commit resources for each connection. The protection establishes a maximum number of open TCP connections to prevent the computer under attack from becoming saturated.
- **TCP Port Scan**: detects if a host tries to connect to several ports on the protected computer in a specific time period. The solution filters both the requests to open ports and the replies to the malicious computer. This prevents the attacking computer from obtaining information about the status of the ports.
- **TCP Flags Check**: detects TCP packets with invalid flag combinations. It acts as a complement to the protection against port scanning by blocking attacks of that type such as "SYN&FIN" and "NULL FLAGS". It also complements the protection against OS fingerprinting attacks as many of these are based on replies to invalid TCP packets.
- **Header Lengths**
  - **IP**: rejects inbound packets with an IP header length that exceeds a specific limit.
  - **TCP**: rejects inbound packets with a TCP header length that exceeds a specific limit.
  - **Fragmentation overlap**: checks the status of the packet fragments to be reassembled at the destination, protecting the system against memory overflow attacks due to missing fragments, ICMP redirects masked as UDP, and computer scanning.
- **UDP Flood**: rejects UDP streams to a specific port if the number of UDP packets exceeds a preconfigured threshold in a particular period.
- **UDP Port Scan**: protects the system against UDP port scanning attacks.
- **Smart WINS**: rejects WINS replies that do not correspond to requests sent by the computer.
- **Smart DNS**: rejects DNS replies that do not correspond to requests sent by the computer.
- **Smart DHCP**: rejects DHCP replies that do not correspond to requests sent by the computer.

- **ICMP Attack**: this filter performs various checks:
  - **Small PMTU**: by inspecting ICMP packets, the protection detects invalid MTU values used to generate a denial-of-service attack or slow down outbound traffic.
  - **SMURF**: the attack involves sending large amounts of ICMP (echo request) traffic to the network broadcast address with a source address spoofed to the victim's address. Most computers on the network will reply to the victim, multiplying traffic flows. The protection rejects unsolicited ICMP replies if they exceed a certain threshold in a specific time period.
  - **Drop unsolicited ICMP replies**: rejects all unsolicited ICMP replies and ICMP replies that have expired due to timeout.
- **ICMP Filter echo request**: the solution 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 aimed at taking advantage of vulnerabilities associated with the operating system detected. This protection complements the TCP Flag Checker.

10.7. Device Control (Windows devices)

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

The Device Control feature lets you configure the way the protected computer will behave when connecting or using a removable or mass storage device. Select the device or devices you want to authorize or block, and specify their usage.



Activate device control: on

Removable storage units: Allow read and write

CD/DVD units: Block

Bluetooth devices: Block

Mobile devices: Allow

Image capture devices: Allow

Modems: Block

Figure 63: device Control settings

Follow the steps below to enable the Device Control feature:

- Select the **Enable device control** checkbox **(1).**
- From the drop-down menu, select the authorized usage level for each type of device **(2)**

- 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**.

10.7.1 Allowed devices

Sometimes, you may need to block a certain category of devices but allow the use of some specific devices belonging to that category.

In that case you can create a whitelist, that is, a list of devices that will be allowed despite belonging to an unauthorized category.

Panda Adaptive Defense 360 lists all devices connected to each computer. Click the ⊕ icon in the **Allowed devices** section to display the list of all devices connected to the computers on your network. Use this list to select those devices that you want to exclude from the general block rules defined for each type of device. Finally, use the 🗑 button to delete existing exclusions.

10.7.2 Exporting/importing a list of allowed devices

Once you have finished configuring your list of allowed devices, you can export it to a text file. You can also do the opposite, that is, create a text file with the devices that you want to allow, and import it to the **Panda Adaptive Defense 360** Web console.

To export and import exclusion lists, use the **Export** and **Import** options from the context menu ⋮.

10.7.3 Obtaining a device's unique ID

If you want to exclude a device from the Device Control feature without having to wait for the user to connect it and then exclude it manually, obtain the device's ID. To do this, follow the steps below:

- In the Windows Device Manager, access the properties of the USB device that you want to identify in order to exclude it.
- Go to the **Details** tab and select **Resources** from the **Property** menu. A value called CM_DEVCAP_UNIQUEID should be displayed.
- Next, select **Device Instance Path** from the **Property** menu to obtain the device's unique ID.

If no CM_DEVCAP_UNIQUEID value is displayed, it will not be possible to identify the device uniquely. You will have to use the device's hardware ID to identify it.

In the Property menu, select Hardware ID. This value will allow you to exclude every USB device of the same model as the one you have identified, as it won't be possible to differentiate one specific device from the others.

Once you have the unique IDs of all the devices that you want to allow, you can create your whitelist and import it as explained in the previous section.

10.8. Web Access Control

This protection allows network administrators to limit access to specific Web categories, and configure a list of URLs to allow and deny access to. This module enables companies to optimize network bandwidth and increase business productivity.

To enable and disable it, click the **Enable Web access control** option.

10.8.1 Configuring time periods for the Web Access Control feature

This option allows you to limit access to certain Web page categories and blacklisted sites during business hours, and authorize it during non-business hours and weekends.

To configure Internet access time limits, select the **Enable only during the following times** option.

Next, select the times at which you want the Web Access Control to be enabled. To enable it only during certain times, select the relevant box and use the time grid to select the times that you want.

- To select whole days, click the relevant day of the week.
- To select the same time period for every day of the week, click the relevant hours.
- To select every day of the month, click the **Select all** button.
- To deselect your selection and start over, click the **Clear** button.

10.8.2 Denying access to specific Web pages

Panda Adaptive Defense 360 groups Web pages into 64 categories. All you have to do is select those categories that you want to deny access to.

Use the available category list to do so. If a user visits a Web page that belongs to one of the forbidden categories, a warning Web page will be displayed indicating that access is denied and the reason.

Denying access to pages categorized as unknown

You can deny access to pages categorized as unknown simply by selecting the relevant checkbox.

⚠ *Bear in mind that internal and intranet sites accessible on ports 80 and 8080 may be categorized as unknown, resulting in users not being able to access them. To avoid this, you can add any pages you want to the exclusion whilelist explained below.*

10.8.3 List of allowed/denied addresses and domains

You can set a list of pages that will always be allowed (whitelist) or blocked (blacklist), regardless of the category that they belong to.

You can edit these lists at any time.

- Enter the URL of the relevant address or domain in the text box.
- Click **Add**.
- Use the **Delete** and **Clear** buttons to edit the list according to your needs.
- Finally, click **OK** to save the settings.

As soon as a website coincides with one of the whitelisted/blacklisted sites (either wholly or partially), it will be allowed/blocked. In the case of long URLs, it will be enough to enter the beginning of the URL in the appropriate box.

10.8.4 Database of all URLs accessed from computers

Each computer on the network keeps a database of the URLs accessed from it. This database can only be consulted locally, that is, on each computer itself, for a period of 30 days.

The data displayed is as follows:

- User ID.
- Protocol (HTTP or HTTPS).
- Domain.
- URL.
- Returned category.
- Action (Allow/Deny).
- Date accessed.
- Access counter (by category and domain).

10.9. Antivirus for Exchange servers

To be able to enable the protection for Exchange servers, you must have as many licenses as the number of mailboxes to protect.

The protection for Exchange servers supports Exchange 2003, 2007, 2010, 2013 and 2016, and consists of the following three modules:

- Antivirus
- Anti-spam
- Content filter

Additionally, and depending on the moment when **Panda Adaptive Defense 360** scans the email traffic, we can differentiate between two protection modes: mailbox protection and transport protection.

Table 13 shows the Exchange versions supported by each protection module and scan mode.

Scan mode/Protection module	Antivirus	Anti-Spam	Content Filtering
Mailbox	2003, 2007, 2010		
Transport	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016

Table 13: exchange versions supported by each protection module and scan mode

10.9.1 Configuring the antivirus protection based on the scan mode

The protection for Exchange servers lets you choose between two types of scans:

- Mailbox protection
- Transport protection

Mailbox protection

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

The mailbox protection is only available in the Antivirus module for Exchange 2003, 2007 and 2010.

Transport protection

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

It scans for viruses, hacking tools and suspicious/potentially unwanted programs sent to the Exchange Server mailboxes.

You can enable/disable the mailbox and/or the transport protection by clicking the relevant checkboxes.

Mailbox protection

The mailbox protection behaves differently depending on whether the Exchange server is Exchange Server 2013-2016 or a different version.

Exchange 2013-2016 does not allow message manipulation. That is, if a message contains a dangerous item, the entire message will be moved to quarantine. In such a case, the end user protected with **Panda Adaptive Defense 360** will receive a message with the original subject but the message body replaced with a warning text. This text will prompt the user to contact the network administrator to recover the original message.

With all other versions of Exchange Server, **Panda Adaptive Defense 360** will take the action defined by Panda Security when a malware item is detected: disinfect the attachment if disinfection is possible, or send it to quarantine if disinfection is not possible. That is, the end user will receive the original message with the clean attachments or, if disinfection is not possible, a replacement file called “security_alert.txt” with information about the reason for the detection.

10.9.2 Software to detect

Select the relevant options to detect different types of threats:

- Detect viruses
- Detect hacking tools and PUPs

10.9.3 Intelligent mailbox scan

The intelligent mailbox scan runs during periods of low server activity, scanning the email messages stored on the organization's Exchange server. Moreover, it only scans those files that have not been previously scanned with the downloaded signature file. Every time there is an update of the signature file, Panda Adaptive Defense 360 will automatically launch a new intelligent mailbox scan.

10.9.4 Restoring messages with viruses and other threats

Configure the SMTP server that will forward the messages restored from the management console by entering the required information:

- **SMTP server**: enter the mail server's IP address or domain.
- **This server requires authentication**: select this option is the SMTP serve is not an open relay.
- **User**
- **Password**

If you don't configure an SMTP server, the messages will be restored to a folder on the Exchange server's hard drive.

10.10. Anti-spam for Exchange servers

Use the **Detect spam** button to enable or disable this protection.

Upon enabling the anti-spam protection, **Panda Adaptive Defense 360** will show a pop-up message offering the possibility to add a series of exclusion rules to improve the performance of your mail servers.

10.10.1 Actions to perform on spam messages

Specify what to do with spam messages:

- **Let the message through**: the tag *Spam* will be added to the subject line of the message. This is the default option.
- **Move the message to...** You will have to specify the email address that the message will be moved to. In addition, the tag *Spam* will be added to the subject line of the message.
- **Delete the message**
- **Flag with SCL (Spam Confidence Level)**

SCL

The Spam Confidence Level (SCL) is a value from 0 to 9 assigned to all messages that indicates the likelihood that a message is spam. A value of 9 indicates an extremely high likelihood that a message is spam. 0 is assigned to messages that are not spam. The SCL value can be used to configure a threshold in Active Directory above which you consider a message to be spam. The solution will flag all messages with the relevant SCL value and let them through.

Then, the administrator will establish the action to be taken on each message based on the threshold set in Active Directory.

10.10.2 Allowed addresses and domains

This is a whitelist of trusted email addresses and domains whose messages won't be scanned by the anti-spam protection.

If you want to specify more than one address/domain, separate them with ",".

10.10.3 Spam addresses and domains

This is a blacklist of email addresses and domains whose messages will be intercepted and deleted by the protection.

Keep in mind the following aspects when configuring these lists:

- If a domain is blacklisted but an address in the domain is whitelisted, the address will be allowed. However, all other addresses in the domain will be blocked.
- If a domain is whitelisted but an address in the domain is blacklisted, that address will be

blocked. However, all other addresses in the domain will be allowed.

- If a domain (e.g.: domain.com) is blacklisted and one of its subdomains (e.g.: mail1.domain.com) is whitelisted, the addresses in the subdomain will be allowed. However, all other addresses in the domain or in any other of its subdomains will be blocked.
- If a domain is whitelisted, all subdomains in the domain will also be whitelisted.

10.11. Content Filtering for Exchange servers

The Content Filtering feature allows administrators to filter email messages based on the extension of their attachments.

Once you have set a list of potentially dangerous files, configure the action to take on them.

You can also filter email attachments with double extensions.

- **Action to take**: select whether you want to delete files with dangerous attachments or move them to a specific folder. This can very helpful if you want to analyze those files at a later stage.
- **Consider attachments with the following extensions dangerous**: enter the extensions of those files you want to consider dangerous. You can use the **Add**, **Delete**, **Clear** and **Restore** buttons to configure the list to your needs.
- **Consider attachments with double extensions dangerous, except for the following**: select this option to block all messages containing files with double extensions, except for the ones you allow. Use the **Add**, **Delete**, **Clear** and **Restore** buttons to configure the list of double extensions to allow.

Detection log

All detections that take place on an Exchange server are logged locally in a CSV file. This allows network administrators to obtain additional information when a message does not reach the intended recipient.

This file is called `ExchangeLogDetections.csv` and can be found in the following folder:

```
%AllUsersProfile%\Panda Security\Panda Cloud Office Protection\Exchange
```

The CSV file contains the following fields arranged in a tabular form:

- **Date**: date when the message arrived at the Exchange server.
- **From**
- **To**
- **Subject**
- **Attachments**: list of message attachments.
- **Protection**
- **Action**

11. Android security settings

Settings for Android devices
Updates
Antivirus

11.1. Introduction

Panda Adaptive Defense 360's **Settings** menu provides the parameters required to configure the security settings for smartphones and tablets. Click the **Android devices** panel on the left-hand menu to display a list of the security configurations already created.

This chapter explains the available security settings for Android devices, and gives recommendations to protect smartphones and tablets.

11.2. Introduction to the security settings for Android devices

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

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

11.3. Updates

The update options are described in chapter 14 Software updates

11.4. Antivirus

The antivirus protection for Android devices protects smartphones and tablets against the installation of malware-infected apps and PUPs, scanning both your devices and their SD memory cards on access and on demand.

Select the **Enable permanent antivirus protection** checkbox to enable malware detection.

Exclusions

The Android protection allows you to exclude any of the installed apps from the scans. To do that, enter the names of the packages to exclude, separated with commas.

To look up an app's package name, find the app in the Google Play app store using a Web browser. The package name will be listed at the end of the URL after the '?id='.

12. Panda Data Control (monitoring of sensitive data)

12.1. Introduction

Panda Data Control is the security module in **Panda Adaptive Defense 360** that aids compliance with data protection regulations, and provides visibility and monitoring of the personal data (*PII*) stored in the IT infrastructure of organizations.

Panda Data Control discovers, audits and monitors, in real time, the complete lifecycle of PII files: including data at rest, the actions taken on files and their exfiltration.

> ***See the Panda Data Control administrator guide for more details on the specific admin console for this service.***

12.2. Panda Data Control requirements

12.2.1 Supported platforms

Panda Data Control supports Microsoft Windows platforms from version XP SP3 and Windows Server 2003 SP1 and later. Other operating systems such as Linux or macOS are not supported.

12.2.2 Recognized data types

Panda Adaptive Defense 360 uses Machine Learning algorithms and regular expressions in all compatible files discovered to detect personal information. Data types recognized as PII are as follows:

- Bank account numbers.
- Credit card numbers.
- Personal and fiscal ID numbers.
- IP addresses.
- Email addresses.
- Phone numbers.
- Driving license numbers.
- Passport numbers.
- Social security numbers.
- First names and last names.
- Places and countries.
- Postal addresses and ZIP/postal codes.

12.2.3 Supported countries

The format of recognized data varies from country to country. **Panda Data Control** recognizes data from the countries listed below:

- Germany
- Spain
- France
- Sweden
- UK
- Italy
- Portugal
- Netherlands
- Switzerland
- Finland
- Denmark

12.2.4 IFilter components

Panda Data Control requires certain third-party components to be installed on users' computers in order to correctly interpret the contents of their files. These components are called "IFilters" and are not part of the **Panda Adaptive Defense 360** installation package. Microsoft Search, Microsoft Exchange Server and Microsoft Sharepoint Server, along with other operating system services and independent products, use the IFilter components to index users' files and enable content-based searches.

Each supported file format has its own associated IFilter component, and many are pre-installed in the basic Windows configuration, although others have to be installed or updated manually.

Microsoft Filter Pack is a free distribution package containing all the IFilter components associated with the Microsoft Office suite. Once installed, **Panda Data Control** will be able to analyze the content of all file formats supported by the suite.

12.2.5 Installing the Microsoft Filter Pack component

Microsoft Filter Pack and Microsoft Office

The Microsoft Filter Pack component is included in the Office suite, though only the IFilter components corresponding to Office suite products installed on users' computer will be installed automatically. To ensure that all 2010 version components are available on the computer, see section **Installing Microsoft Filter Pack separately**.

Installing Microsoft Filter Pack separately

To install Microsoft Filter Pack, click the following URL:

https://www.microsoft.com/en-us/download/details.aspx?id=17062

The package is compatible with Windows XP SP3, Windows 2013 SP1 and later, though in some cases it may be necessary to install the Microsoft Core XML Services 6.0 library.

12.3. Panda Data Control settings

To access the **Panda Data Control** settings**:**

- Click **Settings** in the top menu, then **Sensitive data** in the side bar**.**
- Click **Add** to open the **Panda Data Control** settings window**.**

12.3.1 Searching for computers that don't meet the Panda Data Control requirements

In order to analyze file contents, **Panda Data Control** requires all IFilter components associated with compatible file formats to be installed on users' computers.

To detect computers without all or any of the IFilter components installed, click **Check now** in the settings screen. The **Computers** area will open with a list filtered by the criteria **Computers without Microsoft Filter Pack**.

12.3.2 Personal data monitoring

Panda Data Control looks for and monitors PII files in a similar way to **Panda Adaptive Defense 360** searching for and monitoring users' files for viruses and threats.

Personal data monitoring

Panda Data Control monitors the actions of processes run on files identified as PII. Such files contain the personal information (ID numbers, first and last names, addresses or other details) regarding customers, suppliers, company employees, etc.

In order for Panda Data Control to start monitoring the actions of the processes run on PII files stored on workstations or servers, click **Enable personal data monitoring**.

Search for personal data on the entire computer (recommended)

Panda Data Control runs a complete scan of the file system to search for PII files and create a database with the personal information discovered. Each time the personal information identification technology is updated, **Panda Adaptive Defense 360** will automatically run through the file system to update the database.

It is neither necessary nor possible to run an analysis on-demand. The system will automatically launch an analysis of the file system each time the Data Control intelligence is updated, and the first time this feature is enabled.

In order for **Panda Adaptive Defense 360** to run through the file system in search of personal information files:

- Click **Search for personal data on the entire computer (recommended).**

12.3.3 Data searches on computers

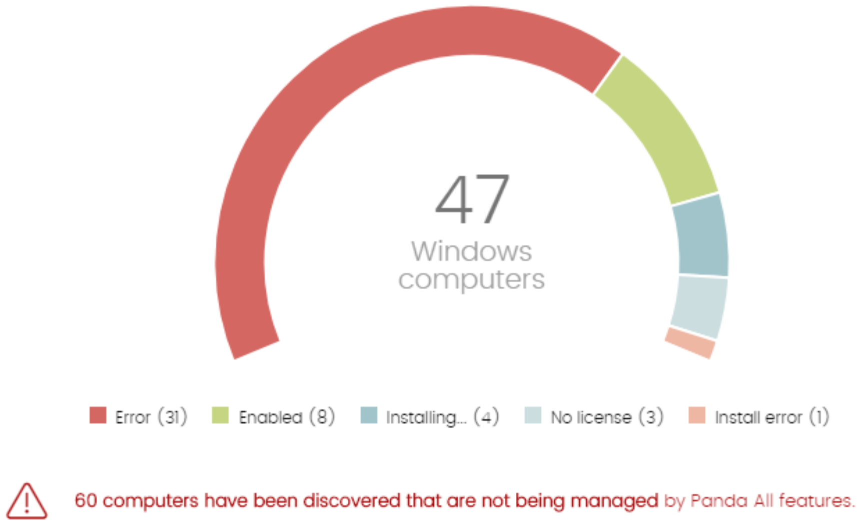
Panda Data Control lets you locate files by their name or by content, provided they have been indexed previously. To enable file searches, click **Allow data searches on computers** and **Panda Data Control** will begin the process of indexing files stored on users' computers.

To see the indexing status of computers, click **View your computers' indexing status**. The **Data Control Status** list, explained later in this chapter, will open with the status of **Panda Data Control** on each computer in the network with a license for this module.

12.4. Panels and widgets

This section looks at the widgets on the **Panda Data Control** dashboard, the different areas and hotspots included along with the tooltips and their meanings. Click **Status** in the top menu, and **Data Control** in the side bar.

12.4.1 Data Control status



60 computers have been discovered that are not being managed by Panda All features.

Figure 64: 'Data Control status' panel

This widget shows those computers where Panda Data Control is working properly, and those where an error has occurred. The status of the computer is depicted by a circle with various colors and associated counters. The panel shows as a percentage and as a graph the computers with the same status.

- **Meaning of the data displayed**

- **Error**: computers with **Panda Data Control** but for some reason, the module does not respond to requests from the Panda Security server.
- **No license**: computers that are not managed by **Panda Data Control** as there are insufficient licenses, or available licenses have not been assigned.
- **Installing**: computers on which **Panda Data Control** is currently being installed.
- **Install error**: computers on which the installation process has not been completed.
- **Disabled**: computers whose sensitive data settings don't have the option **Enable personal data monitoring** or **Data searches on computers** enabled.
- **Enabled**: computers whose sensitive data settings have both the **Enable personal data monitoring** and **Data searches on computers** options enabled.
- **Center**: total number of computers that don’t have **Panda Data Control** running.

- **Lists accessible from the panel**

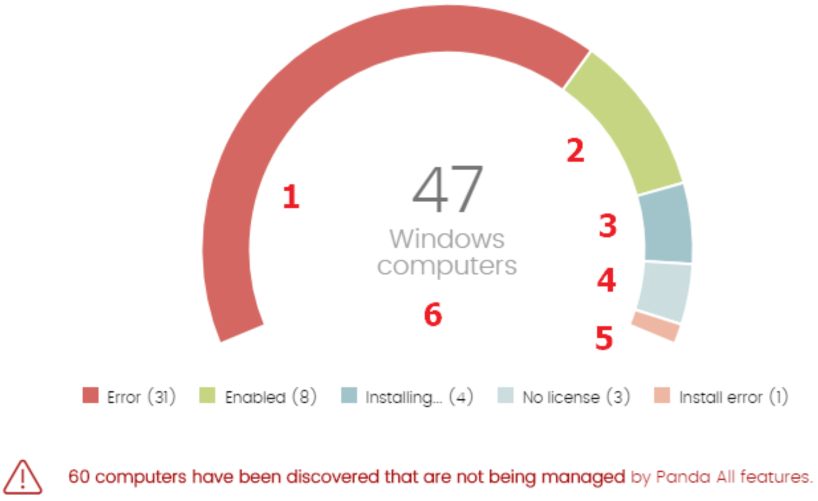


Figure 65: hotspots in the ‘Data Control statusl’ panel

The following lists are displayed according to the hotspot clicked on in the panel:

- **(1) Data Control status** list filtered by **Data Control status** = Error
- **(2) Data Control status** list filtered by **Data Control status** = Personal data monitoring enabled
- **(3) Data Control status** list filtered by **Data Control status** = Installing…
- **(4) Data Control status** list filtered by **Data Control status** = No license

- **(5) Data Control status** list filtered by **Data Control status** = Install error
- **(6) Data Control status** list filtered by **Data Control status** = No filters

12.4.2 Offline computers

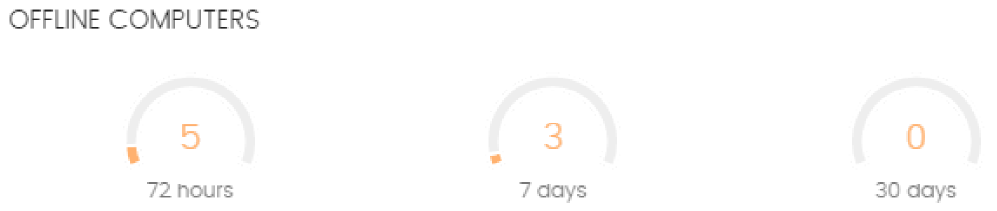


Figure 66: 'Offline computers' panel

Offline computers shows the network computers that have not connected to the Panda Security cloud for a given period of time. These computers are likely to have some kind of problem and will require specific attention from the administrator.

- **Meaning of the data displayed**

- **72 hours**: number of computers that haven't sent their status in the last 72 hours.
- **7 days**: number of computers that haven't sent their status in the last 7 days.
- **30 days**: number of computers that haven't sent their status in the last 30 days.

- **Lists accessible from the panel**

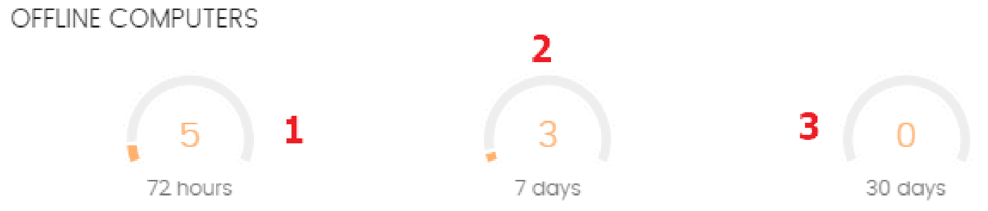


Figure 67: 'Offline computers' panel hotspots

The following lists are displayed according to the hotspot clicked on in the panel:

- **(1) Data Control status** list filtered by **Last connection** = More than 72 hours ago
- **(2) Data Control status** list filtered by **Last connection** = More than 7 days ago
- **(3) Data Control status** list filtered by **Last connection** = More than 30 days ago

12.4.3 Update status

This displays the status of computers with respect to updates of the **Panda Data Control** module.

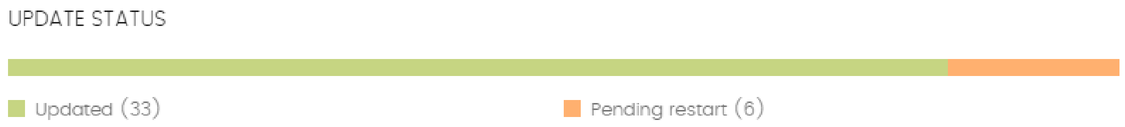


Figure 68: 'Update status' panel

- **Meaning of the data displayed**

- **Updated**: number of computers with **Panda Data Control** updated.
- **Outdated**: number of computers with **Panda Data Control** not updated.
- **Pending restart**: number of computers with **Panda Data Control** installed but that have not yet restarted and so it is not updated.

- **Lists accessible from the panel**

The following lists are displayed according to the hotspot clicked on in the panel:

- **(1) Data Control status** list filtered by **Protection up to date**= Yes
- **(2) Data Control status** list filtered by **Protection up to date** = Pending restart
- **(3) Data Control status** list filtered by **Protection up to date** = No

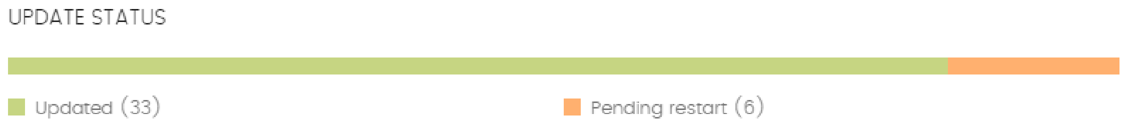


Figure 69: hotspots in the 'Update status' panel

12.4.4 Indexing status

This displays the status of the computers with respect to the indexing status of the storage drives connected.

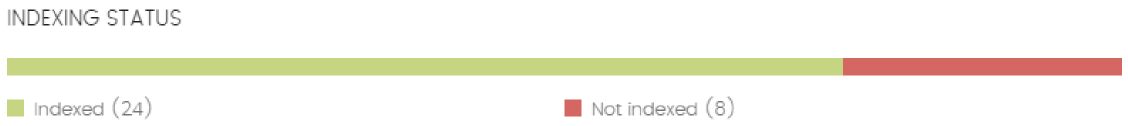


Figure 70:' Indexig status' panel

- **Meaning of the data displayed**

- **Indexed**: number of computers with the contents of the storage drives completely indexed.
- **Not indexed**: number of computers with the contents of the storage drives not indexed.

- **Indexing**: number of computers with the indexing of the storage drives still in progress.

- **Lists accessible from the panel**

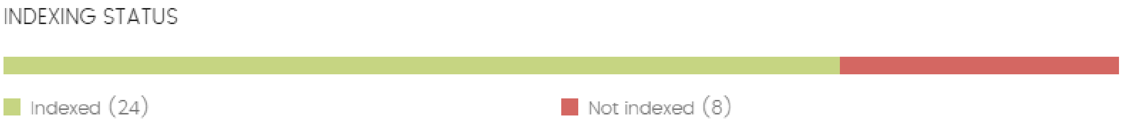


Figure 71: hotspots in the 'Indexing status' panel

The following lists are displayed according to the hotspot clicked on in the panel:

- **(1) Data Control status** list filtered by **Indexing status** = Indexing
- **(2) Data Control status** list filtered by **Indexing status** = Not indexed
- **(3) Data Control status** list filtered by **Indexing status** = Indexed

12.5. Available lists

12.5.1 'Data Control status' list

This list shows all network computers, and includes filters regarding the status of the **Panda Data Control** module to locate the computers or mobile devices that meet the criteria established in the panel.

Field	Comments	Values
Computer	Computer name.	Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree to which the computer belongs.	Character string
Personal data monitoring	Panda Data Control module status.	⊗ Install error and Error ⊖ Disabled ⬇ Installing ✓ Enabled ☒ No license
Searches	Indicates whether Panda Data Control can search for files on the computer's storage devices, and if not, it specifies the reason.	⊗ Install error and Error ⊖ Disabled ⬇ Installing ✓ Enabled ☒ No license

Field	Comments	Values
Updates	Indicates whether the Panda Data Control module installed on the computer is the latest release or not. When the mouse pointer moves over the field, the version of the protection is indicated.	Updated Pending restart No
Microsoft Filter Pack	Indicates whether all necessary Microsoft Filter Pack components are installed on the computer or not.	Installing Not installed Not available
Indexing status	Indicates the status of the file indexing process.	Indexing Indexed Not indexed Not available
Last connection	Last time the Panda Adaptive Defense 360 status was sent to the Panda Security cloud.	Date

Table 14: 'Data Control status' list fields

Fields in the exported file

Field	Comments	Values
Client	Client account to which the service belongs.	Character string
Computer type	Type of device.	Workstation Laptop Mobile device Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain to which the computer belongs.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree to which the computer belongs.	Character string
Agent version		Character string
Installation date	Date on which Panda Adaptive Defense 360 was successfully installed on the computer.	Date
Last connection date	The last time the computer status was sent to the Panda Security cloud.	Date
Last update on	Date of the last agent update.	Date

Field	Comments	Values
Platform	Operating system installed on the computer.	Windows Linux macOS Android
Operating system	Operating system on the computer, internal version and patches.	Character string
Updated protection	Whether the protection is updated to the latest version or not.	Binary
Protection version	Internal version of the protection module.	Character string
Updated knowledge	Whether the signature file on the computer is the latest version or not.	Binary
Last update on	Date of the last signature file download.	Date
Personal data monitoring	Status of the Panda Data Control module.	Install error Error Disabled Installing Enabled No license
Searches	Indicates whether Panda Data Control can search for files on the computer's storage devices, and if not, it specifies the reason.	Install error Error Disabled Installing Enabled No license
Microsoft Filter Pack	Indicates whether all necessary Microsoft Filter Pack components are installed on the computer or not.	Installed Not installed Not available
Indexing status	Indicates the status of the file indexing process.	Indexing Indexed Not indexed Not available
Isolation status	Indicates if the computer has been isolated from the network or if it communicates normally with other network computers.	Isolated Not isolated
Installation error date	Date of the unsuccessful attempt to install Panda Data Control.	Date
Installation error	Reason for the installation error.	Character string

Table 15: fields in the exported 'Data Control status' file

Filter tool

Field	Comments	Values
Computer type	Filters computers according to type.	Workstation Laptop Mobile device Server
Find computer	Filters computers by name.	Character string
Last connection	Filters according to the last time the Panda Data Control status was sent to the Panda Security cloud.	All More than 72 hours ago More than 7 days ago More than 30 days ago
Updated protection	Filters according to the protection version installed on computers.	All Yes No Pending restart
Indexing status	Filters computers according to the file indexing status.	Indexing Indexed Not indexed Not available
Microsoft Filter Pack	Filters computers according to whether they have all necessary components of Microsoft Filter Pack.	All False True
Data Control status	Filters computers according to the status of the Panda Data Control module.	Installing… Enabled Personal data monitoring disabled Data searches on the computer disabled Error Install error No license

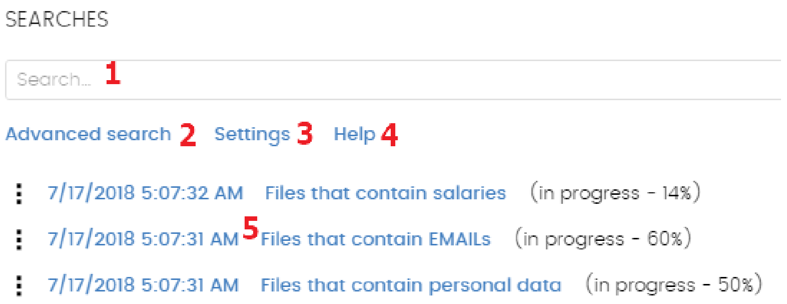
Table 16: filters available in the 'Data Control status' list

12.6. File searches

Panda Data Control locates files by name, extension or content in the storage drives that have been indexed on the network computers, using the **Searches** widget in the dashboard.

Searches are run in real time: as soon as administrators launch a search, it is run on the network computers and displays results as they come in, without waiting for the search to complete.

To access the **Searches** widget, click **Status** in the top menu, then **Data Control** in the side bar.



SEARCHES

Search... 1

⋮ 7/17/2018 5:07:32 AM Files that contain salaries (in progress - 14%)

⋮ 7/17/2018 5:07:31 AM Files that contain EMAILs (in progress - 60%)

⋮ 7/17/2018 5:07:31 AM Files that contain personal data (in progress - 50%)

Figure 72: 'Searches' panel

The widget has the following features:

- **(1)** Text box to enter search criteria. See **Error! Reference source not found.** Search syntaxes for a description of the search terms permitted by **Panda Data Control**.
- **(2) Advanced search**: defines the scope of the search.
- **(3) Settings:** access to the **Panda Data Control** settings profiles. For more details, see 12.3 Panda Data Control settings.
- **(4) Help:** link to Panda Security's support article, showing updated **Panda Data Control** search syntax.
- **(5) Previous searches:** searches that have been used before and that can be relaunched if required.

12.6.1 Search requirements and parameters

To run searches successfully, bear in mind the following requirements:

- The user account that launches the search from the Web console must have a role assigned with permissions to **Search for data on computers**. See chapter 12 Panda Data Control (monitoring of sensitive data) for more information on roles.
- The computers on which searches are run must have a **Panda Data Control** license assigned.
- The computers on which searches are run must have a **Sensitive data** settings profile assigned with the options **Search for personal data on the entire computer (recommended)** and **Allow data searches on computers** enabled.

Search parameters

- The maximum number of simultaneous searches in the management console per user account is 10. After this number an error message appears.
- The maximum number of searches saved per user account is 30. After this number an error message appears.
- The maximum number of results in total for each search is 10,000 records. Results in excess of this number will not be displayed.
- The maximum number of results per computer is 10,000 / number of computers on which the search is run. So, if you search on a network of 100 computers, the maximum number of results displayed will be 10,000 / 100 = 100 results per computer.

- The minimum number of results displayed per computer, regardless of the number of computers on the network, is 10.
- The maximum number of computers on which searches can be run simultaneously is 50. If the total number of computers in the search is greater, they will be queued until the searches in progress are completed.

12.6.2 Creating searches

Creating a free search

- Click **Status** in the top menu, then **Data Control** in the side bar**.**
- In the **Searches** widget text box, enter the search terms, in accordance with the search syntax described in section 12.6 File searches.
- Click the 🔍 icon or click **Enter**.

Once you have entered the search, the **Search results** window will open.

Creating a guided search

- Click **Status** in the top menu, then **Data Control** in the side bar.
- Click **Advanced search**.
- Select **Guided search**
- Configure the search parameters.

Advanced search parameters

- **Name of the search**: set a name for the search.
- **Search for files with**: enter the content to search for. There are three text boxes:
  - **Any of these exact words or phrases**: the search will look for files that contain any or all of the specified words or entries.
  - **All of these exact words or phrases**: the search will look for files that contain all of the specified words or entries.
  - **None of these exact words or phrases**: the search will look for files that do not contain any of the specified words or entries.
  - **Filter by file type**: select the type of file to search for the specified content. See section 12.7 Program extensions supported by Panda Data Control.
- **Narrow search to**:
  - **Computers**:
    - **All:** search for the content in all computers with a **Panda Data Control** license assigned and with the search option enabled in the settings.
    - **The following computers**: displays a list of the computers with a **Panda Data Control** license assigned. Use the checkboxes to select the computers to search for the specified content.
    - **The following computer groups**: displays the folder structure with the computer hierarchy configured in **Panda Adaptive Defense 360**. Use the checkboxes to select the groups to search for the specified content.

- **Cancel the search automatically**: select the search timeout period for computers that are switched off or offline.

12.6.3 Previous searches

Both free searches and guided searches are saved so they can be launched quickly in the future.

Once a new search has been created, it will appear in the **Searches** widget along with the date and time it was created, as well as the name and a key indicating the status (**In progress**, **Canceled**) or no status (**Finished**).

Editing a previous search

To change the name of a previous search, click the search context menu and select **Change name**.

Launching a previous search

Click the context menu of the search and click **Relaunch search**. The status of the search will change, specifying the percentage of the task completed.

Canceling and deleting previous searches

Click the context menu of the search. Click **Cancel** to stop the search, and **Delete** to cancel the search and remove it from the **Searches** widget.

12.6.4 Viewing search results

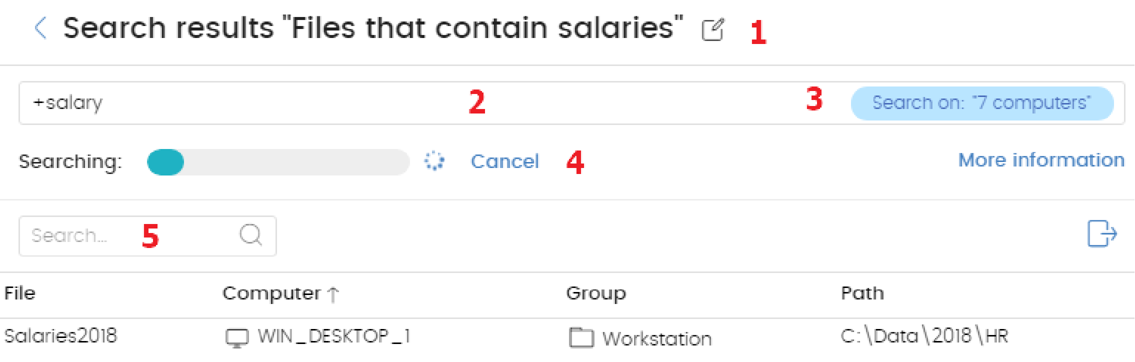
To see the results of a search, go to the **Search results** list, either by:

- Clicking on a previous search.
- Creating a new search.

The list shows the computers that contain the search term entered, along with the name of the file detected and other information.

List header

Quick search parameters:



File	Computer ↑	Group	Path
Salaries2018	WIN_DESKTOP_1	Workstation	C:\Data\2018\HR

Figure 73: 'Search results' window

- **(1)** ✎ **icon**: change the search name.
- **(2) Text box**: search content.
- **(3) Search on: "x computers"**: opens the advanced search window to narrow the search.
- **(4) Searching**: search status (**In progress**, **Canceled).** If the search has not begun or is complete, no status is indicated.
- **(5) Search text box**: filters the results by computer name.

List fields

Field	Comments	Values
File	Name of the file found.	Character string
Computer	Name of the computer on which the file has been found.	Character string
Group	Panda Adaptive Defense 360 group to which the computer belongs.	Character string
Path	Path on the storage device where the file is located.	Character string

Table 17: 'Search results' list fields

Fields in the exported file

Field	Comments	Values
File	Name of the file found.	Character string
Computer	Name of the computer on which the file was found.	Character string
Group	Panda Adaptive Defense 360 group to which the computer belongs.	Character string
Path	Path on the storage device where the file was found.	Character string
ID card numbers	Indicates whether any ID card numbers (or similar) were found in the file.	Boolean
Passport numbers	Indicates whether any passport numbers were found in the file.	Boolean
Credit card numbers	Indicates whether any credit card numbers were found in the file.	Boolean
Bank account numbers	Indicates whether any bank account numbers were found in the file.	Boolean
Driver's license numbers	Indicates whether any driving licenses were found in the file.	Boolean

Field	Comments	Values
Social security numbers	Indicates whether any social security numbers were found in the file.	Boolean
Email addresses	Indicates whether any email addresses were found in the file.	Boolean
Tax ID numbers	Indicates whether any fiscal ID numbers were found in the file.	Boolean
IPs	Indicates whether any IP addresses were found in the file.	Boolean
First and last names	Indicates whether any first and last names were found in the file.	Boolean
Addresses	Indicates whether any postal addresses were found in the file.	Boolean
Postal codes	Indicates whether any postql/ZIP codes were found in the file.	Boolean
Phone numbers	Indicates whether any phone numbers were found in the file.	Boolean

Table 18: fields in the 'Search results' exported file

12.6.5 Search syntax

Panda Data Control offers flexible searches of files by content using plain text and parameters to narrow the scope of the results. The indexing process stores the text content of the file in a standard format which is used when generating content searches.

Syntax allowed in quick searches

- **Word**: search for "word" in the document content and metadata.
- **WordA WordB**: search for "worda" or "wordb" (logical operator OR) in the document content.
- **"WordA WordB"**: search for "worda" and "wordb" consecutively in the document content.
- **+WordA +WordB**: search for "worda" and "wordb" in the document content.
- **+Worda -Wordb**: search for "worda" but not "wordb" in the document content.
- **Word***: search for all words that start with "word". The wildcard "*" is only allowed at the end of the search term.
- **Wo?rd**: search for words that begin with "wo", and end in "rd" and have a single alphabet character in between. The character "?" can be located at any point.
- **Word~**: search for all words that contain the string "word".

Syntax allowed in guided searches

Guided searches do not allow "+" or "-". Instead, search words are entered in different text boxes. If the characters "+" or "-"are used, they will simply form part of the search term.

Personal data types available

To narrow the scope of results, **Panda Data Control** supports the use of qualifiers to indicate data types or file characteristics in quick and advanced searches.

Parameters are:

- **PiiType:** specifies the type of PII data detected in the file.
- **HasPii:** indicates that the file has the PII data.
- **Filename**: indicates the name of the file.
- **FileExtension**: indicates the file extension.

The values allowed in these parameters are:

- **PiiType:BANKACCOUNT**: files that contain any bank account details.
- **PiiType:CREDITCARD**: files that contain any credit card details.
- **PiiType:IDCARD**: files that contain any national ID card numbers (or similar).
- **PiiType:SSN**: files that contain any social security numbers.
- **PiiType:IP**: files that contain any IP addresses.
- **PiiType:EMAIL**: files that contain any email addresses.
- **PiiType:PHONE**: files that contain any phone numbers.
- **PiiType:ADDRESS**: files that contain any postal addresses.
- **PiiType:FULLNAME**: files that contain any first names and last names.
- **PiiType:PASSPORT**: files that contain any passport details.
- **PiiType:DRIVERLIC**: files that contain any driving license details.
- **HasPii:True**: files that contain any PII data.
- **Filename**:"file name": files with the specified file name.
- **Fileextension**: "file extension": files with the specified file extension.

Syntax for PII data searches

PII data types can be used in all search types (quick or guided) alone or combined with other character strings.

- **PiiType:IDCARD:** search for files with ID card data detected.
- **+PiiType:IDCARD +"Panda Security":** search for files containing a list of ID card details in the company (with the character string "Panda Security").
- **+Filename**:**scan* +fileextension:docx -PiiType:fullname:** search for scan files (files whose name starts with "scan") in Word (.docx extension) and that are not officially signed (no Fullname -first names and last names - were detected.)

12.6.6 Process of normalization and searching for character strings

The data extracted from the files found on users’ computers is stored in a database on the computer itself after undergoing a process of normalization. This process varies depending on whether **Panda Data Control** considers the data as a PII data type or unidentified text.

The normalization process directly affects the searches, as it contrasts the search parameters with the data stored after normalization. That is, the search is performed on the normalized data and not on the original data contained in users’ files.

Separating characters

Panda Data Control identifies a group of special characters that it considers as separators between words and which can be completely removed or replaced by a single space. These characters are as follows

- **Return**: \r
- **Line break**: \n
- **Tab key**: \t
- **Characters**: " : ; ! ? - + _ * = ( ) [ ] { } , . | % \ / ’

Transformation of indexed character strings to lowercase

Regardless of whether the character string is recognized as a PII type or not, before it is stored in the database, it is transformed to lowercase. Administrator searches are also transformed to lowercase, so writing in uppercase or lowercase does not affect the search result.

General rules for normalizing data recognized as personal data

- In PII types formed by numeric characters (telephone numbers, bank account numbers, etc.) separating characters are deleted and the resulting string is stored as a single entity. For example "1.42.65.116-C" would be stored as PII type IDCARD "14265116C".
- IP addresses and email addresses are stored as they are.
- For First Names and Last Names and Addresses, each word is stored independently and those containing numbers are deleted. For example "25 Upper Nelson Mandela Boulevard” would be stored as "upper", "nelson", "mandela", "boulevard”.

General rules for normalizing data not recognized as personal data

- Numerical and alphanumeric data (words formed by letters and numbers) that are not detected as PII are deleted in the normalization process, and therefore they do not return any results in searches.
- Each separating character detected divides the character string into two independent words and means that the separator character is not stored. For instance, the string "house.forest" is stored as "house" and "forest" and the separator character "." is deleted.

Tips for constructing searches that are compatible with the normalization process

- It is preferable to use lowercase letters.
- Numeric characters which are part of strings that are not identified as a PII entry compatible

with **Panda Data Control** are deleted in the normalization process, and should not therefore be used in searches.

- To search for **bank account numbers, credit card numbers, ID card numbers, social security numbers, passport numbers, driver's license numbers** don't use separating characters.
- To search for **IP addresses** and **email addresses**, enter them as they are.
- To search for **phone numbers**, remove any separating characters, and enter the country code if necessary without the "+" sign.
- To find **postal addresses** or **first and last names**, don't use the numeric characters.

12.7. Program extensions supported by Panda Data Control

Suite name	Product	Extensions
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW

	Draw	- ODG - OTG - STD
	Math	- ODF - SXM
	Base	- ODB
	Impress	- OTP - ODP - STI - SXI
	Calc	- OTS - ODS - SXC
Plain text		TXT
Web browsers	- Internet Explorer - Chrome - Opera - Other	- HTM - HTML - MHT - OTH
Mail clients	- Outlook - Outlook Express	EML
Others	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Table 19: list of supported program extensions

12.8. Packers and compressors supported

Name of file compressor / packer / algorithm	Extensions
7-ZIP	.7z
bzip2	.bz2
gzip	.gz

Name of file compressor / packer / algorithm	Extensions
Binhex	.hqx
LHARC	.lha .lzh
Lempel-Ziv & Haruyasu	.lzh
Lempel–Ziv–Oberhumer / lzop	.lzo
Multi-Purpose Internet Mail	.mme
Lotus Notes Traveler	.nts
WinRAR	.rar
Tar	.tar
Tar & GZip	.tgz
Uuencode	.uu .uue
XXEncoding	.xx .xxe
PkZip / PKWare	.zip

Table 20: list of compressor/packer extensions supported

13. Panda Patch Management (Updating vulnerable programs)

13.1. Introduction

Panda Patch Management is a built-in module on Aether Platform that finds those computers on the network with known software vulnerabilities and updates them centrally and automatically. It minimizes the attack surface, preventing malware from taking advantage of the software flaws that may affect the organization's workstations and servers in order to infect them.

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

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

The features provided by **Panda Patch Management** are accessible via the following sections in the management console:

- **To configure the discovery of missing patches**: go to the **Patch management** settings section (top menu **Settings**, side panel).
- **To have visibility into the update status of the entire IT network**: go to the **Patch management** dashboard (top menu **Status**, side panel).
- **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**).
- **To view a history of all installed patches**: check the **Installation history** list (top menu **Status**, side panel **My lists**, **Add**).
- **To patch computers**: go to top menu **Tasks**, and create an **Install patches** scheduled task. You can also patch computers via the context menus available in the group tree (top menu **Computers**), on the lists, and on the **Computer details** screen.

13.2. General workflow

Panda Patch Management is a comprehensive tool for patching and updating the operating systems and all programs installed on the computers on your network. To effectively reduce the attack surface of your computers, follow the steps below:

- Make sure **Panda Patch Management** works properly on the protected computers on your network.
- Make sure that all published patches are installed.
- Install the selected patches.

- 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.

13.2.1 Make sure that Panda Patch Management works properly

Follow the steps below:

- Make sure that all computers on your network have a **Panda Patch Management** license assigned and the module is installed and running. Use the **Patch management status** widget.
- Make sure that all computers with a **Panda Patch Management** license assigned can communicate with the Panda Security cloud. Use the **Time since last check** widget.
- Make sure the computers that will receive the patches have the Windows Update service running with automatic updates disabled.

> ***We advise that you disable automatic updates in the Windows Update service settings so that Panda Patch Management can control when to apply patches. Otherwise, Windows Update will overlap with Panda Patch Management. Regardless of these settings, certain Microsoft patches require that Windows Update be running.***

13.2.2 Make sure that all published patches are installed

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

- To view missing patches by type and criticality level, use the **Patch criticality** widget.
- To view details of the patches that are missing on a computer or computer group:
  - Go to the computer tree (top menu **Computers**, **Folder** tab in the side panel), and click the context menu of a computer group containing Windows computers. Select **View available patches.** The **Available patches** list will be displayed filtered by the relevant group.

    Or,
  - Go to the computers screen (top menu **Computers**, right panel) and click a computer's context menu. Select **View available patches**. The **Available patches** list will be displayed filtered by the relevant computer.
- To get an overview of all missing patches:
  - Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
  - Use the filter tool to narrow your search.
- To find those computers that don't have a specific patch installed:
  - Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
  - Use the filter tool to narrow your search.

- Click the context menu of the specific computer-patch and select the option **View which computers have the patch available**.

13.2.3 Install the patches

Patches and updates are installed via quick tasks and scheduled tasks. Quick tasks install patches in real time but do not restart the target computer, even though this may be required in order to complete the installation process. Scheduled tasks allow you to configure all parameters related to the patch installation operation. Refer to chapter 15 Tasks for more information about tasks in **Panda Adaptive Defense 360.**

Despite the management console is a very flexible tool that allows you to install patches in multiple ways, generally speaking you can apply the following strategies:

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

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

Target / Patch	One or multiple specific patches	One, multiple or all types of patches
One or multiple computers	Available patches list (1)	Tasks (1)
A group	Available patches list (2)	Tasks (2)
Multiple or all groups	Available patches list (3)	Tasks (3)

Table 21: patch installation based on the target and the patches to install

Available patches list (1)

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

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
- Use the filter tool to narrow your search.
- Click the checkboxes besides the computers-patches you want to install, and select **Install** from the action bar to create a quick task, or **Schedule installation** to create a scheduled task.

Tasks (1)

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

- Go to top menu **Computers** and click the **Folders** tab in the computer tree (left panel).

Next, select the group that the target computers belong to. If the target computers belong to multiple groups, click the **All** root group.

- Click the checkboxes besides the computers that the patches will be applied to.
- From the action bar, click **Schedule patch installation**.
- Configure the task, click the **Save** button and publish it.

Available patches list (2)

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

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

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

Tasks (2)

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

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

Available patches list (3)

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

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
- Use the filter tool to find the patch to install.
- Click the checkbox besides the patch to install and click **Schedule installation** to create a task.
- Go to top menu **Tasks** and edit the task you have just created.
- In the **Recipients** field, add the groups that the patch will be applied to (use the **Computer groups** section to do this). Remove any additional computer that may appear in the **Additional computers** section.
- Click **Back**, finish configuring the task and click **Save**.
- Publish the task.

To install multiple specific patches on multiple computer groups, repeat these steps as many times as patches you want to install.

Tasks (3)

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

- Go to top menu **Tasks**, click **Add task** and select **Install patches**.
- Set the **Recipients** field, indicating the computers and groups that the patches will be applied to.
- Select the types of patches to install.
- Click **Save** and publish the task.

13.2.4 Make sure the programs installed on your computers 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 the EOL programs on your network:

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel.
- Select the **End-of-Life programs** list.

The list displays a line for each computer-EOL program pair found.

13.2.5 Check the history of patch and update installations

Follow these steps to find out if a specific patch is installed on your network computers:

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel.
- Select the **Installation history** list.

The list displays a line for each computer-installed patch pair found, with information about the affected program's or operating system's name and version, and the patch criticality/type.

13.2.6 Check the patch status of those computers where incidents have been recorded

Refer to chapter 16 Malware and network visibility for more information about the available tools for monitoring the security status of your IT network.

Panda Adaptive Defense 360 correlates those computers where incidents have been recorded with their patch status so that it is possible to determine whether an infected computer or a computer where threats have been detected has missing patches.

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

- Go to top menu **Status**, click on the **Malware activity**, **PUP activity**, **Currently blocked programs being classified**, or **Threats detected by the antivirus** widgets and click a computer-threat. Information about the threat detected on the computer will be displayed.
- In the **Affected computer** section, click the **View available patches** button. The **Available patches** list will be displayed, filtered by the relevant computer.
- Select all of the available patches for the computer and click **Install** from the action bar in order to create a quick patch installation task.

> *It is advisable to isolate any infected computer that needs patching and shows network traffic in the threat's lifecycle. This will minimize the risk of spreading the infection to other computers on the corporate network while the patch operation is taking place. Refer to chapter 18 Forensic analysis for more information about the malware lifecycle. Refer to chapter 19 Remediation tools for more information on how to isolate a network computer.*

13.3. Configuring the discovery of missing patches

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

Follow these steps to configure the discovery of missing patches:

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

13.3.1 General options

Click the **Automatically search for patches** switch to enable the patch search functionality. If the switch is not on the ON position, the lists in the module won't display missing patches, although it will still be possible to apply them via the patch installation tasks.

13.3.2 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.

13.3.3 Patch criticality

Sets the criticality of the patches that **Panda Patch Management** will look for in its cloud-hosted database.

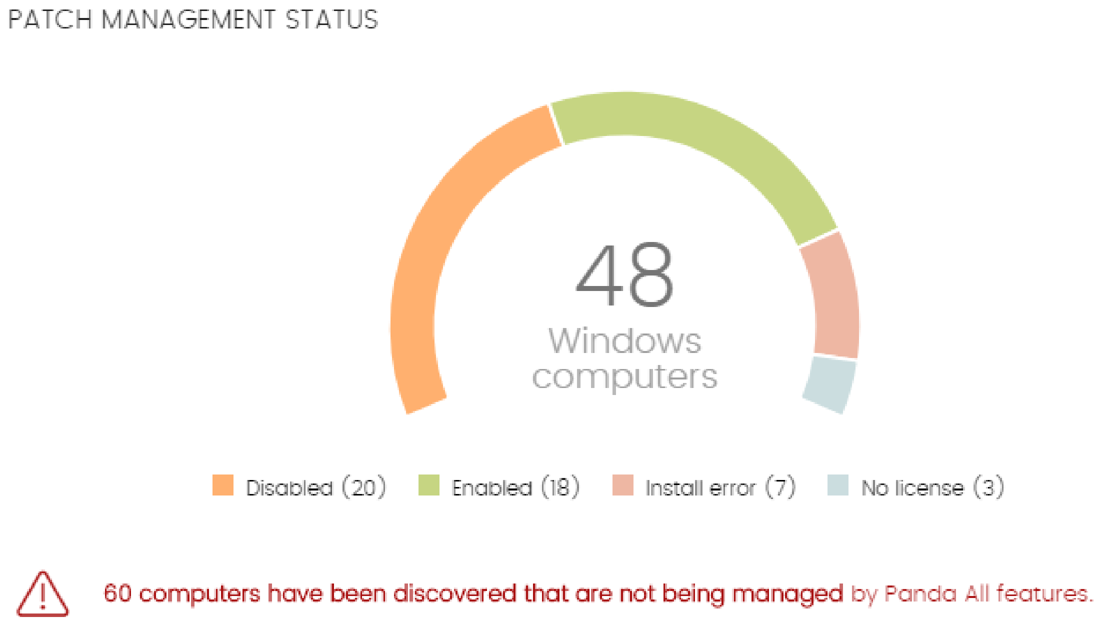
The criticality level of patches is defined by the vendor of the software affected by the vulnerability. The classification criteria are not universal. We recommend that, prior to installing a patch, you check its description, especially for those patches not classified as 'critical'. This way, you can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

13.4. Available panels/widgets

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

13.4.1 Patch management status

Shows those computers where **Panda Patch Management** is working properly and those where there have been errors or problems installing or running the module. The status of the module is represented with a circle with different colors and associated counters. The panel offers a graphical representation and percentage of those computers with the same status.



60 computers have been discovered that are not being managed by Panda All features.

Figure 74: 'Patch management status' panel

- **Meaning of the data displayed**

- **Enabled**: shows the percentage of computers where **Panda Patch Management** was installed successfully, is running properly and the assigned settings enables the module to search for patches automatically.

- **Disabled**: shows the percentage of computers where **Panda Patch Management** was installed successfully, is running properly but the assigned settings prevent the module from searching for patches automatically.
- **No license**: computers where **Panda Patch Management** is not working because there are insufficient licenses or because an available license has not been assigned to the computer.
- **Installation error**: indicates the computers where the module could not be installed.
- **Central area**: shows the total number of computers compatible with the **Panda Patch Management** module.

- **Lists accessible from the panel**

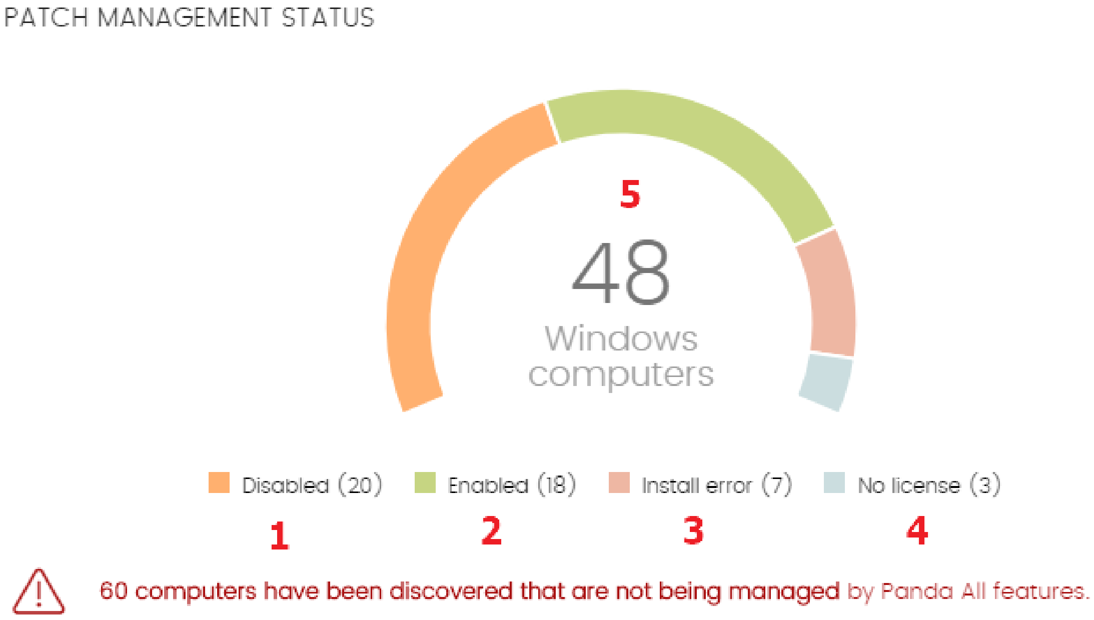


Figure 75: hotspots in the 'Patch management status' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Patch management status** list filtered by **Patch management status** = Disabled
- **(2) Patch management status** list filtered by **Patch management status** = Enabled
- **(3) Patch management status** list filtered by **Patch management status** = No license
- **(4) Patch management status** list filtered by **Patch management status** = Installation error
- **(5) Patch management status** list without any filters

13.4.2 Time since last check

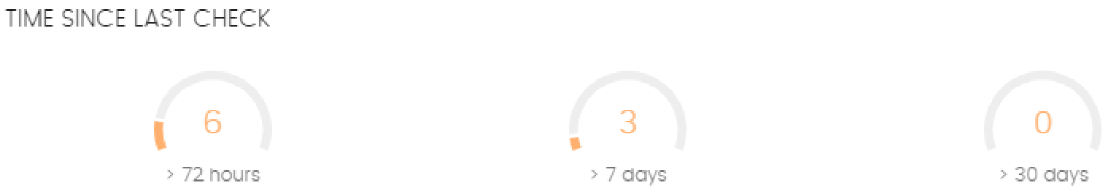


Figure 76: 'Time since last check' panel

Displays computers that have not connected to the Panda Security cloud to report their patch status for a certain amount of time. Such computers are susceptible to security problems and require special attention from the administrator.

- **Meaning of the data displayed**

- **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.

- **Lists accessible from the panel**

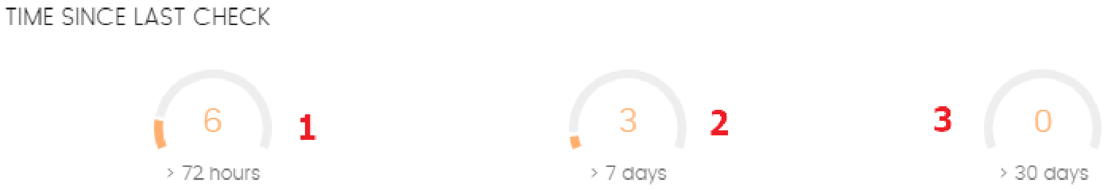
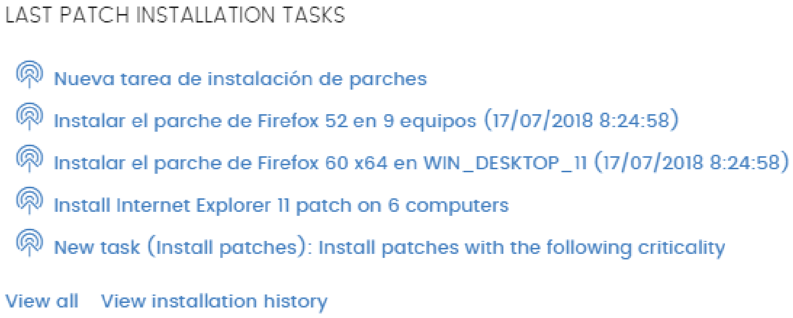


Figura 77: hotspots in the 'Time since last check' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Patch management status** list filtered by **Last checked** = More than 3 days ago and **Patch management status** = Enabled and Disabled.
- **(2) Patch management status** list filtered by **Last checked** = More than 7 days ago and **Patch management status** = Enabled and Disabled.
- **(3) Patch management status** list filtered by **Last checked** = More than 30 days ago and **Patch management status** = Enabled and Disabled.

13.4.3 Last patch installation tasks



LAST PATCH INSTALLATION TASKS

- Nueva tarea de instalación de parches
- Instalar el parche de Firefox 52 en 9 equipos (17/07/2018 8:24:58)
- Instalar el parche de Firefox 60 x64 en WIN_DESKTOP_11 (17/07/2018 8:24:58)
- Install Internet Explorer 11 patch on 6 computers
- New task (Install patches): Install patches with the following criticality

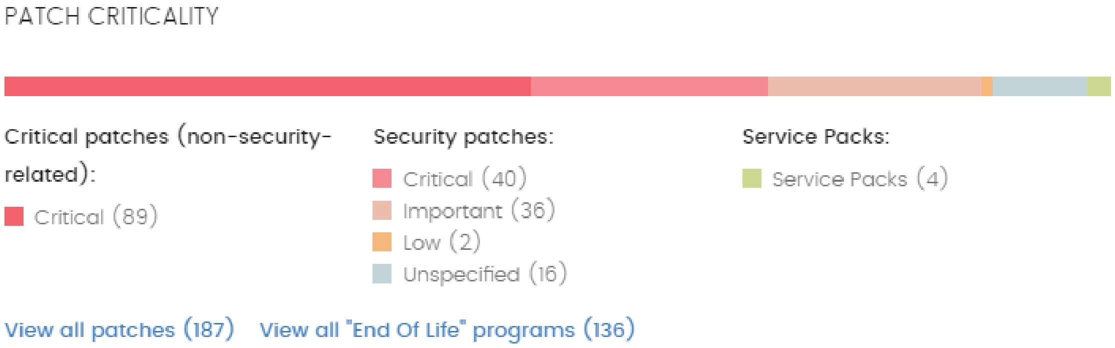
View all   View installation history

Figure 78: 'Last patch installation tasks' panel

Shows a list of the last patch installation tasks created. This widget displays multiple links through which you can manage the patch installation tasks:

- Click a task to edit its settings.
- Click the **View all** link to access the top menu **Tasks**. There you'll see all the tasks that have been created.
- Click the **View installation history** link to access the **Installation history** list. There you'll see the patch installation tasks that have finished successfully or with errors.

13.4.4 Patch criticality



PATCH CRITICALITY

Critical patches (non-security-related):

🟥 Critical (89)

Security patches:

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

Service Packs:

🟩 Service Packs (4)

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

Figure 79: 'Path criticality' panel

Shows the number of computer-missing patch pairs on the network, sorted by patch type. Each missing patch is counted as many times as there are computers that don't have it installed.

- **Meaning of the data displayed**

- **Critical patches (non-security-related) - Critical**: number of non-security patches rated 'critical' and pending application.
- **Security patches - Critical**: number of security patches rated 'critical' and pending application.

- **Security patches - Important**: number of security patches rated 'important' and pending application.
- **Security patches - Low**: number of security patches rated 'low' and pending application.
- **Security patches** – **Unspecified**: number of security patches that don't have a severity rating and are pending application.
- **Service Packs** – **Service Packs**: number of patch and hotfix bundles that are pending application.
- **View all patches**: number of patches of any severity, related or not to system security and which are pending application.
- **View all "End Of Life" programs**: number of programs found which are no longer supported by the relevant vendor.

- **Lists accessible from the panel**

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Available patches** list filtered by **Criticality** = Critical (non-security-related).
- **(2) Available patches** list filtered by **Criticality** = Critical (security-related).
- **(3) Available patches** list filtered by **Criticality** = Important (security-related).
- **(4) Available patches** list filtered by **Criticality** = Low (security-related).
- **(5) Available patches** list filtered by **Criticality** = Unspecified (security-related).
- **(6) Available patches** list filtered by **Criticality** = Service Pack.
- **(7) Available patches** list without any filters.
- **(8)** "**End of Life**" **programs** list without any filters.

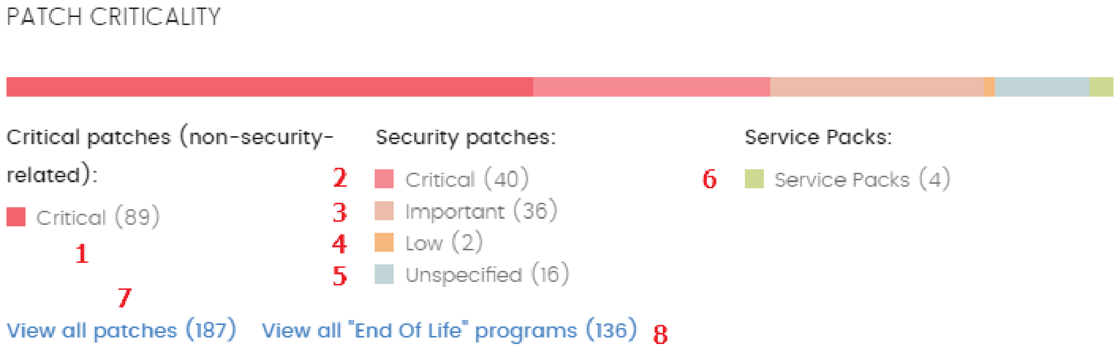


Figure 80: hotspots in the 'Path criticality' panel

13.5. Available lists

13.5.1 'Patch management status' list

This list shows all computers on the network that are compatible with **Panda Patch Management** (with filters to allow administrators to identify those workstations and servers that are not using the service due to one of the reasons displayed in the associated panel).

Field	Comments	Values
Computer	Name of the computer with outdated software.	Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to.	Character string
Patch management	Module status.	✓ Enabled ⊖ Disabled ⊗ Installation error (failure reason) ☒ No license
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 Adaptive Defense 360 status was last reported to the Panda Security cloud.	Date

Table 22: fields in the 'Patch management status' list

Fields displayed in the exported file

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	Workstation Laptop Mobile device Server
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to.	Character string
Agent version		Character string
Installation date	Date when the Panda Patch Management module was successfully installed on the computer.	Date
Last connection date	Date when the agent last connected to the Panda Security cloud.	Date
Platform	Operating system installed on the computer.	Windows Linux macOS Android
Operating system	Operating system installed on the computer, internal version and patch status.	Character string

Field	Comments	Values
Exchange Server	Version of the mail server installed.	Character string
Protection updated	Indicates whether the installed protection has the latest released version.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date when the signature file was last updated.	Date
Patch management status	Module status.	Enabled Disabled Installation error No license
Pending restart	The computer requires a reboot to finish installing one or more downloaded patches.	Binary value
Last check date	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date
Isolation status	Indicates if the computer has been isolated or can communicate normally with all other computers on the network.	Isolated Not isolated
Installation error date	Date when the administrator attempted to install the Panda Patch Management module and the operation failed.	Date
Installation error	Failure reason	Download error Execution error

Table 23: fields in the 'Patch management status' exported file

Filter tool

Field	Comments	Values
Computer type	Type of device.	Workstation Laptop Server
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	All More than 3 days ago More than 7 days ago More than 30 days ago
Last connection	Date when the agent last connected to the Panda Security cloud	Date
Pending patches requiring a restart	The computer requires a reboot to finish installing one or more downloaded patches.	Boolean
Patch management status	Module status.	Enabled Disabled Installation error No license

Table 24: filters available in the 'Patch management status' list

13.5.2 'Available patches' list

Shows a list of all missing patches on the network computers and published by Panda Security. Each line in the list corresponds to a patch-computer pair.

Field	Comments	Values
Computer	Name of the computer with outdated software.	Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Criticality	Update severity rating and type.	Critical (non-security-related) Critical (security-related) Important (security-related) Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack

Table 25: fields in the 'Available patches' list

Fields displayed in the exported file

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	Workstation Laptop Mobile device Server
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Criticality	Update severity rating and type.	Critical (non-security-related) Critical (security-related)

Field	Comments	Values
		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
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Last seen	Date when the computer was last discovered.	Date
Is downloadable	Indicates if the patch is available for download or requires an additional support contract with the software vendor in order to have access to it.	Boolean
Download size (KB)	Patch size in compressed format. Applying the patch may require more space on the target computer's storage media than indicated in this field.	Numeric value

Table 26: fields in the 'Available patches' exported file

Filter tool

Field	Comments	Values
Computer type	Type of device.	Workstation Laptop Server
Find computer	Computer name.	Character string
Computer	Name of the computer with outdated software.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string

Field	Comments	Values
Criticality	Update severity rating and type.	Critical (non-security-related) Critical (security-related) Important (security-related) Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack
Show non-downloadable patches	Lets you select whether you want to display those patches that are not available for download as they require an additional support contract with the software vendor in order to have access to them.	Boolean

Table 27: filters available in the 'Available patches' list

13.5.3 'End-of-Life programs' list

Shows programs that are no longer supported by the relevant vendor. These programs are particularly vulnerable to malware and cyberthreats.

Field	Comments	Values
Computer	Name of the computer with EOL software.	Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program entered its EOL stage.	Date

Table 28: fields in the 'End-of-Life programs' list

Fields displayed in the exported file

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	Workstation Laptop Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense 360	Character string

Field	Comments	Values
	folder tree that the computer belongs to.	
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program entered its EOL stage.	Date
Last seen	Date when the computer was last discovered.	Date

Table 29: fields in the 'End-of-Life programs' exported file

Filter tool

Field	Comments	Values
Find computer	Computer name.	Character string

Table 30: filters available in the 'End-of-Life programs' list

13.5.4 'Installation history' list

Shows the patches that **Panda Adaptive Defense 360** attempted to install and the computers that received them in a given time interval.

Field	Comments	Values
Date	Date when the patch or update was installed.	Date
Computer	Name of the computer that received the patch or update.	Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to.	Character string
Program	Name of the program or Windows operating system that received the patch or update.	Character string
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	
Criticality	Severity rating of the installed patch.	Critical (non-security-related) Critical (security-related) Important (security-related) Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack
Installation	Installation status of the patch or update.	Installed Pending restart Error

Table 31: fields in the 'Installation history' list

Fields displayed in the exported file

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	Workstation Laptop Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense 360 folder tree that the computer belongs to.	Character string
Date	Date of the installation attempt.	Date
Program	Name of the program or Windows operating system that received the patch or update.	Character string
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the installed patch.	Critical (non-security-related) Critical (security-related) Important (security-related) Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Installation	Installation status of the patch or update.	Installed Pending restart Error
Installation error	The Panda Patch Management module didn't install correctly	Unable to download: Installer not available Unable to download: The file is corrupted Not enough disk space
Download URL	URL for downloading the patch individually.	Character string

Table 32: fields in the 'Installation history' exported file

Filter tool

Field	Comments	Values
Computer type	Type of device.	Workstation Laptop Server
Find computer	Computer name.	Character string
From	Start date for the search range.	Date
To	End date for the search range.	Date
Criticality	Severity rating of the installed patch.	Critical (non-security-related) Critical (security-related) Important (security-related) Moderate (security-related) Low (security-related) Unspecified (security-related) Service Pack
Installation	Installation status of the patch or update.	Installed Pending restart Error
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string

Table 33: filters available in the 'Installation history' list

13.6. Downloading and installing patches

In order to install patches and updates, **Panda Patch Management** uses the task infrastructure implemented in **Panda Adaptive Defense 360.**

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

13.6.1 Patch installation

To speed up the configuration process when patching computers, **Panda Adaptive Defense 360** lets you create patching tasks by leveraging preconfigured parameters. The number of preconfigured parameters will differ (all, some or none) depending on where in the management console you create the task from:

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

- From the **Computers** screen.

The preconfigured parameters can be as follows:

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

Top menu Tasks

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

Follow the steps below to create a patch installation task:

- Go to top menu **Tasks**, click **Add task** and select **Install patches**.
- In the **Recipients** field, select the groups and computers that will receive the task.
- Schedule the task. See chapter 15 Tasks for more information.
- Select the type of patches to install. When creating a new task from scratch you cannot specify individual patches.
- Set the restart options in case the target workstation or server needs to be restarted to finish installing the patch.
  - **Do not restart automatically**: upon completing the patch installation task, a window is displayed to the target computer user with the options **Restart now** and **Remind me later**. If the latter is selected, a reminder will be displayed 24 hours later.
  - **Automatically restart workstations only**: upon completing the patch installation task, a window is displayed to the target computer user with the **Restart now** option, a **Minimize** button and a **4-hour** countdown timer. This window will be maximized every 30 minutes as a reminder to the user. Less than one hour before the restart, the minimize button will be disabled. When the countdown finishes, the computer will be restarted.
  - **Automatically restart servers only**: this option behaves in the same way as **Automatically restart workstations only**.
  - **Automatically restart both workstations and servers**: this option behaves in the same way as **Automatically restart workstations only.**
- Click **Save** and publish the task.

'Available patches' list

Lets you create tasks using preconfigured computer-patch pairs.

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

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
- Select the computer-patch pairs that suit your needs.
- If you select multiple patches, click **Install** (quick task) or **Schedule installation** (scheduled task) from the action bar in order to install them.

- Quick tasks are automatically published.
- Scheduled tasks are not published immediately and may require configuration changes. Go to the **Tasks** menu at the top of the console to edit and publish a scheduled task.

- If you select a single computer-patch pair, you can use the computer's context menu to select **Install** or **Schedule installation**.

Folder tree

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

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

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

The Computers screen

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

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

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

13.6.2 Patch download and bandwidth savings

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

*Proxy nodes cannot download patches or updates. Likewise, no patches or updates are downloaded if the node or computer with the cache/repository role does not have direct access to the Panda Security cloud, or indirect access via a corporate proxy. Refer to chapter 22 **Controlling and monitoring the management console** for more information about roles in Panda Adaptive Defense 360.*

Nodes with the cache/repository role store patches for a maximum of 30 days; after then the patches are deleted. If a computer requests a patch from a cache node, but the node doesn't have the patch in its repository, the computer will wait for the cache node to download it. The wait time will depend on the size of the patch to download. If the node cannot download the patch, the computer will attempt to download it directly instead.

Once a patch has been applied to a target computer, it will be deleted from the computer's storage media.

13.6.3 Installation task sequence

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

In contrast, scheduled patch installation tasks start downloading the necessary patches when configured in the settings. However, if the start time of multiple tasks coincides, the module will introduce a short random delay of up to 2 minutes to prevent downloads from overlapping and minimize bandwidth usage to a certain extent.

14. Software updates

Protection engine updates

Communications agent updates

Knowledge updates

14.1. Introduction

Panda Adaptive Defense 360 is a cloud-based managed service that doesn't require customers to update the back-end infrastructure that supports the protection service. However, it is necessary to update the software installed on the customer's computers.

The components installed on users' computers are the following:

- **Aether Platform** communications agent
- **Panda Adaptive Defense 360** protection engine
- Signature file for the traditional antivirus protection

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

Module	Platform			
	Windows	macOS	Linux	Android
Panda agent	On-demand			
Panda Adaptive Defense 360 protection	Configurable	Configurable	Configurable	No
Signature file	Enable/Disable	Enable/Disable	Enable/Disable	No

Table 34: update procedures based on platform and module

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

14.2. Configuring protection engine updates

To configure the **Panda Adaptive Defense 360** protection engine updates, you must create and assign a 'Per-computer settings' configuration profile. To do this, go to the **Settings** menu, and select **Per-computer settings** from the left-hand menu.

14.2.1 Updates

To enable the automatic updates of the **Panda Adaptive Defense 360** protection module, select the **Automatically update Aether on devices** checkbox. This will enable all other settings options on the screen. If that option is cleared, the protection module will never be updated.

⚠ *It is not advisable to disable the protection engine updates. Computers with outdated protection will be more vulnerable to malware and advanced threats over time.*

Running updates at specific time intervals

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

- Start time
- End time

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

Running updates on specific days

Use the drop-down menu to specify the day the update should be run:

- **Any day**: the updates will run when they are available.
- **Days of the week**: use the checkboxes to select the days of the week when the **Panda Adaptive Defense 360** updates will run. If an update is available, it will run on the first day of the week that coincides with the administrator's selection.
- **Days of the month**: use the menus to set the days of the month when the **Panda Adaptive Defense 360** updates will run. If an update is available, it will run on the first day of the month that coincides with the administrator's selection.
- **On the following days**: use the menus to set a specific date range for the **Panda Adaptive Defense 360** updates. This option lets you select update intervals that won't be repeated over time. After the specific date, no updates will be run. This option forces the administrator to constantly establish a new update interval as soon as the previous one has expired.

Computer restart

Panda Adaptive Defense 360 lets you define a logic for computer restarts, if needed, by means of the drop-down menu at the bottom of the settings window:

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

14.3. Configuring communications agent updates

The **Panda agent** is updated on demand. **Panda Adaptive Defense 360** will display a notification in the management console indicating the availability of a new agent version. From then on, the administrator will be able to launch the update whenever they want to.

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

14.4. Configuring knowledge updates

To configure **Panda Adaptive Defense 360's** signature file updates, go to the security configuration profile assigned to the computer, depending on its type.

14.4.1 Windows, Linux and macOS devices

Go to **Settings**, and select **Workstations and servers** from the left-hand menu.

Go to **General**. There you will see the following options:

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

⚠ *It is not advisable to disable the automatic knowledge updates. A computer with out-of-date knowledge may be vulnerable to threats.*

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

14.4.2 Android devices

Go to **Settings**, and select **Android devices** from the left-hand menu.

Panda Adaptive Defense 360 lets you restrict software updates so that they don't consume mobile data.

Select this option to restrict updates to those occasions when there is an available Wi-Fi connection for your smartphone or tablet.

15. Tasks

15.1. Introduction

A task is a resource implemented in **Panda Adaptive Defense 360** that allows administrators to associate a process with two variables: repetition interval and execution time.

- **Repetition interval**: tasks can be configured to be performed only once, or repeatedly through specified time intervals.
- **Execution time**: tasks can be configured to be run immediately after being set (immediate task), or at a later stage (scheduled task).

15.1.1 General process of launching a task

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

- **Task creation and configuration**: select the computers, the characteristics of the task, the time/date, the frequency, and the way it will behave in the event of an error.
- **Task publication**: once you create a task, you must activate it by entering it in the **Panda Adaptive Defense 360** task scheduler. Activated tasks will be run on the scheduled day/time.
- **Task execution**: the task will be run when the configured conditions are met.

15.2. Task creation

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

- Tasks area
- Computer tree
- Computers area
- Lists

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

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

15.3. Creating a task from the Tasks area

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

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

15.3.1 Task recipients

Click **Recipients.** A window will open for you to select the computers that will receive the configured task. Click ⊕ to add a new computer, and 🗑 to remove computers.

To access the computer selection window you must first save the task.

15.3.2 Task schedule and frequency

You can configure the following schedule options:

- **Starts:** indicates the task start time/date.
- **Maximum run time**: indicates the maximum time that the task can take to complete. After that time the task will be canceled if it is not completed.
- **Repeat**: indicates the frequency of the task from the time/date indicated in the **Starts** field**.**

Starts

- **As soon as possible (enabled)**: the task will be launched immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified if the computer is **turned off**.
- **As soon as possible (disabled)**: the task will run on the date selected in the calendar. Specify whether to take into account the computer's local time or the **Panda Adaptive Defense 360 server time.**
- **If the computer is turned off**: if the computer is turned off or cannot be accessed, the task won't run. The task scheduler lets you establish the task's expiration date, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available).
    - **Do not run**: the task is immediately canceled if the computer is not available at the scheduled time.
    - **Run the task as soon as possible, within:** lets you define the time interval during which the task will be run if the computer becomes available.

- **Run when the computer is turned on:** there is no time limit. The system waits for the computer to be available to launch the task.

Maximum run time

- **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 interval, the task will be canceled returning an error.
- **Repeat**: indicates a repeat interval (every day, month or day) from the date specified in the **Starts** field**.**

15.3.3 Task publication

Once you have created and configured a task, it will be added to the list of configured tasks. However, the task will not be active until it is published. To publish a task, click the **Publish now** button.

As soon as you publish a task, it will be added to the **Panda Adaptive Defense 360** task scheduler, which will launch the task based on its settings.

15.4. Task management

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

15.4.1 List of created tasks

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

Field	Comments	Values
Icon	The task type	📡 Patch installation task 🔍 On-demand scan task
Name	Task name	Character string
Date	Date when the task was created	Date

Table 35: fields in the 'Tasks' list

Filter tool

Field	Comments	Values
Type	The task type	Scan Disinfection Patch installation
Search task	Task name	Character string

Field	Comments	Values
Schedule	Task frequency	All Immediate One-time Scheduled
Sort list	Sorting order for the tasks on the list	Sort by creation date Sort by name Ascending Descending

Table 36: filters available in the 'Tasks' list

15.4.2 Modifying a published task

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

> *You can only change the name and description of a published task. To modify a published task, you must copy it*

Canceling a published task

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

Deleting a task

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

> *Deleting a task also deletes its results*

Copying tasks

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

Viewing a task's results

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

Table 37 shows the fields in the task table:

Field	Comment	Values
Computer	Name of the computer where the scheduled scan took place	Character string

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

Table 37: filtering parameters for task results

Table 38 displays the available search filters:

Field	Comment	Values
Date	Drop-down menu with the date when the task became 'Active' based on the configured schedule. A task will launch immediately, or wait until the target machine is available. This date is specified in the Date column.	Date
Detections	Lets you specify whether to display computers with detections or clean computers.	Binary value
Status	**Pending**: the task has not been run yet as the execution window has not been reached **In progress**: the task is underway **Success**: the task finished successfully **Failed**: the task failed and returned an error **Canceled (the task could not start at the scheduled time)** **Canceled:** the task was manually canceled **Canceled (maximum run time exceeded)** **Canceled**	Enumeration

Table 38: task search filters

Editing tasks

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

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

15.5. Updating the recipients of scheduled tasks

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

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

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

When it comes to determining which computers will receive a configured task, there are three cases depending on the task:

- Immediate tasks
- Scheduled one-time tasks
- Scheduled recurring tasks

15.5.1 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 status of the task for the affected computers will be Pending.

Adding computers to the task

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

Removing computers from the task

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

15.5.2 Scheduled one-time tasks

These are two possible scenarios with these tasks:

Tasks which started running less than 24 hours ago

During the first 24 hours after a task starts running, you can add or remove computers from the task or the target groups.

This 24-hour period is established to cover all time zones for multinational companies with a presence in several countries.

15.5.3 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 the task. Even if you add new computers to the target group, they won't receive the task. However, it will be possible to withdraw computers from the task. Taking a computer out of the target group will cancel the task on that computer.

Scheduled recurring tasks

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

The status of the task for each computer will be gradually shown as Aether Platform receives the relevant information.

16. Malware and network visibility

16.1. Introduction

Panda Adaptive Defense 360 offers administrators three large groups of tools for viewing the security status and the networks they manage:

- The dashboard, with real-time, up-to-date information
- Custom lists showing incidents, detected malware and managed devices along with their status
- Networks status reports with information collected and consolidated over time

For information about the consolidated reports, see Chapter 21 Reports

Visualization and monitoring tools determine in real time the network security status as well as the impact of any possible security breaches in order to facilitate the implementation of appropriate security measures.

16.2. Overview of the Status menu

The **Status** menu includes the main visualization tools and has several sections, which you can see below:

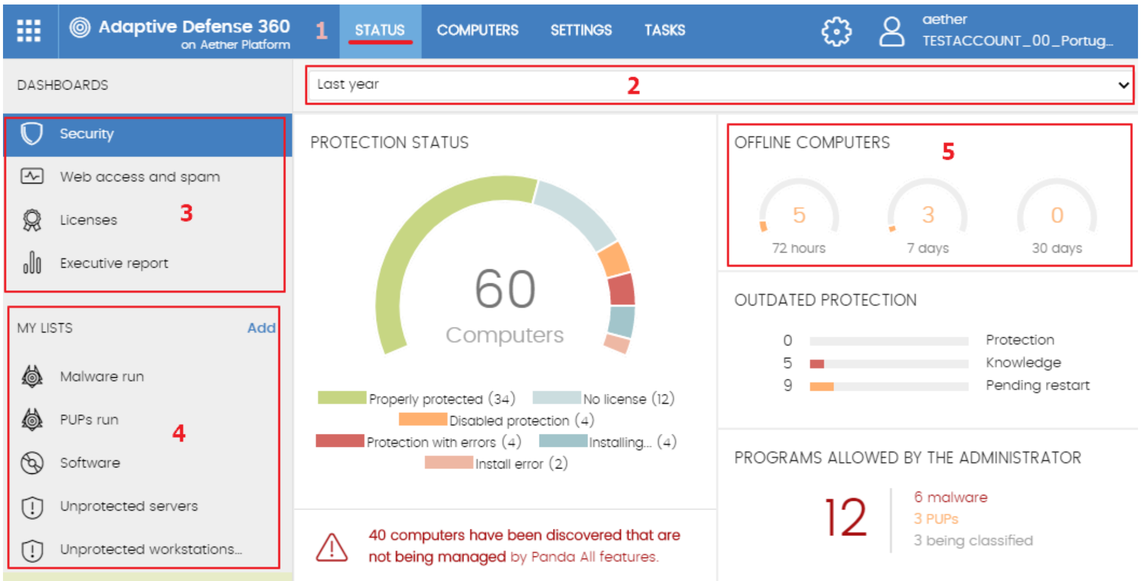


Figure 81: status window (dashboard and access to lists)

Accessing the dashboard (1)

You can access the dashboard through the **Status** menu at the top of the screen. From the dashboard you can access different widgets, as well as the lists.

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

Time period selector (2)

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

- Last 24 h
- Last 7 days
- Last month
- Last year

Not all information panels offer information for the last year. Those that don't support this option have a notice at the top to this effect.

Dashboard selector (3)

- **Security**: security status of the IT network.
- **Web access and spam**: blocking and filtering of Internet contents and unsolicited email on Microsoft Exchange servers.
- **Licenses:** refer to chapter 21 for more information about license management.
- **Executive report:** refer to chapter 21 for more information about how to configure and generate reports.

This chapter deals with the resources provided in sections **Security** and **Web and spam access**.

My lists (4)

The lists are data tables with the information presented in the panels. This includes highly detailed information and has search tools to locate the information you need.

Information panels/widgets (5)

The dashboard has a series of widgets related to a specific aspect of network security.

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

All the graphs have a key explaining the meaning of the data, and have hotspots that can be selected to display lists with predefined filters.

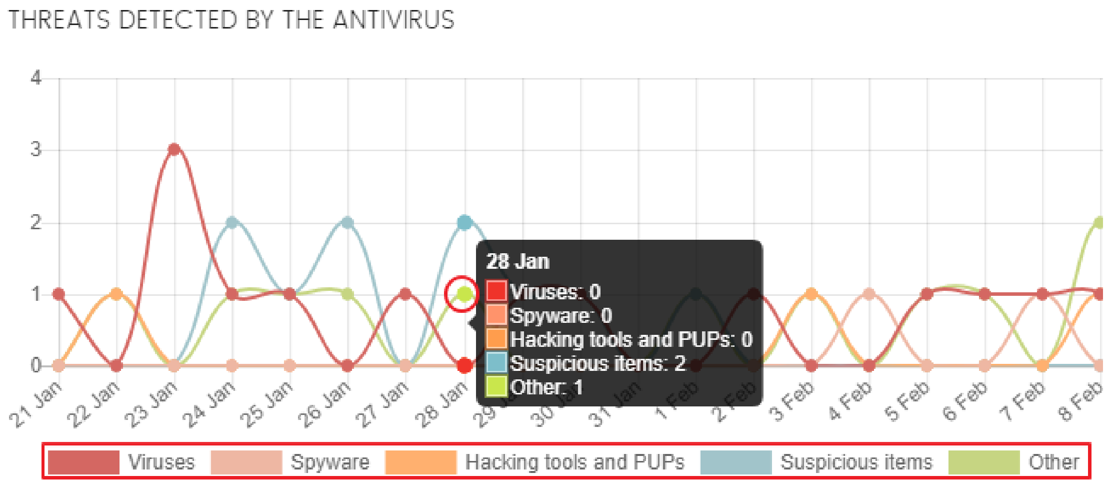


Figure 82: tooltips with detailed information and keys about the data shown

Panda Adaptive Defense 360 uses several types of graphs to display information in the most practical way based on the type of data displayed:

- Pie charts
- Histograms
- Bar charts

Click the items in the graphs to display more detailed lists.

16.3. Available panels/widgets

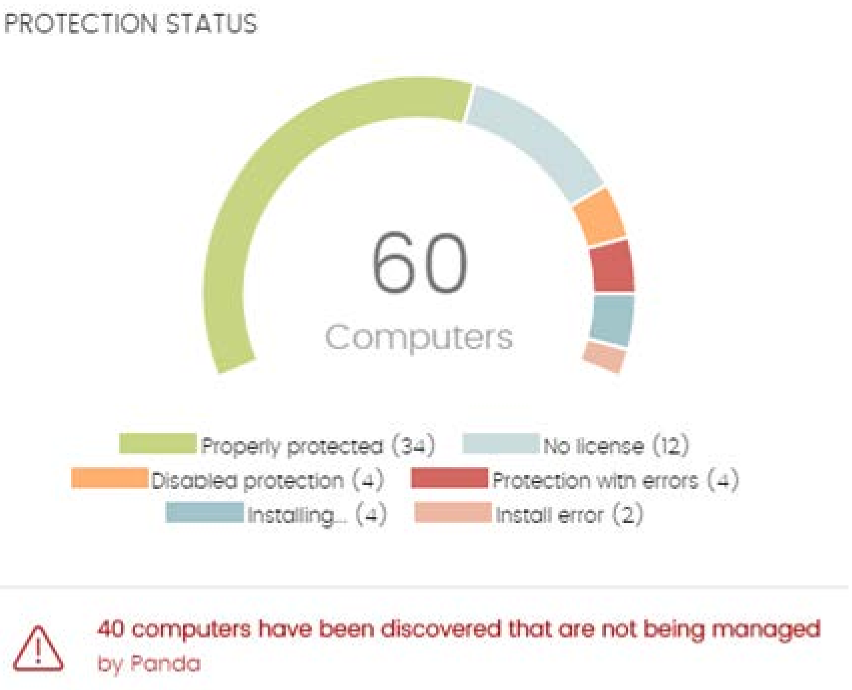
Below is a description of the different widgets displayed on the **Panda Adaptive Defense 360** dashboard, their areas and hotspots, as well as their tooltips and their meaning.

16.3.1 Protection status

Protection status shows those computers where **Panda Adaptive Defense 360** is working properly and those where there have been errors or problems installing or running the protection module. The status of the network computers is represented with a circle with different colors and associated counters.

The panel offers a graphical representation and percentage of those computers with the same status.

The sum of all percentages can be greater than 100% as the status types are not mutually exclusive. A computer can have different statuses at the same time.



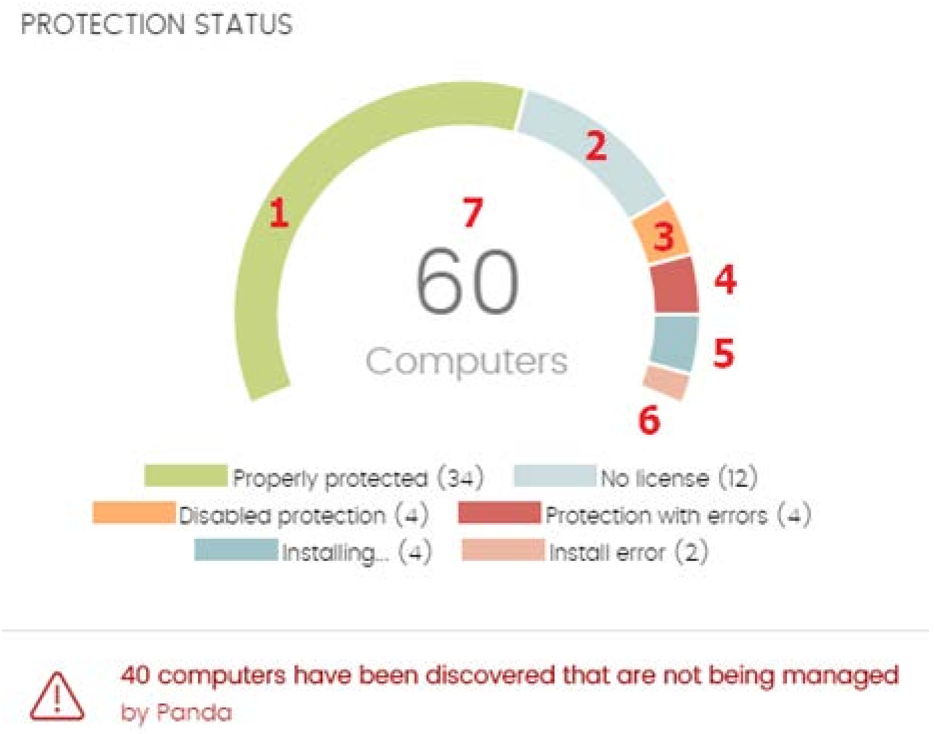
40 computers have been discovered that are not being managed by Panda

Figure 83: 'Protection status' panel

- **Meaning of the data displayed**

- **Properly protected**: indicates the percentage of computers where **Panda Adaptive Defense 360** installed without errors and is working properly.
- **Installing**: this indicates the percentage of computers on which **Panda Adaptive Defense 360** is currently being installed.
- **No license**: computers without a license are those that are not protected because there are insufficient licenses or because an available license has not been assigned to the computer.
- **Disabled protection**: these are computers that don't have the antivirus or the advanced protection enabled, if the latter is available for the operating system on that particular computer.
- **Protection with errors**: this includes computers with **Panda Adaptive Defense 360** installed, but for one reason or another the protection module is not responding to the requests from the Panda Security server.
- **Install error**: this indicates the computers on which the installation of the protection has not been properly completed.
- **Center**: the center of the pie chart indicates the total percentage of unprotected computers out of all of those visible to **Panda Adaptive Defense 360**. For a computer to be visible it must have the **Panda agent** installed.

- **Lists accessible from the panel**



40 computers have been discovered that are not being managed by Panda

Figure 84: hotspots in the 'Protection status' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Computer protection status** list filtered by **Protection status** = Properly protected
- **(2) Computer protection status** list filtered by **Protection status** = Installing...
- **(3) Computer protection status** list filtered by **Protection status** = Disabled protection
- **(4) Computer protection status** list filtered by **Protection status** = Protection with errors
- **(5) Computer protection status** list filtered by **Protection status** = No license
- **(6) Computer protection status** list filtered by **Protection status** = Install error
- **(7) Computer protection status** list without any filters

16.3.2 Offline computers

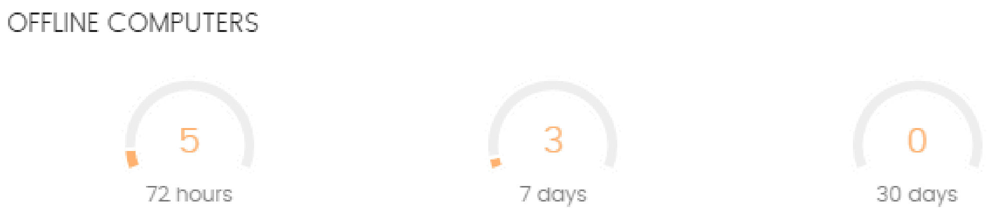


Figure 85: 'Offline computers' panel

Offline computers displays the computers that have not connected to the Panda Security cloud for a certain amount of time. Such computers are susceptible to security problems and require special attention from the administrator.

- **Meaning of the pie charts displayed**

- **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.

- **Lists accessible from the panel**

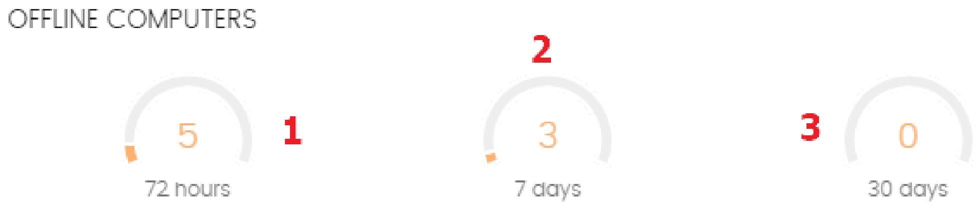


Figure 86: hotspots in the 'Offline computers' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Offline computers** list filtered by **Last connection** = More than 72 hours ago
- **(2) Offline computers** list filtered by **Last connection** = More than 7 days ago
- **(3) Offline computers** list filtered by **Last connection** = More than 30 days ago

16.3.3 Outdated protection

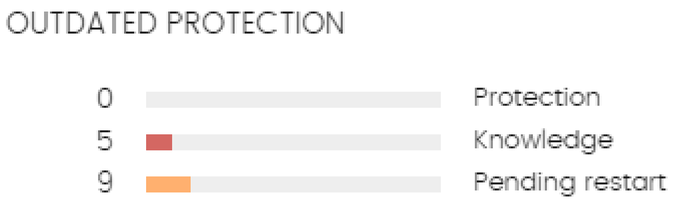


Figure 87: 'Outdated protection' panel

Outdated protection displays the computers on which the latest version of the signature file is more than three days older than the latest one released by Panda Security. It also displays the computers on which the latest version of the antivirus engine is more than seven days older than the latest one released by Panda Security. Such computers are therefore vulnerable to attacks from threats.

- **Meaning of the bars**

The panel shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts:

- **Protection**: for at least seven days the computer has had a version of the antivirus engine older than the latest one released by Panda Security.
- **Knowledge**: it has been at least three days since the computer has updated the signature file.
- **Pending restart**: the computer requires a restart to complete the update.

- **Lists accessible from the panel**

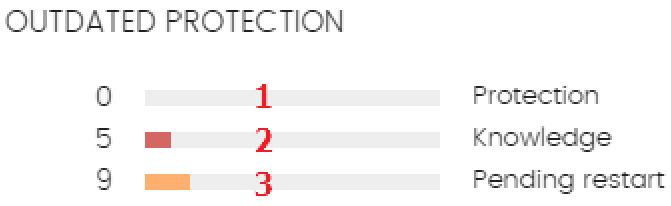


Figure 88: hotspots in the 'Outdated protection' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Computer protection status** list filtered by **Updated protection** = No
- **(2) Computer protection status** list filtered by **Knowledge** = No
- **(3) Computer protection status** list filtered by **Updated protection** = Pending restart

16.3.4 Currently blocked programs being classified

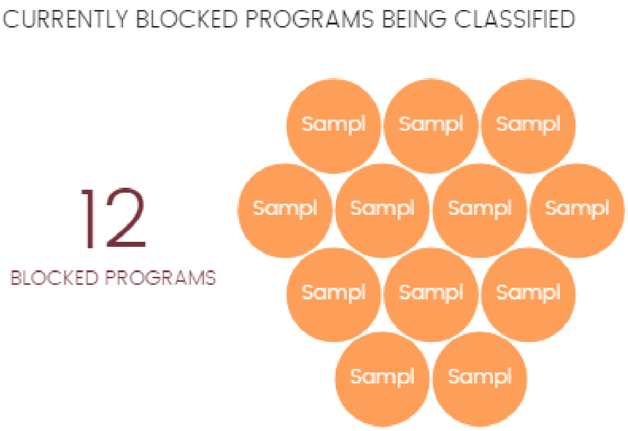


Figure 89: 'Currently blocked programs being classified' panel

The information displayed in **Currently blocked programs being classified** is a history of blocked items that have not yet been classified. It covers from the start-up of the service to the current moment, and is not affected by the administrator selecting the time period.

In the example panel, there are 12 blocked items in classification. These are 12 applications that have been blocked and are being investigated. Each one is represented by a circle.

The total number of blocked items in classification represents the different applications (different MD5s) that are being blocked. This number is regardless of the number of attempts to run the blocked application on each computer in the network.

Each version of the program (different MD5) is shown independently.

The size of the circles reflects the number of computers where the blocked unknown program was detected. In this way, a process that is run on many computers will have a single large circle allocated, compared to a process that has only been run on a single computer, which will be represented with a smaller circle.

- **Meaning of the colors used in the panel**

In the panel, blocked applications are displayed with the color code indicated below:

- **Orange**: programs with average chances of being malware.
- **Dark orange**: programs with high chances of being malware.
- **Red**: programs with very high chances of being malware.

When you hover the mouse pointer over the circle, each circle expands to show the complete name and a series of icons representing key actions:

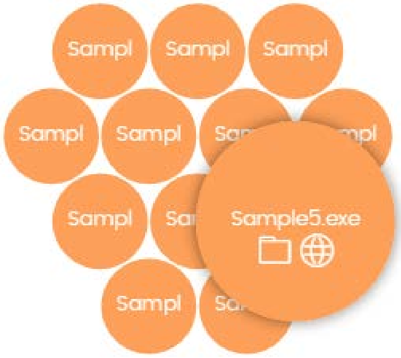


Figure 90 graphical representation of a program in the process of classification:

- **Folder**: the program has read data from the user's hard disk.
- **Globe**: the program has connected to another computer.

- **Lists accessible from the panel**

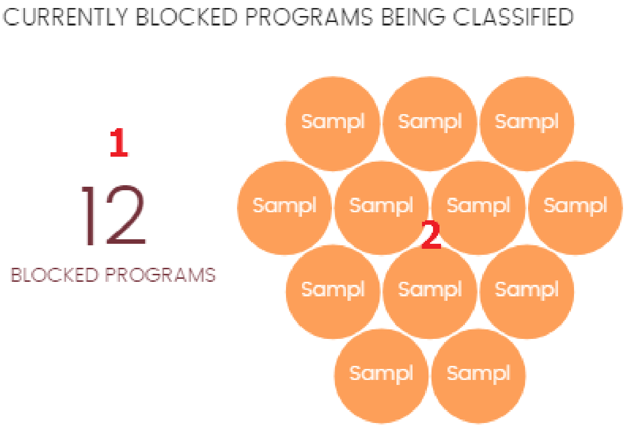


Figure 91: hotspots in the 'Currently blocked programs being classified' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Currently blocked programs being classified** list with no filters
- **(2) Currently blocked programs being classified** list filtered by **Search** = File hash

16.3.5 Programs allowed by the administrator

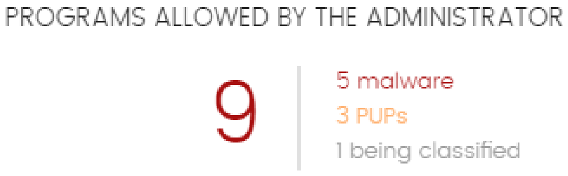


Figure 92: 'Programs allowed by the administrator' panel

Panda Adaptive Defense 360 blocks all programs classified as malware and, in addition, depending on the advanced protection settings, it can also block unknown programs until they are analyzed and given a security rating.

If a user cannot wait for this classification to be issued, or the administrator wants to allow the running of an item already classified as a threat, **Panda Adaptive Defense 360** has tools to avoid such items from being blocked.

Panda Adaptive Defense 360 allows the execution of all libraries and binaries used by the programs allowed by the administrator, except for those that are known threats.

- **Meaning of the information displayed in the panel**

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

- Malware
- PUP
- Being classified

- **Lists accessible from the panel**

- **(1) Programs allowed by the administrator** list with no filters
- **(2) Programs allowed by the administrator** list filtered by **Current classification** = Malware
- **(3) Programs allowed by the administrator** list filtered by **Current classification** = PUP
- **(4) Programs allowed by the administrator** list filtered by **Current classification** = Being classified (blocked and suspicious items)

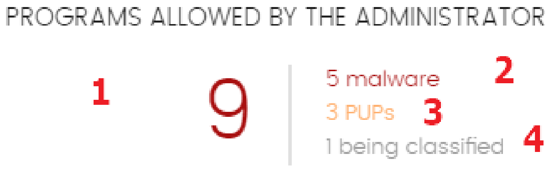


Figure 93: hotspots in the 'Programs allowed by the administrator' panel

16.3.6 Malware/PUP activity

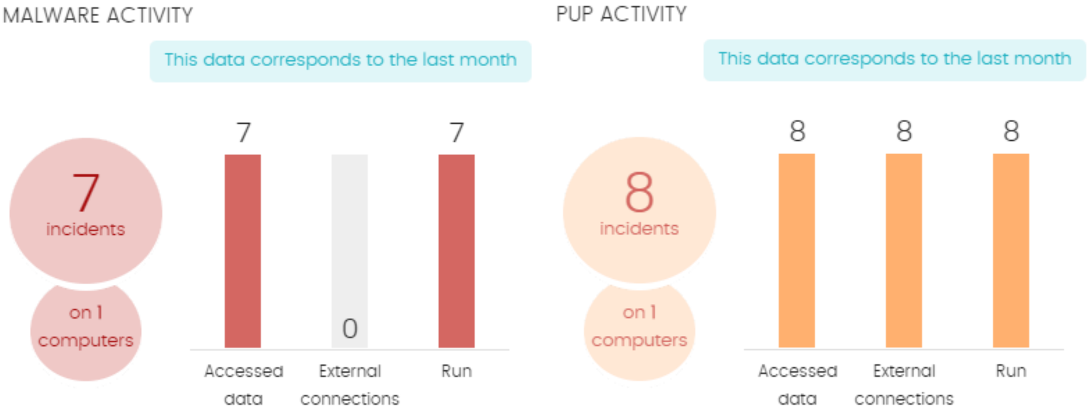


Figure 94: 'Malware/PUP activity' panel

Shows the incidents detected in the processes run by the workstations and servers on the network, as well as on their file systems. These incidents are reported both by the real-time scans as well as by the on-demand scan tasks.

Panda Adaptive Defense 360 generates an incident in the PUP/Malware Activity panel for each computer-threat-different type of threat triplet encountered on the network. If the original cause of the warning is not resolved, a maximum of two incidents will be generated every 24 hours for each computer-threat detected that requires attention.

- **Meaning of the information displayed in the panel**

- **Number of incidents/alerts & number of computers where they are detected**
- **Accessed data**: number of alerts that include one or more attempts to access user information on the computer's hard disk.
- **External connections**: number of alerts regarding connections to other computers.
- **Run**: number of malware samples run.

> *The Malware activity, PUP activity, and Exploit activity panels show data over a maximum period of one month. Should the administrator set a greater time period, an explanatory text will be displayed above the list.*

- **Lists accessible from the panel**

The lists accessible from the panel will display different information based on the hotspot clicked:

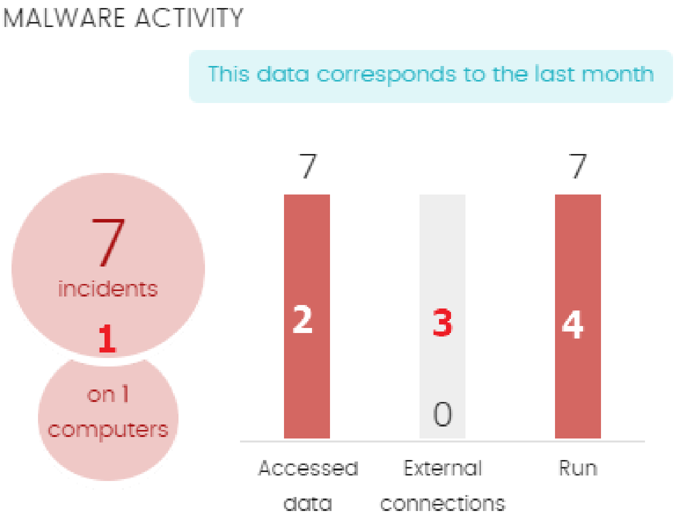


Figure 95: hotspots in the 'Malware/PUP activity' panel

- **(1) Malware activity** list filtered by **Threat type** = (Malware OR PUP)
- **(2) Malware activity** list filtered by **Accessed data** = True
- **(3) Malware activity** list filtered by **External connections** = True
- **(4) Malware activity** list filtered by **Run** = True

16.3.7 Exploit activity

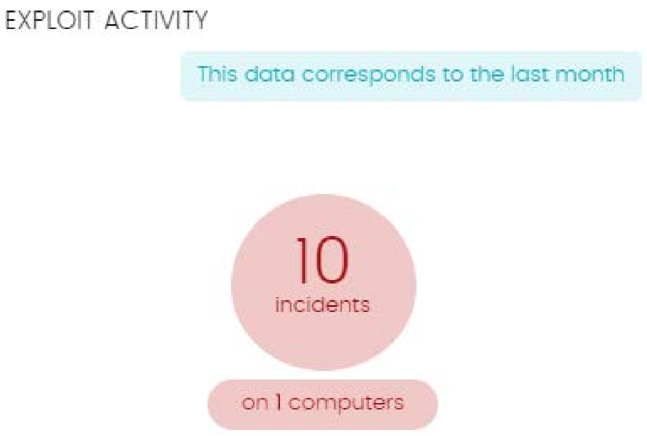


Figure 96: 'Exploit activity' panel

The Exploit activity panel shows the number of vulnerability exploit attacks suffered by the Windows computers on the network. **Panda Adaptive Defense 360** reports an incident in the Exploit activity panel for each computer/different exploit attack pair found on the network. If an attack is repeated, a maximum of 10 incidents will be reported every 24 hours for each computer-exploit pair found.

- **Meaning of the information displayed in the panel**

- **Number of incidents/attacks & number of computers where they are detected**

- **Lists accessible from the panel**

Regardless of where you click in the panel, the list displayed will show a list of all the exploits detected across the network with no filters.

16.3.8 Classification of all programs run and scanned

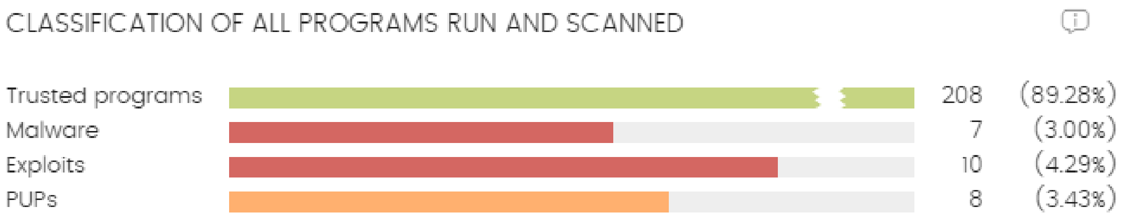


Figure 97: 'Classification of all programs run and scanned' panel

The purpose of this panel is to quickly display the percentage of goodware and malware items seen and classified on the customer's network during the time period selected by the administrator.

- **Meaning of the bars used in the panel**

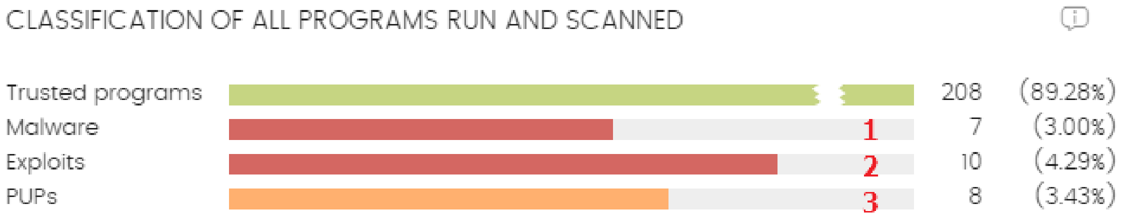
The panel displays four horizontal bars, along with the number of events associated with each category and a percentage over the total number of events.

> *The data in this panel corresponds to the entire IT network, not only to those computers that the administrator has permissions on based on the credentials used to log in to the console. Unclassified items are not shown in the panel.*

- **Trusted programs**: applications seen on the customer's network which have been scanned and classified as goodware.
- **Malicious programs:** programs that attempted to run or were scanned in the selected period, and were classified by **Panda Adaptive Defense 360** as malware or a targeted attack.
- **Exploits**: number of attempts to exploit the applications installed across the network.
- **PUPs:** programs that attempted to run or were scanned in the selected period, and were classified by **Panda Adaptive Defense 360** as a PUP (Potentially Unwanted Program).

- **Lists accessible from the panel**

The lists accessible from the panel will display different information based on the hotspot clicked:



CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED

Trusted programs	208	(89.28%)
Malware	7	(3.00%)
Exploits	10	(4.29%)
PUPs	8	(3.43%)

Figure 98: hotspots in the 'Classification of all programs run and scanned' panel

Click the **Malicious programs**, **Exploits** and **PUPs** bars to display the following information:

- **(1) Malware activity** list with no preconfigured filters
- **(2) Exploit activity** list with no preconfigured filters
- **(3) PUP activity** list with no preconfigured filters

16.3.9 Threats detected by the antivirus

Threats detected by the antivirus consolidates all the intrusion attempts that **Panda Adaptive Defense 360** has dealt with in the selected time period.

The data covers all infection vectors and all supported platforms, so administrators are able to get specific data (volume, type, form of attack) related to the malware that reached the network during a selected period of time.

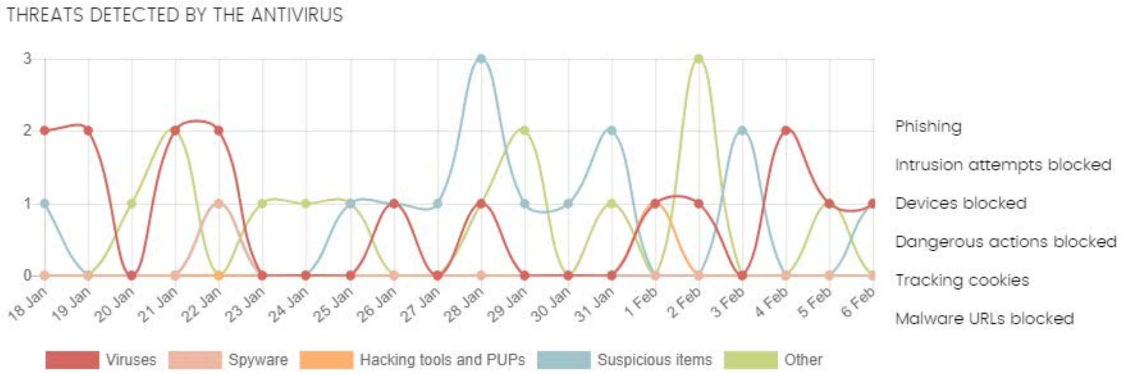


Figure 99: 'Threats detected by the antivirus' panel

- **Meaning of the information displayed in the panel**

This panel comprises two sections: a line chart and a summarized list.

The line chart represents detections on the network over time, split into malware categories:

- Viruses and spyware
- Hacking tools and PUPs
- Suspicious items
- Phishing
- Other

The Y axis shows events and the X axis dates.

The list on the right shows the events that the administrator may want to review in order to look for symptoms or potentially dangerous situations.

- **Intrusion attempts blocked**: these are attacks that are blocked by the firewall and the intrusion prevention system
- **Devices blocked**: peripheral devices blocked by the device control feature
- **Dangerous operations blocked**: detections made by scanning local behavior
- **Tracking cookies**: detection of cookies used to track users' Web activity
- **Malware URLs blocked**: web addresses that lead to pages containing malware

- **Lists accessible from the panel**

The lists accessible from the panel will display different information based on the hotspot clicked:

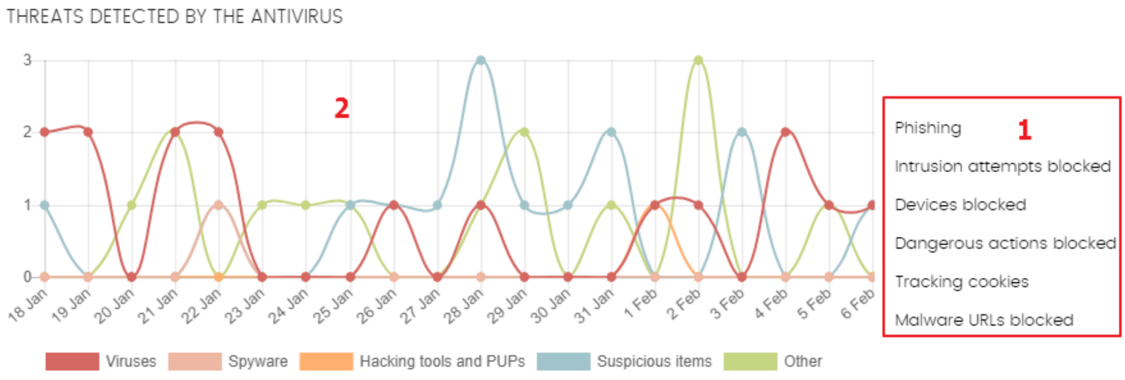


Figure 100: hotspots in the 'Threats detected by the antivirus' panel

- **(1) Threats detected by the antivirus** list filtered by **Threat type** = (Phishing OR Intrusion attempts blocked OR Devices blocked OR Dangerous operations blocked OR Tracking cookies OR Malware URLs)
- **(2) Threats detected by the antivirus** list with no filters

16.3.10 Content filtering for Exchange servers

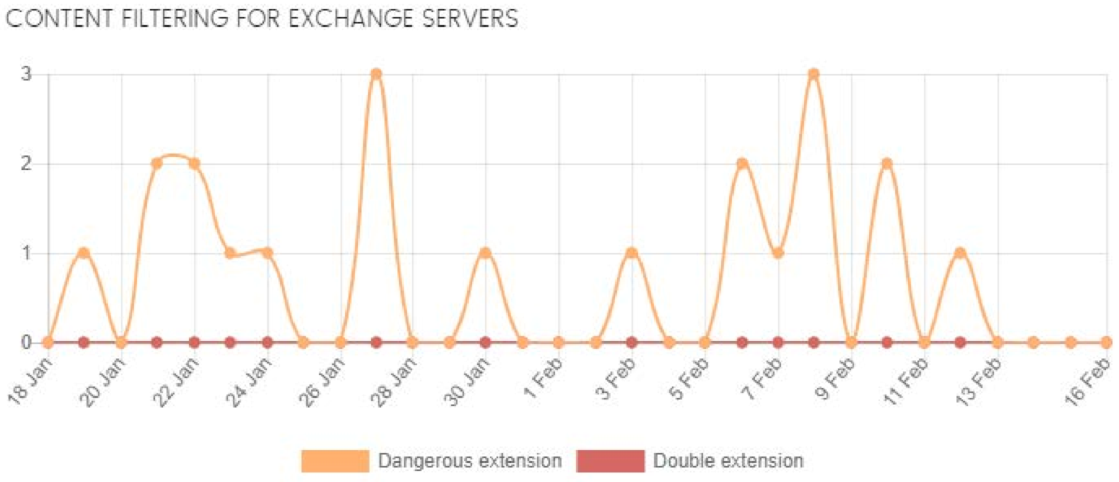


Figure 101: 'Content filtering for Exchange servers' panel

This panel shows the number of messages blocked by the Exchange Server content filter.

- **Meaning of the information displayed in the panel**

This shows two types of data: the number of messages filtered for having a dangerous extension, and for having a double extension.

Hover the mouse pointer over the chart to display a tooltip with the following information:

- **Dangerous extension**: the number of messages filtered for having an attachment with a dangerous extension.

- **Double extension**: the number of messages filtered for having an attachment with a double extension.

16.3.11 Web access

This panel displays a pie chart with the different Web page categories requested by network users.

- **Meaning of the information displayed in the panel**

The pie chart shows the 10 most important Web page categories that **Panda Adaptive Defense 360** identifies when categorizing the pages visited by network users:

- Hate and intolerance
- Criminal activity
- Job search
- Dating and personals

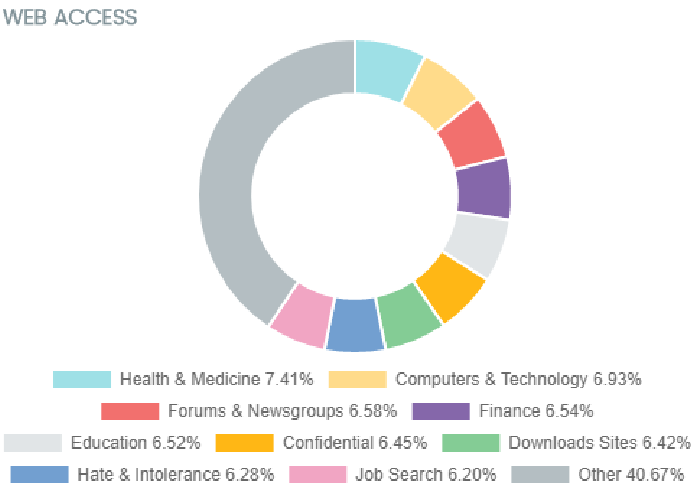


Figure 102: 'Web access' panel

- Finance
- Confidential
- Entertainment
- Government
- Illegal drugs
- Other

The pie chart key shows the percentage of Web page requests for each category.

- **Lists accessible from the panel**

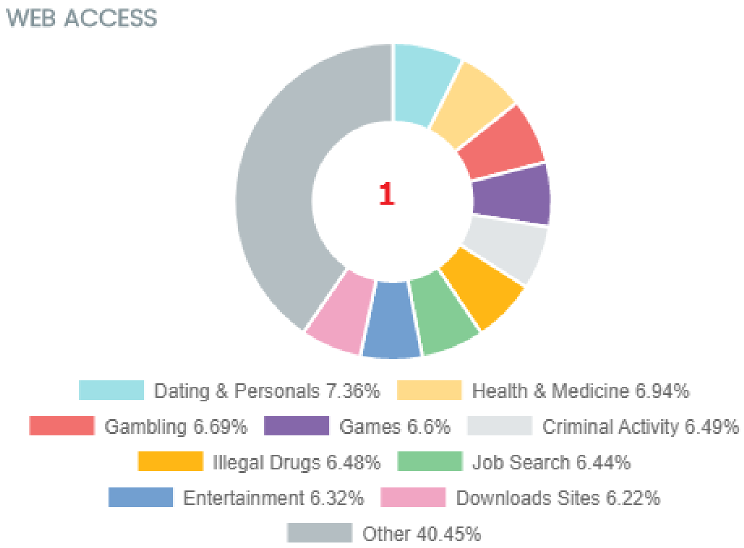
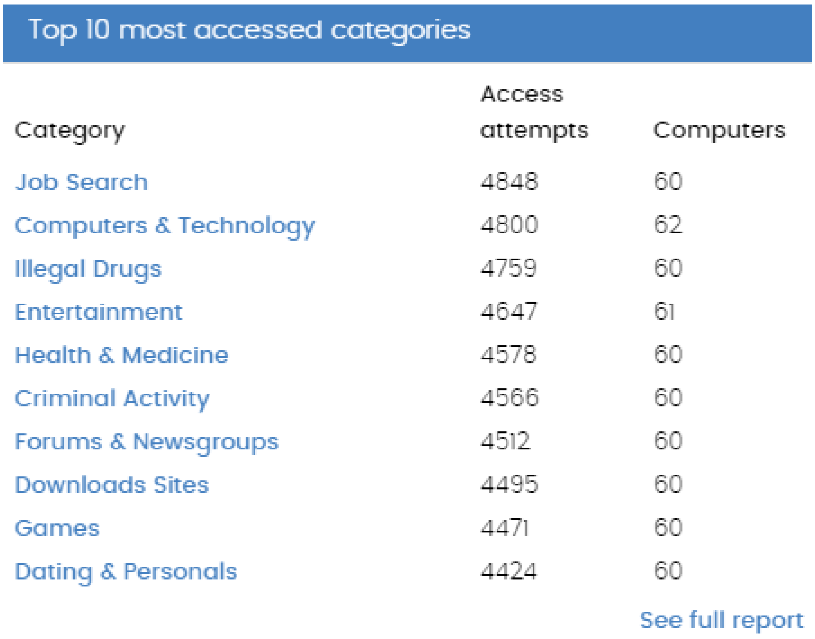


Figure103: hotspots in the 'Web access' panel

- **(1) Web access by computer** list filtered by **Category** = Selected category

16.3.12 Top 10 most accessed categories



Top 10 most accessed categories

Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60

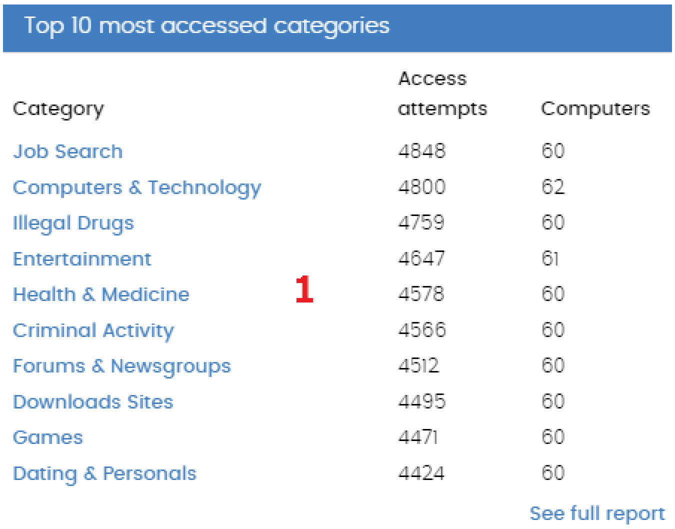
See full report

Figure 104: 'Most accessed categories' panel

This displays the number of visits and the number of computers that have accessed the ten most visited Web page categories.

Each category gives the total number of visits in the selected date range, and the number of computers that have accessed one or more times.

- **Lists accessible from the panel**



Top 10 most accessed categories

Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60

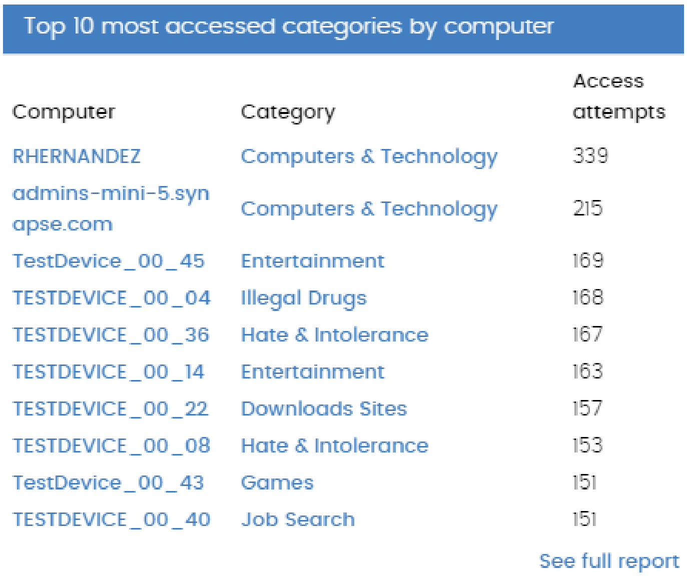
See full report

Figure 105: hotspots in the 'Top ten most accessed categories' panel

The lists accessible from the panel will display different information based on the hotspot clicked:

- **(1) Web access by computer** list filtered by **Category** = Selected category
- **(2) Web access by computer** list with no filters

16.3.13 Top 10 most accessed categories by computer



Top 10 most accessed categories by computer

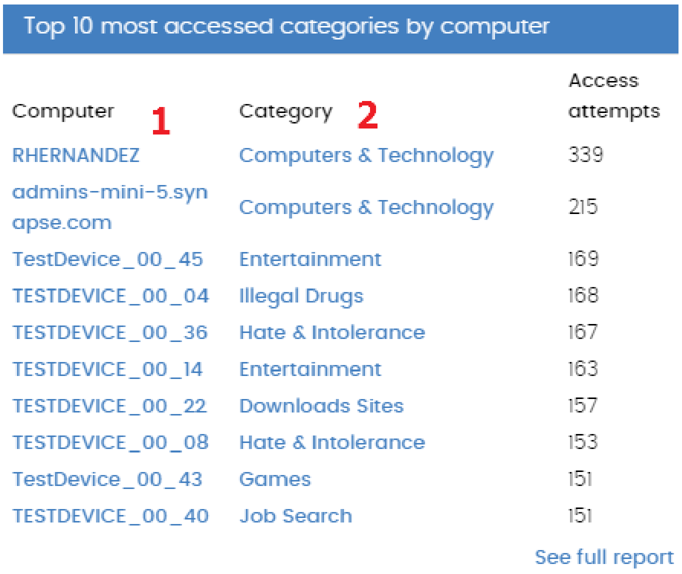
Computer	Category	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

See full report

Figure 106: 'Top 10 most accessed categories by computer' panel

This displays the number of Web page visits, ordered by category, of the ten computers that have used the Web most.

- **Lists accessible from the panel**



Top 10 most accessed categories by computer

Computer	Category	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

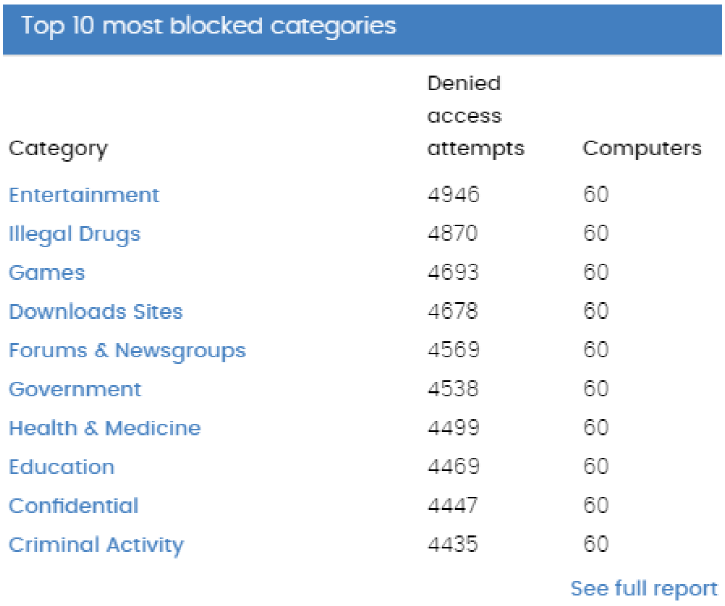
See full report

Figure 107: hotspots in the 'Top 10 most accessed categories by computer' panel

The lists accessible from the panel will display different information based on the hotspot clicked.

- **(1) Web access by computer** list filtered by **Computer** = Selected computer
- **(2) Web access by computer** list filtered by **Category** = Selected category

16.3.14 Top 10 most blocked categories



Top 10 most blocked categories

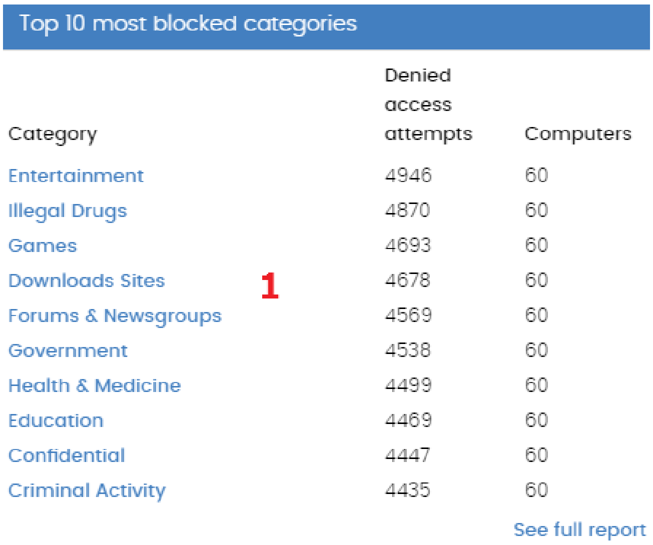
Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

See full report

Figure 108: 'Top ten most blocked categories' panel

This panel indicates the ten most frequently blocked Web page categories, along with the number of access attempts blocked, and the number of computers that attempted to access and were blocked.

- **Lists accessible from the panel**



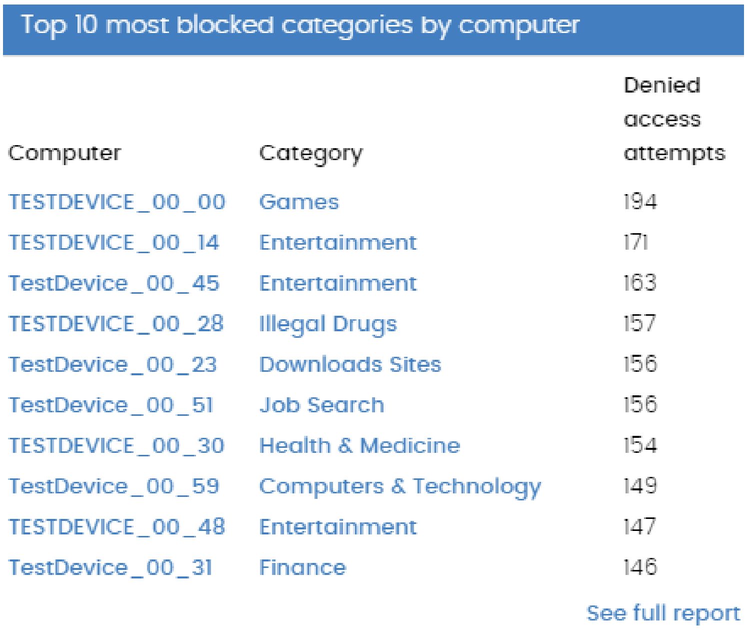
Top 10 most blocked categories

Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

Figure 109: hotspots in the 'Top 10 most blocked categories' panel

- **(1) Web access by computer** list filtered by **Computer** = Selected computer

16.3.15 Top ten most blocked categories by computer



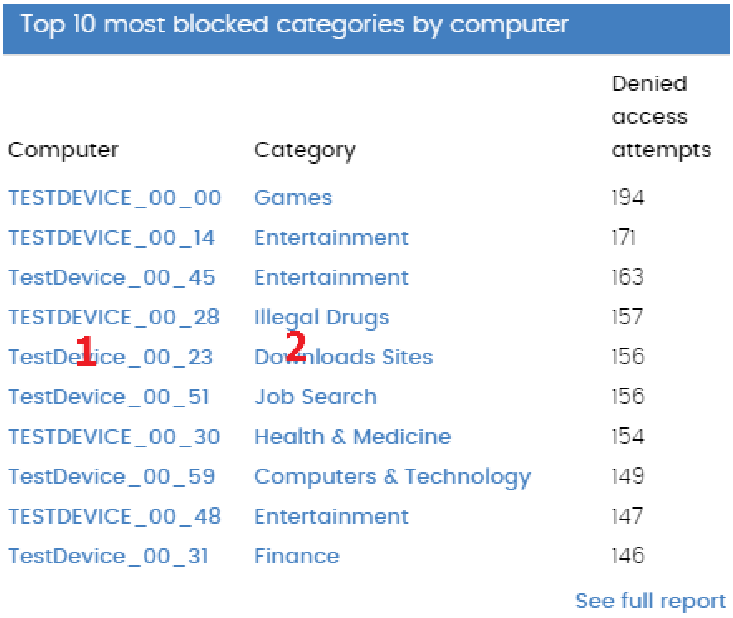
Top 10 most blocked categories by computer

Computer	Category	Denied access attempts
TESTDEVICE_00_00	Games	194
TESTDEVICE_00_14	Entertainment	171
TestDevice_00_45	Entertainment	163
TESTDEVICE_00_28	Illegal Drugs	157
TestDevice_00_23	Downloads Sites	156
TestDevice_00_51	Job Search	156
TESTDEVICE_00_30	Health & Medicine	154
TestDevice_00_59	Computers & Technology	149
TESTDEVICE_00_48	Entertainment	147
TestDevice_00_31	Finance	146

Figure 110: 'Top 10 most blocked categories by computer' panel

This panel shows the computer-category combinations with the most Web page visits blocked, indicating the name of the computer, the category, and the number of access attempts denied for each computer-category combination.

- **Lists accessible from the panel**



Top 10 most blocked categories by computer

Computer	Category	Denied access attempts
TESTDEVICE_00_00	Games	194
TESTDEVICE_00_14	Entertainment	171
TestDevice_00_45	Entertainment	163
TESTDEVICE_00_28	Illegal Drugs	157
TestDevice_00_23	Downloads Sites	156
TestDevice_00_51	Job Search	156
TESTDEVICE_00_30	Health & Medicine	154
TestDevice_00_59	Computers & Technology	149
TESTDEVICE_00_48	Entertainment	147
TestDevice_00_31	Finance	146

See full report

Figure 111: hotspots in the 'Top ten most blocked categories by computer' panel

- **(1) Web access by computer** list filtered by **Computer name** = Selected computer
- **(2) Web access by computer** list filtered by **Category** = Selected category

16.4. Introduction to the lists

Panda Adaptive Defense 360 structures the information collected at two levels: a first level that presents the data graphically in panels or widgets, and a second, more detailed level, where the data is presented in tables. Most of the tables have an associated list so that the administrator can quickly access the information in a graph and then get more in depth data if required from the lists.

16.4.1 Templates, settings and views

The **Panda Adaptive Defense 360** lists are, in effect, *templates*, that allow one or more *settings*. A list can be thought of as the source of data about a specific area.

Settings are values specifically assigned to the search tools and filters associated to each template.

The *settings* of a *template* result in a list which the administrator can edit and consult later. This way, administrators can save time defining searches and filters about *Lists* which they can use again later.

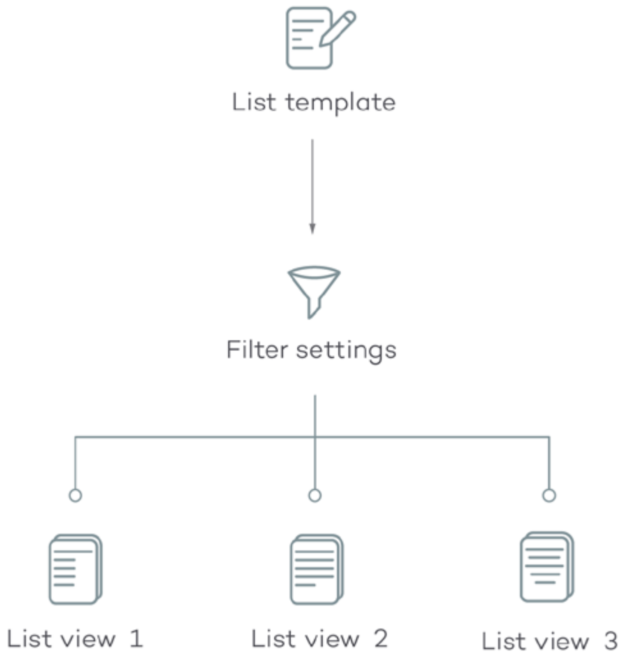


Figure 112: generating three lists from the same template/data source

List templates

There are eleven templates that correspond to the types of information displayed below:

- Threats detected by the antivirus
- Intrusion attempts blocked
- Devices blocked
- Malware and PUP activity
- Exploit activity
- Currently blocked programs in the process of classification
- Access to Web pages by category
- Access to Web pages by computer
- Computer protection status
- Licenses
- Unmanaged computers discovered

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

Settings

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

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

List view/Lists

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

16.4.2 My lists panel

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

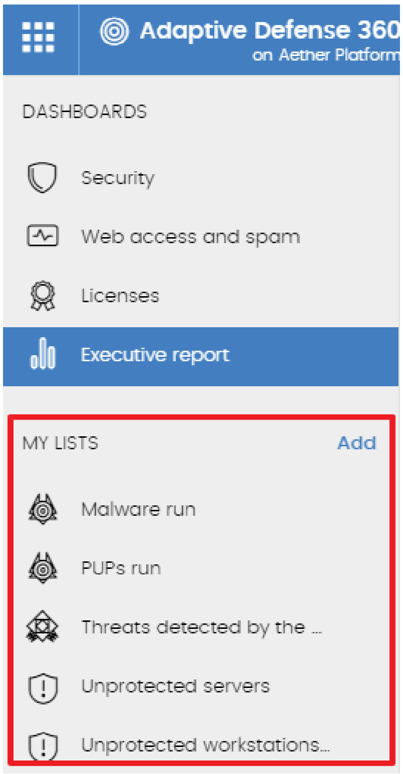


Figure 113: 'My lists' side panel

16.4.3 Creating custom lists

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

- **From the My lists side menu**

Click **Add** in the panel on the left to display a window with a drop-down menu with the eleven available templates.

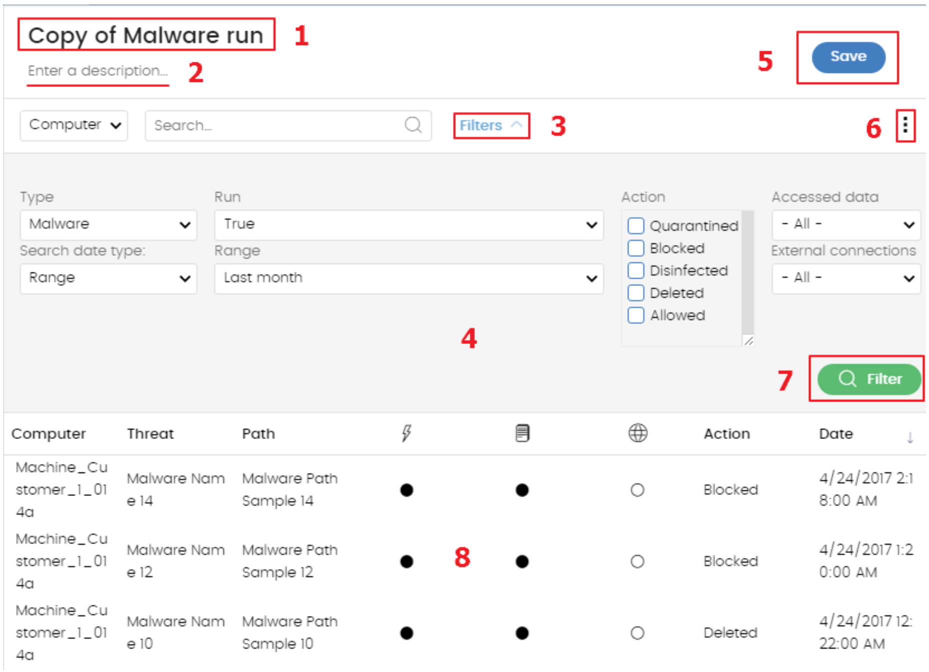
- **From a dashboard panel**

- Click a widget on the dashboard to open its associated template.

- Click its context menu **(6)** and select **Copy**. A new list will be created. (Figure 115)
- Edit the list filters, name and description and click **Save (5).**

- **From an existing list**

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



Copy of Malware run

Enter a description...

Computer

Search...

Type: Malware

Run: True

Search date type: Range

Range: Last month

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

Accessed data: - All -

External connections: - All -

Computer	Threat	Path				Action	Date
Machine_Customer_1_014a	Malware Name 14	Malware Path Sample 14	●	●	○	Blocked	4/24/2017 21:8:00 AM
Machine_Customer_1_014a	Malware Name 12	Malware Path Sample 12	●	●	○	Blocked	4/24/2017 12:0:00 AM
Machine_Customer_1_014a	Malware Name 10	Malware Path Sample 10	●	●	○	Deleted	4/24/2017 12:22:00 AM

Figure 114: overview of a list

- **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 view will be created which you can edit according to your preferences.

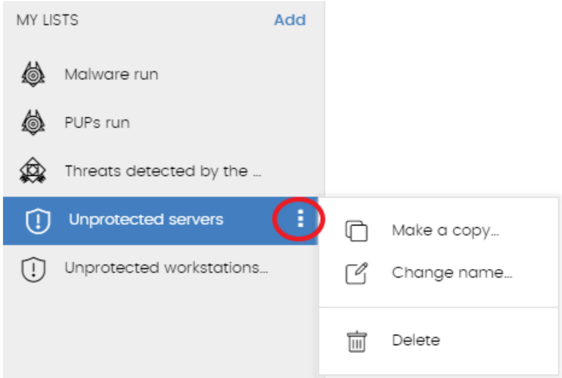


Figure 115: context menu of the lists available in the 'My lists' panel

16.4.4 Deleting a list

There are two different ways to delete a list:

- **From the My lists panel**

- From the **My lists** panel, click the context menu of the list you want to delete.
- Click the 🗑 icon.

- **From the list itself**

- Click the list's context menu **(6)**
- Click the 🗑 icon from the drop-down menu displayed.

16.4.5 Configuring a custom list

To define a new list, follow the steps below:

- Assign a new name to the list **(1).** By default, the console creates a new name for the list by adding the string “New” to the type of list, or “Copy” if the list is a copy of a previous one.
- Assign a description **(2)**: this step is optional.
- Click the link **Filters (3)** to display the settings and search section.
- Set the data filter **(4)** to display the relevant details.
- Click **Filter (7)** to apply the configured filter in order to check if it meets your needs. The search result will be displayed in the list **(8)**.
- Click **Save (5)**. The list will be added to the panel on the left under **My lists**, and can be accessed by clicking on the name.

Also, in the menu button **(6)** there is an option to export the list to CSV format and to make a copy of it.

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

16.4.6 Available actions on computers in lists

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

16.5. Available lists

16.5.1 'Computer protection status' list

This list displays all the network computers in detail, with filters that let you locate those workstations or mobile devices that are not protected due to one of the reasons displayed in the panel.

Field	Comments	Values
Computer	Name of the unprotected computer	Character string
Advanced protection **Antivirus**	Status of the advanced protection Status of the antivirus protection	☁ Not installed ☒ Error ☑ Enabled ⚠ Disabled ∅ No license
Updated protection	Indicates whether the installed protection is updated to the latest version released Hover the mouse pointer over the field to see the version of the installed protection	✓ Updated ✗ Not updated (7 days without updating since last release) ! Pending restart
Knowledge	Indicates whether the signature file installed on the computer is updated to the latest version Hover the mouse pointer over the field to see the date of the latest version installed	✓ Updated ✗ Not updated (3 days without updating since last release)
Last connection	Date of the last time that the Panda Adaptive Defense 360 status was sent to the Panda Security cloud.	Date

Table 39: fields in the 'Computer protection status' list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server

Field	Comments	Values
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 Adaptive Defense 360 folder tree to which the computer belongs	Character string
Agent version		Character string
Installation date	Date on which the Panda Adaptive Defense 360 software was successfully installed on the computer	Date
Last update on	Date the agent was last updated	Date
Platform	Operating system installed on the computer	Windows Linux macOS Android
Operating system	Operating system installed on the computer, internal version and patches applied	Character string
Exchange Server	Version of the mail server installed	Character string
Protection updated	Indicates whether the installed protection has the latest version released	Binary value
Protection version	Internal version of the protection module	Character string
Knowledge updated	Indicates whether the signature file installed on the computer is the latest version	Binary value
Last update on	Date the signature file was last updated	Date
Advanced protection **File antivirus** **Mail antivirus** **Web browsing antivirus** **Firewall protection** **Device control** **Antivirus for Exchange Server** **Anti-spam for Exchange Server** **Web access control**	Protection status	Not installed Error Enabled Disabled No license

Table 40: fields in the 'Computer protection status' exported file

Filter tool

Field	Comments	Values
Computer type	Type of device	Workstation Laptop Mobile device Server
Find computer	Computer name	Character string
Last connection	Last time that the Panda Adaptive Defense 360 status was sent to the Panda Security cloud	All More than 72 hours More than 7 days More than 30 days
Protection updated	Indicates whether the installed protection has the latest version released	All Yes No Pending restart
Platform	Operating system installed on the computer	All Windows Linux Mac Android
Knowledge	Update status of the antivirus protection signature file	Binary value
Reason why the computer is unprotected		Not installed Protection with errors Enabled Protection disabled No license No protection

Table 41: filters available in the 'Computer protection status' list

16.5.2 'Currently blocked programs being classified' list

This list shows those files in which **Panda Adaptive Defense 360** has preliminarily detected some risk despite their classification is not fully complete. These files are blocked during the time it takes to fully classify them.

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Path	Name of the unknown file and its path on the user's computer	Character string

Field	Comments	Values
Accessed data	The unknown file accessed files located on the user's computer	Binary value
Made external connections	The unknown file has communicated with remote computers to send or receive data	Binary value
Protection mode	Operating mode of the advanced protection when the unknown file was detected	Audit Hardening Lock
Likelihood of being malicious	Likelihood that the unknown file is actually malware	Medium, High, Very High
Date	Date when the unknown file was first seen	Date

Table 42: fields in the 'Currently blocked programs' list

Fields displayed in the exported file

Refer to chapter 18 Forensic analysis for more information about this file

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Threat	Name of the unknown file	Character string
Path	Name of the unknown file and its path on the user's computer	Character string
Protection mode	Operating mode of the protection when the unknown file was detected	Audit Hardening Lock
Accessed data	The unknown file has accessed data on the user's computer	Binary value
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary value
Likelihood of being malicious	Probability that the unknown file turns out to be malicious	Medium, High, Very high
Date	Date the unknown file was first detected	Date
Dwell time	Time that the file has been on the customer's network without	Date

Field	Comments	Values
	classification	
User	User account under which the file was run	Character string
Hash	String identifying the file	Character string
Source computer	Displays the name of the computer the blocked program came from, if applicable	Character string
Source IP address	Displays the IP address of the computer the blocked program came from, if applicable	Character string
Source user	The user that was logged in on the computer that the blocked program came from	Character string

Table 43: fields in the 'Currently blocked files' exported file

Filter tool

Field	Comments	Values
Search date type	**Range**: lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month
Search	**Computer**: device on which the unknown item was detected **Threat:** file name **Hash**: string that identifies the file **Source**: allows you to search by the user, IP address or name of the computer that the blocked item came from	Character string
Protection modes	Operating mode of the advanced protection when the unknown file was detected	Hardening Lock
Accessed data	The unknown file has accessed data on the user's computer	Binary value
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary value

Table 44: filters available in the 'Currently blocked programs' list

16.5.3 'History of blocked programs' list

This list shows a history of all threats and unknown files in the process of classification that have been allowed to run by the administrator.

This list is not accessible through any panels in the dashboard. To access it, click the **History** link on the **Currently blocked programs being classified** screen.

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Path	Name of the unknown file and its path on the user's computer	Character string
Action	Action taken by Panda Adaptive Defense 360	Blocked Reclassified as GW Reclassified as MW Reclassified as PUP
Accessed data	The unknown file accessed files located on the user's computer	Binary value
Made external connections	The unknown file has communicated with remote computers to send or receive data	Binary value
Protection mode	Operating mode of the advanced protection when the unknown file was detected	Audit Hardening Lock
Excluded	The unknown file has been unblocked/excluded by the administrator, allowing it to run	Binary value
Likelihood of being malicious	Likelihood that the blocked item is actually malware	Medium, High, Very High
Date	Date when the unknown file was first seen	Date

Table 45: fields in the 'History of blocked programs' list

Fields displayed in the exported file

Refer to chapter 18 Forensic analysis for more information about this file

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Threat	Name of the unknown file	Character string

Field	Comments	Values
Path	Path of the unknown file on the user's computer	Character string
Protection mode	Operating mode of the advanced protection when the unknown file was detected	Audit Hardening Lock
Action	Action taken by Panda Adaptive Defense 360	Blocked Reclassified as GW Reclassified as MW Reclassified as a PUP
Accessed data	The unknown file has accessed data on the user's computer	Binary value
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary value
Excluded	The unknown file has been unblocked/excluded by the administrator to allow it to run	Binary value
Likelihood of being malicious	Probability that the unknown file turns out to be malicious	Medium, High, Very high
Date	Date the unknown file was first detected	Date
Dwell time	Time that the file has been on the customer's network without classification	Date
User	User account under which the file was run	Character string
Hash	String identifying the file	Character string
Source computer	Name of the computer the blocked program came from, if applicable	Character string
Source IP address	IP address of the computer the blocked program came from, if applicable	Character string
Source user	The user that was logged in on the computer that the blocked program came from	Character string

Table 46: fields in the 'History of blocked programs' exported file

Filter tool

Field	Comments	Values
Search	**Computer**: device on which the unknown file was detected **Threat**: name of the threat **Hash**: string that identifies the file	Character string

Field	Comments	Values
	Source: allows you to search by the user, IP address or name of the computer that the blocked item came from	
Range	Lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month
Action	Action taken by Panda Adaptive Defense 360	Blocked Reclassified as GW Reclassified as MW Reclassified as PUP
Excluded	The unknown file has been unblocked/excluded by the administrator so it can be run	Binary value
Protection mode	Operating mode of the advanced protection when the unknown file was detected	Hardening Lock
Accessed data	The unknown file has accessed data on the user's computer	Binary
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary

Table 47: filters available in the 'History of blocked programs' list

16.5.4 'Programs allowed by the administrator' list

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

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

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead	Character string
Type	Type of file	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
File	Name of the unknown file or file that contains the threat	Character string

Field	Comments	Values
Hash	String identifying the file	Character string
Allowed by	Console user that created the exclusion	Character string
Allowed since	Date when the administrator created the file exclusion	Date
Delete 🗑	Lets you revoke the file exclusion	

Table 48: fields in the 'Programs allowed by the administrator' list

Fields in the exported file

Fields	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead	Character string
Current type	Type of file at the time the list is accessed	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
Original type	Type of file at the time it was first allowed to be blocked	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Allowed by	Console user that created the exclusion	Character string
Allowed since	Date that the administrator created the file exclusion	Date

Table 49: fields in the 'Programs allowed by the administrator' exported file

Filter tool

Field	Comments	Values
Search	**Threat**: name of the malware or PUP **Allowed by**: console user that created the exclusion **File**: name of the file containing the threat **Hash**: string that identifies the file	Character string
Current classification	File classification at the time the list is accessed	Malware PUP

Field	Comments	Values
		Goodware Being classified (Blocked and suspicious)
Original classification	File classification at the time it was first blocked	Malware PUP Blocked Suspicious

Table 50: filters available in the 'Programs allowed by the administrator' list

16.5.5 'History of Programs allowed by the administrator' list

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

This list doesn't have a corresponding panel in the dashboard. To access it, click the **History** link in the **Programs allowed by the administrator** window.

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Type	Type of threat allowed to run	Malware PUP Blocked Suspicious
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Action	Action taken on the allowed item	Exclusion removed by the user Exclusion removed after reclassification Exclusion added by the user Exclusion kept after reclassification
User	User account under which the relevant action was taken	Character string
Date	Date the event took place	Date

Table 51: fields in the 'History of Programs allowed by the administrator' list

Fields included in the exported file

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the	Character string

Field	Comments	Values
	name of the file will be specified instead.	
Current type	Type of threat the last time it was allowed to run.	Malware PUP Blocked Suspicious
Original type	File type when the event occurred.	
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Action	Action taken	Exclusion removed by the user Exclusion removed after reclassification Exclusion kept by the user Exclusion kept after reclassification
User	User account of the user that allowed the threat	Character string
Date	Date the event took place	Date

Table 52: fields in the 'History of Programs allowed by the administrator' exported file

Filter tool

Field	Comments	Values
Search	**User:** user account of the user that allowed the threat **File**: name of the file containing the threat **Hash**: string identifying the file	Character string
Current classification	File classification at the time the list is accessed	Malware PUP Goodware Being classified (Blocked and suspicious)
Original classification	File classification at the time it was first blocked	Malware PUP Blocked Suspicious

Field	Comments	Values
Action	Action taken on the allowed item	Exclusion removed by the user Exclusion removed after reclassification Exclusion kept by the user Exclusion kept after reclassification

Table 53: filters available in the 'History of Programs allowed by the administrator' list

16.5.6 'Malware/PUP activity' list

This shows administrators the list of threats found on the computers protected by **Panda Adaptive Defense 360**. This is necessary in order to locate the source of problems, determine the seriousness of incidents and, where necessary, take any troubleshooting measures and update the organization's security policy.

Field	Comments	Values
Computer	Name of the computer on which the threat was detected	Character string
Threat	Name of the threat detected	Character string
Path	Full path of the infected file	Character string
Already run	The threat has run and the computer could be compromised	Binary value
Accessed data	The threat has accessed data on the user's computer	Binary value
Made external connections	The threat has communicated with other computers to send or receive data	Binary value
Action	Action taken on the malware	Quarantined Blocked Disinfected Deleted Allowed
Date	Date when the threat was detected on the computer	Date

Table 54: fields in the 'Malware/PUP activity' list

Fields displayed in the exported file

Refer to chapter 18 Forensic analysis for more information about this file

Field	Comments	Values
Computer	Name of the computer on which the threat was detected	Character string
Threat	Name of the threat detected	Character string
Path	Full path of the infected file	Character string
Action	Action taken on the malware	Quarantined Blocked Disinfected Deleted Allowed
Run	The threat has run and the computer could be compromised	Binary value
Accessed data	The threat has accessed data on the user's computer	Binary value
Made external connections	The threat has communicated with other computers to send or receive data	Binary value
Excluded	The threat has been excluded by the administrator so it can be run	Binary value
Date	Date when the threat was detected on the computer	Date
Dwell time	Time that the threat has been on the network without classification	Character string
User	User account under which the threat was run	Character string
Hash	String identifying the file	Character string
Source computer	Name of the computer the infection originated from, if applicable	Character string
Source IP address	IP address of the computer the infection originated from, if applicable	Character string
Source user	The user that was logged in on the computer the infection originated from.	Character string

Table 55: fields in the 'Malware/PUP activity' exported file

Filter tool

Field	Comments	Values
Search	**Computer**: device on which the threat was detected **Threat**: name of the threat **Hash**: string that identifies the file **Infection source**: allows you to search by the user, IP address or name of the computer that the infected file came	Character string

Field	Comments	Values
	from	
Type	Type of threat	Malware PUP
Range	Lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month Last year
Run	The threat has run and the computer could be compromised	True False
Action	Action taken on the threat	Quarantined Blocked Disinfected Deleted Allowed
Accessed data	The threat has accessed data on the user's computer	Binary value
Made external connections	The threat has communicated with other computers to send or receive data	True False

Table 56: filters available in the 'Malware/PUP' activity list

16.5.7 'Exploit activity' list

Shows a list of all computers with programs compromised by vulnerability exploit attempts. The purpose of this list is to provide administrators with the necessary information to find the source of a problem, assess the severity of an incident and, if required, take the necessary remediation measures and update the company's security policies.

Panda Adaptive Defense 360 can take the following actions on detected exploits:

- **Allowed**: the exploit was allowed to run as the anti-exploit protection was configured in 'Audit' mode.
- **Blocked**: the exploit was blocked before it could run.
- **Allowed by the user**: the computer user was asked for permission to end the compromised process, but decided to let the exploit run.
- **Process ended**: the exploit has been deleted, but managed to partially run.
- **Pending restart**: the user has been informed of the need to restart their computer in order to completely remove the exploit. Meanwhile, the exploit has continued to run.

Field	Comment	Values
Computer	Name of the computer where the threat was detected	Character string
Compromised program	Program hit by the exploit attack	Character string

Field	Comment	Values
Action	Action taken on the exploit	Allowed by the user Allowed Blocked Process ended Pending restart
Exploit run	Indicates if the exploit managed to run or was blocked before it could affect the vulnerable program	Binary
Date	Date when the exploit attempt was detected on the computer	Date

Table 57: fields in the 'Exploit activity' list

Fields displayed in the exported file

Field	Comments	Values
Computer	Name of the computer where the threat was detected	Character string
Compromised program	Program hit by the exploit attack	Character string
Hash	String identifying the compromised program	Character string
Last action	Action taken on the exploit	Allowed by the user Allowed by the administrator Blocked (immediately) Blocked after the process was ended
Risk	Indicates if the computer is or has been at risk, or the exploit was blocked before it could affect the vulnerable program	Binary value
Date	Date when the exploit attempt was detected on the computer	Date

Table 58: fields in the 'Exploit activity' exported file

Filter tool

Field	Comments	Values
Search	**Computer**: device on which the threat was detected **Hash**: string that identifies the compromised program	Character string
Range	Lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month

Field	Comments	Values
Exploit run	Indicates if the exploit managed to run or was blocked before it could affect the vulnerable program	Binary value
Action	Action taken on the exploit	Allowed by the user Allowed Blocked Process ended Pending restart

Table 59: filters available in the 'Exploit activity' list

16.5.8 'Threats detected by the antivirus' list

The list of detections offers consolidated and complete information about all the detections made on all supported platforms, and from all infection vectors scanned that are used by hackers to infect computers on the network.

Field	Comments	Values
Computer	Name of the computer on which the threat was detected	Character string
IP address	The computer's primary IP address	Character string
Group	Group in the Panda Adaptive Defense 360 Groups tree that the computer belongs to	Character string 'All' group Native group Active Directory group
Threat type	Type of threat detected	Virus Spyware PUPs and hacking tools Phishing Suspicious item Dangerous operation Tracking cookie Malware URL Other
Path	File system path of the threat	Character string
Action	Action taken by Panda Adaptive Defense 360	Deleted Disinfected Quarantined Blocked Process ended
Date	Date of detection	Date

Table 60: fields in the 'Threats detected by the antivirus' list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account to which the service belongs	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Name of the computer on which the threat was detected	Character string
Malware name	Name of the threat detected	Character string
Threat type	Type of threat detected	Virus Spyware Hacking tools and PUPs Phishing Suspicious item Dangerous action Tracking cookie Malware URL Other
Malware type	Threat subclass	Character string
Number of detections	Number of times that Panda Adaptive Defense 360 detected the threat on the selected date	Number
Action	Action taken by Panda Adaptive Defense 360	Deleted Blocked Process ended
Detected by	Specifies the protection engine that made the detection	Device Control Anti-spam for Exchange Content filtering for Exchange Mailbox protection for Exchange Transport protection for Exchange File protection Firewall Email protection Adaptive Defense On-demand scans Web access control Web protection
Detection path	File system path of the threat	Character string
Excluded	The threat has been excluded from scans by the administrator so it can be run	Binary value
Date	Date of detection	Date
Group	Group in the Panda Adaptive Defense 360 Groups tree to which the computer belongs	Character string
IP address	Primary IP address of the computer where the detection was made	Character string

Field	Comments	Values
Domain	Windows domain to which the computer belongs	Character string
Description		Character string

Table 61: fields in the 'Threats detected by the antivirus' exported file

Filter tool

Field	Comments	Values
Computer	Name of the computer on which the threat was detected	Character string
Search date type	**Range**: lets you set the time period, from the current moment back **Custom date**: lets you choose a specific date from a calendar	Last 24 hours Last 7 days Last month Last year
Computer type	Type of device	Workstation Laptop Mobile device Server
Threat type	Type of threat detected	Virus Spyware Hacking tools and PUPs Phishing Suspicious item Dangerous action Tracking cookie Malware URL Other

Table 62: filters available in the 'Threats detected by the antivirus' list

16.5.9 'Blocked devices' list

This list provides details of the network computers that have restricted access to peripherals.

Field	Comments	Values
Computer	Name of the computer	Character string
IP address	The computer's primary IP address	Character string
Group	Folder in the Adaptive Defense folder tree to which the computer belongs	Character string 'All' group Native group Active Directory group

Field	Comments	Values
Type	Type of device affected by the security settings	Removable storage drive Imaging device CD/DVD drive Bluetooth device Modem Mobile device
Action	Action taken on the device	Block Allow read access Allow read & write access
Date	Date and time when the action was taken	Date

Table 63: fields in the 'Blocked devices' list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Computer name	Character string
Name	Name of the peripheral connected to the computer and affected by the security settings	Character string
Instance ID	ID of the affected device	Character string
Number of detections	Number of times a disallowed action has been detected on the device	Numeric value
Action	Action taken on the device	Block Allow read access Allow read & write access
Detected by	Module that detected the disallowed operation	Device Control
Date	Date when the disallowed operation was detected	Date
Group	Folder in the Adaptive Defense folder tree to which the computer belongs	Character string
IP address	The computer's primary IP address	Character string
Domain	Windows domain the computer belongs to	Character string

Table 64: fields in the 'Blocked devices' exported file

Filter tool

Field	Comments	Values
Computer type	Type of device	Workstation Laptop Mobile device Server
Find computer	Computer name	Character string
Search date type	**Range**: lets you set the time period, from the current moment back **Custom range**: lets you choose a specific date from a calendar	Last 24 hours Last 7 days Last month
Device type	Type of device affected by the security settings	Removable storage drive Imaging device CD/DVD drive Bluetooth device Modem Mobile device

Table 65: filters available in the 'Blocked devices' list

16.5.10 ‘Web access by category’ list

Field	Comments	Values
Category	Category that the accessed Web page belongs to	List of all supported categories
Allowed access attempts	Number of accesses allowed to the category specified in the Category field	Number
Allowed computers	Number of computers allowed to access the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number
Denied computers	Number of computers denied to access the category specified in the Category field	Number

Table 66: fields in the ‘Web access by category’ list

Fields in the exported file

Field	Comments	Values
Category	Category that the accessed Web page belongs to	List of all supported categories

Field	Comments	Values
Allowed access attempts	Number of accesses allowed to the category specified in the Category field	Number
Allowed computers	Number of computers allowed to visit the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number
Denied computers	Number of computers denied to access the category specified in the Category field	Number

Table 67: fields in the 'Web access by category' exported file

Filter tool

Field	Comments	Values
Search date type	**Range**: lets you set the time period, from the current moment back **Custom date**: lets you choose a specific date from a calendar	Last 24 hours Last 7 days Last month
Category	Category that the accessed Web page belongs to	List of all supported categories

Table 68: filters available in the 'Web access by category' list

16.5.11 'Web access by computer' list

The 'Web access by computer' list shows all the computers on the network and the visits allowed or denied to Web pages (sorted by category).

Field	Comments	Values
Computer	Name of the computer	Character string
IP address	Primary IP address of the computer	Character string
Group	Group in the Panda Adaptive Defense 360 Groups tree that the computer belongs to	Character string 🌐 'All' group 📁 Native group AD Active Directory group
Category	Category that the accessed Web page belongs to	List of all supported categories
Allowed access attempts	Number of accesses allowed to the category specified in the Category field	Number

Field	Comments	Values
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number

Table 69: fields in the 'Web access by computer' list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Name of the computer	Character string
Category	Category that the accessed Web page belongs to	List of all supported categories
Allowed access attempts	Number of accesses allowed to the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number
Group	Group in the Panda Adaptive Defense 360 Groups tree that the computer belongs to	Character string
IP address	Primary IP address of the computer	Character string
Domain	Windows domain the computer belongs to	Character string
Description		Character string

Table 70: fields in the 'Web access by computer' exported file

Filter tool

Field	Comments	Values
Search date type	**Range**: lets you set the time period, from the current moment back **Custom date**: lets you choose a specific date from a calendar	Last 24 hours Last 7 days Last month
Category	Category that the accessed Web page belongs to	List of all supported categories
Computer type	Type of device	Workstation Laptop Mobile device Server

Field	Comments	Values
Computer	Name of the computer	Character string

Table 71: filters available in the 'Web access by computer' list

16.5.12 'Licenses' list

The 'Licenses' list is covered in chapter 5 Licenses.

16.5.13 'Unmanaged computers discovered' list

The Unmanaged computers discovered list is covered in chapter 6.

16.6. Default lists

The management console includes four lists generated by default:

- Unprotected workstations and laptops
- Malware run
- PUPs run
- Unprotected servers

Unprotected workstations and laptops

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

- Computers on which the **Panda Adaptive Defense 360** software is currently being installed or that have an installation problem.
- Computers with the protection disabled or with errors.
- Computers without a license assigned or with expired licenses.

Malware run

This locates the network computers on which threats have run in the last month. These devices may be infected for one of these reasons:

- The administrator has unblocked an unknown item before it has been classified and it turned out to be malware
- The administrator excluded a known threat from scans in order to run it.
- The computer was in Audit or Hardening mode and the threat existed prior to the installation of **Panda Adaptive Defense 360**

PUPs run

This locates the network computers on which unwanted programs have run in the last month. These devices may be infected for one of these reasons:

- The administrator has unblocked an unwanted program before it has been classified and it turned out to be malware.
- The administrator excluded an unwanted program from scans in order to run it.
- The computer was in Audit or Hardening mode and the unwanted program existed prior to the installation of **Panda Adaptive Defense 360**

Unprotected servers

This list lets you locate all servers, regardless of the operating system installed, that may be vulnerable to threats due to a problem with the protection:

- Servers on which the **Panda Adaptive Defense 360** software is currently being installed or that have an installation problem.
- Servers with the protection disabled or with errors.
- Servers without a license assigned or with expired licenses

17. Managing threats, quarantined items and items being classified

17.1. Introduction

Panda Adaptive Defense 360 provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This balance is achieved through the use of several configurable tools:

- Tools for managing blocked items being classified
- Tools for managing the execution of processes classified as threats
- Tools for managing the backup/quarantine area

Considerations about managing blocked unknown items

Panda Adaptive Defense 360 ensures network protection through two operational modes available in the advanced protection settings for Windows devices: **hardening** and **Lock**. These modes prevent the execution of all unknown processes on users' computers.

Refer to chapter 10 for more information about Panda Adaptive Defense 360's advanced protection modes.

Panda Security's Machine Learning technologies in the company's Big Data environments scan all unknown processes, automatically returning a classification within the first 24 hours since they were first seen. Unknown processes are accurately and unambiguously classified as goodware and malware, and this classification is shared with all Panda Security customers, so that they can all benefit from the company's malware knowledge.

Panda Adaptive Defense 360 blocks the execution of every process being classified, thus preventing potential risk situations. However, in a minority of cases, these automated scans cannot classify the unknown process with the level of accuracy required (99.999%), and manual intervention is needed by a malware specialist.

In these cases, and should the item being classified be essential for the company's activities, the administrator may consider it necessary to take a certain risk and let the item run.

Considerations about managing processes classified as malware

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

Considerations about quarantine management

Finally, administrators may want to have access to items classified as threats and deleted from users' computers.

17.2. Tools for managing blocked items and exclusions

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

All of these tools are accessible from the **Status (1)** menu at the top of the console. Click the relevant widget on the dashboard (see Figure 98).

Lists of items blocked by Panda Adaptive Defense 360

- **To get a list of currently blocked items classified as malware**: Malware activity panel and Classification of all programs run and scanned panel **(4).**
- **To get a list of currently blocked items classified as PUPs**: PUP activity panel and Classification of all programs run and scanned panel **(5).**
- **To get a list of currently blocked items classified as exploits**: Exploit activity panel and Classification of all programs run and scanned panel **(6).**
- **To get a list of currently blocked items classified as viruses**: Threats detected by the antivirus panel (7).
- **To get a list of currently blocked items in the process of classification**: Currently blocked programs being classified panel (2).

Lists of items excluded from blocking by the administrator

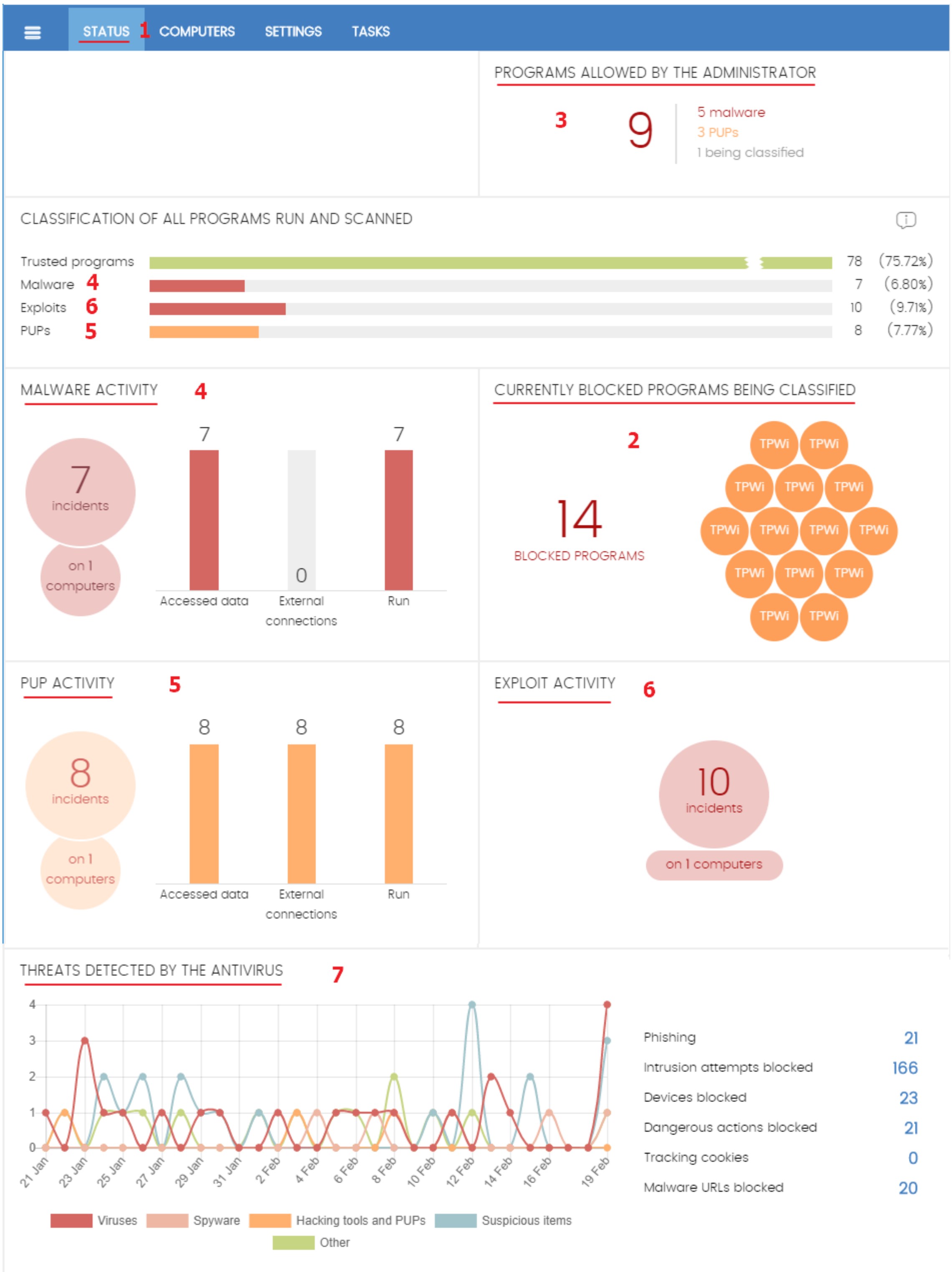
- To **get a list of all programs classified as a threat, a PUP or an unknown item currently excluded from blocking**: Programs allowed by the administrator panel (3).
- **To get a history of currently excluded items**: Programs allowed by the administrator panel (3), History context menu.
- **To see the state changes of excluded items**: Programs allowed by the administrator panel (3), History context menu.
- To get a list of all programs classified as compromised by an exploit and allowed by the system: Exploit activity panel and Classification of all programs run and scanned panel (6).

Adding and removing exclusions

- **To add a malware exclusion**: go to the **Malware activity** panel **(4)**, select a threat, click **Do not detect again**
- **To add a PUP exclusion**: go to the **PUP activity** panel **(5)**, select a threat, click **Do not detect again**
- **To add a virus exclusion**: go to the **Threats detected by the antivirus** panel **(5)**, select a threat, click **Restore and do not detect again**
- **To remove an exclusion:** go to the **Programs allowed by the administrator** panel **(3)**, select a threat and click the 🗑 icon

Changing block policies

- **To change the solution's behavior when an item is reclassified**: go to the Programs allowed by the administrator panel **(3),** click the **Change behavior link**.



STATUS 1 COMPUTERS SETTINGS TASKS

PROGRAMS ALLOWED BY THE ADMINISTRATOR 3

9 — 5 malware, 3 PUPs, 1 being classified

CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED

Trusted programs	78	(75.72%)
Malware 4	7	(6.80%)
Exploits 6	10	(9.71%)
PUPs 5	8	(7.77%)

MALWARE ACTIVITY 4

7 incidents on 1 computers

Accessed data	External connections	Run
7	0	7

CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED 2

14 BLOCKED PROGRAMS

PUP ACTIVITY 5

8 incidents on 1 computers

Accessed data	External connections	Run
8	8	8

EXPLOIT ACTIVITY 6

10 incidents on 1 computers

THREATS DETECTED BY THE ANTIVIRUS 7

Phishing	21
Intrusion attempts blocked	166
Devices blocked	23
Dangerous actions blocked	21
Tracking cookies	0
Malware URLs blocked	20

Figure 116: dashboard tools to manage blocked items and exclusions

17.3. Action diagrams for known and unknown processes

Panda Adaptive Defense 360 blocks all programs classified as malware by default. Additionally, and depending on the advanced protection settings, it will also block never-seen-before programs until they have been scanned and a verdict has been returned about their security.

If a user cannot wait for an unknown item to be classified, or the administrator wants to allow an item classified as malware to run, **Panda Adaptive Defense 360** implements tools to create an exclusion and allow a blocked item to run.

> ⚠ *IMPORTANT: we generally advise that you don't unblock blocked items. Items blocked for being considered dangerous pose a real threat to the integrity of your IT systems and the data stored across your network. Panda Adaptive Defense 360 classifies items with 99.9999% accuracy, and the unknown items blocked are very likely to end up being classified as dangerous. That's why we recommend that you do not unblock as yet unknown items or items classified as malware/PUP.*

17.3.1 Action diagram for known files

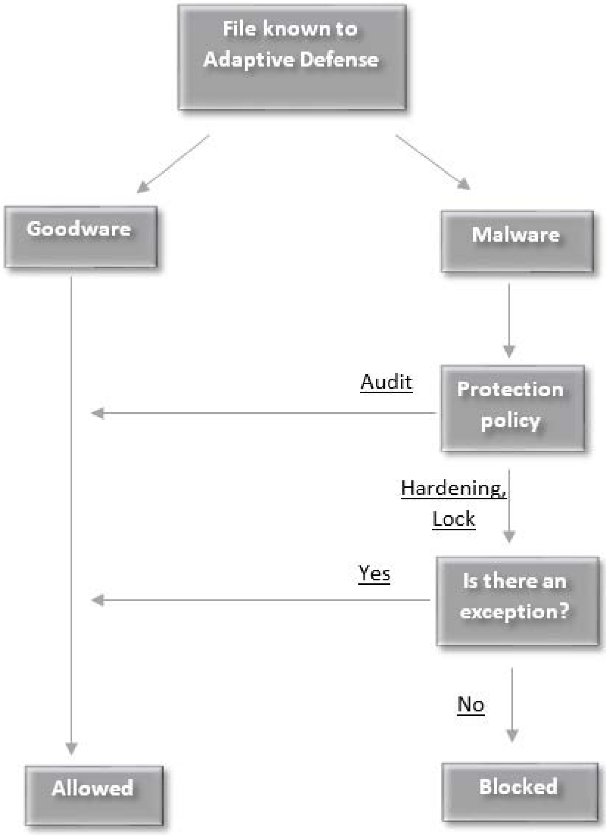


Figure 117: action diagram for known classified processes

Processes classified by **Panda Adaptive Defense 360** as malware with the advanced protection set to a mode other than **Audit** will be blocked unless the administrator creates an exclusion that allows them to run.

17.3.2 Unknown files

Unknown (not yet classified) processes that are detected with the advanced protection set to a mode other than **Audit** will be blocked unless the network administrator creates an exclusion. Regardless of the exclusion, **Panda Adaptive Defense 360** will classify the file and, depending on the verdict and the reclassification policy selected, the file will be blocked or allowed to continue running.

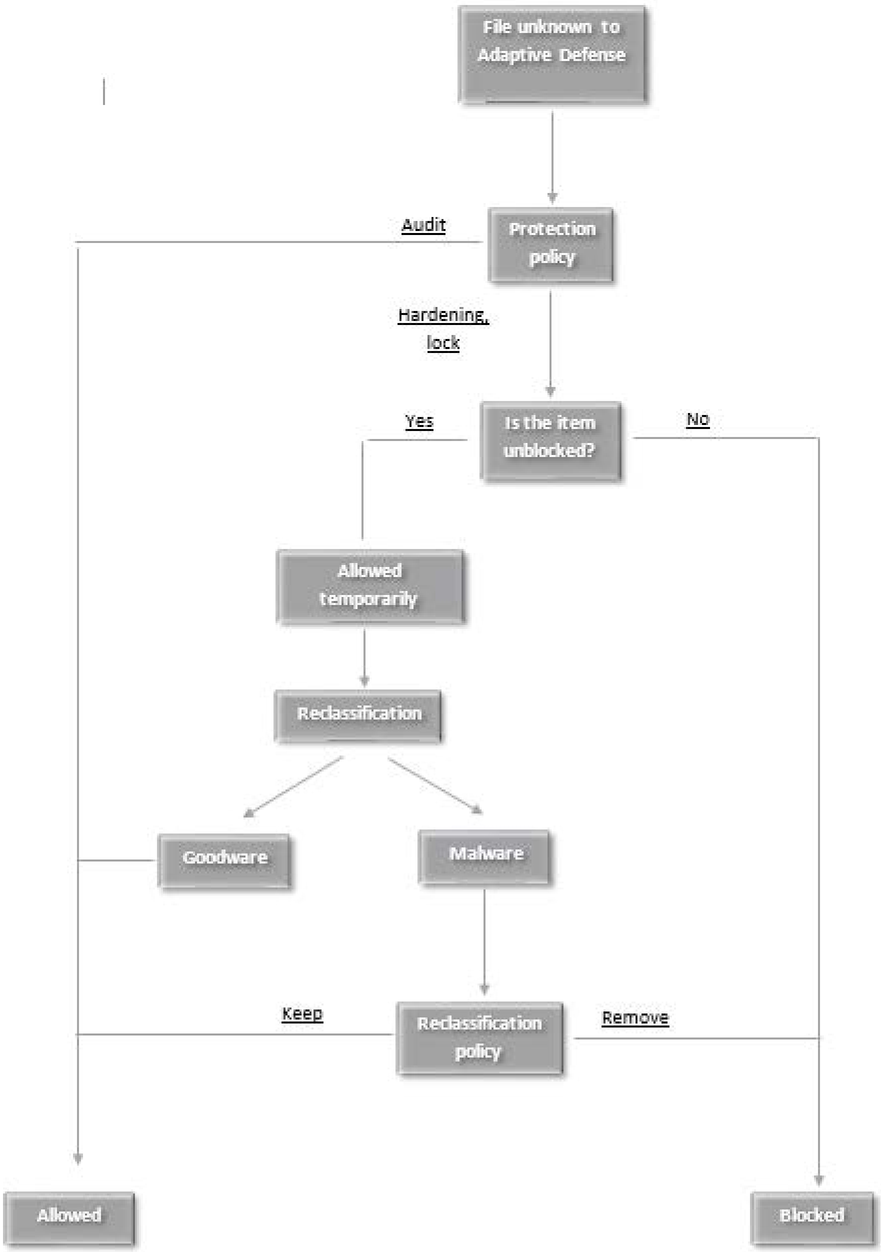


Figure 118: action diagram for unknown processes

17.4. Reclassification policy

The reclassification policies let you define the way **Panda Adaptive Defense 360** will automatically behave when an item that was unblocked by the administrator changes its internal state and it is necessary to make a new decision about whether to block/unblock it.

There are two possibilities when the administrator chooses to unblock a previously blocked (unknown) item: if the unknown item is finally classified as goodware, no further action will need to be taken, as the system will continue to allow it to run. However, if the unknown item is finally classified as malware, the administrator will have to choose the action that **Panda Adaptive Defense 360** must take:

- **Delete it from the list of Programs allowed by the administrator**: the exclusion will be removed and the item will be blocked, unless the administrator manually generates a new exclusion for the file.
- **Keep it on the list of Programs allowed by the administrator**: the exclusion is kept. That is, the item will be allowed to run.

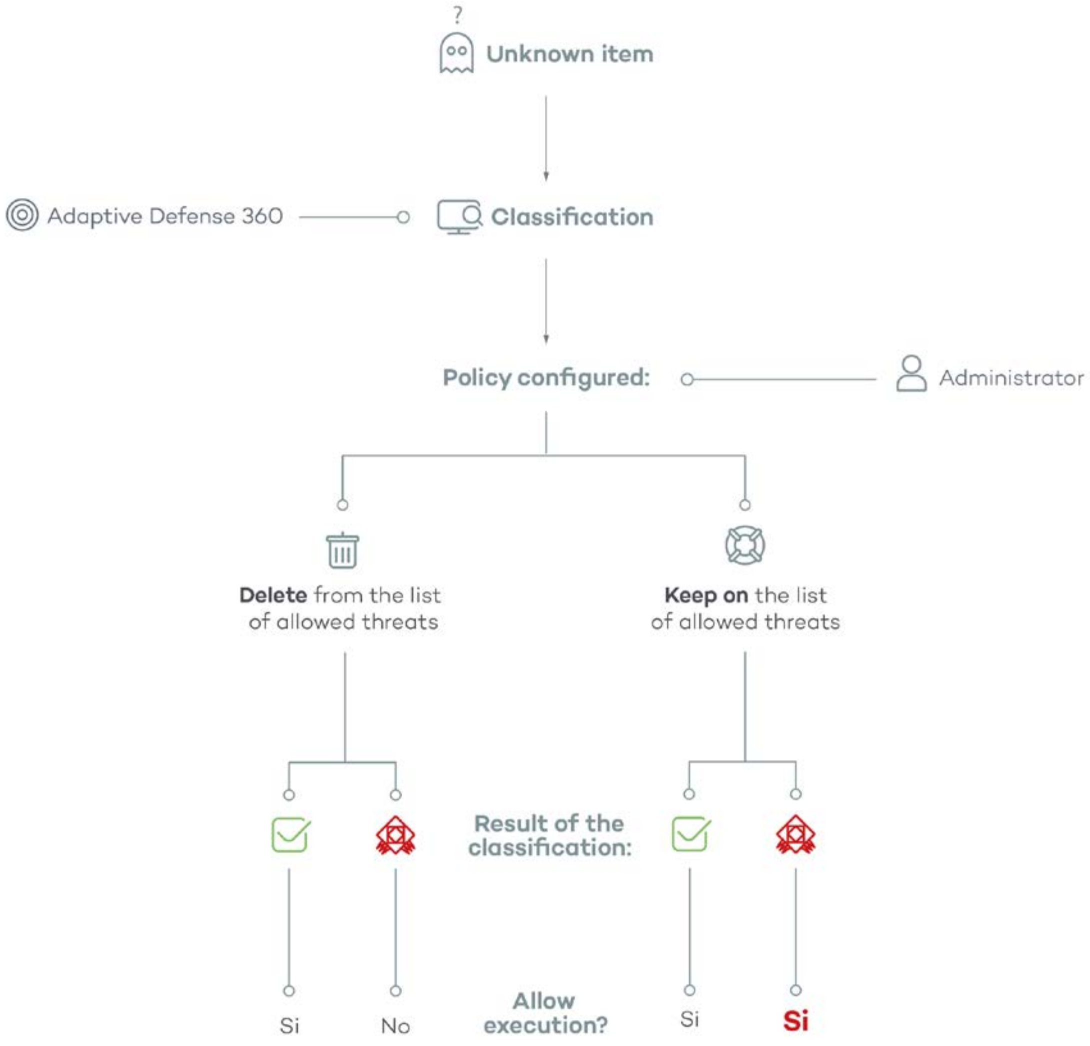


*Figure 119: **Panda Adaptive Defense 360**'s behavior based on the reclassification policy selected and the classification result*

17.4.1 Changing the reclassification policy

Go to the **Status** menu at the top of the console and click the **Programs allowed by the administrator** panel. Click the **Change behavior** link to select the reclassification policy to apply.

Reclassification policies are general for all computers on the network irrespective of the assigned settings

Selecting **Keep it on the list of Programs allowed by the administrator** will display a warning on the **Programs allowed by the administrator** screen, indicating that this can lead to potentially dangerous situations. Example: an unknown item that is pending classification is unblocked by the administrator in order to allow its execution while the classification process is taking place. Once fully identified, the item turns out to be dangerous. In this case, should the option **Keep it on the list of Programs allowed by the administrator** be selected, the malicious item would continue to be allowed to run..

17.4.2 Reclassification traceability

It is very important to know if **Panda Adaptive Defense 360** has reclassified an unknown item, especially if the administrator selected the **Keep it on the list of Programs allowed by the administrator** policy.

Traceability using the History of allowed threats

To view the history of reclassifications of an excluded file, go to the **Programs allowed by the administrator** panel and click the context menu to display the history of allowed threats. A list will appear with the name of all allowed threats and the events that have taken place (**Action** column).

Traceability using the alerts

Panda Adaptive Defense 360 sends administrators an alert every time an unknown item gets blocked. Not only this, they can also receive a notification every time a previously unblocked item is reclassified.

To enable email notifications when an unknown file is blocked:

- Go to the **Settings** menu, click **My alerts** from the left-hand side menu and enable email alerts for the following circumstances:
    - A program that is being classified gets blocked
    - A file allowed by the administrator is finally classified

17.5. Unblocking/Excluding items

Depending on whether you want to allow the execution of a file that is in the process of classification, or of a file classified as a threat, go to the **Currently blocked programs being classified** or **Malware/PUP activity** panel.

> ⚠ *Excluding or unblocking a program causes Panda Adaptive Defense 360 to allow the execution of both the program and all of its libraries and binary files (unless they are known threats).*

17.5.1 Excluding unknown items pending classification

If users cannot wait for the system to automatically unblock a file once it has been classified, the administrator can use the button **Unblock** in the **Currently blocked items being classified** window to allow its execution.

Once unblocked, the item will disappear from the **Currently blocked items being classified** screen, and will be run under the administrator's responsibility. Nevertheless, **Panda Adaptive Defense 360** will continue scanning the process until it is identified and classified. The unblocked item will appear in the **Programs allowed by the administrator** list, described later in the chapter.

17.5.2 Excluding items classified as malware or PUP

Excluding an item classified as malware from the scans is equivalent to unblocking a blocked item that is pending classification, although in this case you are allowing the execution of a program that **Panda Adaptive Defense 360** has already classified as harmful or dangerous.

Go to the **Malware/PUP activity** panel, select a threat, and click the **Do not detect again** button to allow it to run.

Once excluded from the scans, the item in question will stop generating incidents in the **Malware/PUP activity** panels, and will be added to the **Threats and other excluded items** list, as explained in the next section**.**

17.6. Managing excluded items

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

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

List of currently excluded items

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

History

Click the context menu to display a history of all files excluded in **Panda Adaptive Defense 360** and the actions taken on them. This list allows you to view all the states that a file has gone through (allowed or blocked), from the time it entered the **Programs allowed by the administrator** list until it exited it.

17.7. Strategies to supervise installation of new software

During the normal operation of a computer protected with **Panda Adaptive Defense 360**, the solution may detect a small percentage of unknown programs that need classification, and depending on the advanced configuration selected, these programs may be blocked until the classification process returns a verdict (goodware or malware). This will prevent end users from temporarily using those programs.

If the IT department controls the installation of programs on the network and wants to minimize the impact of unknown software on users' activities, while ensuring security, it is advisable to prepare the environment for the execution of new software before deploying it massively across the network.

This process can be divided into four phases:

Configuring a test PC

The aim of this phase is to determine if the software to be installed on the network is known or unknown to Panda Security. To do this, you can use the PC of a network user or use a computer dedicated to this purpose. This computer should be configured in **Hardening** mode.

Installing the software

This step consists of installing the software and running it normally. If **Panda Adaptive Defense 360** finds an unknown module or program, it will block it, displaying a pop-up window on the local computer. Also, a new item will be added to be **Currently blocked items being classified** panel. Internally, **Panda Adaptive Defense 360** will log the events generated by the program, sending the binary files to the cloud for analysis.

If no items are blocked in **Hardening** mode, change the advance protection settings to **Lock** mode, and run the newly installed program again. If new items are blocked, they will be shown in the **Currently blocked items being classified** panel.

Reclassifying blocked programs

As soon as **Panda Adaptive Defense 360** returns a verdict about the blocked programs, it will send an email to the administrator informing them of whether it will unblock them or keep them blocked depending on whether they are goodware or malware. If all processes are classified as goodware, the installed software will be valid for use across the organization's network.

Sending the program directly to Panda Security's cloud

Since **Panda Adaptive Defense 360** is designed to not interfere with network performance when sending files to Panda Security's cloud, file send can be delayed. To speed up the send process, contact Panda Security's Support Department.

17.8. Managing the backup/quarantine area

Panda Adaptive Defense 360's quarantine is a backup area that stores the items deleted after being classified as a threat.

Quarantined items are stored on each user's computer, in the Quarantine folder located in the software installation directory. This folder is encrypted and cannot be accessed by any other process. Thus, it is not possible to directly access or run any quarantined items, unless you do it using the Web console's restore tool.

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

Panda Adaptive Defense 360 also quarantines suspicious files automatically, provided they meet the conditions established by Panda Security's PandaLabs department.

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

- The item is classified as malicious but there is a disinfection routine for it: it is disinfected and restored to its original location.
- The item is classified as malicious, and there is no disinfection routine for it: it is quarantined for seven days.
- The item is identified as harmless: it is restored to its original location.
- Suspicious items are quarantined for a maximum of 30 days. If they finally turn out to be goodware, they are automatically restored to their original location.

Panda Adaptive Defense 360 doesn't delete files from users' computers. All deleted files are actually sent to the backup area.

17.8.1 Viewing quarantined items

Administrators can view quarantined items through the lists and the following dashboard widgets:

- Malware activity
- PUP activity
- Threats detected by the antivirus

Use the filtering tools to view quarantined items (use the **Action** filter: "Quarantined" or "Deleted").

17.8.2 Restoring quarantined items

To restore a quarantined item, select it and click **Restore and do not detect again**. This will copy the item to its original location and restore its original permissions, owner, the registry keys associated with the file and any other information.

18. Forensic analysis

Details of blocked programs and threats

The action tables

The execution graphs

Excel tables

Interpreting the action tables and execution graphs

18.1. Introduction

Next-generation malware is characterized by going undetected for long periods of time, taking advantage of this to access corporate sensitive data and intellectual property. Its objective is economic gain, either through blackmail by encrypting corporate documents for ransom, or selling the information obtained to the competition, among other strategies common to these types of attacks.

When the **Panda Adaptive Defense 360** dashboard displays an infection risk, it needs to be determined to what extent the network has been compromised and the source of the infection. To do this, it is essential to know the actions taken by the malware in order to implement the necessary preventive and remedial measures. **Panda Adaptive Defense 360** continuously monitors all actions triggered by threats, and stores them to show their progress, from the time they were first seen on the network until their neutralization.

Panda Adaptive Defense 360 presents this information in several ways depending on the level of detail and the information required:

- Through detail pages
- Through action tables
- Through graphs
- Through Excel files.

18.2. Details of threats and currently blocked programs in the process of classification

The **Status** menu at the top of the console lets you access lists of detected threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified.**

Click a specific threat to open a window (**Malware detection, PUP detection, Exploit detection** or **Blocked program details**) where you can find detailed information about the threat on the **Details** tab**.**

18.2.1 Malware detection, PUP detection and currently blocked programs in the process of classification

These windows are divided into five sections:

- **Overview**
- **Affected computer**
- **Threat impact on the computer**
- **Infection source**
- **Occurrences on other computers**

Overview

- **Threat**: name of the threat and unique hash that identifies it.
- **Action**: action taken by **Panda Adaptive Defense 360** on the item.
  - Quarantined
  - Blocked
  - Disinfected
  - Deleted

> *Refer to chapter 17 for more information about the actions administrators can take on the items found.*

Affected computer

- **Computer**: name of the computer where the threat was found, IP address and folder in the Groups tree.
- **View available patches**: provided the Panda Patch Management module is enabled, this button shows all patches and updates that are missing from the computer.
- **User**: operating system user under which the threat was loaded and run.
- **Protection mode**: operating mode of the advanced protection when the detection occurred (**Audit**, **Hardening**, **Lock**).
- **Detection path**: file system path of the threat.

Threat impact on the computer

- **Threat**: name of the detected threat and file identification string (hash). Two buttons are available to search for additional information on Google and VirusTotal's website. If the threat is a newly discovered threat, the text **New threat** will be displayed.
- **Activity**: summary of the most important actions taken by the malware:
  - **Has run**
  - **Has accessed data files**

  - **Has exchanged data with other computers**

- **Detection date**
- **Dwell time**: time during which the threat has been on the system without being classified.

Infection source

- **Source computer**: displays the name of the computer the infection originated from, if applicable.
- **Source IP address**: displays the IP address of the computer the infection originated from, if applicable.
- **Source user**: the user that was logged in on the computer the infection originated from.

Occurrences on other computers

Displays all computers on the network where the malware has been seen.

- **Computer**: computer name
- **File path:** name and path of the file that contains the malware
- **First seen**: date the threat was first detected on the computer

You can also access a chart detailing the malware activity. This chart is discussed later in this chapter.

18.2.2 Exploit detection

This window is divided into five sections:

- **Overview**
- **Affected computer**
- **Exploit impact on the computer**
- **Infection source**
- **Occurrences on other computers**

Overview

- **Compromised program**: name of the program that was hit by the exploit and hash that identifies it.
- **Action**: shows the action taken by **Panda Adaptive Defense 360** on the program hit by the exploit.
  - **Allowed**: the exploit was allowed to run as the anti-exploit protection was configured in “Audit” mode.
  - **Blocked**: the exploit was blocked before it could run.
  - **Allowed by the user**: the computer user was asked for permission to end the compromised process, but decided to let the exploit run.

- **Process ended**: the exploit has been deleted, but managed to partially run.
- **Pending restart**: the user has been informed of the need to restart their computer in order to completely remove the exploit. Meanwhile, the exploit has continued to run.

Affected computer

- **Computer**: name of the computer where the threat was found, IP address and folder in the Groups tree.
- **User**: operating system user under which the threat was loaded and run.
- **Protection mode**: operating mode of the advanced protection when the detection occurred (**Audit**, **Hardening**, **Lock**).
- **Detection path**: file system path of the threat.

Exploit impact on the computer

- **Compromised program**: name and path of the program that was hit by the exploit attempt. If **Panda Adaptive Defense 360** detects that the program is not updated to the latest available version, the ⚠ **Vulnerable program** warning message is displayed**.**
- **Activity** ⚡ : indicates if the exploit managed to run before being detected by **Panda Adaptive Defense 360**.
- **Detection date**
- **Last accessed URLs:** list of the last URLs accessed by the vulnerable process hit by the exploit

You can also access a chart detailing the exploit activity. This chart is discussed later in this chapter.

18.3. Action tables

The **Status** menu at the top of the console lets you access lists of detected threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified.**

Click a specific threat to open a window (**Malware detection, PUP detection, Exploit detection** or **Blocked program details**) where you can find detailed information about the actions taken by the threat on the **Activity** tab**.**

The **Activity** tab displays an action table with the most relevant events triggered by the threat.

The number of actions and events triggered by a process is very high. Therefore, displaying all of them would hinder the extraction of useful information to perform a forensic analysis.

The table content is initially sorted by date, making it easier to follow the progress of the threat.

The table below shows the fields included in the action table:

Field	Comments	Values
Date	Date of the action	Date
Times	Number of times the action was executed. A single action executed several times consecutively will only appear once on the list	Numeric value
Action	Action logged by the system and command line associated with it	Downloaded from Communicates with Accesses data Is run by Runs Is created by Creates Is modified by Modifies Is loaded by Loads Is deleted by Deletes Is renamed by Renames Is killed by Kills process Creates remote thread Thread injected by Is opened by Opens Creates Is created by Creates key pointing to Exe file Modifies key pointing to Exe file
Path/URL/Registry Key/IP:Port	Action entity. It can have the following values depending on the action type:	**Registry key**: for actions that involve modifying the Windows registry **IP:Port**: for actions that involve communicating with a local or remote computer **Path**: for actions that involve access to the computer hard disk **URL**: for actions that involve access to a URL

Field	Comments	Values
File Hash/Registry Value/Protocol-Direction/Description	This field complements the entity field	File Hash: for actions that involve access to a file Registry Value: for actions that involve access to the registry Protocol-Direction: for actions that involve communicating with a local or remote computer. Possible values are: • TCP • UDP • Bidirectional • Unknown • Description
Trusted	The file is digitally signed	Binary value

Table 72: fields displayed in a threat's action table

18.3.1 Subject and predicate in actions

To correctly understand the format used to present the information in the action list, a parallel needs to be drawn with the natural language:

- All actions have as the subject the file classified as a threat. This subject is not indicated in each line of the action table because it is common throughout the table.
- All actions have a verb which relates the subject (the classified threat) with an object, called entity. The entity is indicated in the **Path/URL/Registry key/IP:port** field of the table.
- The entity is complemented with a second field which adds information to the action: **file Hash/Registry Value/Protocol-Direction/Description**.

Table 73 shows two actions carried out by the same hypothetical malware:

Date	Times	Action	Path/URL/Registry Key/IP	File Hash/Registry Value/Protocol/Description	Trusted
3/30/2015 4:38:40 PM	1	Communicates with	54.69.32.99/80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Loads	PROGRAM_FILES|\ MOVIES TOOLBAR\SAFETYN	9994BF035813FE8EB6BC98E CCBD5B0E1	NO

Table 73: action list of a sample threat

The first action indicates that the malware (subject) **connected to (action)** the IP address `54.69.32.99:80` (entity) through the TCP-bidirectional protocol.

The second action indicates that the malware (subject) **loaded** (action) the library `PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL` with hash `9994BF035813FE8EB6BC98ECCBD5B0E1`.

As with natural language, two types of sentences are implemented in **Panda Adaptive Defense 360**:

- **Active**: these are predicative actions (with a subject and predicate) related by an active verb. In these actions, the verb of the action relates the subject, which is always the process classified as a threat, and a direct object, the entity, which can be multiple according to the type of action.
- **Passive**: these are actions where the subject (the process classified as a threat) becomes the passive subject (which receives, rather than executes the action), and the verb is passive (to be + participle). In this case, the passive verb relates the passive subject which receives the action with the entity, which performs the action.

Examples of active actions are:

- Communicates with
- Loads
- Creates

Examples of passive actions are:

- Is created by
- Is downloaded from

Table 74 shows an example of a passive action:

Date	Times	Action	File Path/URL/Registry Key/IP	File Hash/Registry Value/Protocol/Description	Trusted
3/30/2015 4:51:46 PM	1	Is run by	WINDOWS|\ explorer.exe	7522F548A84ABAD8FA516DE5AB3931EF	NO

Table 74: example of a passive action

In this action, the malware (passive subject) **is run by** (passive action) the `WINDOWS|\explorer.exe` program (entity) with hash `7522F548A84ABAD8FA516DE5AB3931EF`.

Active actions let you inspect in detail the steps taken by the threat. By contrast, passive actions usually reflect the infection vector used by the malware (which process ran it, which process copied it to the user's computer, etc.).

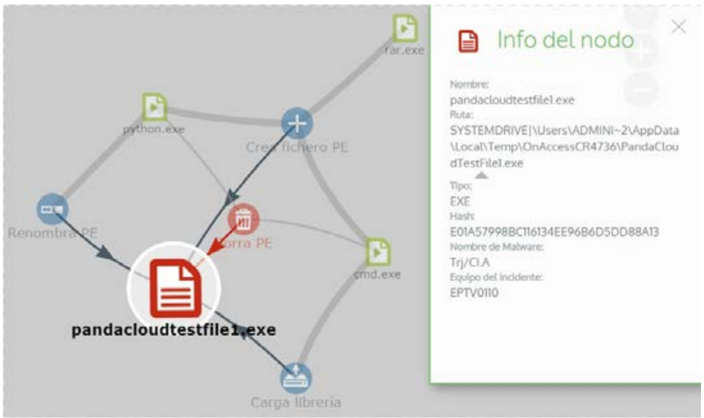
18.4. Execution graphs

The **Status** menu at the top of the console lets you access lists of detected threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified.**

Click a specific threat. A different window will open depending on the type of threat: **malware detection, PUP detection, Exploit detection** or **Blocked program details**. Go to the **Activity** tab and click the **View activity graph** button.

Execution graphs offer a graphical representation of the information shown in the action tables, emphasizing the temporal aspect. These graphs provide an at-a-glance idea of the actions triggered by the threat.



Nombre:
pandacloudtestfile1.exe
Ruta:
SYSTEMDRIVE|\Users\ADMINI~2\AppData\Local\Temp\OnAccessCR4736\PandaCloudTestFile1.exe
Tipo:
EXE
Hash:
E01A57998BC116134EE96B6D5DD88A13
Nombre de Malware:
Trj/Cl.A
Equipo del incidente:
EPTV0110

Figure 120: example of a graph representing a threat's activities

18.4.1 Diagrams

Execution graphs represent the actions taken by threats with two elements:

- **Nodes**: they mostly represent actions or information items.
- **Lines and arrows**: they join the action and information nodes to establish a temporal order, and assign each node the role of “subject” or “predicate”.

18.4.2 Nodes

The nodes show information through their associated icon, color, and descriptive panel on the right of the screen when selected with the mouse.

The color code used is as follows:

- **Red**: untrusted item, malware, threat.
- **Orange**: unknown/unclassified item.
- **Green**: trusted item, goodware.

Table 75 shows action-type nodes with a brief description:

Symbol	Description
⬇	File download Compressed file created
📥	Socket/communication used
⇥	Monitoring initiated
▶	Process created
+	Executable file created Library created Key created in the registry
✎	Executable file modified Registry key modified
📝	Executable file mapped for write access
🗑	Executable file deleted
📤	Library loaded
⚙	Service installed

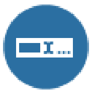
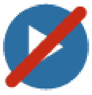
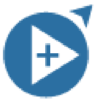
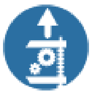
Symbol	Description
	Executable file renamed
	Process stopped or closed
	Thread created remotely
	Compressed file opened

Table 75: graphical representation of the malware actions shown in the execution graph

Table 76 shows descriptive-type nodes with a brief description:

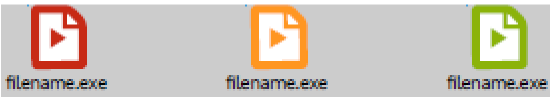
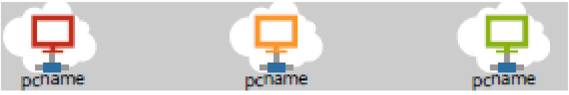
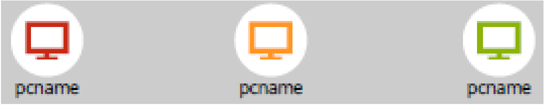
Symbol	Description
	File name and extension **Green**: goodware **Orange**: unclassified item **Red**: malware/PUP
	Internal computer (it is on the corporate network) **Green**: trusted **Orange**: unknown **Red**: untrusted
	External computer **Green**: trusted **Orange**: unknown **Red**: untrusted
	Country associated with the IP address of an external computer
	File and extension
	Registry key

Table 76: graphical representation of descriptive-type nodes in the execution graph

18.4.3 Lines and arrows

The lines of the graphs relate the different nodes and help to establish the order in which the actions performed by the threat were executed.

The two attributes of a line are:

- **Line thickness**: indicates the number of occurrences that this relationship has had in the graph. The greater number of occurrences, the greater the size of the line
- **Arrow**: marks the direction of the relationship between the two nodes

18.4.4 The timeline

The timeline helps control the display of the string of actions carried out by the threat over time. Using the buttons at the bottom of the screen you can position yourself at the precise moment when the threat carried out a certain action, and retrieve extended information that can help you in the forensic analysis processes.

The timeline of the execution graphs looks like this:

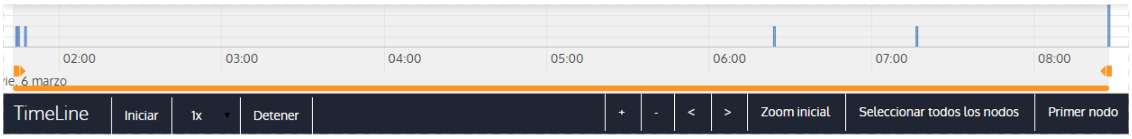


Figure 121: graphical representation of a threat's timeline

You can select a specific interval on the timeline dragging the interval selectors to the left or right to cover the timeframe of most interest to you.

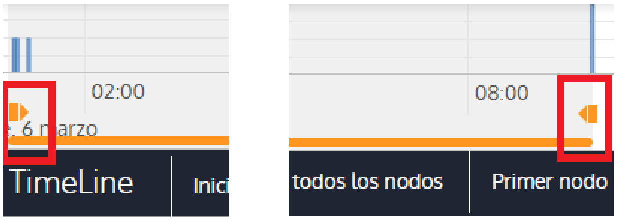


Figure 122: time selectors

After selecting a timeframe, the graph will only show the actions and nodes that fall within that interval. The rest of the actions and nodes will be blurred on the graph.

The actions carried out by the threat are represented on the timeline as vertical bars accompanied by a timestamp, which indicates the hour and minute when they occurred.

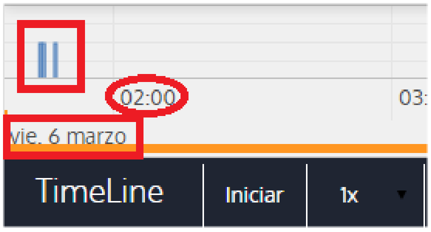


Figure 123: timestamp, date and actions carried out by the threat

18.4.5 Zoom in and Zoom out

The + and – buttons of the time bar allow you to zoom in or zoom out for higher resolution if there are many actions in a short time interval.

18.4.6 Timeline

To view the string of actions run by the threat, the following controls are used:

- **Start**: starts the execution of the timeline at a constant speed of 1x. The graphs and lines representing the actions will appear while passing along the timeline.
- **1x**: establishes the speed of traveling along the timeline.
- **Stop**: stops the execution of the timeline.
- **+ and -**: zoom in and zoom out of the timeline.
- **< and >**: moves the node selection to the immediately previous or subsequent node.
- **Initial zoom**: restores the initial zoom level if modified with the + and – buttons.
- **Select all nodes**: moves the time selectors to cover the whole timeline.
- **First node**: establishes the time interval at the start, a necessary step for initiating the display of the complete timeline.

To display the full path of the timeline, first select "First node" and then "Start". To set the travel speed, select the button 1x.

18.4.7 Filters

The controls for filtering the information shown in the execution graph are at the top of the graph.

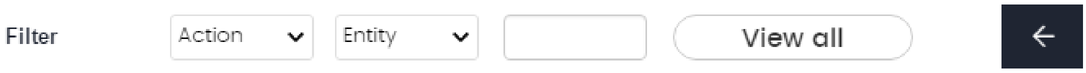


Figure 124: filters in the execution graph

The available filtering criteria are:

- **Action:** drop-down menu which lets you select an action type from all those executed by the threat. This way, the graph will only show the nodes that match the action type selected and the adjacent nodes associated with this action.

- **Entity**: drop-down menu which lets you choose an entity (the content of the field Path/URL/Registry Key/IP:Port).

18.4.8 Node movement and general zoom

To move the graph in four directions and zoom in or zoom out, you can use the controls in the top right of the graph.

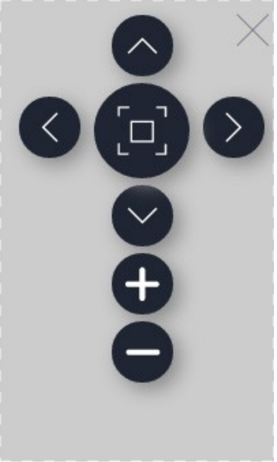
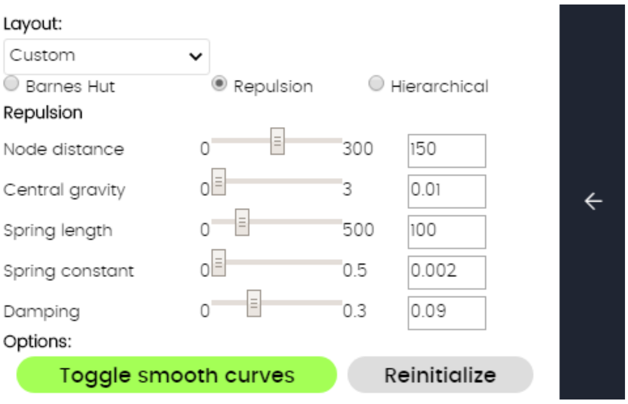


Figure 125: buttons to zoom in and zoom out of the graph

To zoom in and zoom out more easily, you can use the mouse's scroll wheel.

The X symbol allows you to leave the graph view. If you would rather hide the timeline button zone to use more space on the screen for the graph, you can select the ↓ icon located in the bottom right of the graph.

Finally, you can configure the behavior of the graph through the panel below. To access it, click the → button in the top left corner of the graph.



Layout:

Custom

○ Barnes Hut ● Repulsion ○ Hierarchical

Repulsion

	Min	Max	Value
Node distance	0	300	150
Central gravity	0	3	0.01
Spring length	0	500	100
Spring constant	0	0.5	0.002
Damping	0	0.3	0.09

Options:

Figure 126: execution graph settings panel

18.5. Excel tables

The **Status** menu at the top of the console lets you access lists of threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified**

Click the context menu and select **Export list and details** from the drop-down menu displayed. An Excel file will be downloaded with the full lifecycle of all threats on the list.

Field	Comments	Values
Date	Date when the action took place	Date
Hash	String identifying the threat	Character string
Threat	Threat name	
User	User account under which the threat was run	Character string
Computer	Name of the computer where the threat was detected	Character string
Path	Name and path to the threat on the user's computer	Character string
Accessed data	The threat accessed files located on the user's computer	Binary value
Action	Action logged by the system	Downloaded from Communicates with Accesses data Run by Runs Created by Creates Modified by Modifies Loaded by Loads Deleted by Deletes Renamed by Renames Killed by Kills process Creates remote thread Thread injected by Opened by Opens Creates Created by Creates registry key to run Modifies registry key to run
Command Line	Command line associated with the action	Character string

Field	Comments	Values
Event date		Date
Times	Number of times the action was executed. A single action executed several times consecutively will only appear once on the list	Numeric value
Path/URL/Registry Key/IP:Port	Action entity. It can have the following values depending on the action type:	Registry key: for actions that involve modifying the Windows registry IP:Port: for actions that involve communicating with a local or remote computer Path: for actions that involve access to the computer hard disk URL: for actions that involve access to a URL
File Hash/Registry Value/Protocol-Direction/Description	This field complements the entity field	File hash: for actions that involve access to a file Registry value: for actions that involve access to the registry Protocol-Direction: for actions that involve communicating with a local or remote computer. Possible values are: • TCP • UDP • Bidirectional • Unknown • Description
Trusted	The file is digitally signed	Binary value

Table 77: fields in the 'List and details' exported file

18.6. Interpreting the action tables and execution graphs

The action tables and execution graphs are graphical representations of the evidence collected on the customer's computers. These must be interpreted by the organization's network administrator. A certain degree of technical knowledge is necessary to be able to extract activity patterns and key information in each situation.

Below we provide some basic guidelines to interpret the action tables with some real-life examples of threats.

The name of the threats indicated here can vary among different security vendors. You should use the hash ID to identify specific malware.

18.6.1 Example 1: viewing the actions executed by the malware Trj/OCJ.A

The **Details** tab shows the key information about the malware found. In this case the important data is as follows:

- **Threat**: trj/OCJ.A
- **Computer**: XP-BARCELONA1
- **Detection path**: TEMP|\Rar$EXa0.946\appnee.com.patch.exe

Activity

The **Activity** tab shows some actions. This is because **Panda Adaptive Defense 360** was configured in **Hardening** mode and the malware already resided on the computer when **Panda Adaptive Defense 360** was installed. The malware was unknown at the time of running.

Hash

Use the hash string to obtain more information on sites such as VirusTotal to get a general idea of the threat and how it works.

Detection path

The path where the malware was detected for the first time on the computer belongs to a temporary directory and contains the RAR string. Therefore, the threat comes from a RAR file temporarily uncompressed in the directory, and which gave the appnee.com.patch.exe executable as the result.

Activity tab

Step	Date	Action	Path
1	3:17:00	Is created by	PROGRAM_FILES|\WinRAR\WinRAR.exe
2	3:17:01	Is run by	PROGRAM_FILES|\WinRAR\WinRAR.exe
3	3:17:13	Creates	TEMP|\bassmod.dll
4	3:17:34	Creates	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifies	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Deletes	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
7	3:17:41	Creates	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifies	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll

Step	Date	Action	Path
9	3:17:59	Runs	PROGRAM_FILES|\Google\Chrome\Application\chrome.exe

Table 78: list of actions performed by Trj/OCJ.A

Steps 1 and 2 indicate that the malware was uncompressed by WinRar.Exe and run from that program. The user opened the compressed file and clicked its binary.

Once run, in step 3 the malware created a DLL file (bassmod.dll) in a temporary folder, and another one (step 4) in the installation directory of the Adobe Acrobat 11 program. In step 5, it modified an Adobe DLL file, to take advantage perhaps of a program vulnerability.

After modifying other DLL files, it launched an instance of Google Chrome which is when the timeline finishes. **Panda Adaptive Defense 360** classified the program as a threat after that string of suspicious actions and stopped its execution.

The timeline shows no actions on the registry, so it is very likely that the malware is not persistent or wasn't able to modify the registry to ensure it could survive a computer restart.

The software Adobe Acrobat 11 was compromised so a reinstall is recommended. Thanks to the fact that **Panda Adaptive Defense 360** monitors both goodware and malware executables, the execution of a compromised program will be detected as soon as it triggers dangerous actions, and ultimately be blocked.

18.6.2 Example 2: communication with external computers by BetterSurf

BetterSurf is a potentially unwanted program that modifies the Web browser installed on the user's computer, injecting ads in the Web pages they visit.

The **Details** tab shows the key information about the malware found. In this case it shows the following data:

- **Name**: PUP/BetterSurf
- **Computer**: MARTA-CAL
- **Detection path**: PROGRAM_FILES|\VER0BLOCKANDSURF\N4CD190.EXE
- **Dwell time**: 11 days 22 hours 9 minutes 46 seconds

Dwell time

In this case, the dwell time is very long: the malware remained dormant on the customer's network for almost 12 days. This is increasingly normal behavior and may be for various reasons. For example, the malware did not carry out any suspicious actions until very late, or the user downloaded the file but did not run it at the time. In both cases, the threat was unknown to the security service, so there was no malware signature to compare it to.

Activity tab

Step	Date	Action	Path
1	03/08/2015 11:16	Is created by	SMTP, 08c3b650, e9e14f.exe
2	03/18/2015 11:16	Is run by	SYSTEM | \services.exe
3	03/18/2015 11:16	Loads	PROGRAM_FILES|\VER0BLOF\N4Cd190.dll
4	03/18/2015 11:16	Loads	SYSTEM | \BDL.dll
5	03/18/2015 11:16	Communicates with	127.0.0.1/13879
6	03/18/2015 11:16	Communicates with	37.58.101.205/80
7	03/18/2015 11:17	Communicates with	5.153.39.133/80
8	03/18/2015 11:17	Communicates with	50.97.62.154/80
9	03/18/2015 11:17	Communicates with	50.19.102.217/80

Table 79: list of actions performed by PUP/BetterSurf

In this case you can see how the malware communicated with different IP addresses. The first address (step 5) is the infected computer itself, and the rest are external IP addresses to which it connected via port 80 and from which the advertising content was probably downloaded.

The main preventive measure in this case should be to block those IP addresses in the corporate firewall.

Before adding rules to block IP addresses in the corporate firewall, you should consult those IP addresses in the associated RIR (RIPE, ARIN, APNIC, etc.) to see the network to which they belong. In many cases, the remote infrastructure used by malware is shared with legitimate services housed in providers such as Amazon and similar, so blocking certain IP addresses would be the same as blocking access to legitimate Web pages.

18.6.3 Example 3: access to the registry by PasswordStealer.BT

PasswordStealer.BT is a Trojan that logs the user's activity on the infected computer and sends the information obtained to an external server. Among other things, it captures screens, records keystrokes and sends files to a C&C (Command & Control) server.

The **Details** tab shows the key information about the malware found. In this case it shows the following data:

- **Detection path**: APPDATA|\microsoftupdates\micupdate.exe

The name and location of the executable file indicate that the malware poses as a Microsoft update. This particular malware cannot infect computers by itself; it requires the user to run it manually.

Activity tab

The **Activity** tab shows some actions. This is because **Panda Adaptive Defense 360** was configured in **Hardening** mode and the malware already resided on the computer when **Panda Adaptive Defense 360** was installed. The malware was unknown at the time of running.

Action table

Step	Date	Action	Path
1	03/31/2015 23:29	Is run by	PROGRAM_FILESX86 | \internet explorer\iexplore.exe
2	03/31/2015 23:29	Is created by	INTERNET_CACHE | \Content.IE5\QGV8PV80\ index[1].php
3	03/31/2015 23:30	Creates key pointing to Exe file	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\CurrentVersion\Run?MicUpdate
4	03/31/2015 23:30	Runs	SYSTEMX86 | \notepad.exe
5	03/31/2015 23:30	Thread injected by	SYSTEMX86 | \notepad.exe

Table 80: list of actions performed by PasswordStealer.BT

In this case, the malware was generated in step 2 by a Web page and run by Internet Explorer.

The order of the actions has a granularity of 1 microsecond. For this reason, the actions executed within the same microsecond may not appear in order in the timeline, as in step 1 and step 2.

Once run, the malware became persistent in step 3, adding a branch to the Windows registry in order to run every time the computer started up. It then started to execute typical malware actions such as opening the notepad and injecting code in one of its threads.

As a remedial action in this case and in the absence of a known disinfection method, you could minimize the impact of the malware by deleting the malicious registry entry. However, it is quite possible that the malware might prevent you from modifying that entry on infected computers; In that case, you would have to either start the computer in safe mode or with a bootable CD to delete the entry.

Example 4: access to confidential data by Trj/Chgt.F

Trj/Chgt.F was uncovered by WikiLeaks at the end of 2014 as a tool used by government agencies in some countries for selective espionage.

In this example, we'll go directly to the **Activity** tab to show you the behavior of this advanced threat.

Action table

Step	Date	Action	Path
1	4/21/2015 2:17:47 PM	Is run by	SYSTEMDRIVE|\Python27\pythonw.exe
2	4/21/2015 2:18:01 PM	Accesses data	#.XLS
3	4/21/2015 2:18:01 PM	Accesses data	#.DOC
4	4/21/2015 2:18:03 PM	Creates	TEMP|\doc.scr
5	4/21/2015 2:18:06 PM	Runs	TEMP|\doc.scr
6	4/21/2015 2:18:37 PM	Runs	PROGRAM_FILES|\Microsoft Office\Office12\WINWORD.EXE
7	4/21/2015 8:58:02 PM	Communicates with	192.168.0.1/2042

Table 81: list of actions performed by Trj/Chgt.F

The malware was initially run by the Python interpreter (step 1), and later accessed an Excel file and a Word document (steps 2 and 3). In step 4, a file with an SCR extension was run, probably a screensaver with some type of flaw or error that could be exploited by the malware.

In step 7 the malware established a TCP connection. The IP address is private, so the malware connected to the customer's own network.

In a case like this it is important to check the content of the files accessed by the threat in order to assess the loss of information. However, the timeline of this particular attack shows that no information was extracted from the customer's network.

Panda Adaptive Defense 360 disinfected the threat, and automatically prevented all subsequent executions of the malware for this and other customers.

19. Remediation tools

Automatic computer disinfection
On-demand file scanning and disinfection
Computer restart
Computer isolation
Reporting computer problems
External access to the console

19.1. Introduction

Panda Adaptive Defense 360 provides several remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle.

Some of these tools are automatic and don't require administrator intervention, whereas other require the execution of certain actions through the Web console.

Table 82 illustrates the tools available for each platform and their type (manual or automatic).

Remediation tool	Platform	Type	Purpose
Automatic computer disinfection	Windows, macOS, Linux Android	Automatic	To disinfect or quarantine malware at the time of infection
On-demand file scanning and disinfection	Windows, macOS, Linux, Android	Automatic (scheduled)/Manual	To scan, disinfect and quarantine malware immediately or at scheduled times
On-demand restart	Windows	Manual	Forces a computer restart to apply updates, finish manual disinfection tasks and fix protection errors.
Computer isolation	Windows	Manual	Isolates the computer from the network, preventing the exfiltration of confidential information and the propagation of threats to other computers

Table 82: Panda Adaptive Defense 360 remediation tools

19.2. Automatic computer disinfection

Panda Adaptive Defense 360's real-time advanced protection and antivirus protection clean infected computers automatically.

That is, upon detecting malware, **Panda Adaptive Defense 360** will automatically clean the affected item provided there is a disinfection method available. Otherwise, the item will be quarantined.

Automatic disinfection does not require administrator intervention. However, the **File protection** checkbox must be selected in the security settings assigned to the computer.

Refer to chapter 10 for more information about the block modes available in Panda Adaptive Defense 360 and the antivirus protection settings.

Advanced protection mode	Antivirus protection	Behavior
Audit	Enabled	Detection, disinfection, quarantine
Hardening, Lock	Enabled	Detection, blocking of unknown items, disinfection, quarantine
Audit	Disabled	Detection
Hardening, Lock	Disabled	Detection, blocking of unknown items

Table 83: product behavior based on the Adaptive Defense and antivirus settings

19.3. On-demand computer scanning and disinfection

There are two ways to scan and disinfect files on demand: one is to create a scheduled scan task and the other is to run an immediate scan.

> ***Refer to chapter 15 Tasks for more information on how to create and manage scheduled tasks from the Tasks menu***

19.3.1 Creating a task from the computer tree

The computer tree lets you define scan tasks very quickly for all computers in a computer group.

- Go to the **Computers** menu at the top of the console and select the computer tree folder view.
- Click the context menu icon for the group whose computers you want to scan. The context menu will open.
- Click one of the following two options:
  - **Scan now**: lets you create a scan task which will be run immediately on all computers in the group.
  - **Schedule scan**: takes you to the Tasks area where you can create a recurring and/or scheduled task. The task template will be partially populated: the Recipients field will be set with the group selected in the computer tree. Fill in the remaining options, as explained in section 14.3 Creating a task from the Tasks area.

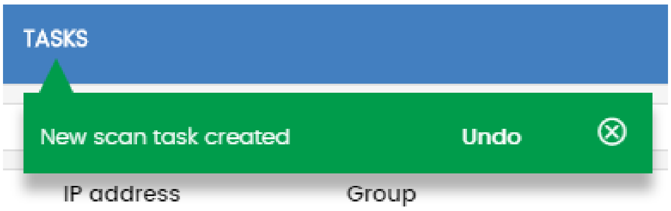
Immediate tasks

Immediate tasks (launched through the Scan now option in the context menu) have the following characteristics:

- You can select the scan type (The entire computer or Critical areas). Refer to section 14.2.2 Task scheduler and repetition for more information.
- You don't need to specify an execution time or repetition interval: they are one-time tasks which start right after being configured.
- You don't need to publish them: they are automatically published by Panda Adaptive

Defense 360.

- The management console will display a pop-up message informing of the success or failure creating the task.



New scan task created

Figure 127: 'Scan task created' message

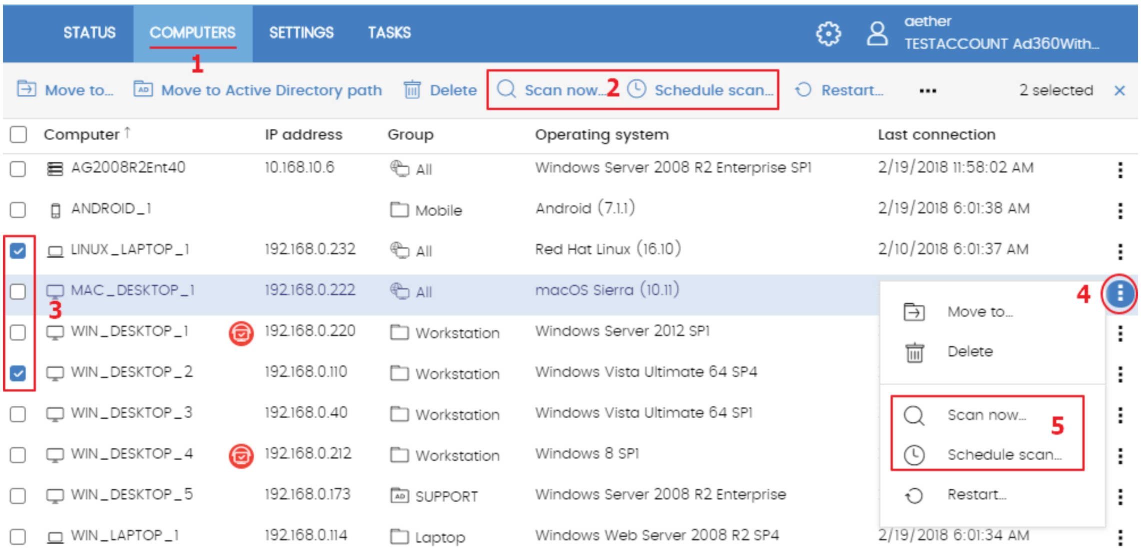
- To view the result of an immediate task, click the Tasks menu at the top of the console.

Scheduled tasks

Scheduled tasks (launched through the Schedule scan option in the context menu) are identical to the tasks created from the Tasks menu and discussed in section 14.3 Creating a task from the Tasks area. The only difference is that the Recipients field will be populated with the group selected in the computer tree. Therefore, it will be necessary to specify the task's execution time and repetition interval, and publish it for activation.

19.3.2 Creating a task from the Computers screen

The Computers screen lets you create immediate and scheduled tasks similarly to the computer tree or the Tasks area. However, in this case you can individually select computers belonging to the same group or subgroup.



□	Computer ↑	IP address	Group	Operating system	Last connection
□	AG2008R2Ent40	10.168.10.6	All	Windows Server 2008 R2 Enterprise SP1	2/19/2018 11:58:02 AM
□	ANDROID_1		Mobile	Android (7.1.1)	2/19/2018 6:01:38 AM
☑	LINUX_LAPTOP_1	192.168.0.232	All	Red Hat Linux (16.10)	2/10/2018 6:01:37 AM
□	MAC_DESKTOP_1	192.168.0.222	All	macOS Sierra (10.11)	
□	WIN_DESKTOP_1	192.168.0.220	Workstation	Windows Server 2012 SP1	
☑	WIN_DESKTOP_2	192.168.0.110	Workstation	Windows Vista Ultimate 64 SP4	
□	WIN_DESKTOP_3	192.168.0.40	Workstation	Windows Vista Ultimate 64 SP1	
□	WIN_DESKTOP_4	192.168.0.212	Workstation	Windows 8 SP1	
□	WIN_DESKTOP_5	192.168.0.173	SUPPORT	Windows Server 2008 R2 Enterprise	
□	WIN_LAPTOP_1	192.168.0.114	Laptop	Windows Web Server 2008 R2 SP4	2/19/2018 6:01:34 AM

Figure 128: context menus and action bar for quick task creation

Choose one of the following resources depending on the number of computers that will receive the task:

- **The computer's context menu**: if the task is to be applied to one computer only.
- **Checkboxes and action bar**: if the task is to be applied to one or more computers belonging to a group or its subgroups.

Context menu associated with a single computer

- Click the **Computers** (1) menu at the top of the console, and select the group in the computer tree that the computer to scan belongs to.
- From the computer list, click the context menu of the computer to scan. (4)
- From the context menu (5), click one of the following two options:
  - **Scan now**: lets you create a scan task which will be run immediately on the selected computer.
  - **Schedule scan**: takes you to the **Tasks** area where you can create a recurring and/or scheduled task. The task template will be partially populated: the Recipients field will display the selected computer. Fill in the remaining options, as explained in section 15.3 Creating a task from the Tasks area.

Checkboxes and action bar

- Click the **Computers (1)** menu at the top of the console, and select the group in the computer tree that the computers to scan belong to.
- Select the computers that will receive the scan task using the checkboxes **(3).** The action bar **(2)** will be immediately displayed at the top of the window.
- Click one of the following icons:
  - **Scan now**: lets you create a scan task which will be run immediately on the selected computers.
  - **Schedule scan**: takes you to the **Tasks** area where you can create a recurring and/or scheduled task. The task template will be partially populated: the Recipients field will display the selected computers. Fill in the remaining options, as explained in section 15.3 Creating a task from the Tasks area

19.3.3 Scan options

The scan options let you configure the scan engine parameters in order to scan the computers' file system. The following options are available:

- **Scan type**
  - **The entire computer**: runs an in-depth scan of the computer, including every connected storage device.
  - **Critical areas**: quick scan of the following directories:
    - %WinDir%\system32
    - %WinDir%\SysWow64
    - Memory
    - Boot system

    - Cookies
  - **Specific items**: lets you enter the full path of massive storage devices. This option supports environment variables. The solution will scan the specified path and every folder and file it may contain.
- **Detect viruses**: detects programs that enter computers with malicious purposes. This option is always enabled.
- **Detect hacking tools and PUPs**: detects potentially unwanted programs, as well as programs that can be used by hackers to carry out actions that cause problems for the user of the affected computer.
- **Detect suspicious files**: in scheduled scans, the computer software is scanned statically, that is, running items are not scanned. Therefore it may be necessary to enable heuristic scanning algorithms to detect all types of threats.
- **Scan compressed files**
- **Exclude the following files from scans**
  - Do not scan files excluded from the permanent protections: the files whose execution was allowed by the administrator won't be scanned. These files will always run, along with any file globally excluded from the console.
  - Extensions
  - Files
  - Directories

19.4. Computer restart

The Web console lets administrators restart computers remotely. This is very helpful if you have computers whose protection needs updating or if there are protection problems to fix.

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- To restart a single computer, click the computer's context menu on the computer list.
- To restart multiple computers, use the checkboxes to select the computers to restart, and click the global context menu.
- From the drop-down menu, select **Restart**.

19.5. Computer isolation

This feature only works on Windows workstations. Linux, macOS and Android devices do not support this technology.

Panda Adaptive Defense 360 lets administrators isolate computers on demand, preventing threats from spreading and blocking the exfiltration of confidential data.

When a computer is isolated, its communications are restricted except for the following:

- Access to the computer from the management console to enable administrators to analyze and resolve any detected problems by using the tools provided by **Panda Adaptive Defense 360**.
- Access and remote control via Panda Systems Management, to enable administrators to gather extended information and resolve problems through the solution's remote management tools (remote desktop, remote command line, remote event viewer, etc.).

For more information about the remote management tools provided by Panda Systems Management, refer to the Systems Management Administrator's Guide at

All other products and services installed on the affected workstation or server won't be able to communicate via the Internet/network unless the administrator sets the appropriate exceptions. Refer to section 19.5.4 Advanced isolation options: Program exclusion.

19.5.1 Computer isolation statuses

The **Isolate computer** and **Stop isolating the computer** operations are performed in real time. However, the process may be delayed if the affected computer is offline. To reflect the exact situation of a computer, **Panda Adaptive Defense 360** distinguishes among four different isolation statuses through the following icons:

- **Isolating** : the administrator launched a request to isolate one or more computers and the request is being processed.
- **Isolated** : the isolation process has been completed and the computer's communications have been restricted.
- **Stopping isolation** : the administrator launched a request to stop isolating one or more computers and the request is being processed.
- **Not isolated**: the process to stop isolating a computer has been completed. The computer is allowed to communicate with other computers based on the settings defined in other modules (firewall, IDS), products, or the operating system itself.

These icons are displayed next to the IP address column in the Licenses and Computer protection status lists, as well as in the Computers area.

19.5.2 Isolating one or more computers from the organization's network

Follow these steps to isolate one or more computers from the network:

- Click the **Computers** menu at the top of the console, or access any of the following computer lists:
  - **Computer protection** status
  - **Licenses**

- Select the computers to isolate by clicking the relevant checkboxes.
- Select **Isolate computer** from the action bar. A window will be displayed with the link **Advanced options**.
- In **Advanced options**, specify the programs that will be allowed to continue communicating with the rest of the network/Internet despite the computer being isolated (isolation exclusion).
- Click **Isolate**. The computer's status will change to **Isolating**.

Follow these steps to isolate a computer group:

- Click the **Computers** menu at the top of the console.
- From the computer tree, click the folder view and select the group to isolate.
- Select the **Isolate computers** option from the context menu and click Isolate.
- To isolate all computers on the network, expand the context menu associated with the **All** node.

19.5.3 Stopping a computer from being isolated

Follow the steps below to stop a computer from being isolated:

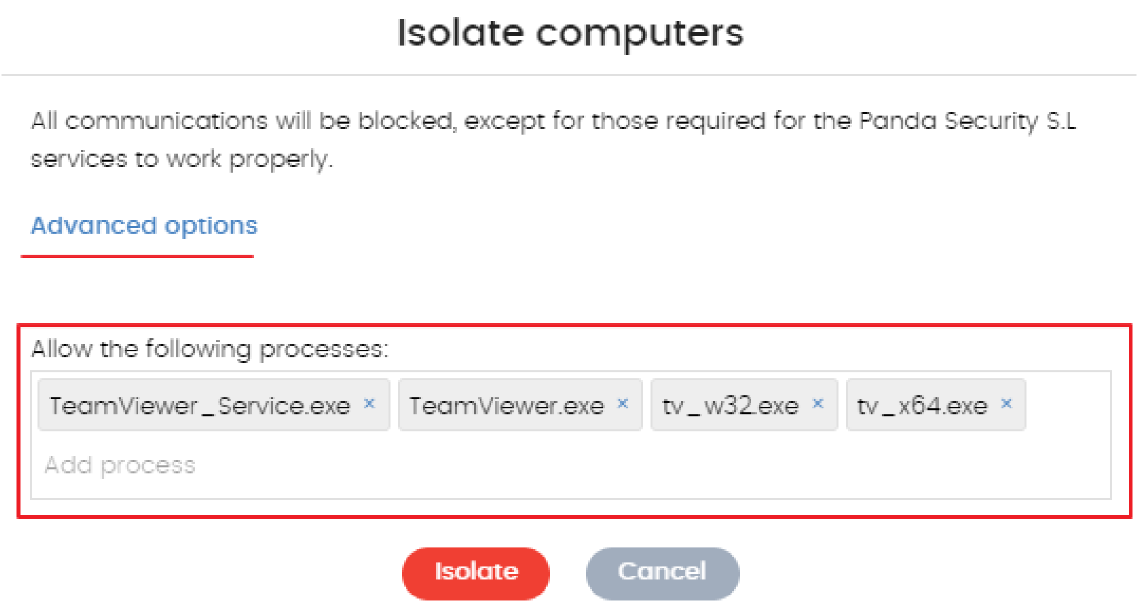
- Follow the steps indicated in section 19.5.2.
- Select **Stop isolating the computer** from the action bar.
- The computer's status will change to **Stopping isolation**.

19.5.4 Advanced isolation options: Program exclusion

Isolating a computer blocks all communications established from the computer with the exception of those established by the Panda Security product processes. All other processes, including those belonging to user programs, will be prevented from communicating with the other computers in the organization. To exclude specific programs from this behavior and allow them to communicate normally, enabling the user to continue making use of certain applications and allowing the administrator to use the tools required to diagnose and resolve issues, click the Advanced options link displayed in the window shown when isolating a computer.

A text box will be shown where you can enter the programs you'd like to exclude from the isolation operation. These programs will continue to communicate normally with the other computers in the organization or with external computers, based on the settings defined in other **Panda Adaptive Defense 360** modules (firewall, IDS), in other products, or in the operating system's firewall.

To speed up the configuration process, the management console maintains the latest settings saved by the administrator regarding excluded processes. This way, when excluding a computer’s processes, the relevant text box will display the processes that were excluded in the preceding isolation operation. These processes can be edited based on the administrator's needs.



Isolate computers

All communications will be blocked, except for those required for the Panda Security S.L services to work properly.

Allow the following processes:

TeamViewer_Service.exe × TeamViewer.exe × tv_w32.exe × tv_x64.exe ×

Figure 129: Isolation settings window

19.5.5 Processes allowed and denied on an isolated computer

Panda Adaptive Defense 360 will allow those communications required for the solution to work properly and for the administrator to be able to perform remote forensic analyses and use the remediation tools provided by Panda Adaptive Defense 360 and Panda Systems Management. Below is a list of the processes that are allowed and denied on an isolated computer.

Allowed processes and services on an isolated computer

- All services required for the computer to be part of the corporate network: DHCP services to obtain IP addresses, ARP, WINS and DNS host name resolution services, etc.
- Services required to communicate with the default gateway.
- Services required by the Panda Adaptive Defense 360 software to communicate with Panda Security's cloud in order to enable the protection engines to work, download signature files and let administrators perform remote management tasks via the Web console.
- Services required by an isolated machine with the discovery computer role to perform discovery tasks.
- Services required by an isolated machine with the cache role to act as a file server.
- Services required by a machine with the Panda proxy role assigned to act as a connection proxy.
- Connections required by Panda Systems Management's remote access tools:
  - Remote command line
  - Remote desktop (VNC, RDP)
  - File transfer
  - Remote file viewer

- Remote registry
- Remote task manager
- Drive information tool
- Remote registry editor
- Quick tasks

- Services required for SNMP monitoring of devices not compatible with Panda Systems Management and with the 'connection node' role assigned.
- Services required for script execution, task execution, etc.

Blocked processes and services on an isolated computer

- Connection to the operating system's Windows Update feature.
- Windows Update and Patch Management policies.
- Communication with the scripts and modules developed by the administrator or integrated from the Panda Systems Management ComStore.
- Web browsing, FTP, mail and other Internet protocols.
- SMB file transfer between PCs on the network.

19.6. Reporting a problem

It is possible that the **Panda Adaptive Defense 360** software may occasionally function incorrectly. Some symptoms could include:

- Errors reporting the computer status.
- Errors downloading knowledge or engine updates.
- Engine errors.

If **Panda Adaptive Defense 360** functions incorrectly on some network computers, you can contact Panda Security's support department through the console and automatically send all the information required for diagnosis. To do this, click **Computers**, select the computers with errors, and click the context menu. A menu will appear entitled **Report a problem**.

19.7. Allowing external access to the Web console

If the administrator finds problems they can't resolve, they can grant Panda Security's support team access to their console. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- On the **Users** tab, click **Allow the Panda Security S.L. team to access my console.**

20. Alerts

Email alerts

20.1. Introduction

The alert system is a tool provided by **Panda Adaptive Defense 360** to quickly notify administrators of important situations to ensure the proper operation of the security service.

Namely, an alert will be sent to the administrator every time one of the following events occur:

- A malware specimen, PUP or exploit is detected
- An unknown item (malware or PUP) is reclassified
- A process unknown to **Panda Adaptive Defense 360** is blocked while it is being classified
- There is a change in the license status
- There are install errors or a computer is unprotected

20.2. Email alerts

Email alerts are messages sent by **Panda Adaptive Defense 360** to the administrator's email account. As previously explained, the system will send a message to the configured recipients' email accounts when certain events occur.

20.2.1 Configuring email alerts

Go to the **Settings** menu at the top of the Web console. Then click **Alerts** from the left-hand menu.

This screen lets administrators specify the email addresses to send messages to (**Send the alerts to the following address**:). You can also enable and disable each of the alert types to send.

20.2.2 Access permissions and alerts

Alerts are defined independently for each user of the Web console. The contents displayed in an alert will vary depending on the managed computers that are visible to the recipient's role.

20.2.3 Alert types

Malware/PUP detections

These alerts have the following characteristics:

- An alert is generated for each malware detected by the real-time protection for files.
- Only for malware detected on Windows computers.
- A maximum of two messages will be sent per computer/malware/day.

The alert message will contain the following information:

- Whether it is the first or second message generated for that threat/computer/day.
- Name of the malicious program.
- Name of the computer where the item was detected.
- Group to which the computer belongs.
- Detection date and time (in UTC format).
- Path of the malicious program.
- Hash.
- Actions taken by the program (life cycle), if it managed to run before being blocked.
- Occurrences on the network: list of computers where the malware was found.

Exploit detections

These alerts have the following characteristics:

- An alert is generated for each exploit attempt detected.
- There is a maximum of 10 alerts per day/computer/exploit.
- Only for exploit attempts detected on Windows computers.

The alert message will contain the following information:

- Name, path and hash of the program that was hit by the exploit attempt
- Name of the computer where the exploit attempt was detected
- Group to which the computer belongs
- Detection date and time (in UTC format)
- Action taken by **Panda Adaptive Defense 360**
- Computer risk level
- Assessment of the target program's security level
- Actions taken by the exploit (life cycle), if it managed to run before being blocked
- Possible source of the exploit

Alerts generated when a program that is being classified gets blocked

These alerts have the following characteristics:

- An alert is generated for each unknown program detected by the real-time protection for files.
- Only for unknown programs detected on Windows computers.

The alert message will contain the following information:

- Name of the unknown program

- Name of the computer where the item was detected
- Group to which the computer belongs
- Detection date and time (in UTC format)
- Path of the unknown program.
- Hash.
- Actions taken by the program (life cycle), if it managed to run before being blocked.
- Occurrences on the network: list of computers where the unknown program was found.

Alerts generated when a file allowed by the administrator is finally classified

Administrator-allowed files are those files which the administrator has allowed to run despite being blocked by **Panda Adaptive Defense 360** for being unknown or having been categorized as a threat. As soon as **Panda Adaptive Defense 360** finishes classifying a previously unknown item, it will inform the administrator of its verdict, as this will affect the action to be taken on the item (allow or block), depending on the reclassification policy defined by the administrator.

Refer to chapter 17 Managing threats, quarantined items and items being classified, for more information about reclassification policies

- **Alert generated when an unknown item is finally classified as goodware**

The system will generate an alert every time an unknown item that was allowed to run by the administrator is finally classified. And, depending on the verdict, the administrator's exclusion will be kept or removed based on the selected reclassification policy. In the case of goodware items, the exclusion will be automatically removed by the system and the item will be allowed to continue running.

- **Alert generated when an unknown item is reclassified as malware/PUP**

The system will generate an alert every time an unknown item that was allowed to run by the administrator is finally classified. And, depending on the verdict, the administrator's exclusion will be kept or removed based on the selected reclassification policy. If the item is classified as malware/PUP and the exclusion is kept, the item will continue to be allowed to run, posing a threat to the system. If, however, the exclusion is removed, the item will be prevented from running, rendering it harmless to the organization.

Malware detections

An alert message will be generated every 15 minutes if the following condition is met:

- Malware is detected in real time by an on-demand or scheduled scan.
- Compatible with Windows, Linux, macOS and Android devices.

The alert message will contain the following information:

- Number of malware threats detected within the time range.
- Number of affected computers.

Hacking tools & PUPS detections

An alert message will be generated every 15 minutes if the following condition is met:

- A PUP or hacking tool is detected in real time by an on-demand or scheduled scan.
- Compatible with Windows, Linux, macOS and Android devices.

The alert message will contain the following information:

- Number of threats detected within the time range.
- Number of affected computers.

Alerts generated when a malware URL is blocked

An alert message will be generated every 15 minutes if the following condition is met:

- A malware URL is detected.
- Compatible with Windows, Linux, macOS and Android devices.

The alert message will contain the following information:

- Number of malware URLs detected within the time range.
- Number of affected computers.

Phishing detections

An alert message will be generated every 15 minutes if the following condition is met:

- A phishing website or email is detected.
- Compatible with Windows, Linux, macOS and Android devices.

The alert message will contain the following information:

- Number of phishing attacks detected within the time range.
- Number of affected computers.

Alerts generated when an intrusion attempt gets blocked

An alert message will be generated every 15 minutes if the following condition is met:

- The IDS module blocks an intrusion attempt.
- Compatible with Windows computers.

The alert message will contain the following information:

- Number of intrusion attempts detected within the time range.
- Number of affected computers.

Alerts generated when access to a device is denied

An alert message will be generated every 15 minutes if the following condition is met:

- The user has accessed a peripheral device blocked by the administrator
- Compatible with Windows, Linux, macOS and Android devices.

The alert message will contain the following information:

- Number of device access attempts blocked.
- Number of affected computers.

Protection and installation errors

These alerts have the following characteristics:

- An alert is generated for each unprotected computer found on the network
- An alert is generated for each computer with a protection or install error

The alert message will contain the following information:

- Name of the unprotected computer
- Group to which the computer belongs
- Computer information (name, description, operating system, IP address, group, Active Directory path, domain)
- Detection date and time (in UTC format)
- Reason: **Protection with errors** or **Install error**

Computers without a license

These alerts have the following characteristics:

- An alert is generated every time the solution fails to assign a license to a computer due to lack of sufficient free licenses

The alert message will contain the following information:

- Name of the unprotected computer
- Group to which the computer belongs
- Computer information (name, description, operating system, IP address, group, Active Directory path, domain)
- Detection date and time (in UTC format)
- Reason: **Computer without a license**

Additionally, an alert will also be generated under the following circumstances:

- Every time a license contract expires

The alert message will contain the following information:

- Number of computers that are left without a license
- Number of expired licenses
- Product whose licenses have expired
- License contract expiration date

Installation errors

These alerts have the following characteristics:

- An alert is generated for each computer on the network every time there is a situation that causes the computer's status to change from protected to unprotected.
- If several circumstances are detected at the same time that may cause a computer's status to change from protected to unprotected, only one alert will be generated with a summary of all those circumstances.
- The following computer statuses will trigger an alert
  - **Protection with errors**: if the status of the antivirus and/or advanced protection installed on a computer shows an error, an alert will be generated. This only applies to those computers with an operating system that supports those protections.
  - **Installation error**: if an installation error occurs that requires user intervention (e.g. insufficient disk space), an alert will be generated. Temporary errors that can be resolved autonomously after a number of retries won't generate alerts.
  - **No license**: if a computer doesn't receive a license after registration because there are aren't any free licenses, an alert will be generated.
- The following computer statuses will not trigger an alert:
  - **No license**: no alerts are generated if the administrator manually removes a computer's license or when Panda Adaptive Defense 360 automatically removes a computer's license because the number of purchased licenses has been reduced.
  - **Installing**: it doesn't make much sense to generate an alert every time the protection is installed on a computer on the network.

- **Disabled protection**: this status is the consequence of a voluntary change of settings, so no alert is generated.
- **Outdated protection**: this status doesn't necessarily mean that the computer is unprotected, despite its protection is out of date.
- **Pending restart**: this status doesn't necessarily mean that the computer is unprotected.
- **Outdated knowledge**: this status doesn't necessarily mean that the computer is unprotected.

The alert message will contain the following information:

- Computer name
- Protection status
- Reason for the change of status

Discovery of an unmanaged computer

An alert message will be generated if the following conditions are met:

- Every time a discovery computer completes a discovery task
- The discovery task finds never-seen-before computers on the network

The alert message will contain the following information:

- Name of the discovery computer.
- Number of discovered computers.
- Link to the list of all unmanaged computers discovered.

21. Reports

On-demand generation of executive reports

Scheduled sending of executive reports

21.1. Introduction

Panda Adaptive Defense 360 allows administrators to generate and send, automatically or manually, executive reports that consolidate all the information collected by the solution in the selected period.

21.2. On-demand generation of executive reports

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

21.2.1 Information required to generate an on-demand report

The following information will be required:

- **Information for the following dates**: specify the time interval to be covered by the report
  - **Last month**
  - **Last 7 days**
  - **Last 24 hours**
- **Information for the following computers**: specify the computers to extract information from
  - **All computers**
  - **Selected computers**: displays the group tree. Use the checkboxes to select the groups you want
- **Include the following content**: lets you select the type of information to be included in the report
  - **License status**: shows the number of contracted and used licenses. For more information, refer to chapter 5 Licenses
  - **Network status**: shows the way the **Panda Adaptive Defense 360** software is working on those computers where it is installed. It includes information from the following dashboard widgets: **Unprotected computers** and **Outdated protection**.
  - **Detections**: shows the threats detected across the network. It includes information from the following dashboard widgets: **Malware activity**, **PUP activity**, **Threats detected by the antivirus** and **Content filtering for Exchange servers.**
  - **Web access and spam**: shows the users' Internet activity. It includes information from the following dashboard widgets: **Web access**, **Top 10 most accessed categories**, **Top 10 most accessed categories by computer**, **Top 10 most blocked categories**, **Top 10 most blocked categories by computer** and **Spam detected on Exchange servers**.

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

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

21.3. Scheduled sending of executive reports

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

21.3.1 Information required to generate a scheduled report

The scheduled reports window displays a list of all configured reports. Click **Add** to add a new scheduled report. To delete a configured report, click the 🗑 icon. To edit a configured report, click its name.

To configure a scheduled report, enter the following information:

- **Name**: name of the scheduled report that will be displayed on the list of configured reports.
- **Send automatically**: lets you schedule the sending of the executive report, or save the settings without sending the report.
- **Date and frequency**: lets you specify the day when the report will be sent and its frequency. Select **Every day**, **Every week** or **Every month**. The content of the drop-down menus will vary depending on your selection.
- **The following information:** this section displays the following settings: **Dates**, **Computers** and **Content**. Click the arrow to the right to configure the following options:
  - **Information for the following dates**: specify the time interval to be covered by the report
    - **Last month**
    - **Last 7 days**
    - **Last 24 hours**
  - **Information for the following computers**: specify the computers to extract information from
    - **All computers**
    - **Selected computers**: displays the group tree. Use the checkboxes to select the groups you want
  - **Include the following content**: lets you select the type of information to be included in the report
    - **License status**: shows the number of contracted and used licenses. For more information, refer to chapter 5 Licenses
    - **Network status**: shows the way the **Panda Adaptive Defense 360** software is working on those computers where it is installed. It includes information from the following dashboard widgets: **Unprotected computers** and **Outdated protection**.
    - **Detections**: shows the threats detected across the network. It includes information

from the following dashboard widgets: **malware activity**, **PUP activity**, **Threats detected by the antivirus** and **Content filtering for Exchange servers**. Refer to chapter 16 Malware and network visibility for more information.

  - **Web access and spam**: shows the users' Internet activity. It includes information from the following dashboard widgets: **web access**, **Top 10 most accessed categories**, **Top 10 most accessed categories by computer**, **Top 10 most blocked categories**, **Top 10 most blocked categories by computer** and **Spam detected on Exchange servers**.

- **To**: enter the email address that the report will be sent to. You can enter multiple addresses separated by commas.

- **CC:**

- **BCC:** use this field to send a copy of the report to a recipient without notifying other recipients that this was done.

- **Subject:** specify the email subject line.

- **Format**: select the format of the email attachment (the report): PDF, Excel, or Word.

- **Language**: select the language of the report.

22. Controlling and monitoring the management console

22.1. Introduction

This chapter describes the resources implemented in **Panda Adaptive Defense 360** to control and monitor the actions taken by the network administrators that access the Web management console.

These resources are as follows:

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

22.2. What is a user account?

A user account is a resource managed by **Panda Adaptive Defense 360**, comprising a set of information that the system uses to regulate administrator access to the Web console and define the actions that administrators can take on users' computers.

User accounts are only used by the administrators that access the **Panda Adaptive Defense 360** console. In general, each administrator will have a unique personal account, and it is possible to create as many accounts as necessary.

Unlike the rest of this manual, where the word "user" refers to the person that uses a computer or device, in this chapter "user" refers to the account used by the administrator to access the Web console

22.2.1 User account structure

A user account comprises the following items:

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

22.2.2 What is the main user?

The main user is the user account provided by Panda Security to the customer when providing the **Panda Adaptive Defense 360** service. This account has the **Full control** role, which is explained below.

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

22.3. What is a role?

A role is a set of permissions for accessing the console that are applied to one or more user accounts. This way, a specific administrator is authorized to view or edit certain resources in the console, depending on the role assigned to the user account with which they access the **Panda Adaptive Defense 360** console.

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

22.3.1 Role structure

A role is made up of the following:

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

22.3.2 Why are roles necessary?

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

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

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

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

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

Depending on its purpose, a computer may be assigned to a technician specialized in this field. For example, Exchange mail servers may be assigned to a group of specialized technicians, and other systems, such as Android devices, may not be visible to this group of technicians.

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

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

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

22.3.3 Full Control role

The **Panda Adaptive Defense 360** license comes with the **Full Control** role predefined. The default administration account belongs to this role, and with this it is possible to take almost all actions that are available in the console.

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

22.3.4 Read-only role

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

The permissions enabled are as follows:

- View security settings for workstations and servers.
- View security settings for Android devices.
- View sensitive data monitoring settings.
- View patch management settings.
- View detections and threats.
- View access to Web pages and spam.
- Access to advanced reports

22.4. What is a permission?

A permission regulates access to a particular aspect of the management console. There are 15 types of permissions that provide access to many aspects of the **Panda Adaptive Defense 360** console. A specific configuration from all available permissions generates a role, which can be assigned to one or more user accounts.

The **Panda Adaptive Defense 360** permissions are as follows:

- Manage users and roles
- Assign licenses
- Modify the Computers tree
- Add, discover and delete computers
- Configure proxies and language
- Modify per-computer settings (updates, passwords, etc.)
- Restart computers
- Configure security settings for workstations and servers
- View security settings for workstations and servers
- Configure security settings for Android devices
- View security settings for Android devices
- View detections and threats
- View access to Web pages and spam
- Access to Advanced Reporting Tool
- Launch scan and disinfection tasks
- Exclude threats temporarily (malware, PUPs and blocked items)
- Configure patch management
- Install patches
- View available patches
- Configure personal data monitoring
- View sensitive data monitoring settings
- Search for data on computers

22.4.1 Understanding permissions

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

Manage users and roles

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

Assign licenses

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

Modify the Computers tree

- **Enabled**: the account user has complete access to the Groups tree, and can create and delete groups, as well as moving computers to groups that have been created.
- **Enabled with permission conflict**: due to the inheritance rules, making changes to the

Computers tree may involve changing the affected computers' settings. If any of the permissions that allow administrators to change settings is disabled, they will only be permitted to create groups, delete empty groups and rename groups. The permissions that allow administrators to change settings are:

- Modify network settings (proxies and cache)
- Modify per-computer settings (updates, passwords, etc.)
- Configure security settings for workstations and servers
- Configure security settings for Android devices
- Launch scan tasks
- Configure personal data monitoring

- **Disabled**: the account user can view the Groups tree and the settings assigned to each group, but cannot create new groups or move computers. They can change the group settings, as this action is governed by the permissions **Configure security for workstations and servers**, or **Configure security for Android devices**.

Add, discover and delete computers

- **Enabled**: the account user can distribute the installer to their network computers and integrate them into the **Panda Adaptive Defense 360** 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 discovery computers.
- **Disabled**: the account user cannot download the installer, nor distribute it to computers. They cannot delete computers from the console or access the computer discovery feature.

Configure proxies and languages

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

Given that moving a computer in the Groups tree can change the assigned Proxy and language settings, when you disable Configure Proxies and languages you also have to disable the permission Modify Groups tree.

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

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

Given that moving a computer in the Groups tree can change the assigned Per-computer settings, when you disable Modify per-computer settings you also have to disable the permission Modify Groups tree.

Restart computers

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

Isolate computers

- **Enabled**: the account user can isolate and stop isolating Windows workstations and servers from the **Computers** menu at the top of the console, and from the **Licenses** and **Protected computers** lists. Computers are isolated through the Isolate computers option available in the context menu and on the action bar.
- **Disabled**: the account user won't be able to isolate computers.

Configure security settings for workstations and servers

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

> ***Given that moving a computer in the Groups tree can change the assigned Workstations and servers settings, when you disable Configure security for workstations and servers you also have to disable the permission Modify Groups tree.***

When you disable this permission, you will see the permission **View security settings for workstations and servers.**

View security settings for workstations and servers

> ***This permission can only be accessed when you disable Configure security for Workstations and servers.***

- **Enabled**: the account user can only see the security settings created as well as the settings of a computer or group.
- **Disabled**: the account user won’t be able to see the security settings created nor access the settings assigned to each computer.

Configure security settings for Android devices

- **Enabled**: the user account can create, edit, delete and assign settings for Android devices.
- **Disabled**: the user account will not be able to create, edit, delete or assign settings for Android devices.

Given that moving a computer in the Groups tree can change the assigned Android device settings, when you disable Configure security for Android devices you also have to disable the permission Modify Groups tree.

When you disable this permission, you will see the permission **View security settings for Android devices**, which is explained below.

View security settings for Android devices

This permission can only be accessed when you disable the permission Configure security for Android devices

- **Enabled**: the account user will be able to see the settings created for Android devices as well as the settings for a specific Android device or group.
- **Disabled**: the account user won't be able to see the settings created for Android devices nor the settings for a specific Android device or group.

View detections and threats

- **Enabled**: the account user will be able to see the panels and lists in the **Security** section of the **Status** menu**,** and create new lists with custom filters.
- **Disabled**: the account user won't be able to see the panels and lists in the **Security** section of the **Status** menu**,** nor create new lists with custom filters.

Access to features related to excluding and unblocking threats and unknown items is determined through the permission Exclude threats temporarily (Malware, PUPs and blocked items).

View access to Web pages and spam

- **Enabled**: the account user will be able to access the panels and lists in the **Web access and spam** section of the **Status** menu.
- **Disabled**: the account user won't be able to access the panels and lists in the **Web access and spam** section of the **Status** menu.

Access to Advanced Reporting Tool

- **Enabled**: the account user will be able to access the **Advanced Reporting Tool** section from the panel on the left in the **Status** menu**.**
- **Disabled**: access to the **Advanced Reporting Tool** section is hidden.

Launch scan and disinfection tasks

- **Enabled**: the account user will be able to create, edit and delete scan tasks.
- **Disabled**: the account user won't be able to create, edit or delete scan tasks. They will only be able to list the tasks and view the settings.

Exclude threats temporarily (Malware, PUPs and blocked items)

- **Enabled**: the account user can unblock, prevent detection, block, not allow and change the behavior with respect to reclassified malware, PUPs and unknown items in the process of classification.
- **Disabled**: the account user won't be able to unblock, prevent detection, block, not allow or change the behavior with respect to reclassified malware, PUPs and unknown items in the process of classification

> ***It is necessary to enable View detections and threats in order to fully implement Exclude threats temporarily (Malware. PUPs, and blocked items).***

Configure patch management

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

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

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

View patch management settings

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

- **Enabled**: the account user can see the patch management settings created as well as the settings assigned to a computer or group. However, they cannot edit those settings.
- **Disabled**: the account user won't be able to see the patch management settings created nor access the settings assigned to each computer.

Install patches

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

- **Enabled**: the account user can create patching tasks and access the following lists: **Available patches**, **'End-Of-Life' programs** and **Installation history**.

- **Disabled**: the account user won’t be able to create patching tasks.

View available patches

This permission is only accessible when you disable the Install patches permission.

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

Configure personal data monitoring

- **Enabled**: the account user can create, edit, delete and assign Personal data monitoring settings to Windows computers.
- **Disabled**: the account user won't be able to create, edit, delete or assign Personal data monitoring settings to Windows computers.

View personal data monitoring

This permission is only accessible when you disable the permission Configure personal data monitoring.

- **Enabled**: the account user is only permitted to see the Personal data monitoring settings created, as well as the settings for a specific computer or computer group.
- **Disabled**: the account user won’t be able to see the Personal data monitoring settings created nor access the settings assigned to each computer.

Search for data on computers

- **Enabled**: the account user can access the widgets for searching for files by their name and content across the corporate network.
- **Disabled**: the account user won't be able to access the widgets for searching for files by their name and content across the corporate network.

22.5. Accessing the user account and role settings

In the **Settings** menu**,** when you click the **Users** panel, there are two sections associated with the management of roles and user accounts:

- **Users**: this lets you create new user accounts and define the roles they belong to.
- **Roles**: this lets you create and edit settings for accessing **Panda Adaptive Defense 360** resources.

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

22.6. Creating and configuring user accounts

In the **Settings** menu, in the panel on the left, click **Users** and then the tab **Users** and you will be able to take all necessary actions related to the creation and editing of user accounts.

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

22.7. Creating and configuring roles

In the **Settings** menu, click **Users** in the left-hand panel and then **Roles,** and you will be able to take all necessary actions related to the creation and editing of roles.

- **Add new role**: click **Add**. You will be asked for the name of the role, a description (optional), to select from the available computers, and a specific configuration of permissions.
- **Edit a role**: click the name of the role to display a window with all the settings that can be edited.
- **Copy a role:** click the ⧉ icon to display a window with a new role with exactly the same settings as the original one.
- **Delete role**: click the 🗑 icon of a role to delete it. If, when you delete a role, it already has user accounts assigned, the process of deleting it will be canceled.

22.8. User account activity log

Panda Adaptive Defense 360 logs every action taken by network administrators in the Web management console. This way, it is very easy to find out who made a certain change, when and on which object.

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

22.8.1 Action log

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

Fields displayed in the 'Actions' list

Field	Comments	Values
Date	Date and time that the action was carried out	Date
User	User account that performed the action	Character string
Action	Type of action	Access Add scheduled report Assign license Block Delete Change 'Per-computer settings' Change 'Security settings' Change group Change parent group Change 'Proxy and language' Cancel Configure discovery Create Unassign license Stop allowing Unblock Discover now Designate cache computer Designate discovery computer Designate Panda proxy Edit Edit description Edit scheduled report Edit name Delete Delete scheduled report Inherit 'Per-computer settings' Inherit 'Security settings' Inherit 'Proxy and language' Install Locate Move to Active Directory path Move computers to their Active Directory path Hide Allow Publish Restart computers Restore communications Revoke cache computer Revoke discovery computer Revoke Panda proxy Sync group

		Make visible
Item type	Type of console object the action was performed on	Threat Settings Android device Computer Unmanaged computer Filter Group Device group Executive report Advanced reports List Preference for sending emails Role Task - Security scan User
Item	Console object the action was performed on	Character string

Table 84: fields in the Action log

Fields displayed in the exported file

Field	Comments	Values
Date	Date and time that the action was carried out	Date
User	User account that performed the action	Character string
Action	Type of action	Access Add scheduled report Assign license Block Delete Change 'Per-computer settings' Change 'Security settings' Change group Change parent group Change 'Proxy and language' Cancel Configure discovery Create Unassign license Stop allowing Unblock Discover now Designate cache computer Designate discovery computer Designate Panda proxy Edit Edit description Edit scheduled report Edit name Delete Delete scheduled report Inherit 'Per-computer settings' Inherit 'Security settings' Inherit 'Proxy and language' Install

Field	Comments	Values
		Locate Move to Active Directory path Move computers to their Active Directory path Hide Allow Publish Restart computers Restore communications Revoke cache computer Revoke discovery computer Revoke Panda proxy Sync group Make visible
Item type	Type of console object the action was performed on	Threat Settings Android device Computer Unmanaged computer Filter Group Device group Executive report Advanced reports List Preference for sending emails Role Task - Security scan User
Item	Console object the action was performed on	Character string

Table 85: fields in the 'Action log' exported file

Filter tool

Field	Comments	Values
From		Date
To		Date
Users		List of all user accounts that have been created in the management console

Table 86: filters available in the Action log

22.8.2 Session log

The **Sessions** section displays a list of all accesses to the management console, and allows you to export the information to an Excel file and filter the information.

Fields displayed in the Sessions list

Field	Comments	Values
Date	Date and time that the access took place	Date
User	User account that accessed the console	Character string
Activity		Log in Log out
IP address	IP address from which the console was accessed	Character string

Table 87: fields in the 'Sessions' list

Fields displayed in the exported file

Field	Comments	Values
Date	Date and time that the access took place	Date
User	User account that accessed the console	Character string
Activity		Log in Log out
IP address	IP address from which the console was accessed	Character string

Table 88: fields in the 'Sessions' exported file

Filter tool

Field	Comments	Values
From		Date
To		Date
Users		List of all user accounts that have been created in the management console

Table 89: filters available the 'Sessions' list

23. Appendix 1: Panda Adaptive Defense 360 requirements

23.1. Requirements for Windows platforms

23.1.1 Supported operating systems

Workstations

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)

Servers

- Windows 2003 (32-bit, 64-bit and R2) SP2 and later
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 and 2016

23.1.2 Hardware requirements

- **Processor**: Pentium 1 GHz
- **RAM**: 1 GB
- **Free space disk for the installation**: 650 MB

23.2. Requirements for Windows Exchange platforms

23.2.1 Supported operating systems

- **Exchange 2003**: Windows Server 2003 (32- bit) SP2+ and Windows Server 2003 R2 (32- bit)
- **Exchange 2007**: Windows Server 2003 (64-bit) SP2+, Windows Server 2003 R2 (64-bit), Windows 2008 (64-bit) and Windows 2008 R2
- **Exchange 2010**: Windows 2008 (64-bit) and Windows 2008 R2
- **Exchange 2013**: Windows Server 2012 and Windows Server 2012 R2
- **Exchange 2016**: Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

23.2.2 Software and hardware requirements

The hardware requirements to install the protection on Exchange server are the ones determined by the Exchange server:

- Exchange 2003:

http://technet.microsoft.com/en-us/library/cc164322(v=exchg.65).aspx

- Exchange 2007:

http://technet.microsoft.com/en-us /library/aa996719(v=exchg.80).aspx

- Exchange 2010:

http://technet.microsoft.com/en-us /library/aa996719(v=exchg.141).aspx

- Exchange 2013

http://technet.microsoft.com/en-us /library/aa996719(v=exchg.150).aspx

- Exchange 2016

https://technet.microsoft.com/en-us /library/aa996719(v=exchg.160).aspx

23.2.3 Supported Exchange versions

- Microsoft Exchange Server 2003 Standard and Enterprise (SP1/SP2)
- Microsoft Exchange Server 2007 Standard and Enterprise (SP0/SP1/SP2/SP3)
- Microsoft Exchange Server 2007 included in Windows SBS 2008
- Microsoft Exchange Server 2010 Standard and Enterprise (SP0/SP1/SP2)
- Microsoft Exchange Server 2010 included in Windows SBS 2011
- Microsoft Exchange Server 2013 Standard and Enterprise
- Microsoft Exchange Server 2016 Standard and Enterprise

23.3. Requirements for macOS platforms

23.3.1 Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra

23.3.2 Hardware requirements

- **Processor**: Intel Core 2 Duo
- **RAM**: 2 GB
- **Free space disk for installation**: 400 MB
- **Ports**: ports 3127, 3128, 3129 y 8310 must be accessible for the Web anti-malware and URL filtering to work

23.4. Requirements for Linux platforms

23.4.1 Supported 64-bit distributions

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

23.4.2 Supported kernel version

From version 3.13 up to version 4.10

23.4.3 Supported file managers

- Nautilus
- PCManFM
- Dolphin

23.4.4 Hardware requirements

- **Processor**: Pentium 1 GHz
- **RAM**: 1.5 GB
- **Free space disk for installation**: 100 MB
- **Ports**: port 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware and URL filtering to work

23.4.5 Installation package dependencies

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

Table 90: required libraries for installation

23.5. Requirements for Android platforms

23.5.1 Supported operating systems

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

23.5.2 Hardware requirements

A minimum of 10 MB of internal memory is required. Depending on the model, it is possible that the required space be larger.

23.5.3 Network requirements

For the push notifications to work correctly from the company's network, it is necessary to open ports 5228, 5229 and 5230 to the whole set of ASN 15169 IP addresses belonging to Google.

23.6. Web console access

The **Panda Adaptive Defense 360** management console can be accessed with the latest version of the following compatible browsers.

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

23.7. Access to service URLs

For **Panda Adaptive Defense 360** to work correctly, the protected computers must be able to access the following URLs.

- https://*.pandasecurity.com
- http://*.pandasecurity.com
- https://*.windows.net

- https://pandasecurity.logtrust.com
- http://*.pandasoftware.com

Inbound and outbound traffic (anti-spam and URL filtering)

- http://*.pand.ctmail.com
- http://download.ctmail.com
- http://dns.ctmail.com.

Ports

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

Patch and update download (Panda Patch Management)

Refer to the following support article https://www.pandasecurity.com/spain/support/card?id=700044 for a full list of the URLs that must be accessible by the network computers that will receive patches, or by the network computers with the cache/ repository role.

24. Appendix 2: creating and managing a Panda Account

Creating a Panda Account
Activating your Panda Account

24.1. Introduction

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

With a Panda Account, it is the administrator who creates and activates the access credentials to the **Panda Adaptive Defense 360** Web console.

24.2. Creating a Panda Account

Follow the steps below to create a Panda Account.

Open the email message received from Panda Security

- After purchasing **Panda Adaptive Defense 360,** you will receive an email message from Panda Security.
- Click the link in the message to access a site from which you will be able to create your Panda Account.

Fill out the form

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

24.3. Activating your Panda Account

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

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

Once your Panda Account has been successfully activated, you will be taken to the Panda Cloud site home page. There, you will able to access your **Panda Adaptive Defense 360** Web console. To do that, simply click the solution's icon in the **My Services** section.

25. Appendix 3: list of uninstallers

On installing **Panda Adaptive Defense 360**, other security products might be detected on the computer. In that case, Table 91 shows the products that will be automatically uninstalled before installing **Panda Adaptive Defense 360** across the network.

Vendor	Product name
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32-bit Edition) AVG Internet Security 2013 (64-bit Edition) AVG AntiVirus Business Edition 2013 (32-bit Edition) AVG AntiVirus Business Edition 2013 (64-bit Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32-bit* AVG Internet Security Business Edition 2011 64-bit (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVGFree v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir PersonalEdition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x Avira Antivirus 15.x
CA	CA Total Defense for Business Client V14 (32-bit Edition) CA Total Defense for Business Client V14 (64-bit Edition) CA Total Defense R12 Client (32-bit Edition) CA Total Defense R12 Client (64-bit Edition)
Bitdefender	BitDefender Endpoint Protection 6.x BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32-bit) Check Point Endpoint Security 8.x (64-bit)
Eset	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32-bit) ESET NOD32 Antivirus 4.X (32-bit) ESET NOD32 Antivirus 4.X (64-bit) ESET NOD32 Antivirus 5 (32-bit) ESET NOD32 Antivirus 5 (64-bit) ESET NOD32 Antivirus 6 (32-bit) ESET NOD32 Antivirus 6 (64-bit)

	ESET NOD32 Antivirus 7 (32-bit) ESET NOD32 Antivirus 7 (64-bit)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
iSheriff	iSheriff Endpoint Security 5.x
Kaspersky	Kaspersky Endpoint Security 10 for Windows (32-bit Edition) Kaspersky Endpoint Security 10 for Windows (64-bit Edition) Kaspersky Endpoint Security 8 for Windows (32-bit Edition) Kaspersky Endpoint Security 8 for Windows (64-bit Edition) Kaspersky Anti-Virus 2010 9.0.0.459* Kaspersky® Business Space Security Kaspersky® Work Space Security Kaspersky Internet Security 8.0, 7.0, 6.0 (with Windows Vista+UAC, UAC must be disabled) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (with Windows Vista+UAC, UAC must be disabled) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee LiveSafe 2016 x86 / x64 McAfee SaaS Endpoint Protection 6.x, 5.X, 10.5.X (64 y 32 bits) McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0 McAfee Internet Security Suite 2007 McAfee Total Protection Service 4.7* McAfee Total Protection 2008
Norman	Norman Security Suite 10.x (32-bit Edition) Norman Security Suite 10.x (64-bit Edition) Norman Security Suite 9.x (32.bit Edition) Norman Security Suite 9.x (64-bit Edition) Norman Endpoint Protection 8.x/9.x Norman Virus Control v5.99
Norton	Norton Antivirus Internet Security 2008* Norton Antivirus Internet Security 2007 Norton Antivirus Internet Security 2006
Microsoft	Microsoft Security Essentials 1.x Microsoft Forefront EndPoint Protection 2010 Microsoft Security Essentials 4.x Microsoft Security Essentials 2.0 Microsoft Live OneCare Microsoft Live OneCare 2.5*
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205
PC Tools	Spyware Doctor with AntiVirus 9.x

Sophos	Sophos Anti-virus 9.5 Sophos Endpoint Security and Control 10.2 Sophos Endpoint Security and Control 9.5 Sophos Anti-virus 7.6 Sophos Anti-virus SBE 2.5* Sophos Security Suite
Symantec	Symantect.cloud - Endpoint Protection.cloud 22.x Symantec.cloud - Endpoint Protection.cloud 21.x (32-bit) Symantec.cloud - Endpoint Protection.cloud 21.x (64-bit) Symantec EndPoint Protection 14.x (32-bit) Symantec EndPoint Protection 14.x (64-bit) Symantec EndPoint Protection 12.x (32-bit) Symantec EndPoint Protection 12.x (64-bit) Symantec EndPoint Protection 11.x (32-bit) Symantec EndPoint Protection 11.x (64-bit) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
Trend Micro	Trend Micro Worry-Free Business Security 8.x (32-bit Edition) Trend Micro Worry-Free Business Security 8.x (64-bit Edition) Trend Micro Worry-Free Business Security 7.x (32-bit Edition) Trend Micro Worry-Free Business Security 7.x (64-bit Edition) Trend Micro Worry-Free Business Security 6.x (32-bit Edition) Trend Micro Worry-Free Business Security 6.x (64-bit Edition) Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x Trend Micro OfficeScan 11.x
Comodo AntiVirus	Comodo Antivirus V 4.1 32-bit
Panda Security	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX and earlier versions
	Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX and earlier versions
	Panda Global Protection 2017* Panda Internet Security 2017* Panda Antivirus Pro 2017* Panda Gold Protection 2017*
	Panda Global Protection 2016* Panda Internet Security 2016* Panda Antivirus Pro 2016* Panda Gold Protection 2016*
	Panda Global Protection 2015* Panda Internet Security 2015* Panda Antivirus Pro 2015*

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

Table 91: list of uninstallers

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

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

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

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

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

* Kaspersky Anti-Virus 6.0 for Windows workstations:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

If you have a program not included on this list, contact the relevant vendor to find out how to uninstall it before installing **Panda Adaptive Defense 360 on Aether**.

26. Appendix 4: key concepts

100% Attestation Service

A service included in the **Panda Adaptive Defense 360** basic license which classifies 100 percent of the processes run on the organization's workstations and servers, identifying them accurately as goodware or malware without creating false positives or false negatives.

Active Directory

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed directory service for finding a range of information on network environments.

Activity graph/execution graph

Graphical representation of the actions triggered by threats over time.

Adaptive protection cycle

A new security approach based on the integration of a group of services providing protection, detection, monitoring, forensic analysis and remediation capabilities into a single management console accessible from anywhere at any time.

Advanced protection

Technology that continuously monitors and collects information from all processes running on the Windows computers on your network, and sends it to Panda Security's cloud for analysis. This information is analyzed using Machine Learning techniques in Big Data environments, returning an accurate classification (goodware or malware).

Advanced reports

See Advanced Reporting Tool (ART).

Adware

Program that automatically runs, displays or downloads advertising to the computer.

Alert

See Incident.

Anti-spam

Technology that searches for unwanted email based on its contents.

Anti-Tamper protection

A set of technologies aimed at preventing tampering of the **Panda Adaptive Defense 360** processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, anti-exploit techniques, etc.), to detect and remove computer viruses and other threats.

APT (Advanced Persistent Threat)

A set of strategies implemented by hackers and aimed at infecting customers' networks through multiple infection vectors simultaneously. They are designed to go undetected by traditional antivirus programs for long periods of time. Their main aim is financial (through theft of confidential information, intellectual property, etc.).

ARP (Address Resolution Protocol)

A telecommunication protocol used for resolution of Internet layer addresses into link layer addresses. On IP networks, this protocol translates IP addresses into physical MAC addresses.

ASLR (Address Space Layout Randomization)

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

Automatic assignment of settings

See Inheritance.

Audit

A **Panda Adaptive Defense 360** operational mode that lets you view the processes run on the protected network without taking any remedial action (disinfect or block).

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.

Behavior change

Panda Adaptive Defense 360 can behave in two ways when an unknown item that was allowed by the administrator is finally classified as goodware or malware:

- Delete it from the list of allowed threats: if the item is classified as goodware it will continue to run. However, if it is classified as malware it will be prevented from running.
- Keep it on the list of allowed threats: the item will be allowed to run regardless of whether it is malware or goodware.

Block

Action taken by the advanced protection that consists of preventing the execution of programs classified as a threat and programs unknown to **Panda Adaptive Defense 360**.

Blocked item

Depending on the way in which the advanced protection has been configured, **Panda Adaptive Defense 360** will prevent the execution of all programs classified as malware/PUP as well as unknown programs until they are fully classified.

Broadcasting

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network simultaneously, without the need to send it individually to each device. Broadcast packets don't go through routers and use different addressing methodology to differentiate them from unicast packets.

Buffer overflow

Anomaly affecting the management of a process' input buffers. In a buffer overflow, if the size of the data received is greater than the allocated buffer, the redundant data is not discarded, but is written to adjacent memory locations. This may allow attackers to insert arbitrary executable code into the memory of a program on systems prior to Microsoft's implementation of the DEP (Data Execution Prevention) technology.

Cache/Repository (role)

Computers that automatically download and store all files required so that other computers with **Panda Adaptive Defense 360** installed can update their signature file, agent and protection engine without having to access the Internet. This saves bandwidth as it won't be necessary for each computer to separately download the updates they need. All updates are downloaded centrally for all computers on the network.

Cloud (Cloud computing)

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

Compromised process

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

Computers without a license

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers are not protected, but are displayed in the Web management console.

CVE (Common Vulnerabilities and Exposures)

List of publicly known cyber-security vulnerabilities defined and maintained by The MITRE Corporation. Each entry on the list has a unique identifier, allowing CVE to offer a common naming scheme that security tools and human operators can use to exchange information about vulnerabilities with each other.

Device control

Module that allows organizations to define the way protected computers must behave when connecting a removable or mass storage device to them.

DEP (Data Execution Prevention)

A feature implemented in operating systems to prevent the execution of code in memory pages marked as non-executable. This feature was developed to prevent buffer-overflow exploits.

DHCP

Service that assigns an IP address to each computer on a network

Dialer

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

Discovery computer (role)

Computers capable of finding unmanaged workstations and servers on the network in order to remotely install the **Panda Adaptive Defense 360** agent on them.

Disinfectable file

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

Domain

Windows network architecture where the management of shared resources, permissions and users is centralized in a server called a Primary Domain Controller (PDC) or Active Directory (AD).

Domain Name System (DNS)

Service that translates domain names into different types of information, generally IP addresses.

Dwell time

Length of time that a threat has remained undetected on the network.

Entity

Predicate or complement included in the action tables of the forensic analysis module.

Entity (Panda Data Control)

A set of data which, taken as a whole, has its own meaning.

End-of-Life (EOL)

A term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life. Once a product reaches its EOL stage, it stops receiving updates or fixes from the relevant vendor, leaving it vulnerable to hacking attacks.

Environment variable

A string consisting of environment information such as a drive, path or file name, which is associated with a symbolic name that Windows can use. You can use the System applet in the Control Panel or the 'set' command at the command prompt to set environment variables.

Exchange server

Mail server developed by Microsoft. Exchange servers store inbound and/or outbound emails and distribute them to users' email inboxes.

Excluded program

Programs that were initially blocked as they were classified as malware or PUP, but have been selectively and temporarily allowed by the administrator, who excluded them from the scans performed by the solution.

Exploit

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

Firewall

Technology that blocks the network traffic that coincides with certain patterns defined in rules established by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

Filter

A dynamic-type computer container that automatically groups together those 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.

Folder tree

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

Forensic analysis

A series of actions and processes carried out by network administrators with special tools in order to track malicious programs and assess the consequences of an infection.

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.

General Data Protection Regulation (GDPR)

A regulation that governs the protection of the personal data of all individuals within the European Union (EU).

Geolocation

Geographical positioning of a device on a map from its coordinates.

Goodware

A file which, after analysis, has been classified as legitimate and safe.

Group

Static container that groups one or more computers on the network. Computers are assigned to groups manually. Groups simplify the assignment of security settings, and facilitate management of all computers on the network.

Hacking tool

Programs used by hackers to carry out actions that cause problems for the user of the affected computer (allowing the hacker to control the computer, steal confidential information, scan communication ports, etc.).

Hardening

A **Panda Adaptive Defense 360** operational mode that blocks unknown programs downloaded from the Internet as well as all files classified as malware.

Heap Spraying

Heap Spraying is a technique used to facilitate the exploitation of software vulnerabilities by malicious processes.

As operating systems improve, the success of vulnerability exploit attacks has become increasingly random. In this context, heap sprays take advantage of the fact that on most architectures and operating systems, the start location of large heap allocations is predictable and consecutive allocations are roughly sequential. This allows attackers to insert and later run arbitrary code in the target system's heap memory space.

This technique is widely used to exploit vulnerabilities in Web browsers and Web browser plug-ins.

Heuristic scanning

Static scanning that employs a set of techniques to inspect suspicious programs based on hundreds of file characteristics. It can determine the likelihood that a program may take malicious actions when run on a user's computer.

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

ICMP (Internet Control Message Protocol)

Error notification and monitoring protocol used by the IP protocol on the Internet.

Identifier

Keyword used in the **Panda Data Control** searches and which allows an entity type to be selected.

IDP (Identity Provider)

Centralized service for managing user identity verification.

IFilter

A plugin that allows Microsoft's search engines to index various file formats so that they become searchable.

Incident

Message relating to **Panda Adaptive Defense 360**'s advanced protection that may require administrator intervention. Incidents are reported to the administrator through the management console or via email (alerts), and to end users through pop-up messages generated by the agent and displayed locally on the protected device.

Indexing

A process that parses the content of files and stores it in a quick-access database to speed up searching processes.

Indirect assignment of settings

See Inheritance.

Infection vector

The means used by malware to infect users' computers. The most common infection vectors are Web browsing, email and pen drives.

Inheritance

A method for automatically assigning settings to all subsets of a larger, parent group, saving management time. Also referred to as 'automatic assignment of settings' or 'indirect assignment of settings'.

IP address

Number that identifies a device interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

IP (Internet Protocol)

Principal Internet communications protocol for sending and receiving datagrams generated on the underlying link level.

Item reclassification

See Behavior change.

Joke

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

Linux distribution

Set of software packets and libraries that comprise an operating system based on the Linux kernel.

Lock

A **Panda Adaptive Defense 360** operational mode that blocks unknown programs as well as all files classified as malware.

MAC address

48-bit hexadecimal number that uniquely identifies a network card or interface.

Machine learning

This is a branch of artificial intelligence whose aim is to develop technologies capable of predicting behaviors from unstructured data delivered in the form of examples.

Malware

This term is used to refer to all programs that contain malicious code (MALicious softWARE), whether it is a virus, Trojan, worm or any other threat to the security of IT systems. Malware tries to infiltrate or damage computers, often without users knowing, for a variety of reasons.

Malware Freezer

A feature of the quarantine/backup module whose goal is to prevent data loss due to false positives. All files classified as malware or suspicious are sent to the quarantine/backup area, thereby avoiding deleting and losing data if the classification is wrong.

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.

Microsoft Filter Pack

IFilter library package that covers all file formats generated with the Microsoft Office suite.

MTU (Maximum Transmission Unit)

Maximum packet size (in bytes) that the transport will transmit over the underlying network.

Network adapter

Hardware that allows communication among different computers connected through a data network. A computer can have more than one network adapter installed, and is identified in the system through a unique identifier.

Network topology

Physical or logical map of network nodes.

Normalization

In **Panda Data Control**, normalization is a task that is part of the text indexing process. It consists of removing all unnecessary characters (typically separator characters and delimiters), before storing them in a database.

OU (Organizational Unit)

Hierarchical method for classifying and grouping objects stored in directories.

Panda Adaptive Defense 360 software

Program installed on the computers to protect. It consists of two modules: the Panda agent and the protection.

Panda Advanced Reporting Tool (ART)

A real-time, advanced service for exploiting the knowledge generated by the products Adaptive Defense and Panda Adaptive Defense 360. It allows organizations to detect unknown threats, targeted attacks and APTs, with graphical representations of the activities performed by the processes run by users, emphasizing events related to security and data extraction.

Panda agent

One of the modules included in the Panda Adaptive Defense 360 software. It manages communications between computers on the network and Panda Security's cloud-based servers, in addition to managing local processes.

Panda Data Control

A module compatible with **Panda Adaptive Defense 360** that finds the PII files stored on an organization's network and monitors access to them in order to ensure compliance with applicable data processing and storage regulations such as the GDPR.

Panda Patch Management

A module compatible with **Panda Adaptive Defense 360** 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.

Panda SIEMFeeder

A module compatible with **Panda Adaptive Defense 360** that sends the telemetry generated by the processes run on the organization's workstations and servers to the company's SIEM server.

Partner

A company that offers Panda Security products and services.

Patch

Small programs published by software vendors to fix their software and add new features.

Payload

In the IT and telecommunications sectors, a message payload is the set of useful transmitted data (as opposed to other data that is also sent to facilitate message delivery: header, metadata, control information, etc.).

In IT security circles, however, an exploit's payload is the part of the malware code that controls the malicious actions taken on the system, such as deleting files, stealing data, etc. (as opposed to the part responsible for leveraging the software vulnerability -the exploit- in order to run the payload).

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Peer to Peer (P2P) functionality

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

Panda Adaptive Defense 360 implements P2P connections to reduce bandwidth usage, as those computers whose signature file has been already updated will share the update locally with those computers that also need to update it.

Phishing

A technique for obtaining confidential information from a user fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

PII (Personally Identifiable Information)

Information that can be used to identify or locate an individual.

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 Adaptive Defense 360** software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Proxy functionality

This feature allows **Panda Adaptive Defense 360** to operate on computers without Internet access, accessing the Web through an agent installed on another computer on the same subnet.

Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the **Panda Adaptive Defense 360** cloud.

Public network

Networks in public places such as airports, coffee shops, etc. These networks require that you establish some limitations regarding computer visibility and usage, especially with regard to file, directory and resource sharing.

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Quarantine

See Backup.

RIR (Regional Internet Registry)

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

Role

Specific permission configuration applied to one or more user accounts, and which authorizes users to view and edit certain resources of the console.

Rootkit

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is used by attackers to hide evidence and utilities on previously compromised systems.

ROP

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

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

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

RWD (Responsive Web Design)

A set of techniques that enable the development of Web pages that automatically adapt to the size and resolution of the device being used to view them.

SCL (Spam Confidence Level)

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

Settings

See Settings profile.

Settings profile

Specific settings governing the protection or any other aspect of the managed computer. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

SIEM (Security Information and Event Management)

Software that provides storage and real-time analysis of the alerts generated by network devices.

Signature file

File that contains the patterns used by the antivirus to detect threats.

SMTP server

Server that uses SMTP (Simple Mail Transfer Protocol) to exchange email messages between computers.

Spam

This term refers to unsolicited email messages that usually contain advertising and are generally sent out massively. Spam can have a range of negative effects on the recipient.

Spyware

A program that is automatically installed with another (usually without the user’s permission and even without the user realizing), and collects personal data.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

Suspicious item

A program with a high probability of being malware after having been scanned by the **Panda Adaptive Defense 360** protection installed on the user’s computer.

SYN

Flag in the TOS (Type Of Service) field of TCP packets that identifies them as connection start packets.

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.

Threat hunting

A set of specialized technologies and human resources that allows lateral movements and other early indicators of malware activity to be detected, before they can take harmful actions against corporate security.

TLS (Transport Layer Security)

New version of protocol SSL 3.0.

Trojans

Programs that reach computers disguised as harmless software to install themselves on computers and carry out actions that compromise user confidentiality.

Trusted network

Networks in private places such as offices and households. Connected computers are generally visible to the other computers on the network, and there is no need to establish limitations on file, directory and resource sharing.

UDP (User Datagram Protocol)

A transport-layer protocol which is unreliable and unsuited for connections for exchanging IP packets.

Unblocked program

Program blocked during the classification process but temporarily and selectively allowed by the administrator to avoid disrupting user activity.

User (console)

Information set used by **Panda Adaptive Defense 360** to regulate administrator access to the Web console and establish the actions that administrators can take on the network's computers.

User (network)

A company's workers using computing devices to do their job.

User account

See User.

Virus

Programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

VPN (Virtual Private Network)

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

Vulnerable process

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

Web access control

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

Web console

Tool to manage the advanced security service **Panda Adaptive Defense 360**, accessible anywhere, anytime through a supported Internet browser. The Web console allows administrators to deploy the security software, push security settings, and view the protection status. It also provides access to a set of forensic analysis tools to assess the scope of security problems.

Widget (Panel)

Panel containing a configurable graph representing a particular aspect of network security. **Panda Adaptive Defense 360**'s dashboard is made up of different widgets.

Window of opportunity

The time it takes between when the first computer in the world is infected with a new malware specimen and its analysis and inclusion by antivirus companies in their signature files to protect computers from infections. This is the period when malware can infect computers without antivirus software being aware of its existence.

Workgroup

Architecture in Windows networks where shared resources, permissions and users are managed independently on each computer.

Panda Adaptive Defense 360