Panda Adaptive Defense

Administration guide

Version: 4.00.00-00

Author: Panda Security

Date: 07/12/2021

panda

pandasecurity.com

Legal notice.

Registered trademarks.

Contact information.

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

About the Panda Adaptive Defense Administration guide

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

http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSEoAP-guide-EN.pdf

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

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

Release notes

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

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

Technical documentation not included in this Administration guide for Panda Adaptive Defense-compatible modules and services

- To access the Panda Advanced Reporting Tool User's Guide, go to the following URL:

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

- To access the Panda Data Control User's Guide, go to the following URL:

http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-Guide-EN.pdf

- To access the Panda SIEMFeeder User's Guide, go to the following URL:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-EN.PDF

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-EventDescriptionGuide-EN.pdf

Technical Support

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

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

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

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

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

Survey on the Administration guide

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

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

Contents

Part 1: Panda Adaptive Defense overview

Part 2: The management console

Part 3: Deployment and getting started

Part 4: Managing devices

Part 5: Managing network security

Part 6: Viewing and managing threats

Part 7: Security incident remediation

Part 8: Additional information about Panda Adaptive Defense

Part 1

Panda Adaptive Defense overview

Chapter 1

Preface

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

CHAPTER CONTENT

Audience

The primary audience for this documentation is network administrators who are responsible for managing corporate IT security.

To interpret the information in the management console accurately and draw conclusions that help to bolster corporate security, 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.

What is Panda Adaptive Defense?

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

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

- Panda Adaptive Defense
- Aether Platform

Panda Adaptive Defense

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

Aether Platform

This is the ecosystem where the Panda Security products are run. Aether delivers all the information generated by Panda Adaptive Defense about processes, the programs run by users and the devices installed in real time and in an organized and highly detailed manner.

Aether is a scalable and efficient platform perfectly suited to address the needs of key accounts and MSPs.

Icons

The following icons are used in this Administration guide;

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

⚠ Suggestions and recommendations.

💡 Important advice regarding the use of features in Panda Adaptive Defense.

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

Chapter 2

Panda Adaptive Defense overview

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

CHAPTER CONTENT

Benefits of Panda Adaptive Defense

Panda Adaptive Defense is a solution based on multiple protection technologies that fills the gaps in traditional antivirus solutions, protecting the network against all types of malware, including APTs (Advanced Persistent Threat) and other advanced threats.

It allows the execution of legitimate software only

Panda Adaptive Defense monitors and classifies all processes run on the Windows computers on your 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 Endpoint Protection Plus leverages a new security approach that allows it to adapt precisely to each company's particular environment. To do this, it monitors the execution of all applications, constantly learning from the actions triggered by the processes launched on workstations and servers.

After a brief learning period, Panda Adaptive Defense 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 allow administrators to determine the scope of security incidents and resolve them.

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

Cross-platform service

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

Panda Adaptive Defense features

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

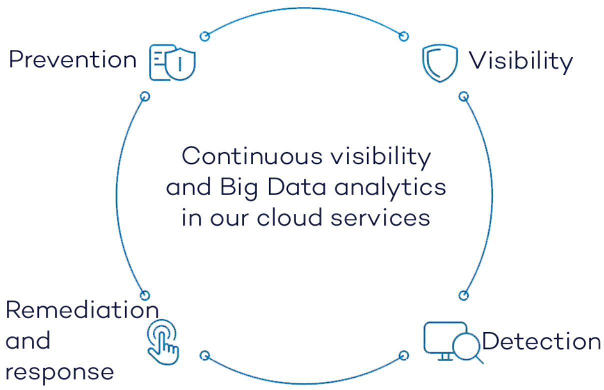

Prevention
Visibility
Continuous visibility and Big Data analytics in our cloud services
Remediation and response
Detection

Figure 2.1: The four pillars of Panda Adaptive Defense's advanced protection

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

Aether Platform features

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

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

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

Key benefits of Aether

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

Cloud management platform

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

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

- Network administrators can access the management console at any moment and from anywhere, using any compatible Internet browser from a laptop, desktop or even mobile devices such as tablets or smartphones.
- It is a high-availability platform, operating 99.99% of the time. Network administrators don't need to design and deploy expensive systems with redundancy to host the management tools.

Real-time communication with the platform

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

Multi-product and cross-platform

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

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

Flexible, granular settings

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

Complete, customized information

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

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

Aether architecture

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

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

Figure 2.2 shows a high-level diagram of Aether Platform.

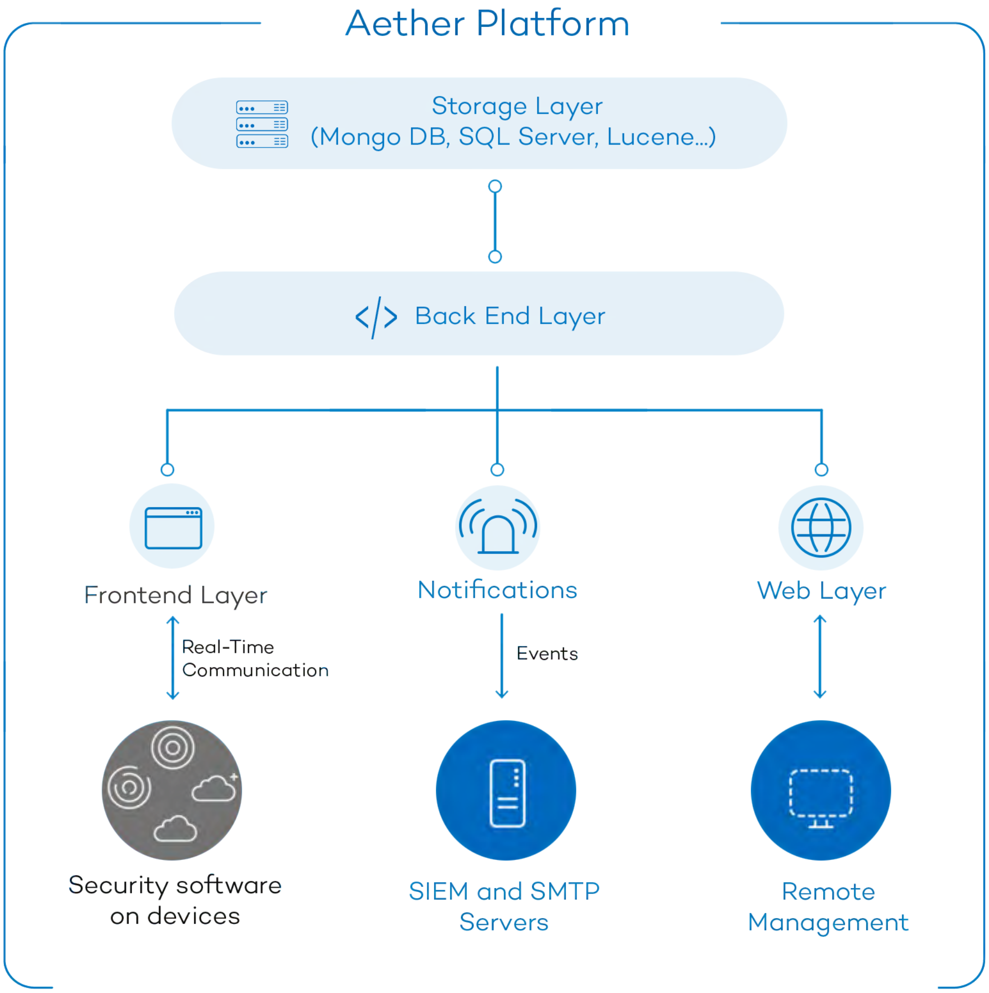


Figure 2.2: Logical structure of Aether Platform

Aether on users' computers

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

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

Panda real-time communications agent

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

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

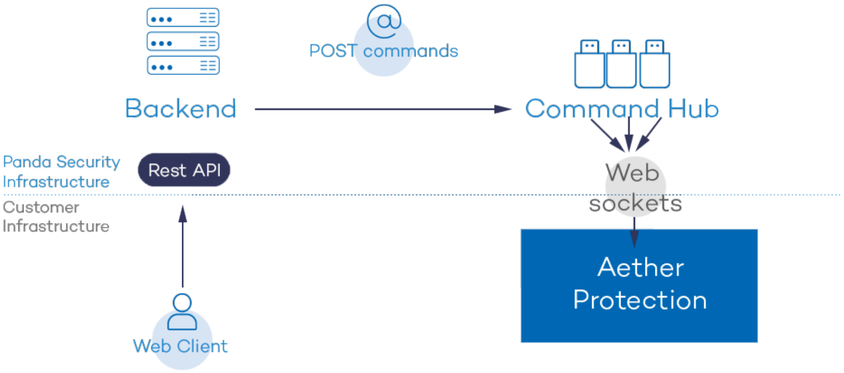


Figure 2.3: Flowchart of the commands entered via the management console

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

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

Panda Adaptive Defense key components

Panda Adaptive Defense is a security service based on analyzing the behavior of the processes run on the computers on each customer's IT infrastructure. This analysis is performed using machine learning techniques in Big Data environments hosted in the cloud.

Figure 2.4 shows the general structure of Panda Adaptive Defense and its components:

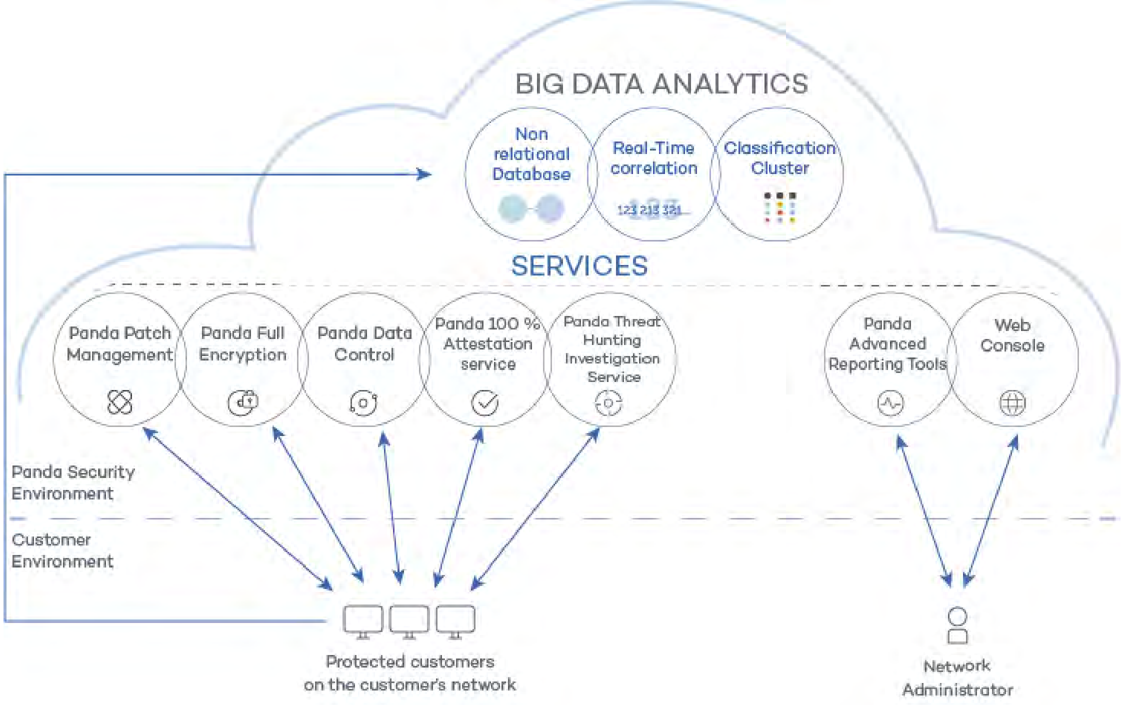


Figure 2.4: Panda Adaptive Defense general structure

- **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 on Windows computers without ambiguity or false positives/negatives.
- **Threat Hunting Investigation Service**: cross-investigation service included in the product’s basic license. It detects unknown threats and ‘Living off the Land’ attacks. These targeted attacks are designed to evade the protections installed on computers.
- **Panda SIEMFeeder (optional)**: integrates Panda Adaptive Defense with third-party SIEM tools.
- **Panda Data Control service (optional)**: a service for finding, inventorying and monitoring the personal information stored in PII files.
- **Panda 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.
- **Panda Full Encryption service (optional)**: encrypts the internal storage devices of Windows

computers in order to minimize data exposure in the event of loss or theft, as well as when storage devices are removed without having deleted their content.

- **Web console**: management console server.
- Computers protected with the installed software (Panda Adaptive Defense).
- Computer of the network administrator that accesses the Web console.

Big Data analytics infrastructure

This is the cloud-based server cluster that receives the telemetry generated on the computers on the customer's network. This telemetry consists of the actions performed by the user programs monitored by the protection module, their static attributes, and execution context information. All this offers a constant flow of information which is scanned in the cloud using artificial intelligence techniques in order to evaluate the programs' behavior and issue a classification for each running process. This classification is returned to the protection module installed on each computer and is taken as the basis to perform the actions required to keep the computer protected.

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 protected computers 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 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 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.
- There is minimal consumption of CPU resources on the user's computer (2% compared to 5%-15% usage by traditional security solutions), as the entire scanning and classification process is carried out in the cloud. The agent installed simply collects the classification sent by the Panda Adaptive Defense server and takes a corrective action.
- 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.

Web console administration

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

*To check whether your Internet browser is compatible with the service, refer to "***Web console access***" on page* **525**.

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

Computers protected with Panda Adaptive Defense

Panda Adaptive Defense 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 protection module.

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

The Panda Adaptive Defense protection module contains the technologies designed to protect customers' computers. Panda Adaptive Defense 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 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.

100% Attestation Service

This service, included in the product by default for Windows computers, 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 99.98 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 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, 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.

Threat Hunting Investigation Service

A service that detects ‘Living off the Land’ attacks and threats designed to bypass the protections installed on computers. This service leverages the Cytomic Orion product, the advanced Threat Hunting platform developed by Panda Security.

Thanks to the telemetry sent from computers, Cytomic Orion performs cross-analytics of the processes run in customers’ IT infrastructures to detect new threats and create advanced hunting rules. When an indicator of attack is detected, it is validated by the Panda Security team of cybersecurity experts. After it is validated, Panda Adaptive Defense shows the associated indicator of attack (IOA) in the console, along with a description of its characteristics and recommendations for the administrator to resolve the situation.

This service is included in all the Panda Adaptive Defense and Panda Adaptive Defense 360 licenses.

*For more information about how to configure the indicators of attack module, refer to “***Indicators of attack settings***” on page* **367**.

Panda Advanced Reporting Tool service (optional)

Panda Adaptive Defense automatically and transparently sends all the information collected from users' computers to Panda Advanced Reporting Tool, a knowledge storage and exploitation system.

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 provides administrators with additional information on threats and the way users use corporate computers. This information is delivered in the most flexible and visual way to make it easier to understand.

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

Refer to the Panda Advanced Reporting Tool Administration Guide (accessible from the product's Web page).

Panda SIEMFeeder service (optional)

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

The SIEM systems compatible with Panda Adaptive Defense are:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora

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

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 applicable data protection regulations governing the storage and processing of personally identifiable information (PII).

Panda Data Control discovers, audits, and monitors in real time the full lifecycle of the PII files stored on Windows computers: from data at rest to data in use (the operations taken on personal data) and data in motion (data exfiltration). With this information, Panda Data Control generates an inventory showing the evolution of the number of files with personal data found on each computer on the network.

*Refer to the chapter "***Panda Data Control (Personal data monitoring)***" on page* **231** *for more information about the service.*

Panda Patch Management service (optional)

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

Additionally, it finds all programs on the network that have reached their EOL (End-Of-Life) stage. These programs pose a threat as they are no longer supported by the relevant vendor and are a primary target for hackers looking to exploit known unpatched vulnerabilities. With Panda Patch

Management, administrators can easily find all EOL programs in the organization and design a strategy for the controlled removal of this type of software.

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

Panda Full Encryption service (optional)

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

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

Product user profile

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

Supported devices and languages

*For a full description of the platforms supported by the solution, refer to “***Hardware, software and network requirements***” on page* **519**

Supported operating systems

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

Supported Web browsers

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

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

Languages supported in the management console

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

Chapter 3

The adaptive protection cycle

Next-generation malware is designed to stay hidden on corporate networks for long periods of time in order to profit financially from infected systems. This evolution has introduced a new paradigm in malware protection: the adaptive protection cycle. Panda Adaptive Defense implements the necessary resources to detect cyberthreats and protect companies against them, as well as resolving the problems created by malware and adjusting security strategies to prevent future infections.

CHAPTER CONTENT

New security needs

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.

This strategy is rendering the traditional approach of protecting systems using locally stored or cloud-based signature files gradually ineffective. The huge growth in the amount of malware in circulation can be considered in itself a massive brute-force attack on security vendors, as cybercriminals look to increase the window of opportunity for newly developed threats by saturating the resources employed by security companies to scan malware. This is increasing the time lapse between the appearance of a new virus and the release of the appropriate antidote by security companies. Additionally, updating signature files and deploying them across customers' networks further increases malware exposure times, especially in the case of those security providers who still rely on malware signature files and have not moved their security intelligence to the cloud.

In this context, 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.

Panda Adaptive Defense introduces a new security strategy based on what is called 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.

Additionally, this new approach enables IT departments to quickly adapt corporate IT security policies to the changing patterns of advanced malware.

The adaptive protection cycle

The aim of Panda Adaptive Defense is to enable IT departments 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, on one hand, the product of the removal of responsibilities from the company's technical team when it comes to deciding which files are safe and which are dangerous, and for what reason. **With Panda Adaptive Defense, your 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 of the network, resolving problems related to advanced malware, and studying the behavior of APTs and other threats.

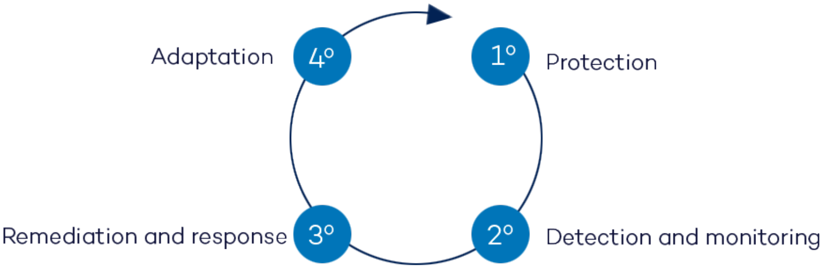


Figure 3.1: The adaptive protection cycle

With all this information and tools, administrators can completely close the corporate security cycle: monitor the status of the network, restore systems to the situation prior to any potential security breach, and determine the scope of attacks in order to implement appropriate contingency measures. This cycle is in a continuous process of refinement and improvement, resulting in a secure, flexible and productive environment for all of the company's users.

The adaptive protection cycle implemented by companies with the help of Panda Adaptive Defense is illustrated in Figure 3.1.

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.

Protection with context-based detections

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

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

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

Program blocking

To increase the security of the Windows computers on the network, administrators can prevent the execution of programs deemed dangerous or not compatible with the activity conducted by the organization.

There are many reasons why an administrator may want to prevent certain programs from being run: programs using too much bandwidth, accessing contents that may pose a security threat, or accessing contents that may affect user or computer performance.

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 implements a number of innovative technologies that allow the network administrator to pinpoint the problem.

Advanced permanent protection

The advanced protection continuously monitors all processes run on the customer's computers. Panda Adaptive Defense collects all actions taken by the processes run on users' computers and sends them to Panda Security's cloud, 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, with the aim 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 implements three operational modes for unknown (not yet classified) processes and processes classified as malware:

- Audit
- Hardening
- Lock

Audit

In Audit mode, Panda Adaptive Defense reports 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 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 as goodware**: they are allowed to run.
- **Files classified by Panda Adaptive Defense as malware**: they are quarantined or disinfected.
- **Unclassified files coming from external sources (Internet, email, USB devices, other computers on the customer's network)**: they are prevented from running until a classification is returned. Once a classification is returned, they are allowed to run (goodware) or quarantined (malware).

The classification process is almost immediate in most cases. That is, a program downloaded from the Internet and unknown to Panda Adaptive Defense will 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: 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 provide maximum security guarantees, Panda Adaptive Defense 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.

*More than 99% of programs found on users' computers are already classified by Panda Adaptive Defense. Thus, only a small minority of programs will be prevented from prevented from running for being unknown. For more information on how to configure the different blocking modes provided by Panda Adaptive Defense, refer to "***Advanced protection***" on page* **226**.

Anti-exploit protection

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

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

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

In short, Panda Adaptive Defense leverages constantly-evolving technologies to provide global anti-exploit protection against advanced vulnerability exploit techniques such as the following:

- Attack Surface Reduction (ASR)
- Data Execution Prevention (DEP)
- Structured Exception Handling Overwrite Protection (SEHOP)
- Null Page Security Mitigation
- Heap Spray Allocation
- Export Address Table Access Filtering (EAF)
- Mandatory Address Space Layout Randomization (ASLR)
- Bottom-Up ASLR Security Mitigation
- Load Library Check - Return Oriented Programming (ROP)
- Memory Protection Check - Return Oriented Programming (ROP)
- Caller Checks - Return Oriented Programming (ROP)
- Simulate Execution Flow - Return Oriented Programming (ROP)
- Stack Pivot - Return Oriented Programming (ROP)
- EternalBlue
- Process Doppelgänging,

Fileless threat detection and THIS service

Fileless/malwareless threats are capable of bypassing traditional signature-based malware detection strategies by not dropping files to the infected computer's hard disk. 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 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.

In addition to this, the THIS service provides Panda Security cybersecurity analysts with the Orion tool. This service analyzes the telemetry obtained from monitoring the processes run on each customer's computers, generating hypotheses which are later confirmed or discarded by higher-level analysts. If a hypothesis is confirmed and the suspicious action patterns detected belong to an unknown attack, the new classification will be distributed to all Panda Security customers for increased global security.

Detection of indicators of attack (IOAs) and Threat Hunting Investigation Service

In many of the cyberattacks targeting companies, hackers try to bypass the security defenses in place by executing a set of coordinated actions for extended periods of time. Many of these actions leverage fileless/malwareless threats, which run without saving files to the infected computer's hard disk in an attempt to evade the traditional malware detection strategies based on signature files. Because these threats reside in the target computer's RAM memory only, they are extremely difficult to detect. Not only that, the impact of their actions is extremely hard to determine with standard forensic analysis procedures. Another strategy cybercriminals use to go unnoticed is to use legitimate operating system tools in order to carry out their attacks.

The Panda Adaptive Defense basic user license includes a cross threat hunting service which analyzes the telemetry flow using the Cytomic Orion tool, generating indicators of attack as a result. These indicators of attack are supervised and validated by a group of Panda Security specialized technicians (hunters), before generating an IOA in the management console.

An IOA (Indicator Of Attack) is an indicator that Panda Adaptive Defense shows in the management console when it detects an event pattern that may belong to a cyberattack. Therefore, it can be an early sign of infection, which alerts the administrator to the existence of an attack in progress, or a warning that a cyberattack managed to penetrate corporate defenses and one or more computers have been compromised to some extent.

Data file monitoring (Panda Data Control)

Panda Adaptive Defense monitors all accesses to users' data files by the processes run on computers. This way, if a malicious item manages to infect a 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.

Vulnerability patching (Panda Patch Management)

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

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

Network status visibility

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

The important thing in this phase 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 dashboard provides key information for this purpose:

- Information on which processes found on the network are unknown to Panda Adaptive Defense 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 blocking level to allow certain unknown programs to run.

*For more information refer to "***Malware and network visibility***" on page* **403**.

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 attack, that is, find out whether there was a data leak, the extent of the attack, which computers were compromised, etc. Panda Adaptive Defense provides tools to help administrators with those tasks.

Response

- The forensic analysis tool provides visibility into all actions taken by malware on infected computers, as well as 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 disk in order to extract confidential information, etc.
- Panda Adaptive Defense 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 the network, preventing data loss. Nevertheless, isolated computers can communicate with the Panda Security cloud in order to enable administrators to remotely investigate incidents without having to physically access the affected system. Additionally, if continued attacks are detected, or user accounts are compromised using the RDP protocol, the indicators of attack (IOA) module can automatically block Remote Desktop connections to stop the attack from spreading.
- Panda Advanced Reporting Tool and Panda Data Control complement and help interpret the data gathered by Panda Adaptive Defense. They give administrators access to graphic 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 provides the traditional disinfection tools typical of antivirus solutions, along with a quarantine to store suspicious and deleted items.

*For more information, refer to “***Remediation tools***” on page* **495**.

Phase 4: Adaptation / Prevention

Once an attack has been analyzed with the remediation and response tools discussed in phase 3, 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 the corporate routers or user permissions on personal computers.

Administrators can strengthen endpoint security with Panda Adaptive Defense by changing the advanced protection settings. If the users in the organization 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 the execution of illegitimate programs.

- **Changing the Panda Patch Management settings**

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

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

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

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

- **Blocking dangerous programs, as well as programs not related to the activity of the organization, or having a strong impact on the performance of computers, users, or the entire network infrastructure.**

Minimize the attack surface of the computers on your network, preventing the execution of programs that access contents likely to contain viruses and other security threats. Improve user productivity as well as computer and network performance, preventing the execution of programs that download large volumes of data or use up computer resources.

Part 2

The management console

Chapter 4: The management console

Chapter 5: Controlling and monitoring the management console

Chapter 4

The management console

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

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

CHAPTER CONTENT

Benefits of the Web console

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

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

The Web console lets administrators deploy the Panda Adaptive Defense installation package 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 security incidents. All these features are provided from a single Web-based console, facilitating the integration of the different tools and minimizing the complexity of using products from different vendors.

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

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

- **Security management from anywhere at anytime**

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

Web console requirements

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

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

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

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

The following requirements are necessary to access the Web console:

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

For more information on how to create a Panda Account to access the Web console, refer to "The Panda Account" on page 551.

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

IDP-based federation

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

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

General structure of the Web console

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

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

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

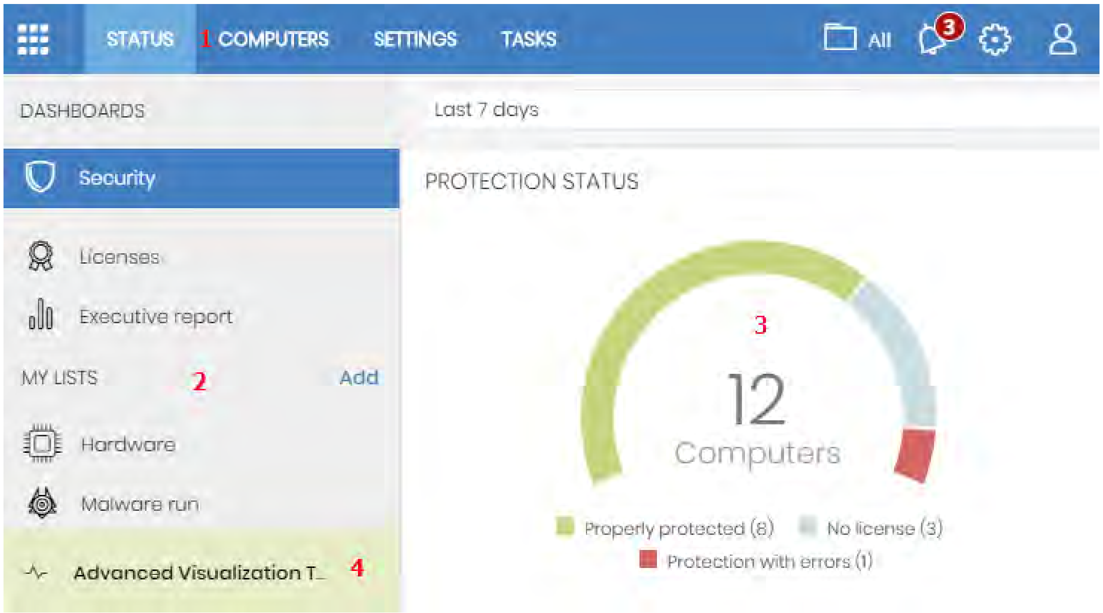


Figure 4.1: Panda Adaptive Defense management console overview

Top menu (1)

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

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

Panda Cloud button

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

Status menu

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

Computers menu

The **Computers** menu provides the basic tools for network administrators to define the computer structure that best adapts to the security needs of their IT network. Choosing the right device structure is essential in order to assign security settings quickly and easily. Refer to "**The Computers area**" on page 145 for more information.

Settings menu

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

*Refer to "**Managing settings**" on page 189 for detailed information on how to create a settings profile in Panda Adaptive Defense.*

Tasks menu

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

Filter by group icon

Limits the information displayed in the console to that collected from the computers belonging to the selected group(s). Refer to "**Filtering results by groups**" on page 157 for more information.

Web notifications icon

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

- Planned maintenance tasks
- Alerts regarding critical vulnerabilities
- Security tips
- Messages to start console upgrade processes. Refer to "**Product updates and upgrades**" on page 135.

Each communication has a priority level associated with it:

- 🔴 Important
- 🟠 Notice
- 🔵 Information

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

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

General options icon ⚙

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

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

Table 4.1: 'General options' menu

User account icon

Displays a drop-down menu with the following options:

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

Table 4.2: 'User account' menu

Side menu (2)

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

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

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

Center panel (3)

Displays all relevant information for the area and subarea selected by the administrator. Figure 4.1 shows the **Status** area, **Security** subarea, with widgets that allow administrators to interpret the security information collected from the network. For more information about widgets, refer to "**Security panels/ widgets**" on page 404.

Shortcut 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 the organization's workstations and servers.

Basic elements of the Web console

Tab menu

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

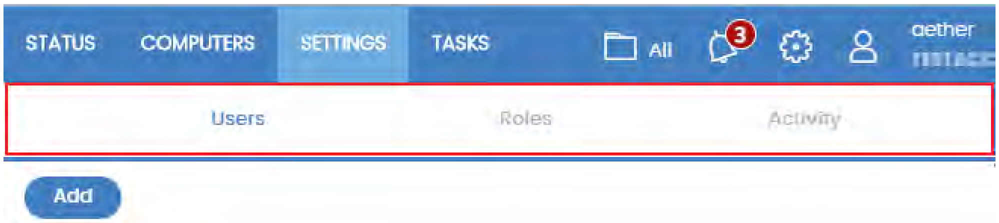


Figure 4.2: Tab menu

Action bar

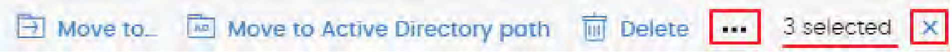


Figure 4.3: Action bar

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

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

Filtering and search tools

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

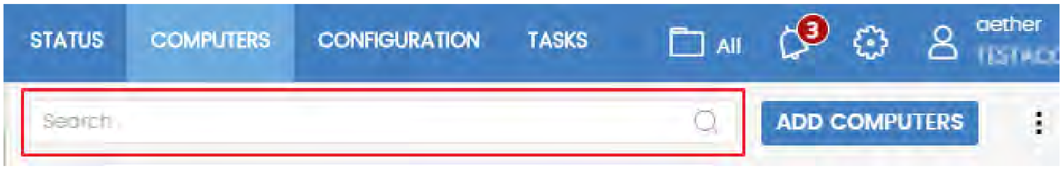
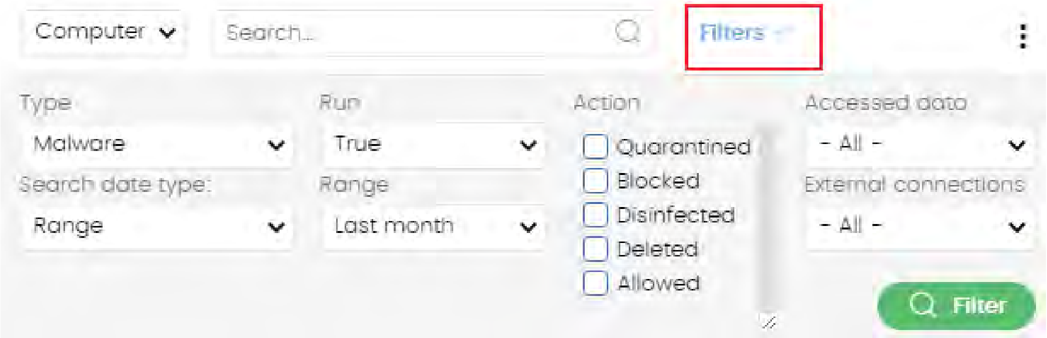


Figure 4.4: Search tool

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



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

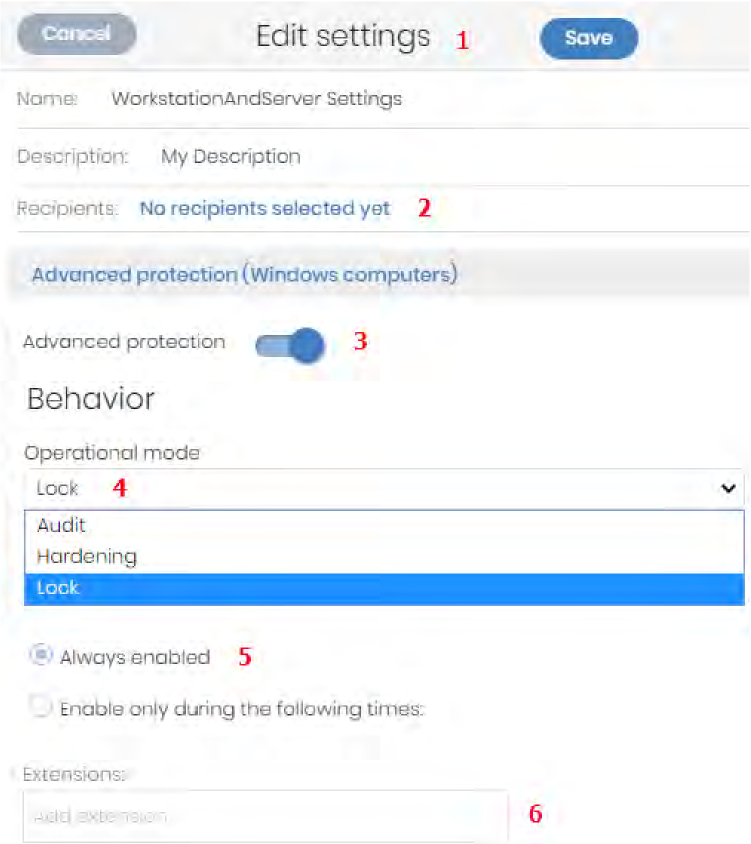
Figure 4.5: Filtering tool for data lists

Other interface elements

The Panda Adaptive Defense Web console uses standard interface elements for configuring settings, such as:

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

- Text fields **(6)**



Name: WorkstationAndServer Settings

Description: My Description

Recipients: No recipients selected yet

Advanced protection

Operational mode: Lock

○ Always enabled

○ Enable only during the following times:

Extensions:

Figure 4.6: Controls for using the management console

Sort button

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

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

Context menus

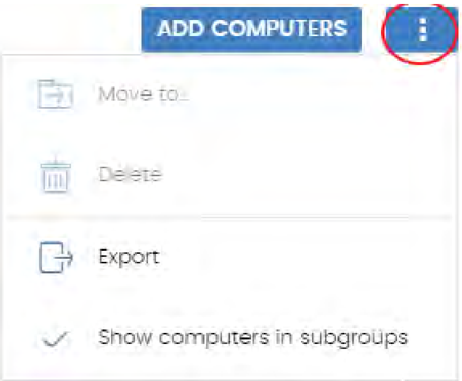


Figure 4.7: Context menu

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

Copy contents and Delete contents buttons

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

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

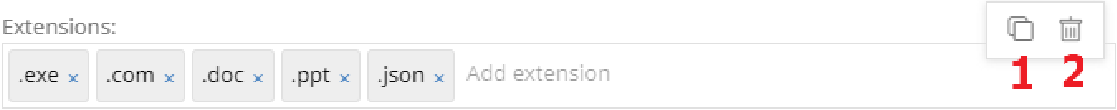


Figure 4.8: Copy and Delete buttons

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

Status area overview

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

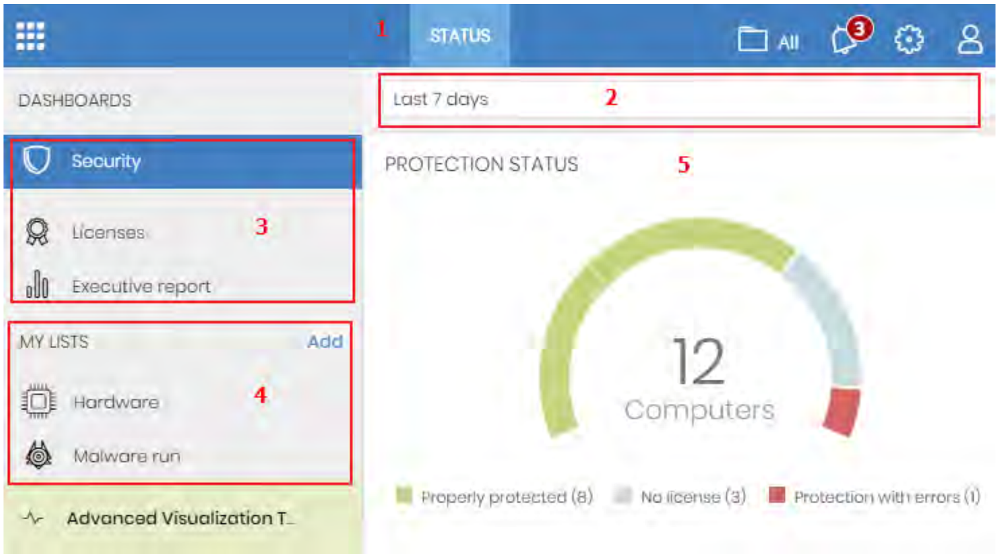


Figure 4.9: Status window (dashboard and access to lists)

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

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

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

- **Time period selector (2)**

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

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

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

- **Dashboard selector (3)**
  - **Security:** security status of the IT network. For more information about the widgets in this section, refer to "Security panels/widgets" on page 404.

- **Patch management**: updates of the operating system and third-party software installed on computers. For more information about the widgets in this section, refer to "Panda Patch Management widgets and panels" on page 299.
- **Data Control**: monitoring of the personal data stored on the computers on your network. For more information about the widgets in this section, refer to "Panda Data Control panels and widgets".
- **Encryption:** encryption status of your computers' internal storage devices. For more information about the widgets in this section, refer to "Panda Full Encryption panels and widgets".
- **Licenses**: status of the Panda Adaptive Defense licenses assigned to the computers on your network. Refer to "Licenses" for more information about license management.
- **Scheduled reports**: refer to "Scheduled sending of reports and lists" for more information on how to configure and generate reports.

- **My lists (4)**

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

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

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

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

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

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

- Pie charts.
- Histograms.
- Line charts.

Managing lists

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

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

Templates, settings and views

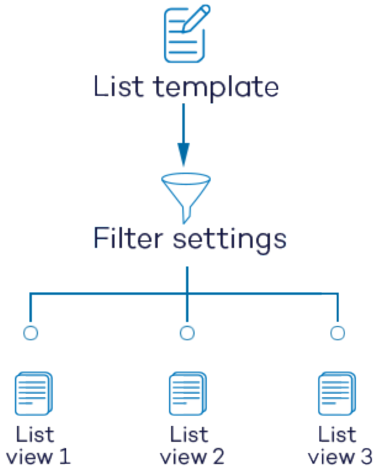


Figure 4.10: Generating three lists from a single template/data source

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

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

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

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

List templates

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

Group	List	Description
General	Licenses	Shows in detail the license status of the computers on your network. Refer to "**Licenses**" on page 128.
	Unmanaged computers discovered	Shows the Windows computers on your network that don't have the Panda Adaptive Defense software installed. Refer to "**Viewing discovered computers**" on page 103.
	Computers with duplicate name	Shows computers with the same name and belonging to the same domain. Refer to "**Computers with duplicate name'**" on page 170.
	Software	Shows the software installed on the computers on your network. Refer to "**'Software'**" on page 168.
	Hardware	Shows the hardware installed on the computers on your network. Refer to "**'Hardware'**" on page 166.

Table 4.3: Templates available in Panda Adaptive Defense

Group	List	Description
Security	Computer protection status	Shows in detail the protection status of the computers on your network. Refer to "**Computer protection status**" on page 412.
	Malware and PUP activity	Shows a list of all threats found on the computers protected with Panda Adaptive Defense. Refer to "**Malware/PUP activity**" on page 418.
	Exploit activity	Shows the number of vulnerability exploit attacks suffered by the Windows computers on your network. Refer to "**Exploit activity**" on page 420.
	Currently blocked programs being classified	Shows a table with those files in which Panda Adaptive Defense has preliminarily detected some risk despite their classification is not fully complete. Refer to "**Malware/PUP activity**" on page 418.
	Indicators of attack (IOA)	Shows details of the advanced indicators of attack detected on the IT network. Refer to "**Indicators of attack (IOA)**" on page 379.
Patch management	Patch management status	Shows in detail all computers on the network compatible with Panda Patch Management. Refer to "**Patch management status**" on page 307.
	Available patches	Shows a list of all missing patches on the computers on your network and published by Panda Security. Refer to "**Available patches**" on page 304.
	Installation history	Shows the patches that Panda Adaptive Defense attempted to install and the computers that received them in a given time interval. Refer to "**Installation history**" on page 317.
	End-of-Life programs	Shows information about the end of life of the programs installed on your network, grouped by the end-of-life date. Refer to "**End-of-Life programs**" on page 316.
	Excluded patches	Shows the computer-patch pairs excluded from installation tasks. Refer to "**Excluded patches**" on page 321.
Activity control	Programs blocked by the administrator	Shows all attempts to run programs blocked by the administrator on the computers on the network. Refer to "**'Program blocking' module lists**" on page 357.
Data protection	Encryption status	Shows information about the computers on your network compatible with the encryption feature. Refer to "**Encryption Status**" on page 347.

Table 4.3: Templates available in Panda Adaptive Defense

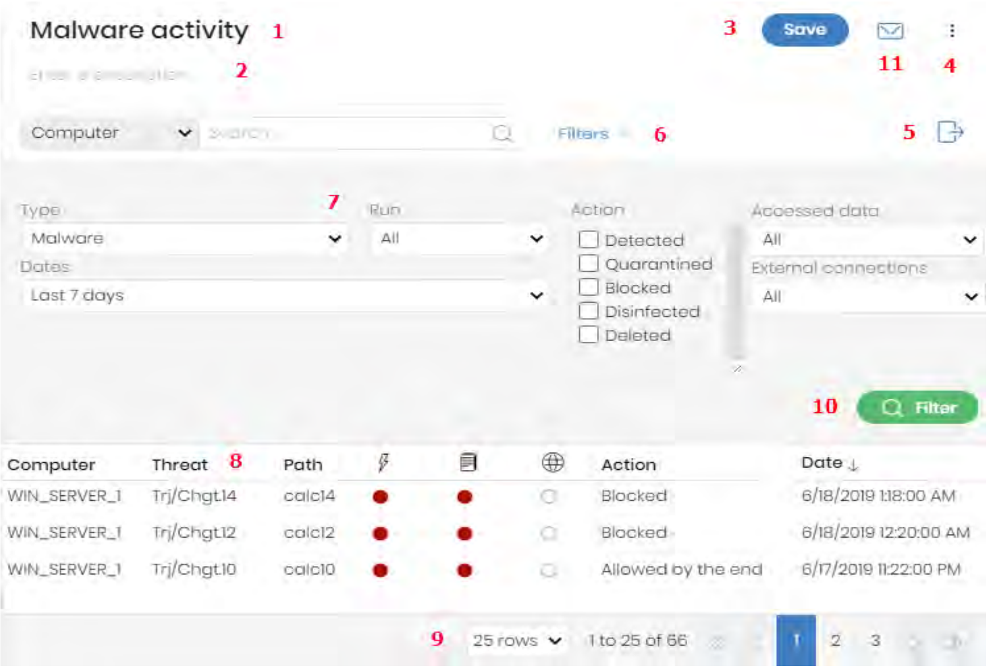
Group	List	Description
	Data Control status	Shows the status of the Panda Data Control module included in Panda Adaptive Defense. Refer to "'Data Control status'" on page 265.
	Files with personal data	Shows all PII files found on your network, along with their type, location and other relevant information. Refer to "'Files with personal data'" on page 270.
	Computers with personal data	Shows the number of PII files found on each computer on your network. Refer to "Computers with personal data" on page 273.
	Files deleted by the administrator	Shows the status of the files deleted by the administrator using the Panda Data Control module. Refer to "'Files deleted by the administrator'" on page 277.

Table 4.3: Templates available in Panda Adaptive Defense

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

List sections

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



Malware activity

Type: Malware
Run: All
Dates: Last 7 days
Action: □ Detected □ Quarantined □ Blocked □ Disinfected □ Deleted
Accessed data: All
External connections: All

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

25 rows 1 to 25 of 66 1 2 3

Figure 4.11: List elements

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

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

Table 4.4: Pagination tools

- **Scheduled send (11)**: Panda Adaptive Defense lets you email a .CSV file with the content of the list. Refer to “**Scheduled sending of reports and lists**” on page 483 for more information.

Operations with lists

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

Creating a custom list

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

- **From the My lists side menu**

  - Click the **Add link** from the **My lists** panel on the left to display a window showing all available templates.
  - Choose a template, configure the filter tools, edit the name and description of the list and click the **Save button (3)**.

- **From a dashboard panel**

  - Click a widget on the dashboard to open its associated template.
  - Click its context menu **(4)** and select **Copy**. A new list will be created.
  - Edit the list filters, name and description and click **Save (3)**.

- **From an existing list**

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

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

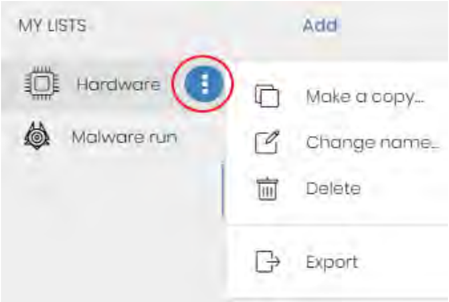


Figure 4.12: Context menu of the lists accessible from the 'My lists' panel

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

Deleting a list

There are various ways to delete a list:

- **From the My lists panel**

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

- **From the list itself**

  - Click the list's context menu **(4)**.

- Click the 🗑 icon from the drop-down menu displayed.

Copying a list

There are various ways to copy a list:

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

Exporting a list

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

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

Exporting a list’s details

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

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

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

Configuring a custom list

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

Scheduling a list to be sent via email

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

Refer to "Scheduled sending of reports and lists" on page 483 for more information

Available actions for computers in lists

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

Default lists

The management console includes various lists generated by default:

- Unprotected workstations and laptops.

- Unprotected servers.
- Hardware
- Software

Unprotected workstations and laptops

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

- Computers on which the Panda Adaptive Defense software is currently being installed or installation failed.
- Computers on which the protection is disabled or has errors.
- Computers without a license assigned or with an expired license.
- Refer to "**Computer protection status**" on page **412** for more information.

Unprotected servers

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

- Servers on which the Panda Adaptive Defense software is currently being installed or installation failed.
- Servers on which the protection is disabled or has errors.
- Servers without a license assigned or with an expired license. Refer to "**Computer protection status**" on page **412** for more information.

Software

Shows a list of the programs installed across your network. Refer to "'**Software**'" on page **168** for more information.

Hardware

Shows a list of the hardware components installed across your network. Refer to "'**Hardware**'" on page **166** for more information.

Chapter 5

Controlling and monitoring the management console

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

These resources are as follows:

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

CHAPTER CONTENT

What is a user account?

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

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

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

User account structure

A user account comprises the following items:

- **Account login email**: this is assigned when the account is created. Its aim is to identify the administrator accessing the account.

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

Two-factor authentication

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

Requirements for enabling 2FA

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

Enabling 2FA

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

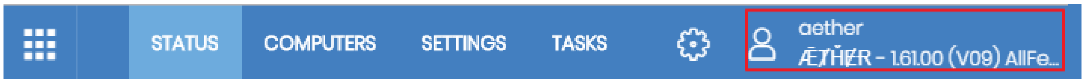


Figure 5.1: Shortcut to your Panda Account

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

Accessing the console using an account with 2FA enabled

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

Forcing all console users to use 2FA

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

- Click the Settings menu at the top of the console. Then, click the **Security tab**.
- Select the option **Require users to have two-factor authentication enabled to access this account**.
- If the user account that forces all console users to have 2FA enabled does not have 2FA enabled for itself, a warning message will be displayed prompting you to access the **Panda Account** and enable the feature. Refer to "**Enabling 2FA**".

What is a role?

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

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

Role structure

A role is made up of the following:

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

Why are roles necessary?

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

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

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

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

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

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

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

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

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

Full Control role

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

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

Read-only role

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

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

What is a permission?

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

Understanding permissions

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

Manage users and roles

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

Assign licenses

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

Modify computer tree

- **Enabled**: the account user has complete access to the group tree, and can create and delete groups, as well as moving computers to already-created groups.
- **Enabled with permission conflict**: because of the inheritance mechanism that applies to the computer tree, any changes made to the tree structure may result in a change to the settings assigned to the affected devices. For example, in cases where the administrator does not have permission to assign settings, if they move a computer from one group to another, the web console will show a warning indicating that, because of the computer move operation and the inheritance mechanism applied, the settings assigned to the computer that was moved may have changed (even if the administrator does not have permission to assign settings). Refer to section "**Manual and automatic assignment of settings**" on page 198.
- **Disabled:** the account user can view the group tree and the settings assigned to each group, but cannot create new groups or move computers.

Add, discover and delete computers

- **Enabled**: the account user can distribute the installer to the computers on the network and integrate them into the console. They can also delete computers from the console and configure all aspects related to the discovery of unmanaged computers: assign and revoke the discovery computer role, edit discovery settings, launch an immediate discovery task, and install the Panda agent remotely from the list of discovered computers.

- **Disabled**: the account user cannot download the installer, nor distribute it to the computers on the network. Neither can they delete computers from the console or access the computer discovery feature.

Modify network settings (proxies and cache)

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

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

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

Restart and repair computers

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

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. To isolate a computer, the **Isolate computers** option available in the context menu and on the action bar must be used.
- **Disabled**: the account user cannot isolate computers.

Configure security for workstations and servers

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

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

View security settings for workstations and servers

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

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

View detections and threats

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

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

Disinfect

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

Exclude threats temporarily (Malware, PUPs and blocked items)

- **Enabled**: the account user can block/unblock and exclude/allow all types of items in the process of classification (malware, PUPs and unknown items).
- **Disabled**: the account user cannot block/unblock or exclude/allow malware, PUPs or unknown items in the process of classification.

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

Configure patch management

- **Enabled**: the account user can create, edit, delete and assign patch management settings to Windows workstations and servers.

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

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

View patch management settings

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

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

Install, uninstall and exclude patches

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

View available patches

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

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

Configure program blocking

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

Disabling this permission will display the **View program blocking settings** permission.

View program blocking settings

This permission is only accessible if you disable the Configure program blocking permission.

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

Configure authorized software

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

Disabling this permission will display the **View authorized software settings** permission.

View authorized software settings

This permission is only accessible if you disable the Configure authorized software permission.

- **Enabled:** the account user can only view the authorized software settings created, as well as the settings assigned to a computer or group.
- **Disabled**: the account user won't be able to view the authorized software settings created, nor access the settings assigned to the computers on the network.

Configure indicators of attack (IOA)

- **Enabled**: the account user can create, edit, delete, and assign indicators of attack (IOA) settings.
- **Disabled**: the account user cannot create, edit, delete, or assign indicators of attack (IOA) settings.

Disabling this permission shows the **View indicators of attack (IOA) settings** permission.

View indicators of attack (IOA) settings

> *This permission is only accessible if you disable the Configure indicators of attack (IOA) permission.*

- **Enabled:** the account user can only see the indicators of attack (IOA) settings created, as well as the settings assigned to a computer or group.
- **Disabled**: the account user cannot see the indicators of attack (IOA) settings created nor access the settings assigned to each computer.

Configure Data Control

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

View Data Control settings

> *This permission is only accessible if you disable the Configure sensitive data search, inventory and monitoring permission.*

- **Enabled**: the account user can only view the Sensitive data monitoring settings created as well as the settings of a computer or group.
- **Disabled**: the account user won't be able to view the Data Control settings created nor access the settings assigned to computers.

Search for data on computers

- **Enabled:** the account user can access the **Searches** widget to search for files by their name and contents across the corporate network.
- **Disabled**: the account user cannot access the **Searches** widget.

View personal data inventory

- **Enabled**: the account user can access the following lists: **Files with personal data** and **Computers with personal data**; and the following widgets: **Files with personal data**, **Computers with personal data** and **Files by personal data type**.
- **Disabled**: the account user cannot access the following lists: **Files with personal data** or **Computers with personal data**; or the following widgets: **Files with personal data**, **Computers with personal data** or **Files by personal data type**.

Delete and restore files

- **Enabled**: the account user can access the **Delete** option included in the context menu available on the **Files with personal data** list to delete and restore files.
- **Disabled**: the account user cannot access the **Delete** option included in the context menu available on the **Files with personal data** list, and therefore cannot delete or restore files.

Configure computer encryption

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

View computer encryption settings

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

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

Access recovery keys for encrypted drives

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

Access advanced security information

- **Enabled**: the account user will be able to access the Advanced Visualization Tool (from the **Status** menu at the top of the console, left-hand side panel **Advanced Visualization Tool**). However, the Data Access Control application included in Panda Advanced Reporting Tool won't be visible to them.
- **Disabled**: access to the Advanced Visualization Tool is prevented.

Access file access information (Data Access Control in Advanced Visualization Tool)

- **Enabled**: the account user will be able to access the Advanced Visualization Tool (from the **Status** menu at the top of the console, left-hand side panel **Advanced Visualization Tool**). The Data Access Control application in Panda Advanced Reporting Tool will be accessible too.

- **Disabled**: access to the Panda Advanced Reporting Tool is prevented.

Access advanced Data Control information

- **Enabled**: the account user will be able to access the Data Control extended console (from the **Status** menu at the top of the console, left-hand side panel **Data Control**).
- **Disabled**: the account user won't be able to access the Data Control extended console (from the **Status** menu at the top of the console, left-hand side panel **Data Control**).

Accessing the user account and role settings

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

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

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

Creating and configuring user accounts

Creating, editing and deleting users

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

Listing created users

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.

- Click the **Users** tab. A list will be displayed with all user accounts created in Panda Adaptive Defense, along with the following information:

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

Table 5.1: User list

Creating and configuring roles

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

Limitations when creating users and roles

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

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

User account activity log

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

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

Session log

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

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

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

Table 5.2: Fields in the 'Sessions' list

- **Fields displayed in the exported file**

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

Table 5.3: Fields in the 'Sessions' exported file

- **Search tool**

Field	Description	Values

Table 5.4: Filters available in the 'Sessions' list

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

Table 5.4: Filters available in the 'Sessions' list

User actions log

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

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

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

Table 5.5: Fields in the 'Actions' log

- **Fields displayed in the exported file**

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

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

- **Search tool**

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

Table 5.7: Filters available in the action log

- **Item types and actions**

Item type	Action	Item
License Agreement	Accept	Version number of the accepted EULA.
Account	Update console	From Initial version to Target version.
	Cancel console update	From Initial version to Target version.
Threat	Allow	Name of the threat the action was performed on.
	Stop allowing	Name of the threat the action was performed on.
Information search	Launch	Name of the search the action was performed on.
	Delete	Name of the search the action was performed on.
	Cancel	Name of the search the action was performed on.
Settings - Remote control	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Network settings	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Per-computer settings	Create	Name of the settings the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Program blocking	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Workstations and servers	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Personal data	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Patch management	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Encryption	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.
	Delete	Name of the settings the action was performed on.
Settings - Authorized software	Create	Name of the settings the action was performed on.
	Edit	Name of the settings the action was performed on.

Table 5.8: Item types and actions

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

Table 5.8: Item types and actions

Item type	Action	Item
	Restart	Name of the device the action was performed on.
	Designate as Panda proxy	Name of the computer the action was performed on.
	Revoke Panda proxy role	Name of the computer the action was performed on.
	Designate as cache computer	Name of the computer the action was performed on.
	Configure cache computer	Name of the computer the action was performed on.
	Revoke cache computer role	Name of the computer the action was performed on.
	Designate as discovery computer	Name of the computer the action was performed on.
	Configure discovery	Name of the computer the action was performed on.
	Revoke discovery computer role	Name of the computer the action was performed on.
	Discover now	Name of the computer the action was performed on.
	Move to Active Directory path	Name of the computer the action was performed on.
	Isolate	Name of the device the action was performed on.
	Stop isolating	Name of the device the action was performed on.
	Uninstall	Name of the device the action was performed on.
	Reinstall agent	Name of the device the action was performed on.
	Reinstall protection	Name of the device the action was performed on
	End the "RDP attack containment" mode on the computer	Name of the device the action was performed on.
Unmanaged computer	Hide	Name of the unmanaged computer the action was performed on.
	Make visible	Name of the unmanaged computer the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
	Delete	Name of the unmanaged computer the action was performed on.
	Edit description	Name of the unmanaged computer the action was performed on.
	Install	Name of the unmanaged computer the action was performed on.
Filter	Create	Name of the filter the action was performed on.
	Edit	Name of the filter the action was performed on.
	Delete	Name of the filter the action was performed on.
Group	Create	Name of the group the action was performed on.
	Edit	Name of the group the action was performed on.
	Delete	Name of the group the action was performed on.
	Change parent group	Name of the group the action was performed on.
	Assign "Network settings"	Name of the group the action was performed on.
	Inherit "Network settings"	Name of the group the action was performed on.
	Assign 'Per-computer settings'	Name of the group the action was performed on.
	Inherit 'Per-computer settings'	Name of the group the action was performed on.
	Assign 'Workstations and servers' settings	Name of the group the action was performed on.
	Inherit 'Workstations and servers' settings	Name of the group the action was performed on.
	Assign 'Sensitive information' settings	Name of the group the action was performed on.
	Inherit 'Sensitive information' settings	Name of the group the action was performed on.
	Sync group	Name of the group the action was performed on.
	Move computers to their Active Directory path	Name of the group the action was performed on.

Table 5.8: Item types and actions

Item type	Action	Item
Advanced reports	Access	
IOA	Archive for a computer	IOA name (Computer name).
	Mark as pending for a computer	IOA name (Computer name).
List	Create	Name of the list the action was performed on.
	Edit	Name of the list the action was performed on.
	Delete	Name of the list the action was performed on.
Patch	Exclude for a specific computer	Name of the patch the action was performed on.
	Exclude for all computers	Name of the patch the action was performed on.
	Stop excluding for a specific computer	Name of the patch the action was performed on.
	Stop excluding for all computers	Name of the patch the action was performed on.
	Mark as 'Manually downloaded'	Name of the patch the action was performed on.
	Mark as 'Requires manual download'	Name of the patch the action was performed on.
Action to take when a threat is reclassified	Edit	
Email sending option	Edit	
Access permission for the Panda Security team	Edit	
Access permission for resellers	Edit	
Email sending option (reseller)	Edit	
Two-factor authentication selection	Edit	
Role	Create	Name of the role the action was performed on.
	Edit	Name of the role the action was performed on.

Table 5.8: Item types and actions

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

Table 5.8: Item types and actions

Item type	Action	Item
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.

Table 5.8: Item types and actions

System events

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

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

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

Table 5.9: Fields in the 'System events' list

- **Fields displayed in the exported file**

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

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

- **Filter tool**

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

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

- **Item types and actions**

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

Table 5.12: Item types and actions

Part 3

Deployment and getting started

Chapter 6: Installing the client software

Chapter 7: Licenses

Chapter 8: Product updates and upgrades

Chapter 6

Installing the client software

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

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

CHAPTER CONTENT

Protection deployment overview

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

Identify the unprotected devices on the network

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

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

Check if the minimum requirements for the target platform are met

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

Select the installation procedure

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

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

Uninstall competitors' products and restart computers

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

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

By default, Panda Adaptive Defense can coexist with other security solutions installed on your computers.

The removal of other products applies to both trial and commercial versions. To uninstall other products from your computers, assign them a **Workstations and servers** settings profile with the **Uninstall other security products** option enabled. While looking for updates, Panda Adaptive Defense checks its assigned settings once a day. Refer to the following article **https://www.pandasecurity.com/es/support/card?id=50021** for a list of the third-party security products that Panda Adaptive Defense uninstalls automatically.

- **Panda Security antivirus products**

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

Table 6.1 summarizes the necessary conditions for a computer restart.

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

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

Determine the computers' default settings

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

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

Installation requirements

*For a complete description of the necessary requirements for each platform, refer to "**Hardware, software and network requirements**" on page 519.*

Requirements for each supported platform

- **Windows**
  - **Workstations**: Windows XP SP3 and later, Windows Vista, Windows 7, Windows 8 and later, and Windows 10.
  - **Servers**: Windows 2003 SP2 and later, Windows 2008, Windows Small Business Server 2011 and later, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server Core 2008 and later.
  - **Versions with an ARM processor**: Windows 10 Home and Pro.
  - **Free space for installation**: 650 MB.
  - **Updated root certificates** in order to use the Panda Patch Management module and establish real-time communications with the management console.
- **macOS**
  - **Operating systems**: macOS 10.10 Yosemite and later.
  - **Free space for installation**: 400 MB.
  - **Ports**: ports 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware to work.
- **Linux**
  - **64-bit operating systems**: Ubuntu 14.04 LTS and later, Fedora 23 and later, Debian 8 and later, Red Hat 6.0 and later, CentOS 6.0 and later, Linux Mint 18 and later, SUSE Linux Enterprise 11.2 and later. It does not require a graphical user interface. To manage the security software, use the `/usr/local/protection-agent/bin/pa_cmd` tool from the command line.
  - **32-bit operating systems**: Red Hat from 6.0 through 6.10 and CentOS from 6.0 through 6.10.

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

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

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

Network requirements

To operate properly, Panda Adaptive Defense needs access to multiple Internet-hosted resources. Generally, it requires access to ports 80 and 443. For a complete list of all the URLs that computers with Panda Adaptive Defense installed need to access, refer to "**Access to service URLs**" on page **526**

Local installation of the client software

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

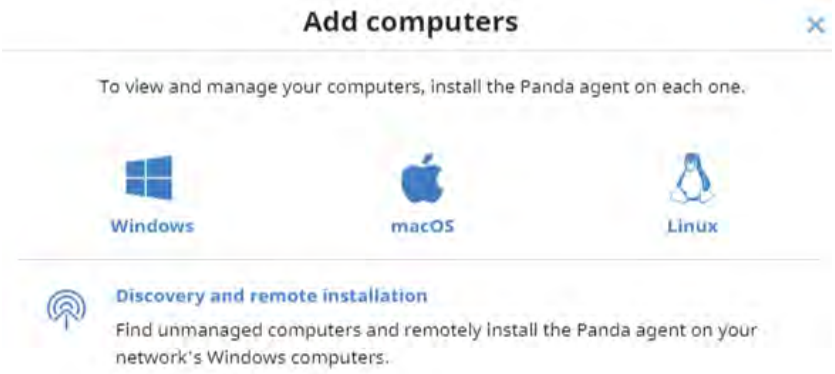
- Downloading the installation package from the Web console.
- Generating a download URL.
- Manually installing the client software.

Downloading the installation package from the Web console

*For more information on how to assign settings to computers, refer to "**Manual and automatic assignment of settings**" on page **198**.*

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

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



Add computers

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

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

Figure 6.1: Window for selecting a platform compatible with Panda Adaptive Defense

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

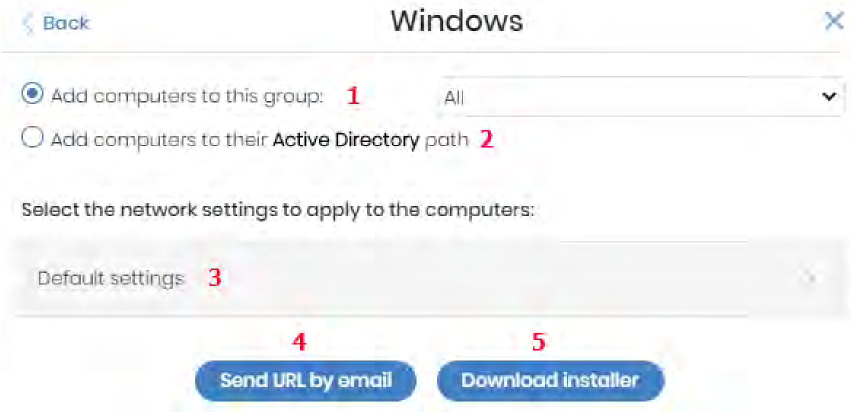
- To integrate the computer into an Active Directory group, click Add computers to their Active Directory path (2). For more information about the different types of groups, refer to "Types of groups" on page 153.

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

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

Next, select Network settings **(3)** to be applied to the computer. For more information on how to create new Network settings, refer to "Creating and managing settings" on page 197.

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



● Add computers to this group: All

○ Add computers to their Active Directory path

Select the network settings to apply to the computers:

Default settings

Figure 6.2: Configuring the download package

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

Integrating computers based on their IP address

When creating a computer group, Panda Adaptive Defense lets you specify a series of individual IP addresses and IP address ranges that will determine which computers will be added to the group when installing the protection on them. Refer to "Creating and organizing groups" on page 154 for more information on how to create groups.

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

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

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

Generating a download URL

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

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

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

Manually installing the client software

Admin permissions are required to install the Panda Adaptive Defense *software on users'* *computers.*

Installing the software on Windows x86 and ARM platforms

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

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

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

Installing the software on Linux platforms with an Internet connection

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

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

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

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

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

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

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

Make sure the following installation directories have been created:

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

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

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

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

- Red Hat 6, 7, 8.

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

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

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

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

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

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

Installing the software on MacOS platforms

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

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

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

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

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

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

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

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

Remote installation of the client software

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

Remote installation is only compatible with Windows platforms.

Operation system and network requirements

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

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

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

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

- They must not have been hidden by the administrator.
- They must not be currently managed by Panda Adaptive Defense on Aether Platform.
- They must be located on the same subnet segment as the discovery computer.

Hidden computers

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

- From the **Unmanaged computers discovered** list, click the **Discovered** button in the top right-hand corner of the screen.

- Select the checkboxes that correspond to the computers that you want to hide.
- To hide multiple computers simultaneously, click the general context menu and select **Hide and do not discover again**.
- To hide a single computer, click the computer's context menu and select **Hide and do not discover again**.

Computer discovery

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

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

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

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

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

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

Table 6.2: Information displayed for each discovery computer

Defining the discovery scope

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

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

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

Scheduling computer discovery tasks

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

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

Manually running discovery tasks

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

Viewing discovered computers

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

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

- **'Unmanaged computers discovered' list**

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

Field	Description	Values
Computer	Name of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	• — **Unmanaged**: the computer is eligible for installation, but the installation process has not started yet. • ☁ **Installing**: the installation process is in progress. • ☁ **Installation error**: displays a message specifying the type of error. Refer to table "**Computer notifications section (2)**" on page **173** for a description of all possible errors. If the cause of the error is unknown, the associated error code will be displayed.
IP address	The computer's primary IP address.	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card.	Character string
Last discovery computer	Name of the last computer that discovered the unmanaged workstation or server.	Character string
Last seen	Date when the computer was last discovered.	Date

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

If the **Status** field shows the text **Installation error,** and the cause of the error is known, a text string will be added with a description of the error. Refer to "**Computer notifications section (2)**" on page **173** for a list of the installation errors reported by Panda Adaptive Defense.

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Name	Name of the discovered computer.	Character string
IP address	The computer's primary IP address.	Character string
MAC address	The computer's physical address.	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card.	Character string
Domain	Windows domain the computer belongs to.	Character string
First seen	Date when the computer was first discovered.	Character string
First seen by	Name of the discovery computer that first saw the workstation/server.	Character string
Last seen	Date when the computer was last discovered.	Date
Last seen by	Name of the discovery computer that last saw the workstation/server	Character string
Description	Description of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	• **Unmanaged**: the computer is eligible for installation, but the installation process has not started yet. • **Installing**: the installation process is in progress. • **Installation error**: message specifying the type of error. Refer to table "Computer notifications section (2)" on page 173 for a description of all possible errors.
Error	Error description.	For more information, refer to table "Computer notifications section (2)" on page 173.
Installation error date	Date and time when the error took place.	Date

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

- **Search tool**

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

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

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "**Computer details**" on page 172 for more information.

Deleted computers

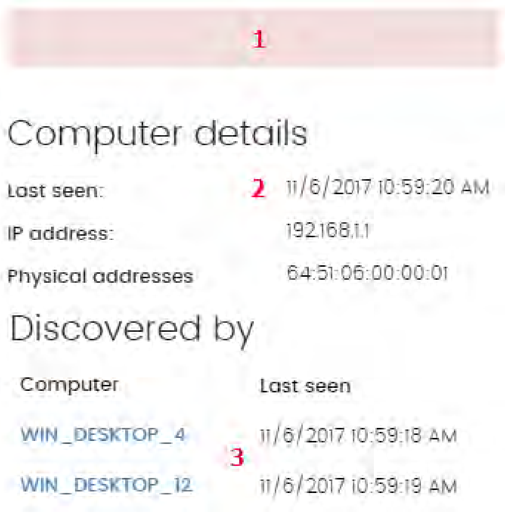
Panda Adaptive Defense doesn't remove from the **Unmanaged computers discovered** list those computers that are no longer accessible because they have been withdrawn from the network due to inspection, malfunction, theft or for any other reason.

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

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

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

Discovered computer details



Computer details

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

IP address: 192168.1.1

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

Discovered by

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

Figure 6.3: Discovered computer details

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

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

Computer alerts

Status	Type	Solution
Error installing the Panda agent	This message specifies the reason why the agent installation failed.	
	Wrong credentials	Launch the installation again using credentials with sufficient permissions to perform the installation.
	Unable to connect to the computer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to download the agent installer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to copy the agent installer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to install the agent	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to register the agent	Make sure the computer is turned on and meets the remote installation requirements.
Error installing the Panda Adaptive Defense protection	This message indicates the reason for the protection installation failure.	
	Insufficient disk space to perform the installation	Refer to "Hardware requirements" on page 523 for more information about the necessary requirements to install Panda Adaptive Defense.

Table 6.6: 'Computer alerts' section

Status	Type	Solution
	Windows Installer is not operational	Make sure the Windows Installer service is running. Stop and start the service.
	Removal of the third-party protection installed was canceled by the user	Accept the removal of the third-party antivirus solution found.
	Another installation is in progress	Wait for the current installation to finish.
	Error automatically uninstalling the third-party protection installed	Refer to **Supported uninstallers** for a complete list of the third-party solutions that Panda Security can uninstall.
	There is no uninstaller available to remove the third-party protection installed	Contact tech support to obtain the relevant uninstaller.
Installing the Panda agent	Once the installation process is complete, the computer will no longer appear on the list of unmanaged computers discovered.	
Unmanaged computer	The computer doesn't have the Panda agent installed. Make sure the computer is compatible with Panda Adaptive Defense and meets the requirements specified in chapter "**Hardware, software and network requirements**" on page 519.	

Table 6.6: 'Computer alerts' section

Computer details

Field	Description
Computer name	Name of the discovered computer.
Description	Lets you assign a description to the computer, even though it is currently not managed.
First seen	Date/time when the computer was first discovered.
Last seen	Date/time when the computer was last discovered.
IP address	IP address of the computer's network interface card.
Physical addresses (MAC)	Physical address of the computer's network interface card.
Domain	Windows domain the computer belongs to.
NIC manufacturer	Manufacturer of the computer's network interface card.

Table 6.7: 'Computer details' section

Last discovery computer

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

Table 6.8: 'Last discovery computer' section

Remote installation of the software on discovered computers

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

From the 'Unmanaged computers discovered' list

- Go to the **Unmanaged computers discovered** list.
  - Click the **Status** menu at the top of the console and go to the **My lists** section on the left-hand side menu. Click the **Add** link. From the drop-down menu, select the **Unmanaged computers discovered** list.
  - Go to the **Status** menu at the top of the console. In the **Protection status** widget, click the link **XX computers have been discovered that are not being managed by** Panda Adaptive Defense.
  - Go to the **Computers** menu at the top of the console. Click **Add computers** and select **Discovery and remote installation**. A wizard will be displayed. Click the link **View unmanaged computers discovered**.
- From the **Unmanaged computers discovered** list, select **Discovered** or **Hidden** depending on the status of the relevant computers.
- Select the checkboxes next to the computers that you want to install the software on.
  - To install it on multiple computers simultaneously, click the general context menu and select **Install Panda agent**.
  - To install it on a single computer, click the computer's context menu and then click **Install Panda agent**.
- Configure the installation by following the steps described in section "**Downloading the installation package from the Web console**".
- You can enter one or multiple installation credentials. Use the local administrator credentials for the target computer(s) or domain administrator credentials in order to install the software successfully.

From the Computer details window

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

Installation with centralized tools

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

Using the command line to install the installation package

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

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

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

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

Deploying the agent from Panda Patch Management

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

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

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

Component features and requirements

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

Component size:

- Panda Adaptive Defense 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 Adaptive Defense installer. Depending on the version, the installer will take up between 6 to 8 MB on each computer.

Deploying the agent with Microsoft Active Directory

Limitations of Microsoft Active Directory when deploying the security software

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

Steps to prepare an installation GPO

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

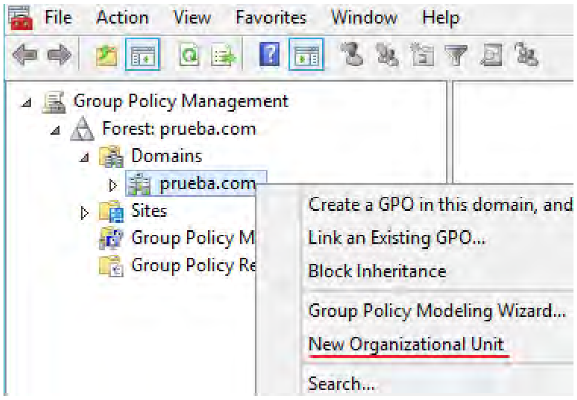


Figure 6.4: New Organizational Unit

1. Download and share the Panda Adaptive Defense installation package.

- Place the Panda Adaptive Defense installer in a shared folder accessible to all the computers that are to receive the software.

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

- Open the mmc and add the Group Policy Management snap-in.
- Right-click the domain node, and click New and Organizational Unit to create a new Organizational Unit named "Aether deployment".

3. Create a new GPO with the installation package

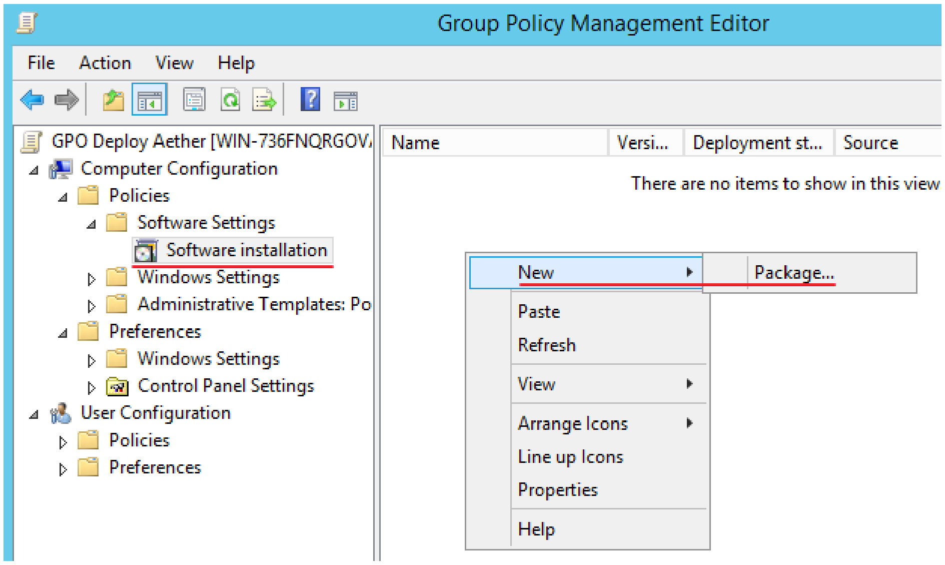
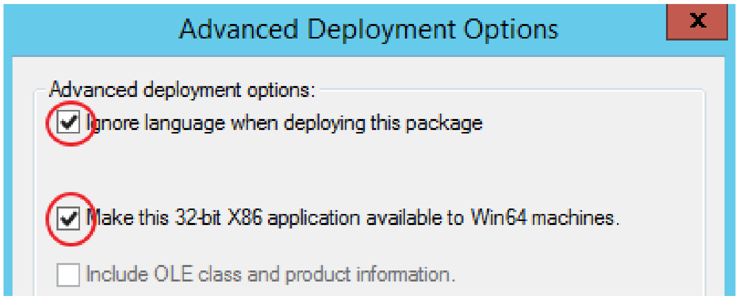


Figure 6.5: New installation package

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

4. Edit the package properties



Advanced deployment options:

☑ Ignore language when deploying this package

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

□ Include OLE class and product information.

Figure 6.6: Configuring the deployment options

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

Installation using gold image generation

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

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

Gold images and Panda Adaptive Defense

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

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

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

Non-persistent environments and Panda Adaptive Defense

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

Creating a gold image for persistent VDI environments

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

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

- Install the Panda Adaptive Defense client software using the steps described in section “**Local installation of the client software**”.

- Make sure the computer is connected to the Internet and assign it a settings profile with updates of the Panda Adaptive Defense protection and knowledge enabled. Refer to “**Managing settings**” on page 189 and chapter “**Product updates and upgrades**” on page 135 for more information on how to create and assign settings to computers respectively.
- Run `Panda Aether Tool` and click the **Start cache scan** button to scan the computer and preload the Panda Adaptive Defense goodware cache.
- Click the **Unregister device** button to delete the computer ID. Make sure the **Is a gold image** checkbox is cleared.
- Turn off the computer and generate the image with the virtual environment management software that you use.

Creating a gold image for non-persistent VDI environments

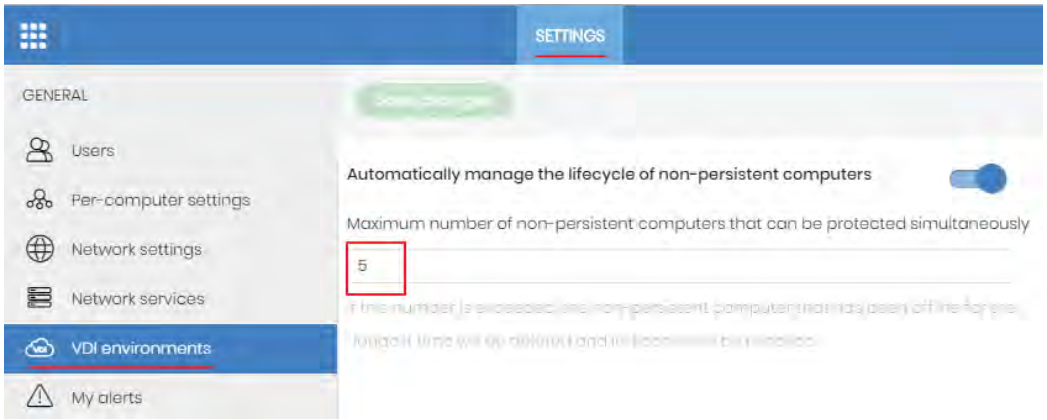
In the case of a non-persistent VDI environment, you'll need two Panda Adaptive Defense update settings profiles: one to update the gold image when preparing it and for maintenance purposes, and one to disable updates when running the gold image as it doesn't make sense to use bandwidth to update Panda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

Preparing the gold image

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

- Install the Panda Adaptive Defense client software using the steps described in section “**Local installation of the client software**”.
- .Make sure the computer is connected to the Internet and assign it a settings profile with updates of the Panda Adaptive Defense protection and knowledge enabled. Refer to “**Managing settings**” on page 189 and chapter “**Product updates and upgrades**” on page 135 for more information on how to create and assign settings to computers respectively.
- Run `Panda Aether Tool` and click the **Start cache scan** button to scan the computer and preload the Panda Adaptive Defense goodware cache.
- Click the **Unregister device** button to delete the computer ID. Make sure the **Is a gold image** checkbox is selected.
- Assign the computer a settings profile that disables updates of the Panda Adaptive Defense protection and knowledge.
- Disable the Panda Endpoint Agent service from the Windows service dashboard to prevent it from starting automatically when using the gold image on virtual instances.
- Turn off the computer and generate the image with the virtual environment management software that you use.
- Go to the **Settings** menu at the top of the console, click **VDI environments** from the left-hand side panel and configure the maximum number of computers that can be active simultaneously. This will

allow automatic management of the licenses used by these computers.



Automatically manage the lifecycle of non-persistent computers

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

5

Figure 6.7: Configuring the number of licenses assigned to non-persistent VDI computers

Running Panda Adaptive Defense in a non-persistent VDI environment

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

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

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

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

Maintaining the gold image in a non-persistent VDI environment

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

- Enable the Panda Endpoint Agent service.
- Make sure the computer is connected to the Internet, and assign it a settings profile with updates of the Panda Adaptive Defense protection and knowledge enabled.
- Run `Panda Aether Tool` and click the **Start cache scan** button to scan the computer and preload the Panda Adaptive Defense goodware cache.
- Click the **Unregister device** button to delete the computer ID. Make sure the **Is a gold image** checkbox is selected.

- Assign the computer a settings profile that disables updates of the Panda Adaptive Defense protection and knowledge.
- Disable the Panda Endpoint Agent service to prevent it from starting automatically when using the gold image on virtual instances.
- Turn off the computer and generate the image with the virtual environment management software that you use.
- In the VDI environment, replace the previous image with the new one.
- Repeat this maintenance process at least once a month.

Viewing non-persistent computers

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

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

Installation process on Windows computers

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

1. **Agent integration into Aether**: the agent sends information from the computer where it is installed to Panda's cloud for integration into the platform.
2. **Protection module installer download**: the agent downloads and installs the protection module.
3. **Signature file download**: the agent downloads the known malware signature file.
4. **Settings download**: the agent downloads the default and administrator-created settings to apply to the computer.
5. **Connectivity check to Panda's cloud**: if connectivity fails, the error type is reported in the following places:
   - **The agent installation console**: an error message is displayed along with the URLs that could not be accessed. Click the Retry button to perform a new check.
   - **The Windows Event Viewer (Event log)**: an error message is displayed along with the URLs that could not be accessed.
   - **The Web console**: an error message is displayed along with the URLs that could not be accessed.

Checking deployment

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

- Using the **Protection status** widget. Refer to "Protection status" on page 404.
- Using the **Computer protection status** list. Refer to "Computer protection status" on page 412.
- Using the Event Viewer Application log on Windows computers.

Windows Event Viewer

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

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

Table 6.9: Agent installation result codes in the Event Viewer

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

Table 6.9: Agent installation result codes in the Event Viewer

Uninstalling the software

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

Manual uninstallation

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

Refer to "Setting up the password" on page 217 for more information on how to create or remove an agent uninstallation password.

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

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

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

- **On Windows 8 or later:**
  - Control Panel > Programs > Uninstall a program.
  - Alternatively, type 'uninstall a program' at the Windows Start screen.
- **On Windows Vista, Windows 7, Windows Server 2003 and later:**
  - Control Panel > Programs and Features > Uninstall or change a program.
- **On Windows XP:**
  - Control Panel > Add or remove programs.
- **On macOS:**
  - Finder > Applications > Drag the icon of the protection to uninstall to the recycle bin, or run the following command `sudo sh /Applications/Protection-Agent.app/Contents/uninstall.sh`.
  - Dragging the icon to the recycle bin doesn't uninstall the agent. To remove it, you have to run the following command `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`
- **On Linux:**

Open the command line and enter:

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

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

Manual uninstallation result

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

Remote uninstallation

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

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

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

Remote reinstallation

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

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

Remote reinstallation requirements

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

Accessing the feature

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

- "**Computer protection status**" on page **412**.
- **"Patch management status**" on page **307**.
- **"'Data Control status'**" on page **265**.
- **"Encryption Status**" on page **347**.
- "**Licenses**" on page **130**.
- "**'Hardware'**" on page **166**.

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

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

Discovering computers whose software needs reinstalling

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

Reinstalling the software on a single computer

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

Reinstalling the software on multiple computers

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

'Reinstall protection' selection window

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

- **Reinstall the protection immediately (requires restart)**: the computer's protection will be reinstalled in one minute. If the target computer is not available at that particular time because it is turned off or offline, the restart command will remain on the Panda Adaptive Defense server for 1 hour.
- **Delay reinstallation for a certain time**: the computer's protection will be reinstalled according to the time configured by the administrator. If the target computer is not available because it is turned off or offline, the restart command will remain on the Panda Adaptive Defense server for 7 days.

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

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

‘Reinstall agent’ selection window

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

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

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

Error codes

Refer to “**Possible errors in the protection software reinstallation process**” on page 176 for a list of all possible error codes and the recommended actions to resolve them.

Chapter 7

Licenses

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

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

CHAPTER CONTENT

Definitions and basic concepts

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

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

License contracts

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

- **Product type**: Panda Adaptive Defense, Panda Full Encryption, Panda Patch Management, Panda Adaptive Defense with Panda Advanced Reporting Tool, Panda Adaptive Defense with Panda Data Control, Panda Adaptive Defense with Panda Advanced Reporting Tool and Panda Data Control.
- **Contracted licenses**: number of licenses in the license contract.
- **License type**: NFR, Trial, Commercial, Subscription.
- **Expiration date**: date when all licenses in the license contract expire and the computers cease to be protected.

Computer status

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

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

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

License status and groups

There are two possible statuses for contracted licenses:

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

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

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

Types of licenses

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

Assigning licenses

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

Refer to "Managing computers and devices" on page 143 for more information about the search tool, the folder tree and the filter tree.

Automatic assignment of licenses

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

Manual assignment of licenses

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

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

Releasing licenses

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

Automatic release

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

Manual release

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

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

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

Processes associated with license assignment

Case 1: Excluded computers and those with assigned licenses

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

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

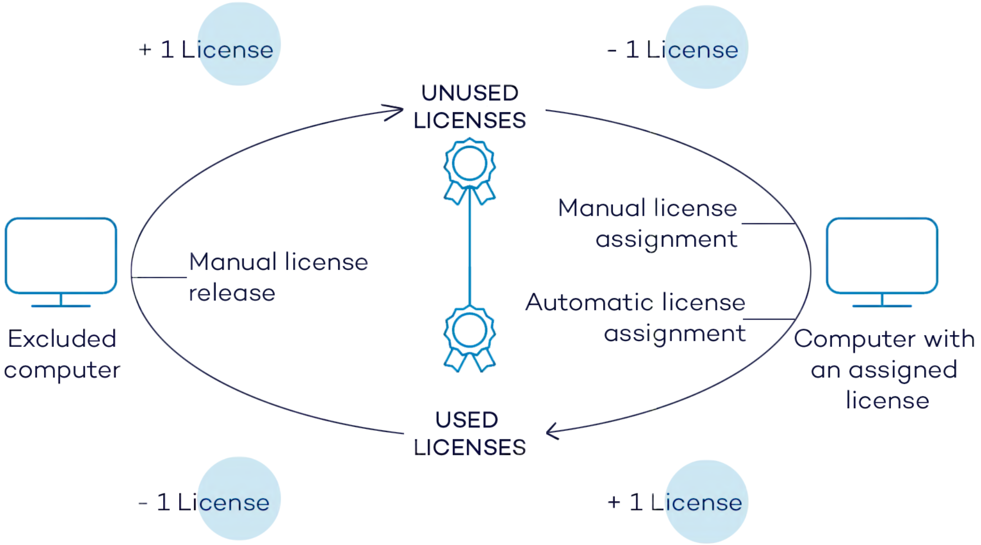


Figure 7.1: Modification of license groups with excluded computers and those with licenses assigned

Case 2: Computers without an assigned license

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

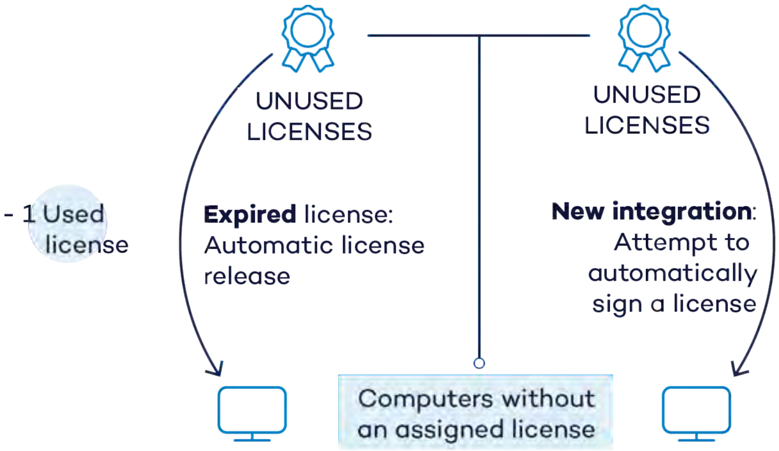

UNUSED LICENSES
UNUSED LICENSES
- 1 Used license
Expired license: Automatic license release
New integration: Attempt to automatically sign a license
Computers without an assigned license

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

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

Licenses module panels/widgets

Accessing the dashboard

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

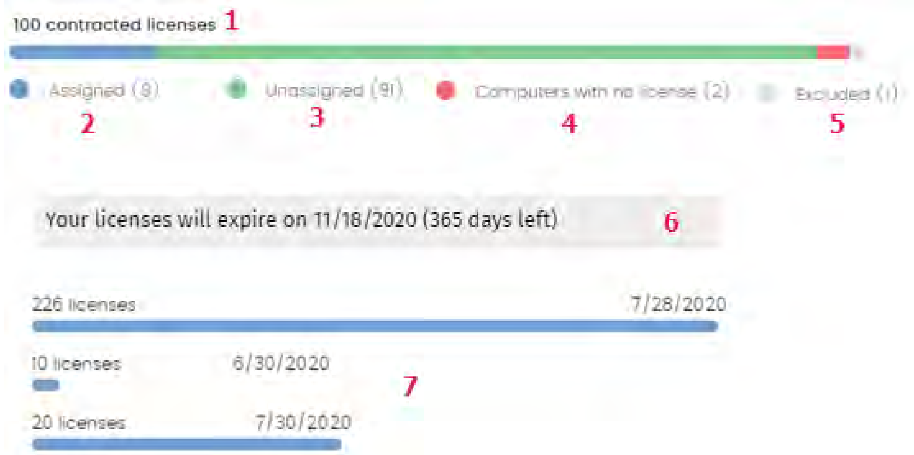
Required permissions

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

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

Licenses

The panel shows how the contracted product licenses are distributed.



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

Figure 7.3: License panel with three license contracts

- **Meaning of the data displayed**

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

Table 7.1: Fields in the 'Licenses' panel

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

Table 7.1: Fields in the 'Licenses' panel

- **Lists accessible from the panel**

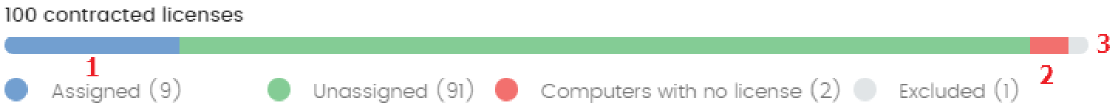


Figure 7.4: Hotspots in the 'Contracted licenses' panel

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

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

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

Licenses module lists

Accessing the lists

There are two ways to access the lists:

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

Or,

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

Required permissions

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

Licenses

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

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

Table 7.3: Fields in the ‘Licenses’ list

- **Fields displayed in the exported file**

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

Table 7.4: Fields in the 'Licenses' exported file

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

Table 7.4: Fields in the 'Licenses' exported file

- **Filter Tool**

Field	Description	Values
Find computer	Computer name.	• Character string
Computer type	Purpose of the computer within the organization's network	• Workstation • Laptop
Platform	Operating system installed on the computer.	• All • Windows
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the computer status was last sent to Panda Security's cloud.	• All • More than 72 hours ago • More than 7 days ago • More than 30 days ago

Table 7.5: Filters available in the 'Licenses' list

Field	Description	Values
License status	The computer's license status.	• Assigned • No license • Excluded

Table 7.5: Filters available in the 'Licenses' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window.Refer to "**Computer details**" on page 172 for more information.

Expired licenses

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

Expiration notifications

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

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

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

Withdrawal of expired licenses

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

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

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

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

Computer search based on license status

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

> *Refer to "*Creating and organizing filters*" on page* 147 *for more information on how to create filters in* Panda Adaptive Defense.

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

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

Table 7.6: Fields in the 'Licenses' filter

Chapter 8

Product updates and upgrades

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

CHAPTER CONTENT

Updatable modules in the client software

The components installed on users' computers are the following:

- Aether Platform communications agent.
- Panda Adaptive Defense protection engine.
- Signature file.

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

Module	Platform		
	Windows	macOS	Linux
Panda agent	On demand		
Panda Adaptive Defense protection	Configurable	Configurable	Configurable
Signature file	Enable /Disable	Enable /Disable	Enable /Disable

Table 8.1: Update procedures based on the client software component

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

Protection engine updates

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

Updates

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

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

Running updates at specific time intervals

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

- Start time

- End time

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

Running updates on specific days

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

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

Computer restart

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

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

Communications agent updates

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

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

Knowledge updates

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

Windows, Linux and macOS devices

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

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

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

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

Management console upgrades

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

Considerations prior to upgrading the console version

Although this is a process that takes place entirely on the Panda Security servers, upgrading the console version can push new versions of the security software to the customer's computers. This can result in high traffic loads and the need to restart the computers on the network in some cases. To reduce the traffic during updates, refer to "Configuring downloads via cache computers" on page 213.

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

Starting the management console upgrade

- Click the **Web notifications** icon 🔔3 on the upper-right side of the top menu. The unread notifications appear.
- If there is a console upgrade available, a message entitled **New management console version** is shown, along with the **New features and improvements** link, the version to which the console will be upgraded, and the **Upgrade console now** button. This type of notification cannot be deleted, as it

does not show the ✕ icon. Refer to "Web notifications icon" on page 45.

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

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

Canceling the upgrade

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

Part 4

Managing devices

Chapter 9

Managing computers and devices

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

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

CHAPTER CONTENT

The Computers area

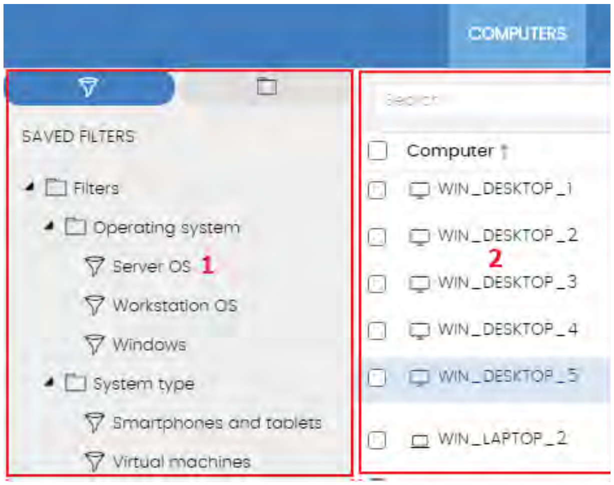


Figure 9.1: General view of the panels in the Computers area

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

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

Show computers in subgroups

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

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

The Computer tree panel

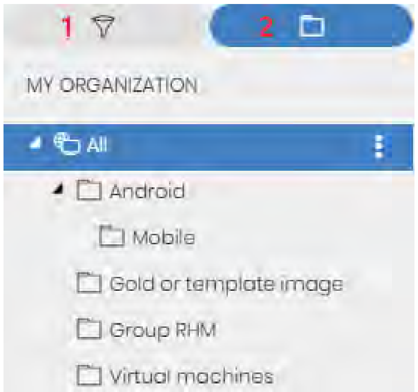


Figure 9.2: The Computers tree panel

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

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

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

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

*For more information on how to locate unprotected computers or those with certain security characteristics or protection status, refer to "***Malware and network visibility***" on page* **403***. For more information on how to assign security settings profiles, refer to "***Manual and automatic assignment of settings***" on page* **198***. For more information on how to take remediation actions, refer to "***Remediation tools***" on page* **495**.

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

Filter tree

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

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

What is a filter?

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

A computer can belong to more than one filter.

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

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

Predefined filters

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

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

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

Table 9.1: Predefined filter list

Creating and organizing filters

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

Creating filters

To create a filter, follow the steps below:

- Click the context menu of the folder where the filter will be created.
  - If you want to create a hierarchical structure of filters, create folders and move your filters to them.

A folder can contain other folders with filters.

- Click **Add filter**.
- Specify the name of the filter. It does not have to be a unique name. Refer to "Configuring filters" for more information on how to configure a filter.

Creating folders

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

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

Deleting filters and folders

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

You cannot delete the 'Filters' root node

Moving and copying filters and folders

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

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

Renaming filters and folders

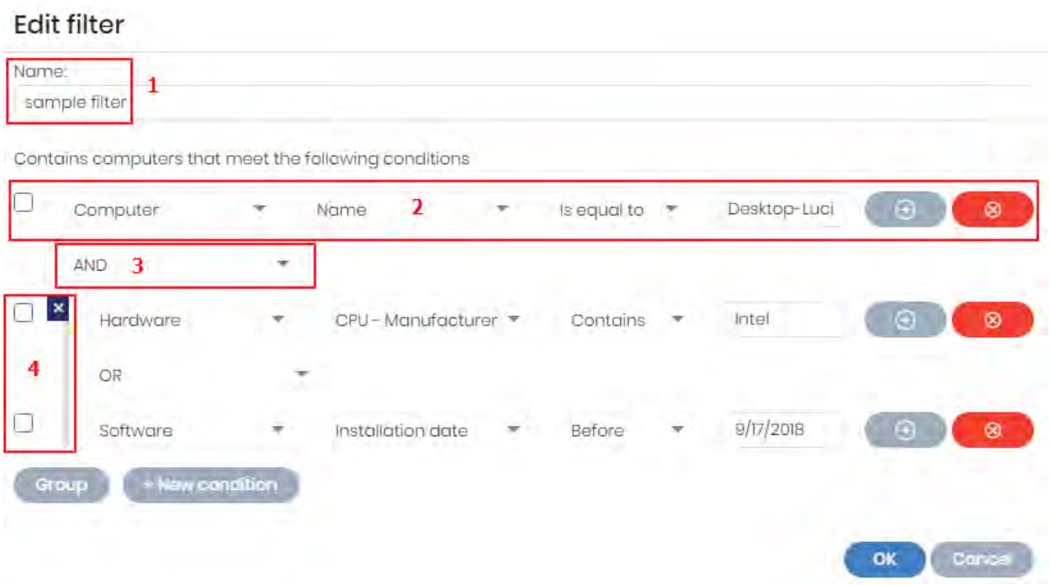
- Click the context menu of the branch to rename.
- Click **Rename**.
- Enter the new name.

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

Configuring filters

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

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


Edit filter

Name: sample filter

Contains computers that meet the following conditions

Computer	Name	Is equal to	Desktop-Luci
AND			
Hardware	CPU - Manufacturer	Contains	Intel
OR			
Software	Installation date	Before	9/17/2018

Figure 9.3: Filter settings overview

A filter has four sections

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

Filter rules

A filter rule comprises the items described below:

- **Category**: this groups the properties in sections to make it easy to find them.
- **Property:** the characteristic of a computer that determines whether or not it belongs to the filter.
- **Operator**: this determines the way in which the computer's characteristics are compared to the values set in the filter.
- **Value**: the content of the property. Depending on the type of property, the value field will change to reflect entries such as 'date', etc.

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

Logical operators

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

Filter rule groupings

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

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

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

Common use cases

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

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

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

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

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

Computers without a specific patch installed

Lists computers that don’t have a specific patch installed. Refer to “**Panda Patch Management (Updating vulnerable programs)**” on page **285** for more information about Panda Patch Management.

- **Category**: Software
- **Property**: Software name

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

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

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

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

Computers that cannot connect to the Panda Security security intelligence services

Finds all computers that have problems connecting to one of the Panda Security security intelligence services. Create the following rules interconnected with the OR operator:

- **Rule:**
  - **Category**: Security
  - **Property**: Connection for sending events
  - **Condition**: Equals
  - **Value**: With problems

Isolated computers

Lists computers that have been isolated from the network. Refer to "**Computer isolation**" on page **501**.

- **Category**: Computer
- **Property**: Isolation status
- **Condition**: Is equal to
- **Value**: Isolated

Computers in RDP attack containment mode

Lists computers that have received a high number of RDP connection attempts which have started to be blocked by Panda Adaptive Defense 360.

- **Category**: Computer
- **Property**: "RDP attack containment" mode
- **Condition**: Is equal to
- **Value**: True

Integration with other management tools

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

- **Category**: Computer
- **Property**: Name
- **Condition**: In
- **Value**: computer name list

Group tree

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

To access the group tree, follow the steps below:

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

What is a group?

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

> *The maximum number of levels in a group is 10.*

Types of groups

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

Table 9.2: Group types in Panda Adaptive Defense

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

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

Active Directory groups

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

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

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

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

Creating and organizing groups

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

Creating a group

- Click the context menu of the parent group to which the new group will belong, and click **Add group**.
- Enter the name of the group in the Name text box and click the **Add** button.

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

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

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

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

Deleting groups

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

The 'All' root node cannot be deleted.

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

Moving groups

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

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

Renaming groups

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

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

Importing IP-based assignment rules to existing groups

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

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

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

  - For IP ranges: add a line per range:

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

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

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

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

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

Exporting IP-based assignment rules

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

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

Moving computers from one group to another

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

Moving groups of computers to groups

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

Moving a single computer to a group

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

- Follow the steps described above for moving groups of computers, but simply select a single computer.

- Find the computer that you want to move and click the ⋮ menu icon to its right.
- From the details screen of the computer that you want to move:
  - From the panel with the list of computers, click the computer you want to move in order to display its details.
  - Find the **Group** field and click **Change**. This will display a window with the target group tree.
  - Select the target group to move the computer to and click **OK**.

Moving computers from an Active Directory group

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

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

Moving computers to an Active Directory group

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

Returning multiple computers to their Active Directory group

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

Filtering results by groups

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

Configuring the filter by groups

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

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

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

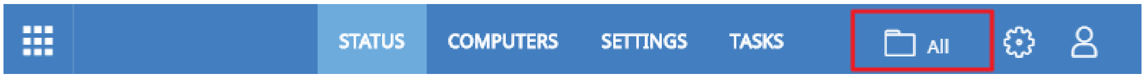


Figure 9.4: Filtering results by groups

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

Filtering groups

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

- Click the 🔍 icon at the top of the group tree. A text box appears.
- Enter the letters of the name of the group to find. All groups whose name starts with, ends with, or contains the character string entered are shown.
- After you have completed your search, select the group you are interested in and click the ✕ icon to show the full group tree again, maintaining your selection.

Disinfection tasks

The group tree allows you to assign disinfection tasks to all computers belonging to a group and its subgroups.

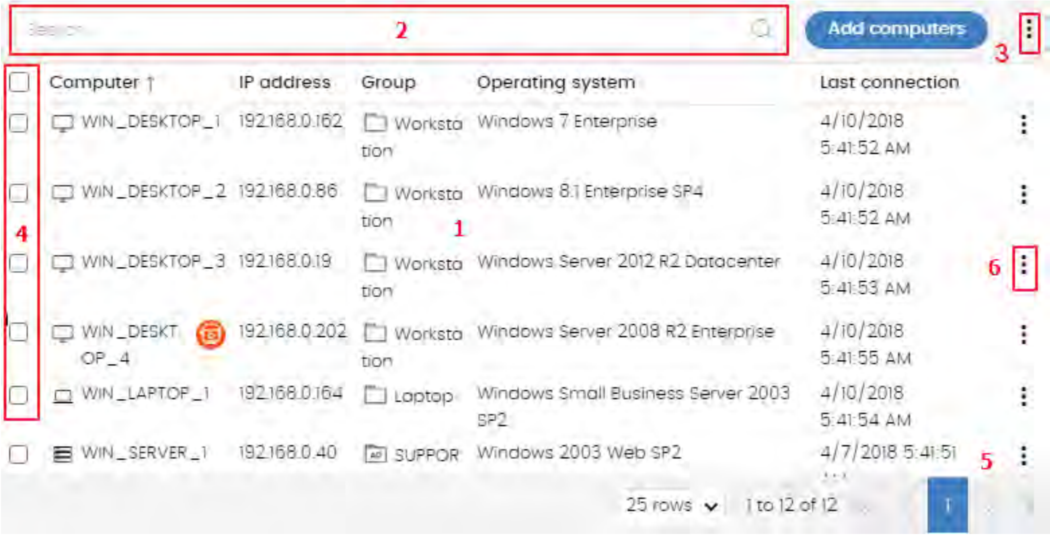
Click the **Disinfect** option to launch an immediate scan of all computers belonging to a group or any of its subgroups.

Available lists for managing computers

Accessing the lists

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

the content of the selected item.



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

Figure 9.5: The Computer list panel

Required permissions

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

Computers

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

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

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

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

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

The following information is displayed for each computer.

Field	Description	Values
Computer	Computer name and type.	Character string • Workstation or server. • Laptop. •
Computer status	Agent reinstallation: • Reinstalling the agent. • Agent reinstallation error. Protection reinstallation: • Reinstalling the protection • Protection reinstallation error. • Pending restart.	Icon
	Computer isolation status: • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated.	
	"RDP attack containment" mode: • Computer in "RDP attack containment" mode. • Ending "RDP attack containment" mode.	
IP address	The computer's primary IP address.	IP address
Description	Description assigned to the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory path	Path to the computer in the company's Active Directory.	Character string

Table 9.3: Fields in the 'Computers' list

Field	Description	Values
IP address	The computer's primary IP address.	IP address • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated.
Group	Folder within the Panda Adaptive Defense group tree to which the computer belongs, and its type.	Character string • Group. • IP-based group • Active Directory AD or root domain. • Organizational Unit. • Group tree root.
Operating system	Name and version of the operating system installed on the computer.	Character string
Last connection	Date when the computer status was last sent to Panda Security's cloud.	Date
Last logged-in user	Name of the user accounts currently logged-in to the console on the computer.	Character string

Table 9.3: Fields in the 'Computers' list

- **Campos mostrados en el fichero exportado**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	Comma-separated list of the IP addresses of all cards installed on the computer.	Character string
Physical addresses (MAC)	Comma-separated list of the physical addresses of all cards installed on the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string

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

Field	Description	Values
Active Directory	Path to the computer in the company's Active Directory.	Character string
Group	Folder within the Panda Adaptive Defense group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
System boot date	Date when the computer was last booted.	Date
Installation date	Date when the Panda Adaptive Defense software was successfully installed on the computer.	Date
Last connection	Last time the computer connected to the cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS
Operating system	Name of the operating system installed on the computer, internal version and patching status.	Character string
Virtual machine	Indicates whether the computer is physical or virtual.	Boolean
Is a non-persistent computer	Indicates if the operating system of the virtual machine resides on a storage device that persists between restarts, or reverts to its original state instead.	Boolean
Protection version	Internal version of the protection module installed on the computer.	Character string
Last update on	Date when the protection was last updated.	Date
Licenses	Licensed product.	Panda Adaptive Defense
Network settings	Name of the network settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the network settings.	Character string
Security for workstations and servers	Name of the security settings applied to the workstation or server.	Character string
Settings inherited from	Name of the folder from which the computer inherited its security settings.	Character string
Per-computer settings	Name of the settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited its settings.	Character string

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

Field	Description	Values
Data Control	Name of the personal data monitoring (Panda Data Control) settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited its personal data monitoring settings.	Character string
Patch management	Name of the patching (Panda Patch Management) settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the patching settings.	Character string
Encryption	Name of the encryption (Panda Full Encryption) settings applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the encryption settings.	Character string
Program blocking	Name of the program blocking settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer inherited the program blocking settings	Character string
Isolation status	Shows the isolation status of the computer.	• Isolated • Isolating • Stopping isolation • Not isolated
Description	Description assigned to the computer.	Character string
Last logged-in user	Names of the user accounts, separated by commas, that are currently logged in to the console on a Windows computer.	Character string
Requested action	Requested action that is pending execution or is in progress.	• Restart • Protection reinstallation • Agent reinstallation
Requested action failed	Type of error reported by the requested action.	• Wrong credentials • Discovery computer not available • Unable to connect to the computer • Operating system not supported

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

Field	Description	Values
		• Unable to download the agent installer • Unable to copy the agent installer • Unable to uninstall the agent • Unable to install the agent • Unable to register the agent • Action requires input from the user
Last proxy used	Access method used by Panda Adaptive Defense the last time it connected to Panda Security's cloud. This data is not updated immediately, so it might take up to 1 hour for the correct value to show.	Character string

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

- **Filter tools**

Field	Description	Values
Computer	Computer name.	Character string

Table 9.5: Filters available in the 'Computers' list

- **Management tools**

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

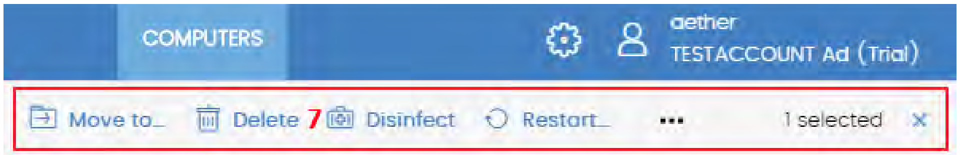


Figure 9.6: Action bar

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

Action	Description
Refresh computer information	Forces the agent installed on the computer to take the following actions: • Check for pending actions. Check for pending tasks • Check for applied settings. • Send status information. This icon is shown only for computers with the Real-time communication feature enabled. Refer to "Configuring real-time communication" on page 215.
Move to	Opens a window showing the group tree. Choose the group to move the computer to. The computer will inherit the settings assigned to the target group. Refer to "Creating and managing settings" on page 197
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 client software from it. Refer to "Uninstalling the software" on page 118 for more information.
Restart	Restarts the computer. "Computer restart" on page 500 for more information.
Disinfect	Lets you run a disinfection task immediately.
Isolate computer	Blocks all communications established from and to the computer, except for those required to connect to Panda Security's cloud. Refer to "Isolating one or more computers from the organization's network" on page 502.
Stop isolating the computer	Restores all communications to and from the computer. Refer to "Stopping a computer from being isolated" on page 503 for more information.
Schedule patch installation	Refer to "Panda Patch Management (Updating vulnerable programs)" on page 285 for more information on how to install patches on Windows computers
Reinstall protection (requires restart)	Reinstalls the protection if a malfunction occurs. Refer to "Remote reinstallation" on page 120 for more information.
× selected	Undoes the current selection.

Table 9.6: Computer management tools

My lists panel

Accessing the My lists panel

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel. A window appears with all available lists.

From the **General** group, select the **Hardware**, **Software**, or **Computers with duplicate name** list.

> *Refer to "Managing lists" on page 53 for more information about the available list types and how to work with them.*
>
> *For more information about the fields as well as the filter and search tools implemented in each list, refer to the chapter on the group the list belongs to.*

Required permissions

No additional permissions are required to access the **My lists** panel.

'Hardware'

Shows the hardware components installed on each computer on the network. Each hardware component is shown independently each time it is detected on a computer.

Field	Description	Values
Computer	Name and type of computer that contains the hardware component.	Character string • 🖥 Workstation or server • 💻 Laptop.
Group	Folder within the Panda Adaptive Defense folder tree to which the computer belongs.	Character string
CPU	Make and model of the microprocessor installed on the computer. The number of installed cores is shown in brackets.	Character string
Memory	Total amount of RAM memory installed.	Character string
Disk capacity	Sum of the capacity of all the internal hard disks connected to the computer.	Character string
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	Date
Context menu	Management tools. Refer to "Management tools" for more information.	

Table 9.7: Fields in the 'Hardware' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder within the Panda Adaptive Defense group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS
Operating system	Name of the operating system installed on the computer, internal version and patch status.	Character string
System	Name of the computer's hardware model.	Character string
CPU-N	Model, make and characteristics of CPU number N.	Character string
CPU-N Number of cores	Number of cores in CPU number N.	Numeric value
CPU-N Number of logical processors	Number of logical cores reported to the operating system by the Hyper-Threading/SMT (simultaneous multithreading) system.	Numeric value
Memory	Sum of all the RAM memory banks installed on the computer.	Character string
Disk-N Capacity	Total space on internal storage device number N.	Character string
Disk-N Partitions	Number of partitions on internal storage device number N reported to the operating system.	Numeric value
TPM spec version	Versions of the APIs compatible with the TPM chip.	Character string

Table 9.8: Fields in the 'Hardware' exported file

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

Table 9.8: Fields in the 'Hardware' exported file

- **Filter tool**

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

Table 9.9: Filters available in the 'Hardware' list

'Software'

Shows all programs installed on the computers on your network. For each package, the solution reports the number of computers that have it installed, as well as the software version and vendor.

Click any of the software packages to open the "**Computer list**" filtered by the selected package. The list will show all computers on the network that have that package installed.

Field	Description	Values
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Version	Internal version of the software package.	Character string
Computers	Number of computers with the selected package installed.	Numeric value

Table 9.10: Fields in the 'Software' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Version	Internal version of the software package.	Character string

Table 9.11: Fields in the 'Software' exported file

Field	Description	Values
Computers	Number of computers that have the package installed.	Numeric value

Table 9.11: Fields in the 'Software' exported file

- **Fields displayed in the detailed Excel export file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer that contains the package found.	Numeric value
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Installation date	Date the software was installed.	Date
Size	Installed software size.	Numeric value
Version	Internal version of the software package.	Character string
Group	Folder within the Panda Adaptive Defense group tree to which the computer belongs.	Character string
IP address	The computer’s primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 9.12: Fields in the detailed export file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Platform	Operating system make.	• WindowsLinux • macOS

Table 9.13: Filters available in the 'Software' list

- **Computers list window**

Clicking any of the rows in the list displays the list of computers filtered by the selected software.Refer to “Computers” for more information.

Computers with duplicate name’

Shows computers on the network with the same name and belonging to the same domain. Of all computers with the same name found on the network, those computers that have been offline for the longest time will be considered redundant and will be displayed in the list. The computer that has been online most recently will be considered the correct one and won’t be shown in the list. This way, the administrator will be able to safely select and delete all duplicates at once.

To delete duplicate computers, select them using the relevant checkboxes and click Delete from the toolbar. A window will be shown asking you if you wish to uninstall the Panda Adaptive Defense agent.

Deleting computers from the ***Computers with duplicate name*** *list without uninstalling the Panda Adaptive Defense agent only removes them from the Panda Adaptive Defense console. Those computers will appear in the Panda Adaptive Defense console the next time they connect to the cloud. Before deleting computers in bulk without knowing which ones are true duplicates, we advise that you first check to see which computers reappear in the console before deleting the agent from any computers.*

Field	Description	Values
Computer	Computer name and type.	Character string: • 🖥 Workstation or server • 💻 Laptop computer.
IP address	The computer’s primary IP address.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security‘s cloud.	Date

Table 9.14: Fields in the ‘Computers with duplicate name’ list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer’s primary IP address.	Character string

Table 9.15: Fields in the ‘Computers with duplicate name’ exported file

Field	Description	Values
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Protection version	Internal version of the protection module installed on the computer.	Character string
Installation date	Date the Panda Adaptive Defense software was successfully installed on the computer.	Date
Last connection date	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	Date
Platform	Type of operating system installed.	• WindowsLinux • macOS
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Active Directory	Full path to the computer in the company's Active Directory.	Character string
Last logged-in user	Names of the user accounts that are currently logged in to the console on the computer.	Character string
Last bootup date	Date when the computer was last booted.	Date

Table 9.15: Fields in the 'Computers with duplicate name' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Platform	Operating system make.	• All • Windows • Linux • macOS
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago

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

Field	Description	Values
		• Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago

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

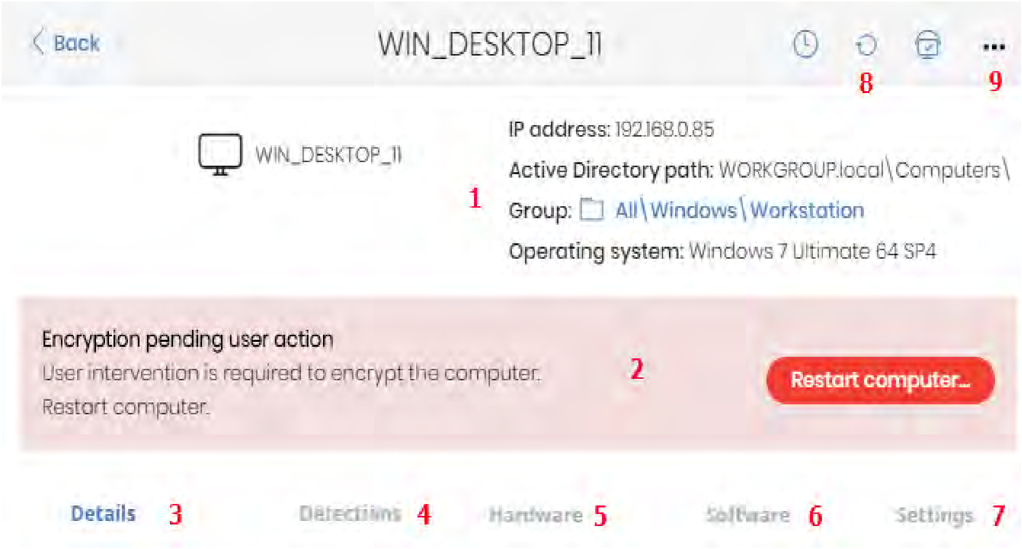
- **Computer details window**

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

Computer details

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

The details screen is divided into the following sections:



IP address: 192.168.0.85
Active Directory path: WORKGROUP.local\Computers\
Group: All\Windows\Workstation
Operating system: Windows 7 Ultimate 64 SP4

Encryption pending user action
User intervention is required to encrypt the computer.
Restart computer.

Figure 9.7: Computer details overview

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

- **Settings (7)**: this shows the security settings and other settings assigned to the computer.
- **Toolbar (8)**: groups the operations available for the managed computer.
- **Hidden icons (9)**: if the window is not large enough, some tools will be hidden.

General section (1)

This contains the following information:

Field	Description
Computer name and icon indicating the type of computer	Computer name.
IP address	The computer's IP address.
Active Directory path	Full path to the computer in the company's Active Directory.
Group	Folder in the group tree to which the computer belongs.
Operating system	Full version of the operating system installed on the computer.
Computer role	Indicates if the computer has any of the following roles assigned to it: discovery computer, cache or proxy.

Table 9.17: Fields in the computer details' General section

Computer notifications section (2)

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

Isolated computers

Alert	Description	Reference
Isolated computer	The administrator has isolated the computer and all connections have been blocked except for those required by Panda Adaptive Defense to work properly.	Refer to "Computer isolation" on page 501 for more information.
We're trying to isolate this computer	The Panda Adaptive Defense server is attempting to isolate the computer but the operation is not yet complete because the computer is offline or turned off.	Refer to "Offline computers" on page 406 for more information.

Table 9.18: Alerts related to the computer isolation feature

Alert	Description	Reference
We're trying to stop isolating this computer	The Panda Adaptive Defense server is attempting to stop isolating the computer but the operation is not yet complete because the computer is offline or turned off.	Refer to "**Offline computers**" on page 406 for more information.

Table 9.18: Alerts related to the computer isolation feature

Computers in containment mode

Alert	Description	Reference
Computer in "RDP attack containment" mode	The computer has received a high number of failed RDP connection attempts, and all RDP connections have been blocked to contain the attack.	Refer to "**Detection and protection against RDP attacks**" on page 373.
We're trying to end the "RDP attack containment" mode on this computer.	The administrator has manually ended the "RDP attack containment" mode on the computer, but the operation is not yet complete. This may be due to the fact that the computer is turned off, offline, pending restart, or the action is in progress.	Refer to "**Detection and protection against RDP attacks**" on page 373.

Table 9.19: Alertas relacionadas con la funcionalidad de contención de equipos

Licenses

Alert	Description	Reference
Computer without a license	There are no free licenses to assign to the computer. Release an assigned license or purchase more Panda Adaptive Defense licenses.	Refer to "**Releasing licenses**" on page 126.
	There are free licenses but none of them have been assigned to this computer.	Refer to "**Assigning licenses**" on page 125.

Table 9.20: Alerts related to license assignment

Possible errors in the protection software installation process

⚠ *Panda server connection errors occurred while installing the protection software are indicated by an error code, its associated extended error code, and an extended error subcode (if available). Refer to 19.13 for more information.*

Alert	Description	Reference
Unprotected computer	There was an error installing the protection on the computer. With errors whose origin is known, a description of the cause will be displayed. If the origin is unknown, the associated error code will be displayed.	Refer to "Installation requirements" on page 94.
	A reboot is required to complete the installation due to a previous uninstallation.	Refer to "Computer restart" on page 500.
Error installing Data Control	There was an error installing Data Control on the computer.	Refer to "Panda Data Control requirements" on page 235.
Error installing the protection and Data Control	There was an error installing the protection and the Data Control module on the computer.	Refer to "Installation requirements" on page 94 and section "Panda Data Control requirements" on page 235.
Error installing the patch manager	There was an error installing the patch management module on the computer.	Refer to "Make sure that Panda Patch Management works properly" on page 287.
Error installing the encryption module	There was an error installing the encryption module on the computer.	Refer to "Panda Full Encryption (Device encryption)" on page 329.
Error installing the Panda agent	Wrong credentials.	Refer to "Remote installation of the software on discovered computers" on page 109.
	The discovery computer is not available.	Refer to widget "Offline computers" on page 406 and section "Assigning the role of 'Discovery computer' to a computer on your network" on page 102.
	Unable to connect to the target computer because it is turned off or doesn't comply with the hardware or network requirements.	Refer to widget "Offline computers" on page 406 and section "Installation requirements" on page 94.
	The computer's operating system is not supported.	Refer to "Installation requirements" on page 94.
	Unable to download the agent installer due to a network error.	Refer to "Network requirements" on page 96.
	Unable to copy the agent installer due to low free disk space on the computer.	Refer to "Requirements for each supported platform" on page 95.
	Unable to copy the agent installer because the target computer is turned off or doesn't meet the remote installation requirements.	Refer to widget "Offline computers" on page 406 and section "Installation requirements" on page 94.

Table 9.21: Alerts related to the installation of the Panda Adaptive Defense software

Alert	Description	Reference
	Unable to register the agent.	Refer to widget “Offline computers” on page 406 and “Installation requirements” on page 94
Error communicating with servers	The computer cannot connect to one or more servers in the Panda cloud.	For more information, refer to “Hardware, software and network requirements” on page 519

Table 9.21: Alerts related to the installation of the Panda Adaptive Defense software

Possible errors in the protection software reinstallation process

> ⚠ *Panda server connection errors occurred while reinstalling the protection software are indicated by an error code, its associated extended error code, and an extended error subcode (if available). Refer to* 19.13 *for more information.*

Alert	Description	Reference
Pending protection reinstallation	The administrator requested that this computer’s protection be reinstalled but the operation has not been performed yet. This may be due to the fact that the computer is turned off or offline, or the time to wait before forcing the restart hasn’t elapsed yet.	Refer to widget “Offline computers” on page 406 and section “Remote reinstallation requirements” on page 120
Pending agent reinstallation	The administrator requested that this computer’s agent be reinstalled but the operation has not been performed yet. This may be due to the fact that the computer is turned off or offline, or the time to wait before forcing the restart hasn’t elapsed yet.	Refer to widget “Offline computers” on page 406 and section “Remote reinstallation requirements” on page 120
Error installing the Panda agent	Wrong credentials.	
	Discovery computer not available.	Refer to widget “Offline computers” on page 406
	Unable to connect to the computer as it is turned off or doesn’t meet the remote installation requirements.	Refer to widget “Offline computers” on page 406 and section “Remote reinstallation requirements” on page 120
	Operating system not supported as it doesn’t meet the remote installation requirements.	Refer to “Remote reinstallation requirements” on page 120

Table 9.22: Alerts related to the reinstallation of the Panda Adaptive Defense agent

Alert	Description	Reference
	Unable to download the agent installer to the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "**Offline computers**" on page **406** and section "**Remote reinstallation requirements**" on page **120**
	Unable to copy the agent installer to the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "**Offline computers**" on page **406** and section "**Remote reinstallation requirements**" on page **120**
	Unable to uninstall the agent from the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "**Offline computers**" on page **406** and section "**Remote reinstallation requirements**" on page **120**
	Unable to install the agent on the target computer as it is turned off or doesn't meet the remote installation requirements.	Refer to widget "**Offline computers**" on page **406** and section "**Remote reinstallation requirements**" on page **120**
	Unable to register the computer's agent because the computer is turned off or doesn't meet the remote installation requirements.	Refer to widget "**Offline computers**" on page **406** and section "**Remote reinstallation requirements**" on page **120**

Table 9.22: Alerts related to the reinstallation of the Panda Adaptive Defense agent

Panda Adaptive Defense software malfunction errors

Alert	Description	Reference
Unprotected computer	An error was encountered in the advanced protection. Restart the computer to fix the problem.	Refer to "**Computer restart**" on page **500**.
Data Control error	An error was encountered in Data Control. Restart the computer to fix the problem.	Refer to "**Computer restart**" on page **500**.
Error encrypting the computer	Unable to encrypt the computer due to an error.	Refer to "**Computer restart**" on page **500**.

Table 9.23: Alerts related to Panda Adaptive Defense software malfunction errors

Pending user or administrator action

Alert	Description	Reference
Encryption pending user action	The user must restart the computer or enter the relevant encryption credentials to complete the encryption process.	Refer to "**Computer restart**" on page **500**. Refer to "**Encryption and decryption**" on page **336**.

Table 9.24: Alerts related to lack of user or administrator action

Alert	Description	Reference
Pending restart	The administrator has requested that the computer be restarted but it hasn't restarted yet as it is offline or the time period for a forced reboot has not ended yet.	Refer to "**Offline computers**" on page 406.
Reinstalling protection	The administrator has requested that the computer's protection be reinstalled but the operation is not yet complete because the computer is turned off or offline, the amount of time to wait before forcing the reinstallation is not over yet, or the reinstallation is in progress	Refer to "**Remote reinstallation**" on page 120.
Unprotected computer	The advanced protection is disabled. Enable the protection.	Refer to "**Manual and automatic assignment of settings**" on page 198, section "**Creating and managing settings**" on page 197 and section "**Advanced protection**" on page 226.
Computer offline for N days	The computer is turned off or doesn't meet the network access requirements.	Refer to "**Network requirements**" on page 96.
Protection out-of-date	The protection requires the local user to manually restart the computer to complete the installation*.	Only on computers running the Home and Starter versions of Windows.
Connection problems with the Panda servers	The computer cannot successfully connect to the servers that store the security intelligence.	Refer to "**Network requirements**" on page 96.
The administrator has changed the protection status from the computer's local console	The administrator has changed the protection settings from the agent installed on the workstation or server. Consequently, the current settings do not match the settings defined from the Web console.	

Table 9.24: Alerts related to lack of user or administrator action

Computer with out-of-date protection

Alert	Description	Reference
Protection out-of-date	A reboot is required to complete the protection update process.	Refer to "**Computer restart**" on page 500.

Table 9.25: Alerts related to out-of-date Panda Adaptive Defense software

Alert	Description	Reference
	An error occurred while attempting to update the protection. Make sure the computer meets the hardware and network requirements.	Refer to "**Installation requirements**" on page 94 and the section on available hard disk space in "**Hardware section (5)**" on page 184
	Updates are disabled for the computer. Assign the computer a settings profile with updates enabled.	Refer to "**Protection engine updates**" on page 136
Malware and threat knowledge out-of-date	Knowledge updates are disabled for this computer. Assign the computer a settings profile with updates enabled.	Refer to "**Knowledge updates**" on page 138.

Table 9.25: Alerts related to out-of-date Panda Adaptive Defense software

Details section (3)

The information on this tab is divided into three sections: **Computer**, **Security** and **Data Protection**.

- **Computer**: information about the device settings. This information is provided by the Panda agent.
- **Security**: status of the Panda Adaptive Defense protection modules.
- **Data Protection**: status of the modules responsible for protecting the content of the data stored on computers.

Computer

Field	Description
Name	Computer name.
Description	Descriptive text provided by the administrator.
Physical addresses (MAC)	Physical addresses of the network interface cards installed.
IP addresses	List of all the IP addresses (primary addresses and aliases).
Domain	Windows domain the computer belongs to. This is empty if the computer does not belong to a domain.
Active Directory path	Path to the computer in the company's Active Directory.
Group	Group in the group tree to which the computer belongs. To change the computer's group, click **Change**.
Operating system	Operating system installed on the computer.
Virtual machine	Indicates whether the computer is physical or virtual.

Table 9.26: Fields in the Details tab's Computer section

Field	Description
Is a non-persistent desktop	Indicates if the operating system of the virtual machine resides on a storage device that persists between restarts, or reverts to its original state instead.
Licenses	Panda Security product licenses installed on the computer. Refer to "Licenses" on page 123 for more information.
Agent version	Internal version of the Panda agent installed on the computer.
Last bootup date	Date when the computer was last booted.
Installation date	Date when the computer's operating system was last installed.
Last proxy used	Access method used by Panda Adaptive Defense the last time it connected to Panda Security's cloud. This data is not updated immediately, so it might take up to 1 hour for the correct value to show.
Last connection	Date when the client software last connected to the Panda Security cloud. The communications agent connects at least every four hours.
Last settings check	Date Panda Adaptive Defense last connected to Panda Security's cloud checking for changes to the settings.
Last logged-in user	Names of the user accounts that are currently logged in to the console on the computer.

Table 9.26: Fields in the Details tab's Computer section

Security

This section indicates the status (Enabled, Disabled, Error) of the Panda Adaptive Defense technologies that protect the computer against malware.

Field	Description
Advanced protection	Protection against advanced threats, APTs and exploits.
Patch management	Installation of patches and updates for Windows operating systems and third-party applications. Detection of the patch status of the computers on the network and removal of problematic patches.
Program blocking	Blocking of the running of programs considered dangerous or not compatible with the organization's activity by the administrator.
Last check date	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.
Protection version	Internal version of the protection module installed on the computer.
Knowledge update date	Date when the signature file was last downloaded to the computer.

Table 9.27: Fields in the Details tab's Security section

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

Table 9.27: Fields in the Details tab's Security section

Data Protection

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

Field	Description
Personal data monitoring	Monitors files containing data that could identify users or company customers (Panda Data Control module).
Allow data searches on this computer	Indicates if the computer has a settings profile assigned that allows it to receive searches for files and report their results.
Personal data inventory	Provided that content-based searches of files are allowed, Panda Data Control will parse all files contained in the supported storage media to retrieve their content and generate a database.
Indexing status	• Not indexed • Indexed • Indexed (text only) • Indexed (all content) • Indexing
Hard disk encryption	Encryption module status: • **Not available**: the computer is not compatible with Panda Full Encryption. • **No information**: the computer has not yet sent any information about the encryption module. • **Enabled**: the computer has a settings profile assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: the computer has a settings profile assigned to decrypt its storage devices and no errors have occurred. • **Error**: the settings configured by the administrator don't allow an authentication method supported by Panda Full Encryption to be applied on the operating system version installed on the computer. • **Error installing**: error downloading or installing the necessary executables to manage the encryption service if they were not already installed on the computer. • **No license**: the computer doesn't have a Panda Full Encryption license assigned. **Get recovery key**: opens a window showing the IDs of the computer's encrypted storage media. Click any of them to display the relevant recovery key. Refer to "Getting the recovery key" on page 340.

Table 9.28: Fields in the Data protection section

Field	Description
	Encryption process status: • **Unknown**: there are drives whose status is unknown. • **Unencrypted disks**: some of the drives compatible with the encryption technology are neither encrypted nor in the process of being encrypted. • **Encrypted disks**: all drives compatible with the encryption technology are encrypted. • **Encrypting**: at least one of the computer drives is being encrypted. • **Decrypting**: at least one of the computer drives is being decrypted. • **Encrypted by the user**: all storage media are encrypted by the user. • **Encrypted by the user (partially)**: some storage media are encrypted by the user.
Authentication method	• **Unknown**: the authentication method is not compatible with those supported by Panda Full Encryption. • **Security processor (TPM)** • **Security processor (TPM) + Password** • **Password**: authentication method based on a PIN, extended PIN or passphrase. • **USB**: authentication method based on a USB drive. • **Not encrypted**: none of the drives compatible with the encryption technology is encrypted or in the process of being encrypted.
Encryption date	Date when the computer was fully encrypted for the first time.
Removable storage drive encryption	Encryption module status: • **Not available:** the computer is not compatible with Panda Full Encryption. • **No information**: the computer has not yet sent any information about the encryption module. • **Enabled**: the computer has settings assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: the computer has settings assigned to decrypt its storage devices and no errors have occurred.

Table 9.28: Fields in the Data protection section

Field	Description
	• **Error**: the settings configured by the administrator don't allow an authentication method supported by Panda Full Encryption to be applied on the operating system version installed on the computer. • **Install error**: error downloading or installing the executables required to manage the encryption service if they were not already installed on the computer. • **No license**: the computer doesn't have a Panda Full Encryption license assigned. **View encrypted devices on this computer:** opens a window showing the IDs of the computer's encrypted external storage media. Click any of them to display the relevant recovery key. Refer to "Getting the recovery key" on page 340.

Table 9.28: Fields in the Data protection section

Detections section (4)

Shows counters associated with the computer's security and patch level through the following widgets:

Panel	Description
Malware activity	Refer to "Malware/PUP activity" on page 408.
Currently blocked programs being classified	Refer to "'Currently blocked programs being classified' panel" on page 433.
Programs blocked by the administrator	Refer to "Programs blocked by the administrator" on page 357.
PUP activity	Refer to "Malware/PUP activity" on page 408.
Exploit activity	Refer to "Exploit activity" on page 410.
Available patches	Refer to "Available patches" on page 304.
End-of-Life programs	Refer to "End-of-Life programs" on page 302.
Detected indicators of attack (IOA)	Refer to "Detected indicators of attack (IOA)" on page 396.
Evolution of detections	Refer to "Evolution of detections" on page 393.

Table 9.29: List of widgets available in the Detections section

Hardware section (5)

This section contains information about the hardware resources installed on the computer:

Field	Description	Values
CPU	Information about the computer's microprocessor, along with a line chart showing CPU consumption at different time intervals based on your selection.	• 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Memory	Information about the memory chips installed, along with a line chart with memory consumption at different time intervals based on your selection.	• 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Disk	Information about the mass storage system, along with a pie chart with the current percentage of free/used space.	• Device ID • Size • Type • Partitions • Firmware revision • Serial number • Name
BIOS	Information about the BIOS installed on the computer.	• Version • Manufacture date • Serial number • Name • Manufacturer
TPM	Information about the security chip located on the computer's motherboard. To be used by Panda Adaptive Defense, the TPM must be enabled, activated and owned.	• **Manufacturer version**: internal version of the chip. • **Spec version**: supported API versions. • **Version** • **Manufacturer** • **Activated**: the TPM is ready to receive commands. This is used on systems with multiple TPMs. • **Enabled**: the TPM is ready to work as it has been enabled in the BIOS. • **Owner**: the operating system can interact with the TPM.

Table 9.30: Fields in the computer details' Hardware section

Software section (6)

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

Search tool

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

Field	Description
Name	Name of the installed program.
Publisher	The program's developer.
Installation date	Date when the program was last installed.
Size	Program size.
Version	Internal version of the program.

Table 9.31: Fields in the computer details' Software section

- To narrow your search, select the type of software you want to find from the drop-down menu:
  - Programs only
  - Updates only
  - All software

Installations and uninstallations

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

Field	Description
Event	• 🗑 Software uninstallation. • 💾 Software installation.
Name	Name of the installed program.
Publisher	Company that developed the program.
Date	Date the program was installed or uninstalled.
Version	Internal version of the program.

Table 9.32: Fields in the Installations and uninstallations section

Settings section (7)

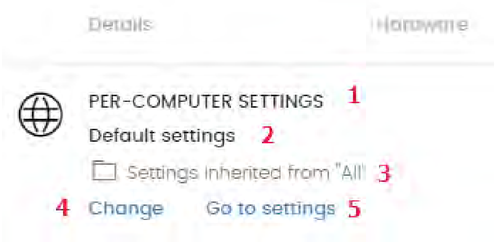


Figure 9.8: Managing and editing the assigned settings

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

- **(1) Settings type**: indicates the type of settings assigned to the computer. Refer to "Introduction to the various types of settings" on page 191 for information about the different types of settings available in Panda Adaptive Defense.
- **(2) Settings name**.
- **(3) Method used to assign the settings**: directly assigned to the computer or inherited from a parent group.
- **(4) Button to change the settings profile assigned to the computer.**
- **(5) Button to edit the settings profile options**.

Refer to "Managing settings" on page 189 for more information on how to create and edit settings profiles.

Action bar (8)

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

Action	Description
Move to	Moves the computer to a standard group.
Move to Active Directory path	Moves the computer to its original Active Directory group.
Delete	Releases the Panda Adaptive Defense license and deletes the computer from the Web console.
Disinfect	Lets you run a disinfection task immediately.
Isolate computer	Prevents the computer from establishing external communications in order to help administrators perform forensic analysis tasks on compromised computers. For more information, refer to "Isolating one or more computers from the organization's network" on page 502
Stop isolating the computer	Restores communications with other computers. Refer to "Stopping a computer from being isolated" on page 503 for more information.
Schedule patch installation	Creates a task that installs all released patches missing from the target computer. See section "Download and install the patches" on page 289 for more information

Table 9.33: Actions available from the computer details window

Action	Description
Restart	Restarts the computer immediately. Refer to "**Computer restart**" on page **500** for more information.
Reinstall protection (requires restart)	Reinstalls the protection if a malfunction occurs. Refer to "**Remote reinstallation**" on page **120** for more information.
Report a problem	Opens a support ticket for Panda Security's support department. Refer to "**Reporting a problem**" on page **505** for more information.

Table 9.33: Actions available from the computer details window

Hidden icons (9)

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

Chapter 10

Managing settings

Settings, also called “settings profiles” or simply “profiles”, offer administrators a simple way of establishing security and connectivity parameters for the computers managed through Panda Adaptive Defense.

CHAPTER CONTENT

Strategies for creating settings profiles

Administrators can create as many profiles and variations of settings as they deem necessary to manage network security. A new settings profile should be created for each group of computers with similar protection needs.

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

Overview of assigning settings to computers

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

1. Creation of groups of similar computers or computers with identical connectivity and security requirements.
2. Assigning computers to the corresponding group.
3. Assigning settings to groups.
4. Deployment of settings to network computers.

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

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

*For more information on the group tree and how to assign computers to groups, refer to "***The Computer tree panel***" on page* **145**

Immediate deployment of settings

Once a settings profile is assigned to a group, it will be applied to the computers in the group immediately and automatically, in accordance with the inheritance rules described in section "Indirect assignment of settings: the two rules of inheritance". Settings are applied to computers in just a few seconds.

For more information on how to disable the immediate deployment of settings, refer to "Configuring real-time communication" on page 215

Multi-level tree

In medium-sized and large organizations, there could be a wide range of settings. To facilitate the management of large networks, Panda Adaptive Defense lets you create group trees with various levels so that you can manage all computers on the network with sufficient flexibility.

Inheritance

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

Manual settings

To prevent settings from being applied to all inferior levels in the group tree, or to assign settings different from the inherited ones to a certain computer on a branch of the tree, it is possible to manually assign settings to groups or individual computers.

Default settings

Initially, all computers in the group tree inherit the settings established in the **All** root node. This node comes with a series of default settings created in Panda Adaptive Defense with the purpose of protecting all computers from the outset, even before the administrator accesses the console to establish a security setting profile.

Introduction to the various types of settings

Panda Adaptive Defense separates the settings to apply to managed computers into different types of profiles, each of which covers a specific aspect of security.

Below we provide you with an introduction to the different types of settings supported by Panda Adaptive Defense:

Configuration	Description
Users	Manage the user accounts that will be able to access the management console, the actions they can take (roles) and their activity. Refer to "**Controlling and monitoring the management console**" on page 63 for more information.
Per-computer settings	Configure settings templates to define the update frequency of the Panda Adaptive Defense security software installed on workstations and servers. This section also lets you define global settings to prevent tampering and unauthorized uninstallation of the protection. Refer to "**Configuring the agent remotely**" on page 207 for more information.
Network settings	Configure settings templates to define the language of the Panda Adaptive Defense software installed on workstations and servers, and the connection type used to connect to Panda Security's cloud. Refer to "**Configuring the agent remotely**" on page 207 for more information.
Network services	Define the behavior of the Panda Adaptive Defense software with regard to communication with neighboring computers on the customer's network. • **Proxy:** globally define the computers that will act as a proxy server to allow isolated computers with Panda Adaptive Defense installed to access the cloud. Refer to "**Proxy role**" on page 208 for more information. • **Cache**: globally define the computers that will act as repositories of signature files, security patches and other components used to update the Panda Adaptive Defense software installed across the network. Refer to "**Cache/repository role**" on page 209 for more information. • **Discovery**: globally define the computers responsible for discovering unprotected computers on the network. Refer to "**Discovery computer role**" on page 211 for more information.
VDI environments	Define the largest number of computers that can be simultaneously active in a non-persistent virtualization environment to facilitate license assignment.
My alerts	configure the alerts to be sent to the administrator's mailbox. Refer to "**Alerts**" on page 477 for more information.
Workstations and servers	Configure settings templates to define how Panda Adaptive Defense will behave to protect the computers on your network against threats and malware. Refer to "**Security settings for workstations and servers**" on page 223 for more information.
Indicators of attack (IOA)	Configure templates for detecting sophisticated infection strategies that typically use multiple attack vectors and operating system tools for extended periods of times. Refer to "**Indicators of attack settings**" on page 367.

Table 10.1: Description of the types of settings available in Panda Adaptive Defense

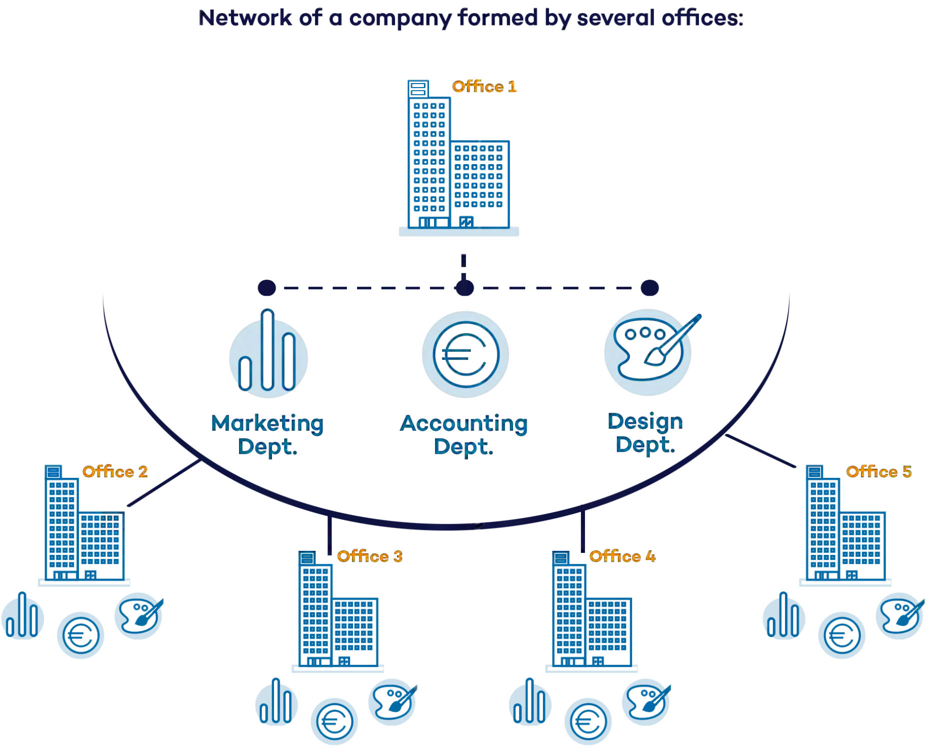
Configuration	Description
Program blocking	Configure settings templates to define how Panda Adaptive Defense will behave to prevent the execution of certain programs. Refer to "**Program blocking settings**" on page **355** for more information.
Authorized software	Lets you configure templates for preventing unknown programs in the process of classification from being blocked. Refer to "**Authorized software settings**" on page **361**.
Patch management	Configure settings templates to define the discovery of the new security patches published by vendors for the Windows operating systems and third-party software installed across the network. Refer to "**Panda Patch Management (Updating vulnerable programs)**" on page **285** for more information.
Data Control	Configure settings templates to define how Panda Adaptive Defense will monitor the personal data stored on your network's storage systems. Refer to "**Panda Data Control (Personal data monitoring)**" on page **231** for more information.
Encryption	Configure settings templates to encrypt the content of your computers' internal storage devices. Refer to "**Panda Full Encryption (Device encryption)**" on page **329** for more information.

Table 10.1: Description of the types of settings available in Panda Adaptive Defense

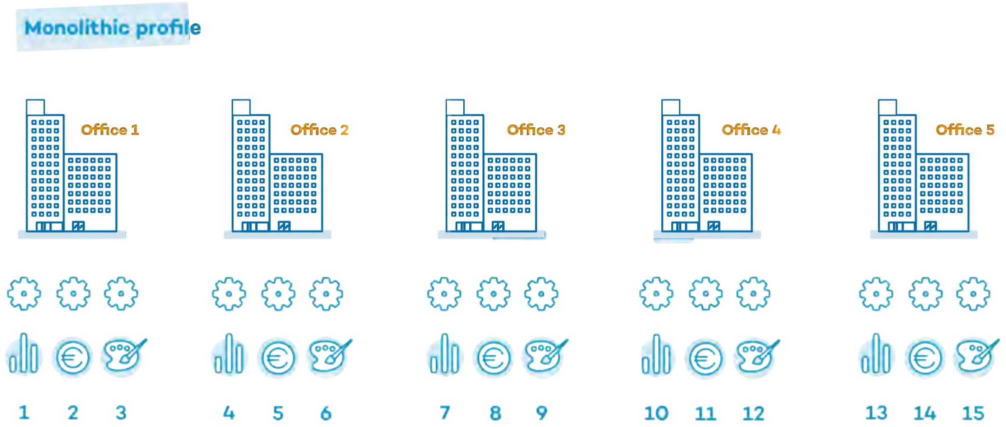
Modular vs monolithic settings profiles

By supporting different types of profiles, Panda Adaptive Defense uses a modular approach for creating and deploying the settings to apply to managed computers. The reason for using this modular approach and not just a single, monolithic profile that covers all the settings is to reduce the number of profiles created in the management console. This in turn will reduce the time that administrators have to spend managing the profiles created. The modular approach means that the settings are lighter than monolithic profiles, which result in numerous large and redundant settings profiles with little differences between each other.

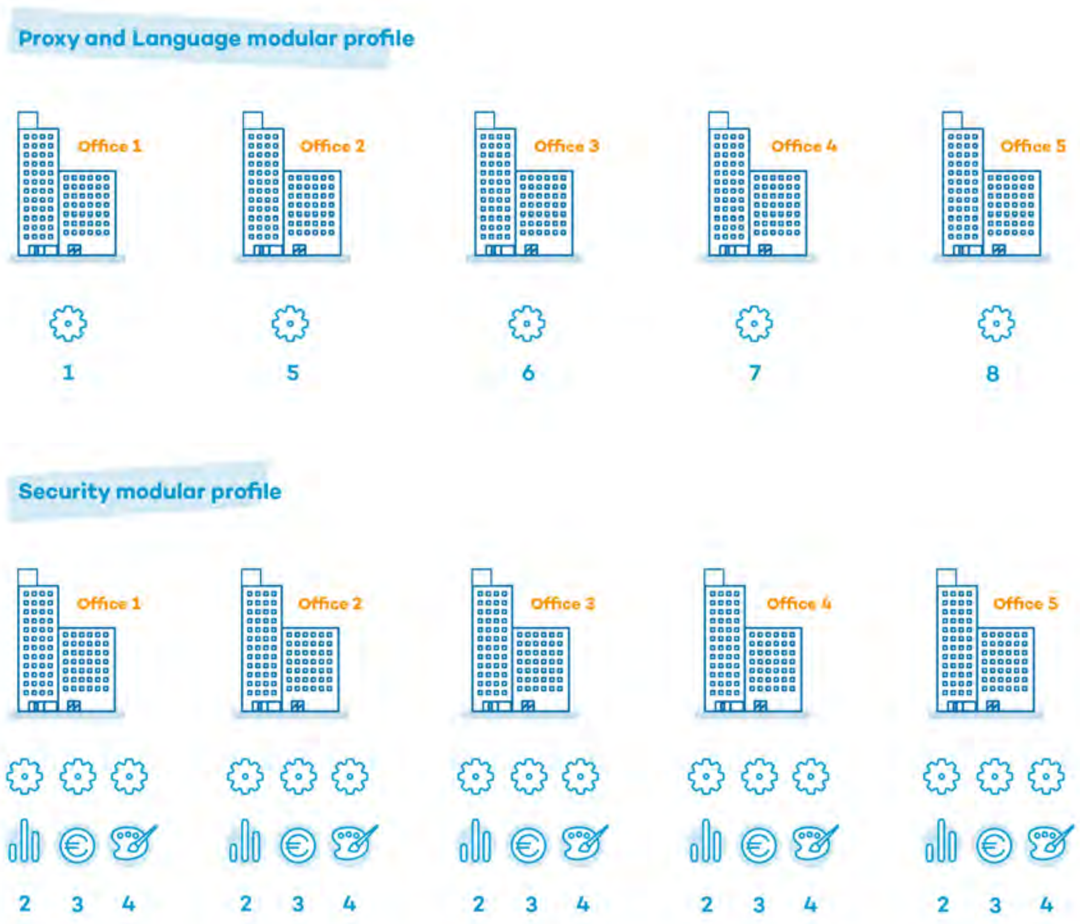
Case study: creating settings for several offices



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



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



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

Settings management, permissions, and visibility

Permissions to manage settings

To manage settings, the user account that accesses the management console must have the permission associated with the type of settings to manage assigned to it. For more information about a specific permission, refer to "**Understanding permissions**" on page 68.

Settings	Permissions
Users	• Manage users and roles.
Per-computer settings	• Configure per-computer settings (updates, passwords, etc.).

Table 10.2: Permissions related to each type of settings template

Settings	Permissions
Network settings	• Modify network settings (proxies and cache).
Network services	• **Panda proxy tab**: to view the list of computers with the Panda proxy role assigned to them, no specific permission is required. To modify the computer list, the Modify network settings (proxies and cache) permission is required. • **Discovery tab**: to view the list of computers with the discovery computer role assigned to them, the Add, discover, and delete computers permission is required. To modify the computer list, the Modify network settings (proxies and cache) permission is required. • **Cache tab**: to view the list of computers with the cache role assigned to them, no specific permission is required. To modify the computer list, the Modify network settings (proxies and cache) and Add, discover, and delete computers permissions are required.
DVI environments	• To view these settings, no specific permission is required. • To modify the settings, the Add, discover, and delete computers permission is required.
My alerts	• The required permissions are related to the type of alert to be sent. Refer to "Alerts" on page 477.
Workstations and servers	• Configure security for workstations and servers. • View security settings for workstations and servers.
Indicators of attack (IOA)	• Configure indicators of attack (IOA). • View indicators of attack (IOA) settings.
Program blocking	• Configure program blocking. • View program blocking settings.
Authorized software	• Configure authorized software. • View authorized software settings.
Patch management	• Configure patch management. • View patch management settings.
Data Control	• Configure Data Control. • View Data Control settings.
Encryption	• Configure computer encryption. • View computer encryption settings.

Table 10.2: Permissions related to each type of settings template

Computer visibility

To modify the recipients of a settings profile, the user account that modifies the settings template must have visibility into the computers to add. That is, a user account cannot add or delete computers in a settings profile if those computes are not visible to it.

Additionally, a user account can only modify an existing settings profile created by another user account if it has the right permissions for that action. The management console does not take into account the visibility of the account that modifies the settings: the changes made will be pushed to all the computers originally assigned to the settings, even if these settings were created by a user account with greater visibility than the account that modifies them.

Creating and managing settings

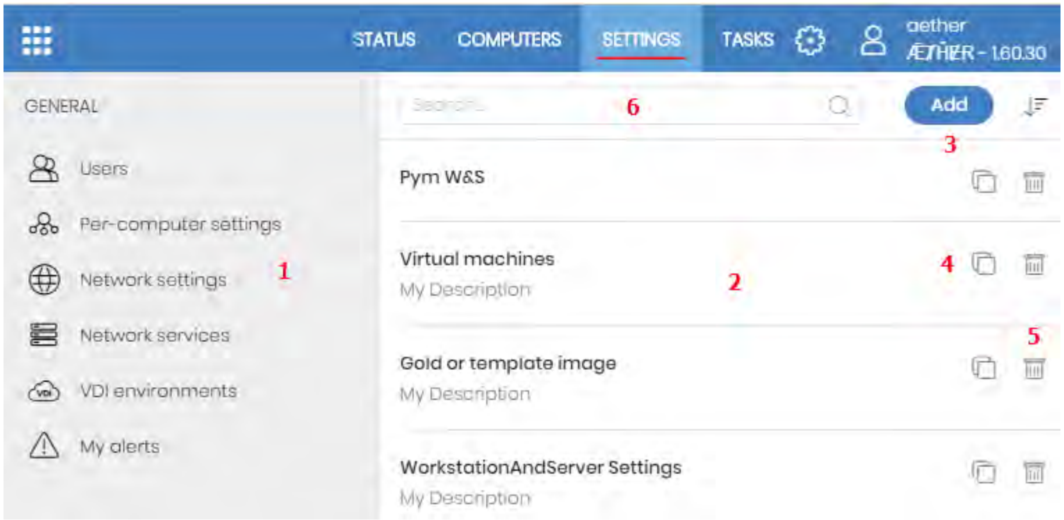


Figure 10.1: Screen for creating and managing settings profiles

Click Settings in the menu bar at the top of the screen to create, copy and delete settings. The panel on the left contains different sections corresponding to the various types of available settings profiles (1). In the right-hand panel, you can see the profiles of the selected category that have already been created (2), and the buttons for adding (3), copying (4) and deleting profiles (5). Use the search bar (6) to quickly find existing profiles.

The settings created from Panda Partner Center display the green tag Panda Partner Center. Placing the mouse pointer on the tag displays the following message: "These settings are managed from Panda Partner Center.

The settings created from Panda Partner Center are read only and only enable you to change their recipients. For more information, refer to Settings management for Panda-based products of the Panda Partner Center guide.

Creating settings

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

Sorting settings

Click the ↓☰ icon **(7)** to display a context menu with all available sort options:

- Sorted by creation date
- Sorted by name
- Ascending/Descending

Copying, deleting and editing settings

- Use the icons **(4)** and **(5)** to copy and delete a settings profile, although if it has been assigned to one or more computers, you won't be able to delete it until it has been freed up.
- Click a settings profile to edit it.

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

Manual and automatic assignment of settings

Once you have created a settings profile, it can be assigned to computers in two different ways:

- Manually (directly).
- Automatically through inheritance (indirectly).

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

Manual/direct assignment of settings

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

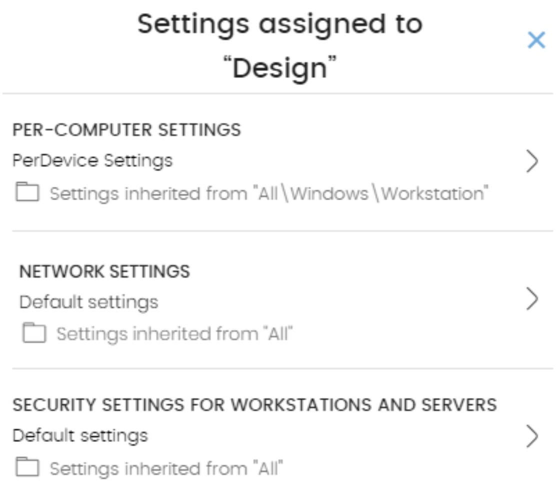
Once a settings profile has been created, there are three ways of assigning it:

- From the **Computers** menu at the top of the console (group three in the left-hand menu).
- From the target computer's details (accessible from the **Computers** list panel).
- From the profile itself when it is created or edited.

> *For more information about the group tree, refer to "Group tree" on page 152.*

From the group tree

Follow these steps to assign a settings profile to the computers in a group:



Settings assigned to "Design"

PER-COMPUTER SETTINGS
PerDevice Settings
Settings inherited from "All\Windows\Workstation"

NETWORK SETTINGS
Default settings
Settings inherited from "All"

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

Figure 10.2: Example of inherited and manually assigned settings

- Click the **Computers** menu at the top of the console, and select a group from the group tree in the left-hand menu.
- Click the group's context menu.
- Click **Settings**. A window will open with the profiles already assigned to the selected group and the type of assignment:
  - **Manual/Direct assignment**: the text **Directly assigned to this group** will be displayed.
  - **Inherited/Indirect assignment**: the text **Settings inherited from** will be displayed, followed by the name and full path of the group the settings were inherited from.
- Select a category of settings and then select the specific settings to apply. They will be deployed immediately to all members of the group and its sub-groups.

From the Computers list panel

Follow these steps to assign a settings profile to a specific computer:

- Go to the **Computers** menu at the top of the console, and click the group or filter that contains the computer to which you want to assign the settings. Click the computer in the list of computers in the right-hand panel to see its details.
- Click the **Settings** tab. This will display the various types of profiles assigned to the computer and the type of assignment:
  - **Manual/Direct assignment**: the text **Directly assigned to this group** will be displayed.
  - **Inherited/Indirect assignment**: the text **Settings inherited from** will be displayed, followed by the name and full path of the group the settings were inherited from.
- Select a category of settings and then select the specific settings to apply. They will be applied immediately to the computer.

From the settings profile itself

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

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

- Go to the **Settings** menu at the top of the console and select the type of settings that you want to assign from the left-hand side menu.

- Select a specific settings profile from those available, and click **Recipients**. A window will be displayed divided into two sections: **Computer groups** and **Additional computers.**
- Click the ⊕ buttons to add individual computers or computer groups to the settings profile.
- Click **Back**. The profile will be assigned to the selected computers and the new settings will be applied immediately.

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

Indirect assignment of settings: the two rules of inheritance

Indirect assignment of settings takes place through inheritance, which allows automatic deployment of a settings profile to all computers below the node to which the settings were initially assigned.

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

- **Automatic inheritance rule**

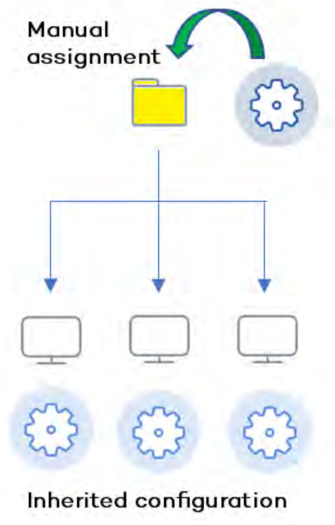


Figure 10.3: Inheritance/indirect assignment

A single compute or computer group automatically inherits the settings of the parent group (the group above it in the hierarchy).

The settings are manually assigned to the parent group, and automatically deployed to all child items (computers and computer groups with computers inside).

- **Manual priority rule**

Manually assigned profiles have priority over inherited ones.

By default, computers receive the settings inherited from a parent node. However, if at some point, you manually assign a new settings profile to a computer or computer group, all items below said computer or group will receive and apply the manually assigned settings and not the original inherited ones.

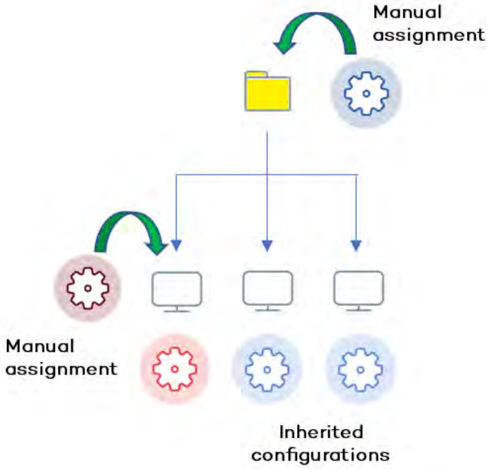


Figure 10.4: Priority of manually assigned settings over inherited ones

Inheritance limits

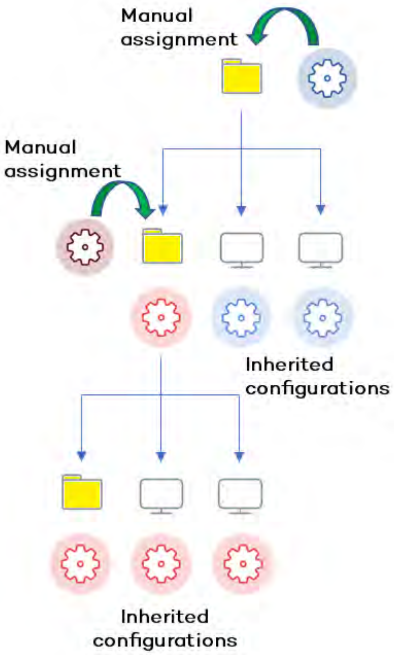


Figure 10.5: Inheritance limits

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

This node and all of its child nodes will receive the manually assigned settings and not the original inherited ones.

Overwriting settings

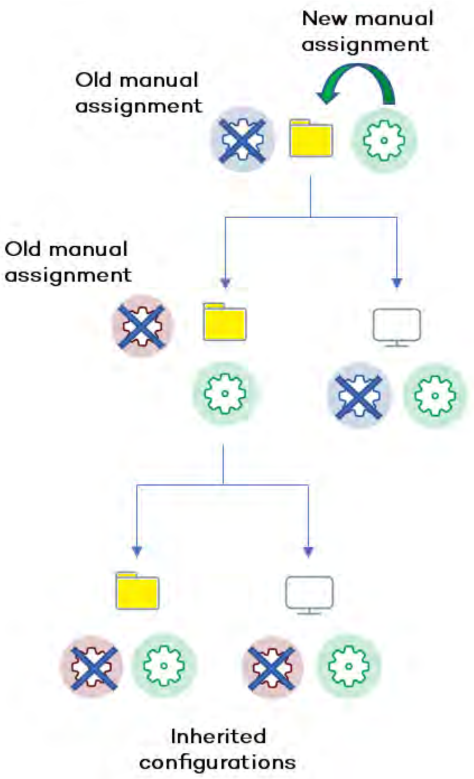


Figure 10.6: Overwriting manual settings

As illustrated in the previous point, the manual priority rule dictates that manually applied settings have preference over inherited ones.

Bearing that in mind, any change made to the settings in a higher-level node will affect the nodes below it in the following two ways:

- **If the child nodes don't have manual settings assigned**: the new settings assigned to the parent node will be applied to all its child nodes.
- **If any of the child nodes already have manual settings assigned**: the parent node will try to automatically apply the new settings it has received to all its child nodes. However, and based on the inheritance rules, those settings won't be applied to any child nodes that already have manual settings.

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

Make all inherit these settings

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

The new settings will be inherited by all nodes in the tree, overwriting any previous manual settings all the way down to the lowest level child nodes.

Keep all settings

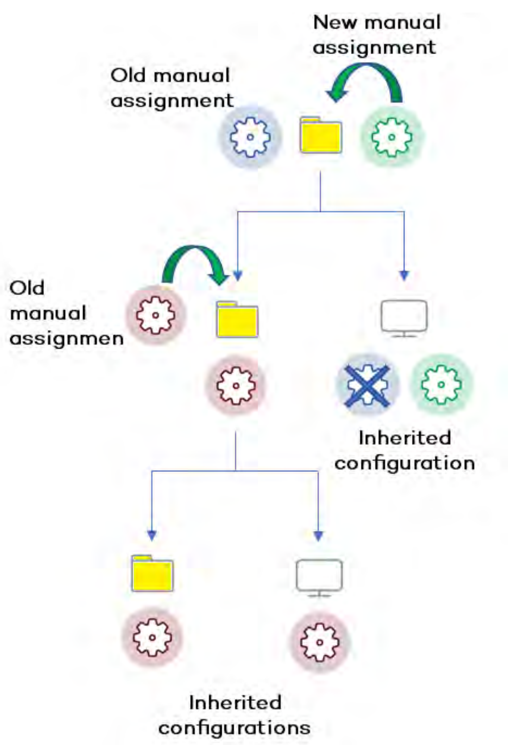


Figure 10.7: Keeping manual settings

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

That is, if you choose to keep the existing manual settings, the propagation of the new inherited settings will stop at the first manually configured node. .

- **Deleting manually assigned settings and restoring inheritance**

Follow these steps to delete a manually assigned profile from a folder, and restore the settings inherited from a parent node:

- Go to the **Computers** menu at the top of the console. From the group tree in the panel on the left, click the group with the manually assigned settings that you want to delete.
- Click the branch's context menu icon and select **Settings**. A pop-up window will appear with the profiles assigned. Select the manually assigned profile you want to delete.
- At the bottom of the list you will see the button **Inherit from parent group** along with the settings that will be inherited if you click it, and the group from which they will be inherited.

Moving groups and computers

When moving computers from one branch in the tree to another, the way Panda Adaptive Defense operates with respect to the settings to apply will vary depending on whether the items moved are groups or individual computers.

Moving individual computers

If you move a single computer that has manual settings assigned, those settings will be kept in the new location. However, if the computer to move has inherited settings, they will be overwritten with the settings established in the new parent group.

Moving groups

If you move a group, Panda Adaptive Defense will display a window asking the following question: "**Do you want the settings inherited by this group to be replaced by those in the new parent group?**"

- If you answer **YES**, the process will be the same as with moving a single computer: the manual settings will be kept and the inherited settings overwritten with those established in the parent node.

- If the answer is **NO**, the manual settings will also be kept but the original inherited settings of the moved group will have priority and as such will become manual settings.

Exceptions to indirect inheritance

All computers that are integrated into a native group in the Web console receive from Panda Adaptive Defense the network settings assigned to the target group using the standard indirect assignment/inheritance mechanism. However, if a computer is integrated into an Active Directory or IP-based group in the Web console, the network settings must be manually assigned. This change in the way network settings are assigned will in turn result in a change in behavior when that computer is subsequently moved from one group to another: it will no longer indirectly inherit the network settings assigned to the target group, but will retain its own.

This particular behavior of the inheritance feature is due to the fact that, in mid-size and large companies, the department that manages security may not be the same as the one that manages the company's Active Directory. For this reason, a group membership change made by the technical department that maintains the Active Directory can inadvertently lead to a change of network settings within the Panda Adaptive Defense console. This situation could leave the protection agent installed on the affected computer without connectivity and therefore with less protection. By manually assigning network settings, you prevent settings changes when a computer changes groups in the Panda Adaptive Defense console due to a group change in the company's Active Directory.

Viewing assigned settings

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

- From the group tree.
- From the **Settings** menu at the top of the console.
- From the computer's **Settings** tab.
- From the exported list of computers.

Viewing settings from the group tree

- Click the **Computers** menu at the top of the console. Then, click the ▣ tab at the top of the left-side panel in order to display the group tree.
- Click the context menu of the relevant branch, and select **Settings** from the pop-up menu displayed. A window will open with the settings profiles assigned to the folder.

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

- **Settings type**: indicates the settings class the profile belongs to.

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

Viewing settings from the Settings menu at the top of the console

- Go to the **Settings** menu at the top of the console and select a type of settings from the left-hand side menu.
- Select the relevant settings profile from those available.
- If the settings profile has been assigned to one or more computers or groups, a button called **View computers** will be displayed.
- Click the **View computers** button. You will be taken to the **Computers** screen, which will display a list of all computers with those settings assigned, regardless of whether they were assigned individually or through computer groups. At the top of the screen you'll see the filter criteria used to generate the list.

Viewing settings from a computer's Settings tab

Go to the **Computers** menu at the top of the console. Select a computer from the panel on the right and click it to view its details. Go to the **Settings** tab to see the profiles assigned to the computer.

Viewing settings from the exported list of computers

From the computer tree (group tree or filter tree), click the general context menu and select **Export**:

*Refer to "***Fields in the 'Computers list' exported file***" on page* 161.

Chapter 11

Configuring the agent remotely

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

- Define the computer's role towards the other protected workstations and servers.
- Protect the Panda Adaptive Defense client software from unauthorized tampering by hackers and advanced threats (APTs).
- Define the visibility of the agent on the workstation or server, and its language.
- Configure the communication established between the computers on the network and the Panda Security cloud.

CHAPTER CONTENT

Configuring the Panda agent role

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

- Proxy
- Discovery computer
- Cache

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

> *Only computers with a Windows operating system can take on the Proxy, Cache, or Discovery Computer roles.*

Proxy role

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

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

Requirements for configuring a computer as a proxy server

- The computer must be a Windows computer with Panda Adaptive Defense installed.
- Support for the 8.3 file naming format. Refer to the following MSDN article **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN** for information on how to enable this feature.
- TCP port 3128 must not be in use by other applications.
- The computer's firewall must be configured to allow incoming and outgoing traffic on port 3128..
- The name of the computer with the proxy role assigned to it must be resolved from the computer that uses it.

Configuring a computer as a proxy server

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Panda proxy** tab. A list will be displayed showing all computers already configured as a proxy.
- Click **Add Panda proxy**. A window will be displayed with all computers managed by Panda Adaptive Defense that meet the necessary requirements to work as a proxy for the network.
- Use the search box to find a specific computer and click it to add it to the list of computers with the proxy role assigned.

Revoking the proxy role assigned to a computer

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Panda proxy** tab. This will display all computers configured as a proxy.
- Click the 🗑 icon of the computer whose proxy role you want to revoke.

> *To configure the use of a computer with the proxy role assigned, refer to “***Configuring proxy-based Internet access lists***”.*

Cache/repository role

Panda Adaptive Defense lets you assign the cache role to one or more computers on your network. These computers will automatically download and store all files required by other computers with Panda Adaptive Defense installed. This saves bandwidth as it won’t be necessary for each computer to separately download the updates they need. All updates will be downloaded centrally and once for all computers that require them.

Cached items

A computer with the cache role assigned can cache the following items for different time periods based on their type:

- **Signature files**: until they are no longer valid.
- **Installation packages**: until they are no longer valid.
- **Update patches for Panda Patch Management**: 30 days.

> ⚠ *For a computer to be able to download patches from another computer with the cache role assigned to it, both computers must belong to the same subnet. Due to this, the cache computer must be assigned automatically. Refer to “***Configuring downloads via cache computers***”.*

Cache node capacity

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

Configuring a computer as a cache

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

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

Revoking the cache role

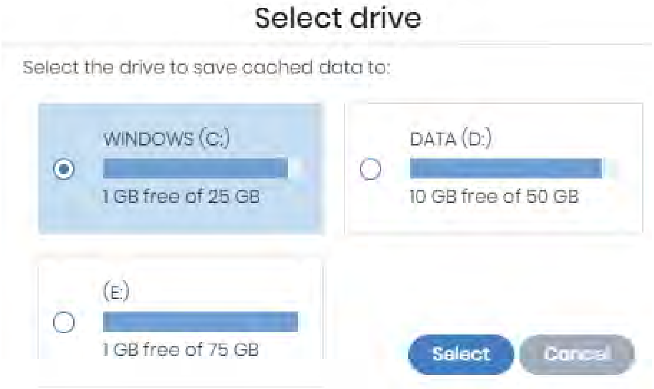
- Click the **Settings** menu at the top of the console. Then, click **Network services** from the side menu and click the **Cache** tab.
- Click the 🗑 icon of the computer that you want to stop acting as a cache.

Setting the storage drive

You can configure the Panda Adaptive Defense agent to store cached items on a specific volume/ drive of the cache computer. Please note that the folder path on the drive will be fixed. Follow these steps to configure this option:

- Click the **Settings** menu at the top of the console. Then, click **Network services** from the menu on the left and click the **Cache** tab.
- From a computer with the cache role assigned and which has already reported its status to the cloud, click the **Change** link. A window will appear with all available drives.
- The following information is displayed for each drive: volume name, mapped drive, free space, and

total space.



Select drive

Select the drive to save cached data to:

- ● WINDOWS (C:) 1 GB free of 25 GB
- ○ DATA (D:) 10 GB free of 50 GB
- ○ (E:) 1 GB free of 75 GB

Figure 11.1: Volume selection window for a computer with the cache role assigned

- To view the percentages of used and free space, hover the mouse pointer over the bars. A tooltip with the relevant information will be displayed.
- Only drives with 1 GB or more of free space will be available for selection. Select the drive where you want to store the cached items and click the **Select** button. Panda Adaptive Defense will start copying the cached items. Once the process is complete, they will be deleted from their original location.

You can only select the drive where you want to store the cached items on computers which have reported their status to the Panda Adaptive Defense server. If this condition is not met, the drive that stores the Panda Adaptive Defense installation files will be selected by default. Once the status has been reported, the ***Change*** *link for the computer with the cache role assigned will be displayed, and you will be able to select the storage drive. It may take several minutes for a computer to report its status.*

If there is not enough free space or a write error occurs when selecting the storage drive, a message will be displayed under the computer with the cache role assigned indicating the source of the problem.

Discovery computer role

Click the **Settings** menu at the top of the console and then **Network services** from the menu on the left. You'll find the **Discovery** tab, which is directly related to the installation and deployment of Panda Adaptive Defense across the customer's network.

*Refer to "***Computer discovery***" on page 102 for more information about the Panda Adaptive Defense discovery and installation processes.*

Configuring proxy-based Internet access lists

Panda Adaptive Defense lets you assign computers on the network one or more Internet connection methods, based on the resources available in the company's IT infrastructure.

Panda Adaptive Defense supports various Internet access methods which can be configured by the administrator and which it turns to when it needs to connect to Panda Security's cloud. Once selected, the access method won't change until it is no longer accessible, when Panda Adaptive Defense will move to the next method in the list until it finds one that is valid. Once it gets to the end of the list, it will go back to the beginning until all connection methods have been tried at least once.

The connection types supported by Panda Adaptive Defense are as follows:

Proxy type	Description
Do not use proxy	Direct access to the Internet. Computers access the Panda Security cloud directly to download updates and send status reports. If you select this option, the Panda Adaptive Defense software will communicate with the Internet using the computer settings.
Corporate proxy	Access to the Internet via a proxy installed on the company's network. • **Address:** the proxy server's IP address. • **Port:** the proxy server's port. • **The proxy requires authentication**: select this option if the proxy requires a user name and password. • **User name**: the user name of an existing proxy account. • **Password**: the password of the proxy account.
Automatic proxy discovery using Web Proxy Autodiscovery Protocol (WPAD)	Queries the network via DNS or DHCP to get the discovery URL that points to the PAC configuration file. Alternatively, you can directly specify the HTTP or HTTPS resource that hosts the PAC configuration file.
Panda Adaptive Defense proxy	Access via the Panda Adaptive Defense agent installed on a computer on the network. This option lets you centralize all network communications through a computer with the Panda agent installed. To configure a computer to access the Internet via a Panda Adaptive Defense proxy, click the **Select** computer link. A window will open with a list of all available computers on the network with the proxy role. Select one of the computers and click the Add button.

Table 11.1: Types of Internet access methods supported by Panda Adaptive Defense

*You can configure an access list consisting of multiple computers with the proxy role. To do that, first assign the Panda Adaptive Defense proxy role to one or more computers on the network with Panda Adaptive Defense installed, using the steps described in section "*Configuring a computer as a proxy server*".*

Configuring an access list

To configure an access list, create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the Add button or select an existing settings profile in order to edit it.
- In the Proxy section, click the ⊕ icon. A window will be displayed, listing all available connection types.
- Select one of the connection types (table 11.1) and click the **OK** button. The connection type will be added to the list.
- To modify the order of the connection methods, select an item by clicking its checkbox and use the ↑ and ↓ arrows to move the item up and down in the list.
- To delete a connection method, click the 🗑 icon.
- To change a connection method, select it by clicking its checkbox and click the ✎ icon A window will be displayed prompting you to select a new method.

Fallback mechanism

- **Direct connection**: Panda Adaptive Defense tries to connect directly to the Panda Security cloud, if this option was not previously configured in the access list.
- **Internet Explorer**: Panda Adaptive Defense tries to retrieve the computer's Internet Explorer proxy settings with the profile of the user currently logged in to the computer.
  - If the proxy requires explicit credentials, this method cannot be used.
  - If Internet Explorer is configured to use a PAC (Proxy Auto-Config) file, the Panda agent will use the URL in the configuration file, provided the resource access protocol is HTTP or HTTPS.
- **WinHTTP**: Panda Adaptive Defense reads the default proxy settings.
- **WPAD**: the solution queries the network via DNS or DHCP to retrieve the discovery URL that points to the PAC configuration file, if this option was not previously configured in the access list.

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

Configuring downloads via cache computers

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

- **Automatic mode**: the computer that starts the download will use the cache computers found on the network that meet the requirements specified in section "Requirements for using a cache computer in automatic mode". If multiple cache computers are found, downloads will be balanced so as not to overload a single cache computer.

- **Manual mode**: in this mode, it is the administrator who manually sets the cache computer that will be used to download data from Panda Security's cloud. Manually selected cache nodes have the following differences from automatically selected ones:
  - The fact that a computer has multiple cache nodes assigned does not mean that downloads will be shared among them.
  - If the first computer in the list is not available, the solution will move to the next computer until it finds one that works. If it cannot find any available computers, it will try to access the Internet directly.

Requirements for using a cache computer in automatic mode

- The computer with the cache role assigned and the computer that downloads items from it must be on the same subnet. If a cache computer has multiple network cards, it will be able to act as a repository on each network segment to which it is connected.

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

- All other computers will automatically discover the presence of the cache node and will redirect their update requests to it.
- A protection license has to be assigned to the cache node in order for it to operate.
- The firewall must be configured to allow incoming and outgoing UPnP/SSDP traffic on UDP port 21226 and TCP port 18226.

Discovery of cache nodes

As soon as you designate a computer as cache, it will broadcast its status to the network segments to which its interfaces connect. From then on, all workstations and servers set to automatically detect cache nodes will receive that notification and will connect to the cache computer. Should there be more than one designated cache node on a network segment, all computers on the subnet will connect to the most appropriate node based on the amount of free resources it has.

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

Configuring assignment of cache nodes

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and select one of the existing settings profiles.
- Go to the **Cache** section and select one of the following two options:
  - **Automatically use the cache computers seen on the network**: the computers that receive these settings will automatically look for cache nodes on their network segment.

- **Use the following cache computers (in order of preference)**: click the ⊕ icon to add computers with the cache role assigned and set up a list of cache nodes. The computers that receive these settings will connect to the cache nodes specified in the list in order to download files.

Configuring real-time communication

Panda Adaptive Defense communicates with Aether Platform in real time to retrieve the settings configured in the console for protected computers. Therefore, only a few seconds elapse between the time the administrator assigns a settings profile to a computer and the time it is applied.

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

Requirements for real-time communication

- Real-time communications are compatible with all operating systems supported by Aether, except Windows XP and Windows 2003.
- If a computer accesses the Internet via a corporate proxy, the HTTPS connections must not manipulated. Many proxies use Man-in-the-Middle techniques to scan HTTPS connections or work as cache proxies. When that happens, real-time communications won’t work.

Disabling real-time communication

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Add** button or select an existing settings profile to edit it.
- In the **Proxy** section, click **Advanced options** and clear the **Enable real-time communication** checkbox.

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

Configuring the agent language

To set up the language of the Panda agent for one or more computers, you must create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Add** button or select an existing settings profile to edit it.
- Go to the **Language** section and select a language from the list:

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

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

Configuring agent visibility

In those companies where the security service is 100% managed by the IT Department, there is no need for the Panda Adaptive Defense agent icon to be displayed in the notification area of managed computers. Follow the steps below to show or hide the icon:

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Open the **Preferences** section and select or clear the **Show icon in the system tray** option.

Configuring the Anti-Tamper protection and password

Anti-Tamper protection

Many advanced threats make use of techniques for disabling the security software installed on computers. The Anti-Tamper protection prevents unauthorized modification of the way the protection operates, preventing the software from being stopped, paused, or removed, by way of a password.

Panda Adaptive Defense's Anti-Tamper protection works as follows:

- The default **Per-computer settings** provided by the solution include a unique, predefined password for each customer. This password cannot be changed as all default settings are read-only.

- The **Per-computer settings** generated by users allow the Anti-Tamper protection to be enabled or disabled according to the organization's needs.

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

Enabling / disabling the Anti-Tamper protection

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

> *Turning off the* ***Enable Anti-Tamper protection*** *or* ***Request password to uninstall the protection from computers*** *security options will cause a security warning to be displayed when saving the settings. It is not recommend to turn off these security options.*

Password-protection of the agent

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

Setting up the password

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

> *If a computer loses its assigned license, either because it is manually removed or because it expires or is canceled, the Anti-Tamper protection and the password-based uninstallation protection will be disabled.*

Part 5

Managing network security

Chapter 12

Security settings for workstations and servers

All protection features provided by Panda Adaptive Defense can be managed through the security settings for workstations and servers. This section allows administrators to protect corporate assets against computer threats of many different types by assigning security settings profiles to them.

Next is a description of the options available for configuring the security of your workstations and servers. It also includes practical recommendations on how to protect all computers on your network, without negatively impacting users' activities.

For additional information about the 'Workstations and servers' module, refer to:

- "**Creating and managing settings**" on page 197: information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**" on page 63: managing user accounts and assigning permissions.

CHAPTER CONTENT

Accessing the security settings for workstations and servers

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Workstations and servers** from the side menu.
- Click the **Add** button to open the **Workstations and servers** settings window.

Required permissions

Permission	Access type
Configure security for workstations and servers	Create, edit, delete, copy, or assign settings for workstations and servers.
View security settings for workstations and servers	View the 'Workstations and servers' settings.

Table 12.1: Permissions required to access the 'Workstations and servers' settings

Introduction to the security settings

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

Section	Description
General	Lets you configure updates, the removal of competitor products, and file exclusions from scans.
Advanced protection	Lets you configure the behavior of the advanced protection and the anti-exploit protection against APTs, targeted attacks, and advanced malware capable of leveraging exploits.

Table 12.2: Available modules in Panda Adaptive Defense

General settings

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

Local alerts

Field	Description
Show malware, firewall, and device control alerts	Enter a descriptive message to inform users of the reason for the alert. The Panda Adaptive Defense agent will show a pop-up window with the configured text.
Show an alert every time the Web access control feature blocks a page	Shows a pop-up window on the workstation or server every time Panda Adaptive Defense blocks access to a Web page.

Table 12.3: Fields in the 'Local alerts' section

Updates

*Refer to "***Product updates and upgrades***" on page* **135** *for more information on how to update the agent, the protection, and the signature file of the client software installed on users' computers.*

Uninstall other security products

*Refer to "***Protection deployment overview***" on page* **92** *for more information on how to configure the action to take if another security product is already installed on users' computers.*

Refer to **Supported uninstallers** *for a full list of the competitor products that* Panda Adaptive Defense *uninstalls automatically from users' computers.*

Files and paths excluded from scans

Configure items on your computers that won't be blocked, deleted, or disinfected when scanning for malware.

This setting disables the advanced protection. Because this setting can cause potential security holes, Panda recommends that you only use it to resolve performance problems.

Disk files

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

Field	Description
Extensions	Lets you specify the extensions of files that won't be scanned.
Directories	Lets you specify folders whose contents won't be scanned.
Files	Lets you specify files that won't be scanned. You can use wildcard characters '*' and '?'.

Table 12.4: Disk files that won't be scanned by Panda Adaptive Defense

Advanced protection

Behavior

The advanced protection enables the monitoring of the processes run on Windows, macOS, and Linux computers and the sending of all generated telemetry to the Panda Security cloud. This information is incorporated into the investigation processes in charge of classifying files as goodware or malware, with no ambiguity or place for suspicious files. Thanks to this technology, it is possible to detect unknown malware and advanced threats such as APTs on Windows and Linux computers.

These advanced detection features enable Panda to provide the 100% Attestation Service for Windows computers, which classifies all files found on the customer's IT network, leaving no room for 'unknown files'.

Operating mode (Windows only)

Field	Description
Audit	Detected threats are reported, but they aren't blocked or disinfected.
Hardening	Allows the execution of the unknown programs already installed on users' computers. However, unknown programs coming from an untrusted source (the Internet, external storage drives, or other computers on the customer's network) are blocked until a classification is returned. 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.

Table 12.5: Operating modes of the advanced protection for Windows.

- **Report blocking to computer users**: This section allows you to enter a descriptive message to inform users that a file has been blocked by the advanced protection or anti-exploit module. The Panda

Adaptive Defense agent will show a pop-up message with the configured text. To configure the informational message and enable users to decide whether or not to run blocked items, click the option **Give computer users the option to run unknown blocked programs (recommended for advanced users and administrators only).**

Detect malicious activity (Linux only)

Panda Adaptive Defense sends the telemetry obtained from the monitoring of the activity of the macOS and Linux workstations and servers to the Panda cloud. This information enables Panda Adaptive Defense to perform contextual detections and stop advanced threats..

Field	Description
Audit	Detected threats are reported but the malware found isn't blocked.
Block	Detected threats are reported and blocked. Select this option if you are sure the detected activity is caused by malware.
Do not detect	Malware is not detected or reported.

Table 12.6: Operating modes of the Linux protection

Anti-exploit

⚠ *The anti-exploit technology is not available on Windows ARM systems.*

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 trusted 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 the user or from other processes.

If a vulnerable process receives inputs maliciously crafted by hackers, there can be a malfunction that allows the attacker to inject 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's security.

The anti-exploit protection included in Panda Adaptive Defense detects all attempts to inject malicious code into the vulnerable processes run by users, and neutralizes them in two different ways depending on the exploit detected:

- **Exploit blocking**

In this case, Panda Adaptive Defense detects the injection attempt while it is still in progress. As the injection process hasn't been completed yet, the targeted process is not 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 targeted computer will receive a block notification depending on the settings established by the administrator.

- **Exploit detection**

In this case, Panda Adaptive Defense 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 that elapses between when the exploit is detected and when the compromised process is ended, Panda Adaptive Defense will report 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 can end a compromised process automatically to minimize the negative effects of an attack, or delegate the decision to the user, asking them for permission 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 the computer.

Anti-exploit protection settings

- **Anti-exploit**: lets you enable/disable the anti-exploit protection.
- **Advanced code injection**: detects advanced mechanisms for injecting code in running processes.

Field	Description
Audit	Reports exploit detections in the Web console, without taking any action against them or displaying any information to the computer user.
Block	Blocks exploit attacks. It may require ending the compromised process. • **Report blocking to the computer user:** the user will receive a notification, and the compromised process will be automatically ended if required.

Table 12.7: Operating modes of Panda Adaptive Defense's advanced anti-exploit protection

Field	Description
	• **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 compromised 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.

Table 12.7: Operating modes of Panda Adaptive Defense's advanced anti-exploit protection

Given that many exploits continue to run malicious code until the relevant process is ended, an exploit won't appear as resolved in the Exploit activity panel of the Web console until the compromised program is terminated.

Privacy

Panda Adaptive Defense collects the name and full path of the files it sends to Panda Security's cloud for analysis, as well as the name of the logged-in user. This information is used in the reports and forensic analysis tools shown in the Web console. If you don't want this information to be sent to Panda Security's cloud, clear the relevant checkbox in the **Privacy** section.

Network usage

Every executable file found on users' computers that is unknown to Panda Adaptive Defense is sent to the Panda Security cloud for analysis. This behavior is configured so that it has no impact on the customer's network bandwidth:

- The maximum number of MB that can be sent per hour/agent is 50.
- Each unknown file is sent only once for all customers using Panda Adaptive Defense.
- Bandwidth management mechanisms are implemented in order to prevent intensive usage of network resources.

To configure the maximum number of MB that an agent can send per hour, enter a value in the corresponding box. To establish unlimited transfers, set the value to 0.

Chapter 13

Panda Data Control (Personal data monitoring)

Files classified as PII (Personally Identifiable Information) are files that contain information that can be used to identify individuals related to the organization (customers, employees, suppliers, etc.). This information is of a highly personal nature and includes different types of data, such as social security numbers, phone numbers, email addresses, etc.

Panda Data Control is the security module in Panda Adaptive Defense 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 provides three key features:

- Generates a complete, daily inventory of the PII files found on the network, along with basic information such as their name, extension and the name of the computer where the file was detected.
- 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).
- Provides tools to perform flexible, content-based searches and delete duplicate personal data files to limit their presence across the network.

For additional information about the Panda Data Control module, refer to the following section:

- "Creating and managing settings" on page 197: information on how to create, edit, delete, or assign settings to the computers on your network.
- "Controlling and monitoring the management console" on page 63: managing user accounts and assigning permissions.
- "Managing lists" on page 53: information on how to manage lists.

Refer to the Panda Data Control Administration Guide *for more details on the specific management console for this service.*

CHAPTER CONTENT

Introduction to Panda Data Control operation

To fully understand the processes involved in the discovery and monitoring of the personal data stored across an organization, it is necessary to become familiar with some concepts associated with the technologies used by Panda Data Control.

Entity

Each word or group of words with their ow meaning referring to a certain type of personal information is called 'entity'. These entities include personal ID numbers, first and last names, phone numbers, and other.

Given the highly ambiguous and variable nature of natural language, each entity can have different formats depending on the language, and so it is necessary to apply flexible, adaptable algorithms for the detection of personally identifiable information. Generally, analyzing entities consists of applying a set of predefined formats or expressions to data and uses the local context surrounding the detection, as well as the presence or absence of certain keywords, to avoid false positives. Refer to "**Supported entities and countries**".

PII file

Once an entity is identified, the context in which it appears is evaluated to determine if the information it provides is enough to identify a specific person. If it is, the file will be susceptible of being protected with specific processing and access protocols that enable the organization to comply with the applicable legislation (GDPR, PCI, etc.). This evaluation process leverages a monitored machine learning model and a mature model based on the analysis of entities and the global context of documents to finally classify a file with detected entities as a PII file to protect.

Unstructured files and IFilter components

Panda Data Control scans unstructured files (text files with different formats, spreadsheets, PowerPoint presentation files, etc.) searching for entities and classifying files as PII files or non-PII files. However, to correctly interpret the content of unstructured files, certain third-party components must be installed on users' computers. These components are called 'IFilters' and are not part of the Panda Adaptive Defense installation package. Microsoft Search, Microsoft Exchange Server, and Microsoft SharePoint Server, along with other operating system and third-party product services, 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 of them come preinstalled with the Windows operating system. However, other components must be manually installed or updated.

Microsoft Filter Pack is a free single point-of-distribution for Office IFilters. Once installed, it allows Panda Data Control to parse the content of all file formats supported by the Microsoft Office productivity suite. Refer to "**Installing the Microsoft Filter Pack component**".

Indexing process

This consists of inspecting and storing the contents of all files supported by Panda Data Control in order to generate an inventory of PII files and allow content-based searches of files. Indexing processes have a low impact on computer performance although they may take considerable time. For this reason, administrators can schedule the start of the indexing task or limit its scope in order to expedite the process and improve the results returned by searches. Refer to "**The indexing process**"

Normalization process

When performing an indexing process, Panda Data Control applies certain rules to homogenize the data gathered. The aim of this process is to store each word individually and increase its findability, as well as reducing search times. The rules to apply during the normalization process will vary depending on whether the content to store is an entity or plain text. Refer to "**Normalization process**".

PII file inventory

Once a computer has been indexed and all entities and PII files have been identified, Panda Data Control generates an inventory, accessible to the administrator, with the names of the files and their characteristics. This inventory is sent to the Panda Adaptive Defense server once a day. Refer to "**PII file inventory**".

Panda Data Control does not send the contents of the PII files found on the network to the Panda Adaptive Defense server. Only their attributes (name, extension, etc.) and the number and type of found entities are sent.

File searches

Panda Data Control find files by their name, extension, or content on the indexed storage drives found on the computers on the network.

Searches are performed in real time: as soon as the administrator launches a search task, it is deployed to the target computers and starts sending results as they are obtained, without waiting for the task to be completed. Refer to "**File searches**".

Monitoring of the actions taken on PII files

Panda Data Control monitors the events that affect PII files and sends them to the Advanced Visualization Tool console. This tool shows the evolution of PII files, enabling administrators to view if they have been copied, moved, emailed, etc. For more information about Panda Data Control, refer to the Panda Data Control Administration Guide available at **https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-AETHER-Guide-EN.pdf**.

Panda Data Control requirements

Supported platforms

Panda Data Control supports Microsoft Windows platforms from version XP SP3 and later and Windows Server 2003 SP1 and later. Other operating systems such as Linux or macOS are not supported.

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, refer to "**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.

The indexing process

This consists of inspecting and storing the contents of all files supported by Panda Data Control. This process is indispensable to generate the PII file inventory and to search for files on computers by their contents. The indexing process is configured transparently when enabling any of the aforementioned two features. The indexed information is stored locally in the following path on each user's computer: `%ProgramData%\Panda Security\Panda Security Protection\indexstore`.

Despite indexing processes have a low impact on computer performance, they may take considerable time. For that reason, Panda Data Control is configured to launch the process only once on each computer on the network at the time the module is enabled and every time the entity detection technology is updated for improvement purposes.

Once the indexing process is complete, Panda Data Control will start monitoring the creation of new files as well as the deletion and modification of existing ones, updating the index and sending newly detected entities to the Panda Adaptive Defense server every 24 hours.

Configuring the scope, schedule, and type of indexing processes

You can exclude certain files and folders from indexing processes and even change the accuracy of the searches conducted by Panda Data Control.

- To exclude certain files or folders from indexing processes, refer to "**Exclusions**".
- To change the accuracy of searches, refer to "**Index the following content**".
- To schedule indexing processes, refer to "**Schedule indexing**"

PII file inventory

> ⚠ *Panda Data Control does not send the contents of the PII files found on the network to the Panda Adaptive Defense server. Only their attributes (name, extension, etc.) and the number and type of found entities are sent.*

The PII file inventory shows the PII files that Panda Data Control has found on the customer's network.

To enable the inventory feature, refer to “Personal data (inventory, searches, and monitoring)”.

Viewing inventories

Panda Data Control incorporates multiple tools to monitor the PII files found on the network and view the entities they contain.

- To view statistics of the number of PII files found on the network, refer to “Files with personal data”.
- To view statistics of the number of computers that contain PII files on the network, refer to “Computers with personal data”.
- To get a detailed list of the PII files found on the network, refer to “‘Files with personal data’”.
- To get a detailed list of the computers that contain PII files on the network, refer to “Computers with personal data”.

Continuous monitoring of files

PII file monitoring

Panda Data Control collects all events related to the creation, modification, and deletion of PII files, providing visibility into all actions taken and enabling detection of dangerous situations such as data theft, unauthorized access to information, etc.

To view the actions taken on PII files, go to the **Advanced Visualization Tool** at the bottom of the side panel accessible from the **Status** top menu. For more information, refer to the Panda Data Control User Guide available at https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-AETHER-Guide-EN.pdf.

To enable the monitoring of the actions taken on PII files, refer to “Personal data (inventory, searches, and monitoring)”.

Monitoring of files specified by the administrator

In addition to automatically monitoring the files classified as PII by Panda Data Control, administrators can add new files to monitor by using rules. Refer to “Rule-based monitoring of files” on page 251 for more information.

File searches

Requirements for conducting searches

To search for files with specific contents on the computers on the network, the following requirements must be met:

- The user account used to launch the search from the Web console must have a role with the permission **Search for data on computers**. Refer to “Controlling and monitoring the management console” on page 63 for more information about roles.

- The computers targeted by the search must have a Panda Data Control license assigned.
- The computers targeted by the search must have a Data Control settings profile assigned with the option **Allow data searches on computers** enabled. Refer to "Panda Data Control settings".

Searches widget

This is the entry point for the file search feature. It allows searches to be viewed and managed.

To access the **Searches** widget, click **Status** in the top menu, then **Data Control** in the side panel.

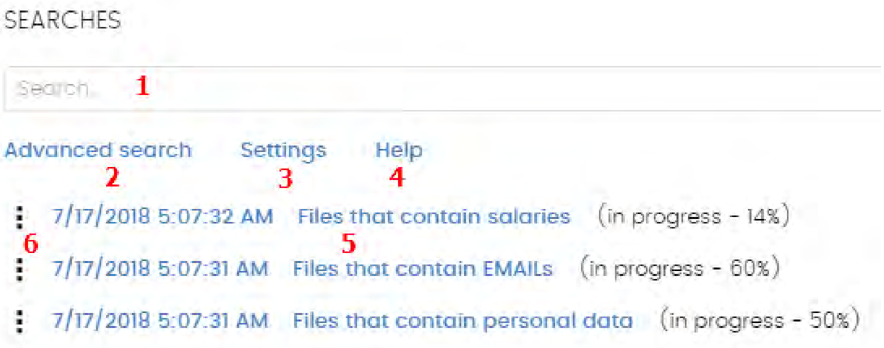

SEARCHES
Search
1
Advanced search
2
Settings
3
Help
4
6
5
7/17/2018 5:07:32 AM Files that contain salaries (in progress - 14%)
7/17/2018 5:07:31 AM Files that contain EMAILs (in progress - 60%)
7/17/2018 5:07:31 AM Files that contain personal data (in progress - 50%)

Figure 13.1: 'Searches' panel

The widget has the following features:

- **(1)** Text box to enter search criteria. Refer to "Search syntax" 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 Data Control settings profiles. For more information, refer to "Panda Data Control settings".
- **(4) Help**: link to Panda Security's support article, showing updated information about the Panda Data Control search syntax.
- **(5) Previous searches**: searches that have been used before and that can be relaunched if required.
- **(6) Search context menu**: lets you edit the name of the search and its parameters, as well as relaunching and deleting it.

Search requirements and parameters

To run searches successfully, bear in mind the following requirements:

- The user account used to launch the search from the Web console must have a role with the permission **Search for data on computers**. Refer to "Controlling and monitoring the management console" on page 63 for more information about roles.
- The computers targeted by the search must have a Panda Data Control license assigned.

- The computers on which searches are run must have a Data Control settings profile assigned with the option **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.

Normalization process

> *The normalization process doesn't affect the entity detection process.*

Panda Data Control applies a number of rules to the data obtained from the indexing process in order to homogenize it. Since the searches run by administrators are performed on the normalized data, it is necessary to know these rules as they may affect the results shown in the console.

- **String conversion to lowercase letters**

Before storing a string in the database, it is converted to lowercase letters.

- **Separating characters**

Panda Data Control detects the following special characters as separators between words. These characters will be removed from indexes unless they are part of an entity.

  - **Carriage return:** `\r`
  - **Line break**: `\n`
  - **Tab key**: `\t`
  - **Characters:** `"  : ; ! ? – + _ * = ( ) [ ] { } , . | % \ / ’`

For example “`Panda.Data(Control`” will be stored as three separate words without the punctuation characters: “`panda`”, “`data`” y “`control`”.

- **Entity normalization**

The entity normalization process follows independent rules:

Entity	Separating characters	Indexing settings
• Bank account numbers • Credit card numbers • Personal ID numbers • Phone numbers • Driver’s license numbers • Passport numbers • Social security numbers	They are removed. The entity is stored in the index as a single set.	They are ignored
• IP addresses • Email addresses	They are respected. The entity is stored in the index as a single set.	They are ignored
• First and last names • Postal addresses	They are used as separators. The entity is stored in the index as multiple items.	They are observed

Table 13.1: Entity normalization rules

- **Entity normalization examples**
  - “1.42.67.116-C” is stored as IDCARD entity “14267116C”.
  - “192.168.1.1” is stored as IP entity “192.168.1.1”.
  - “Sesame Street 5 1st Floor” is stored as “sesame”, “street”, “floor” if the indexing method is **Text only** or as “sesame”, “street”, “5”, “1”, “floor” if the indexing method is **All**.

Creating searches

Creating a free search

- Click the **Status** menu at the top of the console. Then, click **Data Control** from the side panel.
- In the **Searches** widget text box, enter the search terms, in accordance with the search syntax described in section “**Search syntax**”.
- Click the 🔍 icon or press Enter.

Once you have entered the search, the **Search results** window will open. Refer to “**Previous searches**” for more information on how to edit previously defined searches.

Creating a guided search

- Click the **Status** menu at the top of the console. Then, click **Data Control** from the side panel.

- Click the **Advanced search** link.
- Select **Guided search**.
- Configure the search parameters.

- **Advanced search parameters:**

Parameter	Description
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: • **All of these exact words or phrases**: the search will look for files that contain all of the specified words or entries. • **Any of these exact words or phrases**: the search will look for files that contain any or 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.
Personal data	Select the relevant checkboxes to specify the entities that the PII files to find must include. • **All**: all selected entities must appear in the PII file for it to be included in the search results (AND logic). • **Any**: all or at least one of the selected entities must appear in the PII file for it to be included in the search results (OR logic).
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. 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.

Table 13.2: Advanced search parameters

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**).

Changing the name of a previous search

Click the context menu of the search (**6** in figure 13.1) and select **Change name**.

Creating a copy of a previous search

To duplicate a previous search, click the context menu of the search (**6** in figure 13.1) and select **Make a copy**. A window will be displayed with the search settings and the search name changed to 'Copy of'.

Launching a previous search

Click the context menu of the search (**6** in figure 13.1) 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 (**6** in figure 13.1). Click **Cancel** to stop the search and **Delete** to cancel the search and remove it from the **Searches** widget.

Editing a previous search

Click the context menu of the search (**6** in figure 13.1) and select **Edit search**. The **Advanced search** window will open, where you'll be able to edit the search parameters.

Viewing search results

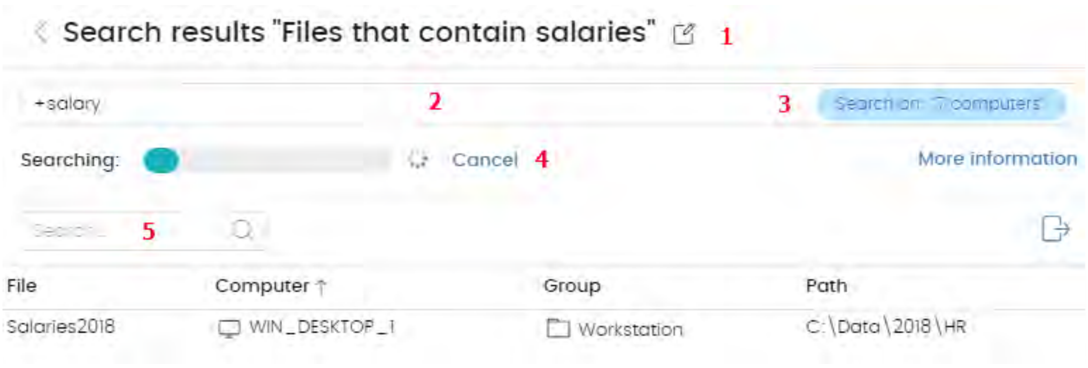
To see the results of a search, go to the **Search results** list, either by:

- 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:



Search results "Files that contain salaries"

+salary

Searching:

File	Computer ↑	Group	Path
Salaries2018	WIN_DESKTOP_1	Workstation	C:\Data\2018\HR

Figure 13.2: '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 where the file was found.	Character string
Group	Panda Adaptive Defense group to which the computer belongs.	Character string
Path	Path on the storage device where the file is located.	Character string

Table 13.3: 'Search results' list fields

- **Fields displayed in the exported file**

Field	Comments	Values
File	Name of the file found.	Character string
Computer	Name of the computer where the file was found.	Character string
Group	Panda Adaptive Defense group to which the computer belongs.	Character string
Path	Path on the storage device where the file is located.	Character string
Personal ID numbers	Indicates whether any personal ID 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 driver's license numbers were found in the file.	Boolean
Social security numbers	Indicates whether any social security numbers were found in the file.	Boolean

Table 13.4: Fields in the 'Search results' exported file

Field	Comments	Values
Email addresses	Indicates whether any email addresses 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
Phone numbers	Indicates whether any phone numbers were found in the file.	Boolean

Table 13.4: Fields in the 'Search results' exported file

Search syntax

Panda Data Control allows administrators to perform flexible searches for files by content using plain text and parameters to narrow the scope of the results.

Syntax allowed in quick searches

- **Word**: searches for 'word' in the document content and metadata.
- **WordA WordB**: searches for 'worda' or 'wordb' (logical operator OR) in the document content.
- "**WordA WordB**": searches for 'worda' and 'wordb' consecutively in the document content.
- **+WordA +WordB**: searches for 'worda' and 'wordb' in the document content.
- +**WordA** -**WordB**: searches for 'worda' but not 'wordb' in the document content.
- **Word***: searches for all words that start with 'word'. The wildcard '*' is only allowed at the end of the search term.
- **Wo?rd**: searches 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~**: searches 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:

Qualifiers	Description
PiiType	Specifies the type of PII data detected in the file.
HasPii	Indicates that the file has PII data.
Filename	Indicates the name of the file.
FileExtension	Indicates the file extension.

Table 13.5: Available qualifiers

The values allowed in these parameters are:

Qualifiers	Description
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 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

Table 13.6: Values allowed in qualifiers

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**: searches for files with Personal ID data detected.
- **+PiiType:IDCARD +'company'**: searches for files containing a list of personal ID details in the company (with the character string 'company').

- **+Filename:scan* +fileextension:docx -PiiType:fullname**: searches 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.)

Tips for building searches that are compatible with the normalization process

- It is preferable to use lowercase letters.
- Bear in mind the settings you have previously configured regarding the type of content to index and excluded files, as those settings will determine the number of results returned in searches.
- To search for **bank account numbers**, **credit card numbers**, **personal ID numbers**, **social security numbers**, **passport numbers**, or **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**, don't use the numeric characters.

Searching for duplicate files

With the aim to help centralize sensitive information in one place and minimize the exposure of this type of data, Panda Data Control provides a feature to look for and delete duplicate files.

What is a duplicate file?

Two files are duplicated when their content is identical, regardless of the normalization process described in section "Normalization process" or the settings defined by the administrator in section "Index the following content". This comparison doesn't take into account the names and extensions of the files.

Searching for duplicate files

Follow these steps to search for duplicate files:

- From the **My lists** side panel:
  - Go to top menu **Status** and click **Add** from the **My lists** side panel. A window will open with all available lists.
  - Click the **Files with personal data** list. A list will be displayed with all PII files found across the network.
- From the **Files with personal data** widget:
  - Go to top menu **Status** and click the **Data Control** dashboard on the left side. Next, click one of the items in the **Files with personal data** widget. The list **Files with personal data** will be displayed filtered by the selected criteria.
- From the **Files by personal data type** widget:
  - Go to top menu **Status** and click the **Data Control** dashboard on the left side. Next, click one of the

items in the **Files by personal data type** widget. The list **Files with personal data** will be displayed filtered by the selected criteria.

- From the context menu of the relevant file, click the **Search for copies of the file** option. A list will be displayed with all files with the same content found across the network.

Deleting and restoring files

Deleting files from computers on the network

Panda Data Control lets you delete indexed files shown in computer inventories. File deletion is an asynchronous operation launched by the network administrator from their console and which takes place when the agent receives a request from the Panda Adaptive Defense server and the following conditions are met:

- The file is not in use.
- The content of the file has not changed with respect to the file stored in the inventory.
- The file has not been deleted by the computer user in the time between when the inventory was generated and when the administrator launched the deletion action.
- The computer is online. If this condition is not met, Panda Data Control will mark the file as **Pending deletion** until the computer connects to the Panda Adaptive Defense server.

Deletion action statuses

As file deletion is an asynchronous operation, it can have the following statuses:

- **Deleted**: the file has been moved to the backup area.
- **Pending deletion**: Panda Data Control is waiting for the computer to connect to the Panda Adaptive Defense server in order to delete it.
- **Error**: it was not possible to delete the file due to an error.

Backing up the files deleted by Panda Data Control

Files deleted by Panda Data Control are not permanently erased from the computers' hard disks. Instead, they are moved to a backup area where they are kept for 30 days, after which they are permanently deleted.

This area is automatically excluded from inventories, searches, and the file monitoring feature, and cannot be accessed by the software installed on users' computers.

Deleting files

Follow the steps below to delete one or more files:

- From the **My lists** side panel:

  - Go to top menu **Status** and click **Add** from the **My lists** side panel. A window will open with all available lists.
  - Click the **Files with personal data** list. A list will be displayed with all PII files found across the network.
- From the **Files with personal data** widget:
  - Go to top menu **Status** and click the **Data Control** dashboard on the left side. Next, click one of the items in the **Files with personal data** widget. The list **Files with personal data** will be displayed filtered by the selected criteria.
- From the **Files by personal data type** widget:
  - Go to top menu **Status** and click the **Data Control** dashboard on the left side. Next, click one of the items in the **Files by personal data type** widget. The list **Files with personal data** will be displayed filtered by the selected criteria.
- Follow the steps below to delete multiple files:
  - Select the checkboxes next to the files to delete.
  - Click the 🗑 icon at the top of the window. A confirmation dialog box will be displayed.
- Follow the steps below to delete a single file:
  - From the context menu of the file to delete, click the **Delete** option. A confirmation dialog box will be displayed.
- If you confirm the action, the file will appear in red and with the ⊗ icon indicating that the file is pending deletion.

Viewing deleted files

Follow the steps below to view the files deleted by the administrator:

- Go to top menu **Status** and click **Add** from the **My lists** side panel. A window will open with all available lists.
- Click the **Files deleted by the administrator** list. A list will be displayed with all PII files found on the network that were previously deleted or restored by the administrator.

Restoring files previously deleted by the administrator

Panda Data Control lets you restore, to their original location, all files previously deleted by the administrator through the console, provided they still remain in the backup area (up to 30 days after they were deleted). File restore is an asynchronous operation launched by the network administrator from their console and which takes place when the agent receives a request from the Panda Adaptive Defense server and the following conditions are met:

- **The file remains in the backup area**: deleted files are kept in the backup area for up to 30 days after being deleted. After that period, they are deleted permanently with no option for recovery,
- **There is no other file with the same name in the restore path**: if there is another file with the same

name in the restore path, Panda Data Control will restore the file to the `Lost&Found` folder.

- **The restore path exists**: if the restore path doesn't exist, Panda Data Control will restore the file to the `Lost&Found` folder.
- **The computer is online**: if the computer is offline, Panda Data Control will mark the file as **Pending restore** until the computer connects to the Panda Adaptive Defense server.

Restore action statuses

As file restore is an asynchronous operation, it can have the following statuses:

- Restored
- Pending restore
- Error

Restoring deleted files

Follow the steps below to restore the files deleted by the administrator:

- **Accessing the restore feature:**
    - Go to top menu **Status** and click **Add** from the **My lists** side panel. A window will open with all available lists.
    - Click the **Files deleted by the administrator** list. A list will be displayed with all PII files found on the network that were previously deleted or restored by the administrator.

or

- Go to top menu **Status** and click the **Data Control** dashboard on the left side. Next, click the **Files deleted by the administrator** widget. The list **Files deleted by the administrator** will be displayed with no preconfigured filters.

- **Follow the steps below to restore multiple files:**
    - Select the checkboxes next to the files to recover.
    - Click the ⟲ icon at the top of the window. A confirmation dialog box will be displayed.
    - If you confirm the restore action, the file's status will change to **Restoring**.
- **Follow the steps below to restore a single file:**
    - Click the context menu of the file to recover.
    - Click the **Restore** option. A confirmation dialog box will be displayed.
    - If you confirm the restore action, the file's status will change to **Restoring**.

Panda Data Control settings

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Data Control** from the side menu.
- Click the **Add** button to open the **Add** settings window.

Required permissions

Permission	Access type
Configure Data Control	Create, edit, delete, copy, or assign Data Control settings.
View Data Control settings	View the Data Control settings.

Table 13.7: Permissions required to access the Data Control settings

Requirements for finding and monitoring Microsoft Office documents

To find computers on the network lacking some or all of the required IFilter components, click the **Check now** link from the settings window. The **Computers** area will open with a list filtered by the following criteria: **Computers without Microsoft Filter Pack**.

Personal data (inventory, searches, and monitoring)

- **Generate and keep an up-to-date inventory of personal data**: shows the PII files detected on the network in the dashboard widgets and in lists. Refer to "Panda Data Control panels and widgets" and "Panda Data Control lists". For the PII files stored on a specific computer to appear in the console, the inventory process must have completed on that computer.
- **Monitor personal data on disk**: monitors the process actions executed on the PII files stored on computers.
- **Monitor personal data in email**: monitors the actions executed on the personal data stored in email messages.

> ⚠ *The monitoring of personal data in email is compatible with Microsoft Exchange accounts and Microsoft Outlook 2013 and 2016 clients. This service is only available for customers who purchased Panda Adaptive Defense version 3.72.00 or earlier.*

- **Allow data searches on computers**: lets you search for files by their name or contents, provided they have been previously indexed. When selecting this option, Panda Data Control will start indexing the files stored on users' computers. Refer to "File searches".

Exclusions

Administrators can exclude from searches those files stored on the computers on the network whose contents they do not consider appropriate to take into account.

- **Extensions**: enter the extensions of the files to exclude.
- **Files**: enter the names of the files to exclude. You can use wildcard characters ? and *.
- **Folders**: enter the folders whose files you want to exclude. You can use system variables and wildcard characters ? and *.

Rule-based monitoring of files

Administrators can define rules for Panda Data Control to monitor files not classified as PII. The system can store up to ten rules, each of which must have a unique name.

- **Monitor files on disk**

Lets you monitor the actions taken on the files selected in section **Monitoring rules**.

- **Monitor files in email**

Lets you monitor the actions taken on the email attachments that meet the rules defined in section **Monitoring rules**.

Monitoring rules

Displays the list of default file extensions to which monitoring is applied. You can add or remove extensions from the list. This list is common to all created rules.

⚠ *If you assign a "file extension" property to a rule, the rule will monitor only those files whose extension coincides with the extensions you specify. It won't monitor all files whose extension coincides with those in the default list.*

To add a monitoring rule, click the **+** icon. This will open the **Add monitoring rules** window where you will be able to configure the rule settings.

- Fill in the name and description fields.
- Enter the condition criteria.

Property	Operator	Value
File name	Is equal to / Is not equal to	• Text field. Wildcard characters * and ? are supported.
File path	Is equal to / Is not equal to	• Text field. Wildcard characters * and ? are supported. • If a file system path is entered, the separator character will be \ by default.

Table 13.8: Fields for configuring conditions

Property	Operator	Value
File content	Is equal to / Is not equal to	• Text field. Wildcard characters * and ? are supported.
File extension	Is equal to / Is not equal to	• Text field. Wildcard characters are not supported. • File extensions must be entered without the dot.

Table 13.8: Fields for configuring conditions

- **New condition**: add more conditions to the rule. Logical operators AND/OR will be applied.

- **Logical operators**

To combine two or more conditions in the same rule, use the logical operators AND and OR. As soon as you add a second or more conditions to a rule, a drop-down menu with the available logical operators will be automatically displayed. These operators will apply to the adjacent conditions.

- **Rule condition groupings**

In a logical expression, parentheses are used to alter the order in which the operators that relate rule conditions are evaluated.

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

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

Advanced indexing options

To view the indexing status of your network, click the **View your computers' indexing status** link. This will open the "'Data Control status'".

Index the following content

This section lets you define the type of content to be considered when generating inventories and performing searches.

Computers whose contents have already been indexed and receive a change of settings will delete the index and restart the indexing process from the beginning.

You can choose between two different types of indexing operations depending on whether you just want to generate an inventory of PII files across the network or search files by content:

- **Index text only:** only text is indexed unless it is part of an entity recognized by Panda Data Control. With this indexing option selected, searches by content will be more limited. Therefore, this option is recommended if you just want to generate an inventory of PII files across the network.

- **Index all content**: this option indexes both texts and alphanumeric characters. This is the recommended option if, in addition to generating an inventory of PII files across the network, you also want to perform accurate content searches.

> *Panda Data Control will search for contents in files based on the option selected in the* ***Index the following content*** *section. If your computers have different indexing settings assigned, search results may not be homogeneous.*

Schedule indexing

This section lets you set the days and times when you want the indexing process to start if required:

- **Always enabled**: there is not a set schedule. The indexing process will start when needed.
- **Enable only during the following times**: select, in the calendar, the days and times when you want the indexing process to start.
- Use the **Clear** and **Select all** buttons to clear or select all cells in the calendar (the latter is equivalent to selecting the **Always enabled** option).

Write to removable storage drives

This section enables you to restrict write to USB external storage media.

- **Allow write to removable drives only when the drive is encrypted**: if this option is selected, the user can only write to previously encrypted USB external storage media.

Panda Data Control panels and widgets

Accessing the dashboard

To access the dashboard, click the **Status** menu at the top of the console. Then, click **Data Control** from the side menu.

Required permissions

Permission	Access to widgets
No permissions	• Deployment status • Offline computers • Update status • Indexing status • Features enabled on computers • Files deleted by the administrator

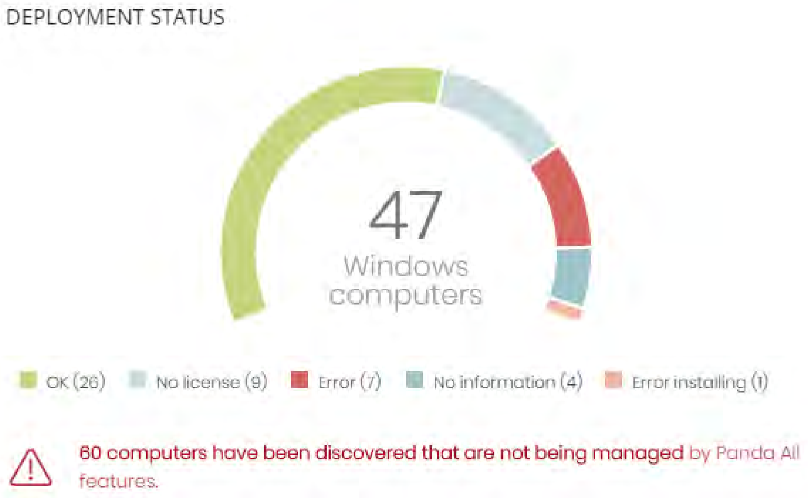
Table 13.9: Permissions required to access the Panda Data Control widgets

Permission	Access to widgets
View personal data inventory	• Files with personal data • Files by personal data type • Computers with personal data
Search for data on computers	• Searches

Table 13.9: Permissions required to access the Panda Data Control widgets

Deployment status

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.



60 computers have been discovered that are not being managed by Panda All features.

Figure 13.3: 'Deployment status' panel

- **Meaning of the data displayed**

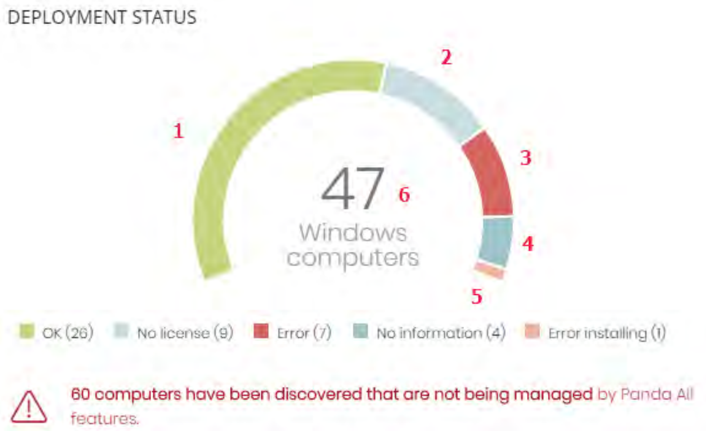
Data	Description
OK	Computers where Panda Data Control is installed, licensed, and is working properly.
Error	Computers with Panda Data Control installed, but for one reason or another the module does not respond to the requests sent from the Panda Security servers.
No license	Computers not managed by Panda Data Control because there are insufficient licenses or they haven't been assigned one of the available licenses.
Error installing	Computers on which the installation process could not be completed.
No information	Computers that have just received a license and haven't reported their status to the server yet and computers with an outdated agent.

Table 13.10: Description of the data displayed in the 'Deployment status' panel

Data	Description
Center	Sum of all computers compatible with Panda Data Control.

Table 13.10: Description of the data displayed in the ‘Deployment status’ panel

- **Lists accessible from the panel**



⚠ 60 computers have been discovered that are not being managed by Panda All features.

Figure 13.4: Hotspots in the ‘Deployment status’ panel

Click the hotspots shown in figure 13.4 to access the **Data Control status** list with the following predefined filters:

Hotspot	Filter
(1)	Data Control status = OK.
(2)	Data Control status = No license.
(3)	Data Control status = Error.
(4)	Data Control status = No information.
(5)	Data Control status = Error Installing.
(6)	No filters.

Table 13.11: Filters available in the ‘Data Control status’ list

Offline computers

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.

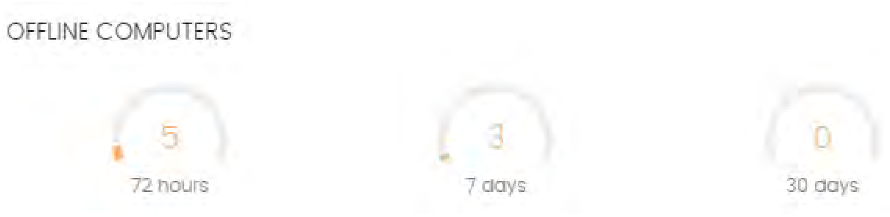


Figure 13.5: 'Offline computers' panel

- **Meaning of the data displayed**

Data	Description
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.

Table 13.12: Description of the data displayed in the 'Offline computers' panel

- **Lists accessible from the panel**

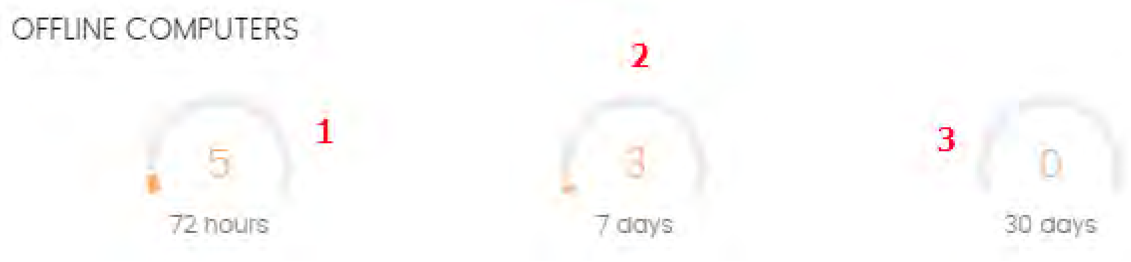


Figure 13.6: Hotspots in the 'Offline computers' panel

Click the hotspots shown in figure 13.6 to access the **Data Control status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 13.13: Filters available in the 'Data Control status' list

Update status

This displays the status of computers with respect to updates of the Panda Data Control module.

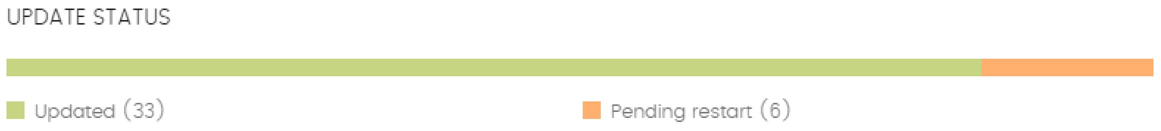


Figure 13.7: 'Update status' panel

- **Meaning of the data displayed**

Data	Description
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.

Table 13.14: Description of the data displayed in the 'Update status' panel

- **Lists accessible from the panel**

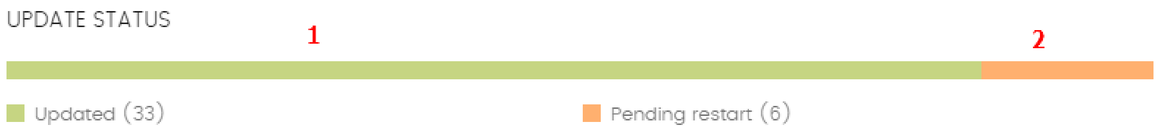


Figure 13.8: Hotspots in the 'Update status' panel

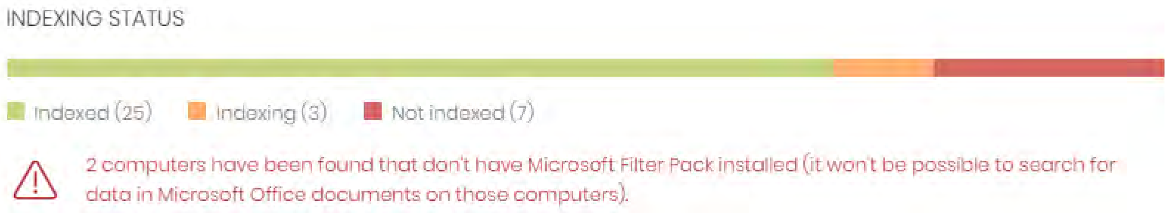
Click the hotspots shown in figure 13.8 to access the **Data Control status** list with the following predefined filters:

Hotspot	Filter
(1)	Protection up to date = Yes.
(2)	Protection up to date = Pending restart.
(3)	Protection up to date = No.

Table 13.15: Filters available in the 'Data Control status' list

Indexing status

This displays the status of the computers with respect to the indexing status of the storage drives connected.



INDEXING STATUS

🟩 Indexed (25) 🟧 Indexing (3) 🟥 Not indexed (7)

⚠ 2 computers have been found that don't have Microsoft Filter Pack installed (it won't be possible to search for data in Microsoft Office documents on those computers).

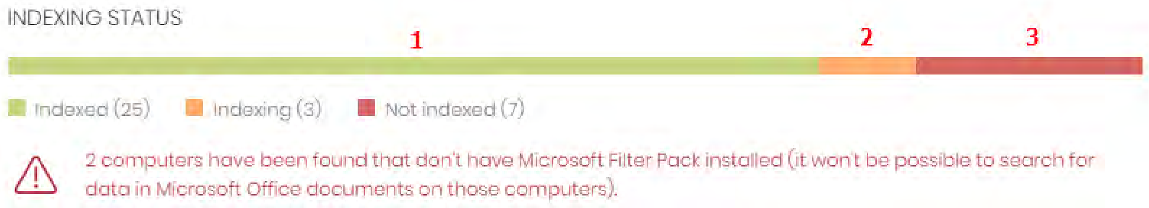
Figure 13.9: 'Indexing status' panel

- **Meaning of the data displayed**

Data	Description
Indexed	Number of computers where the contents of the storage drives are fully indexed. Requires that the searches and/or inventory be enabled. Refer to "**Panda Data Control settings**"
Not indexed	Number of computers where the contents of the storage drives are not indexed. Requires that the searches and/or inventory be enabled. Refer to "**Panda Data Control settings**"
Indexing	Number of computers where the contents of the storage drives are in the process of being indexed. Requires that the searches and/or inventory be enabled. Refer to "**Panda Data Control settings**"

Table 13.16: Description of the data displayed in the 'Indexing status' panel

- **Lists accessible from the panel**



INDEXING STATUS

🟩 Indexed (25) 🟧 Indexing (3) 🟥 Not indexed (7)

⚠ 2 computers have been found that don't have Microsoft Filter Pack installed (it won't be possible to search for data in Microsoft Office documents on those computers).

Figure 13.10: Hotspots in the 'Indexing status' panel

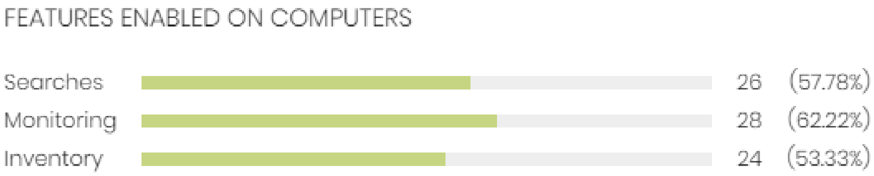
Click the hotspots shown in figure 13.10 to access the **Data Control status** list with the following predefined filters:

Hotspot	Filter
(1)	Indexing status = Indexed.
(2)	Indexing status = Indexing.
(3)	Indexing status = Not indexed.

Table 13.17: Filters available in the 'Data Control status' list

Features enabled on computers

Shows the total number of computers on the network where Panda Data Control is correctly installed and licensed, and which have reported the status of the three features that make up the module as **Enabled**.



FEATURES ENABLED ON COMPUTERS

Searches 26 (57.78%)
Monitoring 28 (62.22%)
Inventory 24 (53.33%)

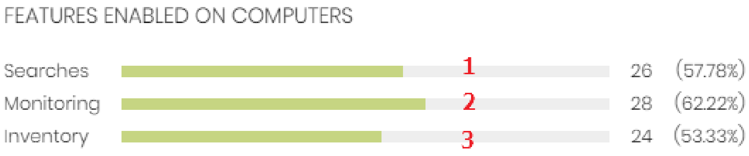
Figure 13.11: 'Features enabled on computers' panel

- **Meaning of the data displayed**

Data	Description
Searches	Shows the total number of computers which have reported the status of the feature for performing content-based searches in PII files as Enabled.
Monitoring	Shows the total number of computers which have reported the status of the PII file monitoring feature as Enabled.
Inventory	Shows the total number of computers which have reported the status of the PII inventory feature as Enabled.

Table 13.18: Description of the data displayed in the 'Features enabled on computers' panel

- **Lists accessible from the panel**



FEATURES ENABLED ON COMPUTERS

Searches 1 26 (57.78%)
Monitoring 2 28 (62.22%)
Inventory 3 24 (53.33%)

Figure 13.12: Hotspots in the 'Features enabled on computers' panel

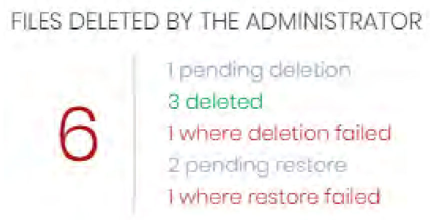
Click the hotspots shown in figure 13.12 to access the **Data Control status** list with the following predefined filters.

Hotspot	Filter
(1)	Data searches on computers enabled = Yes.
(2)	Personal data monitoring enabled = Yes.
(3)	Personal data inventory enabled = Yes.

Table 13.19: Filters available in the 'Data Control status' list

Files deleted by the administrator

Shows the different statuses of the files deleted by the administrator.



FILES DELETED BY THE ADMINISTRATOR

6

1 pending deletion
3 deleted
1 where deletion failed
2 pending restore
1 where restore failed

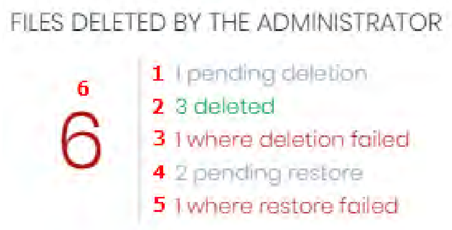
Figure 13.13: ‘Files deleted by the administrator’ panel

- **Meaning of the data displayed**

Data	Description
Pending deletion	Files marked for deletion which have not been deleted yet.
Deleted	Deleted files that remain in the backup area.
Where deletion failed	Files which could not be deleted.
Pending restore	Files marked for restore which have not been restored yet.
Restored	Files which have been moved from the backup area to their original location.

Table 13.20: Description of the data displayed in the ‘Files deleted by the administrator’ panel

- **Lists accessible from the panel**



FILES DELETED BY THE ADMINISTRATOR

6
6

1 1 pending deletion
2 3 deleted
3 1 where deletion failed
4 2 pending restore
5 1 where restore failed

Figure 13.14: Hotspots in the ‘Files deleted by the administrator’ panel

Clicking the hotspots shown in figure 13.14 will open lists with the following predefined filters:

Hotspot	List	Filter
(1)	Files with personal data.	Pending deletion.
(2)	Files deleted by the administrator.	Status = Deleted.
(3)	Files with personal data.	Error deleting.
(4)	Files deleted by the administrator.	Status = Pending restore.

Table 13.21: Lists accessible from the 'Files deleted by the administrator' panel

Hotspot	List	Filter
(5)	Files deleted by the administrator.	Status = Error restoring.
(6)	Files deleted by the administrator.	Status = All.

Table 13.21: Lists accessible from the 'Files deleted by the administrator' panel

Files with personal data

Shows the number of files with personal data found on the network and the total number of files with personal data found in the last daily inventory generated.

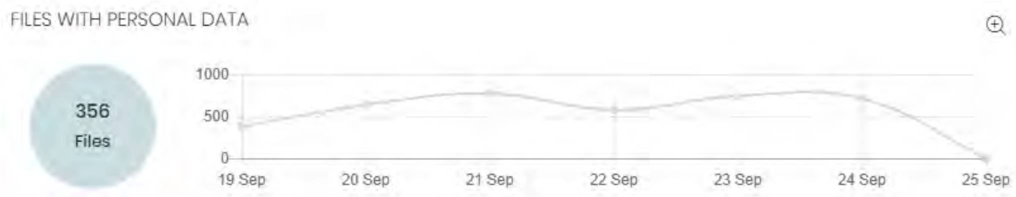


Figure 13.15: 'Files with personal data' panel

- **Meaning of the data displayed**

Data	Description
Bubble	Total number of PII files found according to the last inventory sent by each computer.
Line	Number of PII files found in the daily inventories generated on the dates indicated in the X-axis, on all computers on the network.

Table 13.22: Description of the data displayed in the 'Files with personal data' panel

- **Lists accessible from the panel**

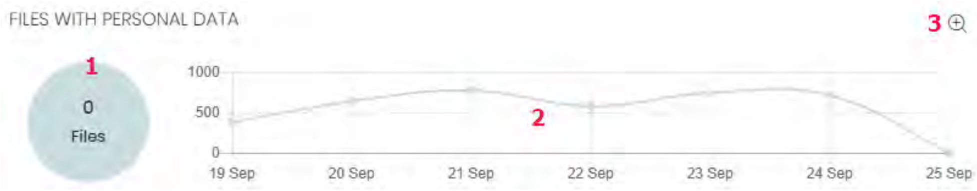


Figure 13.16: Hotspots in the 'Files with personal data' panel

Click the hotspots shown in figure 13.16 to access the **Files with personal data** list with the following predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Date 1 = selected date and Date 2 = current date.
(3)	Opens a window with more detailed information.

Table 13.23: Filters available in the 'Files with personal data' list

- **'Files with personal data' extended graph**

Clicking the ⊕ icon opens a window with an extended version of the **Files with personal data** graph. This graph displays a different line for the number of PII files containing each of the supported entities.

Follow the steps below to configure the information displayed in the graph:

- Click the legend keys to enable/disable the relevant data series.
- Click the **Hide all data** link to display the number of PII files containing any type of entity.
- Click **Show all data** to display the number of PII files containing each type of supported entity.

Computers with personal data

Shows the number of workstations and servers with files containing personal data found in the last daily inventory generated.

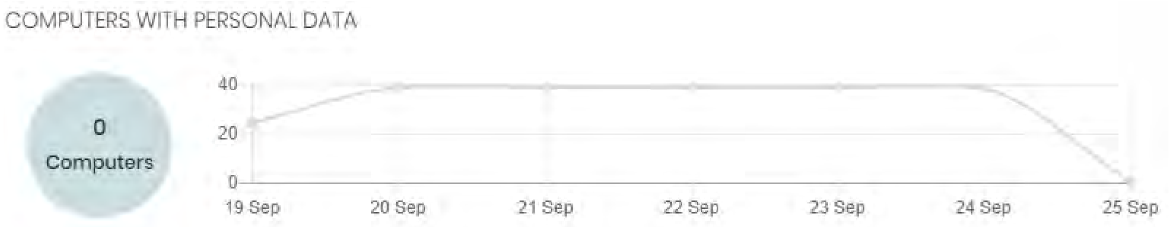


Figure 13.17: ‘Computers with personal data’ panel

- **Meaning of the data displayed**

Data	Description
Bubble	Number of computers containing PII files according to the last data sent by each computer.
Line	Total number of computers containing PII files found in the daily inventories generated on the dates indicated in the X-axis.

Table 13.24: Description of the data displayed in the ‘Computers with personal data’ panel

- **Lists accessible from the panel**

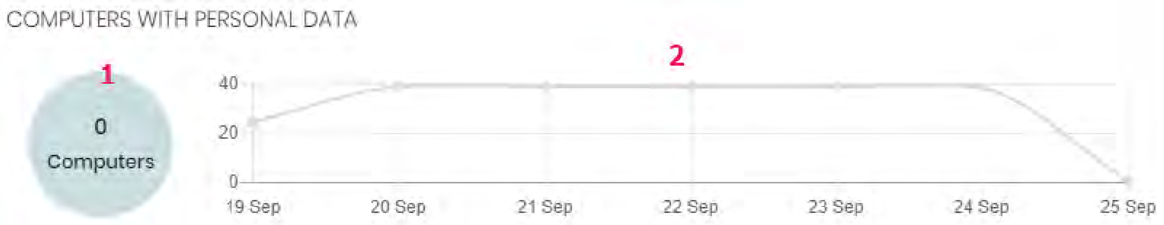


Figure 13.18: Hotspots in the ‘Computers with personal data’ panel

Click the hotspots shown in figure 13.18 to access the **Computers with personal data** list with the following predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Date 1 = selected date and Date 2 = current date.

Table 13.25: Filters available in the 'Computers with personal data' list

Files by personal data type

Shows the number of PII files found in the last daily inventory generated, by entity type.

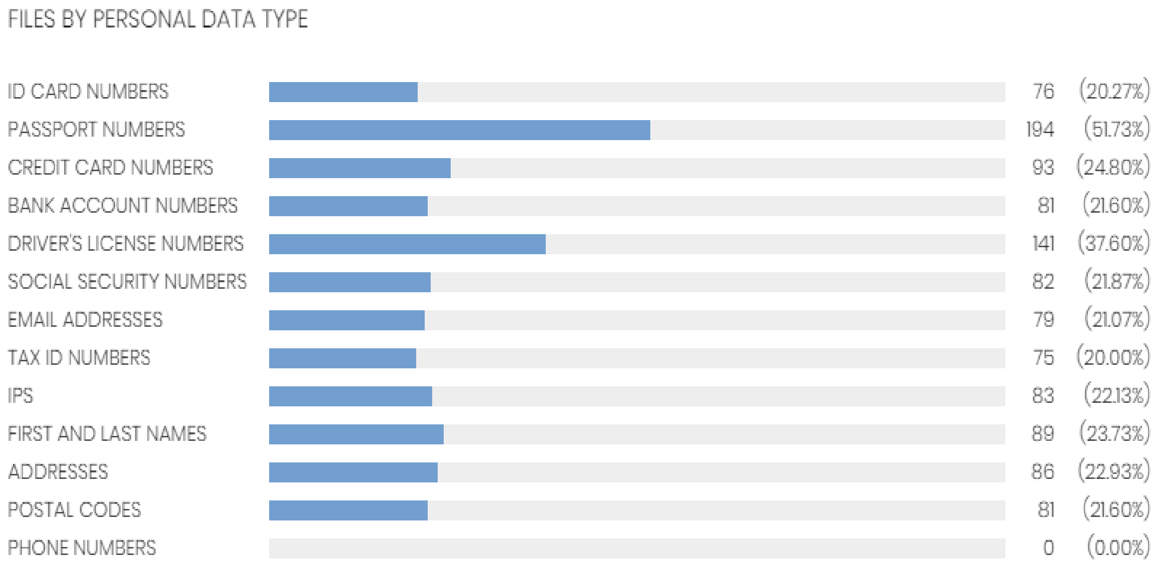


Figure 13.19: 'Files by personal data type' panel

- **Meaning of the data displayed**

Data	Description
Data	Total number of PII files found in the last daily inventory generated, by entity type, and percentage over the total number of PII files detected.

Table 13.26: Description of the data displayed in the 'Files by type personal data' panel

- **Lists accessible from the panel**

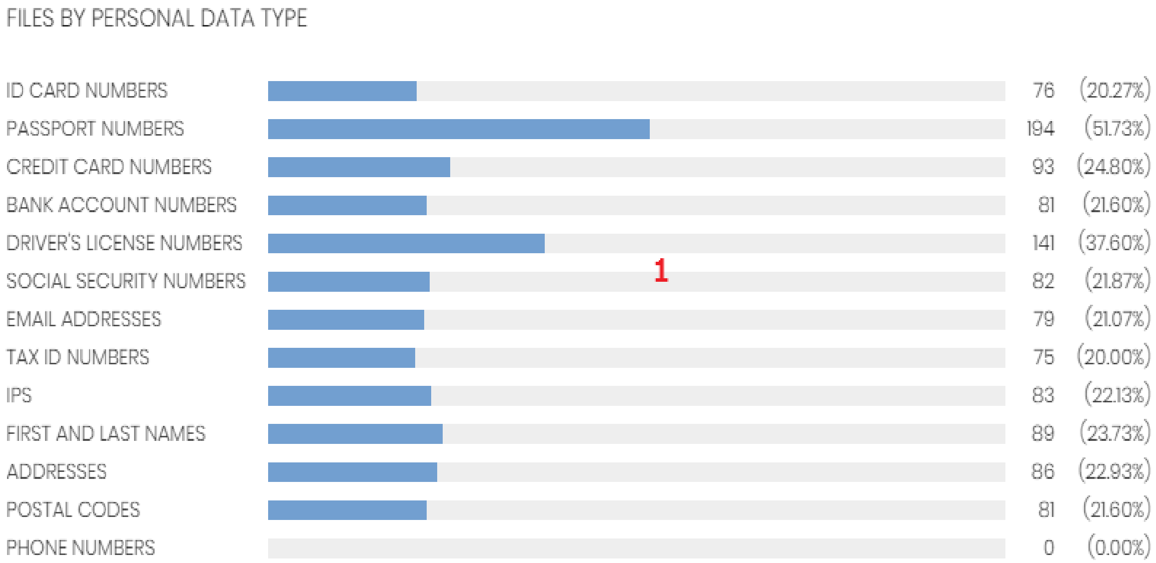


Figure 13.20: Hotspots in the 'Files by personal data type' panel

Click the hotspot shown in the figure above to access the **Files with personal data** list with the following predefined filters:

Hotspot	Filter
(1)	Personal data = Selected entity.

Table 13.27: Filters available in the 'Files with personal data' list

Panda Data Control lists

Accessing the lists

There are two ways to access the lists:

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

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window will open with all available lists.
- Select a list from the **Data protection** section to view the associated template. Edit it and click **Save**. The new list will be added to the side menu.

Required permissions

Permission	Access to lists
No permissions	• Data Control status
View personal data inventory	• Files with personal data • Computers with personal data • Files deleted by the administrator

Table 13.28: Permissions required to access the Panda Data Control lists

'Data Control status'

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 within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Computer status	Agent reinstallation: • Reinstalling the agent. • Agent reinstallation error. Protection reinstallation: • Reinstalling the protection. • Protection reinstallation error. Pending restart.	Icon
	Computer isolation status: • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated	

Table 13.29: 'Data Control status' list fields

Field	Comments	Values
	"RDP attack containment" mode: • Computer in "RDP attack containment" mode. • Ending "RDP attack containment" mode	
Personal data monitoring	Indicates if Panda Data Control can monitor the personal data files found on the computer's storage devices. If it cannot, it will indicate the reason.	• Error installing and Error • Disabled • Enabled • No license • No information
Inventory	Indicates if Panda Data Control can generate an inventory of the personal data files found on the computer's storage devices. If it cannot, it will indicate the reason.	• Error installing and Error • Disabled • Enabled • No license • No information
Searches	Indicates whether Panda Data Control can search for files on the computer's storage devices, and if not, it specifies the reason.	• Error installing and Error • Disabled • Installing • Enabled • No license • No information
Updated	Indicates whether the Panda Data Control module installed on the computer is the latest release or not. Hover the mouse pointer over the field to see the version of the installed protection	• Updated • Pending restart • Not updated
Microsoft Filter Pack	Indicates whether all necessary Microsoft Filter Pack components are installed on the computer or not.	• Installed • Not installed • Info unavailable

Table 13.29: 'Data Control status' list fields

Field	Comments	Values
Indexing status	Indicates the status of the file indexing process.	• ⟳ Indexing • ✓ Indexed (Text only or All content) • ⊗ Not indexed • — Not available
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	Date

Table 13.29: 'Data Control status' list fields

*To view a graphical representation of the list data, go to the following widgets as appropriate: "**Deployment status**", "**Offline computers**", "**Update status**", "**Features enabled on computers**", or "**Indexing status**".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	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 within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Agent version		Character string
Installation date	Date the Panda Adaptive Defense software 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 the agent was last updated.	Date

Table 13.30: Fields in the 'Data Control status' exported file

Field	Comments	Values
Platform	Operating system installed on the computer.	• Windows •
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether the protection is updated to the latest version or not.	Binary value
Protection version	Internal version of the protection module.	Character string
Updated knowledge	Indicates whether the signature file on the computer is the latest version or not.	Binary value
Last update on	Date of the last signature file download.	Date
Personal data monitoring	Indicates if Panda Data Control can monitor the personal data files found on the computer's storage devices. If it cannot, it will indicate the reason.	• Error installing • Error • Disabled • OK • No license • No information
Personal data inventory	Indicates if Panda Data Control can generate an inventory of the personal data files found on the computer's storage devices. If it cannot, it will indicate the reason.	• Error installing • Error • Disabled • OK • No license • No information
Searches	Indicates whether Panda Data Control can search for files on the computer's storage devices, and if not, it specifies the reason.	• Error installing • Error • Disabled • OK • No license • No information
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

Table 13.30: Fields in the 'Data Control status' exported file

Field	Comments	Values
Indexing type	Shows the indexing type applied to the computer.	• Text only • All content
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 of the unsuccessful attempt to install Panda Data Control.	Date
Installation error	Reason for the installation error.	Character string

Table 13.30: Fields in the 'Data Control status' exported 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 • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Updated protection	Filters according to the protection version installed on computers.	• All • Yes • No • Pending restart
Indexing status	Filters computers according to the file indexing status.	• All • Indexing • Indexed • Not indexed • Not available
Indexing type	Shows those computers that have a specific type of indexing assigned.	• All • Text only • All content

Table 13.31: Filters available in the 'Data Control status' list

Field	Comments	Values
Microsoft Filter Pack	Filters computers according to whether they have all necessary components of Microsoft Filter Pack.	• All • False • True
Full Encryption status	Filters computers according to the status of the Panda Data Control module.	• Installing... • No information • OK • Personal data monitoring disabled • Data searches on computers disabled • Error • Error installing • No license • Personal data monitoring enabled • Data searches on computers enabled • Personal data inventory enabled • Personal data inventory disabled

Table 13.31: Filters available in the 'Data Control status' list

'Files with personal data'

Shows all PII files found on the network, along with their type, location, and other relevant information.

Since Panda Data Control only keeps the last complete inventory generated for each machine, those computers that were turned off at the time when the inventory was generated will only display information in the **Files with personal data** list if the date displayed in the **Last seen** column falls within the range selected for the Panda Data Control feature.

Field	Comments	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
File	File name.	Character string
Path	Full path to the folder that contains the file on the computer.	Character string

Table 13.32: Fields in the 'Files with personal data' list

Field	Comments	Values
Personal data	Personal data type found in the file.	• Personal ID number entity • Passport number entity • Credit card number entity • Bank account number entity • Social Security Number entity • Driver's license number entity • Email address entity • IP address entity • First name and last name entity • Physical address entity • Phone number entity
Last seen	Date when the last snapshot of the computer's file system was taken.	Date

Table 13.32: Fields in the 'Files with personal data' list

*To view a graphical representation of the list data, go to widget "***Files by personal data type***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
File	File name.	Character string
Path	Full path to the folder that contains the file on the computer.	Character string
Personal ID numbers	ID card number entity.	Boolean
Passport numbers	Passport number entity.	Boolean
Credit card numbers	Credit card number entity.	Boolean
Bank account numbers	Bank account number entity.	Boolean

Table 13.33: Fields in the 'Files with personal data' exported file

Field	Comments	Values
Driver's license numbers	Driver's license number entity.	Boolean
Social security numbers	Social Security Number entity.	Boolean
Email addresses	Email address entity.	Boolean
IPs	IP address entity.	Boolean
First and last names	First name and last name entity.	Boolean
Addresses	Physical address entity.	Boolean
Phone numbers	Phone number entity.	Boolean
Last seen	Date when the device was last included in the daily inventory.	Date
Status	File status	• Deleted • Pending deletion • Restored • Pending restore • Error restoring
Error	• The file is in use. • The content of the file has changed with respect to the file in the inventory. • The file has been deleted by the computer user in the time between when the inventory was generated and when the administrator launched the deletion action. • An error occurred attempting to delete the file.	Character string

Table 13.33: Fields in the 'Files with personal data' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Filters computers according to type.	• Workstation • Laptop • Server
Last seen	Shows the inventory of the computers that were last seen within the selected date range.	• All • Last 24 hours • Last 7 days • Last month • Last year

Table 13.34: Filters available in the 'Files with personal data' list

Field	Comments	Values
Personal data	Indicates the entity type found in the PII file.	• Personal ID numbers • Credit card numbers • Driver's license numbers • Email addresses • IPs • Addresses • Phone numbers • Passport numbers • Bank account numbers • Social security numbers • Tax ID numbers • First and last names

Table 13.34: Filters available in the 'Files with personal data' list

Computers with personal data

Shows the number of PII files found on each computer on the network. The list displays different types of information depending on the way the **Date 1** and **Date 2** filters are configured:

- If fields **Date 1** and **Date 2** are set, the list will display the variation in the number of PII files found on each computer between those two dates. That is, it will display the evolution of the number of PII files found on each computer on the network.
- If fields **Date 1** and **Date 2** are empty, the list will display the number of PII files found on each computer on the network, according to the result of the last complete inventory generated.
- If field **Date 1** is set, the list will display the number of PII files found on each computer on the network, according to the result of the complete inventory generated on the selected date.

To view a list of the PII files found on a computer, click its name. The Files with personal data list will open filtered by the name of the selected computer.

Field	Comments	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Files (date)	File name.	Character string

Table 13.35: Fields in the 'Computers with personal data' list

Field	Comments	Values
Variation	Difference between the number of PII files found on Date 1 and Date 2. If the number is positive, the icon ↑ will be displayed. If the number is negative, the icon will be this: ↓	Numeric value

Table 13.35: Fields in the 'Computers with personal data' list

*To view a graphical representation of the list data, go to widget "***Computers with personal data***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Date 1	Start date to see the evolution of PII files.	Date
Inventory date	Date when the computer's complete inventory was generated.	Date
Files with personal data	Number of PII files found on the date specified on Date 1,	Numeric value
Passport numbers	Number of PII files containing the Passport number entity found on the date specified on Date 1.	Numeric value
Credit card numbers	Number of PII files containing the Credit card number entity found on the date specified on Date 1.	Numeric value
Bank account numbers	Number of PII files containing the Bank account number entity found on the date specified on Date 1.	Numeric value
Driver's license numbers	Number of PII files containing the Driver's license number entity found on the date specified on Date 1.	Boolean
Social security numbers	Number of PII files containing the Social Security Number entity found on the date specified on Date 1.	Numeric value
Email addresses	Number of PII files containing the Email address entity found on the date specified on Date 1.	Numeric value
Tax ID numbers	Number of PII files containing the Tax ID number entity found on the date specified on Date 1.	Numeric value
IPs	Number of PII files containing the IP address entity found on the date specified on Date 1.	Numeric value

Table 13.36: Fields in the 'Computers with personal data' exported file

Field	Comments	Values
First and last names	Number of PII files containing the First and last names entity found on the date specified on Date 1.	Numeric value
Addresses	Number of PII files containing the Physical address entity found on the date specified on Date 1.	Numeric value
Phone numbers	Number of PII files containing the Phone number entity found on the date specified on Date 1.	Numeric value
Date 2	End date to see the evolution of PII files.	Date
Inventory date	Date when the computer's complete inventory was generated.	Date
Files with personal data	Number of PII files found on the date specified on Date 2,	Numeric value
Passport numbers	Number of PII files containing the Passport number entity found on the date specified on Date 2.	Numeric value
Credit card numbers	Number of PII files containing the Credit card number entity found on the date specified on Date 2.	Numeric value
Bank account numbers	Number of PII files containing the Bank account number entity found on the date specified on Date 2.	Numeric value
Driver's license numbers	Number of PII files containing the Driver's license number entity found on the date specified on Date 2.	Boolean
Social security numbers	Number of PII files containing the Social Security Number entity found on the date specified on Date 2.	Numeric value
Email addresses	Number of PII files containing the Email address entity found on the date specified on Date 2.	Numeric value
Tax ID numbers	Number of PII files containing the Tax ID number entity found on the date specified on Date 2.	Numeric value
IPs	Number of PII files containing the IP address entity found on the date specified on Date 2.	Numeric value
First and last names	Number of PII files containing the First and last names entity found on the date specified on Date 2.	Numeric value
Addresses	Number of PII files containing the Physical address entity found on the date specified on Date 2.	Numeric value
Phone numbers	Number of PII files containing the Phone number entity found on the date specified on Date 2.	Numeric value

Table 13.36: Fields in the 'Computers with personal data' exported file

- **Filter tool**

Field	Comments	Values
Find	Filters the list by computer name.	Character string
Date 1	First date to compare.	Date
Date 2	Second date to compare.	Date
Computer type	Filters computers according to type.	• Workstation • Laptop • Server
Personal data	Indicates the entity type found in the PII file.	• Personal ID numbers • Credit card numbers • Driver's license numbers • Email addresses • IPs • Addresses • Phone numbers • Passport numbers • Bank account numbers • Social security numbers • Tax ID numbers • First and last names
Variation	Shows computers with a positive/negative variation in the number of PII files found.	• **Positive**: the number of files found on date 2 is higher than the number of files found on date 1. • **Negative**: the number of files found on date 2 is lower than the number of files found on date 1. • **All**

Table 13.37: Filters available in the 'Computers with personal data' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "**Details section (3)**" on page 179 for more information.

'Files deleted by the administrator'

This list shows the status of those files that have received a deletion or restore task and are still accessible on the computers on the network or in the backup area.

Field	Comments	Values
Date	Date when the file status changed.	Date
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
File	File name.	Files with personal data
Path	Location of the file in the computer's file system.	Character string
Performed by	Management console account responsible for the file status change.	Character string
Status	File status	• All • Deleted • Pending deletion • Restored • Pending restore • Error restoring

Table 13.38: Fields in the 'Files deleted by the administrator' list

*To view a graphical representation of the list data, go to widget "**Files deleted by the administrator**".*

- **Fields displayed in the exported file (history)**

This list displays the deletion and restore actions performed by the administrator on the files on the network.

Field	Comments	Values
Date	Date when the file status changed.	Date
Computer	Computer name.	Character string

Table 13.39: Fields in the 'Files deleted by the administrator' list

Field	Comments	Values
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
File	File name.	Files with personal data
Path	Location of the file in the computer's file system.	Character string
Performed by	Management console account responsible for the file status change.	Character string
Status	File status	• All • Deleted • Pending deletion • Restored • Pending restore • Error restoring

Table 13.39: Fields in the 'Files deleted by the administrator' list

- **Fields displayed in the exported file (detailed history)**

This list displays all deletion and restore actions performed by the administrator over time on the files on the network.

Field	Comments	Values
Date	Date when the file status changed.	Date
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
File	File name.	Files with personal data
Path	Location of the file in the computer's file system.	Character string
Performed by	Management console account responsible for the file status change.	Character string
Status	File status	• All • Deleted • Pending deletion

Table 13.40: Fields in the 'Files deleted by the administrator' exported file

Field	Comments	Values
		• Restored • Pending restore • Error restoring

Table 13.40: Fields in the ‘Files deleted by the administrator’ exported file

- **Filter tool**

Field	Comments	Values
Status	File status	• All • Deleted • Pending deletion • Restored • Pending restore • Error restoring

Table 13.41: Filters available in the ‘Files deleted by the administrator’ list

Supported program extensions

Suite name	Product	Extensions
Office	Word	- DOC - DOT - DOCX - DOCM - RTF
	Excel	- XLS - XLSM - XLSX - XLSB - CSV
	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

Table 13.42: List of supported program extensions

Suite name	Product	Extensions
	Calc	• OTS • ODS • SXC
Plain text		TXT
Web browsers	• Internet Explorer • Chrome • Opera • Other	• HTM • HTML • MHT • OTH
Mail clients	• Outlook • Outlook Express	EML
Other	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Table 13.42: List of supported program extensions

Supported packers and compressors

Name of file compressor / packer / algorithm	Extensions
7-ZIP	7Z
bzip2	BZ2
gzip	GZ
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 13.43: List of supported compressor/packer extensions

Supported entities and countries

Panda Data Control supports the following data types or entities:

- Bank account numbers.
- Credit card numbers.
- Personal ID numbers.
- IP addresses.
- Email addresses.
- Phone numbers.
- Driver’s license numbers.
- Passport numbers.
- Social security numbers.

- First names and last names.
- Postal addresses and ZIP/postal codes.

Supported countries

The format of recognized data varies from country to country. Panda Data Control recognizes data from the countries listed below:

- Germany
- Austria
- Belgium
- Denmark
- Spain
- Finland
- France
- Hungary
- Ireland
- Italy
- Norway
- Netherlands
- Portugal
- Sweden
- Switzerland
- United Kingdom

Chapter 14

Panda Patch Management (Updating vulnerable programs)

Panda Patch Management is a built-in module on Aether Platform that finds those computers on the network with known software vulnerabilities and updates them centrally and automatically. It minimizes the attack surface, preventing malware from taking advantage of the software flaws that may affect the organization's workstations and servers in order to infect them.

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

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

Panda Patch Management is not compatible with Windows ARM systems.

For additional information about the Panda Patch Management module, refer to:

- "**Creating and managing settings**" on page 197: information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**" on page 63: managing user accounts and assigning permissions.
- "**Managing lists**" on page 53: information on how to manage lists.

CHAPTER CONTENT

Panda Patch Management features

The features provided by Panda Patch Management are accessible via the following sections in the management console:

- **To configure the discovery of missing patches**: go to the **Patch management** settings section (top menu **Settings**, side panel). Refer to "Configuring the discovery of missing patches"

- **To configure patch exclusions**: go to the **Available patches** list. Refer to "Exclude patches for all or some computers".
- **To have visibility into the update status of the entire IT network**: go to the **Patch Management** dashboard (top menu **Status**, side panel). Refer to "Patch management status"
- **To view lists of missing patches**: check the **Patch management status, Available patches** and **End-of-Life programs** lists (top menu **Status**, side panel **My lists**, **Add**). Refer to "Panda Patch Management module lists"
- **To view a history of all installed patches**: check the **Installation history** list (top menu **Status**, side panel **My lists**, **Add**)**.** Refer to "Installation history"
- **To patch computer:** Select one of the following options:
  - From the **Last patch installation tasks** widget, click the **View installation history** link. Refer to "Last patch installation tasks".
  - Go to the **Status** menu at the top of the console, click **Add** in the **My lists** section of the side panel and select the **Installation history** list. Refer to "Installation history".
  - Go to the **Tasks** menu at the top of the console, select the task that installed the patch to uninstall and click **View installed patches**.
  - Click the patch to uninstall. A screen will be displayed with the patch details and the **Uninstall** button if the patch supports this option. Refer to "Uninstalling a patch".

General workflow

Panda Patch Management is a comprehensive tool for patching and updating the operating systems and all programs installed on the computers on your network. To effectively reduce the attack surface of your computers, follow the steps below:

- Make sure Panda Patch Management works properly on the protected computers on your network.
- Make sure that all published patches are installed.
- Isolate computers with unpatched known vulnerabilities.
- Install the selected patches.
- Uninstall any patches that are causing malfunction problems (rollback).
- Exclude patches for all or certain computers
- Make sure the programs installed on your computers are not in EOL (End-Of-Life) stage.
- Regularly check the history of patch and update installations.
- Regularly check the patch status of those computers where incidents have been recorded.

Make sure that Panda Patch Management works properly

Follow the steps below:

- Make sure that all computers on your network have a Panda Patch Management license assigned and the module is installed and running. Use the "**Patch management status**" widget.
- Make sure that all computers with a Panda Patch Management license assigned can communicate with the Panda Security cloud. Use the "**Time since last check**" widget.
- Make sure the computers that will receive the patches have the Windows Update service running with automatic updates disabled.

*Select the **Disable Windows Update** on computers option in the Patch Management settings for Panda Adaptive Defense to manage the service correctly. For more information, refer to "**General options**".*

Make sure that all published patches are installed

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

- To view missing patches by type and criticality level, use the "**Patch criticality**" widget.
- To view details of the patches that are missing on a computer or computer group:
  - Go to the computer tree (top menu **Computers**, **Folder** tab in the side panel), and click the context menu of a computer group containing Windows computers. Select **View available patches.** The "**Available patches**" will be displayed filtered by the relevant group.

Or,

  - Go to the computers screen (top menu **Computers**, right panel) and click a computer's context menu. Select **View available patches**. The "**Available patches**" will be displayed filtered by the relevant computer.

- To get an overview of all missing patches:
  - Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the **Available patches** list.
  - Use the filter tool to narrow your search.
- To find those computers that don't have a specific patch installed:
  - Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the "**Available patches**".
  - Use the filter tool to narrow your search.
  - Click the context menu of the specific computer-patch and select the option **View which computers have the patch available**.

Isolate computers with unpatched known vulnerabilities

Follow these steps to identify and isolate computers that have not yet received published patches that fix known vulnerabilities:

- Go tb1o top menu **Status**, click **Add** in the **My list** section of the side panel and select the "**Available patches**".
- Click the context menu of a patch in the list and select the **Isolate computer** option.

Download and install the patches

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

> *The patches released by Microsoft won't be installed successfully if the Windows Update service is stopped on the target workstation or server. However, to prevent Panda Patch Management from overlapping with Windows Update, it is recommended that Windows Update be set to be inactive on the computer. Refer to* "**General options**" *for more information.*

Patches and updates are installed via quick tasks and scheduled tasks. Quick tasks install patches in real time but do not restart the target computer, even though this may be required in order to complete the installation process. Scheduled tasks allow you to configure all parameters related to the patch installation operation. Refer to "**Tasks**" on page **507** for more information about tasks in Panda Adaptive Defense.

- **Patch download and bandwidth savings**

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

> *Proxy nodes cannot download patches or updates. Likewise, no patches or updates can be downloaded if the node or computer with the cache/repository role does not have direct access to the Panda Security cloud, or indirect access via a corporate proxy. Refer to* "**Configuring the Panda agent role**" *on page* **208** *for more information about roles in Panda Adaptive Defense.*

Nodes with the cache/repository role store patches for a maximum of 30 days; after then, the patches will be deleted. If a computer requests a patch from a cache node, but the node doesn't have the patch in its repository, the computer will wait for the cache node to download it. The wait time will depend on the size of the patch to download. If the node cannot download the patch, the computer will attempt to download it directly instead.

Once a patch has been applied to a target computer, it will be deleted from the storage media where it resides.

- **Installation task sequence**

Patch installation tasks may require downloading patches from the vendor's servers if the nodes on the network with the cache/repository role don't already have the relevant patches. In this scenario, please note that quick tasks start downloading the necessary patches as soon as they are created.

This may result in high bandwidth usage if those tasks affect many computers or there is a large amount of data to download.

In contrast, scheduled patch installation tasks start downloading the necessary patches when configured in the settings. However, if the start time of multiple tasks coincides, the module will introduce a short random delay of up to 2 minutes to prevent downloads from overlapping and minimize bandwidth usage to a certain extent.

- **Interrupting patch installation tasks**

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

- **Patch download strategies**

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

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

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

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

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

Case 1: from the 'Available patches' list

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

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the "**Available patches**".
- Use the filter tool to narrow your search.
- Click the checkboxes besides the computers-patches you want to install, and select **Install** from the action bar to create a quick task, or **Schedule installation** to create a scheduled task.

Case 2: from the computer tree

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

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

Case 3: from the 'Available patches' list

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

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

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

Case 4: from the computer tree

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

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

Case 5: from the 'Available patches' list

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

- Go to top menu **Status**, click **Add** in the **My list** section of the side panel and select the "Available patches".
- Use the filter tool to find the patch to install.
- Click the checkbox besides the patch to install and click **Schedule installation** to create a task.
- Go to top menu **Tasks** and edit the task you have just created.
- In the **Recipients** field, add the groups that the patch will be applied to (use the **Computer groups** section to do this). Remove any additional computer that may appear in the **Additional computers** section.
- Click **Back**, finish configuring the task and click **Save**.
- Publish the task.

To install multiple specific patches on multiple computer groups, repeat these steps as many times as patches you want to install.

Case 6: from the Tasks top menu

*To manage **Install patches** tasks, the user account used to access the web console must have the **Install, uninstall, and exclude patches** permission assigned to its role. For more information about the permission system implemented in Panda Adaptive Defense, refer to "Understanding permissions" on page 68.*

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

- Go to top menu **Tasks**, click **Add task** and select **Install patches**.
- Set the **Recipients** field, indicating the computers and groups that the patches will be applied to.
- Schedule the task. Refer to "Task schedule and frequency" for more information.
- Specify the criticality level of the patches to install.
- Specify which products will receive patches by selecting the relevant checkboxes in the product tree. Since the product tree is a 'living' resource that changes over time, please keep the following rules in mind when selecting items from the tree:
  - Selecting a node will also select all of its child nodes and all items dependent on them. For example, selecting Adobe will also select all nodes below that node.
  - If you select a node, and Panda Patch Management automatically adds a child node to that branch, that node will be selected as well. For example, as previously explained, selecting Adobe will also select all of its child nodes. In addition to this, if, later, Panda Patch Management adds a new program or family to the Adobe group, that program or family will be selected as well. In contrast to this, if you manually select a number of child nodes from the Adobe group, and later Panda Patch Management adds a new child node to the group, this won't be automatically

selected.

- The programs to patch are evaluated at the time when tasks are run, not at the time when they are created or configured. For example, if Panda Patch Management adds an entry to the tree after the administrator has created a patch task, and that entry is selected automatically in accordance with the rule in the previous point, the task will install the patches associated with that new program when being run.

- Set the restart options in case the target workstations or servers need to be restarted to finish installing the patch.
  - **Do not restart automatically**: upon completing the patch installation task, a window will be displayed to the target computer user with the options **Restart now** and **Remind me later**. If the latter is selected, a reminder will be displayed 24 hours later.
  - **Automatically restart workstations only**: upon completing the patch installation task, a window will be displayed to the target computer user with the **Restart now** option, a **Minimize** button and a 4-hour countdown timer. This window will be maximized every 30 minutes as a reminder to the user. Less than one hour before the restart, the minimize button will be disabled. When the countdown finishes, the computer will restart automatically.
  - **Automatically restart servers only**: this option behaves in the same way as **Automatically restart workstations only**, but applies to servers only.
  - **Automatically restart both workstations and servers**: this option behaves in the same way as **Automatically restart workstations only**, but applies to both workstations and servers.
- Click **Save** and publish the task.

Download patches manually

There are cases in which Panda Patch Management cannot get a download URL to install the required patch automatically. This can happen due to many reasons: the patch requires payment or is not a publicly available patch and requires user registration prior to download, for example. The EULAs that protect certain patches may prevent Panda Security from downloading them for distribution. In those cases, it must be the administrator who manually downloads the patch and shares it across the network for those computers that require it.

Panda Patch Management provides a mechanism for administrators to add manually downloaded patches to the patch repository from the Web console.

To manually add a patch to the repository, you must have the download URL of the patch as provided by the vendor of the product to update. Once you have it, follow the steps below:

- Identify patches that must be manually downloaded.
- Get the download URL from the vendor.
- Integrate the downloaded patch into the patch repository.
- Enable the downloaded patch for installation.
- Optional: Disable a patch for installation

Identify patches that must be manually downloaded

- Go to the **Status** menu at the top of the console and click **Add** from the **My lists** side panel. A list will be shown with all available lists.
- Click the **Available patches** list and configure the following filter:
  - **Installation**: Requires manual download.
  - **Show non-downloadable patches**: Yes.
- Click the **Filter** button. The list will display all patches reported by Panda Patch Management as required to update the computers on the network and which cannot be automatically downloaded.

Get the download URL

- Click one of the patches in the list obtained in step "Identify patches that must be manually downloaded". The patch details will be displayed.
- Click the **Download URL** field to start downloading the patch. Take note of the file name shown in the **File name** field.

Integrate the downloaded patch into the patch repository

- Find a computer on the network that has Panda Adaptive Defense installed and the cache role and copy the downloaded file to the following path:

```
c:\Programdata\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy.
```

If the computer's storage drive is different from the drive set by default in the Panda Adaptive Defense software installation process, go the following path:

```
x:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy
```

Where x is the drive where the computer's repository is located. Refer to "Setting the storage drive" on page 210 for more information.

- If the **ManuallyDeploy** folder does not exist, create it with read and write admin permissions.
- If needed, rename the newly copied patch to the name displayed in the **File name** field mentioned in section "Get the download URL".

Enable the downloaded patch for installation

- After the patch has been copied to the repository, go back to the **Available patches** list and click the context menu of the manually downloaded patch.
- Click the Mark as '**Manually downloaded**' option from the drop-down menu. From then on, the patch's status will change from **Requires manual download** to **Pending (manually downloaded)** for all computers that need to install it. Once the patch's status is **Pending (manually downloaded)**, its

context menu will show all options required to install it just like an automatically downloaded patch. Refer to "**Download and install the patches**".

Panda Patch Management does not check to see if there are patches with the Pending (manually downloaded) status on computers with the cache role. Nor does it check to see whether all computers on the network that require a patch actually have a cache computer assigned that has the patch in its repository. It is the administrator's responsibility to make sure that the cache computers to be used in patch downloads have all necessary manually downloaded files in their ManuallyDeploy folder.

Disable a patch for installation

To remove a patch from the patch repository, follow the steps below:

- Go to the **Available patches** list and configure a filter with the following features:
  - **Installation**: Pending (manually downloaded).
  - **Show non-downloadable patches**: Yes.
- Click the **Filter** button. The list will display all patches manually downloaded and enabled for installation.
- Click the context menu of a patch enabled for installation and select the option Mark as '**Requires manual download**' ☁. From then on, the patch will no longer belong to the repository of installable patches, and the installation options will be removed from its context menu.

Uninstall problematic patches

Sometimes, the patches published by software vendors do not work correctly, which can lead to serious problems. This can be avoided by selecting a small number of test computers prior to deploying a patch across the entire network. In addition to this, Panda Patch Management also lets you remove (roll back) installed patches.

Requirements to uninstall an installed patch

- The administrator must have the **Install/Uninstall patches** permission enabled. Refer to "**Install, uninstall and exclude patches**" for more information.
- The patch must have been successfully installed.
- The patch must support the rollback feature. Not all patches support this feature.

Uninstalling a patch

- Go to the patch uninstallation screen. There are three ways to do this:
  - Go to the **Status** menu at the top of the console, click **Add** in the **My lists** section of the side panel and select the "**Installation history**".

  - Access the list of installed patched via the **Tasks** menu at the top of the console. Select the task that installed the patch you want to uninstall and click the **View installed patches** link in the top-right corner of the screen.
  - Access the “Last patch installation tasks” widget. Then, click the **View installation history** link.

- From the list displayed, select the patch you want to uninstall.
- If the patch can be removed, the **Uninstall the patch** button will be displayed. Click the button to access the computer selection screen.
  - Select **Uninstall from all computers** to remove the patch from all computers on the network.
  - Select **Uninstall from "{{hostName}}" only** to remove the patch from the selected computer only.
- Panda Patch Management will create an immediate execution task to uninstall the patch.
- If a restart is required to finish uninstalling the patch, the solution will wait for the user to restart it manually.

> *Uninstalled patches will be shown again in the lists of available patches, and will be installed again the next time a scheduled patch installation task is run, unless they are excluded. However, if a patch is withdrawn by the corresponding vendor, it will no longer be shown or installed. Refer to “*Exclude patches for all or some computers*”.*

Check the result of patch installation/uninstallation tasks

The **Tasks** menu at the top of the console lets you view those tasks in which patches have been installed or uninstalled from computers. Both provide a **View results** option that lets you view on which computers the action was taken and which patches were installed/uninstalled. For more information, refer tos “Patch installation/uninstallation task results” and “View installed/uninstalled patches”.

Exclude patches for all or some computers

Network administrators have the option to prevent the installation of malfunctioning patches or patches that significantly change the characteristics of the target program. This is called excluding the patch. To exclude a patch, follow the steps below:

- Go to the Status menu at the top of the console. Then, click **Add** from the **My lists** menu on the left. Click the **Available patches** list. This list displays a line for each computer-available patch pair. An available patch is a patch that has not been installed yet on a specific computer or has been uninstalled from it.
- To exclude a single patch, click the context menu associated with the patch ⋮ and select the **Exclude** ⊘ option. A window will open for you to select the exclusion type.
  - **Exclude for X only**: excludes the patch for the selected computer only.
  - **Exclude for all computers**: excludes the patch for all computers on the network.
- To exclude several patches and/or a single patch for multiple computers, select them using the

relevant checkboxes, click the action bar and choose the **Exclude** ⃠ option. A window will open for you to select the exclusion type.

- **Exclude for the selected computers only**: excludes the patches for the selected computers only.
- **Exclude for all computers**: excludes the patches for all computers on the network.

> ⚠ *When you exclude a patch, you exclude a specific version of the patch. That is, if you exclude a patch, and later the software vendor releases a later version of that patch, this won't be automatically excluded.*

Make sure the programs installed are not in EOL (End-Of-Life) stage

Programs in EOL (End-Of-Life) stage do not receive any type of update from the relevant software vendor, therefore it is advisable to replace them with an equivalent program or a more advanced version.

Follow these steps to find those programs on the network that have reached their EOL or will reach it shortly:

- Go to the **Status** menu at the top of the console and click **Patch Management** from the side panel.
- You'll see the "End-of-Life programs" widget, which is divided into the following sections:
  - **Currently in EOL**: programs on the network that do not receive updates from the relevant vendor.
  - **In EOL (currently or in 1 year)**: programs on the network that have reached their EOL, or will reach their EOL in a year.
  - **With known EOL date**: programs on the network with a known EOL date.

Follow these steps to find all programs on your network with a known EOL date:

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel.
- Select the "End-of-Life programs" list.

The list displays a line for each computer-EOL program pair found.

Check the history of patch and update installations

Follow these steps to find out if a specific patch is installed on your network computers:

- Go to top menu **Status** and click **Add** in the **My lists** section in the side panel.
- Select the "Installation history".

The list displays a line for each computer-installed patch pair found, with information about the affected program's or operating system's name and version, and the patch criticality/type.

Check the patch status of computers with incidents

Panda Patch Management correlates those computers where incidents have been recorded with their patch status so that it is possible to determine whether an infected computer or a computer where threats have been detected has missing patches.

To check whether a computer where an incident has been detected has missing patches:

- Go to top menu **Status**, widget **Malware activity**, **PUP activity**, **Exploit activity**, or **Currently blocked programs being classified**, and click a computer-threat. Information about the threat detected on the computer is displayed.
- In the **Affected computer** section, click the **View available patches** button. The **Available patches** list will be displayed, filtered by the relevant computer.
- Select all of the available patches for the computer and click **Install** from the action bar in order to create a quick patch installation task.

*Since the patching process may require downloading patches from the software vendor's servers and therefore delay their application, it is advisable to isolate any infected computer that needs patching and shows network traffic in the threat's 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 "***Forensic analysis***" on page* 451 *for more information about the malware lifecycle. Refer to "***Computer isolation***" on page* 501 *for more information on how to isolate a network computer.*

Configuring the discovery of missing patches

Accessing the settings

- Go to the **Settings** menu at the top of the console and click **Patch management** from the side menu.
- Click the **Add** button to open the **Patch management** settings window.

Required permissions

Permission	Access type
Patch management	Create, edit, delete, copy, or assign 'Patch management' settings.
View patch management settings	View the 'Patch management' settings

Table 14.2: Permissions required to access the 'Patch management' settings

General options

- Click **Disable Windows Update on computers** for Panda Patch Management to manage updates exclusively and without interfering with the local Windows Update settings.

- Click the **Automatically search for patches** switch to enable the patch search functionality. If the switch is not on the ON position, the lists in the module won't display missing patches, although it will still be possible to apply them via the patch installation tasks.

Search frequency

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

Patch criticality

Sets the criticality of the patches that Panda Patch Management will look for.

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

Panda Patch Management widgets and panels

Accessing the dashboard

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

Required permissions

Permissions	Access to widgets
No permissions	• Patch management status • Time since last check
Install, uninstall, and exclude patches	• End-of-Life programs • Available patches • Last patch installation tasks
View available patches	• End-of-Life programs • Available patches • Last patch installation tasks

Table 14.3: Permissions required to access the 'Patch management' widgets

Patch management status

Shows those computers where Panda Patch Management is working properly and those where there have been errors or problems installing or running the module. The status of the module is represented with a circle with different colors and associated counters. The panel offers a graphical representation and percentage of those computers with the same status.

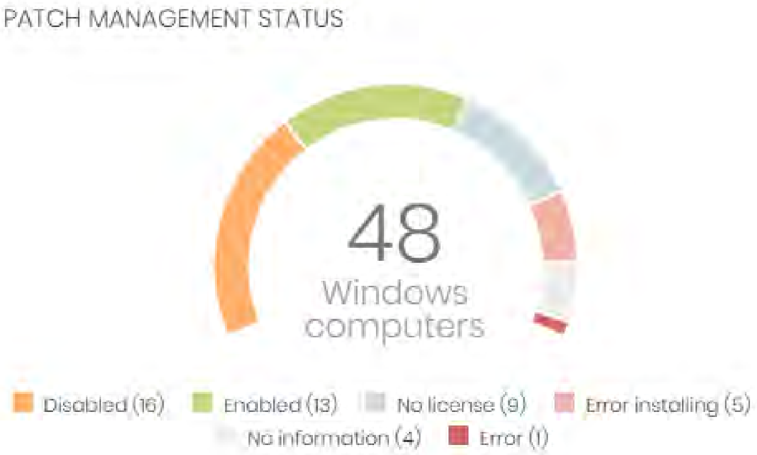


Figure 14.1: 'Patch management status' panel

- **Meaning of the data displayed**

Data	Description
Enabled	Shows the percentage of computers where Panda Patch Management was installed successfully, is running properly and the assigned settings enables the module to search for patches automatically.
Disabled	Shows the percentage of computers where Panda Patch Management was installed successfully, is running properly but the assigned settings prevent the module from searching for patches automatically.
No license	Computers where Panda Patch Management is not working because there are insufficient licenses or because an available license has not been assigned to the computer.
Installation error	Indicates the computers where the module could not be installed.
No information	Computers that have just received a license and haven't reported their status to the server yet, and computers with an outdated agent.
Error	Computers where the Panda Patch Management module does not respond to the requests sent from the server, or its settings are different from those defined in the Web console.
Central area	Shows the total number of computers compatible with the Panda Patch Management module.

Table 14.4: Description of the data displayed in the 'Patch management status'

- **Lists accessible from the panel**

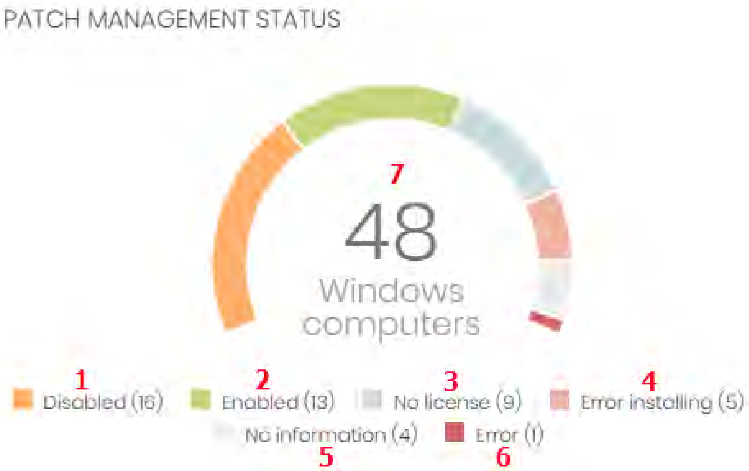


Figure 14.2: Hotspots in the 'Patch management status' panel

Click the hotspots shown in the figure 14.2 to access the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Patch management status = Disabled
(2)	Patch management status = Enabled
(3)	Patch management status = No license
(4)	Patch management status = Installation error
(5)	Patch management status = No information
(6)	Patch management status = Error
(7)	No filters

Table 14.5: Filters available in the ‘Patch management status’ list

Time since last check

Displays computers that have not connected to the Panda Security cloud to report their patch status for a certain amount of time. Such computers are susceptible to security problems and require special attention from the administrator.

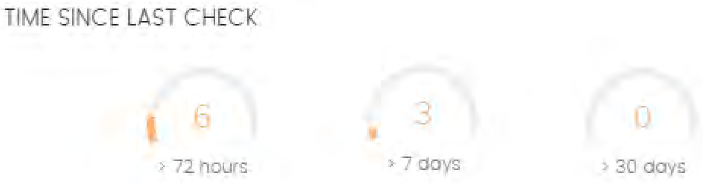


Figure 14.3: 'Time since last check' panel

- **Meaning of the data displayed**

Data	Description
72 hours	Number of computers that have not reported their patch status in the last 72 hours.
7 days	Number of computers that have not reported their patch status in the last 7 days.
30 days	Number of computers that have not reported their patch status in the last 30 days.

Table 14.6: Description of the data displayed in the ‘Time since last check’ panel

- **Lists accessible from the panel**

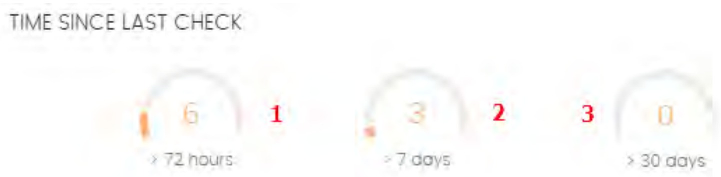


Figure 14.4: Hotspots in the 'Time since last check' panel

Click the hotspots shown in the figure 14.4 to access the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago and Patch management status = Enabled or Disabled or No information or Error.
(2)	Last connection = More than 7 days ago and Patch management status = Enabled or Disabled or No information or Error.
(3)	Last connection = More than 30 days ago and Patch management status = Enabled or Disabled or No information or Error.

Table 14.7: Filters available in the Time since last check' panel

End-of-Life programs

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

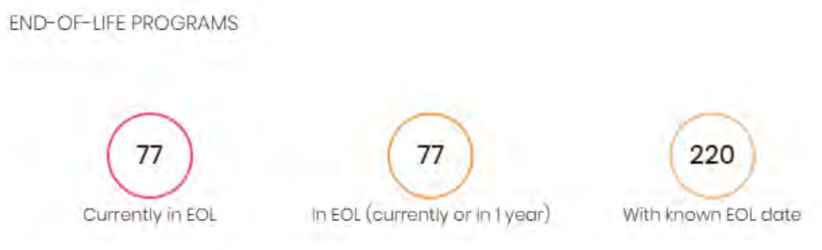


Figure 14.5: 'End-of-Life programs' panel

- **Meaning of the data displayed**

Data	Description
Currently in EOL	Programs on the network that have reached their EOL.
Currently in EOL	Programs on the network that have reached their EOL or will reach it in a year.
With known EOL date	Programs on the network with a known EOL date.

Table 14.8: Description of the data displayed in the ‘End of life’ panel

- **Lists accessible from the panel**

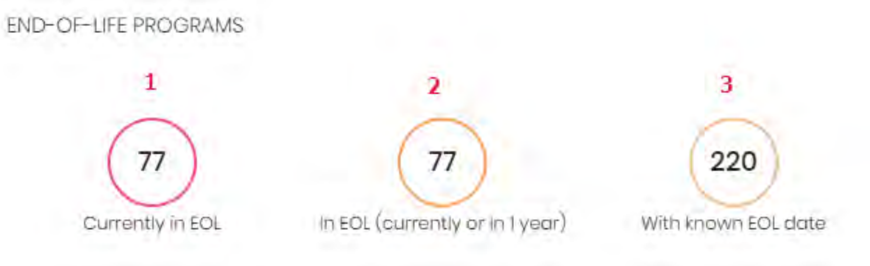


Figure 14.6: Hotspots in the 'End-of-Life programs' panel

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

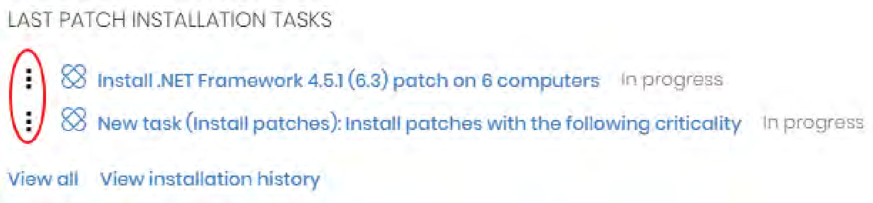
Hotspot	Filter
(1)	End-of-Life date = Currently in EOL
(2)	End-of-Life date = In EOL (currently or in 1 year)
(3)	End-of-Life date = All

Table 14.9: Filters available in the "End Of Life’ list

Last patch installation tasks

Refer to "Task management" on page 513 for more information on how to edit an existing task.

Shows a list of the last patch installation tasks created. This widget displays multiple links through which you can manage the patch installation tasks:



LAST PATCH INSTALLATION TASKS

Install .NET Framework 4.5.1 (6.3) patch on 6 computers In progress

New task (Install patches): Install patches with the following criticality In progress

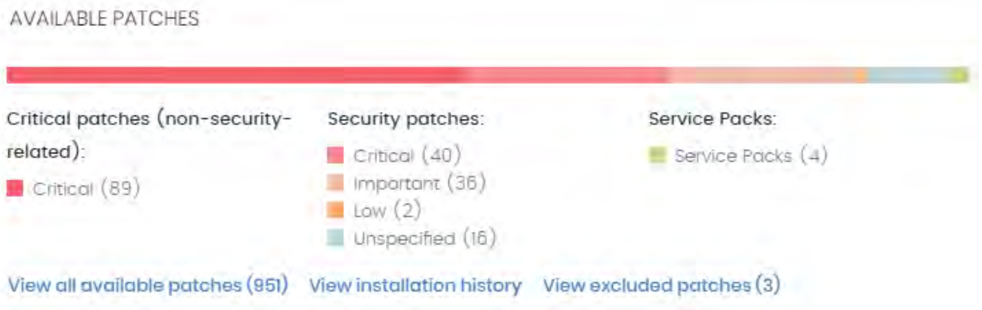
View all View installation history

Figure 14.7: 'Last patch installation tasks' panel

- Click a task to edit its settings.
- Click the **View all** link to access the top menu **Tasks**. There you'll see all the tasks that have been created.
- Click the **View installation history** link to access the **Installation history** list. There you'll see the patch installation tasks that have finished successfully or with errors.
- Click the context menu associated with a task to display a drop-down menu with the following options:
  - **Cancel**: interrupts the task before starting to install patches on the target computer.
  - **View results**: shows the task results.

Available patches

Shows the number of computer-missing patch pairs on the network, sorted by patch type. Each missing patch is counted as many times as there are computers that don't have it installed.



AVAILABLE PATCHES

Critical patches (non-security-related):

🟥 Critical (89)

Security patches:

🟥 Critical (40)

🟧 Important (36)

🟧 Low (2)

🟦 Unspecified (16)

Service Packs:

🟩 Service Packs (4)

View all available patches (951) View installation history View excluded patches (3)

Figure 14.8: 'Available patches' panel

- **Meaning of the data displayed**

Data	Description
Security patches - Critical	Number of security patches rated 'critical' and pending application
Security patches - Important	Number of security patches rated 'important' and pending application
Security patches - Low	Number of security patches rated 'low' and pending application
Security patches – Unspecified	Number of security patches that don't have a severity rating and are pending application
Other patches (non-security-related)	Number of non-security patches that are pending application
Service Packs	Number of patch and hotfix bundles that are pending application
View all available patches	Number of patches of any severity, related or not to system security and which are pending application

Table 14.10: Description of the data displayed in the 'Available patches' panel

- **Lists accessible from the panel**

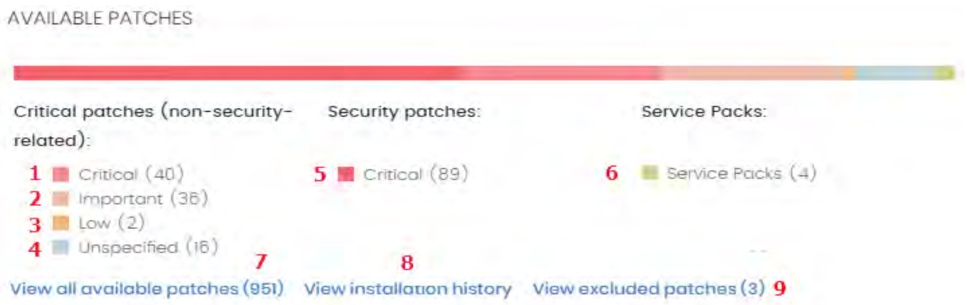


Figure 14.9: Hotspots in the 'Available patches' panel

Clicking the hotspots shown in figure 14.9 will open lists with the following predefined filters:

Hotspot	List	Filter
(1)	Available patches	Criticality = Critical (security-related)
(2)	Available patches	Criticality = Important (security-related)
(3)	Available patches	Criticality = Low (security-related)
(4)	Available patches	Criticality = Unspecified (security-related)
(5)	Available patches	Criticality = Other patches (non-security-related)
(6)	Available patches	Criticality = Service Pack

Table 14.11: Filters available in the 'Available patches' list

Hotspot	List	Filter
(7)	Available patches	No filters.
(8)	Installation history	No filters.
(9)	Excluded patches	No filters.

Table 14.11: Filters available in the ‘Available patches’ list

Panda Patch Management module lists

Accessing the lists

There are two ways to access the lists:

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

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window will open with all available lists.
- Select a list from the **Patch management** section to view the associated template. Edit it and click **Save**. The new list will be added to the side menu.

The patch installation and uninstallation lists can be accessed from the **Last patch installation tasks** widget by clicking **View installation history**.

The **Patch installation/uninstallation task results** and **View installed/uninstalled patches** lists can be accessed from the **Task** menu at the top of the console by clicking **View results** in a patch installation or uninstallation task.

Required permissions

Permissions	Access to lists
No permissions	• Patch management status
Install, uninstall, and exclude patches	Access to lists and context menus to install and uninstall patches: • Available patches • Installation history • End-of-Life programs • Excluded patches • Patch installation/uninstallation task results • View installed/uninstalled patches

Table 14.12: Permissions required to access the ‘Patch management’ lists

Permissions	Access to lists
View available patches	Read-only access to lists: • Available patches • Installation history • End-of-Life programs • Excluded patches • Patch installation/uninstallation task results • View installed/uninstalled patches

Table 14.12: Permissions required to access the 'Patch management' lists

Patch management status

This list shows all computers on the network that are compatible with Panda Patch Management (with filters to allow administrators to identify those workstations and servers that are not using the service due to one of the reasons displayed in the associated panel).

Field	Comments	Values
Computer	Name of the computer with outdated software.	Character string
Computer status	Agent reinstallation: • ⚙ Reinstalling the agent. • ⚙ Agent reinstallation error Protection reinstallation: • ⚙ Reinstalling the protection. • ⚙ Protection reinstallation error. • ↻ Pending restart.	Icon
	Computer isolation status: • 🖥 Computer in the process of being isolated. • 🖥 Isolated computer. • 🖥 Computer in the process of stopping being isolated	

Table 14.13: Fields in the 'Patch management status' list

Field	Comments	Values
	“RDP attack containment” mode: • 👤 Computer in “RDP attack containment” mode. • 👤 Ending "RDP attack containment" mode	
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Patch management	Module status.	• ✓ Enabled • ⊖ Disabled • ⊗ Installation error (failure reason) • ☒ No license • — No information • ⊗ Error
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date
Last connection	Date when the Panda Adaptive Defense status was last reported to the Panda Security cloud.	Date

Table 14.13: Fields in the 'Patch management status' list

*To view a graphical representation of the list data, go to widget “**Patch management status**”.*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
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

Table 14.14: Fields in the 'Patch management status' exported file

Field	Comments	Values
Group	Folder in the Panda Adaptive Defense 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
Operating system	Operating system installed on the computer, internal version and patch status.	Character string
Protection updated	Indicates whether the installed protection has the latest released version.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date when the signature file was last updated.	Date
Patch management status	Module status.	• Enabled • Disabled • Installation error • No license • No information • Error
Requires restart	The computer requires a reboot to finish installing one or more downloaded patches.	Boolean
Last check date	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	Date
Isolation status	Indicates if the computer has been isolated or can communicate normally with all other computers on the network.	• Isolated • Not isolated
Installation error date	Date when the administrator attempted to install the Panda Patch Management module and the operation failed.	Date
Installation error	Failure reason	• Download error • Execution error

Table 14.14: Fields in the 'Patch management status' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Last checked	Date when Panda Patch Management last queried the cloud to check whether new patches had been published.	• All • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the agent last connected to the Panda Security cloud	Date
Pending restart to complete patch installation	The computer requires a reboot to finish installing one or more downloaded patches.	Boolean
Patch management status	Module status.	• Enabled • Disabled • Installation error • No license • No information • Error

Table 14.15: Filters available in the 'Patch management status' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "**Computer details**" on page 172 for more information.

Available patches

Shows a list of all missing patches on the network computers and published by Panda Security. Each line in the list corresponds to a patch-computer pair.

Field	Comments	Values
Computer	Name of the computer with outdated software.	Character string
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Table 14.16: Fields in the 'Available patches' list

Field	Comments	Values
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Indicates the patch installation status: • **Pending**: the patch is available for the computer but hasn't been installed yet. • **Requires manual download**: the patch must be manually downloaded and copied to a cache computer by the administrator. Refer to "**Download patches manually**". • **Pending (manually downloaded):** the patch has been manually downloaded and is already included in the patch repository. Refer to "**Download patches manually**". • **Pending restart:** the patch has been installed but the computer has not been restarted. Some patches may not be applied until the computer is restarted.	
Context menu	Displays an actions menu: • **Install**: lets you create a quick task to immediately install the patch on the computer. • **Schedule installation**: lets you create a scheduled task to install the patch on the computer. • **Isolate computer**: lets you isolate the computer from the network. • **View all available patches for the computer**: displays all available patches for the computer that have not been installed yet. • **View which computers have the patch available**: displays all computers that have the patch available for installation.	

Table 14.16: Fields in the 'Available patches' list

*To view a graphical representation of the list data, go to widget "***Available patches***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer with outdated software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Group	Folder in the Panda Adaptive Defense 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
Date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.17: Fields in the 'Available patches' exported file

Field	Comments	Values
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Last seen	Date when the computer was last discovered.	Date
Is downloadable	Indicates if the patch is available for download or requires an additional support contract with the software vendor in order to have access to it.	Boolean
Download size (KB)	Patch size in compressed format. Applying the patch may require more space on the target computer's storage media than indicated in this field.	Numeric value
Status	Indicates the patch installation status: • **Pending**: the patch is available for the computer but hasn't been installed yet. • **Requires manual download**: the patch must be manually downloaded and copied to a cache computer by the administrator.Refer to "**Download patches manually**". • **Pending (manually downloaded)**: the patch has been manually downloaded and is already included in the patch repository.Refer to "**Download patches manually**".	Character string
File name	Name of the file that contains the patch.	Character string
Download URL	HTTP resource for downloading the patch in the software vendor's infrastructure.	Character string

Table 14.17: Fields in the 'Available patches' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Find computer	Computer name.	Character string
Computer	Name of the computer with outdated software.	Character string

Table 14.18: Filters available in the 'Available patches' list

Field	Comments	Values
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Displays patches that are in the process of installation, filtering them by the installation stage they are in.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Show non-downloadable patches	Shows those patches that cannot be directly downloaded by Panda Patch Management as there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.)	Boolean

Table 14.18: Filters available in the 'Available patches' list

- **'Patch detected' window**

Click any of the rows in the list to open the **Patch detected** window. This window can provide the following content:

- Information about the available patch and the **Install patch** button.
- Information about the patch in the process of installation. The text **Pending restart** appears next to the **Install patch** button.

Click the **Install patch** button. A pop-up window appears for you to select the recipients of the patch installation task:

- **The current computer:** the task will have the computer selected in the list as recipient.
- **Install on all computers in the selected filter**: select a filter from the filter tree displayed. The patch will be installed on all computers in the selected filter.
- **Install on all computers:** the patch will be installed on all computers on the network.

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer	Name of the computer with outdated software.	Character string
Installation status	Indicates if the patch is already included in the repository that contains the patches to be applied to computers or if it must be manually downloaded and added to the patch repository by the administrator.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update may require more space on the target computer's storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its installation requirements (if any).	Character string
Download URL	URL for downloading the patch individually.	Character string
File name	Name of the file that contains the patch.	Character string

Table 14.19: Fields in the 'Patch detected' window

End-of-Life programs

Shows programs that are no longer supported by the relevant vendor. These programs are particularly vulnerable to malware and cyberthreats.

Field	Comments	Values
Computer	Name of the computer with EOL software.	Character string
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program entered its EOL stage.	Date (in red if the program has reached its EOL).

Table 14.20: Fields in the 'End-of-Life programs' list

*To view a graphical representation of the list data, go to widget "***End-of-Life programs***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program entered its EOL stage.	Date
Last seen	Date when the computer was last discovered.	Date

Table 14.21: Fields in the 'End-of-Life programs' exported file

- **Filter tool**

Field	Comments	Values
Find computer	Computer name.	Character string
End-of-Life date	Date when the program will reach its EOL.	• All • Currently in End of Life • In End of Life (currently or in 1 year)

Table 14.22: Filters available in the 'End-of-Life programs' list

- **'Program details' window**

Clicking any of the programs in the list opens the **Program details** window.

Field	Comments	Values
Program	Name of the program or Windows operating system that reached its end of life.	Character string
Family	Bundle, suite, or program group the software belongs to.	Character string
Publisher/ Company	Company that designed or published the program.	Character string
Version	Program version.	Character string
EOL	Date when the program reached its end of life.	Date

Table 14.23: Fields in the 'Program details' window

Installation history

Shows the patches that Panda Patch Management attempted to install and the computers that received them in a given time interval.

Field	Comments	Values
Date	Date when the patch or update was installed.	Date
Computer	Name of the computer that received the patch or update.	Character string
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Program	Name of the program or Windows operating system that received the patch or update.	Character string
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	Character string

Table 14.24: Fields in the 'Installation history' list

Field	Comments	Values
Criticality	Severity rating of the installed patch.	• Other patches • Critical • Important • Moderate • Low • Unspecified • Service Pack
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • Uninstalled • The patch is no longer required
Context menu	Displays a drop-down menu with options.	• **View task**: shows the settings of the patch installation or uninstallation task.

Table 14.24: Fields in the 'Installation history' list

*To view a graphical representation of the list data, go to widget "***Last patch installation tasks***".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Client account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Date	Date of the installation attempt.	Date
Program	Name of the program or Windows operating system that received the patch or update.	Character string

Table 14.25: Fields in the 'Installation history' exported file

Field	Comments	Values
Version	Version of the program or operating system that received the patch.	Character string
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the installed patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Installation error	The Panda Patch Management module didn't install correctly	• **Unable to download**: Installer not available • **Unable to download**: The file is corrupted • **Not enough disk space**
Download URL	URL for downloading the patch individually.	Character string
Result code	Code indicating the result of the patch installation task. Success or reason for failure. Refer to the vendor's documentation for more information on how to interpret the result code	Numeric value

Table 14.25: Fields in the 'Installation history' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Find computer	Computer name.	Character string
From	Start date for the search range.	Date
To	End date for the search range.	Date
Criticality	Severity rating of the installed patch.	• Critical (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Installation status of the patch or update.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string

Table 14.26: Filters available in the 'Installation history' list

- **'Patch installed' window**

Clicking any of the rows in the list opens the Patch installed window. This window provides detailed information about the patch.

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Table 14.27: Fields in the 'Patch installed' window

Field	Comments	Values
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	- Other patches (non-security-related) - Critical (security-related) - Important (security-related) - Moderate (security-related) - Low (security-related) - Unspecified (security-related) - Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Installation date	Date the patch was successfully installed on the computer.	Date
Result	Installation status of the patch or update.	- Installed - Requires restart - Error - The patch is no longer required - Uninstalled
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update may require more space on the target computer's storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its installation requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 14.27: Fields in the 'Patch installed' window

Excluded patches

This list shows those patches that the administrator has excluded, preventing them from being installed on the computers on the organization's network. The list displays a line for each computer-excluded patch pair, except in the case of those patches excluded for all computers on the network, for which a single line is displayed.

Field	Comments	Values
Computer	The content of this field will vary depending on the target of the exclusion: • 🖥 If the patch was excluded for a single computer, the field will display the computer name. • 🌐 If the patch was excluded for all computers in the account, the text "(All)" will be displayed.	Character string
Group	Folder in the Panda Adaptive Defense group tree to which the computer belongs.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the excluded patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Excluded by	Management console user account who excluded the patch	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.28: Fields in the 'Excluded patches' list

*To view a graphical representation of the list data, go to widget "**Available patches**".*

- **Fields displayed in the exported file**

Field	Comments	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	The content of this field will vary depending on the target of the exclusion: • If the patch was excluded for a single computer, the field will display the computer name. • If the patch was excluded for all computers in the account, the text "(All)" will be displayed.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	The computer's description entered by the network administrator.	Character string
Group	Folder in the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the excluded patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its requirements (if any).	Character string

Table 14.29: Fields in the 'Excluded patches' exported file

Field	Comments	Values
Release date	Date when the patch was released for download and application.	Date
Download size (KB)	Patch size in compressed format. Applying the patch may require more space on the target computer's storage media than indicated in this field.	Numeric value
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.29: Fields in the 'Excluded patches' exported file

- **Filter tool**

Field	Comments	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer for which patches have been excluded.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Show non-downloadable patches	Shows those patches that cannot be directly downloaded by Panda Patch Management as there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.)	Boolean
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Criticality	Severity rating of the excluded patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related)

Table 14.30: Filters available in the 'Excluded patches' list

Field	Comments	Values
		• Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.30: Filters available in the 'Excluded patches' list

- **'Excluded patch' window**

Clicking any of the rows in the list opens the **Excluded patch** window. This window provides detailed information about the patch excluded from installation tasks.

Field	Comments	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or Windows operating system with missing patches.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related)
		• Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update may require more space on the target computer's storage media than indicated in this field.	Numeric value

Table 14.31: Fields in the 'Excluded patch' window

Field	Comments	Values
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and its installation requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 14.31: Fields in the 'Excluded patch' window

Patch installation/uninstallation task results

This list shows the results of the patch installation or uninstallation tasks performed on the computers on your network.

Field	Description	Values
Name	Name of the computer the patch was installed/ uninstalled from.	Character string
Group	Panda Adaptive Defense group to which the computer belongs.	Character string
Status	Task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Patches installed/ uninstalled	Number of patches installed/uninstalled.	Character string.
Start date	Date the installation task started.	Date
End date	Date the installation task ended.	Date

Table 14.32: Fields in the 'Installation/uninstallation task results' list

*To view a graphical representation of the list data, go to widget "***Last patch installation tasks***".*

- **Filter tools**

Field	Description	Values
Status	Installation/uninstallation task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Applied/ Uninstalled patches	Computers on which patches have been installed/uninstalled.	• All • No patches installed/uninstalled • With patches installed/uninstalled

Table 14.33: Filters available in the 'Patch installation/uninstallation task results' list

View installed/uninstalled patches

This list shows the patches installed on computers and other additional information.

Field	Description	Values
Computer	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Panda Adaptive Defense group to which the computer belongs.	Character string
Program	Patched program.	Character string
Version	Program version.	Character string
Patch	Installed/uninstalled patch.	Character string
Criticality	Relevance of the installed/uninstalled patch.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.34: Fields in the 'View installed/uninstalled patches' list

Field	Description	Values
Result	Indicates if the task was completed successfully or failed.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Date	Date the task was run.	Date

Table 14.34: Fields in the 'View installed/uninstalled patches' list

*To view a graphical representation of the list data, go to widget "***Last patch installation tasks***".*

Chapter 15

Panda Full Encryption (Device encryption)

Panda Full Encryption is a built-in module on Aether Platform that encrypts the content of the data storage media connected to the computers managed by Panda Adaptive Defense. By doing this, it minimizes the exposure of corporate data in the event of data loss or theft as well as when storage devices are removed without having deleted the data.

Panda Full Encryption is compatible with Windows 7 and later versions of the OS (see section "**Supported operating system versions**") and enables you to monitor the encryption status of network computers and centrally manage the corresponding recovery keys. It also takes advantage of hardware resources such as TPM, delivering great flexibility when it comes to choosing the optimum authentication system for each computer.

For more information about the different features of the Panda Full Encryption module, see the following sections:

- "**Creating and managing settings**": information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**": managing user accounts and assigning permissions.
- "**The management console**": information on how to manage lists.

CHAPTER CONTENT

Introduction to encryption concepts

Panda Full Encryption uses the tools integrated in Windows operating systems to manage encryption on network computers protected with Panda Adaptive Defense.

In order to understand the processes involved in the encryption and decryption of information, we will first present some concepts related to the encryption technology used.

TPM

TPM (Trusted Platform Module) is a chip included in the motherboards of some desktops, laptops and servers. Its main aim is to protect users’ sensitive data, stored passwords and other information used in login processes.

The TPM is also responsible for detecting changes in the chain of startup events on a computer, for example preventing access to a hard drive from a computer other than the one used for its encryption.

The minimum version of TPM supported by Panda Full Encryption is 1.2. and Panda Security recommends it is used along with other supported authentication systems. The TPM may be disabled in the computer BIOS in some scenarios and it may be necessary to enable it manually.

Supported password types

- **PIN**

The PIN (Personal Identification Number) is a sequence of numbers that serves as a simple password and is necessary to start a computer with an encrypted drive. Without the PIN, the boot sequence is not completed and it is impossible to access the computer.

- **Extended PIN**

If the hardware is compatible, Panda Full Encryption uses an extended or enhanced PIN combining letters and numbers to increase the complexity of the password.

Given that the extended PIN is required in the process of starting up the computer, before the operating system is loaded, the limitations of the BIOS may restrict access from the keyboard to the 7-bit ASCII table. Moreover, keyboards other than EN-US, such as QWERTZ or AZERTY keyboards, may lead to errors when entering the extended PIN. For this reason, Panda Full Encryption checks that the characters entered by users belong to the EN-US charset before setting the extended PIN in the process of encrypting the computer.

- **Passphrase**

A passphrase is similar to a password, but is typically longer. It consists of alphanumeric characters and is equivalent to the extended PIN.

Panda Full Encryption prompts users for a different type of password based on the following circumstances:

- **Passphrase**: if the computer has a TPM installed.
- **Extended PIN**: if the computer operating system and hardware support it.
- **PIN**: if the other options are not valid.

USB key

This allows you to store the encryption key on a USB device formatted with NTFS, FAT or FAT32. This means that you don't have to enter any password to start up the computer, but you do need to connect the USB device.

Some older PCs cannot access USB devices during the startup process. Check whether the computers in your organization have access to USB devices from the BIOS.

Recovery key

When an irregular situation is detected on a computer protected by Panda Full Encryption, or if you forget the password, the computer will ask you for a 48-digit recovery key. This password is managed from the management console and must be entered in order to complete the startup process in these circumstances. Each encrypted drive will have its own specific recovery key.

Panda Full Encryption *only stores the recovery keys for the computers it manages. The management console will not display the passwords for computers encrypted by users or those not managed by Panda Security.*

The recovery key will be requested in the following circumstances:

- When the PIN or passphrase is entered incorrectly repeatedly in the startup process.
- When a computer protected with TPM detects a change to the startup sequence (hard disk protected with TPM and connected to another computer).
- When the motherboard has been changed and consequently the TPM.
- On disabling or deleting the TPM content.
- On changing the startup settings.
- When the startup process is changed:
  - BIOS update.
  - Firmware update.
  - UEFI update.
  - Changes to the boot sector.
  - Changes to the master boot record.
  - Changes to the boot manager.
  - Changes to the firmware in certain components that take part in the boot process (video cards, disk controllers, etc), known as the Option ROM.
  - Changes to other components that take part in the initial startup phases.

BitLocker

This is the software installed on some versions of Windows 7 and later and which is responsible for encrypting and decrypting the data stored on the computer drives. Panda Full Encryption installs BitLocker automatically on those server versions that do not have it but are compatible.

System partition

This is a small area of the hard disk -approximately 1.5 gigabytes- which is unencrypted and is required for the computer to correctly complete the startup process. Panda Full Encryption automatically creates this system partition if it does not already exist.

Encryption algorithm

The encryption algorithm in Panda Full Encryption is AES-256, though computers with drives encrypted by users with other algorithms are also compatible.

Panda Full Encryption service overview

The general encryption process covers several areas that administrators should be aware of in order to adequately manage network resources that could contain sensitive information or compromising data if the drive were to be lost or stolen:

- **Meeting minimum hardware and software requirements:** See section "**Panda Full Encryption minimum requirements**" to see the limitations and specific conditions of each supported platform.
- **Previous encryption status of the user's computer**: Depending on whether BitLocker was used before on the user's computer, the process of integration in Panda Adaptive Defense may vary slightly.
- **Assigning encryption settings**: Determine the encryption status (encrypted or not) of network computers and the authentication methods.
- **Interaction of the user with the encryption process:** The initial encryption process requires user interaction. See section "**Encryption of previously unencrypted drives**".
- **Viewing the network encryption status** with the widgets/panels in the **Status** menu, **Full Encryption** side panel. See section "**Panda Full Encryption panels and widgets**" for a complete description of the widgets included in Panda Full Encryption. Filters are also supported to locate computers in the lists according to their status. See section "**Available filters**".
- **Restriction of encryption permissions to security administrators**: The roles system described in "**Understanding permissions**" on page **68** covers the functionality of the encryption module and viewing of the status of network computers.
- **Access to the recovery key**: Where users forget the PIN/passphrase or when the TPM has detected an irregular situation, the network administrator can centrally obtain the recovery key and send it to the user. See section "**Getting the recovery key**"

General features of Panda Full Encryption

Supported authentication types

Depending on whether there is a TPM and on the OS version, Panda Full Encryption allows different combinations of authentication methods. These are as follows, and in the order that they are recommended by Panda Security:

- **TPM + PIN**: compatible with all supported versions of Windows. The TPM chip must be enabled in the BIOS and a PIN must be established.
- **Only TPM**: compatible with all supported versions of Windows. The TPM chip must be enabled in the BIOS except in Windows 10, where it is automatically enabled.
- **USB key**: requires a USB device and that the computer can access USB drives during startup. Required on Windows 7 computers without TPM.
- **Passphrase**: only available on Windows 8 and later without TPM.

By default, Panda Full Encryption uses an encryption method that includes the use of the TPM if available. If you choose an authentication routine not included in the above list, the management console will display a warning indicating that the computer will not be encrypted.

Supported storage devices

Panda Full Encryption encrypts all internal mass storage devices:

- Fixed storage drives on the computer (system and data)
- Virtual hard drives (VHD), though only used space, regardless of what appears in the management console.
- Removable hard drives.
- USB drives.

The following are not encrypted:

- Dynamic hard disks.
- Very small partitions.
- Other external storage devices.

Panda Full Encryption minimum requirements

The minimum requirements are split into:

- Versions of the Windows operating system and compatible families.
- Hardware requirements.

Supported operating system versions

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows Server 2008 R2 and later (including Server Core editions)

Hardware requirements

- TPM 1.2 and later if this method of authentication is used.
- USB key and computer that supports reading USB devices from the BIOS in Windows 7.

Management of computers according to their prior encryption status

Management of computers by Panda Full Encryption

For a computer to be managed by Panda Full Encryption, it must meet the following conditions:

- It must meet the minimum requirements described in section "**Panda Full Encryption minimum requirements**".
- The computer must have successfully received, at least once, settings from the management console that establish the encryption of the drives.

Computers that previously had some drives encrypted and have not received settings to encrypt their drives will not be managed by Panda Full Encryption and, therefore, the administrator will not have access to the recovery key or the status of the computer.

However, computers that have received settings to encrypt drives, regardless of their previous status (encrypted or not) will be managed by Panda Full Encryption.

Uninstallation of the Panda Adaptive Defense agent

Regardless of whether the computer was managed by Panda Full Encryption or not, if the drives were encrypted, when uninstalling Panda Adaptive Defense they will be left as they are. However, centralized access to the recovery key will be lost.

If the computer is subsequently reinstated in Panda Adaptive Defense, the last stored recovery key will be displayed.

Encryption and decryption

Encryption of previously unencrypted drives

The encryption process starts when the Panda Adaptive Defense agent installed on the user's computer downloads Encryption settings. At that moment, the user will see a window that will guide them through the process.

The total number of steps involved varies depending on the type of authentication chosen by the administrator and the previous status of the computer. If any of the steps ends in an error, the agent will report it to the management console and the process will stop.

It is not permitted to encrypt computers from a remote desktop session as it is necessary to restart the computer and enter a password before loading the operating system, actions that are not possible with a standard remote desktop tool.

The encryption process will begin when installation or uninstallation of patches run by Panda Full Encryption has finished.

Below we describe the complete encryption process and whether feedback is displayed to the computer user and if a restart is required:

Step	Process on the computer	User interaction
1	The agent receives the settings from the encryption module, which asks for the content of the storage drives installed to be encrypted.	None.
2	If the computer is a server and does not have BitLocker tools installed, they are downloaded and installed.	A window is displayed requesting permission to restart the computer and complete installation of BitLocker or to postpone the process. If 'postpone' is selected, the request will be made again during the next login. **Requires restart.**
3	If the computer wasn't previously encrypted, the system partition is created.	A window appears asking for permission to restart the computer and complete the creation of the system partition or postpone it. If 'postpone' is selected, the process will be stopped and the user will be asked again during the next login. **Requires restart.**

Table 15.1: Steps for encrypting previously unencrypted drives

Step	Process on the computer	User interaction
4	If there is a group policy previously established by the administrator and which conflicts with those set by Panda Full Encryption, an error message will appear and the process will stop. The group policies configured by Panda Full Encryption are: In the local group policy editor, follow this path: Local computer policy > Computer configuration > Administrative templates > Windows components > BitLocker drive encryption > Operating system drives. Select Not set for the specified policies to avoid this error.	If the administrator has not defined global group policies that conflict with the local ones defined by Panda Full Encryption, no message will appear.
5	Preparing the TPM if it exists, and whether the authentication method selected requires this component and whether it was previously enabled from the BIOS.	This requires confirming a restart so that the user can enter the BIOS on the computer to enable the TPM. In Windows 10 there is no need to alter the BIOS but restart is required. The restart in step 3, if required, will combine with this one.
6	Preparing the USB device if the authentication method selected requires this component.	This requires users to plug in a USB device to store the password for starting the computer.
7	Storing the PIN if the authentication method selected requires this component.	The user is required to enter the PIN. If alphanumeric characters are used and the hardware is not compatible with those characters, error "-2144272180" will be displayed. In that case, a numerical PIN must be entered.
8	Storing the passphrase if the authentication method selected requires this component.	The user is required to enter the passphrase.
9	The recovery key is generated and sent to the Panda Security cloud. Once it has been received, the process continues on the user's computer.	None.
10	Checking that the hardware on the computer is compatible with the encryption technology. The encryption process begins.	Confirmation of restart is required in order to check the hardware used in the various authentication methods. **Requires restart.**
11	Encryption of drives.	The encryption process begins and runs in the background, without interfering with the user. The length of the process will depend on the drive being encrypted. On average, the encryption time will be about 2-3 hours.

Table 15.1: Steps for encrypting previously unencrypted drives

Step	Process on the computer	User interaction
		Users can use and switch off computers. In the latter case, the process will continue whenever the computer is restarted.
12	The encryption process takes place silently and from then on is completely invisible to the user.	Depending on the authentication method selected, the user may need to enter a USB key, a PIN, a passphrase or nothing at all when the computer restarts.

Table 15.1: Steps for encrypting previously unencrypted drives

Encryption of previously encrypted drives

If any drive on the computer is already encrypted, Panda Full Encryption will alter certain parameters so that it can be centrally managed. The action taken is as follows:

- If the authentication method chosen by the user does not coincide with the one specified in the settings, the latter will change, and the user will be asked for the necessary passwords or hardware resources. If it is not possible to assign an authentication method compatible with the platform and specified by the administrator, the computer will continue using the user's encryption and will not be managed by Panda Full Encryption.
- If the encryption algorithm used is not supported (not AES-256), no change will take place to avoid complete decryption and encryption of the drive but the computer will be managed by Panda Full Encryption.
- If there are both encrypted and unencrypted drives, all drives will be encrypted with the same authentication method.
- If the previous authentication method required a password to be entered, and is compatible with the methods supported by Panda Full Encryption, the user will be asked for the password in order to unify the authentication method in all drives.
- If the user chose encryption settings different from those set by the administrator (encryption solely of the occupied sectors not the whole drive), no changes will be made in order to minimize the encryption process.
- At the end of the process, the device will be managed by Panda Full Encryption. A recovery key will be generated and sent to Panda Security's cloud.

Encryption of new drives

If a user creates a new drive after the encryption process is complete, Panda Full Encryption will encrypt it immediately, respecting the encryption settings assigned by the network administrator.

Decrypting drives

There are three scenarios:

- If Panda Full Encryption encrypts a computer, from that moment the administrator can assign settings to decrypt it.

- If a computer was encrypted by the user prior to the installation of Panda Full Encryption and is assigned encryption settings, it will be considered encrypted by Panda Full Encryption and can be decrypted by assigning settings from the management console.
- If a computer was already encrypted by the user prior to installing Panda Full Encryption and has never been assigned encryption settings, it will not be considered encrypted by Panda Full Encryption and cannot be decrypted by assigning settings from the management console.

Local editing of BitLocker settings

The computer user has access to the local BitLocker settings from the Windows tools, but the changes made will immediately revert to the settings established by the network administrator through the management console. The way that Panda Full Encryption responds to a change of this type is described below:

- **Disable automatic locking of a drive**: It reverts to automatic locking.
- **Eliminate the password of a drive**: A new password will be requested.
- **Decrypt a drive previously encrypted by** Panda Full Encryption: The drive will automatically be encrypted.
- **Encrypt a decrypted drive**: If the Panda Full Encryption settings imply decrypting drives, the user action takes preference and the drive won’t be decrypted.

Encrypting and decrypting external hard drives and USB keys

As users can connect and disconnect external storage devices from their computers at any time, the way Panda Full Encryption works with these devices is as follows:

- If the workstation or server does not have BitLocker installed and running, the agent will not download the required packages and the device will not be encrypted. Nor will any messages be displayed to the user.
- If the computer has BitLocker installed and running, a pop-up message will be displayed to the user prompting them to encrypt the device in the following situations:
  - Every time they connect an unencrypted USB storage device.
  - If there is an unencrypted device connected to the computer at the time the administrator enables the encryption settings from the Web console.
- The encryption message will be displayed to the user for 5 minutes, after which it will disappear. Regardless of whether the user agrees to encrypt the device or not, they will be able to use the device normally, unless settings have been configured that prevent the use of unencrypted devices. Refer to “**Write to removable storage drives**” on page **253**.
- Encrypting a USB device does not require creating a system partition.
- If the external storage device is already encrypted by a solution other than Panda Full Encryption, and the user connects it to their computer, the encryption message will not be displayed and the device can be used normally. Panda Full Encryption will not send the recovery keys to the Web

console.

- Writing to the USB device won't be allowed if the option **Write to removable storage drives** in Panda Data Control is set to ON and the device has not bee encrypted by BitLocker or by Panda Full Encryption. Refer to "**Write to removable storage drives**".
- To decrypt a device encrypted by Panda Full Encryption, the user can use BitLocker manually.
- Only the space used is encrypted.
- All partitions on the device are encrypted with the same key.

⚠ *Removing a USB device when the encryption process is not complete might corrupt its contents*

Panda Full Encryption response to errors

- **Errors in the hardware test**: The hardware test runs every time the computer is started up until it is passed, at which time the computer will automatically begin encryption.
- **Error creating the system partition**: Many of the errors that occur when creating the system partition can be rectified by the user (e.g. lack of space). Periodically, Panda Full Encryption will automatically attempt to create the partition.
- **User refusal to activate the TPM chip**: The computer will display a message on startup asking the user to activate the TPM chip. Until this condition is resolved, the encryption process will not commence.

Getting the recovery key

In cases where the user has lost the PIN/passphrase/USB device or where the TPM chip has detected a change to the series of events for starting the device, it will be necessary to enter the recovery key. Panda Full Encryption keeps all the recovery keys for the encrypted network computers that it manages.

To get the recovery key for a computer, follow the steps below:

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

Panda Full Encryption panels and widgets

Accessing the dashboard

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

Required permissions

No additional permissions are required to access the widgets associated with Panda Full Encryption.

Encryption Status

This shows all the computers that support Panda Full Encryption as well as their encryption status.

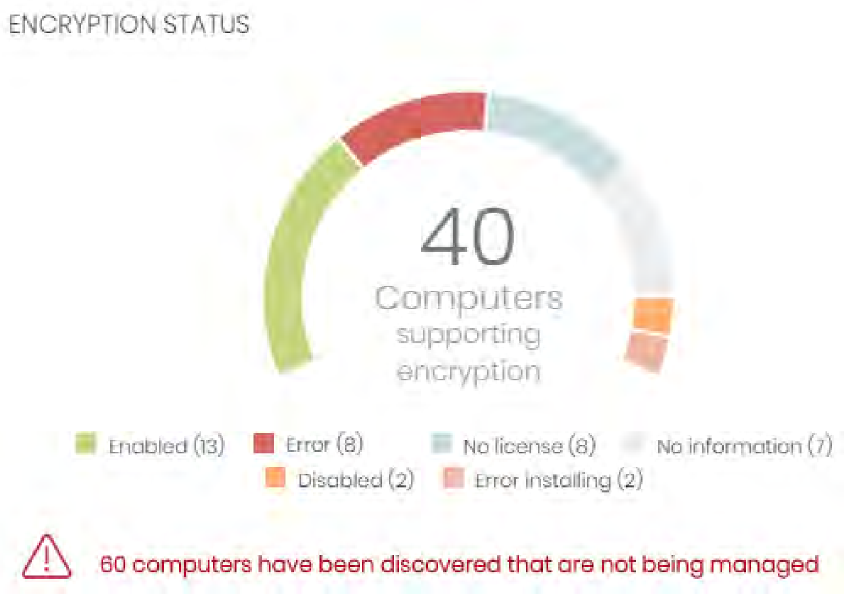


Figure 15.1: Encryption status pane

- **Meaning of the data**

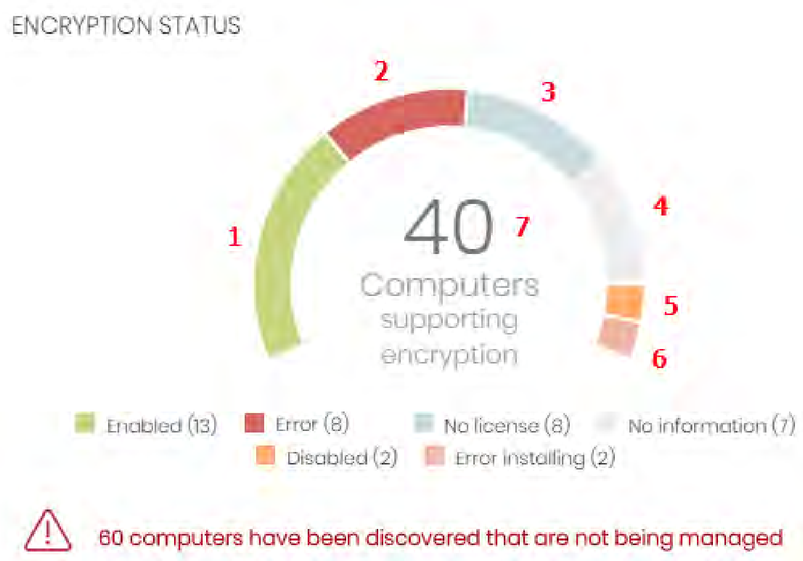
Status	Description
Enabled	Computers with Panda Full Encryption installed, settings assigned to encrypt the computer and which haven't reported encryption or installation errors.
Disabled	Computers with Panda Full Encryption installed, settings assigned to not encrypt the computer and which haven't reported encryption or installation errors.
Error	It hasn't been possible to carry out the action that the administrator specified in the encryption or decryption settings.
Error installing	It hasn't been possible to install and download BitLocker if it were required.

Table 15.2: Meaning of the Encryption Status panel

Status	Description
No license	The computer is compatible with Panda Full Encryption but no license is assigned.
No information	Computers with a recently assigned license and which haven't yet reported their status to the server, or a computer with an out-of-date agent.

Table 15.2: Meaning of the Encryption Status panel

- **Lists accessible from the panel**



60 computers have been discovered that are not being managed

Figure 15.2: Hotspots in the Encryption Status panel

Click the hotspots shown in figure 16.2 to access the **Encryption Status** list with the following predefined filters:

Hotspot	Filter
(1)	Encryption status = Enabled
(2)	Encryption status = Error
(3)	Encryption status = No license
(4)	Encryption status = No information
(5)	Encryption status = Disabled
(6)	Encryption status = Error installing
(7)	No filter

Table 15.3: Filters available in the Encryption Status list

Computers Supporting Encryption

This shows the computers that are compatible (or not) with the encryption technology, grouped by type.

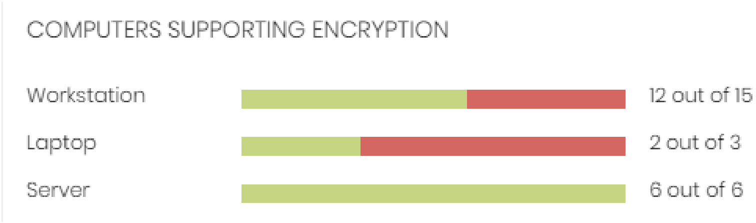


Figure 15.3: Computers Supporting Encryption panel

- **Meaning of the data displayed**

Data	Description
Workstation - green	Workstations that support encryption.
Workstation - red	Workstations that don't support encryption.
Laptop - green	Laptops that support encryption.
Laptop - red	Laptops that don't support encryption.
Server - green	Servers that support encryption.
Server - red	Servers that don't support encryption.

Table 15.4: Description of the Computers Supporting Encryption panel

- **Lists accessible from the panel**

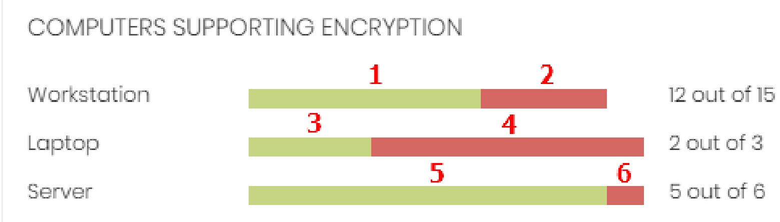


Figure 15.4: Hotspots in the Computers Supporting Encryption panel

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

Hotspot	Filter
(1)	Computer type = Workstation
(2)	List of computers filtered by **Encryption not supported.**
(3)	Type of computer = Laptop
(4)	List of computers filtered by **Encryption not supported.**

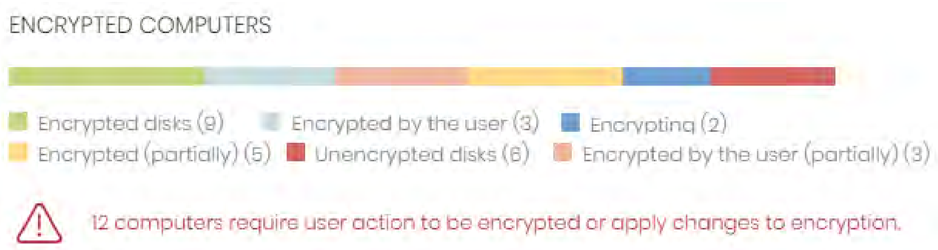
Table 15.5: Lists accessible from the Encryption Status panel

Hotspot	Filter
(5)	Type of computer = Server
(6)	List of computers filtered by **Encryption not supported.**

Table 15.5: Lists accessible from the Encryption Status panel

Encrypted Computers

This shows the encryption status of the network computers that support Panda Full Encryption.


ENCRYPTED COMPUTERS
🟩 Encrypted disks (9)
⬜ Encrypted by the user (3)
🟦 Encrypting (2)
🟨 Encrypted (partially) (5)
🟥 Unencrypted disks (6)
🟧 Encrypted by the user (partially) (3)

12 computers require user action to be encrypted or apply changes to encryption.

Figure 15.5: Encrypted Computers panel

- **Meaning of the data displayed**

Data	Description
Unknown	Disks encrypted with an authentication method not supported by Panda Full Encryption.
Unencrypted disks	None of the disks on the computer are encrypted by the user nor by Panda Full Encryption.
Encrypted disks	All the disks on the computer are encrypted by Panda Full Encryption.
Encrypting	At least one of the disks on the computer is in the process of being encrypted.
Decrypting	At least one of the disks on the computer is in the process of being decrypted.
Encrypted by the user	All the disks on the computer are encrypted, but some or all of them were encrypted by the user.
Encrypted by the user (partially)	One or more disks on the computer are encrypted by the user and the rest are either unencrypted or are encrypted by Panda Full Encryption.
Encrypted (partially)	At least one of the disks on the computer is encrypted by Panda Full Encryption but the rest are unencrypted.

Table 15.6: Description of the Encrypted Computers panel

- **Lists accessible from the panel**

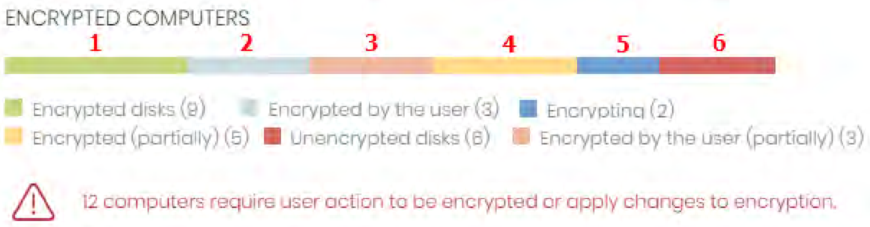


Figure 15.6: Hotspots in the Encrypted Computers panel

Click the hotspots shown in figure 15.6 to access the **Encryption Status** list with the following predefined filters:

Hotspot	Filter
(1)	Disk encryption = Encrypted disks
(2)	Disk encryption = Encrypted by the user
(3)	Disk encryption = Encrypted by the user (partially)
(4)	Disk encryption = Encrypted (partially)
(5)	Disk encryption = Encrypting
(6)	Disk encryption = Unencrypted disks
(7)	Disk encryption = Decrypting
(8)	Disk encryption = Unknown

Table 15.7: Lists accessible from the Encryption Status panel

Authentication Method Applied

This displays the network computers with encryption according to the type of encryption used.

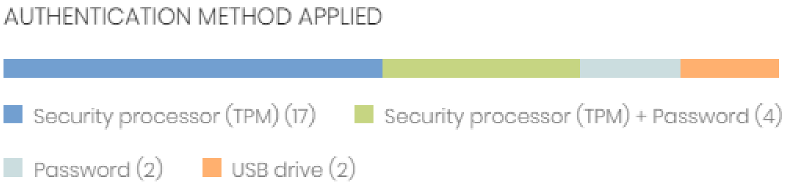


Figure 15.7: Authentication Method panel

- **Meaning of the data displayed**

Data	Description
Unknown	The authentication method selected by the user is not supported by Panda Full Encryption.

Table 15.8: Description of the Authentication Method Applied panel

Data	Description
Security processor (TPM)	The authentication method used is TPM.
Security processor (TPM) + Password	The authentication method used is TPM and PIN or passphrase requested on startup.
Password	The authentication method is PIN or passphrase requested on startup.
USB drive	The authentication method is a USB key connected during startup.
Unencrypted	None of the disks on the computer are encrypted.

Table 15.8: Description of the Authentication Method Applied panel

- **Lists accessible from the panel**

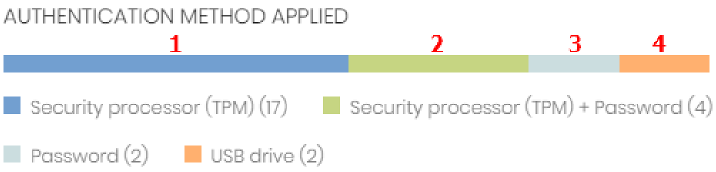


Figure 15.8: Hotspots in the Authentication Method Applied panel

Click the hotspots shown in figure 15.8 to access the **Encryption Status** list with the following predefined filters:

Hotspot	Filter
(1)	Authentication method = Security processor (TPM)
(2)	Authentication method = Security processor (TPM) + Password
(3)	Authentication method = Password
(4)	Authentication method = USB drive
(5)	Authentication method = Unknown
(6)	Authentication method = Unencrypted

Table 15.9: Lists accessible from the Authentication Method Applied panel

Panda Full Encryption lists

Accessing the lists

There are two ways to access the lists:

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

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window will open with all available lists.
- Select a list from the **Data protection** section to view the associated template. Edit it and click **Save**. The new list will be added to the side menu.

Required permissions

Administrators don't need additional permissions to access the Encryption status list.

Encryption Status

This list shows all the computers on the network managed by Panda Adaptive Defense and that support Panda Full Encryption. It includes filters related to the module to see the encryption status of the network.

Field	Comment	Values
Computer	Name of the computer that supports the encryption technology.	Character string
Computer status	Agent reinstallation: • Reinstalling the agent. • Agent reinstallation error. Protection reinstallation: • Reinstalling the protection. • Protection reinstallation error. • Pending restart.	Icon
	Computer isolation status: • Computer in the process of being isolated. • Isolated computer. • Computer in the process of stopping being isolated	
	"RDP attack containment" mode: • Computer in "RDP attack containment" mode. • Ending "RDP attack containment" mode	

Table 15.10: List fields

Field	Comment	Values
Group	Folder within the Panda Adaptive Defense folder tree to which the computer belongs.	Character string
Operating system	Operating system and version installed on the workstation or server.	Character string
Encryption status	Status of the Panda Full Encryption module.	• No information • Enabled • Disabled • Error • Error installing • No license
Disk encryption	Encryption status of the disks on the computer.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted by the user (partially) • Encrypted (partially)
Authentication method	Authentication method selected for the encrypted disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted
Last connection	The last time the agent connected to the Panda Security cloud.	Date

Table 15.10: List fields

To view a graphical representation of the list data, go to widget “**Encrypted Computers**”.

- **Fields displayed in the exported file**

Field	Comment	Values
Client	Client account to which the service belongs.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer that supports the encryption technology.	Character string
IP address	Primary IP address of the computer.	Character string
Domain	Windows domain to which the computer belongs.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder within the Panda Adaptive Defense folder tree to which the computer belongs.	Character string
Agent version	Internal version of the Panda module agent.	Character string
Installation date	Date that Panda Adaptive Defense was installed on the computer.	Date
Last connection		Date
Platform	Operating system installed on the computer.	Character string
Operating system	Internal version and patches of the operating system installed.	Character string
Updated protection	The protection module installed on the computer is the latest version released.	Boolean value
Protection version	Internal version of the protection module.	Character string
Updated knowledge	The signature file on the computer is the latest version.	Boolean value
Last update	Date the signature file was downloaded.	Date
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Disk status	Status of the computer's internal storage media with regard to encryption.	• Unknown • Unencrypted disks • Encrypted disks

Table 15.11: Fields in the exported file

Field	Comment	Values
		• Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Encryption pending user action	User actions (entering data or restarting) are pending to complete the encryption process.	Boolean value
Authentication method	Authentication method chosen for the encryption.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted
Encryption date	Date when the first drive was encrypted and the computer was considered completely encrypted (all supported drives were encrypted).	Date
TPM spec version	Version of the TPM specifications supported by the chip on the computer.	Character string
Encryption installation error date	Date of the last reported installation error.	Date
Encryption installation error	An error occurred installing Panda Full Encryption on the computer.	Character string
Encryption error date	Last date that an encryption error was reported on the computer.	Date
Encryption error	The encryption process returned an error.	Character string

Table 15.11: Fields in the exported file

- **Filter tool**

Field	Comment	Values
Encryption date from	Date from which the computer was considered completely encrypted.	Date
Encryption date to	Date until which the computer was considered completely encrypted.	Date

Table 15.12: List filters

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Disk status	Status of the computer's internal storage media with regard to encryption.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Hard disk encryption	Panda Full Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Authentication method	Authentication method selected.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • Not encrypted
Last connection	The last time the Panda Adaptive Defense status was sent to the Panda Security cloud.	Date

Table 15.12: List filters

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "Details section (3)" on page 179 for more information.

Encryption settings

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Encryption** from the side menu.

- Click the **Add** button to open the settings window.

Required permissions

Permission	Access type
Configure computer encryption	Create, edit, delete, copy, or assign Encryption settings.
View computer encryption settings	View the Encryption settings.

Table 15.13: Permissions required to access the Encryption settings

Panda Full Encryption settings

Encrypt all hard disks on computers

This indicates whether the computers will be encrypted or not. Depending on the previous status of the computers, the way that Panda Full Encryption acts will vary:

- If the computer is encrypted with Panda Full Encryption and **Encrypt all hard disks on computers** is disabled, all encrypted drives will be decrypted.
- If the computer is encrypted but not with Panda Full Encryption, and **Encrypt all hard disks on computers** is disabled, there will be no change.
- If the computer is encrypted but not with Panda Full Encryption, and **Encrypt all hard disks on computers** is enabled, the internal encryption settings will be adjusted to coincide with the encryption methods supported by Panda Full Encryption, thereby avoiding re-encrypting the drive. See section "**Encryption of previously encrypted drives**".
- If the computer is not encrypted and **Encrypt all hard disks on computers** is enabled, all the drives will be encrypted as described in section "**Encryption of previously unencrypted drives**"

Ask for password to access the computer

This enables password authentication on starting up the computer. Depending on the platform and whether there is TPM hardware, two types of passwords are permitted:

- **Computers with TPM**: a PIN type password will be requested.
- **Computers without TPM**: a passphrase will be requested.

> ⚠ *If this option is set to 'No' and the computer doesn't have access to a compatible TPM security processor, the disks will not be encrypted.*

Do not encrypt computers that require a USB drive for authentication

To prevent the use of USB devices supported by Panda Full Encryption in authentication, administrators can disable their use.

> ⚠ *Only Windows 7 without TPM can use USB authentication. If administrators disable USB devices, these computers will not be encrypted.*

Encrypt used disk space only

The administrator can minimize the encryption time by restricting the feature to the sectors of the hard disk that are actually being used. The sectors released after deleting a file will remain encrypted, but the space that was free prior to the encryption of the hard disk will remain unencrypted, and will be accessible to third parties using tools for recovering deleted files.

Prompt for removable storage drive encryption

Displays a window prompting the user to encrypt the external mass storage devices and USB keys connected to the computer. Refer to "**Encrypting and decrypting external hard drives and USB keys**" for more information about the behavior and requirements for this setting.

Available filters

To locate network computers with any of the encryption statuses defined in Panda Adaptive Defense, use the filter tree resources shown in section "**Filter tree**" on page **146**. The available filters are as follows:

- Encryption
  - Encryption pending user action
  - Disk encryption
  - Encryption date
  - Authentication method
  - Is waiting for the user to perform encryption actions
- Settings
  - Encryption
- Computer
  - Has a TPM
- Hardware
  - TPM - Activated
  - TPM - Manufacturer

  - TPM - Owner
  - TPM - Version
  - TPM – Spec version
- Modules
  - Encryption

Chapter 16

Program blocking settings

To increase the security of the Windows computers on their network, administrators may want to prevent the execution of certain programs deemed dangerous or not compatible with the activity conducted by their organization. There are many reasons why an administrator may choose to prevent the execution of certain programs:

- Programs which, because of their high requirements, use too much bandwidth or establish too many connections, compromising the company's connectivity performance if run concurrently by multiple users.
- Programs that allow users to access contents that may contain security threats, or are protected by licenses not purchased by the organization.
- Programs that allow users to access contents not related to the company's activity and which may affect user productivity.

For additional information about the 'Program blocking' module, refer to:

- "Creating and managing settings" on page 197: information on how to create, edit, delete, or assign settings to the computers on your network.
- "Controlling and monitoring the management console" on page 63: managing user accounts and assigning permissions.
- "Managing lists" on page 53: information on how to manage lists.

CHAPTER CONTENTS

Program blocking settings

Accessing the settings

- Click the **Settings** menu at the top of the console. Then, click **Program blocking** from the side menu.
- Click the **Add** button to open the **Program blocking** settings window.

You can only assign program blocking settings to Windows workstations and servers.

Required permissions

Permission	Access type
Configure program blocking	Create, edit, delete, copy, or assign program blocking settings.
View program blocking settings	View the program blocking settings.

Table 16.1: Permissions required to access the program blocking settings

Program blocking settings options

To create a new settings profile or edit an existing one, enter the following information:

Field	Description
Names of the programs to block	Names of the files that Panda Adaptive Defense will prevent from running. This text box accepts lists of file names copied, pasted and separated by carriage returns. Wildcards are not supported in order to avoid overly broad settings that may compromise proper operation of the computer.
MD5 codes of the programs to block	MD5 codes of the files that Panda Adaptive Defense will prevent from running. This text box accepts lists of MD5 codes copied, pasted and separated by carriage returns.
Notify computer users about blocked applications	Enter a descriptive message to inform users that a file has been blocked. The Panda Adaptive Defense agent will show a pop-up message with the configured text.

Table 16.2: Configuring a Program blocking security profile

Do not block operating system programs or components that may be required to run user programs properly.

Panda Adaptive Defense won't block any of its programs or modules to ensure proper operation of the security solution installed.

‘Program blocking’ module lists

Accessing the lists

There are two ways to access the lists:

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

Or,

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window will open with all available lists.
- Select the **Programs blocked by the administrator** list from the **Activity control** section to view the associated template. Edit it and click **Save**. The new list will be added to the side menu.

Required permissions

Permission	Access to lists
View detections and threats	Programs blocked by the administrator

Table 16.3: Permissions required to access the blocked programs list

Programs blocked by the administrator

Shows details of the programs blocked by Panda Adaptive Defense on workstations and servers.

Field	Description	Values
Computer	Computer name.	Character string
Path	Path and name of the program blocked by the administrator.	Character string
Date	Date when Panda Adaptive Defense blocked the program.	Date

Table 16.4: Fields in the ‘Programs blocked by the administrator’ list

*To view a graphical representation of the list data, go to widget “***Programs blocked by the administrator***”.*

- **Fields displayed in the exported file**

Field	Description	Values
Path	Path and name of the program blocked by the administrator on the computer.	Character string

Table 16.5: Fields in the ‘Programs blocked by the administrator’ exported file

Field	Description	Values
Hash	MD5 of the program blocked by the administrator.	Character string
Date	Date when Panda Adaptive Defense blocked the program.	Date
Logged-in user	Operating system user account under which the blocked program was run.	Character string
Action	Action taken by Panda Adaptive Defense	“Blocked” character string

Table 16.5: Fields in the ‘Programs blocked by the administrator’ exported file

- **Filter tool**

Field	Description	Values
Find computer	Lets you search for computers by name.	Character string
Dates	Lets you narrow the scope of the data displayed by time period.	• Last 7 days • Last month

Table 16.6: Filters available in the 'Programs blocked by the administrator' list

- **Blocked program details window**

Click any of the items on the list to view detailed information about the blocked program.

Field	Description	Values
Blocked program	Name of the blocked file.	Character string
Computer	Name of the computer where the program was blocked, IP address, and group it belongs to.	Character string
Logged-in user	User account under which the blocked program tried to run.	Character string
Name	Name of the blocked file.	Character string
Path	Storage device and computer folder where the blocked program is located.	Character string
Hash	MD5 of the blocked program.	Character string
Detection date	Date the program was blocked.	Date

Table 16.7: Fields in the ‘Blocked program details’ window

Program blocking panels/widgets

Accessing the dashboard

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

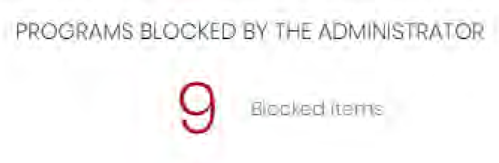
Required permissions

Permission	Access to widgets
View detections and threats	• Programs blocked by the administrator

Table 16.8: Permissions required to access the blocked programs widget

Programs blocked by the administrator

Shows the number of execution attempts recorded across the IT network and blocked by Panda Adaptive Defense based on the settings defined by the network administrator.



PROGRAMS BLOCKED BY THE ADMINISTRATOR

9 Blocked items

Figure 16.1: 'Programs blocked by the administrator' panel

- **Meaning of the data displayed**

Data	Description
Blocked items	Number of execution attempts recorded across the IT network and blocked by Panda Adaptive Defense in the specified period.

Table 16.9: Description of the data displayed in the 'Programs blocked by the administrator' panel

- **Lists accessible from the panel**

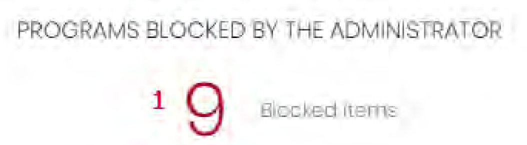


Figure 16.2: Hotspots in the 'Programs blocked by the administrator' panel

Click the hotspots shown in figure 16.2 to access the **Programs blocked by the administrator** list with the following predefined filters:

Hotspot	Filter
(1)	No filters.

Table 16.10: Filters available in the 'Programs blocked by the administrator' list

Chapter 17

Authorized software settings

In Hardening and Lock modes of the advanced protection, Panda Adaptive Defense prevents the execution of programs that are unknown by Panda intelligence until they are classified. This behavior could have drawbacks and create minor delays for users in very specific situations, above all when the network administrator knows the source of the program and the reason why it has been blocked, for example:

- Specific niche programs with very few users.
- Programs that update automatically from the vendor's website without user interaction.
- Programs whose functions are distributed across hundreds of libraries which are loaded in memory and therefore blocked as and when they are used by the user from program menus.
- Programs operating on a client-server model, where the client side is hosted on a shared network resource.
- Polymorphic software which dynamically generates executable files.

For more information about the 'Authorized software' module, refer to the following links:

- "**Creating and managing settings**" on page **197**: information on how to create, edit, delete, or assign settings to the computers on your network.
- "**Controlling and monitoring the management console**" on page **63**: managing user accounts and assigning permissions.
- "**Advanced protection**" on page **226**: configuring Lock and Hardening modes.

CHAPTER CONTENTS

Authorized software and exclusions

In Panda Adaptive Defense there are three features to prevent blocking of programs:

- **Using excluded files and paths**: prevents certain items or areas on the computer from being scanned. Unknown software won't be prevented from running. This, however, could represent a security hole and is not recommended for use except where there are problems with the computer's performance. Refer to "Files and paths excluded from scans" on page 225.
- **Unblocking programs in the process of classification**: temporarily allows blocked programs to run but with a reactive approach: the administrator cannot unblock a program unless it has first been blocked. As certain software can consist of several components, and each of them may have to be unblocked individually, the cycle of blocking and unblocking can take some time.
- **Configuring authorized software**: the administrator proactively authorizes users to run unknown programs before Panda Security issues a classification. This module is useful when the advanced protection is in Lock or Hardening mode and finds an unknown program, preventing its use.

The 'Authorized software' module enables you to approve the execution of executable binary files, excluding script files, standalone DLLs, and other files. If Panda Adaptive Defense blocks a program because it loads an unknown DLL, authorize the executable file specified in the pop-up message shown on the user's computer. After the program is authorized, all DLL files and resources it uses are also allowed.

Authorized software settings

Accessing the settings

- Click the **Settings** menu at the top of the console, then **Authorized software** in the side menu.
- Click **Add** to open the **Add settings** window.

Authorized software settings can only be assigned to Windows servers or workstations.

Required permissions

Permission	Access type
Configure authorized software	Create, edit, delete, copy, or assign authorized software settings.
View authorized software settings	View the authorized software settings.

Table 17.1: Permissions required to access the authorized software settings.

‘Authorized software’ module functions

Network users will be able to run unknown software which is in the process of classification as long as the network administrator has permitted it by using an authorized software rule.

Once it has been analyzed, Panda Adaptive Defense classifies the program (goodware or malware). If the program represents a threat, it will be blocked regardless of whether it appears in the authorized software settings.

Authorized software’ module settings

Authorized software settings consist of one or more rules, each of which refers to a single software component or family of programs which Panda Adaptive Defense will allow to run even though it has been blocked because its classification is not yet known.

Creating an authorized software rule

Click the ⊕ **Authorize programs** link to create a rule with the information shown below, and then click **Authorize**:

Field	Description
Name	Rule name.
MD5	MD5 hashes of the files Panda Adaptive Defense will allow to run. Refer to section “**Calculating the MD5 of one or more files**”.
Product name	This is the ‘Product name’ field from the header of the file to be unblocked. To get this value, right-click the program and select **Properties**, **Details.**
File path	Path of the program on the server or workstation. Environment variables are accepted.
File name	File name. Wildcards * and ? are accepted.
File version	This is the ‘Version’ field from the header of the file to be unblocked. To get this value, right-click the program and select **Properties**, **Details.**
Signature	This is the SHA-1 digital signature of the file. Refer to section “**Getting the sha1 thumbprint of a signed program**”.

Table 17.2: Configuring an authorized software rule

Deleting an authorized software rule

- Click the 🗑 icon to the right of the authorized software rule to delete.
- Click **Save** in the top right of the screen to save the newly edited authorized software settings.

Editing an authorized software rule

- Click the name of the authorized software rule. The **Authorize programs** window appears.

- Edit the rule properties and click **Authorize**.
- Click **Save** in the top right of the screen. The authorized software settings will be updated.

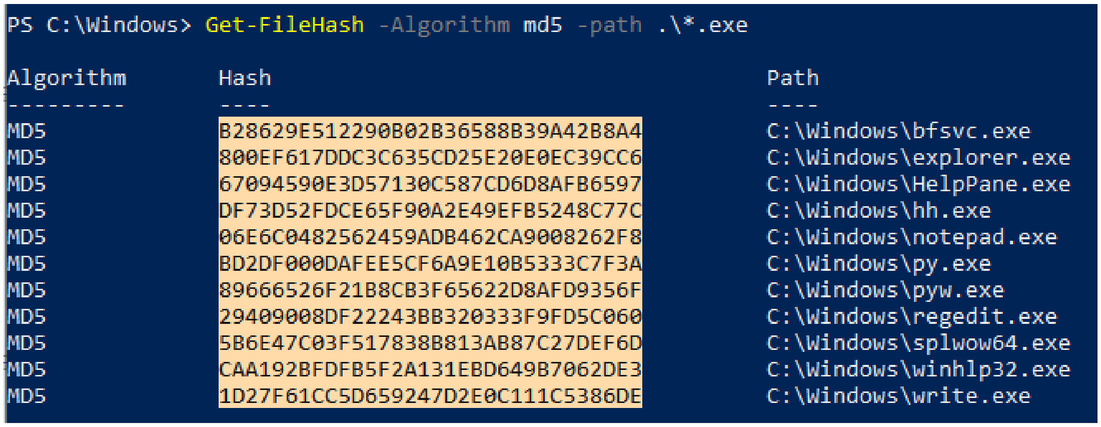
Copying an authorized software rule

- Click the ⧉ icon to the right of the authorized software rule to copy. The **Authorize programs** window appears. The **Name** contains the name of the rule with the prefix "Copy of".
- Edit the rule properties and click **Authorize**.
- Click **Save** in the top right of the screen. The authorized software settings will be updated.

Calculating the MD5 of one or more files

There are many tools available to calculate the MD5 of a file. In this section, the PowerShell tool in Windows 10 is used.

- Open the folder containing the files, click the **File** menu of the file explorer and click **Open Windows PowerShell**. A window with the command line appears.



```
PS C:\Windows> Get-FileHash -Algorithm md5 -path .\*.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             B28629E512290B02B36588B39A42B8A4                                       C:\Windows\bfsvc.exe
MD5             800EF617DDC3C635CD25E20E0EC39CC6                                       C:\Windows\explorer.exe
MD5             67094590E3D57130C587CD6D8AFB6597                                       C:\Windows\HelpPane.exe
MD5             DF73D52FDCE65F90A2E49EFB5248C77C                                       C:\Windows\hh.exe
MD5             06E6C0482562459ADB462CA9008262F8                                       C:\Windows\notepad.exe
MD5             BD2DF000DAFEE5CF6A9E10B5333C7F3A                                       C:\Windows\py.exe
MD5             89666526F21B8CB3F65622D8AFD9356F                                       C:\Windows\pyw.exe
MD5             29409008DF22243BB320333F9FD5C060                                       C:\Windows\regedit.exe
MD5             5B6E47C03F517838B813AB87C27DEF6D                                       C:\Windows\splwow64.exe
MD5             CAA192BFDFB5F2A131EBD649B7062DE3                                       C:\Windows\winhlp32.exe
MD5             1D27F61CC5D659247D2E0C111C5386DE                                       C:\Windows\write.exe
```

Figure 17.1: Command line with the result of Get-FileHas

- Enter the following command and replace $file with the file path. Wildcards * and ? are accepted.

```
PS c:\folder> Get-FileHash -Algorithm md5 -path $files
```

- To copy the MD5 hashes to the clipboard, press the key `Alt` and without releasing, select the hashes with the mouse pointer. Then press `Control + c`.
- To paste all the MD5 hashes from the clipboard to the Panda Adaptive Defense console, click the **MD5** field of the authorized software rule and press the keys `Control + v`.
- Click **Authorize** and then **Save** in the top right of the screen. The authorized software settings will be updated.

Getting the sha1 thumbprint of a signed program

- Right-click the file and select **Properties** from the context menu.

- In the **Properties** window, select the **Digital signatures** tab.
- In the **Signature list,** select the signature with the **Digest algorithm** set to sha1 and click **Details**. The **Digital signature details** window appears.
- In the **Digital signature details** window**,** select the **General** tab and click **View certificate**. The **Certificate** window opens.
- In the **Certificate** path**,** click the **Certification path** tab and check that the final node of the certification path is selected.
- In the **Certificate** window, click the **Details** tab and select the field **Thumbprint.**
- Select the character string from the text box displayed and press the keys `Control + c` to copy it to the clipboard.
- Click the **Signature** field of the authorized software rule and press the keys `Control + v` to paste the thumbprint to the Panda Adaptive Defense console.
- Click **Authorize** and then **Save** in the top right of the screen. The authorized software settings will be updated.

Chapter 18

Indicators of attack settings

In cyberattacks that target companies, hackers attempt to break through security defenses by deploying a series of coordinated actions. These actions take place over long periods of time, and use multiple strategies and infection vectors. Many such actions may appear innocuous individually, but taken as a whole, they can be part of an ongoing cyberattack.

The Panda Adaptive Defense basic user license includes a cross threat hunting service. This service inspects the data flow sent by the security software installed on a customer's computers using advanced automated analysis technologies, in order to identify indicators of attacks in progress. Finally, a team of specialists (hunters) sift through these indicators which are represented on the administrator console as IOAs (Indicators Of Attack).

An IOA is an indicator displayed on the Panda Adaptive Defenseadministrator console when a pattern of events likely to belong to a cyberattack is detected. It could therefore act as an early warning of an infection, alerting an administrator to a potential attack in progress, though it could also be an alert of a cyberattack that has managed to penetrate the company's defenses.

As the existence of an IOA can reveal the existence of an imminent danger, Panda Adaptive Defense not only focuses on detection, but also enables the launching of an automatic response to minimize the attack surface.

For additional information about the Indicators of attack module, refer to:

- "Creating and managing settings" on page 197: information on how to create, edit, delete, or assign settings to the computers on your network.
- "Controlling and monitoring the management console" on page 63: information on managing user accounts and assigning permissions.
- "Managing lists" on page 53: information on how to manage lists.

CHAPTER CONTENTS

Introduction to IOA concepts

This section details the concepts that administrators need to know to understand the processes involved in the detection of IOAs, and in the execution of remedial actions (automatic and manual).

Event

An action executed by a process on the user's computer and monitored by Panda Adaptive Defense Events are sent to the Panda Security cloud in real time as part of the telemetry. Automated analysis advanced technologies, analysts, and threat hunters analyze them in context to determine whether they could be part of the CKC of a cyberattack.

Indicator

This is the detection of an anomalous chain of actions of the processes running on customers' computers. These are sequences of unusual actions that are analyzed in detail to determine whether or not they belong to a cyberattack.

Indicator of attack (IOA)

This is an indicator that is highly likely to represent a cyberattack. These are generally attacks in early stages or in exploit phase. These attacks do not normally use malware, as adversaries usually use the operating system's own tools to execute the attack and thereby hide the traces of their activity. It is advisable to contain or remedy the attack as soon as possible.

To help manage IOAs, Panda Adaptive Defense gives each one a status, which can be manually edited by the administrator:

- **Pending**: The IOA is pending investigation and/or resolution. Administrators must verify whether the attack is real and take the necessary measures to mitigate it. All new IOAs are created with the status 'pending'.
- **Archived**: The IOA has already been investigated by the administrator and the remedial actions have been taken, or were unnecessary as it was a false positive. The administrator closes the IOA for any of these reasons.

Panda Adaptive Defense shows relevant IOA information, such as the MITRE tactic and technique used, the events recorded on the computer that generated the IOA, and, if available, the following reports:

- **Advanced attack investigation**: This includes information about the computer involved, a detailed description of the tactics and techniques used, recommendations to mitigate the attack, and the sequence of events that triggered the generation of the IOA. Refer to "**Fields in the IOA details window**".
- **Attack graph**: This includes an interactive diagram with the sequence of events that led to the

generation of the IOA. Refer to “**Graphs**”.

The reports last for a month after the IOA is generated. After this period, they are no longer accessible. At the same time, a report shows the events that are part of the attack for the thirty days prior to the detection of the IOA.

CKC (Cyber Kill Chain)

In 2011, Lockheed-Martin drafted a a framework or model for defending computer networks, which stated that cyberattacks occur in phases and each of them can be interrupted through certain controls. Since then, the Cyber Kill Chain (CKC) has been adopted by IT security organizations to define the phases of cyberattacks. These phases range from remote reconnaissance of the target’s assets to data exfiltration.

MITRE Corporation

A not-for-profit company that operates several federally-funded R&D centers dedicated to addressing security issues. It offers practical solutions in the fields of defense and intelligence, aviation, civil systems, national security, judiciary, health, and cybersecurity. It is the creator of the ATT&CK framework.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

A set of resources developed by the MITRE Corporation to describe and categorize dangerous actions of cybercriminals based on observations from around the world. ATT&CK is a structured list of the known behaviors of attackers, broken down into tactics and techniques, and expressed as a matrix. As this list is a comprehensive representation of the behaviors that hackers use when they infiltrate networks, it is a useful resource to develop defensive, preventive, and remedial strategies for organizations. For more information about the ATT&CK framework, refer to **https://attack.mitre.org/**.

Technique (‘How’)

In ATT&CK terminology, the techniques represent the way (or the strategy) that an adversary achieves a tactical objective. In other words, ‘how’. For example, an adversary, in order to achieve the objective of accessing credentials (tactic), executes a dump of the data (technique).

Tactic (‘Why’)

In ATT&CK terminology, tactics represent the ultimate motive or goal of a technique. It is the adversary’s tactical objective: the reason for taking an action.

Managing indicators of attack

Enable and configure the detection of IOAs

By default, Panda Adaptive Defense assigns **Indicators of attack (IOA)** settings to all computers on a network, with all types of IOAs enabled by default. To disable the detection of a specific type of IOA:

- In the **Settings** menu, select **Indicators of attack (IOA)** in the side panel.
- Click the **Add** button to open the **Add settings** window.
- Select the IOAs that Panda Adaptive Defense is to search for in the telemetry generated by the computers.
- Select the computers that you wish to receive the new settings and click **OK**.

For more information on how to manage settings, refer to "**Managing settings**" on page **189**.

Show all IOAs detected on a network

- In the **Status** menu, select **Indicators of attack (IOA)** in the side panel.
- At the top of the window, you can see the time period to show.
- The "**Threat Hunting Service**" widget contains the events, indicators, and IOAs detected during that period.
- Click in the **Indicators of attack** area. The "**Indicators of attack (IOA)**" list that opens shows all the IOAs detected during the selected period.

For more information about this widget, refer to "**Threat Hunting Service**".

Find all computers with a specific IOA

- In the **Status** menu, select **Indicators of attack (IOA)** in the side panel.
- Click the type of IOA in the "**Detected indicators of attack (IOA)**" panel or in "**Indicators of attack (IOA) mapped to the MITRE matrix**".
- Click the type of IOA. The "**Indicators of attack (IOA)**" list opens filtered by the specified type of attack.

For more information about these widgets, refer to "**Indicators of attack (IOA) mapped to the MITRE matrix**" and "**Detected indicators of attack (IOA)**".

Find all IOAs detected on a computer

- In the **Status** menu, select **Indicators of attack (IOA)** in the side panel.
- Select a computer from the "**Indicators of attack (IOA) by computer**" panel. The "**Indicators of attack (IOA)**" list opens with the selected computer filter applied.

For more information about this widget, refer to "**Indicators of attack (IOA) by computer**".

Find computers and related IOAs

Each IOA displayed in the **Indicators of attack (IOA)** list has a context menu with the options:

- **View the IOAs detected on this computer** : This shows the **Indicators of attack (IOA)** list filtered by the **Computer** field.
- **View the computers on which this IOA was detected** : This shows the **Indicators of attack (IOA)** list filtered by the **Indicator of attack** field.

For more information about the lists, refer to “**Indicators of attack (IOA) module lists**”.

Archive one or more indicators of attack

When the event that triggered the IOA has been resolved, or when it has been found to be a false positive, an administrator can archive the IOA:

- Click the **Status** menu at the top of the console. Then, click the **Add** link from **My lists** in the side menu. The **Add list** window with the available templates opens.
- In the **Security** section, click the **Indicators of attack (IOA)** template. The list of IOAs detected without filters opens.
- Set the required filters and click the **Filter** button.
- Click the context menu of the indicator to archive, and select **Archive IOA** . The status of the indicator of attack changes to **Archived**.

or:

- Select the checkboxes associated with the indicators of attack to archive.
- In the toolbar, click **Archive IOA** . The status of the indicators of attack switches to **Archived**.

Mark one or more IOAs as pending

Panda Adaptive Defense marks detected IOAs as pending in order to indicate to the administrator that they require attention. An administrator can also mark a previously archived indicator as pending when the event that triggered the IOA has not been completely resolved.

- Click the **Status** menu at the top of the console. Then, click the **Add** link from **My lists** in the side menu. The **Add list** window with the available templates opens.
- In the **Security** section, click the **Indicators of attack (IOA)** template. The unfiltered list opens.
- Set the required filters and click the **Filter** button.
- Click the indicator’s context menu and select the option **Mark IOA as pending** . The indicator will then have the status **Pending**.

Or:

- Select the checkboxes next to the indicators of attack to archive.

- In the toolbar, click **Mark IOA as pending** !. The indicators of attack then have the status **Pending**.

Show details of an IOA and recommendations for resolving the issue

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the **My lists** side menu. The **Add list** window with the available templates opens.
- In the **Security** section, click the **Indicators of attack (IOA)** template. The unfiltered list opens.
- Set the required filters and click the **Filter** button.
- Click an indicator of attack in the list. The **Details** window opens. Refer to "**Details window**".

Detection and protection against RDP attacks

Among the cyberattacks that target companies, RDP brute force attacks are the most frequently used by adversaries, especially where systems are directly exposed to the Internet. Panda Adaptive Defense detects and protects network computers against attacks that use the RDP (Remote Desktop Protocol) as an infection vector.

Using the RDP protocol, users connect to remote computers and run processes that enable them to use resources on another computer. In the case of non-legitimate users, this protocol can also be used to facilitate lateral movements within a corporate network and access other resources hosted on the IT infrastructure.

When the **Brute-force attack against RDP/Credentials compromised after brute-force attack on RDP** setting is enabled (refer to "**Enable and configure the detection of IOAs**"), Panda Adaptive Defense executes the following actions:

- It logs any remote access attempts via RDP on each protected computer over the last 24 hours, which originated outside the customer's network.
- It determines whether the computer is subject to an RDP brute force attack.
- It detects if any of the computer's accounts have already been compromised to access resources on the system.
- It blocks RDP connections to mitigate the attack.

IOA associated with an RDP attack

Panda Adaptive Defense shows the Brute-force attack against RDP IOA on detecting signs of an RDP attack. In this situation, the computer will have received a large number of RDP connections that try to initiate a remote session, but have failed because they do not have valid credentials.

RDP containment modes

- **Initial RDP attack containment mode**

When a computer protected by Panda Adaptive Defense receives a large number of RDP connection attempts that fail due to invalid credentials, the protection software generates the **Brute-force attack against RDP** IOA and puts the computer into **Initial RDP attack containment** mode. In this mode, RDP access to the computer is blocked from IPs outside the customer's network that have sent a large number of connection attempts over the last 24 hours. To allow access by one or more of these IPs, use the **Trusted IPs** list in the **Indicators of attack (IOA)** settings. Refer to "Trusted IPs".

- **Restrictive RDP attack containment mode**

This is triggered when a computer protected by Panda Adaptive Defense already in **Initial RDP attack containment mode** receives a successful login attempt from an account that previously failed due to invalid credentials. At this point, the protection software generates the **Credentials compromised after brute-force attack on RDP** IOA and the account is considered to have been compromised. As a mitigation mechanism, all external RDP connections that have tried to connect at least once with the target computer in the previous 24 hours are blocked.

Configuring the response to an RDP attack

When Panda Adaptive Defense detects an RDP attack or intrusion, there are two response options: report only, or report and block the attack.

To configure the response to an RDP attack:

- In the **Indicators of attack** settings assigned to the computer, click the **Advanced settings** link in the **Brute-force attack against RDP/Credentials compromised after brute-force attack on RDP** section. The settings options associated with this IOA are shown.
- Select the required option from **Response on workstations** and/or **Response on servers:**
  - **Report and block RDP attacks**: Panda Adaptive Defense shows the Brute-force attack against RDP IOA in the console and also sets the relevant containment mode for the target computer.
  - **Report only**: Panda Adaptive Defense only shows the Brute-force attack against RDP IOA in the console.

For more information, refer to "Indicators of attack (IOA) settings options".

Finding network computers in RDP attack containment mode

You can use the following resources to find computers in containment mode:

- With the **XX computers in RDP attack containment mode** list in the **Threat hunting service** widget. Refer to "Threat Hunting Service".
- With the filters available in the **Computer protection status** list. Refer to "Computer protection status" on page 412.

- In the **Computer protection status** exported file. Refer to “Computer protection status” on page 412.
- With a computer tree filter. Refer to “Computers in containment mode” on page 174.

Viewing the computer containment status

The console shows the containment status of computers through the following resources:

- In the **Computer protection status** list, via the icon. Refer to “Computer protection status” on page 412.
- In the exported **Computer protection status** list, in the **RDP attack containment mode** column. Refer to “Computer protection status” on page 412.
- In the **Encryption status** list, via the icon. Refer to “Encryption Status” on page 347.
- In the exported **Encryption status** list, in the **RDP attack containment mode** column. Refer to “Encryption Status” on page 347.
- In the **Patch management status** list, via the icon. Refer to “Patch management status” on page 307.
- In the exported **Patch management status** list, in the **RDP attack containment mode** column. Refer to “Patch management status” on page 307.
- In the **Data Control status** list, via the icon. Refer to “‘Data Control status’” on page 265.
- In the exported **Data Control status** list, in the **RDP attack containment mode** column. Refer to “‘Data Control status’” on page 265.
- In the **Computer**s list, via the icon. Refer to “Available lists for managing computers” on page 158.
- In the exported **Computer**s list, in the **RDP attack containment mode** column. Refer to “Available lists for managing computers” on page 158.
- In the **Indicators of attack (IOA)** list, in the **Action** column. Refer to “Indicators of attack (IOA)”.
- In the exported **Indicators of attack (IOA)** list, in the **Action** column. Refer to “Indicators of attack (IOA)”.
- In the alerts in the **Computer details** window. Refer to “Computers in containment mode” on page 174.
- In the **IOA details** window, in the **Computer** field. Refer to “Details window”.

Automatic termination of RDP attack containment mode

24 hours after containment mode begins, Panda Adaptive Defense evaluates the number of connection attempts via RDP. If it is below certain thresholds, containment mode is terminated, if not, it is extended for a further 24 hours.

IPs blocked during containment mode will continue to be blocked even after the RDP attack has finished. In this way, over time, the security software learns the IPs that cybercriminals use to attack a customer's network and, when all of them have been blocked, the attack will be rendered ineffective and it will no longer be necessary to use containment mode.

Manual termination of RDP attack containment mode

If an administrator considers that the network is secure and there is no longer any danger of RDP attacks, they can manually terminate the block:

- **From the lists specified in "Viewing the computer containment status":**
  - Open one of the lists and select the checkboxes associated to the computers. The toolbar appears.
  - Click the icon **End RDP attack containment mode** 👤.

Or:

  - Click the context menu ⋮ to the right of the computer. A drop-down menu appears with the available options.
  - Select the option **End RDP attack containment mode** 👤.

- **From the computer details window**
  - Open one of the lists indicated in **"Viewing the computer containment status"** and click the computer. This opens the **Computer details** window.
  - Click **End RDP attack containment mode.**

After the manual end of containment mode process has started, the management console immediately sends the command to the computers involved. Depending on whether the device is accessible and operating in real time, the action is executed immediately or the device goes to the **Ending RDP containment mode** status, in which case it will show:

- A flashing 👤 icon in the lists specified in **"Viewing the computer containment status".**
- A warning message in the **Computer details** window.
- A warning message in the **IOA details** window.

*Refer to "**Configuring real-time communication**" on page* **215**

The computer continues in containment mode until the command is executed correctly. If a problem occurs, the action is executed again every 4 hours for the next 7 days. If the action is not completed, the console returns the status to **RDP attack containment mode**.

After containment mode has been manually ended, the following actions are executed:

- All the IPs recorded and blocked on the computer are released, and the technology returns to its original state.

- The computer ceases to block RDP connections.

These actions are only executed when the RDP attack containment mode is manually terminated. If the security software automatically determines that the computer is no longer subject to an RDP attack, it ends the containment status but does not release the IPs and, therefore, does not stop blocking them

Configuring indicators of attack (IOA)

Accessing the settings

- In the **Settings** menu, select **Indicators of attack (IOA)** in the side panel.
- Click **Add**. The **Add settings** window opens.

You can only assign Indicators of attack (IOA) settings to Windows, Linux, and macOS workstations and servers.

Required permissions

Permission	Access type
Configure indicators of attack (IOA)	Create, edit, delete, copy, or assign Indicators of attack (IOA) settings.
View indicators of attack (IOA) settings	View the Indicators of attack (IOA) settings.

Table 18.1: Permissions required to access the Indicators of attack (IOA) settings

Indicators of attack (IOA) settings options

To enable/disable the IOAs that you want to monitor, use the corresponding toggle:

Field	Description
Brute-force attack against RDP Credentials compromised after brute-force attack on RDP	Detects large numbers of remote login attempts over the RDP protocol.
Other IOAs	Panda Security periodically updates the list of indicators of attack to reflect the new strategies used by cybercriminals.

Table 18.2: Types of indicators available in the Indicators of attack (IOA) settings

Automatic response to RDP attacks

Field	Description
Response on workstations	• **Report and block RDP attacks**: Generates an IOA and blocks RDP attacks. Refer to "Detection and protection against RDP attacks" on page 373. • **Only report**: Generates IOAs.
Response on servers	• **Report and block RDP attacks**: Generates an IOA and blocks RDP attacks. Refer to "Detection and protection against RDP attacks" on page 373. • **Only report**: Generates IOAs.

Table 18.3: Automatic response actions to RDP IOAs

Trusted IPs

Enter the list of IPs of the computers that you consider secure. The RDP connections whose sources are in the list are not blocked, but generate indicators in the Indicators of attack (IOA) dashboard. Use commas to separate individual IPs and hyphens to separate ranges of IPs.

Indicators of attack (IOA) module lists

Accessing the lists

The lists can be accessed through two paths:

- Click the **Status** menu at the top of the console. Then, click **Indicators of attack (IOA)** from the side menu and click the relevant widget.

Or:

- Click the **Status** menu at the top of the console. Then, click the **Add** link from the side menu. A window opens with the available lists.
- In the **Security** section, select the **Indicators of attack (IOA)** list to see the corresponding template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

Permission	Access to lists
View detections and threats	• Indicators of attack (IOA)

Table 18.4: Permissions required to access the Indicators of attack (IOA) lists

Indicators of attack (IOA)

This shows details of the IOAs detected by Panda Adaptive Defense on workstations and servers. The generation of IOAs follows these rules:

- Each IOA refers to a single computer and IOA type. If the same chain of suspicious events occurs on multiple computers, a separate IOA is generated for each computer.
- If the same pattern-computer-type triplet is detected several times during an hour, two IOAs will be generated: an initial one when the first is detected, and another every hour indicating the number of repetitions in the **Occurrences** field throughout that hour.

Field	Comment	Values
Computer	Name of the computer with the IOA.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Indicator of attack	Name of the rule that detected the pattern of events that triggered the IOA.	Character string
Occurrences	Number of times an IOA is repeated in 1 hour.	Number
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration
Action	Type of action taken by Panda Adaptive Defense on Brute-force attack against RDP IOAs: • Reported • Attack blocked Refer to "Automatic response to RDP attacks".	Enumeration
Status	• **Archived**: The IOA no longer requires administrator attention because it is a false positive or it has been resolved. • **Pending**: The IOA has not yet been investigated by the administrator. Refer to "Indicator of attack (IOA)".	Enumeration

Table 18.5: Fields in the 'Indicators of attack (IOA)' list

Field	Comment	Values
Date	Date and time the IOA was last detected.	Date

Table 18.5: Fields in the 'Indicators of attack (IOA)' list

- **Fields displayed in the exported file**

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer with the IOA.	Character string
Indicator of attack	Name of the rule that detected the pattern of events that triggered the IOA.	Character string
Occurrences	Number of times an IOA is repeated in 1 hour.	Number
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeración
Action	Type of action taken by Panda Adaptive Defense: • Reported • Attack blocked Refer to "**Automatic response to RDP attacks**".	Enumeration
Status	• **Archived**: The IOA no longer requires administrator attention because it is a false positive or it has been resolved. • **Pending**: The IOA has not yet been investigated by the administrator. Refer to "**Indicator of attack (IOA)**".	Numeric value
Date	Date and time the IOA was last detected.	Date
Date archived	Date it was last archived	Date
Time until archived	Time that has elapsed between the IOA's detection and the administrator verifying it and taking remedial action where necessary.	Date
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string

Table 18.6: Fields in the 'Indicators of attack (IOA)' exported file

Field	Comment	Values
Description	Brief description of the strategy used by the adversary.	Character string

Table 18.6: Fields in the 'Indicators of attack (IOA)' exported file

- **Filter tool**

Field	Description	Values
Search computer	Computer name.	Character string
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration
Action	Type of action taken by Panda Adaptive Defense: • Reported • Attack blocked Refer to "**Automatic response to RDP attacks**".	Enumeration
Dates	The time period in which the IOA was generated.	• Last 24 hours • Last 7 hours • Last month
Technique	Category of the attack technique that generated the IOA, mapped to the MITRE matrix.	Character string
Tactic	Category of the attack tactic that generated the IOA, mapped to the MITRE matrix.	Character string

Table 18.7: Filters available in the 'Indicators of attack (IOA)' list

- **Details window**

Click one of the items in the list to access the details screen. This includes a detailed description of when and where the IOA occurred, as well as details of the pattern of events recorded that led to the IOA.

Field	Comment	Values
Detection date	• Date and time the IOA was last detected. • Date the IOA was archived if it has this status. • Button to archive the IOA or to mark it as pending investigation.	

Table 18.8: Fields in the IOA details window

Field	Comment	Values
Indicator of attack (IOA)	Name of the rule that detected the pattern of events that triggered the IOA.	Character string
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration
Description	Details of the chain of events detected on the customer's computer, and the consequences it may have if the attack achieves its objectives.	Character string
Advanced attack investigation	Report with full details of the IOA: • Computer ID and date. • Detected IOA type name. • Detailed description of the internal functionality of the IOA, mapped to the relevant MITRE tactic and technique. • Operating system tools used in the attack. • Computer details. • Attack severity. • Status of the computer with respect to the attack. • Progress status of the attack. • Users logged in at the time of the attack. • IPs/URLs accessed. • Daily repetitions of the attack. • Diagram of the chain of processes involved in the attack. • Advice for mitigating or remediating the attack.	Button
View attack graph	Interactive graph with the sequence of processes that led to the IOA. Refer to "**Graphs**".	Button
Action	Type of action taken by Panda Adaptive Defense: • Reported • Attack blocked Refer to "**Automatic response to RDP attacks**".	Enumeration
Recommendations	Actions recommended by Panda Security for the administrator.	Character string
Computer	Name and group of the affected computer. If the computer is in containment mode, the **End RDP attack containment mode** button appears. Refer to "**Manual termination of RDP attack containment mode**".	Character string

Table 18.8: Fields in the IOA details window

Field	Comment	Values
Detected occurrences	Number of times an IOA is repeated in 1 hour.	Number
Last event	Date the event that triggered the IOA occurred.	Date
Other details	JSON with fields relevant to the event that led to the generation of the IOA. Refer to "**Format of events used in indicators of attack (IOA)**" on page 529.	Character string
Tactic	Category of the attack tactic that generated the IOA, mapped to the MITRE matrix.	Character string
Technique	Category of the attack technique that generated the IOA, mapped to the MITRE matrix.	Character string
Platform	Operating system and environments where MITRE has previously recorded this type of attack.	Character string
Description	Details of the tactics and techniques used by the IOA detected, according to the MITRE matrix.	Character string

Table 18.8: Fields in the IOA details window

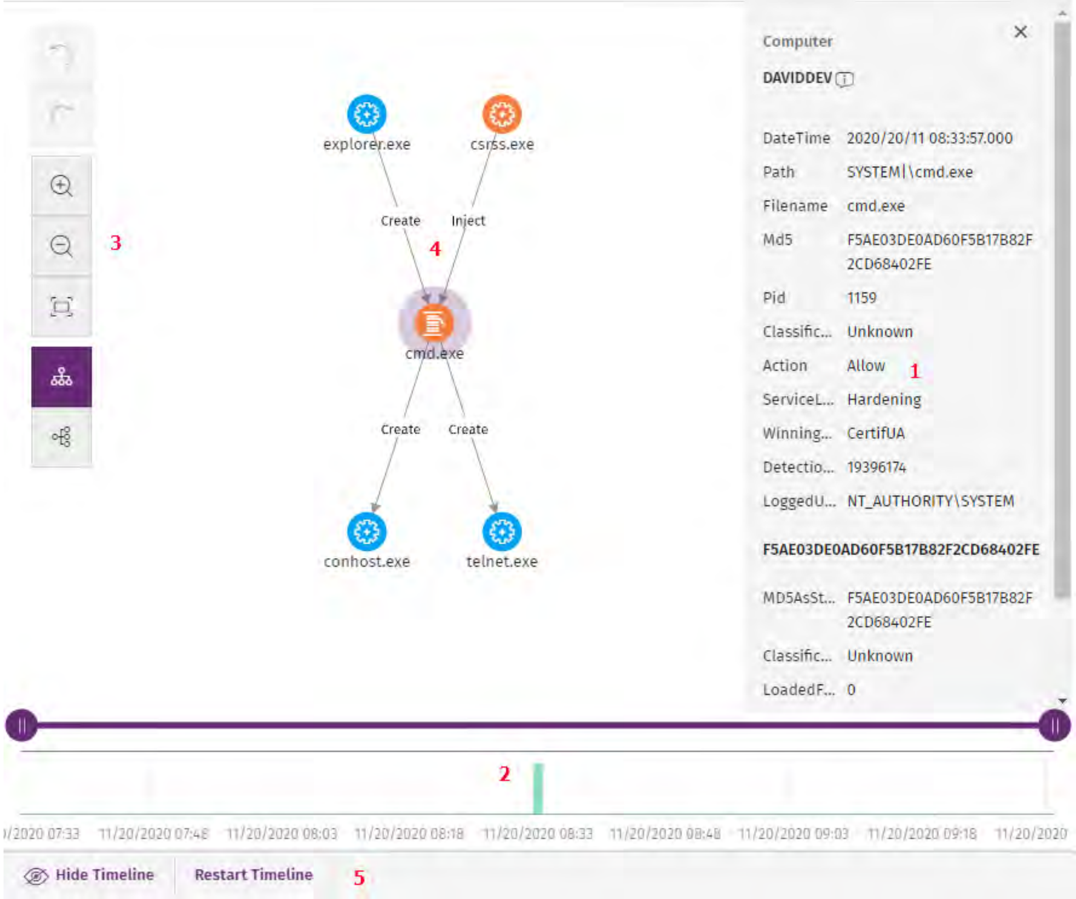
Graphs

Accessing graphs

If the IOA has a graph associated with it, the button **View attack graph** will be shown in the details window of the IOA. To see the details of an IOA, go to the **Indicators of attack (IOA)** list. Refer to "**Accessing the lists**".

Graph structure

The following is a description of the information panels and tools available in a graph:



Computer

DAVIDDEV

DateTime	2020/20/11 08:33:57.000
Path	SYSTEM|\cmd.exe
Filename	cmd.exe
Md5	F5AE03DE0AD60F5B17B82F 2CD68402FE
Pid	1159
Classific...	Unknown
Action	Allow
ServiceL...	Hardening
Winning...	CertifUA
Detectio...	19396174
LoggedU...	NT_AUTHORITY\SYSTEM

F5AE03DE0AD60F5B17B82F2CD68402FE

MD5AsSt...	F5AE03DE0AD60F5B17B82F 2CD68402FE
Classific...	Unknown
LoadedF...	0

Figure 18.1: Graph and tools

- **Information panel for the selected item (1)**: This shows information pertaining to the selected node or line. For more information about the meaning of the fields, refer to "**Format of events used in indicators of attack (IOA)**" on page 529.
- **Timeline (2)**: This shows a histogram with green bars representing the number of events logged at any time. You can extend or reduce the interval in which the events shown occurred. For more information about how to use this resource, refer to "**Timeline**".
- **Graph toolbar (3)**: This enables you to change the way the graph is shown on the page. Refer to "**Graph settings**".
- **Graph (4)**: A graphic illustration of a set of events that uses nodes and arrows to show entities and the relations between them. The order in which the creation of events has been recorded is indicated by a number in each arrow
- **Timeline controls (5)**: This enables you to hide, show, or reset the timeline. Refer to "**Timeline**".

Graph settings

To modify and adapt the graph to your needs, use the graph toolbar, along with the mouse pointer on the nodes. By default, the graph is displayed horizontally and with a sufficient level of zoom to ensure that all nodes are visible without having to move the view.

Graph toolbar

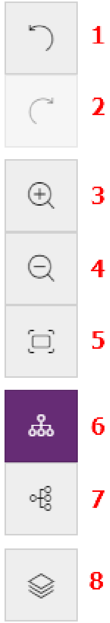


Figure 18.2: To olbar

- To undo the last action performed on the graph, click the **(1)** icon.
- To redo the last undone modification made on the graph, click the **(2)** icon.
- To zoom in on the graph, click the **(3)** icon.
- To zoom out from the graph, click the **(4)** icon.
- To reset the zoom level back to its initial value, click the **(5)** icon.
- To change the graph orientation to horizontal, click the **(6)** icon.
- To change the graph orientation to vertical, click the **(7)** icon
- To show or hide the information layers provided by the graph **(8)**, refer to "Hiding and showing layers".

Hiding and showing layers

To hide part of the information included in the graph and just show the most relevant details, click the **(8)** icon. A drop-down menu with the following options appears:

- **Execution sequence**: This hides or shows numeration of the events that enables the order in which they are run to be determined. Refer to "Arrow styles".
- **Name of relationships**: This hides or shows the names of the events. Refer to "Format of events used in indicators of attack (IOA)" on page 529.
- **Name of entities.**

Selecting nodes on the graph

- **To select a single node on the graph**: Click on the node with the left mouse button.
- **To select multiple non-contiguous nodes on the graph**: Press and hold down the control or shift key while clicking on the nodes you want to select with the left mouse button.
- **To select multiple contiguous nodes on the graph**: Press and hold down the control or shift key, click

on an empty area of the graph, and drag the mouse cursor, drawing a selection box that covers all the nodes you want to select.

By selecting and right-clicking several nodes on the graph, only the options that are common to all selected nodes will be shown in the context menu.

Moving and deleting nodes from the graph

- **To move all nodes and lines on the graph**: Click on an empty area of the graph, and drag the mouse cursor in the appropriate direction.
- **To move a single node**: select the node and drag it in the appropriate direction. All lines connecting the node with its neighbors will move, adjusting themselves to the new position of the node.
- **To delete a single node using the keyboard**:
  - Select the node to delete and press the Delete key. A message appears indicating the total number of nodes that will be deleted from the graph: the selected node and all its child nodes.
  - Click **OK**.
- **To delete a single node using the mouse**:
  - Right-click the node to delete. The context menu opens.
  - Select **Delete (x)**. A message appears indicating the total number of nodes that will be deleted from the graph: the selected node and all its child nodes.
  - Click **OK**.
- **To delete multiple nodes**:
  - Select the nodes to delete and right-click any of them. The context menu opens.
  - Select **Delete (x)**. A message appears indicating the total number of nodes that will be deleted from the graph: the selected nodes and all their child nodes.
  - Click **OK**.

Timeline

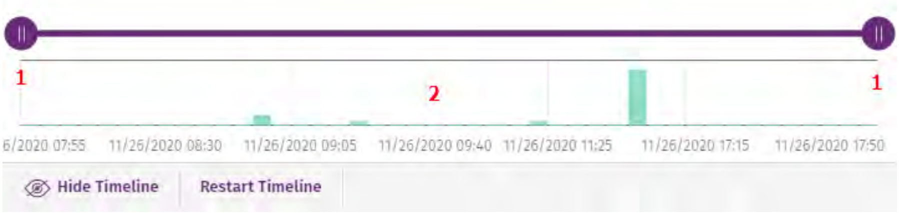


Figure 18.3: Timeline controls

The timeline enables the nodes and the relationships occurred outside the time range defined by the analyst to be dimmed. This way, the events in the events lake that are of no interest are left out of focus, enabling the analyst to concentrate on the most relevant data.

At the bottom of the timeline, there is a histogram with green bars **(2)** that represent the number of events logged at any time. Move the mouse cursor over the bars to show a tooptip indicating the number of events and the date they were logged.

To define a time range using the timeline:

- Click **(1)** and drag it to the left and right. The histogram will be expanded or reduced to fit the new interval.
- The graph will dim the nodes and relationships that are outside of the new range defined.

To hide/show the timeline:

- To hide the panel, click **Hide timeline**.
- To show it again, click **Show timeline**.
- Click **Reset timeline** to set the timeline back to its default settings.

Information contained in graphs

Graphs provide a graphical representation of the execution tree of an IOA, where nodes represent the entities that participate in an operation (processes, files, or communication or operation targets) and arrows represent operations themselves. Graphs use color codes, panels, and other resources that provide information about the represented entities and their relationships.

The resources used to present this information are:

- **Node colors**: Indicate the item classification.
- **Node icons**: Indicate the item type.
- **Status icons**: Indicate the action taken on the item.
- **Arrow colors**: Indicate whether the item was blocked or not.
- **Arrow styles**: Indicate the number and direction of the actions executed between the nodes.
- **Arrow labels**: When clicked, they show information about the action taken by the process in the right panel.
- **Node labels**: When clicked, they show information about the entity in the right panel.

Node colors

Color	Description
🔴	Item classified as malware.

Table 18.9: Color codes used in graph nodes

Color	Description
⚙	- Item classified as a PUP. - Item classified as a suspicious item. - Unclassified item.
(Original color)	Item classified as goodware.

Table 18.9: Color codes used in graph nodes

Node icons

Icon	Description	Icon	Description
⚙	Process If it belongs to a known software package, the icon is shown.	ZIP	Compressed file
≣	Remote thread	⚙	Executable file
▥	Library	</>	Script file
⛨	Protection	⊞	Windows registry branch value
🗀	Folder	🌐	URL used in a communication
🗋	Non-executable file	IP	IP address in a communication

Table 18.10: Icons used in graph nodes

Status icons

Icon	Description	Icon	Description
⚙ 🗑	File deleted	⚙ 🌡	File quarantined

Table 18.11: Icons used to indicate the status of a node

Icon	Description	Icon	Description
	File disinfected		Process deleted

Table 18.11: Icons used to indicate the status of a node

Node labels

Indicate the name of the entity. Click the entity to show a panel with fields describing it on the right of the page.

Arrow colors

Indicate whether Panda Adaptive Defense or Panda Adaptive Defense 360 blocked the action from executing because the process was classified as a threat.

- **Red**: The action was blocked.
- **Black**: The action was allowed.

Arrow styles

- **Arrow thickness**: Represents the number of times the same type of action has been executed between two nodes. The greater the number of actions, the thicker the arrow. On clicking the arrow, the information panel shows the dates on which the first and last actions in the group occurred.
- **Arrow direction**: Reflects the direction of the action.
- **Numeration**: Each arrow has a number that reflects the order in which the event it represents was recorded.

Arrow labels

Indicate the name of the action taken by the process. Click the label to display a panel with fields describing the event on the right of the page.

Node levels displayed by default

Initially, the solution places the node that triggered the IOA at the center of the graph, surrounded by a number of neighboring nodes, which are actually a subset of all nodes related to the IOA:

- **3 upper node levels**: The graph displays parent, grandparent, and great-grandparent nodes of the main node.
- **1 lower node level**: The graph displays child nodes of the main node.

The maximum number of same-level nodes that can be shown is 25. Above that limit, no nodes are shown in order to avoid overloading graphs.

Showing child nodes

If a node on the graph has hidden child nodes, they are indicated with the ⊕ icon at the bottom left of the node. To show its child nodes, right-click on the node. A context menu opens. The following options appear depending on the type of node:

- **Show parent**: Shows the parent nodes of the selected node.
- **Show all activity (number)**: Shows all the child nodes of the node regardless of the type. The maximum number of nodes shown is 25. The total number of events that relate the parent node with the child node is shown.
- **Show children**: Shows a drop-down menu with the type of child nodes to display and the number of nodes of each type:
  - **Data files**: Files with unidentified information.
  - **Script files**: Files with command sequences.
  - **DNS**: Domains that failed to resolve the IP.
  - **Windows registry entries**
  - **Compressed files**
  - **PE files**: Executable files.
  - **Remote threads**
  - **IPs**: IP addresses for either end of the communication.
  - **Libraries**
  - **Processes**
  - **Protection**: Action taken by the antivirus.

By selecting and right-clicking several nodes on the graph, only the options that are common to all selected nodes will be shown in the context menu.

Indicators of attack module panels/widgets

Accessing the dashboard

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

Required permissions

Permission	Access to widgets
View detections and threats	• Threat Hunting Service • Evolution of detections • Indicators of attack (IOA) mapped to the MITRE matrix • Indicators of attack (IOA) detected • Indicators of attack (IOA) by computer

Table 18.12: Permissions required to access the Indicators of attack widgets

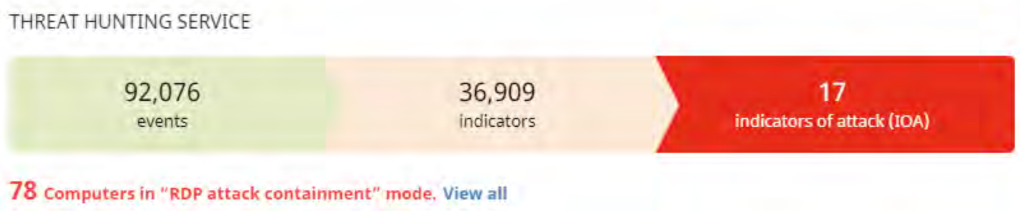
All the widgets, except Threat Hunting Service, only show information generated by the computers on the network on which the role associated with the administrator account used to access the console has visibility.

The Threat Hunting Service widget shows the following data:

- **Events**: Data from the customer's network, regardless of the account visibility.
- **Indicators**: Data from the customer's network, regardless of the account visibility.
- **Indicators of attack (IOA):** Data from the computers visible to the role of the administrator account.

Threat Hunting Service

This shows data regarding the information collected from the customer computers that the Aether platform uses as a basis to determine if there are intrusion attempts against the protected computers.



THREAT HUNTING SERVICE

92,076 events

36,909 indicators

17 indicators of attack (IOA)

78 Computers in "RDP attack containment" mode. View all

Figure 18.4: Threat Hunting Service panel

- **Meaning of the data displayed**

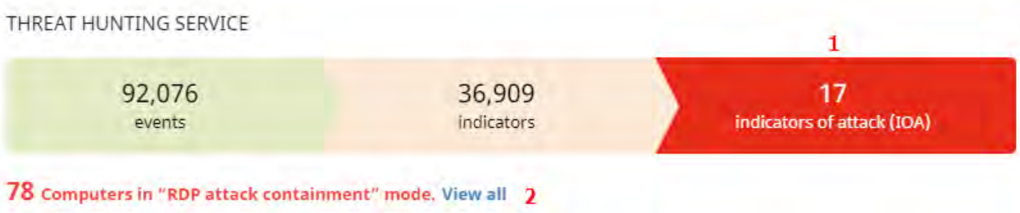
Data	Description
Events	Number of actions carried out by the programs installed on the protected computers of the customer's network, and monitored by Panda Adaptive Defense. These events are received as part of the telemetry and are stored on the Aether platform to look for suspicious patterns of behavior.
Indicators	Number of suspicious behavior patterns detected in the event data flow.
Indicators of attack (IOA)	Number of suspicious behavior patterns with a high probability of belonging to the CKC of a cyberattack.

Table 18.13: Description of the data displayed in the 'Threat Hunting Service' panel

Data	Description
Computers in RDP attack containment mode	Number of computers that have received an attack via the RDP protocol and have been configured in RDP attack containment mode.

Table 18.13: Description of the data displayed in the 'Threat Hunting Service' panel

- **Lists accessible from the panel**


THREAT HUNTING SERVICE

92,076 events

36,909 indicators

17 indicators of attack (IOA)

78 Computers in "RDP attack containment" mode. View all

Figure 18.5: Hotspots in the Threat Hunting Service panel

Click the hotspots shown in figure 18.5 to access the following list with the following predefined filters.

Hotspot	List	Filter
(1)	Indicators of attack (IOA)	No filter.
(2)	Computer protection status	RDP attack containment mode = Yes

Table 18.14: Filters accessible from the 'Threat Hunting Service' panel

Evolution of detections

This shows a line and bar graph with the evolution of the indicators, pending IOAs, and archived IOAs detected on network computers.

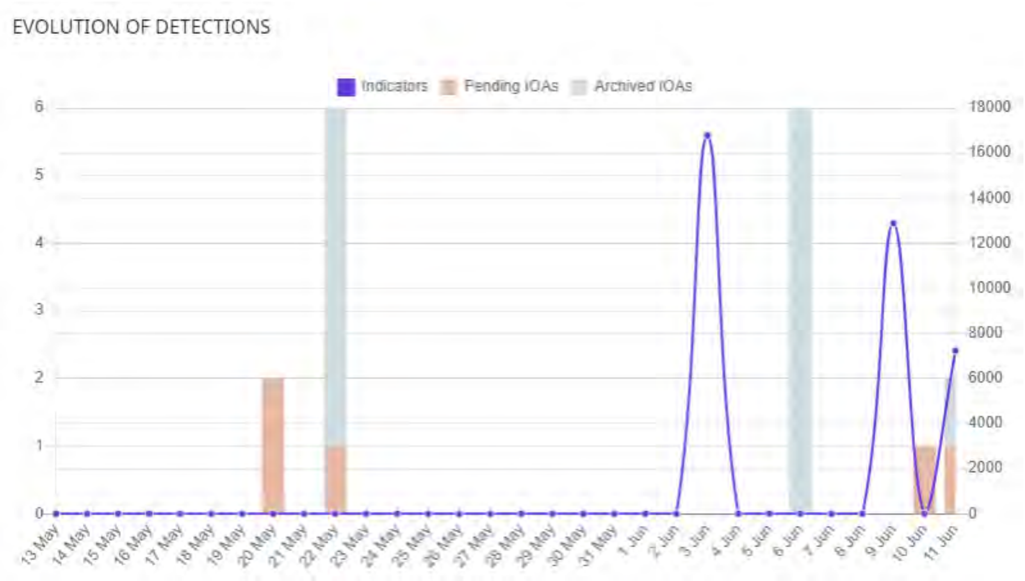


Figure 18.6: 'Evolution of detections' panel

To represent the different scales in the same diagram, the graph has two 'X' axes:

- The X-axis on the left refers to the detected pending and archived IOAs.
- The X-axis on the right refers to the indicators detected.

- **Meaning of the data displayed**

Data	Description
Indicators	Number of suspicious patterns detected in the event flow received.
Pending IOAs	Number of suspicious patterns with a high probability of belonging to the CKC of a cyberattack, and which the administrator has yet to analyze or resolve.
Archived IOAs	Number of suspicious patterns with a high probability of belonging to the CKC of a cyberattack, and which the administrator has already analyzed or resolved, and are not false positives.

Table 18.15: Description of the data displayed in the 'Evolution of detections' panel

- **Lists accessible from the panel**

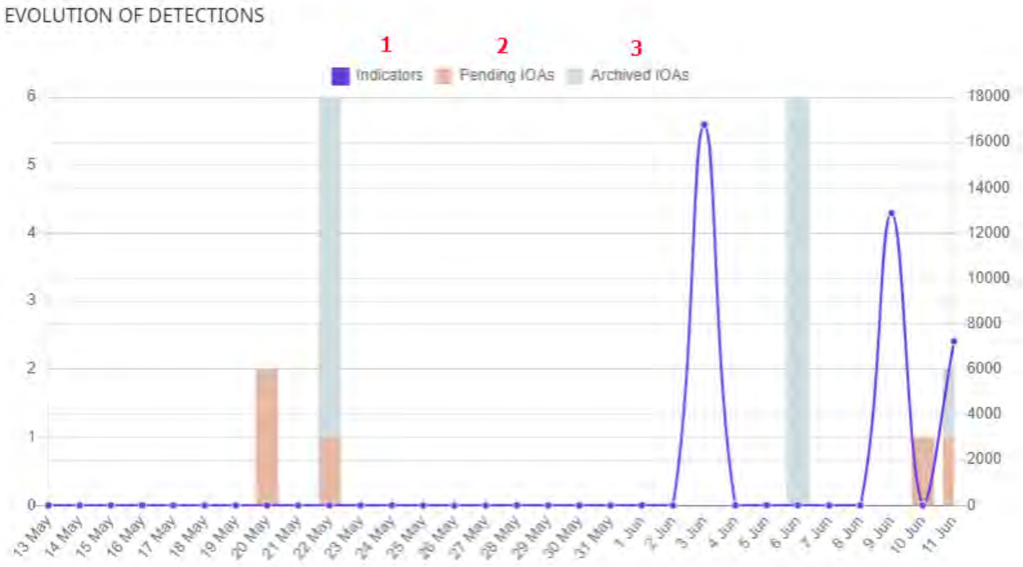


Figure 18.7: Hotspots in the 'Evolution of detections' panel

Click the hotspots shown in figure 18.7 to open the 'Indicators of attack (IOA)' list with the following predefined filters:

Hotspot	Filter
(1)	None
(2)	Status = Pending
(3)	Status = Archived

Table 18.16: Filters available in the 'Indicators of attack (IOA)' list

Indicators of attack (IOA) mapped to the MITRE matrix

This shows a matrix of indicators of attack detected during the selected period and arranged by tactic and technique. Moving the mouse pointer over each area displays a tooltip with:

- The name and code of the technique.
- Total number of detections.

- Number of detections pending.

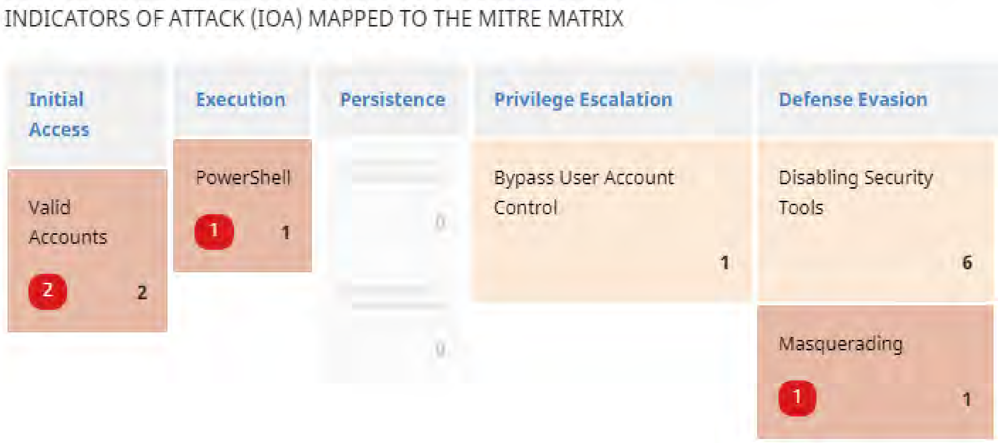

INDICATORS OF ATTACK (IOA) MAPPED TO THE MITRE MATRIX

Figure 18.8: ‘Indicators of attack (IOA) mapped to the MITRE matrix’ panel

- **Meaning of the data displayed**

Data	Description
Red number	Number of indicators of attack detected, with pending status, which use the specified tactic and technique.
Black number	Total number of detected indicators of attack (pending + archived) that use the specified tactic and technique.

Table 18.17: Description of the data displayed in the ‘Indicators of attack (IOA) mapped to the MITRE matrix’ panel

- **Lists accessible from the panel**

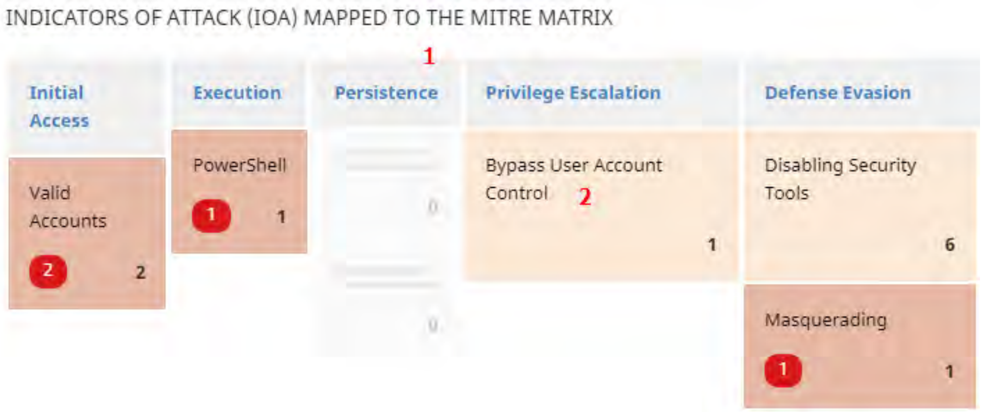

INDICATORS OF ATTACK (IOA) MAPPED TO THE MITRE MATRIX

Figure 18.9: Hotspots in the ‘Indicators of attack (IOA) mapped to the MITRE matrix’ panel

Click the hotspots shown in figure 18.9 to open the **Indicators of attack (IOA)** list with the following predefined filters:

Hotspot	Filter
(1)	Tactic = The tactic selected in the widget
(2)	• Tactic = The tactic selected in the widget • Technique = The technique selected in the widget

Table 18.18: Filters available in the 'Indicators of attack (IOA)' list

Detected indicators of attack (IOA)

Shows the distribution of indicators of attack according by type detected during the selected time period. The greater the number of detected IOAs of a particular type with respect to the rest, the larger the surface area represented in the widget.

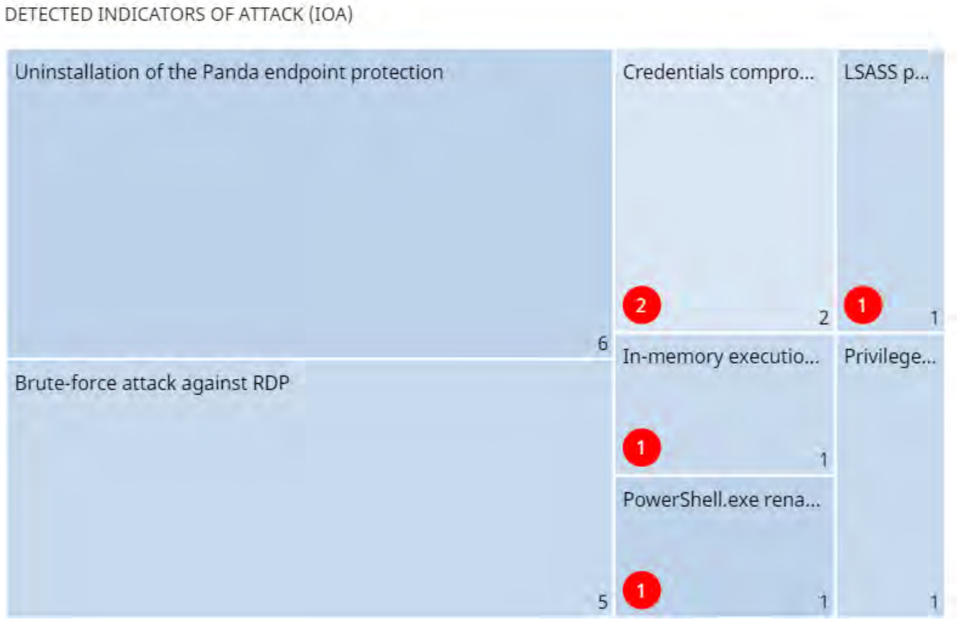

DETECTED INDICATORS OF ATTACK (IOA)
Uninstallation of the Panda endpoint protection
6
Credentials compro...
2
2
LSASS p...
1
1
Brute-force attack against RDP
5
In-memory executio...
1
1
PowerShell.exe rena...
1
1
Privilege...
1

Figure 18.10: 'Detected indicators of attack (IOA)' panel

- **Meaning of the data displayed**

Data	Description
Red number	Number of pending status indicators of attack of a given type detected during the selected period.
White number	Number of pending and archived indicators of attack of a given type detected during the selected period.

Table 18.19: Description of the data displayed in the 'Detected indicators of attack (IOA)' panel

- **Lists accessible from the panel**

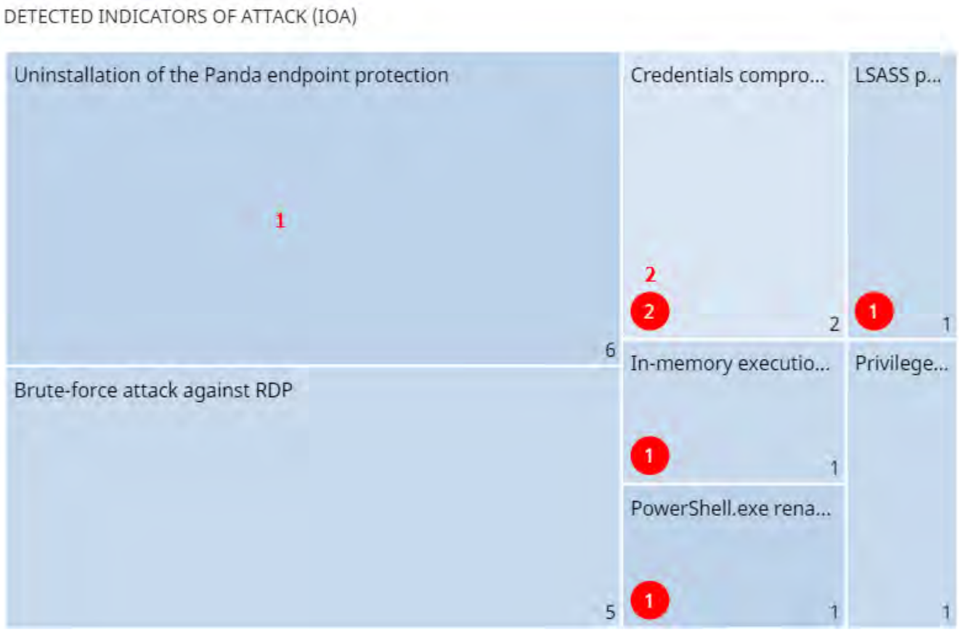

DETECTED INDICATORS OF ATTACK (IOA)
Uninstallation of the Panda endpoint protection
1
6
Credentials compro...
2
2
2
LSASS p...
1
1
Brute-force attack against RDP
5
In-memory executio...
1
1
Privilege...
PowerShell.exe rena...
1
1
1

Figure 18.11: Hotspots in the 'Detected indicators of attack (IOA)' panel

Click the hotspots shown in figure 18.11 to open the **Indicators of attack (IOA)** list with the following predefined filters.

Hotspot	Filter
(1)	Indicator of attack = Indicator of attack selected in the widget
(2)	• Indicator of attack = Indicator of attack selected in the widget • Status = Pending

Table 18.20: Filters available in the 'Indicators of attack (IOA)' list

Indicators of attack (IOA) by computer

This shows the distribution of indicators of attack for each computer on the network during the selected period. The greater the number of detected IOAs on a particular computer with respect to the rest, the larger the surface area represented in the widget.

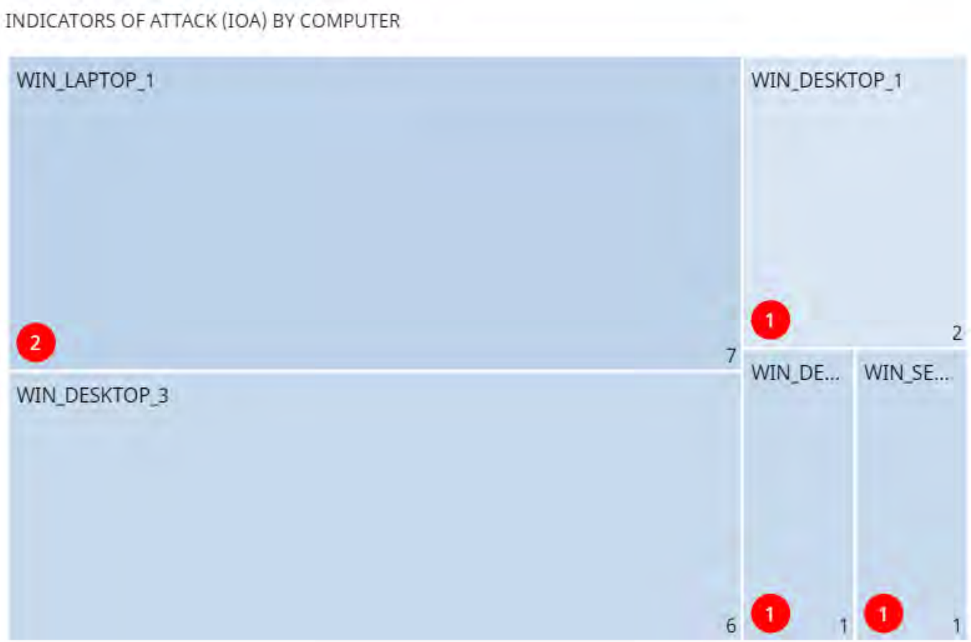


Figure 18.12: 'Indicators of attack (IOA) by computer' panel

- **Meaning of the data displayed**

Data	Description
Red number	Number of pending status indicators of attack detected on a specific computer during the selected period.
White number	Number of pending and archived indicators of attack detected on a specific computer during the selected period.

Table 18.21: Description of the data displayed in the 'Indicators of attack (IOA) by computer' panel

- **Lists accessible from the panel**

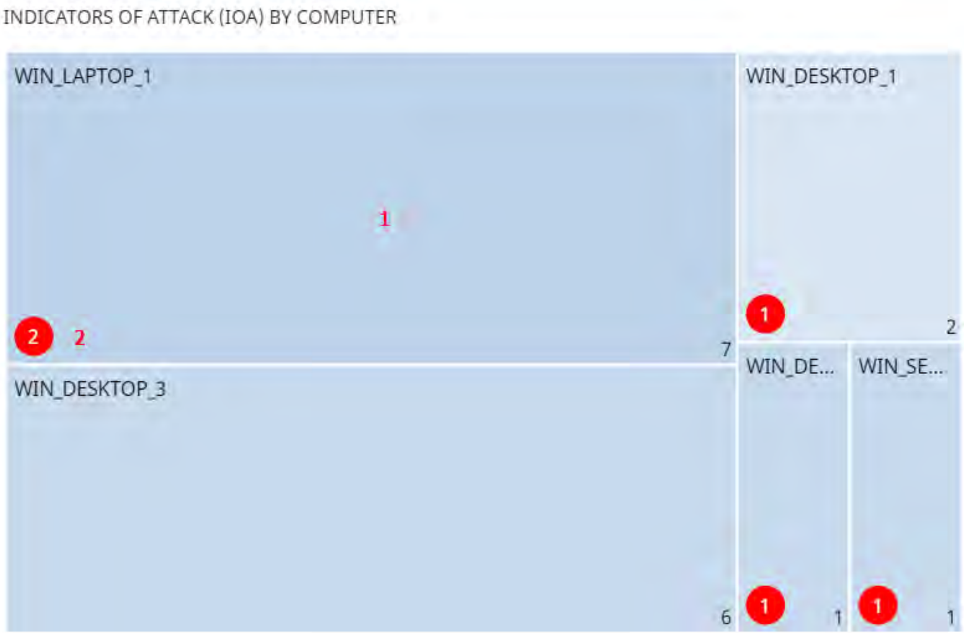


Figure 18.13: Hotspots in the 'Indicators of attack (IOA) by computer' panel

Click the hotspots shown in figure 18.13 to open the **Indicators of attack (IOA)** list with the following predefined filters:

Hotspot	Filter
(1)	Computer
(2)	• Computer • Status = Pending

Table 18.22: Filters available in the 'Indicators of attack (IOA)' list

Part 6

Viewing and managing threats

Chapter 19

Malware and network visibility

Panda Adaptive Defense offers administrators three large groups of tools for viewing the health and safety of the IT network they manage:

- The dashboard, with real-time, up-to-date information.
- Custom lists of incidents, detected malware and managed devices along with their status.
- Networks status reports with information collected and consolidated over time.

*For more information about consolidated reports, refer to "***Scheduled sending of reports and lists***" on page* **483**.

The visualization and monitoring tools determine in real time the network security status as well as the impact of any possible security breaches in order to facilitate the implementation of appropriate security measures.

CHAPTER CONTENT

Security panels/widgets

Panda Adaptive Defense shows the security status of the entire IT network or specific devices through widgets:

- **IT network**: click **Status** in the menu at the top of the console then **Security** from the side menu, You will see counters showing the security status of the computers that are visible to the administrator. Refer to "**Role structure**" on page **66** for information about how to set the computer groups that are visible to the account used to access the management console, and "**Filter by group icon**" on page **45** to restrict the visibility of the groups defined in the role.
- **Computer**: click **Computers** in the menu at the top of the console, choose a computer from the network and click the **Detections** tab. You will see counters showing the security status of the selected computer. Refer to "**Detections section (4)**" on page **183**.

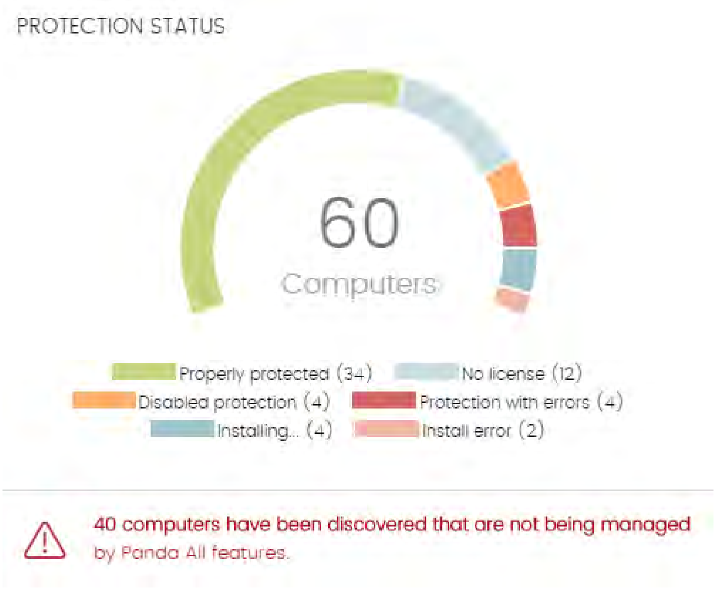
Below is a description of the different widgets displayed on the Panda Adaptive Defense dashboard, their areas and hotspots, as well as their tooltips and their meaning.

Protection status

Shows those computers where Panda Adaptive Defense is working properly and those where there have been errors or problems installing or running the protection module. The status of the network computers is represented with a circle with different colors and associated counters.

The panel offers a graphical representation and percentage of those computers with the same status.

> *The sum of all percentages can be greater than 100% as the status types are not mutually exclusive. A computer can have different statuses at the same time.*



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

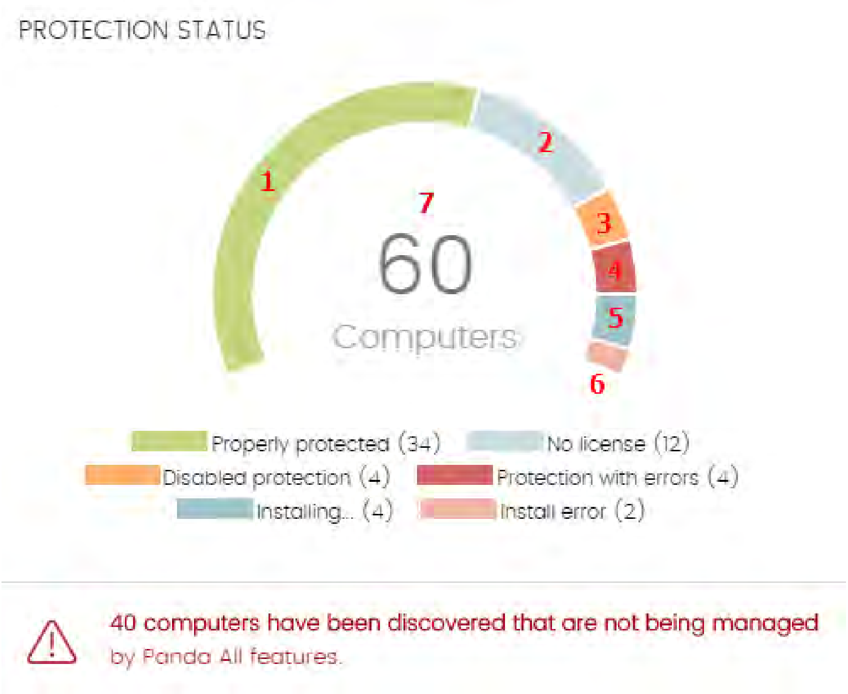
Figure 19.1: 'Protection status' panel

- **Meaning of the data displayed**

Data	Description
Properly protected	Percentage of computers where Panda Adaptive Defense installed without errors and is working properly.
Installing...	Percentage of computers on which Panda Adaptive Defense is currently being installed.
No license	Computers that are unprotected because there are insufficient licenses or because an available license has not been assigned to the computer.
Disabled protection	Computers where the advanced protection is not enabled.
Protection with errors	Computers with Panda Adaptive Defense installed, but whose protection module does not respond to the requests sent from the Panda Security servers.
Installation error	Computers on which the installation process could not be completed.
Central area	Number of computers on the network with a Panda agent installed.

Table 19.1: Description of the data displayed in the 'Protection status' panel

- **Lists accessible from the panel**



⚠ 40 computers have been discovered that are not being managed by Panda All features.

Figure 19.2: Hotspots in the 'Protection status' panel

Click the hotspots shown in figure 19.2 to access the **Computer protection status** list with the following predefined filters:

Hotspot	Filter
(1)	Protection status = Properly protected.
(2)	Protection status = Installing...
(3)	Protection status = Disabled protection.
(4)	Protection status = Protection with errors.
(5)	Protection status = No license.
(6)	Protection status = Installation error.
(7)	No filter.

Table 19.2: Filters available in the 'Computer protection status' list

Offline computers

Displays the computers that have not connected to the Panda Security cloud for a certain amount of time. These computers are susceptible to security problems and require special attention from the administrator.

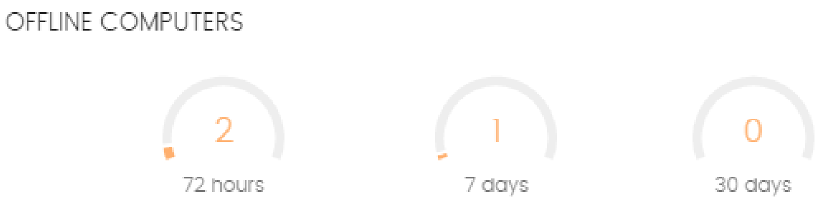


Figure 19.3: 'Offline computers' panel

- **Meaning of the data displayed**

Data	Description
72 hours	Number of computers that have not reported their status in the last 72 hours.
7 days	Number of computers that have not reported their status in the last 7 days.
30 days	Number of computers that have not reported their status in the last 30 days.

Table 19.3: Description of the data displayed in the ‘Offline computers’ panel

- **Lists accessible from the panel**

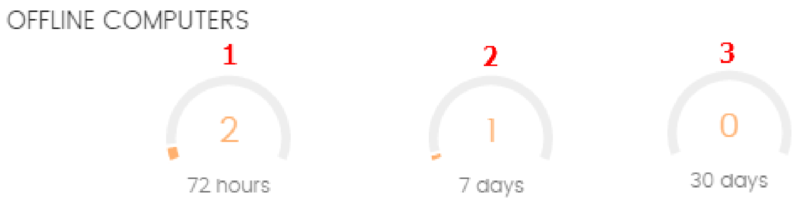


Figure 19.4: Hotspots in the 'Offline computers' panel

Click the hotspots shown in the figure 19.4 to access the **Offline computers** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 19.4: Filters available in the 'Offline computers' list

Outdated protection

Displays the computers whose signature file is more than three days older than the latest one released by Panda Security. It also displays the computers whose antivirus engine is more than seven days older than the latest one released by Panda Security. Such computers are therefore vulnerable to attacks from threats.

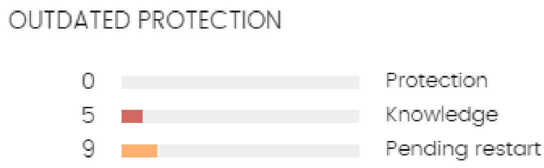


Figure 19.5: 'Outdated protection' panel

- **Meaning of the data displayed**

The panel shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts:

Data	Description
Protection	For at least seven days, the computer has had a version of the antivirus engine older than the latest one released by Panda Security.
Knowledge	It has been at least three days since the computer has updated its signature file.
Pending restart	The computer requires a restart to complete the update.

Table 19.5: Description of the data displayed in the 'Outdated protection' panel

- **Lists accessible from the panel**

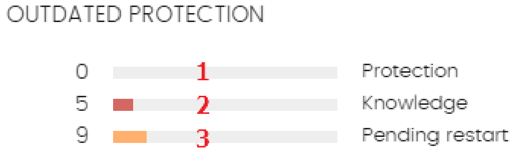


Figure 19.6: Hotspots in the 'Outdated protection' panel

Click the hotspots shown in the figure 19.6 to access the **Computers with out-of-date** protection list with the following predefined filters:

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

Table 19.6: Filters available in the 'Computers with out-of-date protection' list

Malware/PUP activity

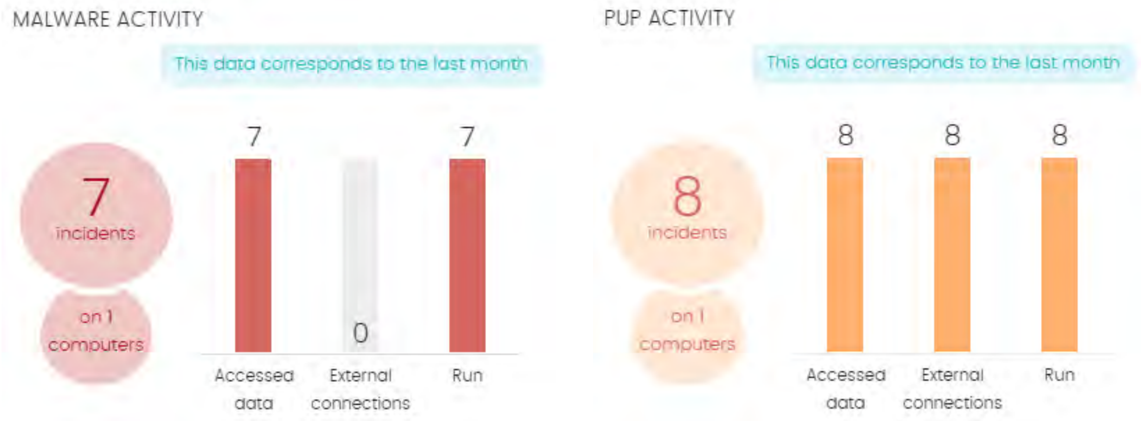


Figure 19.7: 'Malware/PUP activity' panel

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 generates an incident in the Malware/PUP activity panel under the following circumstances:

- For each computer-threat pair found on the network.
- If an incident occurs multiple times in 5 minutes, only the first one will be registered.
- The same incident can be registered a maximum of 2 times every 24 hours.

- **Meaning of the data displayed**

Data	Description
Number of incidents	Number of incidents/alerts & number of computers where they have been detected.
Accessed data	Number of alerts that involve 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 that managed to run.

Table 19.7: Description of the data displayed in the 'Malware/PUP activity' panels

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**

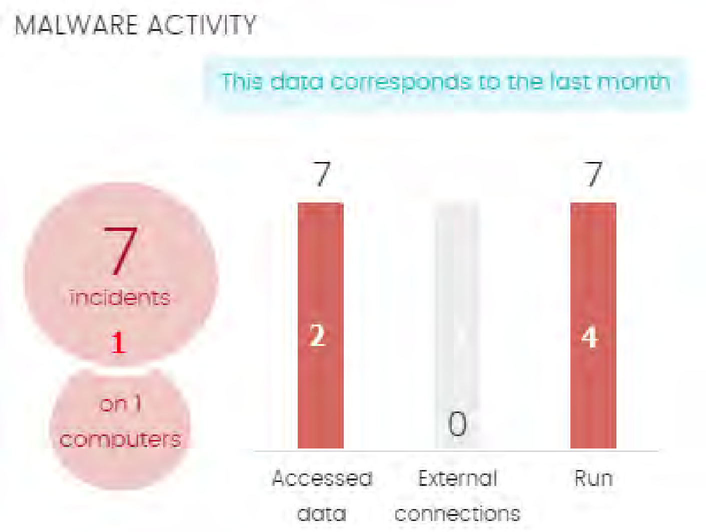


Figure 19.8: Hotspots in the 'Malware/PUP activity' panels

Click the hotspots shown in the figure 19.8 to access the **Malware activity** list with the following predefined filters:

Hotspot	Filter
(1)	Threat type = Malware OR PUP.
(2)	Accessed data = True.
(3)	External connections = True.

Table 19.8: Filters available in the 'Malware/PUP activity' list

Hotspot	Filter
(4)	Run = True.

Table 19.8: Filters available in the 'Malware/PUP activity' list

Exploit activity

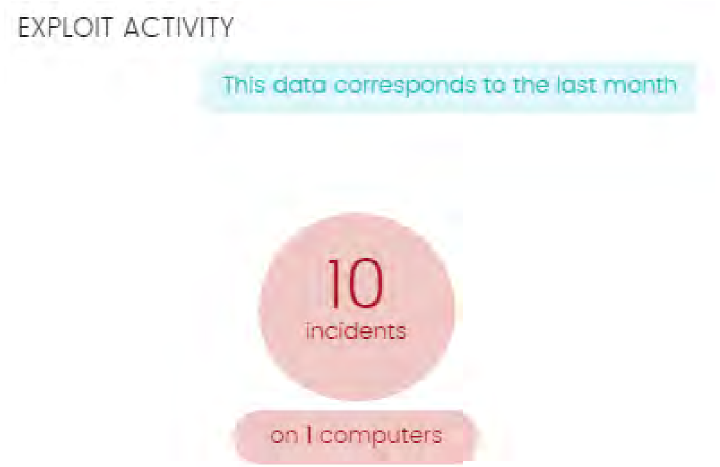


Figure 19.9: 'Exploit activity' panel

Shows the number of vulnerability exploit attacks suffered by the Windows computers on the network. Panda Adaptive Defense reports an incident in the Exploit activity panel for each computer/different exploit attack pair found on the network. If an attack is repeated several times, a maximum of 10 incidents will be reported every 24 hours for each computer-exploit pair found.

- **Meaning of the data displayed**

Data	Description
Number of incidents/attacks	Number of incidents/attacks & number of computers where they have been detected.

Table 19.9: Description of the data displayed in the 'Exploit activity' panel

- **Lists accessible from the panel**

Regardless of where you click in the panel, the **Exploit activity** list displayed will always show a list of all the exploits detected across the network, with no filters.

Classification of all programs run and scanned

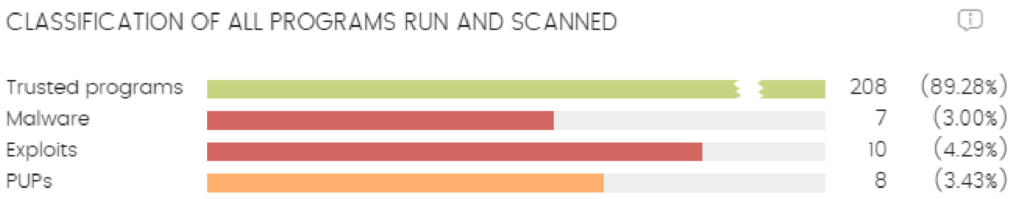


Figure 19.10: 'Classification of all programs run and scanned' panel

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 data displayed**

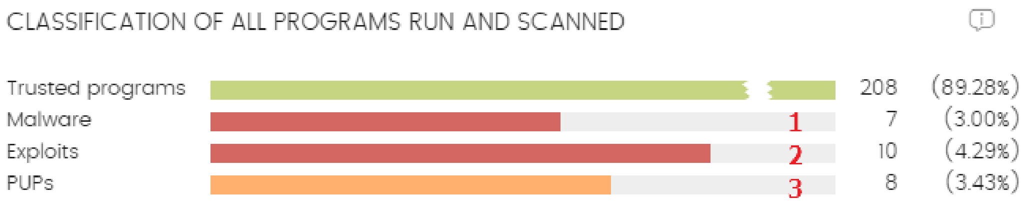
The panel displays four horizontal bars, along with the number of events associated with each category and a percentage over the total number of events.

> *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.*

Data	Description
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 as malware or a targeted attack.
Exploits	Number of attempts to exploit the applications installed across the
PUPs	Programs that attempted to run or were scanned in the selected period, and were classified as a PUP.

Table 19.10: Description of the data displayed in the 'Classification of all programs run and scanned' panel

- **List accessible from the panel**


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 19.11: Hotspots in the 'Classification of all programs run and scanned' panel

Click the hotspots shown in the figure 19.11 to access lists with the following predefined filters:

Hotspot	Filter
(1)	Malware activity list.
(2)	Exploit activity list.
(3)	PUP activity list.

Table 19.11: Lists accessible from the 'Classification of all programs run and scanned' panel

Security module lists

The security lists display the information collected by Panda Adaptive Defense in connection with computer protection activities. They provide highly detailed information as they contain the raw data used to generate the widgets.

There are two ways to access the security lists:

- Go to the **Status** menu at the top of the console and click **Security** from the side panel. Click any of the available widgets to access its associated list. Depending on the item you click on the widget, you'll access different lists with predefined filters.

Alternatively,

- Go to the **Status** menu at the top of the console and click **Add** from the **My lists** side panel. A window will be displayed showing all lists available in Panda Adaptive Defense.
- Click any of the lists in the Security section. The list will open with no filters applied.

Click any of the entries on the list to open a new window with more details about that particular item.

Computer protection status

This list shows all computers on the network, with filters to allow you to search for those computers and mobile devices that are unprotected for some specific reason.

To ensure correct operation of the protection, the computers on the network must communicate with the Panda Security cloud. See the list of URLs that must be accessible from computers in section "Access to service URLs" on page 526

Field	Description	Values
Computer	Computer name.	Character string
Computer status	Agent reinstallation: • ⚙ Reinstalling the agent. • ⚙ Agent reinstallation error. Protection reinstallation: • ⚙ Reinstalling the protection. • ⚙ Protection reinstallation error. • ↻ Pending restart. Computer isolation status: • 🖥 Computer in the process of being isolated. • 🖥 Isolated computer. • 🖥 Computer in the process of stopping being isolated "RDP attack containment" mode: • 👤 Computer in "RDP attack containment" mode. • 👤 Ending "RDP attack containment" mode	Icon
Group	Folder within the Panda Adaptive Defense folder tree to which the computer belongs.	• Character string • 📁 'All' group • 📁 Native group • AD Active Directory group
Advanced protection	Advanced protection status	• ☁ Installing • 🛡 Error. If it is a known error, the cause of the error will be displayed. If it is an unknown error, the error code will be displayed instead

Table 19.12: Fields in the 'Computer protection status' list

Field	Description	Values
		• ⊗ Error • ✓ Enabled • ! Disabled • ∅ No license
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released. Hover the mouse pointer over the field to see the version of the installed protection.	• ✓ Updated. • ⊗ Not updated (7 days without updating since last release). • ↻ Pending restart.
Knowledge	Indicates whether or not the signature file found on the computer is updated to the latest version. Hover the mouse pointer over the field to see the date that the file was last updated.	• ✓ Updated. • ⊗ Not updated (3 days without updating since last release).
Connection to knowledge	Indicates whether the computer can communicate with the Panda Security cloud to send monitored events and download security intelligence.	• ✓ Connection OK • ⊗ One or more services are not accessible • — Information not available
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	Date

Table 19.12: Fields in the 'Computer protection status' list

- **Fields displayed in the exported file**

Field	Description	Values
Client	Customer account that the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string

Table 19.13: Fields in the 'Computer protection status' exported file

Field	Description	Values
Description	Description assigned to the computer.	Character string
Group	Folder within the Panda Adaptive Defense folder tree to which the computer belongs.	Character string
Agent version	Internal version of the Panda agent module.	Character string
Installation date	Date when the Panda Adaptive Defense 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
Operating system	Operating system installed on the computer, internal version and patch status.	Character string
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released.	Binary value
Protection version	Internal version of the protection module.	Character string
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Last update on	Date when the signature file was last updated.	Date
Advanced protection Program blocking	Status of the associated protection.	• **Not installed** • **Error**: if it is a known error, the cause of the error will be displayed. If it is an unknown error, the error code will be displayed instead • **Enabled** • **Disabled** • **No license**

Table 19.13: Fields in the 'Computer protection status' exported file

Field	Description	Values
Advanced protection mode	Current configuration of the advanced protection module.	• Audit • Hardening • Lock
Isolation status	Indicates whether or not the computer is isolated from the rest of the network.	• Isolated • Not isolated
Error date	If an error took place installing Panda Adaptive Defense, date and time of the error.	Date
Installation error	If an error took place installing Panda Adaptive Defense, error description.	Character string
Instalation error code	Displays codes that identify the installation error occurred.	Codes are separated by “;”: • Error code • Extended error code • Extended error subcode
Other security products	Name of any third-party antivirus product found on the computer at the time of installing Panda Adaptive Defense.	Character string
Connection for collective intelligence	Shows the status of the connection between the computer and the servers that store signature files and security intelligence.	• OK • With problems
Connection for sending events	Shows the status of the connection between the computer and the servers that receive the events monitored on protected computers.	• OK • With problems
“RDP attack containment” mode	Status of the “RDP attack containment” mode.	• All • No • Yes

Table 19.13: Fields in the 'Computer protection status' exported file

- **Filter tool**

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server

Table 19.14: Filters available in the 'Computer protection status' list

Field	Description	Values
Find computer	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	Character string
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the Panda Adaptive Defense status was last sent to Panda Security's cloud.	• All • More than 72 hours ago • More than 7 days ago • More than 30 days ago
Updated protection	Indicates whether or not the installed protection is updated to the latest version released.	• All • Yes • No • Pending restart
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Connection to knowledge servers	Indicates whether the computer can communicate with the Panda Security cloud to send monitored events and download security intelligence.	• **All** • **OK** • **With problems**: one or more services are not accessible
Protection status	Status of the protection module installed on the computer.	• Installing... • Properly protected • Protection with errors • Disabled protection • No license • Installation error

Table 19.14: Filters available in the 'Computer protection status' list

Field	Description	Values
Isolation status	Computer isolation status.	• Not isolated • Isolated • Isolating • Stopping isolation
"RDP attack containment" mode	Status of the "RDP attack containment" mode.	• All • No • Yes

Table 19.14: Filters available in the 'Computer protection status' list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to "Details section (3)" on page 179 for more information.

Malware/PUP activity

Shows a list of all threats found on the computers protected with Panda Adaptive Defense. This list provides 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 organization's security policies.

Field	Comments	Values
Computer	Name of the computer where the threat was detected.	Character string
Threat	Name of the detected threat.	Character string
Path	Full path to the infected file.	Character string
Run sometime	The threat ran and the computer might be compromised.	Binary value
Accessed data	The threat accessed data on the user's computer.	Binary value
External connections	The threat communicated with remote computers to send or receive data.	Binary value
Action	Action taken on the threat.	• Quarantined • Blocked • Disinfected • Deleted • Detected
Date	Date when the threat was detected on the computer.	Date

Table 19.15: Fields in the 'Malware/PUP activity' list

- **Fields displayed in the exported file**

*The context menu of the 'Malware/PUP activity' list displays two options: Export and Export list and details. This section deals with the content of the file obtained when selecting Export. For more information about the Export list and details option, refer to "***Excel spreadsheets***" on page* ***468***.

Field	Comments	Values
Computer	Name of the computer where the threat was detected.	Character string
Threat	Name of the detected threat.	Character string
Path	Full path to the infected file.	Character string
Action	Action taken on the malware.	• Quarantined • Blocked • Disinfected • Deleted • Allowed
Run sometime	The threat ran and the computer might be compromised.	Binary value
Accessed data	The threat accessed data on the user's computer.	Binary value
External connections	The threat communicated with remote computers to send or receive data.	Binary value
Excluded	The threat was excluded by the administrator, allowing it to run.	Binary value
Date	Date when the threat was detected.	Date
Dwell time	Time that the threat was on the customer's network without classification.	Time period
User	User account under which the threat was run.	Character string
Hash	String identifying the file.	Character string
Infection source computer	Name of the computer the infection attempt originated from, if applicable.	Character string
Infection source IP address	IP address of the computer the infection attempt originated from, if applicable.	Character string
Infection source user	The user that was logged in on the computer the infection attempt originated from, if applicable.	Character string

Table 19.16: 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 identifying the file. • **Infection source**: lets you search by the user, IP address or name of the computer that the infected file came from.	Character string
Type	Type of threat.	• Malware • PUP
Dates	Lets you set the time period, from the current moment back.	• Last 24 hours • Last 7 days • Last month • Last year
Run	The threat ran and the computer might be compromised.	Binary value
Action	Action taken on the threat.	• Quarantined • Blocked • Disinfected • Deleted • Allowed
Accessed data	The threat accessed data on the user's computer.	Binary value
External connections	The threat communicated with remote computers to send or receive data.	Binary value

Table 19.17: Filters available in the 'Malware/PUP activity' list

- **Details window**

Shows detailed information about the program classified as malware/PUP. For more information, refer to "Malware detection" on page 452.

Exploit activity

Shows a list of all computers with programs compromised by vulnerability exploit attempts. This list provides 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 organization's security policies.

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
Exploit technique	Identifier of the technique used to exploit the program vulnerability.	Character string
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**: the anti-exploit protection was configured in 'Audit' mode and the exploit was allowed to run. • **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.	Enumeration
Date	Date when the exploit attempt was detected on the computer.	Date

Table 19.18: Fields in the 'Exploit activity' list

- **Fields displayed in the exported file**

*The context menu of the 'Exploit activity' list displays two options: Export and Export list and details. This section deals with the content of the file obtained when selecting Export. For more information about the Export list and details option, refer to "***Excel spreadsheets***" on page* **468**.

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
Exploit technique	Identifier of the technique used to exploit the program vulnerability.	Character string
User	User account under which the program that received the exploit attack was run.	Character string
Action	Action taken on the exploit. • **Allowed**: the anti-exploit protection was configured in 'Audit' mode and the exploit was allowed to run. • **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.	Enumeration
Exploit run	Indicates if the exploit managed to run or was blocked before it could affect the vulnerable program.	Binary value
Date	Date when the exploit attempt was detected on the computer.	Date

Table 19.19: Fields in the 'Exploit activity' exported file

- **Filter tool**

Field	Comments	Values
Search	• **Computer**: device on which the threat was detected. • **Hash**: string identifying the compromised program. • **Compromised program:** name or path of the compromised file.	Enumeration

Table 19.20: Filters available in the 'Exploit activity' list

Field	Comments	Values
Dates	Lets you set the time period, from the current moment back.	• Last 24 hours • Last 7 days • Last month
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**: the anti-exploit protection was configured in 'Audit' mode and the exploit was allowed to run. • **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.	Enumeration

Table 19.20: Filters available in the 'Exploit activity' list

- **Details window**

Shows detailed information about the program classified as an exploit. For more information, refer to "Exploit detection" on page 455.

Chapter 20

Managing threats, items in the process of classification, and quarantine

Panda Adaptive Defense provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This balance is achieved through tools that enable you to manage the way detected programs are blocked from executing:

- Programs classified as malware.
- Programs classified as PUPs.
- Programs classified as exploits.
- Programs classified as viruses.
- Unknown programs in the process of classification.

*For more information on how to allow the execution of unknown programs in the process of classification, refer to “**Authorized software settings**” on page 361.*

*For more information about the Hardening and Lock modes of the advanced protection, refer to “**Advanced permanent protection**”.*

CHAPTER CONTENTS

Introduction to threat management tools

Network administrators can change the behavior of Panda Adaptive Defense with regard to found threats and unknown files in the process of classification using the following tools:

- Unblock/stop allowing the execution of unknown processes.
- Delete unknown processes from lists.
- Allow/stop allowing the execution of programs classified as malware, PUPs, viruses, or exploits.
- Change the Panda Adaptive Defense reclassification policy.
- Manage the backup/quarantine area.

Unblock/stop allowing the execution of unknown processes

Panda Adaptive Defense automatically analyzes and classifies all unknown processes in the cloud within the first 24 hours after they are first seen on a workstation or server. This process issues an unambiguous classification (goodware or malware), which is shared with all Panda Security customers so that they can all benefit from the accumulated knowledge.

To strengthen the security of the computers on the network, Panda Adaptive Defense provides the **Hardening** and **Lock** modes in the advanced protection settings. In both modes, Panda Adaptive Defense blocks the execution of processes during the time it takes to classify them, thereby preventing potential risks. This prevents users from running blocked processes until the classification process is complete. The classification process can be performed in two different ways:

- **Automated analysis**: accounts for most cases and takes place in real time.
- **Manual analysis**: if the automated analysis cannot return a classification of the unknown process

with 99.999% certainty, the sample will be manually analyzed by a malware expert. When that happens, the analysis might take some time.

In circumstances where classification is not immediate, the administrator may decide to take a certain risk and allow the execution of the item. Panda Adaptive Defense provides two strategies for doing this:

- **Reactive unblocking**: the administrator allows the execution of an unknown item in the process of classification after the user has attempted to use it and Panda Adaptive Defense has detected and blocked it. Refer to "**Allowing and preventing items to run**".
- **Proactive unblocking**: occurs when the administrator wants to make sure, in advance, that a specific set of programs will not be blocked if they are unknown to Panda Adaptive Defense . The aim of this strategy is to prevent any potential negative impact on user performance, Refer to "**Authorized software settings**" on page **361**.

Allow/stop allowing the execution of malware, PUPs, or exploits

Administrators can allow the execution of software that implements features valued by users but which has been classified as a threat. That is the case of PUPs, for example. These are often toolbars which provide search capabilities but also collect users' private data and confidential corporate information for advertising purposes. Refer to "**Allowing and preventing items to run**".

Change the reclassification policy

After the administrator unblocks an unknown item previously blocked by Panda Adaptive Defense, the classification process will, after some time, catalog the item as malware or goodware. If it is goodware, there are no additional considerations to be made, as Panda Adaptive Defense will continue to allow the item to run. However, if it is malware, the reclassification policy will be applied, which enables the administrator to define the behavior of Panda Adaptive Defense. Refer to "**Reclassification policy**".

Manage the backup/quarantine area

Administrators can retrieve items considered threats and therefore deleted from users' computers.

Behavior of the security software

- **Known files**

If a file is classified as malware/PUP/exploit and an advanced protection policy other than **Audit** is applied, the file will be blocked unless the administrator allows it to run.

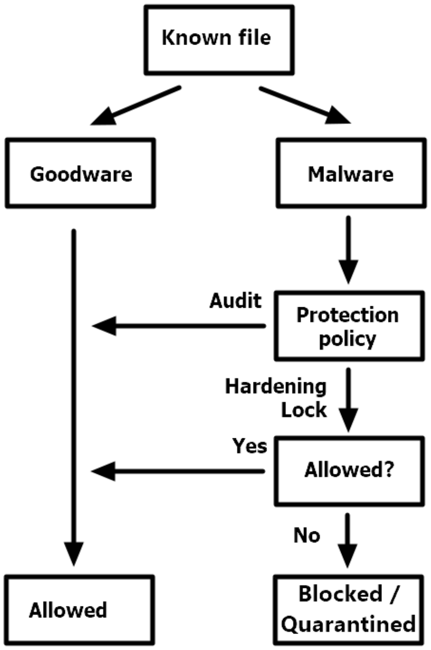


Figure 20.1: Activity diagram for known, classified processes

- **Unknown files**

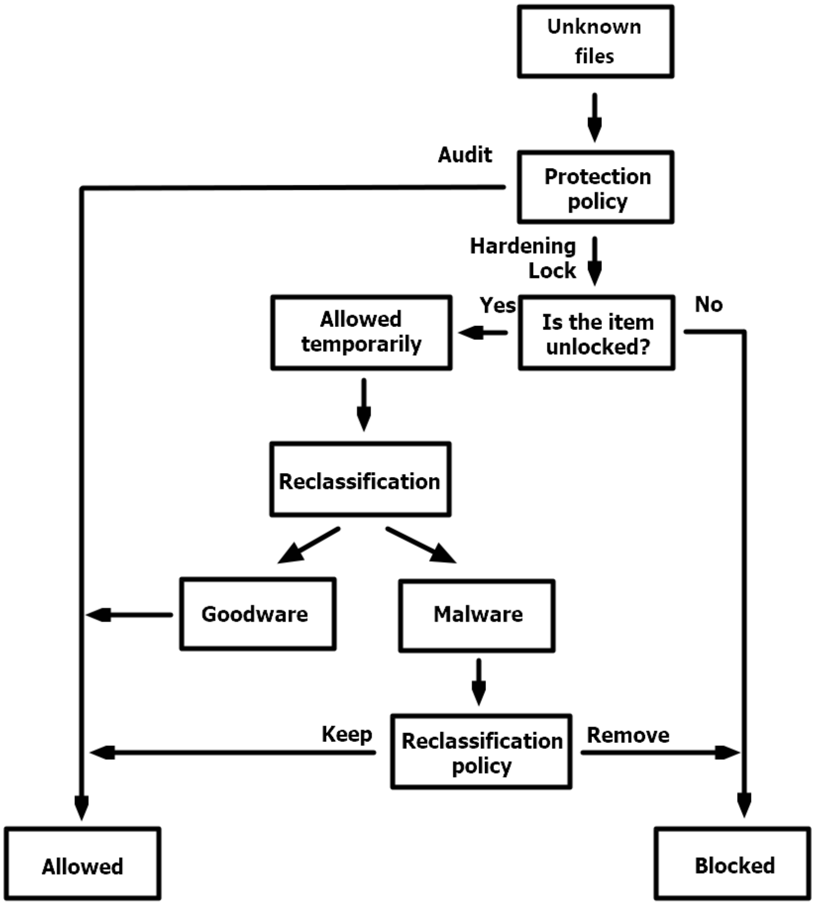


Figure 20.2: Activity diagram for unknown files

With unknown files in the process of classification and an advanced protection policy other than **Audit, Panda Adaptive Defense** will behave as follows:

- If the administrators has not configured the unblocking of the files, they will be blocked.
  - If, once classified, the files are goodware, they will be allowed to run.
  - If, once classified, the files are malware, they will be prevented from running.
- If the administrators has configured the unblocking of the files, they will be allowed to run while the classification process completes. After the process is completed:
  - If the file is goodware, it will continue to be allowed to run.
  - If the file is malware, it will be allowed or prevented from running based on the reclassification policy set by the administrator. Refer to "**Reclassification policy**"

Allowing and preventing items to run

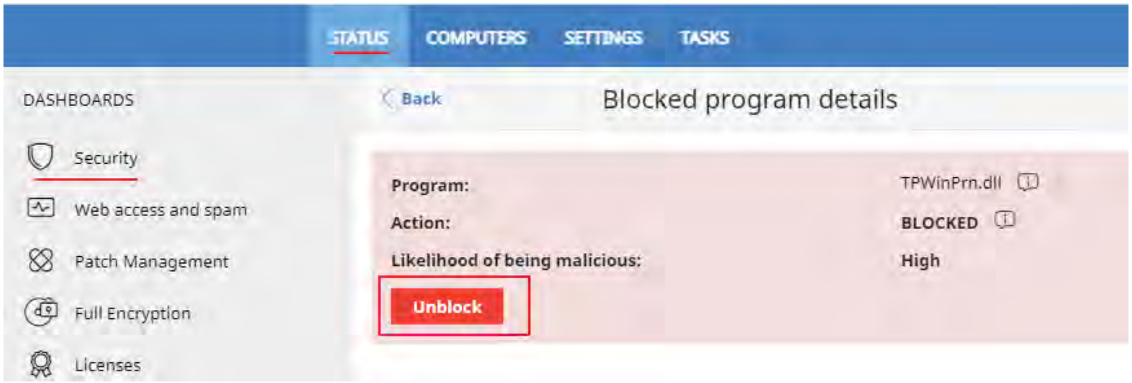
Depending on the type of program that the administrator wants to allow to run, the following panels must be used:

- **Currently blocked programs being classified**: enables you to to unblock items in the process of classification.
- **Malware activity:** enables you to allow the execution of programs classified as malware.
- **PUP activity:** enables you to allow the execution of programs classified as PUPs.
- **Exploit activity:** enables you to allow the execution of exploit techniques.

Unblocking unknown items pending classification

In general, it is not recommended to allow the execution of unclassified items, as this could pose a risk to the integrity of the company data and IT systems.

If users cannot wait for Panda Adaptive Defense to complete the classification of an item to unblock it automatically, the administrator can unblock it manually.



Program: TPWinPrn.dll
Action: BLOCKED
Likelihood of being malicious: High

Figure 20.3: Unblocking an unknown item in the process of classification

To allow the execution of an unknown item in the process of classification:

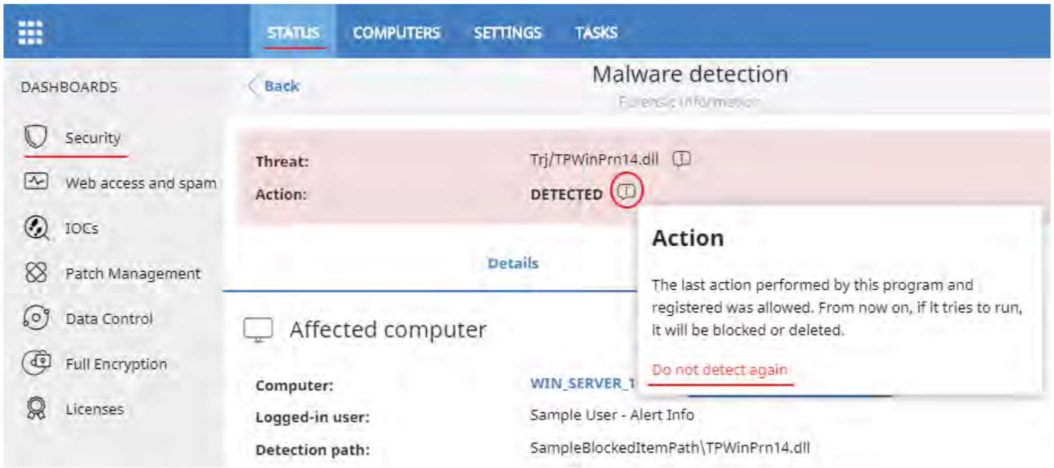
- Click the **Status** menu at the top of the console. Then, click **Security** from the side panel.
- Click on the **Currently blocked programs being classified** panel and select the item you want to unblock from the list.
- Click **Unblock**. A window opens informing you of the risk of unblocking an unknown item, along with a provisional assessment of its risk level.
- Click **Unblock**. Panda Adaptive Defense will perform the following actions:
  - The item will be allowed to run on all managed computers on the IT network.
  - In addition to that, all libraries and binary files used by the program will also be allowed to run, except for those already known and classified as threats.

- The item will be removed from the **Currently blocked programs being classified** list.
- The item will be added to the **Programs allowed by the administrator** list.
- The item will be added to the **History of programs allowed by the administrator** list
- Panda Adaptive Defense will continue to analyze the item until it is finally classified.

Allowing the execution of items classified as malware, PUPs, or exploits

> ⚠ *In general, it is not recommended to allow the execution of items classified as threats, as this poses a clear risk to the integrity of the company data and IT systems.*

If users need to use certain features provided by a program classified as a threat and the administrator considers that the danger posed to the integrity of the managed IT network is low, the administrator can allow the program to run.



Malware detection

Forensic information

Threat: Trj/TPWinPrn14.dll

Action: DETECTED

Affected computer

Computer: WIN_SERVER_1

Logged-in user: Sample User - Alert Info

Detection path: SampleBlockedItemPath\TPWinPrn14.dll

Action

The last action performed by this program and registered was allowed. From now on, if it tries to run, it will be blocked or deleted.

Do not detect again

Figure 20.4: Allowing a threat to run

To allow the execution of a program classified as malware, PUP, or exploit:

- Click the **Status** menu at the top of the console. Then, click **Security** from the side panel.
- Click on the **Malware/PUP/Exploit activity** panel and select the threat that you want to allow to run.
- Click the ⓘ icon in the **Action** field. A window opens explaining the action taken by Panda Adaptive Defense.
- Click the **Do not detect again** link. Panda Adaptive Defense will perform the following actions:
  - The item will be allowed to run on all computers managed by the administrator. With exploits, you will allow the execution of the specific exploit technique that was used on the specific vulnerable program.
  - In addition to that, all libraries and binary files used by the program will also be allowed to run, except for those already known and classified as threats.
  - The item will be added to the **Programs allowed by the administrator** list.

- The item will no longer generate incidents in the **Malware/PUP/Exploit activity** panels.

Stopping allowing the execution of previously allowed items

To block again an item previously allowed by the administrator:

- Click the **Status** menu at the top of the console. Then, click **Security** from the side panel.
- In the **Programs allowed by the administrator** panel, click the type of item that you want to stop allowing to run: **Malware**, **PUP**, **Exploit,** or **Being classified**.
- In the **Programs allowed by the administrator** list, click the 🗑 icon to the right of the item that you want to stop allowing to run:

After you click the 🗑 icon, Panda Adaptive Defense will perform the following actions:

- The item will be removed from the **Programs allowed by the administrator** list.
- An entry will be added to the **History of programs allowed by the administrator** list, with the **Action** column showing the value **Exclusion removed by the user**.
- If the item is classified as malware, PUP, exploit, or virus, it will reappear in the relevant list:
  - **Malware activity**
  - **PUP activity**
  - **Exploit activity**
  - **Threats detected by the antivirus**
- If the item is classified as malware, PUP, exploit, or virus, it will generate incidents again.
- If the item is an unknown item in the process of classification, it will reappear in the **Currently blocked programs being classified** list.

Information about blocked threats

Network administrators have multiple panels and lists available to get information about programs classified as threats:

- **Classification of all programs run and scanned**: refer to "Classification of all programs run and scanned" on page 411 .
- **Malware activity**: refer to "Malware/PUP activity" on page 408.
- **PUP activity**: refer to "Malware/PUP activity" on page 408.
- **Exploit activity:** refer to "Exploit activity" on page 410.

Information about blocked items in the process of

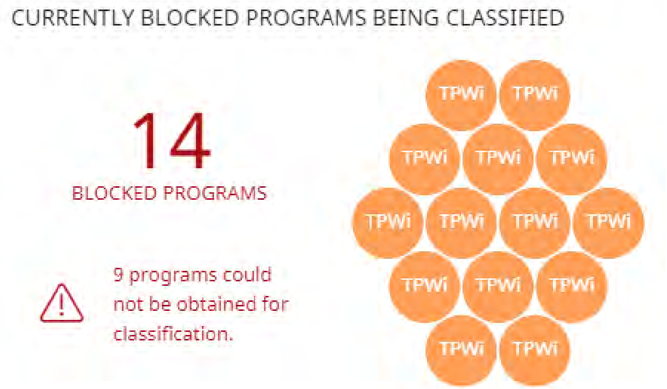
classification

Network administrators have multiple panels and lists available to get information about blocked programs in the process of classification:

- The **Currently blocked programs being classified** panel.
- The **Currently blocked programs being classified** list
- The **History of blocked programs** list

Additionally, administrators can perform maintenance actions on the **Currently blocked programs being classified** list, removing programs that Panda Adaptive Defense cannot analyze for a number or reasons. Refer to "**Deleting unknown processes from lists**".

'Currently blocked programs being classified' panel



CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED

14

BLOCKED PROGRAMS

⚠ 9 programs could not be obtained for classification.

Figure 20.5: 'Currently blocked programs being classified' panel

Shows all blocked items that are not yet classified from the time the service was activated until the present time.

> *This widget is not affected by the time period selected by the administrator in the top menu* ***Status***, ***Security*** *side panel.*

Each blocked program in the process of classification is represented by a circle with the following characteristics:

- Each blocked item with a different MD5 is represented with a circle.
- The color of the circle represents the risk level temporarily assigned to the item.
- The size of the circle represents the number of different computers where the blocked unknown program attempted to run. The size does not represent the number of execution attempts on the computers on the network.
- The number of programs that could not be sent to the Panda Security cloud for analysis is specified.

- **Meaning of the data displayed**

Blocked applications are displayed with the color code indicated below:

Data	Description
Orange	Applications with a medium probability of being malware.
Dark orange	Applications with a high probability of being malware.
Red	Applications with a very high probability of being malware.
Blocked programs	Total number of different applications blocked.
Programs that could not be obtained for classification	Total number of blocked programs where an error occurred when trying to classify them.

Table 20.1: Description of the data displayed in the 'Currently blocked programs being classified' panel

If you place the mouse pointer over a circle, the circle expands, showing the full name of the item and a series of icons representing key actions:

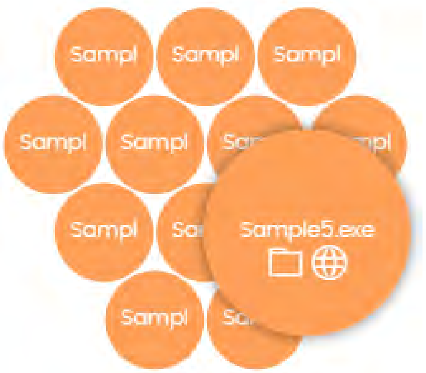


Figure 20.6: Graphical representation of a program in the process of classification

- **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**

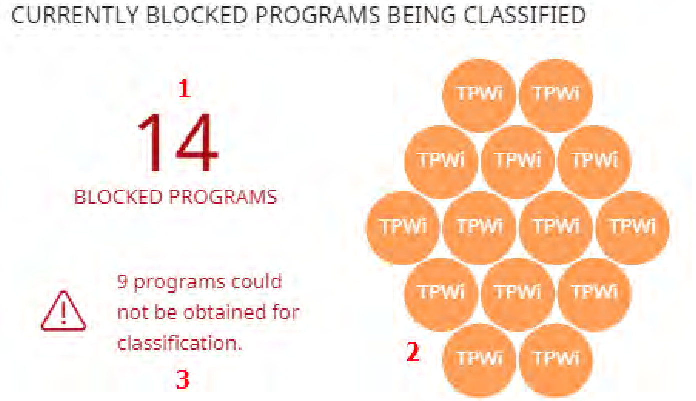

CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED
1
14
BLOCKED PROGRAMS
9 programs could not be obtained for classification.
3
2
TPWi

Figure 20.7: Hotspots in the 'Currently blocked programs being classified' panel

Click the hotspots shown in figure 20.7 to access the **Currently blocked programs being classified** list with the following predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Search = Hash.
(3)	Status = Couldn't get the file

Table 20.2: Filters available in the 'Currently blocked programs being classified' list

'Currently blocked programs being classified' list

Shows a table with all blocked files that are not yet classified.

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Path	Name and location of the unknown file on the user's computer.	Character string
Accessed data 🗐	The unknown file accessed data located on the user's computer.	Boolean
Made external connections 🌐	The unknown file communicated with remote computers to send or receive data.	Boolean
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 item is actually malware.	• Medium • High • Very high

Table 20.3: Fields in the 'Currently blocked program' list

Field	Comment	Values
Status	Classification process status: • All • **Getting the program**: the program is being sent to the Panda Security cloud for analysis. • **Classifying**: the program has been successfully sent to the Panda Security cloud and is being analyzed. • **Couldn't get the file**: an error occurred and the program has not reached the Panda Security cloud.	Enumeration
Date	Date the unknown file was first seen.	Date

Table 20.3: Fields in the 'Currently blocked program' list

- **Fields displayed in the exported file**

> *The context menu of the **Currently blocked programs being classified** list displays a drop-down menu with two options: **Export** and **Export list and details**. This section deals with the content of the file generated when selecting **Export**. For information about the **Export list and details** option, refer to section* "**Excel spreadsheets**"*.*

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Threat	Name of the unknown file.	Character string
Path	Name and location of the unknown file 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 accessed files located on the user's computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean
Likelihood of being malicious	Likelihood that the unknown item is actually a threat when the classification process is completed.	• Medium • High • Very high

Table 20.4: Fields in the 'Currently blocked programs' exported file

Field	Comment	Values
Date	Date the unknown file was first seen.	Date
Dwell time	Period of time during which the threat has been on the customer's network without being classified.	Date
User	User account under which the program was run.	Character string
Hash	String identifying the file.	Character string
Threat source computer	Name of the computer, if the blocked program came from another computer on the customer's network.	Character string
Threat source IP address	IP address of the computer, if the blocked program came from another computer on the customer's network.	Character string
Threat source user	The user who was logged in on the computer that the blocked program came from, if applicable.	Character string
Status	Classification process status: • **Getting the program**: the program is being sent to the Panda Security cloud for analysis. • **Classifying**: the program has been successfully sent to the Panda Security cloud and is being analyzed. • **Couldn't get the file**: an error occurred and the program has not reached the Panda Security cloud.	Enumeration

Table 20.4: Fields in the 'Currently blocked programs' exported file

- **Filter tool**

Field	Comment	Values
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 hours • Last month
Search	• **Computer**: device on which the unknown item resides. • **Threat**: file name. • **Hash**: String identifying the file. • **Threat source**: enables you to search by the user, IP address, or name of the computer that the blocked item came from.	Enumeration

Table 20.5: Filters available in the 'Currently blocked program' list

Field	Comment	Values
Protection modes	Operating mode of the advanced protection when the unknown file was detected.	• Hardening • Lock
Accessed data	The unknown file accessed data located on the user's computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean
Status	Classification process status: • **All** • **Getting the program**: the program is being sent to the Panda Security cloud for analysis. • **Classifying**: the program has been successfully sent to the Panda Security cloud and is being analyzed. • **Couldn't get the file**: an error occurred and the program has not reached the Panda Security cloud.	Enumeration

Table 20.5: Filters available in the 'Currently blocked program' list

- **Details window**

Shows detailed information about the blocked program. Refer to "**Blocking of unknown programs in the process of classification and History of blocked programs**" on page 457.

'History of blocked programs' list

Shows a history of all events that have occurred over time regarding unknown processes blocked.

This list is not accessible through any panels in the dashboard. To access it, click the **History** link in the top-right corner of the **Currently blocked programs being classified** screen.

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Path	Name and location of the unknown file on the user's computer.	Character string

Table 20.6: Fields in the 'History of blocked programs' list

Field	Comment	Values
Action	Action taken by Panda Adaptive Defense	• Blocked • Reclassified as goodware • Reclassified as malware • Reclassified as PUP
Accessed data 📄	The unknown file accessed data located on the user's computer.	Boolean
External connections 🌐	The unknown file communicated with remote computers to send or receive data.	Boolean
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.	Boolean
Likelihood of being malicious	Likelihood that the unknown item is actually a threat when the classification process is completed.	• Medium • High • Very high
Date	Date the unknown file was first seen.	Date

Table 20.6: Fields in the 'History of blocked programs' list

- **Fields displayed in the exported file**

*The context menu of the **History of blocked programs** list displays a drop-down menu with two options: **Export** and **Export list and details**. This section deals with the content of the file generated when selecting **Export**. For information about the **Export list and details** option, refer to section "**Excel spreadsheets**".*

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Threat	Name of the unknown file.	Character string
Path	Location of the unknown file on the user's computer.	Character string

Table 20.7: Fields in the 'History of blocked programs' exported file

Field	Comment	Values
Protection mode	Operating mode of the advanced protection when the unknown file was detected.	• Audit • Hardening • Lock
Action	Action taken by Panda Adaptive Defense	• Blocked • Reclassified as goodware • Reclassified as malware • Reclassified as PUP
Accessed data	The unknown file accessed data located on the user's computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean
Excluded	The unknown file has been unblocked by the administrator, allowing it to run.	Boolean
Likelihood of being malicious	Likelihood that the unknown item is actually a threat when the classification process is completed.	• Medium • High • Very high
Date	Date the unknown file was first seen.	Date
Dwell time	Period of time during which the threat has been on the customer's network without being classified.	Date
User	User account under which the program was run.	Character string
Hash	String identifying the file.	Character string
Threat source computer	Name of the computer the blocked program came from, if applicable.	Character string
Threat source IP address	IP address of the computer the blocked program came from, if applicable.	Character string
Threat source user	The user that was logged in on the computer that the blocked program came from, if applicable.	Character string

Table 20.7: Fields in the 'History of blocked programs' exported file

- **Filter tool**

Field	Comment	Values
Search	• **Computer**: device on which the unknown file resides. • **Threat**: threat name.	Enumeration

Table 20.8: Filters available in the 'History of blocked programs' list

Field	Comment	Values
	• **Hash**: string identifying the file. • **Threat source**: enables you to search by the user, IP address, or name of the computer that the threat came from.	
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 hours • Last month
Action	Action taken by Panda Adaptive Defense.	• Blocked • Reclassified as goodware • Reclassified as malware • Reclassified as PUP
Excluded	The unknown file has been unblocked by the administrator, allowing it to run.	Boolean
Protection modes	Operating mode of the advanced protection when the unknown file was detected.	• Hardening • Lock
Accessed data	The unknown file accessed data located on the user's computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean

Table 20.8: Filters available in the 'History of blocked programs' list

- **Details window**

Shows detailed information about the blocked program. Refer to "**Malware detection**" on page **452**.

Deleting unknown processes from lists

Unknown processes are shown in the "**'Currently blocked programs being classified' panel**" widget until Panda Adaptive Defense finishes analyzing them. Sometimes it is not possible to complete this process because the file is too large to be sent or is no longer available on the user's computer. When that happens, unknown files can accumulate indefinitely in the **Currently blocked programs being classified** widget.

To delete those files from the widget and lists:

- Go to the **Status** menu at the top of the console and click **Security** from the side panel. Click the **Currently blocked programs being classified** widget. The **Currently blocked programs being classified** list opens.

or

- Go to the **Status** menu at the top of the console and click **Add** in the **My lists** section in the side panel. A drop-down menu appears with all available lists.
- Click the **Currently blocked programs being classified** list.
- Select the checkboxes to the left of the files to delete and click the Delete icon from the toolbar. A warning message appears.
- Click the **Delete** button in the message. The deleted items will appear in the **History of blocked programs** list with the **Action** field set to **Deleted from list**. These files cannot be unblocked.

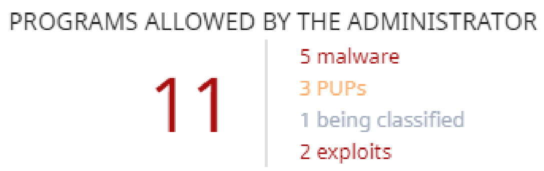
> *The purpose of deleting a blocked program in the process of classification using this procedure is to simplify the list by removing items that could not be analyzed. Internally, Panda Adaptive Defense continues to consider these items as unknown, therefore, if an attempt is made to run them again, they will reappear in the* ***Currently blocked programs being classified*** *panel and* ***Currently blocked programs being classified*** *list.*

List of allowed threats and unknown programs

Network administrators have multiple panels and lists available to get information about programs that were initially blocked by Panda Adaptive Defense and then allowed to run:

- The **Programs allowed by the administrator** panel.
- The **Programs allowed by the administrator** list
- The **History of programs allowed by the administrator** list.

Programs allowed by the administrator



PROGRAMS ALLOWED BY THE ADMINISTRATOR

11

5 malware
3 PUPs
1 being classified
2 exploits

Figure 20.8: 'Programs allowed by the administrator' panel

Shows programs allowed by the administrator which initially were prevented from running by Panda Adaptive Defense because they were classified as a threat (malware, PUP, or exploit) or because they were unknown files in the process of classification.

- **Meaning of the data displayed**

The panel shows the total number of items excluded from blocking by the administrator, broken down by type:

- Malware
- PUP
- Exploit
- Being classified

- **Lists accessible from the panel**

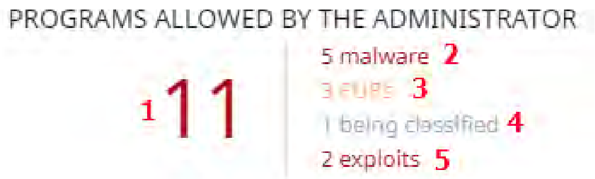


Figure 20.9: Hotspots in the 'Programs allowed by the administrator' panel

Click the hotspots shown in figure 20.9 to access the **Programs allowed by the administrator** list with the following predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Classification = Malware.
(3)	Classification = PUP.
(4)	Classification = Exploit.
(5)	Classification = Being classified (Blocked and suspicious items).

Table 20.9: Filters available in the 'Programs allowed by the administrator' list

'History of programs allowed by the administrator' list

This list shows a history of all events that have occurred over time regarding threats and unknown files in the process of classification which the administrator allowed to run. This list shows all the classifications that a file has gone through, from the time it entered the **Programs allowed by the administrator** list until it left it, as well as all other classifications caused by Panda Adaptive Defense or the administrator.

This list doesn't have a corresponding panel. To access the list, click the **History** link in the top right corner of the **Software allowed by the administrator** list.

Field	Description	Values
Program	Name of the file with malicious code and that is allowed to run.	Character string
Classification	Type of threat that was allowed to run.	• Malware • PUP • Goodware • Exploit • Being classified
Threat	Name of the malware or PUP that is allowed to run. If it has not been identified, the column will display the file's name instead. If it is an exploit, the exploit technique used will be indicated.	Character string

Table 20.10: Fields in the 'History of programs allowed by the administrator' list

Field	Description	Values
Hash	String identifying the file. This is empty if it is an exploit.	Character string
Action	Action taken on the allowed item. • **Exclusion removed by the user**: The administrator allowed the item to be blocked again. • **Exclusion removed after reclassification:** Panda Adaptive Defense applied the action associated to the category after reclassification. • **Exclusion added by the user:** The administrator allowed the item to be run. • **Exclusion kept after reclassification**: Panda Adaptive Defense did not block the item on reclassification.	Enumeration
User	User account under which the file was allowed.	Character string
Date	Date the event took place.	Date

Table 20.10: Fields in the ‘History of programs allowed by the administrator’ list

- **Fields displayed in the exported file**

Field	Description	Values
Program	Name and path of the file with malicious code that was allowed to run.	Character string
Current type	Last classification of the threat allowed to run.	• Malware • PUP • Exploit • Blocked item • Suspicious item
Original type	Original classification of the file when it was allowed to run.	• Malware • PUP • Exploit • Blocked item • Suspicious item
Threat	Name of the malware or PUP that is allowed to run. If it has not been identified, the column will display the file's name instead. If it is an exploit, the exploit technique used will be indicated.	Character string
Hash	String identifying the file. This is empty if it is an exploit.	Character string

Table 20.11: Fields in the 'History of programs allowed by the administrator' exported file

Field	Description	Values
Action	Action taken on the allowed item. • **Exclusion removed by the user**: The administrator allowed the item to be blocked again. • **Exclusion removed after reclassification:** Panda Adaptive Defense applied the action associated to the category after reclassification. • **Exclusion added by the user**: The administrator allowed the item to be run. • **Exclusion kept after reclassification**: Panda Adaptive Defense did not block the item on reclassification.	Enumeration
User	User account which triggered the change to the allowed file.	Character string
Date	Date the event took place.	Date

Table 20.11: Fields in the 'History of programs allowed by the administrator' exported file

- **Filter tool**

Field	Description	Values
Search	• **User**: User account which triggered the change to the allowed file. • **Program**: Name of the file containing the threat. • **Hash**: String identifying the file.	Enumeration
Classification	Type of file the last time it was classified.	• All • Malware • PUP • Goodware • Exploit • Item being classified (Blocked and suspicious items)
Original classification	Original classification of the file when it was allowed to run.	• All • Malware • PUP • Being classified (Blocked) • Being classified (Suspicious item) • Exploit

Table 20.12: Filters available in the 'History of programs allowed by the administrator' list

Field	Description	Values
Action	Action taken on the allowed item. • **Exclusion removed by the user**: The administrator allowed the item to be blocked again. • **Exclusion removed after reclassification:** Panda Adaptive Defense applied the action associated to the category after reclassification. • **Exclusion added by the user**: The administrator allowed the item to be run. • **Exclusion kept after reclassification**: Panda Adaptive Defense did not block the item on reclassification.	Enumeration

Table 20.12: Filters available in the 'History of programs allowed by the administrator' list

Reclassification policy

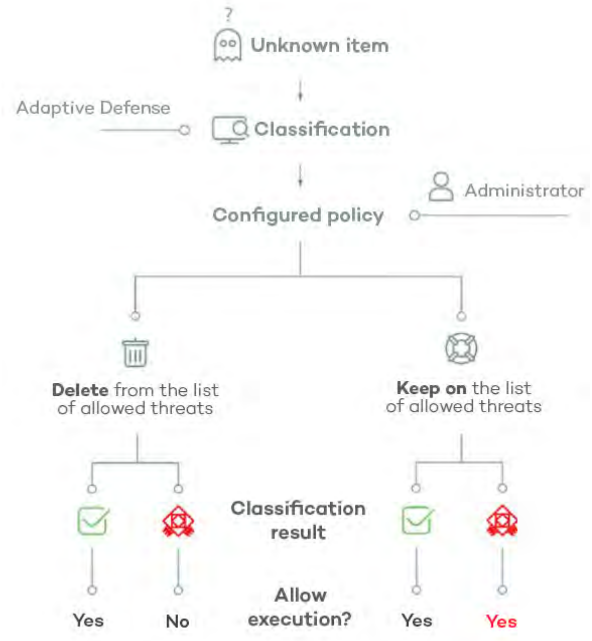


Figure 20.10: Panda Adaptive Defense's behavior based on the reclassification policy selected and the classification result.

The reclassification policy lets you define the way Panda Adaptive Defense will behave when an item that was unblocked by the administrator is reclassified and it is necessary to take a new decision.

In cases where the administrator allows an unknown item to run, Panda Adaptive Defense will classify it as malware or goodware after a period of time. If it is goodware, there are no additional considerations to be made as Panda Adaptive Defense will allow the item to run. However, if it is malware, the reclassification policy will be applied, which enables the administrator to define the behavior of Panda Adaptive Defense.

Changing the reclassification policy

The reclassification policy applies to all devices on the network, regardless of the assigned security settings.

To change how Panda Adaptive Defense behaves when a file is reclassified:

- Click **Status** in the menu at the top of the console then **Security** in the side panel.
- Click the type of item in the **Programs allowed by the administrator** panel:
  - Malware
  - PUPs
  - Being classified
  - Exploits
- Click the **Change behavior** link. A window opens with the reclassification policy to apply.
  - **Remove it from the list of programs allowed by the administrator**: If the unknown file is goodware, it will continue to run normally. If it is malware, the exclusion will be removed automatically and the file 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**: A red shaded area in the **Programs allowed by the administrator** indicates that this choice can lead to potentially dangerous situations. Both when an unknown file is classified as goodware or as malware, the exclusion is maintained and the file continues to run.

> ⚠ *Panda Security advises against using this setting due to the risk of opening a security hole that would allow malware to run on network devices.*

Reclassification traceability

If you select **Keep it on the list of programs allowed by the administrator,** you must know whether Panda Adaptive Defense has reclassified an unknown item in order to know if an allowed program was reclassified as malware.

Traceability using the history of allowed programs

To see the reclassification and event history of an unblocked file:

- Click **Status** in the menu at the top of the console then **Security** in the side panel.
- Click the **Currently blocked programs being classified** panel.
- Click the **View history of blocked items** link. You will see the **History of blocked programs** list.
- Enter the name of the threat in the search tool. The **Action** field indicates the type of event. Refer to “**‘History of blocked programs’ list**”.

Traceability using the alerts

For details of the alerts received, refer to "Alerts" on page 477.

Administrators can receive an email alert whenever an unknown file gets blocked. There is also information about reclassifications of previously unblocked files.

To enable email notifications when an unknown file is blocked:

- Click **Settings** in the top menu, then **My alerts** in the side panel.
- Enable the following alert types:
  - A program that is being classified gets blocked.
  - A file allowed by the administrator is finally classified.

Strategies for supervising file classification

Many IT departments monitor the installation of programs on network devices. In such cases, administrators may want to facilitate users' work by allowing unknown software, but without making any concessions in terms of security.

Below we describe a strategy for installing software in stages, in order to prepare the running of new software before it is installed and used across the entire network.

- Configure a test PC.
- Install the software.
- Reclassify blocked programs.
- Send programs directly to Panda Security's cloud.

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 computer of a network user or one specifically dedicated to this purpose. This computer must be configured in **Hardening** mode.

Installing the software

Install the software and run it normally. If Panda Adaptive Defense finds an unknown module or program, it will block it, displaying a pop-up window on the computer. If that happens, a new item will be added to be **Currently blocked programs being classified** panel. Internally, Panda Adaptive Defense 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 advanced 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 programs being classified** panel.

Reclassifying blocked programs

As soon as Panda Adaptive Defense 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 network.

Sending programs directly to Panda Security's cloud.

As Panda Adaptive Defense is designed not to interfere with network performance when sending files to Panda Security's cloud, the sending of a suspicious file may be delayed. To speed up this process, contact Panda Security's Support Department.

Managing the backup/quarantine area

Panda Adaptive Defense's quarantine is a backup area that stores items that have been deleted after being classified as a threat.

Quarantined items are stored on each user's computer, in the `Quarantine` folder located in the software installation directory. This folder is encrypted and cannot be accessed by any other process. It is therefore not possible to directly access or run the programs there, unless it is through the Web console.The Panda Labs department at Panda Security determines the action to take in accordance with the classification and type of item detected. As such, the following situations can occur:

The quarantine feature supports Windows, macOS, and Linux platforms.

- **Malicious items for which disinfection is possible**: These are disinfected and restored to their original location.
- **Malicious items for which disinfection is not possible**: These are moved to quarantine and remain there for seven days.
- **Non-malicious items**: If goodware is incorrectly classified (false positive), it is automatically restored from quarantine to its original location.
- **Suspicious items**: These are stored in quarantine for 30 days. If it finally turns out to be goodware, it

will be automatically restored to its original location.

> *Panda Adaptive Defense doesn't delete files from users' computers. All deleted files are sent to the backup area.*

Viewing quarantined items

To get a list of the items sent to quarantine:

- Click **Status** in the menu at the top of the console then **Security** in the side panel.
- Click in the panel according to the type of item to restore from quarantine:
  - Malware activity.
  - PUP activity.
  - Exploit activity.
- Select the **Moved to quarantine** checkbox and **Deleted** in the **Action** field. Then click **Filter**.

Restoring items from quarantine

- Click **Status** in the menu at the top of the console then **Security** in the side panel.
- Click the relevant panel according to the type of item to restore from quarantine:
  - Malware activity.
  - PUP activity
  - Exploit activity
- Select the threat from the list where the **Action** field is **Moved to quarantine** or **Disinfected**.
- Click the ⓘ icon in the **Action** field. A window opens explaining the reason the item was moved to quarantine.
- Click the **Restore and do not detect again** link. The item will be moved to its original location. The permissions, owner, and registry entries regarding the file will also be restored.

Chapter 21

Forensic analysis

Panda Adaptive Defense detects and blocks the execution of unknown and specially crafted malware designed to go unnoticed by signature-based traditional antivirus solutions. This is achieved by monitoring the actions taken by processes on customers' computers, which are sent to the Panda Security cloud as part of the telemetry collected. Process monitoring enables us to classify every program run on users' computers and determine the extent to which a customer's network has been compromised. With this information about which actions were carried out by malicious processes, network administrators can take the containment and remediation measures appropriate to each case.

The Web console makes all this information available to users through various resources, each of which provides different levels of detail:

- Through detail pages.
- Through action tables.
- Through graphs.
- Through Excel spreadsheets.

CHAPTER CONTENT

Details of blocked programs in the process of classification

Panda Adaptive Defense provides extended details of programs blocked by any of the advanced detection technologies it incorporates:

- Malware or PUPs detected.
- Exploits detected.
- Programs blocked by advanced security policies.
- Unknown programs blocked which are in the process of classification.

Malware detection

Access to the Malware details and PUP details window

- Click the **Status** menu at the top of the console. Click the **Add** link from the side menu. A window opens with all available lists.
- Click the **Malware and PUP activity** list.
- Set the filters and click the **Launch query** button. A list of items classified as malware or PUP appears.
- Click an item from the list. The **Malware detection** or **PUP detection** window opens.

Or:

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel. All widgets associated with the security module are shown.
- Click the **Malware activity** or **PUP activity** widget.
- Set the filters and click the **Launch query** button. A list of items classified as malware or PUP appears.
- Click an item from the list. The **Malware detection** or **PUP detection** window opens.

The Details window is divided into several sections:

- Overview.
- Affected computer.
- Threat impact on the computer.
- Infection source.
- Occurrences on other computers.

Overview

Field	Description
Threat	Name of the threat and hash identifying it.
Action	Action taken by Panda Adaptive Defense on the item. • Quarantined. • Blocked • Disinfected • Deleted.

Table 21.1: Fields of the Overview section on the Malware detection, PUP detection and Blocked programs in the process of classification screens

Affected computer

*Refer to "**Managing threats, items in the process of classification, and quarantine**" on page **425** for more information about the actions administrators can take on the items found.*

Field	Description
Computer	Name of the computer where the threat was found, IP address and folder in the group 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.
Logged-in user	Operating system user under which the threat was loaded and run.
Detection path	File system path of the threat.

Table 21.2: Fields of the Affected computer section on the Malware detection, PUP detection and Blocked programs in the process of classification screens

Threat impact on the computer

Field	Description
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 newly-discovered, 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** • **View full activity details**: clicking this option displays the **Activity** tab discussed in section "**Action tables**". • **View activity graph**: clicking this option displays the **Activity** graph discussed in section "**Execution graphs**".
Detection date	Date when Panda Adaptive Defense detected the threat on the customer's network.
Dwell time	Time during which the threat was on the customer's network without being classified.

Table 21.3: Fields of the Threat impact on the computer section on the Malware detection, PUP detection and Blocked programs in the process of classification screens

Infection source

Field	Description
Threat source computer	Name of the computer the infection originated from, if applicable.
Threat source IP address	IP address of the computer the infection originated from, if applicable.
Threat source user	User that was logged in on the computer the infection originated from.

Table 21.4: Fields of the Infection source section on the Malware detection, PUP detection and Blocked programs in the process of classification screens

Occurrences on other computers

Displays all computers on the network where the malware has been seen.

Fields	Description
Computer	Computer name.

Table 21.5: Fields of the Occurrences on other computers section on the Malware detection, PUP detection and Blocked programs in the process of classification screens

Fields	Description
File path	Name and path of the file that contains the malware.
First seen	Date when the threat was first detected on the relevant computer.

Table 21.5: Fields of the Occurrences on other computers section on the Malware detection, PUP detection and Blocked programs in the process of classification screens

Exploit detection

Access to the Exploit details window

- Click the **Status** menu at the top of the console. Click the **Add** link from the side menu. A window opens with all available lists.
- Click the **Exploit activity** list.
- Set the filters and click the **Launch query** button. A list of items classified as exploits appears.
- Click an item from the list. The **Exploit detection** window opens.

Or:

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel. All widgets associated with the security module are shown.
- Click the **Exploit activity** widget.
- Set the filters and click the **Launch query** button. A list of items classified as exploits appears.
- Click an item from the list. The **Exploit detection** window opens.

The Details window is divided into several sections:

- Overview.
- Affected computer.
- Threat impact on the computer.

Overview

Fields	Description	Values
Compromised program	Name of the program affected by the vulnerability exploit attempt and hash that identifies it.	• **Path**: path of the program affected by the exploit. • **Version**: version of the program affected by the exploit. • **Hash**: hash of the program affected by the exploit.

Table 21.6: Fields of the 'Overview' section on the 'Exploit detection' screen

Fields	Description	Values
Technique	Identifier of the technique used to exploit the program vulnerability.	Link to a description of the technique used by the exploit.
Action	Shows the action taken by Panda Adaptive Defense on the program affected by the exploit. • **Allowed**: the anti-exploit protection is configured in **Audit** mode. The exploit ran. • **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 was 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 will continue to run.	Enumeration Refer to "**Managing threats, items in the process of classification, and quarantine**" on page 425 for information on how to manage detected threats blocked.

Table 21.6: Fields of the 'Overview' section on the 'Exploit detection' screen

Affected computer

Field	Description
Computer	Name of the computer where the threat was found, IP address and folder in the group tree.
Logged-in user	Operating system user under which the threat was loaded and run.
Path of the compromised program	Path of the program affected by the vulnerability exploit attempt.

Table 21.7: Fields of the Affected computer section on the Exploit detection screen

Exploit impact on the computer

Field	Description
Compromised program	Name and path of the program that was hit by the exploit attempt. If Panda Adaptive Defense detects that the program is not updated to the latest available version, it displays the following warning message: ⚠ **Vulnerable program**.
Activity	• **Has run**: the exploit managed to run before being detected by Panda Adaptive Defense Plus. • **View full activity details**: clicking this option displays the **Activity** tab discussed in section "Action tables". • **View activity graph**: clicking this option displays the **Activity** graph discussed in section "Execution graphs".
Detection date	Date when Panda Adaptive Defense detected the exploit on the customer's network.
Possible source of the exploit	Name and path of the program from which the exploit possibly originated.

Table 21.8: Fields of the Exploit impact on the computer section on the Exploit detection screen

Blocking of unknown programs in the process of classification and History of blocked programs

Access to the Blocked program details window

- Click the **Status** menu at the top of the console. Click the **Add** link from the side menu. A window opens with all available lists.
- Click the **Currently blocked programs being classified** list.
- Set the filters and click the **Launch query** button. A list of unknown items in the process of classification appears.
- Click an item from the list. The **Blocked program details** window opens.
- To open the history of unknown programs blocked, click the **View history of blocked items** link.

Or:

- Click **Status** in the menu at the top of the console. Click **Security** in the side panel. All widgets associated with the security module are shown.
- Click the **Currently blocked programs being classified** widget.
- Set the filters and click the **Launch query** button. A list of unknown items in the process of classification appears.
- Click an item from the list. The **Blocked program details** window opens.

The Details window is divided into several sections:

- Overview.
- Computer.
- Program activity on the computer.
- Source.

Overview

Field	Description
Program	Name of the blocked program.
Action	Blocked.
Likelihood of being malicious	• Low • Medium • High • Very high
Status	Status of the classification process and source of the error if the investigation process could not be completed.

Table 21.9: Fields of the 'Overview' section on the 'Blocked program details' page

Computer

Field	Description
Computer	Name of the computer where the threat was detected, IP address, and folder it belongs to in the group tree.
Logged-in user	Operating system user under which the threat was loaded and run.
Protection mode	Operating mode of the advanced protection when the file was blocked (Audit, Hardening, Lock).
Detection path	Path to the blocked program on the workstation or server.

Table 21.10: Fields of the 'Computer' section on the 'Blocked program details' page

Program activity on the computer

Field	Description
Program	Name of the blocked program.

Table 21.11: Fields of the 'Program activity on the computer' section on the 'Blocked program details' page

Field	Description
Activity	Summary of the most important actions taken by the malware: • **Has run** ⚡ • **Has accessed data files** 📄 • **Has exchanged data with other computers** 🌐 • **View full activity details**: click this button to display the **Activity** tab discussed in section "Action tables". • **View activity graph**: click this button to display the **Activity** graph discussed in section "Execution graphs".
Detection date	Date when Panda Adaptive Defense blocked the program from running.
Dwell time	Time during which the threat was on the customer's network without being classified.

Table 21.11: Fields of the 'Program activity on the computer' section on the 'Blocked program details' page

Source

Field	Description
Source computer	If the file came from another computer on the customer's network, this field indicates the computer name.
Source IP address	If the file came from another computer on the customer's network, this field indicates the computer IP address.
Source user	The user who was logged in on the computer the file came from.

Table 21.12: Fields of the 'Source' section on the 'Blocked program details' page

Action tables

Panda Adaptive Defense shows the actions taken by the programs detected on users' computers by any of the advanced detection technologies it incorporates.

To view a threat's action table, access its Details page (refer to "Details of blocked programs in the process of classification") and click the **Activity** tab.

The action table displays the most relevant events triggered by a threat.

The number of actions and events triggered by a process is very high. 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 action tables:

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 parameters associated with it.	• Downloaded from • Communicates with • Accesses data • Accesses • Is accessed by • LSASS.EXE opens • LSASS.EXE is opened by • Run by • Runs • Created by • Creates • Modified by • Modifies • Loaded by • Loads • Deleted by • Deletes • Renamed by • Renames • Killed by • Kills process • Suspended process • Creates remote thread • Thread injected by • Opened by • Opens • Creates key pointing to Exe file • Modifies key to point to Exe file • Tries to stop • Ended by

Table 21.13: Fields displayed in a threat's action table

Field	Comments	Values
Path/URL/ Registry Key/ IP:Port	Action entity. It has different 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. For more information, refer to "Path format". • **URL**: for actions that involve access to a URL.	
File Hash/ Registry Value/ Protocol-Direction/ Description	This field complements the entity. • **File Hash**: for all actions that involve access to a file. • **Registry Value**: for all actions that involve access to the registry. • **Protocol-Direction**: for all 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 21.13: Fields displayed in a threat's action table

Path format

We use numbers and the " | " character to indicate the storage drive and system folders respectively:

Code	Storage drive type
0	Unknown drive.
1	Invalid path. For example, a drive that does not have a mounted volume.
2	Removable drive. For example, a floppy disk, a USB memory device, or a card reader.
3	Internal drive. For example, a hard disk or an SSD disk.
4	Remote drive. For example, a network drive.

Table 21.14: Codes used for indicating drive types

Code	Storage drive type
5	CD-ROM/DVD drive.
6	RAM disk drive.

Table 21.14: Codes used for indicating drive types

The following is an example of a path:

```
3|TEMP|\app\a_470.exe
```

- **3**: Internal drive. The file is located on the computer's hard disk.
- **|TEMP|**: the file is located in the computer's `\windows\temp\` system folder.
- **\app**: name of the folder where the file is located.
- **a_470.exe**: file name.

Subject and predicate in actions

To correctly understand the format used to present the information in an 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 specified 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) to an object, called entity. The entity is specified 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 21.15 illustrates two actions carried out by the same hypothetical malware:

Date	Times	Action	Path/URL/ Registry Key/ IP:Port	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	9994BF035813FE8EB 6BC98E CCBD5B0E1	NO

Table 21.15: Action list of a sample threat

The first action indicates that the malware (subject) connected to (**Communicates with** action) the IP address `54.69.32.99:80` (entity) through the TCP-bidirectional protocol.

The second action indicates that the malware (subject) loaded (**Loads** 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 Plus:

- **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. Examples of active actions are:
  - Communicates with
  - Loads
  - Creates
- **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) to the entity, which performs the action. Examples of passive actions are:
  - Is created by
  - Is downloaded from

Table 21.16 shows an example of a passive action:

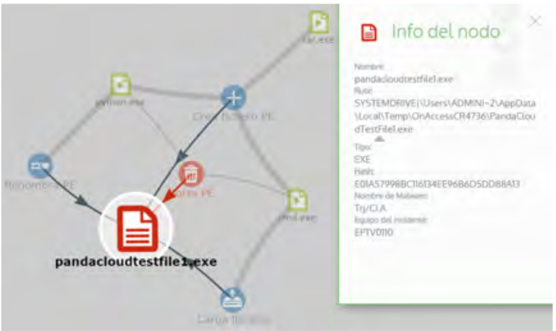
Date	Times	Action	Path/URL/ Registry Key/ IP:Port	File Hash/Registry Value/Protocol/ Description	Trusted
3/30 /2015 4:51:46 PM	1	Is run by	`WINDOWS|\explorer.exe`	`7522F548A84ABAD8FA516D E5AB3931EF`	NO

Table 21.16: 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.).*

Execution graphs



Info del nodo

Nombre:
pandacloudtestfile1.exe
Ruta:
SYSTEMDRIVE|\Users\ADMINI~2\AppData\Local\Temp\OnAccessCR4736\PandaCloudTestFile1.exe
Tipo:
EXE
Hash:
E01A57998BC116134EE96B6D5DD88A13
Nombre de Malware:
Trj/CI.A
Equipo del incidente:
EPTV0110

Figure 21.1: Example of a graph representing a threat's activities

Panda Adaptive Defense lets you view a graph displaying the actions taken by programs detected by any of the advanced detection technologies it incorporates.

To view the execution graph of a threat, access its Details page (refer to "**Details of blocked programs in the process of classification**") and click the **Activity** tab. Click the **View activity graph** button.

- The **Malware and PUP activity** list opens the Malware detection window.
- The **Exploit activity** list opens the Exploit detection window.
- The **Currently blocked programs being classified** list opens the Blocked program details window.

Click the **Activity** tab and then click **View activity graph** to display the threat's execution graph.

Execution graphs offer a graphical representation of the information shown in the action tables, emphasizing the time aspect. These graphs provide an at-a-glance idea of the actions triggered by a threat.

Diagrams

Execution graphs represent the actions taken by threats with two items:

- **Nodes**: they mostly represent actions or information items.
- **Lines and arrows**: they join the action and information nodes to establish a timeline, and assign each node the role of "subject" or "predicate".

Nodes

Nodes show information through their associated icon, color, and description 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 21.17 shows action-type nodes with a brief description:

Symbol	Description	Symbol	Description
⬇	• File download. • Compressed file created.	🗑	Executable file deleted.
📥	Socket/communication used.	⬆	Library loaded.
⇥	Monitoring initiated.	⚙	Service installed.
▶	Process created.	▭	Executable file renamed.
+	• Executable file created. • Library created. • Registry key created.	⊘	Process stopped or closed.
✎	• Executable file modified. • Registry key modified.	▶	Thread created remotely.
✎	Executable file mapped for write access.	⬆	Compressed file opened.
+	• Executable file created. • Library created. • Registry key created.	⊘	Process stopped or closed.
✎	• Executable file modified. • Registry key modified.	▶	Thread created remotely.
✎	Executable file mapped for write access.	⬆	Compressed file opened.

Table 21.17: Graphical representation of malware actions in an execution graph

Table 21.18 shows description-type nodes with a brief description:

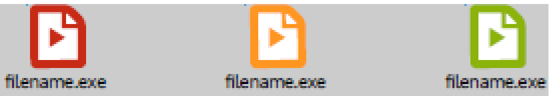
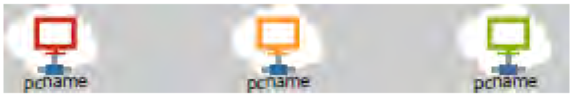
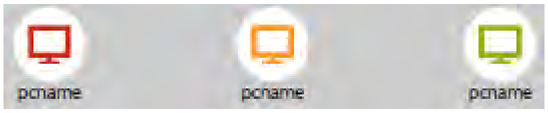
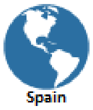
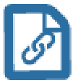
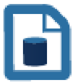
Symbol	Description
	File name and extension. • **Green**: goodware. • **Orange**: unclassified item. • **Red**: malware/PUP.
	Internal computer (it is on the corporate network) • **Green**: trusted. • **Orange**: unknown. • **Red**: untrusted.
	External computer. • **Green**: trusted. • **Orange**: unknown. • **Red**: untrusted.
	Country associated with the IP address of an external computer.
	File and extension.
	Registry key.

Table 21.18: Graphical representation of description-type nodes in an execution graph

Lines and arrows

The lines of the graphs relate the different nodes and help to establish the order in which the actions performed by a 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**: indicates the direction of the relationship between the two nodes.

Timeline

The timeline helps control the display of the string of actions carried out by a 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.

You can select a specific interval on the timeline by dragging the interval selectors to the left or right to cover the timeframe of most interest to you.

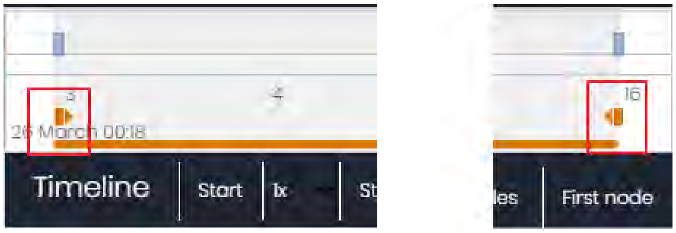


Figure 21.2: Time selectors

After selecting a timeframe, the graph will show only the actions and nodes that fall within that interval. The rest of the actions and nodes will be blurred.

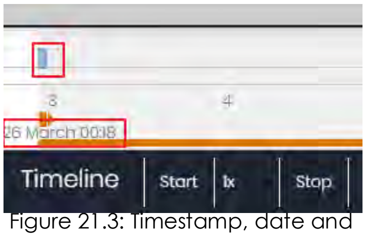


Figure 21.3: Timestamp, date and actions carried out by the threat

The actions carried out by a threat are represented on the timeline as vertical bars accompanied by a timestamp, which indicates the hour and minute when they occurred.

To view the string of actions taken by a 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.

Filters

The controls for filtering the information shown in an execution graph are at the top of the graph.

- **Action:** drop-down menu which lets you select an action type from all those executed by the threat.

The graph will show only 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).

Node movement and general zoom

To move a graph in four directions and zoom in or zoom out, you can use the controls in the top right of the graph.

To zoom in and zoom out more easily, you can use the mouse's scroll wheel.

- The ✕ 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 a graph, click the ⇓ icon located in the bottom right of the graph.
- Finally, you can configure the behavior of a graph through the panel accessible by clicking the ⇨ button in the top left corner of the graph.

Excel spreadsheets

Panda Adaptive Defense gives you the option to export, to an Excel file, extended information about the programs detected by any of the advanced detection technologies it incorporates. For more information about this file, refer to section "**Details of blocked programs in the process of classification**". To download the Excel file, click the ⋮ icon in the upper-right corner of the list. Select the **Export list and details** option to download an Excel file with extended details of all threats on the list.

Field	Description	Values
Date	Action date.	Date
Hash	String identifying the blocked file.	Character string
Policy	Name of the policy that blocked the file. This is shown in the **Detections by advanced security policies** list.	Character string
Threat	Threat name. This is shown in the following lists: • Malware activity • PUP activity • Currently blocked programs being classified • History of blocked programs	Character string
User	User account under which the threat was run.	Character string

Table 21.19: Fields in the 'List and details' exported file

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
Path	Threat name, device, and folder where the file is located on the user's computer.	Character string
Action	Action logged by the system.	• Downloaded from • Communicates with • Accesses data • Accesses • Is accessed by • LSASS.EXE opens • LSASS.EXE is opened by • Run by • Runs • Created by • Creates • Modified by • Modifies • Loaded by • Loads • Deleted by • Deletes • Renamed by • Renames • Killed by • Kills process • Suspended process • Creates remote thread • Thread injected by • Opened by • Opens • Creates key pointing to Exe file • Modifies key to point to Exe file • Tries to stop • Ended by
Command Line	Command-line parameters associated with the action.	Character string

Table 21.19: Fields in the 'List and details' exported file

Field	Description	Values
Event date	Date and time when the event was logged on the customer's computer.	Character string
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 different 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	Indicates whether the blocked file is digitally signed.	Binary value

Table 21.19: Fields in the 'List and details' exported file

Interpreting the action tables and execution graphs

The action tables and execution graphs are graphical representations of the evidence collected on users' 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 herein may vary among different security vendors. We recommend that you use the hash ID to identify specific malware.

Example 1: Trj/OCJ.A malware activity

The **Details** tab shows the key information about the malware found. In this case the most 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 a number of actions because Panda Adaptive Defense was configured in Hardening mode and the malware already resided on the computer when Panda Adaptive Defense 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 and 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 temp directory and contains the 'RAR' string. Therefore, the threat comes from a RAR file temporarily uncompressed into the directory, and which gave the `appnee.com.patch.exe` executable as the result.

- **Activity tab**

Step	Date	Action	Path
1	3:17:00	Created by	`PROGRAM_FILES|\WinRAR\WinRAR.exe`

Table 21.20: List of actions performed by Trj/OCJ.A

Step	Date	Action	Path
2	3:17:01	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\amtlib.dll`
9	3:17:59	Runs	`PROGRAM_FILES|\Google\Chrome\Application\chrome.exe`

Table 21.20: 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 temp 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 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 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.

Example 2: communication with external computers by BetterSurf

BetterSurf is a potentially unwanted program that modifies the Web browser installed on users' computers, 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

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	3/8/2015 11:16	Created by	`TEMP|\08c3b650-e9e14f.exe`
2	03/18/2015 11:16	Created 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 21.21: 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 networks 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.

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, logs 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**

Panda Adaptive Defense was configured in Hardening mode and the malware already resided on the computer when Panda Adaptive Defense was installed. The malware was unknown at the time of running.

- **Action table**

Step	Date	Action	Path
1	31/03/2015 23:29	Run by	PROGRAM_FILESX86|\internet explorer\iexplore.exe
2	31/03/2015 23:29	Created by	INTERNET_CACHE|\Content.IE5\ QGV8PV80\index[1].php
3	31/03/2015 23:30	Creates key pointing to Exe file	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\CurrentVersion\Run?MicUpdate
4	31/03/2015 23:30	Runs	SYSTEMX86|\notepad.exe
5	31/03/2015 23:30	Thread injected by	SYSTEMX86|\notepad.exe

Table 21.22: 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 on 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 can 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	Run by	`SYSTEMDRIVE|\Python27\pythonw.exe`
2	4/21/2015 2:18:01	Accesses data	`#.XLS`
3	4/21/2015 2:18:01	Accesses data	`#.DOC`
4	4/21/2015 2:18:03	Creates	`TEMP|\doc.scr`
5	4/21/2015 2:18:06	Runs	`TEMP|\doc.scr`
6	4/21/2015 2:18:37	Runs	`PROGRAM_FILES|\Microsoft Office\Office12\WINWORD.EXE`
7	4/21/2015 8:58:02	Communicates with	`192.168.0.1/2042`

Table 21.23: 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.

Chapter 22

Alerts

The alert system is a resource provided by Panda Adaptive Defense to quickly notify administrators of situations that might affect the correct operation of the security service.

Namely, an alert is sent to the administrator every time one of the following events occur:

- A malware specimen, PUP or exploit is detected.
- An indicator of attack (IOA) is detected.
- An unknown item (malware or PUP) is reclassified.
- A process unknown to Panda Adaptive Defense is blocked while it is being classified.
- There is a license status change.
- There are installation errors or a computer is unprotected.

CHAPTER CONTENT

Email alerts

Email alerts are messages generated and sent by Panda Adaptive Defense to the configured recipients (typically the network administrator) when certain events occur.

Accessing the alert settings

Click the **Settings** menu at the top of the console. Then, click **My alerts** from the side menu. You’ll access the **Email alerts** window, where you can configure the email alert settings.

Alert settings

The alert settings window is divided into three sections:

- **Send alerts in the following cases**: select which events will trigger an alert. Refer to 22.1 for more information.
- **Send the alerts to the following address**: enter the email addresses of the alert recipients.
- **Send the alerts in the following language**: choose the alert message language from those supported in the console:
  - German
  - Spanish
  - French
  - English
  - Italian
  - Japanese
  - Hungarian
  - Portuguese
  - Russian
  - Swedish

Access permissions and alerts

Alerts are defined independently for each user of the Web console. The contents displayed in an alert will vary depending on the managed computers that are visible to the recipient's role.

Alert types

Type	Frequency	Condition	Information displayed
Malware detections (real-time protection only)	A maximum of two messages per computer-malware-day.	• For each malware detected in real time on a computer.	• Whether it is the first or second message. • Name of the malicious program. • Computer name. • Group. • Date and time (UTC). • Path of the malicious program. • Hash. • Action table of the program. • List of computers where the malware was previously seen.

Table 22.1: Alert table

Type	Frequency	Condition	Information displayed
Exploit detections	A maximum of 10 alerts per day-computer-exploit.	• For each exploit attempt detected.	• Name, path and hash of the program hit by the exploit attempt. • Computer name. • Group. • Date and time (UTC). • Action taken. • Computer risk level. • Assessment of the targeted program's security level. • Action table of the program. • Possible source of the exploit.
PUP detections	A maximum of 2 messages per computer-PUP-day.	• For each PUP detected in real time on a computer.	• First or second message. • Name of the malicious program. • Computer name. • Group. • Date and time (UTC). • Path of the malicious program. • Hash. • Action table of the program. • List of computers where the malware was previously seen.
Blocked program in the process of classification	For each unknown program detected in real time on the file system.	All computers	• Name of the unknown program. • Computer name. • Group. • Date and time (UTC). • Path of the unknown program.

Table 22.1: Alert table

Type	Frequency	Condition	Information displayed
			- Hash. - Action table of the program. - List of computers where the unknown program was previously seen.
Programs blocked by the administrator	Every time a program is blocked.	For all computers	- Program name - Hash - Program path - Computer name - Group to which the computer belongs - User who launched the program - Date when the program was blocked
Classification of a file allowed by the administrator	Administrator-allowed files are those files which the administrator allowed to run despite being blocked by Panda Adaptive Defense because they were unknown or had been categorized as a threat. As soon as Panda Adaptive Defense finishes classifying a previously unknown item, it informs the administrator of its verdict, as this may affect the action to be taken on the item (allow or block), depending on the reclassification policy defined. Refer to "**Reclassification policy**" on page **446** for more information about reclassification policies.		
Indicators of attack (IOA)	Every time the relevant event is detected.	For each computer on the network that has an Indicators of attack (IOA) settings profile assigned to it.	- Affected computer - IP address - Group - Customer - Type of indicator of attack - Risk - Action
Protection errors	Every time the relevant event is detected.	- An unprotected computer is found on the network. - A computer with a protection or installation error is found.	- **Computer name.** - **Group.** - **Description.** - **Operating system.** - **IP address.** - **Active Directory path.**

Table 22.1: Alert table

Type	Frequency	Condition	Information displayed
			• **Domain.** • **Date and time (UTC).** • **Failure reason**: Protection with errors or Installation error.
Computer without a license	Every time the relevant event is detected.	The solution fails to assign a license to a computer due to lack of sufficient free licenses.	• Computer name. • Description. • Operating system. • IP address. • Group. • Active Directory path. • Domain. • Date and time (UTC). • Failure reason: Computer without a license.
Installation error	Every time the relevant event is detected.	• An event occurs that causes a computer's status to change **(1)** from protected to unprotected. • If several circumstances are detected at the same time that may cause a computer's status to change from protected to unprotected, only one alert will be generated with a summary of all those circumstances.	• Computer name. • Protection status. • Reason for the status change.
Unmanaged computer detected	Every time the relevant event is detected.	• A discovery computer finishes a discovery task. • A discovery task finds a never-seen-before computer on the network.	• Name of the discovery computer. • Number of discovered computers. • Link to the list of unmanaged computers discovered.

Table 22.1: Alert table

Status changes (1)

The following computer statuses will trigger an alert:

- **Protection with errors**: if the status of the advanced protection installed on a computer shows an error, an alert is generated.
- **Installation error**: if an installation error occurs that requires user intervention (e.g. insufficient disk space), an alert is generated. Transient errors that can be resolved autonomously after a number of retries won't generate an alert.
- **No license**: if a computer doesn't receive a license after registration because there aren't any free licenses, an alert is generated.

Finally, the following computer statuses will not trigger an alert:

- **No license**: no alert is generated if the administrator manually removes a computer's license or if Panda Adaptive Defense automatically removes a computer's license because the number of purchased licenses has been reduced.
- **Installing**: it doesn't make sense to generate an alert every time the protection is installed on a computer on the network.
- **Disabled protection**: this status is the consequence of a voluntary change of settings, so no alert is generated.
- **Outdated protection**: this status doesn't necessarily mean the computer is unprotected, despite its protection is out of date.
- **Pending restart:** this status doesn't necessarily mean the computer is unprotected.
- **Outdated knowledge:** this status doesn't necessarily mean the computer is unprotected.

Opting out of email alerts

In cases where the email alert recipient wants to opt out of the notifications but cannot access the Panda Adaptive Defense console or doesn’t have enough permissions to modify the settings, the steps below must be taken:

- Click the link at the bottom of the message: “If you don’t want to receive any more messages of this kind, click here.”. A window appears prompting for the email address at which the notifications are being received. The link is valid for 15 days.
- If an email address is entered that is included in any of the Panda Adaptive Defense settings, an email will be sent to that address for the user to confirm that they want to opt of the notifications sent for that account.
- Click the link in the email received to delete the email account from all settings in which it appears. The link is valid for 24 hours.

Chapter 23

Scheduled sending of reports and lists

The reports module sends via email up-to-date information about the security status of a company's IT infrastructure. This method of delivering reports enables you to:

- Share information across departments in a company.
- Keep a history of all the events on the platform, even beyond the capacity limits of the web console.
- Closely monitor the security status of the network without having to access the web console, thereby saving management time.

Automate email reports, enabling stakeholders to stay up-to-speed on all security events, thanks to a tamper-proof system that enables them to accurately assess the network security status.

CHAPTER CONTENTS

Types of reports available

Report features

Report period

- **Consolidated reports**: These include, in a single document, all the information generated over a given period of time.
- **Instant reports**: These reflect the security status of the network at a specific moment in time.

Method of sending

Panda Adaptive Defense enables you to generate and send reports automatically based on the settings established in the task scheduler or manually on demand.

Format

Depending on the type, reports can be sent in PDF and/or CSV format.

Content

Depending on the type of report, its content may be configurable, including any number of modules or restricting results to computers that meet certain criteria.

Report types

Panda Adaptive Defense enables you to generate three types of reports, each with its own features:

- List views
- Executive reports
- Lists of devices

Next is a summary of the features of each type of report:

Type	Period	Sent	Contents	Format
List views	Instant	Automatically	Configurable using searches	CSV
Executive reports	Consolidated	Automatically and on demand	Configurable by categories and groups	PDF, CSV, Excel, Word
Lists of devices	Instant	Automatically	Configurable using filters	CSV

Table 23.1: Summary of report types and their features

Tasks required to generate reports

Users with the read-only role can preview executive reports but cannot schedule the sending of new reports.

Next is a description of the tasks administrators have to perform to use the feature for sending scheduled reports.

List views

Administrators can use a default view or create a new one and set up the search tools so the list shows the required information. After this is done, it is possible to create a scheduled report. Refer to "Creating a custom list" on page 58 for more information on how to create list views with the corresponding searches.

Executive reports

The content is determined when configuring the scheduled report.

List of filtered devices

Administrators have to create a filter or use one of the previously created filters. Refer to "Filter tree" on page 146 for more information on how to configure the filters.

Accessing the sending of reports and lists

From the Scheduled reports section

Click **Status** in the menu at the top of the console. Click **Scheduled reports** in the side panel. A page opens with the tools required for searching for previously created send tasks, editing them, deleting them, or creating new ones.

From a list view

Select the **Status** menu. The left-side panel contains the default views and those created by the administrator.

To schedule the sending of a view:

- **From the context menu**: Click the context menu of the list view and then the option **Schedule report** ✉. A window opens with the information required, which is explained in section "Configuring reports and lists".
- **From the list view**: Click the ✉ icon in the upper-right corner of the window. A window opens with the information required, which is explained in section "Configuring reports and lists".

After the scheduled report has been created, a pop-up message appears in the upper-right corner of the page confirming the creation of the task.

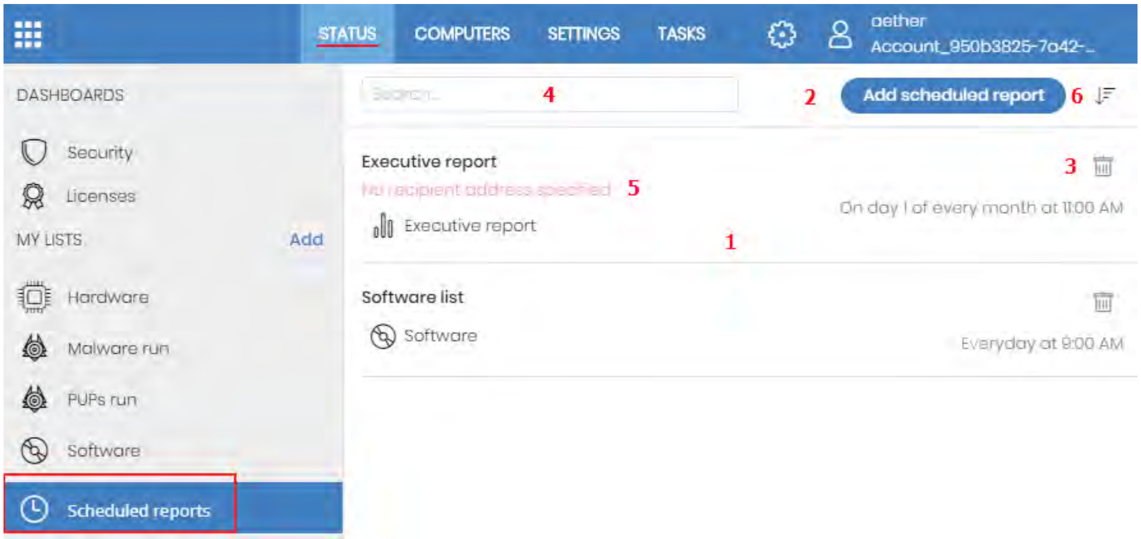
From a filter

- Click the **Computers** menu at the top of the console. Click the ⏷ tab to display the filter tree.
- On clicking a filter, the list of devices is refreshed to show the devices whose characteristics meet the conditions of the selected filter.
- Click the context menu icon ⋮ corresponding to the filter and click **Schedule report**. A window opens with the information required, which is explained in section "Configuring reports and lists".

After the scheduled report has been created, a pop-up message appears in the upper-right or bottom-right corner of the page confirming the creation of the task. This message also includes a link to the list of scheduled reports. Refer to "List of scheduled reports".

Managing reports

To create, delete, edit, and list scheduled reports, click the **Status** menu at the top of the console. Click **Scheduled reports** from the side menu.



Executive report
No recipient address specified
Executive report
On day 1 of every month at 11:00 AM

Software list
Software
Everyday at 9:00 AM

Figure 23.1: Page for managing scheduled sending of lists and reports

List of scheduled reports

In the right-side panel, you can see the list of previously created scheduled reports (Figure 23.1 **1)**.

All the tasks include a name and status. (Figure 23.1 **5**).

Creating scheduled reports

Click the button **Add scheduled report** to display the settings window (Figure 23.1 **2**).

Refer to "Configuring reports and lists" for more information about the data administrators need to provide to create a scheduled report.

Sorting scheduled reports

Click the ⇣ icon **(6)** to expand a context menu with the options for ordering the list.

Deleting and editing scheduled reports

- To delete a scheduled report, use the 🗑 icon to the right. (Figure 23.1 **3**).

- To edit a scheduled report, click its name.

⚠ *A list view or filtered list with a scheduled report configured cannot be deleted until the corresponding report has been deleted.*

The lists sent by a scheduled report correspond to a specific list view or filtered list. If these are edited, the scheduled report will be updated accordingly.

Automatic disabling of scheduled reports

A scheduled report ceases to be sent automatically when any of the following conditions are met:

- If all of the customer's licenses expire.
- If the licenses have expired for the module to which the report corresponds.
- If the administrator account that last modified the scheduled report no longer exists in the console.

Configuring reports and lists

Field	Description
Name	Name of the entry shown in the list of scheduled reports.
Send automatically	Frequency with which the report or list will be sent: • **Every day**: It will be sent every day at the scheduled time. • **Every week**: It will be sent every week on the scheduled day and at the scheduled time • **Every month**: It will be sent every month at the scheduled time on the scheduled date.
Report type	Type of report to send: • Executive report • List • Filter Refer to "**Contents of the reports and lists**".
Preview report	This link is only displayed when the report type chosen is Executive Report. Click here to open a new tab in the browser containing the contents of the report so it can be reviewed before scheduling the report, downloading it, or printing it from the top bar. For lists, the format is CSV and the preview option is therefore not available.

Table 23.2: Information for generating on-demand reports

Field	Description
Dates	Time period covered by the report. • Last month • Last 7 hours • Last 24 hours This field is only displayed for executive reports. The lists contain data relevant to the moment they are created.
Computers	The computers from which data will be extracted to generate the executive report: • **All computers.** • **Selected groups**: Shows the group tree from which individual groups can be selected using the checkboxes. This field is only displayed for executive reports.
To	Target email addresses separated with commas.
CC	Target email addresses (carbon copy recipients) separated with commas.
CCO	Target email addresses (blind copy recipients) separated with commas.
Subject	Summary description of the email.
Format	• **For list views**: A .CSV file is attached to the email. • **For executive reports**: A PDF, Excel, or Word file containing the report is attached to the email.
Language	Language of the report.
Contents	Type of information included in the report: • **Table of contents:** List of the sections in the report. • **License status**: This shows information about the licenses contracted and used as well as their expiration dates. Refer to "Licenses" on page 123. • **Security status**: The status of the Panda Adaptive Defense software on the network computers on which it is installed. • **Detections**: This shows the threats detected on the network. • **Patch management**: This shows the status of computers regarding patches. Refer to "Panda Patch Management widgets and panels" on page 299. • **Encryption**: This shows the encryption status of the computers on the network. Refer to "Panda Full Encryption panels and widgets" on page 341. Refer to "Contents of the reports and lists".

Table 23.2: Information for generating on-demand reports

Contents of the reports and lists

Lists

The content of the lists sent is similar to that generated by the **Export** or **Detailed export** button of a list view. If the list view supports detailed exports, when configuring the send task there are two options:

- **Summary report**: This corresponds to the **Export** option in the list.
- **Full report**: This corresponds to the **Detailed export** option in the list.

The lists that support detailed exports are:

- Software
- Malware and PUPs
- Exploits
- Currently blocked programs being classified

Refer to "Managing lists" on page 53 for more information about the types of lists available in Panda Adaptive Defense and their content.

The list includes the computers visible to the user account that last edited the scheduled report. For this reason, a list edited by an account with less visibility than the account that initially created it contains information for a smaller number of computers than those displayed when it was first created.

Lists of devices

The content of the report sent corresponds to the basic exported list of devices filtered by certain criteria. Refer to "The Computers area" on page 145 for more information about the contents of the .CSV file sent, and "Filter tree" on page 146 for information on how to manage and configure filters.

Executive report

Depending on the settings defined in the **Contents** field, the executive report can have the following data:

Overview

- **Created on**: Date the report was created.
- **Period**: Time period covered by the report.
- **Included information:** Computers included in the report.

Table of contents

Shows a list with links to different sections included in the executive report.

License status

- **Contracted licenses**: Number of licenses contracted.
- **Used licenses**: Number of licenses assigned to the network computers.
- **Expiration date**: Date the license contract expires.

Refer to "Licenses" on page 123.

Network security status

Operation of the protection module on the network computers on which it is installed.

- **Protection status**: Refer to "Protection status" on page 404
- **Online computers**: Refer to "Offline computers" on page 406
- **Up-to-date protection**: Refer to "Outdated protection" on page 407
- **Up-to-date knowledge**: Refer to "Outdated protection" on page 407

Detections

The threats detected on the network

- **Classification of all programs run and scanned**: Refer to "Classification of all programs run and scanned" on page 411.
- **Malware activity**: Refer to "Malware/PUP activity" on page 408.
- **PUP activity**: Refer to "Malware/PUP activity" on page 408.
- **Exploit activity**: Refer to "Exploit activity" on page 410.
- **Latest malware detections**: Refer to "Malware detection" on page 452
- **Latest PUP detections**: Refer to "Malware detection" on page 452
- **Latest exploit detections**: Refer to "Exploit detection" on page 455

Indicators of attack

IOAs detected details.

- **Threat hunting service**: Refer to "Threat Hunting Service" on page 391.
- **Evolution of detections**: Refer to "Evolution of detections" on page 393.
- **Top 10 indicators of attack (IOA) detected**: Refer to "Indicators of attack (IOA)" on page 379.
- **Top 10 indicators of attack (IOA) by computer**: Refer to "Indicators of attack (IOA)" on page 379.

Patch management

Status of computers regarding patches.

- **Patch management status**: Refer to "Patch management status" on page 299.
- **Top 10 computers with most available patches**: List of the ten computers with most patches available but not installed, grouped by type: security patches, non-security patches, and Service Packs. Refer to "Available patches" on page 304.
- **Top 10 most critical patches**: List of the ten most critical patches ordered by the number of computers affected. Refer to "Available patches" on page 304.

Data Control

The status of the Panda Data Control deployment and a list of those computers with most PII files found on the network.

- **Deployment status**: Refer to "Deployment status" on page 254.
- **Files by personal data type:** "Files by personal data type" on page 263.
- **Computers with personal data:** "Computers with personal data" on page 262.
- **Top 10 computers with most personal data files:** "Computers with personal data" on page 262.

Encryption

Encryption status of computers. It includes information collected from the following widgets and lists:

- **Encryption status**: Refer to "Encryption Status" on page 341.
- **Computers supporting encryption**: Refer to "Computers Supporting Encryption" on page 343
- **Encrypted computers**: Refer to "Encrypted Computers" on page 344.
- **Authentication method applied:** Refer to "Authentication Method Applied" on page 345.
- **Last encrypted computers**: Lists the ten computers that have been encrypted most recently by Panda Full Encryption, sorted by encryption date. Each line in the list contains the computer name, group, operating system, authentication method, and encryption date.

Part 7

Security incident remediation

Chapter 24: Remediation tools

Chapter 25: Tasks

Chapter 24

Remediation tools

Panda Adaptive Defense provides several remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle.

Table 24.1 shows the tools available for each platform and their type (manual or automatic):

Remediation tool	Type	Purpose
Automatic computer scanning and disinfection	Automatic (scheduled)/ Manual	Detects and disinfects malware when programs are run.
On-demand computer scanning and disinfection	Manual	Detects malware at the time the administrator launches a remediation task.
On-demand restart	Manual	Forces a computer restart to apply updates, finish manual disinfection tasks and fix protection errors.
Computer isolation	Manual	Isolates the computer from the network, preventing the exfiltration of confidential information and the propagation of threats to other computers.

Table 24.1: Panda Adaptive Defense remediation tools

CHAPTER CONTENT

Automatic computer scanning and disinfection

Panda Adaptive Defense's advanced protection module automatically detects and disinfects the threats found when running the software installed on the computers to protect.

Upon detecting a known threat, Panda Adaptive Defense automatically cleans the affected items provided there is a disinfection method available. Otherwise, the items are quarantined.

On-demand computer scanning and disinfection

Permissions required to manage Scheduled scan tasks

To manage **Scheduled scan** tasks, the user account used to access the web console must have the **Launch scans and disinfect** permission assigned to its role.

For more information about the permission system implemented in Panda Adaptive Defense, refer to "Understanding permissions" on page 68.For more information about how to manage the tasks run on workstations and servers, view their results, and edit their settings, refer to "Tasks" on page 507

Characteristics of on-demand scans

Panda Adaptive Defense scans and disinfects the local file system (network drives are ignored) on demand via immediate tasks with the following characteristics:

- **Maximum run time**: unlimited.
- **Task start**:
  - If the target computer is turned on, the task will start as soon as it is launched.
  - If the target computer is turned off, the task will be postponed until the computer becomes available within the next 7 days.

The computer areas to scan are as follows:

- Memory.
- Internal storage devices.

- Storage devices physically connected to the target computer (USB drives and others).

Additionally, the default actions to take are:

- **When detecting a disinfectable file**: the file is replaced with a clean version.
- **When detecting a non-disinfectable file**: the file is deleted and a backup copy is moved to quarantine.

Creating a task from the computer tree

The computer tree lets you define scan tasks for all computers in a computer group very quickly.

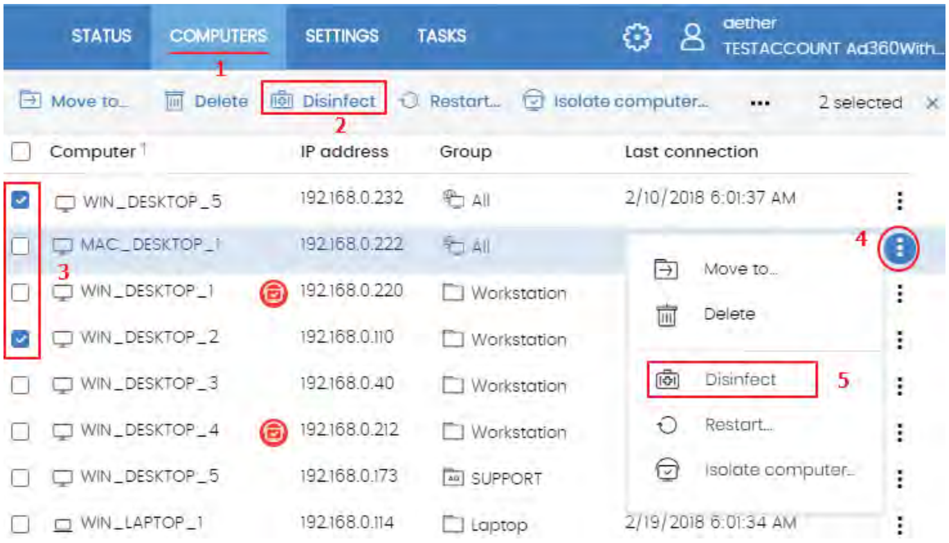
- Go to the **Computers** menu at the top of the console. From the panel on the side, click the □ icon to display the computer tree's folder view.
- From the computer tree, click the context menu icon of the group whose computers you want to scan and disinfect. The context menu of the relevant branch will open.
- Click the **Disinfect** option to create a task to scan and disinfect all computers in the selected group.

Creating a task from the Computers list

The **Computers** area lets you create tasks in a similar way to the computer tree or the **Tasks** area. However, in this case you can individually select computers belonging to the same group or subgroup.

Use one of the following resources depending on the number of computers that will receive the task:

- **Context menu**: if the task is to be applied to one computer only.
- **Checkboxes and action bar**: if the task is to be applied to one or more computers belonging to a group or subgroups.



	Computer	IP address	Group	Last connection
☑	WIN_DESKTOP_5	192.168.0.232	All	2/10/2018 6:01:37 AM
□	MAC_DESKTOP_1	192.168.0.222	All	
□	WIN_DESKTOP_1	192.168.0.220	Workstation	
☑	WIN_DESKTOP_2	192.168.0.110	Workstation	
□	WIN_DESKTOP_3	192.168.0.40	Workstation	
□	WIN_DESKTOP_4	192.168.0.212	Workstation	
□	WIN_DESKTOP_5	192.168.0.173	SUPPORT	
□	WIN_LAPTOP_1	192.168.0.114	Laptop	2/19/2018 6:01:34 AM

Figure 24.1: Context menus and action bar for quick task creation

Context menu associated with a single computer

- Click the Computers **(1)** menu at the top of the console, and select the group in the computer tree that the computer to scan belongs to.
- From the computer list, click the context menu icon of the computer to scan. **(4)**
    - From the context menu displayed, click the Disinfect option (5) to create an immediate scan and disinfection task.

Checkboxes and action bar

- Click the **Computers (1)** menu at the top of the console and select the group in the computer tree that the computer(s) to scan belong to.
- Use the checkboxes **(3)** to select the computers that will receive the task. An action bar **(2)** will be immediately displayed at the top of the window.
- Click the icon to create an immediate scan and disinfection task.

Lists generated by scan tasks

Scan tasks generate lists with results.

Accessing the lists

Follow the steps below to access these lists:

- Go to the **Tasks** menu at the top of the console. Then, click **View results** in the scan task whose results you want to view. You'll access the **Task results** list.
- From the **Task results** list, click **View detections** to access the list of detected items.

Required permissions

Permissions	Access to lists
No permissions	**Scan task results** list.
View detections and threats	Access to a task's **View detections** list.

Table 24.2: Permissions required to access the scan task lists

'Scan task results' list

This list shows the items detected on the computers on your network:

Field	Description	Values
Computer	Name of the scanned computer.	Character string

Table 24.3: Fields in the 'Scan task results' list

Field	Description	Values
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Detections	Number of items found on the computer.	Numeric value
Status	Computer scan task status.	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Start date	Date when the computer scan started.	Date
End date	Date when the computer scan ended.	Date

Table 24.3: Fields in the 'Scan task results' list

- **Filter tools**

Field	Comments	Values
Status	The task status	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Detections	Computers where malware was or wasn't detected	• All • With detections • No detections

Table 24.4: Filters available in the 'Scan task results' list

‘View detections’ list

This list shows details of each malware detection made by the scan task.

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder within the Panda Adaptive Defense folder tree the computer belongs to.	Character string
Threat type	Malware category based on the actions the threat is designed to perform.	• Virus • Spyware • Tracking cookies • Hacking tools and PUPs • Phishing • Dangerous actions blocked • Malware URLs • Other
Path	Threat location on the computer.	Character string
Action	Action performed on the computer.	• Quarantined • Deleted • Disinfected • Blocked • Process ended
Date	Date the action was taken.	Date

Table 24.5: Fields in the ‘View detections’ list

- **Computer details window**

Clicking any of the rows in the list opens the computer details window. Refer to “**Computer details**” on page 172 for more information.

Computer restart

The Web console lets administrators restart computers remotely. This is particularly useful if you have computers that need a restart to finish updating or to fix a protection problem:

- Go to the **Computers** menu at the top of the console and select the computer(s) to restart from the right-hand panel.
  - **To restart a single computer**: click the computer's context menu on the computer list. Select **Restart** from the menu displayed**.**
  - **To restart multiple computers**: use the checkboxes to select the computers to restart. Select **Restart**

↻ from the action bar displayed at the top of the screen.

With computers that are turned off, Panda Adaptive Defense will retain the restart command for up to 7 days, after which, if the computer has not been started, the command will be discarded.

Computer isolation

Panda Adaptive Defense lets administrators isolate computers on demand, preventing threats from spreading and blocking the exfiltration of confidential data.

This feature is compatible with Windows workstations and servers. It is not supported on Linux, macOS or Android devices.

When a computer is isolated, its communications are restricted except for the following:

- Access to the computer from the Web management console. This enables administrators to analyze and resolve any detected problems with the tools provided by Panda Adaptive Defense.
- Access to the computer and remote control via Panda Systems Management. This enables 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 solution's Administration Guide available at **https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Guide-EN.pdf**

All other products and services installed on the affected workstation won't be able to communicate via the Internet/network unless the administrator sets the appropriate exceptions. Refer to "**Allow processes**" for more information.

Computer isolation statuses

The **Isolate computer** and **Stop isolating the computer** operations are performed in real time. However, these processes may be delayed if the affected computer is offline. To reflect the exact situation of a computer, Panda Adaptive Defense distinguishes among four different isolation statuses through the following icons:

Icon	Description
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 are 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, products, or the operating system itself.

Table 24.6: Computer isolation statuses

These icons are displayed next to the **IP address** column in the **Licenses** and **Protection status** lists, as well as in the **Computers** area.

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 choose one of the following computer lists:
  - **Protection status** list.
  - **Licenses** list.
- 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 **We're trying to isolate this computer**.

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.

Stopping a computer from being isolated

- Follow the steps indicated in section "Isolating one or more computers from the organization's network".
- Select **Stop isolating the computer** from the action bar.
- The computer's status will change to **We're trying to stop isolating this computer**.

Advanced options

Allow processes

Isolating a computer blocks all communications established from and to 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:

- Click the **Advanced options** link in the floating window that appears when you isolate a computer.
- In the **Allow the following processes** text box, enter the programs you want to exclude from the isolation operation.

The programs you specify in **Allow the following processes** will be able to communicate normally with the other computers in the organization or with external computers, unless otherwise indicated in the settings defined in other Panda Adaptive Defense modules, in other products installed on the computer, or in the operating system's firewall.

To speed up the configuration process, the management console remembers 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.

Show custom message

Enter a descriptive message to inform users that their computer has been isolated from the network. The Panda Adaptive Defense agent will show a pop-up message with the configured text. You can configure an informational message but choose not to display it to users by selecting the **I prefer not to show any message this time** option. The message won't be displayed until you clear the option.

Communications allowed and denied on isolated computers

Panda Adaptive Defense denies all communications to and from isolated computers except those required for performing remote forensic analyses and using the remediation tools implemented in Panda Adaptive Defense and Panda Systems Management. Below is a list of all communications allowed and denied on isolated computers.

Processes and services allowed on an isolated computer

- System processes:
  - 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.
- Panda Adaptive Defense processes:
  - Services required to communicate with the default gateway.
  - Services required to communicate with Panda Security's cloud in order to allow 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.
- Panda Systems Management processes established between the isolated computer and the administrator's computer:
  - Remote access tools.
  - Services required for SNMP monitoring of devices not compatible with Panda Systems Management and with the 'connection node' role assigned.

Communications blocked on an isolated computer

All communications that are not listed in the section above are denied, including:

- Connection to the operating system's Windows Update service.
- Panda Systems Management's Patch Management and Windows Update policies.

The Panda Patch Management module remains operational on isolated computers.

- 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.
- Remote installation of the protection via Panda Adaptive Defense.

Reporting a problem

As with any technology, the Panda Adaptive Defense software installed on your network computers may occasionally function incorrectly. Some symptoms could include:

- Errors reporting a computer's status.
- Errors downloading knowledge or engine updates.
- Protection engine errors.

If Panda Adaptive Defense functions incorrectly on a computer on the network, you can contact Panda Security’s support department through the console and automatically send all the information required for diagnosis. To do this, click the **Computers** menu at the top of the console, select the computer with errors, and click its context menu. Select **Report a problem** from the menu displayed.

Allowing external access to the Web console

If you find problems you can't resolve, you can grant Panda Security's support team access to your console. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- On the **Users** tab, click **Allow the Panda Security S.L. team to access my console**.

Chapter 25

Tasks

A task is a resource implemented in Panda Adaptive Defense that allows administrators to associate a process with two variables: repetition interval and execution time.

- **Repetition interval**: tasks can be configured to be performed only once, or repeatedly through specified time intervals.
- **Execution time**: tasks can be configured to be run immediately after being set (immediate task), or at a later time (scheduled task).

CHAPTER CONTENT

Introduction to the task system

Accessing the task system

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

- Top menu **Tasks**
- Computer tree (accessible from the top menu **Computers**)
- Lists associated with the different supported modules.

The computer tree and the lists let you schedule and launch tasks easily and quickly, without having to go through the entire configuration and publishing process described in section "**Steps to launch a task**". However, they provide less configuration flexibility.

Steps to launch a task

The primary resource for creating a task is the **Tasks** area accessible from the menu at the top of the console. This area lets you create tasks from scratch, configuring every aspect of the process.

The process of launching a task consists of three steps:

- **Task creation and configuration**: select the affected computers, the characteristics of the task, the time/date the task will be launched, the task frequency, and the way it will behave in the event of an error.
- **Task publication**: the tasks you create must be entered in the Panda Adaptive Defense task scheduler in order to be run on the scheduled day/time.
- **Task execution**: the task is run when the configured conditions are met.

Task types

Panda Adaptive Defense performs the following tasks:

- Scans and disinfects files. Refer to "**On-demand computer scanning and disinfection**" on page **496**.
- Installs patches and updates for the operating system and other programs installed on users' computers. Refer to "**Panda Patch Management (Updating vulnerable programs)**" on page **285**.

Permissions associated with task management

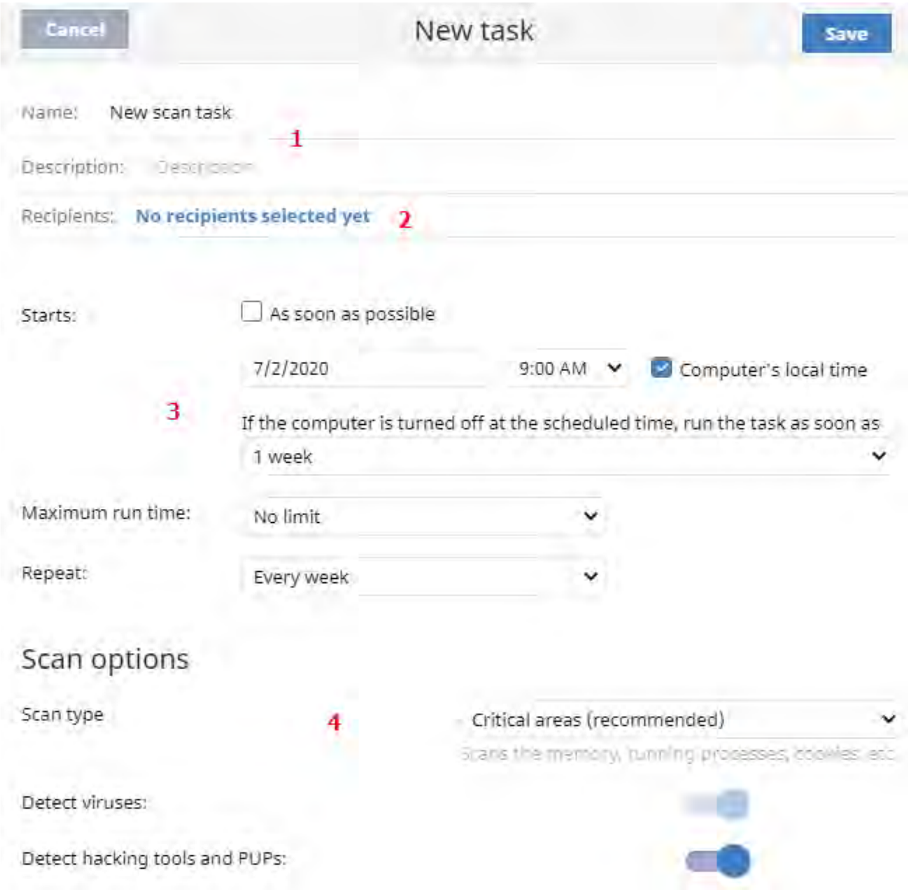
*For more information about the permission system implemented in Panda Adaptive Defense, refer to "**Understanding permissions**" on page **68**.*

To create, edit, delete, or view tasks, you must use a user account that has the appropriate permission assigned to its role. Depending on the task, the required permissions are:

- **Launch scans and disinfect**: to create, delete, and edit **Scheduled scans** tasks.
- **Install, uninstall, and exclude patches**: to create, delete, and edit **Install patches** tasks.
- **View detections**: to view the results of **Scheduled scans** tasks.

Creating a task from the Tasks area

- Click **Tasks** in the top menu. A list of all created tasks will be displayed, along with their status.
- Click the **Add task** button and select a task type from the drop-down menu. A window will be displayed with the task details, divided into multiple areas:
  - **Overview (1)**: task name and description.
  - **Recipients (2)**: computers that will receive the task.
  - **Schedule (3)**: task schedule (day and time the task will be launched).
  - **Settings (4)**: specify the actions to be taken by the task. This section varies based on the task type and is described in the documentation associated with the related module.



Name: New scan task

Description: Description

Recipients: No recipients selected yet

Starts: □ As soon as possible

7/2/2020 9:00 AM ☑ Computer's local time

If the computer is turned off at the scheduled time, run the task as soon as 1 week

Maximum run time: No limit

Repeat: Every week

Scan options

Scan type: Critical areas (recommended)

Scans the memory, running processes, cookies, etc.

Detect viruses: ●

Detect hacking tools and PUPs: ●

Figure 25.1: Overview of the 'New task' window for a scan-type task

Task recipients (2)

- Click the **No recipients selected yet** link in the **Recipients** section. This will open a window where you will be able to select the computers that will receive the configured task.
- Click the ⊕ button to add individual computers or computer groups, and the 🗑 button to remove

them.

To access the computer selection window, you must first save the task. If you haven't saved the task, a warning message will be displayed.

- Click the **View computers** button to view the computers that will receive the task.

Task schedule and frequency

You can configure the following three parameters:

- **Starts:** indicates the task start time/date.

Value	Description
As soon as possible (selected)	The task will be launched immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified **if the computer is turned off**.
As soon as possible (cleared)	The task will be launched on the date selected in the calendar. Specify whether to take into account the computer's local time or the Panda Adaptive Defense server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task won't run. The task scheduler lets you establish the task's expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** the task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** lets you define the time interval during which the task will be run if the computer becomes available. • **Run when the computer is turned on:** there is no time limit. The system waits indefinitely for the computer to be available to launch the task.

Table 25.1: Task launch parameters

- **Maximum run time**: indicates the maximum time that the task can take to complete. After that time, the task will be canceled returning an error.

Value	Description
No limit	There is no time limit for the task to complete.
1, 2, 8, or 24 hours	There is a time limit for the task to complete. After that time, if the task has not finished, it is canceled returning an error.

Table 25.2: Task duration parameters

- **Frequency**: set a repeat interval (every day, week, month, or year) from the date specified in the

Starts: field.

Value	Description
One time	The task is run only once at the time specified in the **Starts:** field.
Daily	The task is run every day at the time specified in the **Starts:** field.
Weekly	Use the checkboxes to select the days of the week on which the task must be run, at the time specified in the **Starts:** field.
Monthly	Choose an option: Run the task on a specific day of every month. If you select the, 29th, 30th, or 31st of the month, and the month does not have that day, the task will be run on the last day of the month. Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 25.3: Configuring the frequency of a task

Automatic conversion of the execution frequency

If any of the computers on the network has an older version of the security software installed, it may not be able to correctly interpret the frequency set by the administrator in the web console. In that case, the computer will establish the following correspondence with regard to the frequency of the tasks to be run:

- **Daily tasks**: no change.
- **Weekly tasks**: the days selected by the administrator are ignored. The first execution occurs on the date specified in the **Starts:** field. Then, the task is rerun every 7 days.
- **Monthly tasks**: the days selected by the administrator are ignored. The first execution occurs on the date specified in the **Starts:** field. Then, the task is rerun every 30 days.

Task publication

Once you have created and configured a task, it will be added to the list of configured tasks. However, it will display the **Unpublished** tag, meaning that it is not yet active.

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

Task list

Click **Tasks** in the top menu to view a list of all created tasks, their type, status, and other relevant information.

Field	Comments	Values
Icon	The task type	• Patch installation or uninstallation task • Disinfection task
Name	The task name	Character string
Schedule	Date the task is set to run.	Character string
Status	• **No recipients:** the task won't run because there are no recipients assigned to it. Assign one or more computers to the task. • **Unpublished:** the task won't run because it hasn't been added to the scheduler queue. Publish the task so that it can be launched by the scheduler based on its settings. • **In progress:** the task is running. • **Canceled**: the task was manually canceled. This does not mean that all processes that were running on the target computers have stopped. • **Finished**: the task finished running on all affected computers, regardless of whether it failed or was performed successfully. This status only applies to one-time tasks.	Character string

Table 25.4: Fields in the 'Tasks' list

- **Filter tool**

Field	Comments	Values
Type	The task type	• Disinfection • Patch installation • Patch uninstallation • All
Search task	Enter the task name	Character string

Table 25.5: Filters available in the 'Tasks' list

Field	Comments	Values
Schedule	The task's repeat frequency	• All • Immediate • Once • Scheduled
Sort list ⇣≡	Task list sort order.	• Sort by creation date • Sort by name • Ascending • Descending

Table 25.5: Filters available in the 'Tasks' list

Task management

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

Modifying a published task

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

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

Canceling a published task

Select the checkboxes to the left of the tasks to cancel. Click the **Cancel** ⊗ icon from the toolbar. The tasks are canceled, but they do not disappear from the Tasks page so you can still view their results. Only tasks whose status is **In progress** can be canceled.

Deleting a task

Executed tasks are not automatically deleted. To delete a task, select it using the checkboxes and click the 🗑 icon. A published task can only be deleted if it is previously canceled.

Deleting a task also deletes its results.

Copying a task

To copy a task, click its ⧉ icon.

Task results

Click the **View results** link of a published task to view its results so far and access a filter tool for finding specific computers among those that received the task.

Some of the fields in the results list are specific to certain tasks. Those fields are described in the documentation associated with the relevant module. Below is a description of the fields that are common to all results lists.

Field	Description	Values
Computer	Name of the computer where the task took place.	Character string
Group	Folder within the Panda Adaptive Defense folder tree that the computer belongs to.	Character string
Status	Status of the task process on the affected computer: • **Pending**: the task was published successfully, but the target computer has not yet received it or has received it but the task has not yet run because it is scheduled to run at a later time. • **In progress**: the task is running on the computer. • **Finished**: the task finished successfully. • **Failed**: the task failed and returned an error. • **Canceled (the task could not start at the scheduled time):** the task could not start at the scheduled time because the target computer was turned off or in a state that prevented the task from running. • **Canceled**: the process was canceled on the computer. • **Canceling:** the task was canceled, but the target computer has not finished canceling the task process. • **Canceled (maximum run time exceeded:** the task was automatically canceled because it exceeded its maximum configured run time.	Character string
Start date	The task start date.	Date
End date	The task end date.	Date

Table 25.6: Common fields in task results lists

- **Task filter tool**

Field	Description	Values
Date	Drop-down menu with the date the task became active based on the configured schedule. An active task will launch immediately or wait until the target machine is available. This date is shown in the Date column.	Date
Status	• **Pending**: the task has not yet started as the execution window has not been reached. • **In progress**: the task is currently running. • **Finished**: the task finished successfully. • **Failed**: the task failed and returned an error. • **Canceled (the task could not start at the scheduled time)**: the target computer was not accessible at the time the task was set to start or during the defined window. • **Canceled**: the task was manually canceled. • **Canceled (maximum run time exceeded)**: the task was automatically canceled because it exceeded its maximum configured run time.	Enumeration

Table 25.7: Search filters in task results

Automatic adjustment of task recipients

If the administrator selects a computer group as the recipient of a task, the computers that finally run the task may vary from those initially selected. This is because groups are dynamic entities that change over time.

That is, you can define a task at a specific time (T1) to be run on a specific group containing a series of computers. However, at the time the task is run (T2), the computers in that group may have changed.

When it comes to determining which computers will receive a configured task, there are three cases depending on the task:

- Immediate tasks.
- One-time scheduled tasks.
- Recurring scheduled tasks.

Immediate tasks

These tasks are created, published, and launched almost simultaneously and only once. The target group is evaluated at the time the administrator creates the task. The task status for the affected computers will be **Pending**.

- **Adding computers to the target group**

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

- **Removing computers from the target group**

You can remove computers from the target group. Move a computer to another group to cancel the task on that computer.

One-time scheduled tasks

There are two possible scenarios for changing the computers included in the target group:

- **Tasks which started running less than 24 hours ago**

Within the first 24 hours after a task started running, it is still possible to add or remove computers from its target groups. This 24-hour period is established to cover all time zones for multinational companies with a presence in several countries.

- **Tasks which started running more than 24 hours ago**

24 hours after a task starts running, it is not possible to add new computers to it. Even if you add new computers to the target group, they won’t receive the task. To cancel the task on a computer, move it outside the target group.

Recurring scheduled tasks

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

Unlike immediate tasks, the status of the task on each computer will not be automatically set to **Pending**. The status of the task on each computer will be shown gradually in the console as the Aether platform receives the relevant information from each machine.

Part 8

Additional information about Panda Adaptive Defense

Chapter 26: Hardware, software and network requirements

Chapter 27: Format of events used in indicators of attack (IOA)

Chapter 28: The Panda Account

Chapter 29: Key concepts

Chapter 26

Hardware, software and network requirements

Most of the security intelligence that Panda Adaptive Defense generates and uses is generated in the cloud. This intelligence is downloaded and leveraged by the security software installed on users' computers. To make sure the security software works correctly, the customer's IT infrastructure must meet the requirements specified in the next sections.

CHAPTER CONTENT

Features by platform

Available features		Windows (Intel & ARM)	Linux	MacOS
General	Web console	X	X	X
	Dashboards	X	X	X
	Filter-based computer organization	X	X	X
	Group-based computer organization	X	X	X
	Languages supported by the agent	11	11	11
Lists and reports	Frequency of sending malware, PUP, and exploit activity data and blocked programs to the server	1 min	10 mins	10 mins
	Frequency of sending detections to the server	15 mins	15 mins	15 mins
	List of detections	X	X	X
	Executive report	X	X	X
	Scheduled executive report	X	X	X
Protections	Anti-Tamper protection	X		
	Contextual detections	X	X	
	Anti-exploit protection (*)	X		
	100% Attestation Service (hardering & lock)	X	X	X
	Threat hunting services (IOAs)	X	X	X
Hardware and software information	Hardware information and list	X	X	
	Software information and list	X	X	X
	Software change log	X	X	X
	Information about the OS patches installed	X		

Table 26.1: Features by platform

Available features		Windows (Intel & ARM)	Linux	MacOS
Settings	Security for workstations and servers	X	X	X
	Password for uninstalling the protection and taking actions locally	X		
	Ability to assign multiples proxies	X		
	Ability to act as Panda proxy	X		
	Ability to use Panda proxy	X	X	X
	Ability to act as a repository/cache	X		
	Ability to use a repository/cache	X		
	Ability to discover unprotected computers	X		
	Email alerts in the event of an infection	X	X	X
	Email alerts when finding unprotected computers	X	X	X
Remote actions from the Web console	Real-time actions	X	X	X
	On-demand scans	X	X	X
	Scheduled scans	X	X	X
	Remote installation of the Panda agent	X		
	Ability to reinstall the protection agent	X		
	Ability to restart computers	X	X	X
	Ability to isolate computers	X		
	Program blocking by hash and name	X		
	Ability to report incidents (PSInfo)	X		
Updates	Signature updates	X	X	X

Table 26.1: Features by platform

Available features		Windows (Intel & ARM)	Linux	MacOS
	Protection upgrades	X	X	X
	Ability to schedule protection upgrades	X	X	X
Modules	Panda Advanced Reporting Tool	X	X	X
	Panda Patch Management (*)	X		
	Panda Data Control	X		
	Panda Full Encryption	X		

Table 26.1: Features by platform

(*) Only available for Intel microprocessors.

Requirements for Windows platforms

Supported operating systems

Workstations with an x86 or x64 microprocessor

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)

Computers with an ARM microprocessor

- Windows 10 Pro
- Windows 10 Home

Servers with an x86 or x64 microprocessor

- Windows 2003 (32-bit, 64-bit and R2) SP2 and later
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2

- Windows Server 2016 and 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 and 2019

IoT and Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits)

Hardware requirements

- **Processor:** x86 or x64-compatible CPU with SSE2 support
- **RAM:** 1 GB
- **Available hard disk space for installation**: 650 MB

Other requirements

For the product to work correctly it is necessary to keep the root certificates of workstations and servers fully up to date. If this requirement is not met, some features such as the ability for agents to establish real-time communications with the management console or the Panda Patch Management module might stop working.

Requirements for macOS platforms

Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.0 Big Sur

Hardware requirements

- **Processor**: Intel® Core 2 Duo
- **RAM**: 2 GB
- **Available hard disk space for installation**: 400 MB
- **Ports**: ports 3127, 3128, 3129 and 8310 must be accessible for the malware detection to work.

Requirements for Linux platforms

Panda Adaptive Defense can be installed on both Linux workstations and servers. If there is no graphical environment installed at the time of installing the solution, the Web filter protection will be disabled. On computers with no graphical environment installed, use the `/usr/local/protection-agent/pa_cmd` tool to manage the protection.

To complete the installation of Panda Adaptive Defense on Linux platforms, the target computer must remain connected to the Internet throughout the installation process.

Supported 64-bit distributions

- **Ubuntu**: 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS, 16.10, 17.04, 17.10, 18,04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04
- **Fedora:** 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, and 34
- **Debian:** 8, 9, 10
- **Red Hat:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, and 8.4
- **CentOS:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, and 8.4
- **Linux Mint:** 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2, 19.3, 20, 20.1
- **SUSE Linux Enterprise**: 11.2, 11.3, 11.4, 12, 12.1, 12.2, 12.3, 12.4, 12.5, 15, 15.1, 15.2

Supported 32-bit distributions

- RedHat 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10
- CentOS 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10

Supported kernel versions

For more information about the supported Linux distributions and kernels, refer to https://www.pandasecurity.com/en/support/card?id=700009#show2.

Panda Adaptive Defense is not supported on special or modified versions of the Linux kernel.

Supported file managers

- Nautilus
- PCManFM
- Dolphin

Hardware requirements

- **Processor:** x86 or x64-compatible CPU with SSE2 support
- **RAM:** 1.5 GB
- **Available hard disk space for installation:** 100 MB.
- **Ports:** ports 3127, 3128, 3129 and 8310 must be accessible for the malware detection to work.
- **Installation package dependencies:**

During the installation process, the Linux agent will download all packages required to satisfy dependencies. Generally speaking, the packages required by the system to work are as follows:

- Libcurl
- OpenSSL
- GCC and Fedora's compilation utilities (make, makeconfig, etc.)

The installation process on Fedora includes compilation of the modules required by the Panda Adaptive Defense agent to work properly.

To display the agent dependencies, run the following commands on a terminal based on the target distribution:

- For Debian-based distributions: `dpkg --info package.deb`
- For Fedora-based distributions: `rpm --qRp package.rpm`

Web console access

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

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

Access to service URLs

For Panda Adaptive Defense to operate properly, the protected computers must be able to access the following URLs.

Product name	URLs
Panda Adaptive Defense	• https://*.pandasecurity.com • Downloading of installers, the generic uninstaller, and policies. • Agent communications (registration, configuration, tasks, actions, status, real-time communications). • Communications between the protection and Collective Intelligence. • Downloading of signature files on Android systems. • http://*.pandasecurity.com • Downloading of signature files (on all systems except Android). • https://*.windows.net • Performance counters (CPU, memory, disk, etc.) • Notifications every 15 minutes if there is no real-time communication.
Root Certificates	• http://*.globalsign.com • http://*.digicert.com • http://*.sectigo.com
Panda Data Control	• https://pandasecurity.devo.com
Panda Patch Management	• All URLs in the following resource: https://forums.ivanti.com/s/article/URL-Exception-List-for-Ivanti-Patch-for-SCCM • https://content.ivanti.com
Activity testing	• http://proinfo.pandasoftware.com/connectiontest.html In the case of Windows protection versions prior to 8.00.16. • http://*.pandasoftware.com For connectivity tests.

Table 26.2: Access to service URLs

Ports

- Port 80 (HTTP)
- Port 443 (HTTPS, WebSocket)
- Port 8080 (access from Orion)

Patch and update download (Panda Patch Management)

Refer to the following support article **https://www.pandasecurity.com/uk/support/card?id=700044** for a full list of the URLs that must be accessible by the network computers that will receive patches, or by the network computers with the cache/ repository role.

Chapter 27

Format of events used in indicators of attack (IOA)

Panda Adaptive Defense monitors the processes run on customers' computers and sends the generated telemetry data to the Panda Security cloud. This data is then at the disposal of specialized threat hunters to detect indicators of attack (IOA) on customers' IT resources.

This telemetry data is stored in a structured format called 'event' and which consists of several fields. Analysts need to understand the meaning of each of these fields to correctly interpret the information regarding each IOA detected.

The information about the event that triggered the IOA is in the **Event details** window, displayed in JSON format, and in the attack graphs. Refer to "Indicators of attack settings" on page 367 for more information about the IOA detection module.

CHAPTER CONTENTS

Fields in events received

An event is a record consisting of fields describing an action taken by a process on a computer. Each type of event has a specific number of fields.

Next is a description of all the fields included in the events along with their meaning, data type, and possible values. Depending on the IOA, some of these fields are shown in:

- The **Other details** section of the **IOA details** window. Refer to "Details window" on page 381.

- The nodes and lines of the attack graph. Refer to "Graphs" on page 383.

Field	Description	Field type
accesstype	File access mask: • **(54) WMI_CREATEPROC**: Local WMI. For all other operations: • https://docs.microsoft.com/en-us/windows/win32/secauthz/access-mask • https://docs.microsoft.com/en-us/windows/win32/fileio/file-access-rights-constants • https://docs.microsoft.com/en-us/windows/win32/fileio/file-security-and-access-rights	Bitmask
accnube	The agent installed on the customer's computer can access the Panda cloud.	Boolean
action	Type of action taken by the Panda Adaptive Defense or Panda Adaptive Defense 360 agent, by the user, or by the affected process: • **0 (Allow)**: The agent allowed the process to run. • **1 (Block)**: The agent blocked the process from running. • **2 (BlockTimeout)**: The agent displayed a pop-up message to the user but the user did not respond in time. • **3 (AllowWL):** The agent allowed the process to run because it is on the local goodware whitelist. • **4 (BlockBL)**: The agent blocked the process from running because it is on the local malware blacklist. • **5 (Disinfect)**: The agent disinfected the process. • **6 (Delete)**: The agent classified the process as malware and deleted it because it could not be disinfected. • **7 (Quarantine)**: The agent classified the process as malware and moved it to the computer's quarantine folder. • **8 (AllowByUser)**: The agent displayed a pop-up message to the user and the user responded with 'Allow execution'. • **9 (Informed)**: The agent displayed a pop-up message to the user. • **10 (Unquarantine)**: The agent removed the file from the quarantine folder. • **11 (Rename)**: The agent renamed the file (this action is used only for testing).	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **12 (BlockURL)**: The agent blocked the URL. • **13 (KillProcess)**: The agent closed the process. • **14 (BlockExploit)**: The agent stopped an attempt to exploit a vulnerable process. • **15 (ExploitAllowByUser)**: The user did not allow the exploited process to be closed. • **16 (RebootNeeded)**: The agent requires that the computer be rebooted to block the exploit attempt. • **17 (ExploitInformed)**: The agent displayed a pop-up message to the user, reporting an attempt to exploit a vulnerable process. • **18 (AllowSonGWInstaller)**: The agent allowed the process to run because it belongs to an installation package classified as goodware. • **19 (EmbebedInformed)**: The agent sent internal operation information to the cloud to improve detection routines. • **21 (SuspendProcess)**: The monitored process tried to suspend the antivirus service. • **22 (ModifyDiskResource)**: The monitored process tried to modify a resource protected by the agent shield. • **23 (ModifyRegistry)**: The monitored process tried to modify a registry key protected by the agent shield. • **24 (RenameRegistry):** The monitored process tried to rename a registry key protected by the agent shield. • **25 (ModifyMarkFile):** The monitored process tried to modify a file protected by the agent shield. • **26 (Undefined):** Error monitoring the process operation. • **28 (AllowFGW):** The agent allowed the operation performed by the monitored process because it is on the local goodware whitelist. • **29 (AllowSWAuthorized):** The agent allowed the operation performed by the monitored process because the administrator marked the file as authorized software.	

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **30 (InformNewPE):** The agent reported the appearance of a new file on the computer because the Drag&Drop feature is turned on in Panda Data Control. • **31 (ExploitAllowByAdmin):** The agent allowed the operation performed by the monitored process because the network administrator excluded the exploit. • **32 (IPBlocked)**: The agent blocked IPs to mitigate an RDP (Remote Desktop Protocol) attack.	
actiontype	Indicates the session type: • **0 (Login)**: Login on the customer's computer. • **1 (Logout)**: Logout on the customer's computer. • **-1 (Desconocido)**: The session type could not be determined.	Enumeration
age	Date the file was last modified.	Date
blockreason	Reason for the pop-up message displayed on the computer: • **0:** The file was blocked because it is unknown and the Panda Adaptive Defense 360 or Panda Adaptive Defense advanced protection mode is set to Hardening or Lock. • **1:** The file was blocked by local rules. • **2**: The file was blocked because the source is untrusted. • **3**: The file was blocked by a context rule. • **4**: The file was blocked because it is an exploit. • **5**: The file was blocked after asking the user to close the process.	Enumeration
bytesreceived	Total bytes received by the monitored process.	Numeric value
bytessent	Total bytes sent by the monitored process.	Numeric value
callstack/sonsize	Size in bytes of the child file.	Numeric value
childattributes	Attributes of the child process: • **0x0000000000000001 (ISINSTALLER)**: Self-extracting (SFX) file. • **0x0000000000000002 (ISDRIVER)**: Driver-type file. • **0x0000000000000008 (ISRESOURCESDLL)**: Resource DLL-type file. • **0x0000000000000010 (EXTERNAL)**: File from outside the computer.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0x0000000000000020 (ISFRESHUNK)**: File recently added to the Panda knowledge base. • **0x0000000000000040 (ISDISSINFECTABLE)**: File for which there is a recommended disinfection action. • **0x0000000000000080 (DETEVENT_DISCARD)**: The event-based context detection technology did not detect anything suspicious. • **0x0000000000000100 (WAITED_FOR_VINDEX)**: Execution of a file whose creation had not been registered. • **0x0000000000000200 (ISACTIONSEND)**: The local technologies did not detect malware in the file and it was sent to Panda for classification. • **0x0000000000000400 (ISLANSHARED)**: File stored on a network drive. • **0x0000000000000800 (USERALLOWUNK)**: File with permission to import unknown DLLs. • **0x0000000000001000 (ISSESIONREMOTE)**: Event originating from a remote session. • **0x0000000000002000 (LOADLIB_TIMEOUT)**: The time elapsed between when the protection intercepted the loading of the library and when it was scanned exceeded 1 second. As a result, the scan changed from synchronous to asynchronous to avoid impacting performance. • **0x0000000000004000 (ISPE)**: Executable file. • **0x0000000000008000 (ISNOPE)**: Non-executable file. • **0x0000000000020000 (NOSHELL)**: The agent did not detect the execution of a shell command on the system. • **0x0000000000080000 (ISNETNATIVE)**: NET Native file. • **0x0000000000100000 (ISSERIALIZER)**: Serializer file. • **0x0000000000200000 (PANDEX)**: File included in the list of processes created by Panda Patch Management. • **0x0000000000400000 (SONOFGWINSTALLER)**: File created by an installer classified as goodware.	

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0x0000000000800000 (PROCESS_EXCLUDED):** File not scanned because of the Panda Adaptive Defense exclusions • **0x0000000001000000 (INTERCEPTION_TXF)**: The intercepted operation was originated by an executable whose image on the disk is being modified. • **0x0000000002000000 (HASMACROS):** Microsoft Office document with macros. • **0x0000000008000000 (ISPEARM):** Executable file for ARM microprocessors. • **0x0000000010000000 (ISDYNFILTERED)**: The file was allowed on the computer because there are no technologies to classify it. • **0x0000000020000000 (ISDISINFECTED)**: The file was disinfected. • **0x0000000040000000 (PROCESSLOST)**: The operation was not logged. • **0x0000000080000000 (OPERATION_LOST)**: Operation with a pre-scan report for which the post-scan report has not been received yet.	
childblake	Blake2 signature of the child file.	Character string
childclassification	Classification of the child process that performed the logged action. • **0 (Unknown)**: File in the process of classification. • **1 (Goodware)**: File classified as goodware. • **2 (Malware)**: File classified as malware. • **3 (Suspect)**: The file is in the process of classification and there is a high probability that it turns out to be malware. • **4 (Compromised)**: Process compromised by an exploit attack. • **5 (GWNotConfirmed)**: The file is in the process of classification and there is a high probability that it is malware. • **6 (Pup)**: File classified as an unwanted program. • **7 (GwUnwanted)**: Equivalent to PUP. • **8 (GwRanked)**: Process classified as goodware. • **-1** (Unknown)	Enumeration
childfiletime	Date of the child file logged by the agent.	Date

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
childfilesize	Size of the child file logged by the agent.	Numeric value
childmd5	Child file hash.	Character string
childpath	Path of the child file that performed the logged operation.	Character string
ChildPID	Child process ID.	Numeric value
childurl	File download URL.	Character string
childstatus	Child process status. • **0 (StatusOk)**: Status OK. • **1 (NotFound)**: Item not found. • **2 (UnexpectedError)**: Unknown error. • **3 (StaticFiltered)**: File identified as malware using static information contained in the Panda Adaptive Defense or Panda Adaptive Defense 360 protection. • **4 (DynamicFiltered)**: File identified as malware using local technology implemented in Panda Adaptive Defense or Panda Adaptive Defense 360. • **5 (FileIsTooBig)**: File too big. • **6 (PEUploadNotAllowed)**: File send was disabled. • **11 (FileWasUploaded)**: File sent to the cloud for analysis. • **12 (FiletypeFiltered)**: Resource DLL, NET Native, or Serializer-type file. • **13 (NotUploadGWLocal)**: Goodware file not saved to the cloud. • **14 (NotUploadMWdisinfect)**: Disinfected malware file not saved to the cloud.	Enumeration
classname	Type of device where the process resides. It corresponds to the class specified in the .INF file associated with the device.	Character string
configstring	Version of the MVMF.xml file in use.	Character string
commandline	Command line configured as a task to be run via WMI.	Character string
confadvancedrules	Panda Adaptive Defense or Panda Adaptive Defense 360 advanced security policy settings.	Character string
copy	Name of the service that triggered the event.	Character string
details	Summary in the form of a group of relevant fields from the event.	Character string

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
description	Description of the USB device that performed the operation.	Character string
detectionid	Unique identifier of the detection made.	Numeric value
devicetype	Type of drive where the process or file that triggered the logged operation resides. • **0 (UNKNOWN)**: Unknown. • **1 (CD_DVD)**: CD or DVD drive. • **2 (USB_STORAGE)**: USB storage device. • **3 (IMAGE)**: Image file. • **4 (BLUETOOTH)**: Bluetooth device. • **5 (MODEM)**: Modem. • **6 (USB_PRINTER)**: USB printer. • **7 (PHONE)**: Mobile phone. • **8 (KEYBOARD)**: Keyboard. • **9 (HID)**: Mouse.	Enumeration
direction	Network connection direction. • **0 (UnKnown)**: Unknown. • **1 (Incoming)**: Connection established from outside the network to a computer on the customer's network. • **2 (Outgoing)**: Connection established from a computer on the customer's network to a computer outside the network. • **3 (Bidirectional)**: Bidirectional.	Enumeration
domainlist	List of domains sent by the process to the DNS server for resolution and number of resolutions per domain.	{domain_name,number#domain_name,number}
domainname	Name of the domain the process tries to access/ resolve.	Character string
errorcode	Error code returned by the operating system when there is a failed login attempt. • **1073741724 (Invalid username)**: The user name does not exist. • **1073741730 (Login server is unavailable)**: The server required to validate the login is not available. • **1073741718 (Invalid password)**: The user name is correct but the password is incorrect. • **1073741715 (Invalid username or authentication info)**: The user name or the authentication information is wrong.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **1073741714 (Invalid username or password)**: Unknown user name or wrong password. • **1073741260 (Account blocked)**: Access blocked. • **1073741710 (Account disabled)**: Account disabled. • **1073741713 (User account day restriction)**: An attempt was made to log in at a restricted time. • **1073741712 (Invalid workstation for login)**: An attempt was made to log in from an unauthorized computer. • **1073741604 (Sam server is invalid)**: The validation server has failed. Cannot perform operation. • **1073741421 (Account expired)**: The account has expired. • **1073741711 (Password expired)**: The password has expired. • **1073741517 (Clock difference is too big)**: The connected computers' clocks are too far out of sync. • **1073741276 (Password change required on reboot)**: The user's password must be changed on next boot. • **1073741275 (Windows error (no risk))**: A bug in Windows and not a risk. • **1073741428 (Domains trust failed)**: The login request failed because the trust relationship between the primary domain and the trusted domain failed. • **1073741422 (Netlogon not initialized)**: An attempt was made to log in, but the `Netlogon` service was not started. • **1073741074 (Session start error)**: An error occurred during login. • **1073740781 (Firewall protected)**: The machine you are logging into is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine. • **1073741477 (Invalid permission)**: The user has requested a type of login that has not been granted.	
errorstring	Character string with debug information on the security product settings.	Character string
eventtype	Event type logged by the agent.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **1 (ProcessOps)**: The process performed operations on the computer's hard disk. • **14 (Download)**: The process downloaded data. • **22 (NetworkOps)**: The process performed network operations. • **26 (DataAccess)**: The process accessed data files hosted on internal mass-storage devices. • **27 (RegistryOps)**: The process accessed the Windows Registry. • **30 (ScriptOps)**: Operation performed by a script-type process. • **31 (ScriptOps)**: Operation performed by a script-type process. • **40 (Detection):** Detection made by the Panda Adaptive Defense active protections. • **42 (BandwidthUsage)**: Volume of information handled in each data transfer operation performed by the process. • **45 (SystemOps)**: Operation performed by the Windows operating system WMI engine. • **46 (DnsOps)**: The process accessed the DNS name server. • **47 (DeviceOps)**: The process accessed an external device. • **50 (UserNotification)**: Notification displayed to the user and response (if any). • **52 (LoginOutOps)**: Login or logout operation performed by the user. • **99 (RemediationOps):** Detection, blocking, and disinfection events from the Panda Adaptive Defense or Panda Adaptive Defense 360 agent. • **100 (HeaderEvent)**: Administrative event with information about the protection software settings and version, as well as computer and customer information. • **199 (HiddenAction)**: Detection event that did not trigger an alert.	
exploitorigin	Origin of the process exploit attempt. • **1 (URL)**: URL address. • **2 (FILE)**: File.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
extendedinfo	Additional information about **Type** events: • **0 (Command line event creation)**: Empty. • **1 (Active script event creation)**: Script file name. • **2 (Event consumer to filter consumer)**: Empty. • **3 (Event consumer to filter query)**: Empty. • **4 (Create User)**: Empty. • **5 (Delete User)**: Empty. • **6 (Add user group)**: Group SID. • **7 (Delete user group)**: Group SID. • **8 (User group admin)**: Group SID. • **9 (User group rdp)**: Group SID.	Character string
failedqueries	Number of failed DNS resolution requests sent by the process in the last hour.	Numeric value
friendlyname	The device's easily readable name.	Character string
firstseen	Date the file was first seen.	Date
hostname	Name of the computer that ran the process.	Character string
infodiscard	Quarantine file internal information.	Character string
ipv4status	IP address type: • **0 (Private)** • **1 (Public)**	Enumeration
isdenied	Indicates whether the reported action was denied.	Binary value
islocal	Indicates whether the task was created on the local computer or on a remote computer.	Binary value
Interactive	Indicates whether the login is an interactive login.	Binary value
idname	Device name.	Character string
key	Affected registry branch or key.	Character string
lastquery	Last query sent to the cloud by the Panda Adaptive Defense or Panda Adaptive Defense 360 agent.	Date
localip	Local IP address of the process.	IP address
localport	Depends on the **direction** field: • **outgoing**: The port of the process run on the computer protected with Panda Adaptive Defense and Panda Adaptive Defense 360. • **incoming**: The port of the process run on the remote computer.	Numeric value
localdatetime	The computer's date (in UTC format) at the time the logged event occurred. This date depends on the computer settings. As a result, it can be incorrect.	Date

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
loggeduser	The user that was logged in to the computer at the time the event was generated.	Character string
machinename	Name of the computer that ran the process.	Character string
manufacturer	Device manufacturer.	Character string
MUID	Internal ID of the customer's computer.	Character string
objectname	Unique name of the object within the WMI hierarchy.	Character string
opentstamp	Date of the WMI notification for WMI_CREATEPROC (54) events.	Bitmask
operation	Type of operation performed by the process. • **0 (CreateProc)**: Process created. • **1 (PECreat)**: Executable program created. • **2 (PEModif)**: Executable program modified. • **3 (LibraryLoad)**: Library loaded. • **4 (SvcInst)**: Service installed. • **5 (PEMapWrite)**: Executable program mapped for write access. • **6 (PEDelet)**: Executable program deleted. • **7 (PERenam)**: Executable program renamed. • **8 (DirCreate)**: Folder created. • **9 (CMPCreat)**: Compressed file created. • **10 (CMOpened)**: Compressed file opened. • **11 (RegKExeCreat)**: A registry branch pointing to an executable file was created. • **12 (RegKExeModif)**: A registry branch was modified, which now points to an executable file. • **15 (PENeverSeen)**: Executable program never seen before by Panda Adaptive Defense. • **17 (RemoteThreadCreated)**: Remote thread created. • **18 (ProcessKilled)**: Process killed. • **25 (SamAccess)**: Access to the computer's SAM. • **30 (ExploitSniffer)**: Sniffing exploit technique detected. • **31 (ExploitWSAStartup)**: WSAStartup exploit technique detected. • **32 (ExploitInternetReadFile)**: InternetReadFile exploit technique detected. • **34 (ExploitCMD)**: CMD exploit technique detected.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **39 (CargaDeFicheroD16bitsPorNtvdm.exe)**: 16-bit file loaded by ntvdm.exe. • **43 (Heuhooks)**: Anti-exploit technology detected. • **54 (Create process by WMI)**: Process created by a modified WMI. • **55 (AttackProduct)**: Attack detected on the agent service, a file, or registry key. • **61 (OpenProcess LSASS):** LSASS process opened.	
operationflags/ integrityLevel	Indicates the integrity level assigned by Windows to the item. • **0x0000** Untrusted level • **0x1000** Low integrity level • **0x2000** Medium integrity level • **0x3000** High integrity level • **0x4000** System integrity level • **0x5000** Protected	Enumeration
operationstatus	Indicates whether the event must be sent to Panda Advanced Reporting Tool: • **0:** Send. • **1:** Filtered by the agent. • **2:** Do not send.	Numeric value
origusername	User of the computer which performed the operation.	Character string
pandaid	Customer ID.	Numeric value
pandaorionstatus	Indicates the status of the customer's computer's time settings compared to the clock in Panda. • **0 (Version not supported)**: The customer's computer does not support synchronization of its time settings to Panda's settings. • **1 (Recalculated Panda Time)**: The customer has fixed and synced the computer's time settings to Panda's settings. • **2**: **(Panda Time Ok)**: The customer's computer's time settings are correct. • **3**: **(Panda Time calculation error)**: Error fixing the computer's time settings.	Enumeration
pandatimestatus	Contents of the DateTime, Date, and LocalDateTime fields.	Date
parentattributes	Attributes of the parent process.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0x0000000000000001 (ISINSTALLER)**: Self-extracting (SFX) file. • **0x0000000000000002 (ISDRIVER)**: Driver-type file. • **0x0000000000000008 (ISRESOURCESDLL)**: Resource DLL-type file. • **0x0000000000000010 (EXTERNAL)**: File from outside the computer. • **0x0000000000000020 (ISFRESHUNK)**: File recently added to the Panda knowledge base. • **0x0000000000000040 (ISDISSINFECTABLE)**: File for which there is a recommended disinfection action. • **0x0000000000000080 (DETEVENT_DISCARD)**: The event-based context detection technology did not detect anything suspicious. • **0x0000000000000100 (WAITED_FOR_VINDEX)**: Execution of a file whose creation had not been registered. • **0x0000000000000200 (ISACTIONSEND)**: The local technologies did not detect malware in the file and it was sent to Panda for classification. • **0x0000000000000400 (ISLANSHARED)**: File stored on a network drive. • **0x0000000000000800 (USERALLOWUNK)**: File with permission to import unknown DLLs. • **0x0000000000001000 (ISSESIONREMOTE)**: Event originating from a remote session. • **0x0000000000002000 (LOADLIB_TIMEOUT)**: The time elapsed between when the protection intercepted the loading of the library and when it was scanned exceeded 1 second. As a result, the scan changed from synchronous to asynchronous to avoid impacting performance. • **0x0000000000004000 (ISPE)**: Executable file. • **0x0000000000008000 (ISNOPE)**: Non-executable file. • **0x0000000000020000 (NOSHELL)**: The agent did not detect the execution of a shell command on the system.	

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0x0000000000080000 (ISNETNATIVE)**: NET Native file. • **0x0000000000100000 (ISSERIALIZER)**: Serializer file. • **0x0000000000200000 (PANDEX)**: File included in the list of processes created by Panda Patch Management. • **0x0000000000400000 (SONOFGWINSTALLER)**: File created by an installer classified as goodware. • **0x0000000000800000 (PROCESS_EXCLUDED)**: File not scanned because of the Orion exclusions. • **0x0000000001000000 (INTERCEPTION_TXF)**: The intercepted operation was originated by an executable whose image on the disk is being modified. • **0x0000000002000000 (HASMACROS):** Microsoft Office document with macros. • **0x0000000008000000 (ISPEARM):** Executable file for ARM microprocessors. • **0x0000000010000000 (ISDYNFILTERED)**: The file was allowed on the computer because there are no technologies to classify it. • **0x0000000020000000 (ISDISINFECTED)**: The file was disinfected. • **0x0000000040000000 (PROCESSLOST)**: The operation was not logged. • **0x0000000080000000 (OPERATION_LOST)**: Operation with a pre-scan report for which the post-scan report has not been received yet.	
parentblake	Blake2 signature of the parent file that performed the operation.	Character string
parentcount	Number of processes with DNS failures.	Numeric value
parentmd5	Parent file hash.	Character string
parentpath	Path of the parent file that performed the logged operation.	Character string
parentpid	Parent process ID.	Numeric value
parentstatus	Parent process status.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0 (StatusOk)**: Status OK. • **1 (NotFound):** Item not found • **2 (UnexpectedError):** Unknown error. • **3 (StaticFiltered):** File identified as malware using static information contained in the Panda Adaptive Defense or Panda Adaptive Defense 360 protection. • **4 (DynamicFiltered):** File identified as malware using local technology implemented in Panda Adaptive Defense or Panda Adaptive Defense 360. • **5 (FileIsTooBig)**: File too big. • **6 (PEUploadNotAllowed)**: File send was disabled. • **11 (FileWasUploaded):** File sent to the cloud. • **12 (FiletypeFiltered)**: Resource DLL, NET Native, or Serializer-type file. • **13 (NotUploadGWLocal)**: Goodware file not saved to the cloud. • **14 (NotUploadMWdisinfect)**: Disinfected malware file not saved to the cloud.	
pecreationsource	Type of drive where the process was created: • **(0) Unknown**: The device type cannot be determined. • **(1) No root dir**: The device path is invalid. For example, the external storage media was extracted. • **(2) Removable media**: Removable storage media. • **(3) Fixed media**: Internal storage media. • **(4) Remote drive**: Remote storage media (for example, a network drive). • **(5) CD-ROM drive** • **(6) RAM disk**	Numeric value
phonedescription	Phone description if the operation involved a device of this type.	Character string
protocol	Communications protocol used by the process. • 1 (**ICMP**) • 2 (**IGMP**) • 3 (**RFCOMM**) • 6 (**TCP**)	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **12** (**RDP**) • **17** (**UDP**) • **58 (ICMPV6)** • **113 (RM)**	
queriedomaincount	Number of different domains sent by the process for which there was a DNS resolution failure in the last hour.	Numeric value
regaction	Type of operation performed on the computer's Windows registry. • **0 (CreateKey)**: A new registry branch was created. • **1 (CreateValue)**: A value was assigned to a registry branch. • **2 (ModifyValue)**: A registry branch value was modified.	Enumeration
remediationresult	User's response to the pop-up message shown by Panda Adaptive Defense 360 or Panda Adaptive Defense. • **0 (Ok)**: The customer accepted the message. • **1 (Timeout)**: The pop-up message disappeared due to lack of action by the user. • **2 (Angry)**: The user chose the option to not block the item from the pop-up message displayed. • **3 (Block)**: The item was blocked because the user did not reply to the pop-up message. • **4 (Allow)**: The user accepted the solution. • **-1 (Unknown**)	Enumeration
remoteip	IP address of the computer that started the remote session.	IP address
remotemachinename	Name of the computer that started the remote session.	Character string
remoteport	Depends on the **direction** field: • **incoming**: The port of the process run on the computer protected with Panda Adaptive Defense and Panda Adaptive Defense 360. • **outcoming**: The port of the process run on the remote computer.	Numeric value
remoteusername	Name of the computer that started the remote session.	Character string
sessiondate	Date the antivirus service was last started or last time it was started since the last update.	Date
sessiontype	Login type:	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0 (System Only)**: Session started with a system account. • **2 (Local)**: Session created physically through a keyboard or via KVM over IP. • **3 (Remote)**: Session created remotely in shared folders or printers. This login type uses secure authentication. • **4 (Scheduled)**: Session created by the Windows task scheduler. • -**1 (Unknown)** • **5 (Service)**: Session created when a service that needs to run in the user session is launched. The session is deleted when the service stops. • **7 (Blocked)**: Session created when a user tries to join a previously blocked session. • **8 (Remote Unsecure)**: Same as type 3 but the password is sent in plain text. • **9 (RunAs)**: Session created when the "`RunAs`" command is used under an account other than the account used to log in, and the "`/netonly`" parameter is specified. If the "`/netonly`" parameter is not specified, a type 2 session is created. • **10 (TsClient)**: Session created when accessing via "`Terminal Service`", "`Remote Desktop`" or "`Remote Assistance`". It identifies a remote user connection. • **11 (Domain Cached)**: User session created with domain credentials cached on the machine, but with no connection to the domain controller.	
servicelevel	Agent execution mode. • **0 (Learning)**: The agent does not block any items but monitors all running processes. • **1 (Hardening)**: The agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. • **2 (Block)**: The agent blocks all unclassified executables and items classified as malware. • **-1 (N/A)**	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
timeout	The local scan took too long to complete and the process was delegated to other mechanisms that do not impact performance.	Boolean
times	Number of times the same communication event occurred in the last hour.	Numeric value
timestamp	Timestamp of the action detected on the customer's computer that generated the indicator.	Date
totalresolutiontime	Indicates the time it took the cloud to respond, and whether the error code query failed. • **0**: The cloud was not queried. • **>0:** Time in milliseconds it took the cloud to respond to the query. • **<0**: Cloud query error code.	Numeric value
type	Type of WMI operation performed by the process. • **0 (Command line event creation):** WMI launched a command line in response to a change in the database. • **1 (Active script event creation):** A script was run in response to receiving an event. • **2 (Event consumer to filter consumer):** This event is generated whenever a process subscribes to receive notifications. The name of the created filter is received. • **3 (Event consumer to filter query):** This event is generated whenever a process subscribes to receive notifications. The query run by the process to subscribe is received. • **4 (Create User):** A user account was added to the operating system. • **5 (Delete User):** A user account was deleted from the operating system. • **6 (Add user group):** A group was added to the operating system. • **7 (Delete user group):** A group was deleted from the operating system. • **8 (User group admin):** A user was added to the admin group. • **9 (User group rdp):** A user was added to the RDP group.	Enumeration
uniqueid	Unique ID of the device.	Character string
url	Download URL launched by the process that generated the logged event.	Character string

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
value	Type of operation performed on the computer's Windows registry. • **0 (CreateKey)**: A new registry branch was created. • **1 (CreateValue)**: A value was assigned to a registry branch. • **2 (ModifyValue)**: A registry branch value was modified.	Enumeration
valuedata	Data type of the value contained in the registry branch. • **00 (REG_NONE)** • **01 (REG_SZ)** • **02 (REG_EXPAND_SZ)** • **03 (REG_BINARY)** • **04 (REG_DWORD)** • **05 (REG_DWORD_BIG_ENDIAN)** • **06 (REG_LINK)** • **07 (REG_MULTI_SZ)** • **08 (REG_RESOURCE_LIST)** • **09 (REG_FULL_RESOURCE_DESCRIPTOR)** • **0A (REG_RESOURCE_REQUIREMENTS_LIST)** • **0B (REG_QWORD)** • **0C (REG_QWORD_LITTLE_ENDIAN)**	Enumeration
vdetevent	Deteven.dll DLL version.	Character string
version	Operating system version of the computer that ran the vulnerable software.	Character string
versionagent	Installed agent version.	Character string
versioncontroller	Psnmvctrl.dll DLL version.	Character string
vtabledetevent	TblEven.dll DLL version.	Character string
vtableramsomevent	TblRansomEven.dll DLL version.	Character string
vramsomevent	RansomEvent.dll DLL version.	Character string
vantiexploit	Anti-exploit technology version.	Character string
vtfilteraxtiexploit	Anti-exploit technology filter version.	Character string
versionproduct	Installed protection product version.	Character string
winningtech	Panda Adaptive Defense 360 or Panda Adaptive Defense agent technology raising the event.	Enumeration

Table 27.1: List of the fields that make up the events stored by Panda Security

Field	Description	Field type
	• **0 (Unknown)** • **1 (Cache)**: Locally cached classification. • **2 (Cloud)**: Classification downloaded from the cloud. • **3 (Context)**: Local context rule. • **4 (Serializer)**: Binary type. • **5 (User)**: The user was asked about the action to take. • **6 (LegacyUser)**: The user was asked about the action to take. • **7 (NetNative)**: Binary type. • **8 (CertifUA):** Detection by digital certificates. • **9 (LocalSignature)**: Local signature. • **10 (ContextMinerva)**: Cloud-hosted context rule. • **11 (Blockmode)**: The agent was in Hardening or Lock mode when the process was blocked from running. • **12 (Metasploit)**: Attack created with the Metasploit Framework. • **13 (DLP):** Data Leak Prevention technology. • **14 (AntiExploit)**: Technology that identifies attempts to exploit vulnerable processes. • **15 (GWFilter)**: Technology that identifies goodware processes. • **16 (Policy):** Panda Adaptive Defense 360 advanced security policies • **17 (SecAppControl):** Security app control technologies. • **18 (ProdAppControl):** Productivity app control technologies. • **19 (EVTContext):** Linux contextual technology. • **20 (RDP)**: Technology to detect/block RDP (Remote Desktop Protocol) intrusions and attacks. • **21 (AMSI)**: Technology to detect malware in AMSI notifications. • **-1 (Unknown)**	
wsdocs	Base-64 encoded list of all documents that were open when an exploit detection occurred.	Character string

Table 27.1: List of the fields that make up the events stored by Panda Security

Chapter 28

The Panda Account

The Panda Account provides administrators with a safer mechanism to self-manage login credentials and access the Panda Security services purchased by their organization than the standard method of receiving credentials by email.

With a Panda Account, it is the administrator who creates and activates the access method to Panda Adaptive Defense's Web console.

> *Users with access to the Panda Account are those who were initially registered in Panda Security, regardless of whether they have been migrated to the WatchGuard provider. Users belonging to the WatchGuard security provider from the start don't have access to the Panda Account.*

CHAPTER CONTENTS

Creating a Panda Account for Panda Security users

Follow the steps below to create a new Panda Account.

Receive the email

- When purchasing Panda Adaptive Defense, you will receive an email from Panda Security.
- Click the link in the message to access a website from which you will be able to create your Panda Account.

Fill out the form

- Enter your information in the form shown.
- Use the drop-down menu located in the bottom-right corner if you want to display the page in a different language.
- Access the License Agreement and the Privacy Policy by clicking the relevant links.
- Click **Create** to finish and receive an email at the address indicated in the form. Use that message to activate your account.

Activating the Panda Account

After it is created, you need to activate your Panda Account. To do this, you must use the message received at the email address you specified when creating your Panda Account.

- Find the message in your inbox.
- Click the activation button. By doing this, the address provided when creating your Panda Account will be confirmed as valid. If the button doesn't work, copy and paste the URL included in the message into your browser.
- The first time you access your Panda Account, you will be asked to confirm your password. Do it and click the **Activate account** button.
- Enter the required information and click **Save data**. If you prefer to provide your data at another time, use the **Not now** option.
- Accept the License Agreement and click **OK**.

Once your Panda Account has been successfully activated, you will be taken to the Cytomic Central site home page. From there, you will be able to access the Panda Adaptive Defense Web console. To do this, click the solution's icon you will find in the **My Services** section.

Editing the Panda Account

If your associated security provider is Panda Security, click the **Edit account** option in Cytomic Central.

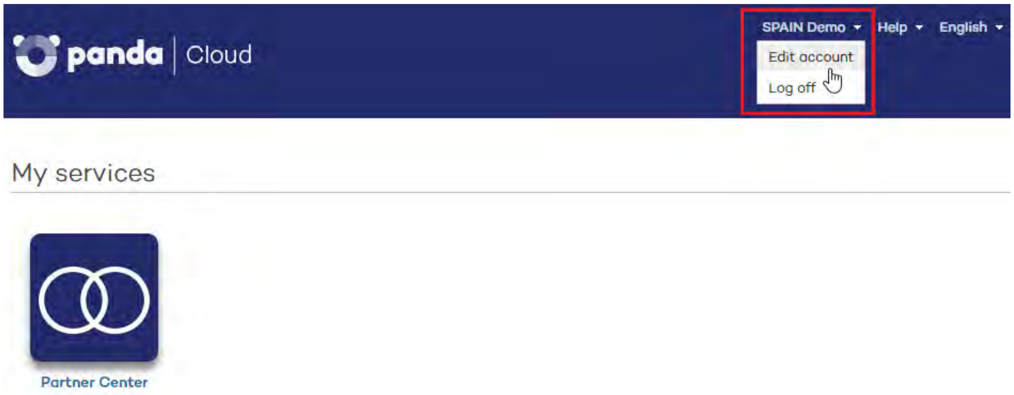


Figure 28.1: Editing the user account

If your associated security provider is WatchGuard, go to https://watchguard.com/

Creating and linking a Panda Account to WatchGuard

For more information on how to activate and link a Panda Account when activating a commercial license, refer to https://www.pandasecurity.com/en/support/card?id=300003.

To manage products from Aether, WatchGuard users must meet the following requirements:

- They must have a WatchGuard user account.
- They must have a Panda Adaptive Defense user account.
- They must link both accounts.

Users belonging to the WatchGuard security provider from the start automatically create a Panda Account when activating a commercial license for a Panda Security product for the fist time.

Users belonging to the WatchGuard security provider but who initially belonged to Panda Security already have a Panda Account. All they have to do is link that account to their WatchGuard Account.

Creating a Panda Account automatically when assigning a commercial license for a Panda Security product

- Go to https://watchguard.com/activate and enter the license key for the Panda Security product.
- Click **I need a Panda account**. A page opens with the account name and ID. We recommend that you save this information. You need this information if you contact Support.
- Click **Submit** and **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.
- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Panda Adaptive Defense.
- To access Panda Adaptive Defense, click **Manage Your Panda Product**. Next, click **Accept and continue** to accept the End User License Agreement.

Linking a Panda Account to a WatchGuard Account when assigning a commercial license for a Panda Security product

- Go to https://watchguard.com/activate and enter the license key for the Panda Security product.
- Click **Link my Panda account**. The Cytomic Central page opens. Enter your Panda Adaptive Defense login credentials. These were sent to you in the welcome email.
- Click the **Log in** button. A page opens indicating that both accounts are linked.
- Click **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.
- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Panda Adaptive Defense.
- To access Panda Adaptive Defense, click **Manage Your Panda Product**. Next, click **Accept and continue** to accept the End User License Agreement.

Chapter 29

Key concepts

Active Directory

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed directory service for finding a range of information on network environments.

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 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 "**Panda Advanced Reporting Tool (ART)**".

Adware

Program that automatically runs, displays or downloads advertising to the computer.

Alert

See "**Incident**".

Anti-Tamper protection

A set of technologies aimed at preventing tampering of the Panda Adaptive Defense processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

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.).

ASLR (Address Space Layout Randomization)

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

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

A set of resources developed by the MITRE Corporation to describe and categorize dangerous adversarial behaviors based on real-world observations. ATT&CK is a structured list of known adversary behaviors, divided into tactics and techniques, and expressed as a matrix. Because this list is a comprehensive representation of behaviors attackers employ when compromising networks, it is useful for organizations that need to develop defensive, preventive, and remedial measurements.

Refer to "**MITRE Corporation**".

Automatic assignment of settings

See "**Inheritance**".

Audit

A Panda Adaptive Defense 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 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.

BitLocker

Software installed on certain versions of Windows 7 and above computers and designed to encrypt and decrypt the data stored on computer volumes. This software is used by Panda Full Encryption.

Blocking

Action performed by Panda Adaptive Defense to prevent programs installed on the user's computer from running due to one of the following reasons:

- The program is classified as a threat
- The program is unknown to Panda Adaptive Defense, the advanced protection policy is configured in lock or hardening mode and the program's origin is untrusted
- The program is blocked by a policy defined by the administrator.

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 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.

CKC (Cyber Kill Chain)

In 2011, the Lockheed-Martin corporation developed a framework or model to defend computer networks which stated that cyberattacks occur in phases and can be disrupted through controls established at each phase. Since then, the Cyber Kill Chain has been adopted by data security organizations to define phases of cyberattacks. These phases range from remote reconnaissance of the target to data exfiltration.

Cloud (Cloud computing)

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

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.

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.

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 agent on them.

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.

Event

A relevant action taken by a process on a user’s computer and monitored by Panda Adaptive Defense. Events are sent to the Panda Security cloud in real time as part of the telemetry flow. There, they are analyzed in their context by analysts, threat hunters, and automatic machine learning processes to determine whether they are part of the Cyber Kill Chain (CKC) of a cyberattack.

Refer to “**CKC (Cyber Kill Chain)**”.

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.

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. After the error occurs, the compromised process will mistakenly interpret certain parts of the data sequence as executable code, triggering dangerous actions that may compromise the security of the targeted computer.

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.

FQDN

A fully qualified domain name (FQDN) is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone. A fully qualified domain name is distinguished by its lack of ambiguity: it can be interpreted only in one way.

General Data Protection Regulation (GDPR)

A regulation that governs the protection of the personal data of all individuals within the European Union (EU). Refer to the following link: **http://www.privacy-regulation.eu/en/index.htm** for the full regulation.

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 operational mode that blocks programs classified as malware and unknown files coming from an untrusted source:

- The Internet.
- External storage drives
- Other computers on the customer's network.

Heap Spraying

Heap Spraying is a technique used to facilitate the exploitation of software vulnerabilities by malicious processes.

As operating systems improve, the success of vulnerability exploit attacks has become increasingly random. In this context, heap sprays take advantage of the fact that on most architectures and operating systems, the start location of large heap allocations is predictable and consecutive allocations are roughly sequential. This allows attackers to insert and later run arbitrary code in the target system's heap memory space.

This technique is widely used to exploit vulnerabilities in Web browsers and Web browser plug-ins.

Heuristic scanning

Static scanning that employs a set of techniques to statically inspect potentially dangerous files. It examines hundreds of characteristics of a file to determine the likelihood that it may take malicious or harmful actions when run on a user's computer.

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

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'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.

indicator

Detection of anomalous actions taken by the processes run on a customer's computers. These infrequent sequences of actions are analyzed in detail to determine whether they are part of the sequence of events involved in a cyberattack.

Refer to "**CKC (Cyber Kill Chain)**".

Indicator of attack (IOA)

This is an indicator with a high probability of being part of a cyberattack. Normally, this is an attack at an early stage or at the exploitation stage. These attacks do not generally use malware, as attackers commonly take advantage of legitimate operating system tools to perform the attack and hide their activity.

Refer to "**indicator**".

Indirect assignment of settings

See "**Inheritance**".

Infection vector

The means used by malware to infect users' computers. The most common infection vectors are Web browsing, email and pen drives.

Inheritance

A method for automatically assigning settings to all subsets of a larger, parent group, saving management time. Also referred to as 'automatic assignment of settings' or 'indirect assignment of settings'.

Inventory

Database kept by Panda Data Control which contains the files classified as PII found across the network.

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 operational mode that blocks unknown programs as well as all files classified as malware.

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.

MITRE Corporation

A not-for-profit organization that operates multiple federally funded research and development centers dedicated to tackling security challenges. It provides practical solutions in the fields of defense and intelligence, aviation, civil agencies, homeland security, healthcare, and cybersecurity, among others. They are the creators of the ATT&CK framework.

Refer to "**ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)**".

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 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 Panda 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 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 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 Full Encryption

A module compatible with Panda Adaptive Defense and designed to encrypt the content of computers' internal storage devices. It aims to minimize the exposure of the data stored by organizations in the event of loss or theft, or when unformatted storage devices are replaced or withdrawn.

Panda Patch Management

A module compatible with Panda Adaptive Defense 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 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.

Passphrase

Also known as enhanced PIN or extended PIN, a passphrase is a PIN that incorporates alphanumeric and non-alphanumeric characters. A passphrase supports lowercase and uppercase letters, numbers, spaces and symbols.

Patch

Small programs published by software vendors to fix their software and add new features.

Payload

In the IT and telecommunications sectors, a message payload is the set of useful transmitted data (as opposed to other data that is also sent to facilitate message delivery: header, metadata, control information, etc.).

In IT security circles, however, an exploit's payload is the part of the malware code that controls the malicious actions taken on the system, such as deleting files, stealing data, etc. (as opposed to the part responsible for leveraging the software vulnerability -the exploit- in order to run the payload).

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Phishing

A technique for obtaining confidential information from a user fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

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 software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the Panda Adaptive Defense cloud.

Public network

Networks in public places such as airports, coffee shops, etc. These networks require that you establish some limitations regarding computer visibility and usage, especially with regard to file, directory and resource sharing.

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Quarantine

See "**Backup**".

Recovery key

If an anomalous situation is detected on a computer protected with Panda Full Encryption, or if you forget the unlock key, the system will request a 48-digit recovery key. This key is managed from the management console and must be entered to start the computer. Each encrypted volume has its own unique recovery key.

RIR (Regional Internet Registry)

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

Role

Specific permission configuration applied to one or more user accounts, and which authorizes users to view and edit certain resources of the console.

Rootkit

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is used by attackers to hide evidence and utilities on previously compromised systems.

ROP

Return-oriented programming (ROP) is a computer security exploit technique that enables 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 enable 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.

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.

Spyware

A program that is automatically installed with another (usually without the user’s permission and even without the user realizing), and collects personal data.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

Suspicious item

A program with a high probability of being malware and classified by our heuristic scanner. This type of technology is only used in the scheduled and on-demand scans launched from the Tasks module, never in real-time scans. Heuristic scanning is used to compensate for the lower detection capability of scheduled scan tasks, in which program code is scanned statically, without running the program.

Refer to “**Heuristic scanning**”.

System partition

Area of the hard disk that remains unencrypted and which is necessary for computers with Panda Full Encryption enabled to start up properly.

Tactic

In ATT&CK terminology, tactics represent the motivation or ultimate goal behind a technique. It is the adversary's tactical goal: the reason for taking an action

Refer to "**ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)**".

Task

Set of actions scheduled for execution at a configured frequency during a specific period of time.

TCO (Total Cost of Ownership)

Financial estimate of the total direct and indirect costs of owning a product or system.

TCP (Transmission Control Protocol)

The main transport-layer Internet protocol, aimed at connections for exchanging IP packets.

Technique

In ATT&CK terminology, techniques represent the means by which adversaries achieve tactical goals. They represent the "how". For example, an adversary looking to steal credentials (tactic), may attempt to dump them (technique).

Refer to "**ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)**".

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.

TPM (Trusted Platform Module)

The TPM is a chip that's part of the motherboard of desktops, laptops and servers. It aims to protect users' sensitive information by storing passwords and other information used in authentication processes.

Additionally, the TPM is responsible for detecting changes to a computer's boot chain, preventing, for example, access to a hard disk from a computer other than the one used to encrypt it.

Trojans

Programs that reach computers disguised as harmless software to install themselves on computers and carry out actions that compromise user confidentiality.

Trusted network

Networks in private places such as offices and households. Connected computers are generally visible to the other computers on the network, and there is no need to establish limitations on file, directory and resource sharing.

Unblocked program

Program blocked during the classification process but temporarily and selectively allowed by the administrator to avoid disrupting user activity.

USB key

A device used on computers with encrypted volumes and which allows the recovery key to be stored on a portable USB drive. With a USB key it is not necessary to enter a password to start up the computer. However, the USB device with the startup password must be plugged into the computer's USB port.

User (console)

Information set used by Panda Adaptive Defense to regulate administrator access to the Web console and establish the actions that administrators can take on the network's computers.

User (network)

A company's workers using computing devices to do their job.

User account

See "**User (console)**".

VDI (Virtual Desktop Infrastructure)

Desktop virtualization solution that hosts virtual machines in a data center accessed by users from a remote terminal with the aim to centralize and simplify management and reduce maintenance costs. There are two types of VDI environments:

- **Persistent VDIs**: the storage space assigned to each user persists between restarts, including the installed software, data, and operating system updates.
- **Non-persistent VDIs**: the storage space assigned to each user is deleted when the VDI instance is restarted, returning to its initial state and undoing all changes made.

Virus

Programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

VPN (Virtual Private Network)

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

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 console

Tool to manage the advanced security service Panda Adaptive Defense, 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'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.

100% Attestation Service

A service included in the Panda Adaptive Defense 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.