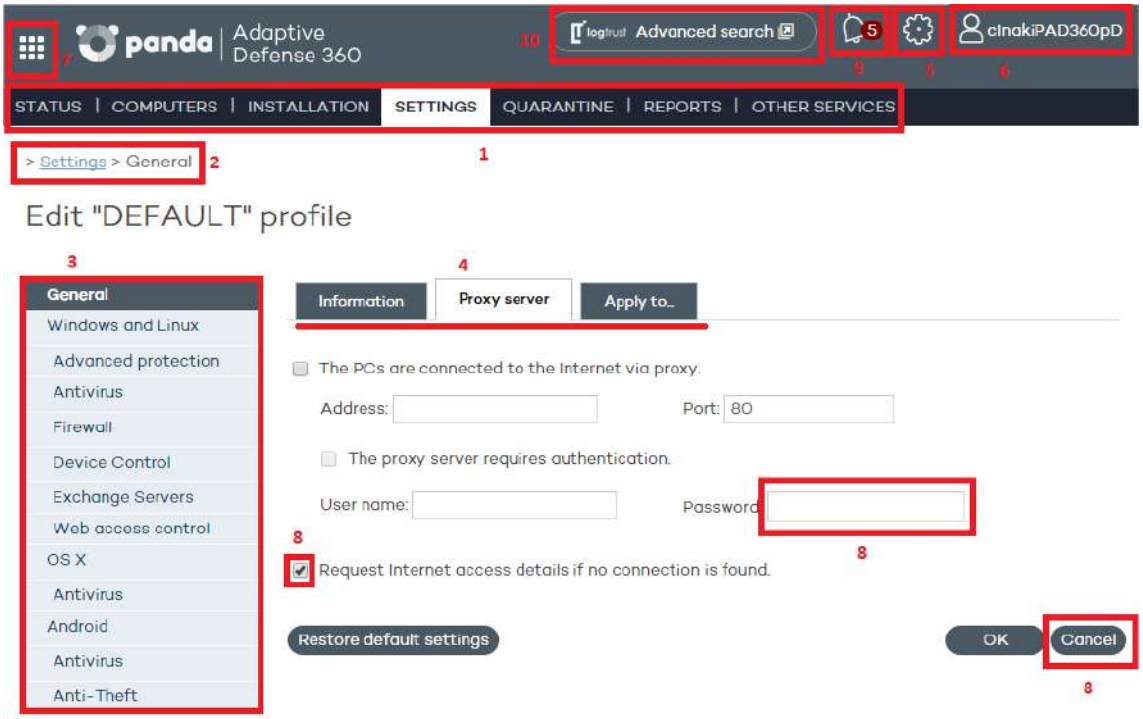
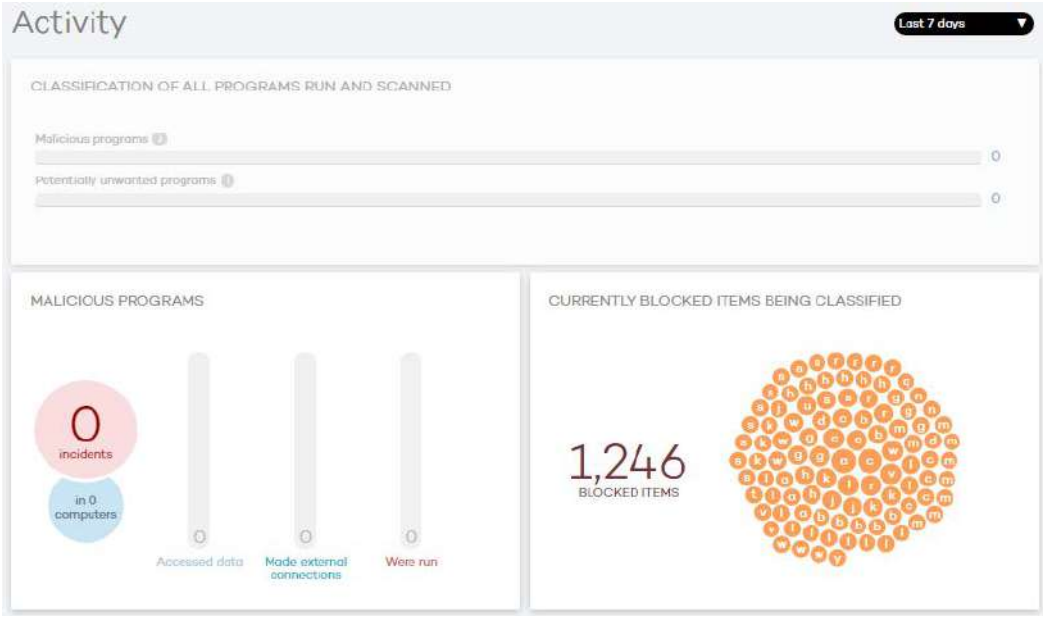
Adaptive Defense 360

Guide for network administrators

Contents





1. Preface

Who is the guide aimed at?

Icons

1.1. Introduction

This guide contains information and instructions to enable users to get the most out of Adaptive Defense 360.

1.2. Who is the guide aimed at?

This guide is aimed at network administrators who need to protect their organization's IT systems and mobile devices, find out the extent of the security problems detected, and define response and remediation plans against targeted attacks and advanced persistent threats (APTs).

Even though Adaptive Defense 360 is a managed service that offers security without the network administrator having to intervene, it also provides clear and detailed information about the activity of the processes and programs run by all users on company systems, regardless of whether they are known or unknown threats or legitimate programs.

In order that network administrators can correctly interpret the information and draw conclusions that can improve corporate security, it is necessary to have some knowledge of Windows processes, file systems and registry, as well as understanding the most frequently used network protocols.

1.3. Icons

The following icons appear in the guide:

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

 Suggestions and recommendations.

 Important advice regarding the use of features in Adaptive Defense 360.

2. Introduction

Key features

User profile

General architecture

2.1. Introduction

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

Adaptive Defense 360 protects IT systems by allowing only legitimate software to run, while monitoring and classifying all processes run on the customer's IT network based on their behavior and nature. Additionally, it completes its security offering by providing monitoring, forensic analysis and remediation tools to help determine the scope of the issues detected and resolve them.

Unlike traditional antiviruses, Adaptive Defense 360 uses a new security concept that allows it to accurately adapt to the environment of any given company, monitoring the running of all applications and learning continuously from the actions taken by each process.

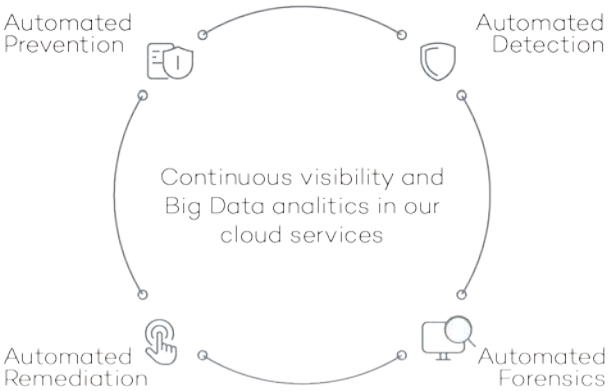
After a brief learning period, Adaptive Defense 360 is able to offer a far greater level of security than traditional antivirus solutions, as well as offering valuable information about the context of any security problems in order to help determine their scope and implement the necessary measures to prevent further incidents.

Adaptive Defense 360 is a cross-platform, cloud-based service compatible with Windows, Linux, Mac OS X and Android; It does not require new infrastructure in the organization, thereby keeping down the TCO.

2.2. Key features of Adaptive Defense 360.

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

- **Visibility:** Traceability of every action taken by running applications.
- **Detection:** Constant monitoring of running processes and real-time blocking of zero-day and targeted attacks, as well as other advanced threats designed to bypass traditional antivirus solutions.
- **Response:** Forensic information for in-depth analysis of every attempted attack, as well as remediation tools.
- **Prevention:** Prevents future attacks by blocking non-goodware applications and using advanced anti-exploit technologies.



2.3. Adaptive Defense 360 user profile

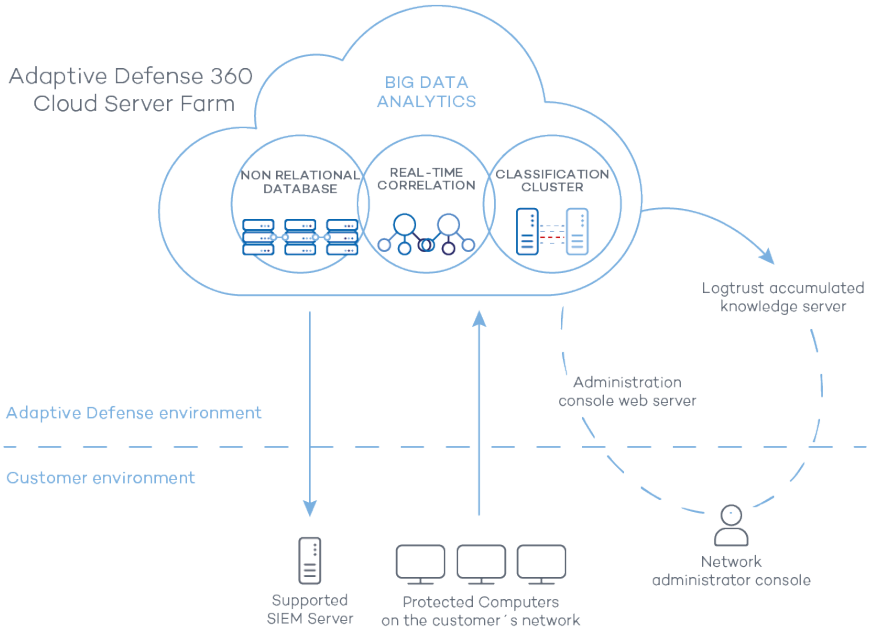
Even though Adaptive Defense 360 is a managed service that offers security without the network administrator having to intervene, it also provides clear and detailed information about the activity of the processes run by all users on the network. This data can be used by administrators to clearly define the impact of potential problems and adapt security protocols to prevent similar situations in the future.

All users with an Adaptive Defense 360 agent installed on their computers will benefit from a guaranteed security service, preventing the running of programs that could represent a threat to the company.

2.4. Adaptive Defense 360 architecture: Key components

Adaptive Defense 360 is an advanced security service based on the analysis of the behavior of the processes run on the customer's IT infrastructure. The analysis of these processes is carried out using machine learning techniques on Big Data infrastructures hosted in the cloud, so customers don't have to install additional hardware or resources in their premises.

The general structure of Adaptive Defense 360 and its components is illustrated below:



Adaptive Defense 360 comprises several components:

- Cloud server farm
- Administration console Web server
- Computers protected by the Adaptive Defense 360 agent
- Computer of the network administrator that accesses the Web console
- Logtrust server for real-time use of accumulated knowledge (optional)
- Third-party SIEM servers compatible with Adaptive Defense 360 (optional)

Below we describe the roles of the architecture components.

2.4.1. Adaptive Defense 360 cloud server farm

The Adaptive Defense 360 cloud server cluster compiles the actions taken by the processes and sent to it from the agents installed on users' computers. Using artificial intelligence techniques, it analyzes the behavior of the processes and classifies them. The classification is returned to the agent to execute a decision and keep corporate computers protected.

The Adaptive Defense 360 server cluster comprises a server farm hosted in the cloud and configured as a Big Data analytics environment continuously applying Machine Learning technologies to classify each process run.

There are several advantages to this new model of analyzing processes in the cloud as opposed to traditional techniques based on sending samples to the antivirus vendor and manual analysis:

- Every process run on the computers protected by Adaptive Defense 360 is monitored and analyzed, which eliminates the uncertainty provided by traditional antivirus solutions, which recognize malware items but cannot identify other applications.
- The delay in classifying processes seen for the first time (the malware window of opportunity) is minimal, as the Adaptive Defense 360 agent relays in real time the actions triggered by each process to the server, which analyzes them looking for suspicious behavior. This drastically

reduces the customer's exposure when dealing with threats and targeted attacks. In addition, the executable files found on users' computers that are not recognized by the Adaptive Defense 360 platform are sent by the agent to our server for analysis.

The sending of the unknown executables is configured to have no impact on the performance of the customer's network. An unknown file is sent only once for all the customers using Adaptive Defense 360*. Bandwidth management mechanisms have also been implemented as well as limits per agent and per hour, in order to minimize the impact on the customer's network.*

- The continuous monitoring of every process allows Adaptive Defense 360 to classify as malware items which initially showed goodware characteristics. That is typical of targeted attacks and other advanced threats designed to remain under the radar.
- Scanning in the cloud frees the customer from having to install and maintain a dedicated hardware and software infrastructure or stay up to date with license payments and manage warranties, notably reducing the TCO.

2.4.2. Administration console Web server

Adaptive Defense 360 is managed entirely through the Web console accessible to administrators from:

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

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

Refer to ***Chapter 5: Web administration console*** *to check whether your browser is compatible with the service.*

The Web console is *responsive* and as such is accessible from smartphones and tablets anytime, anywhere.

2.4.3. Computers protected with Adaptive Defense 360

Adaptive Defense 360 requires the installation of a small software component which has to be installed on all computers on the network.

This component comprises two modules: the communications agent and the protection module.

Even though in this chapter we make a difference between "agent" and "protection", these are two modules that install at the same time and are necessary to correctly manage the security of the computer to protect. This way, both terms -"agent" and "protection"- are used indistinctly to refer to the software component installed on each user's computer.

Communications agent

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

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

The following logic is used to see if the administrator has made configuration changes:

1. The administrator makes a configuration change in the Web console.
2. The server sends a notification to inform the affected computers that a configuration change has been made.

   The affected computers are:

   - If the administrator changes a profile's configuration, the change will affect every computer in the groups that have that profile assigned to them.
   - If the administrator changes a computer's configuration, the change will be notified to every computer in the same group.
3. Each computer checks for new notifications every 15 minutes. If there is a new notification:
   - The computer asks the Adaptive Defense 360 server for the new configuration policies.
   - The server delivers the policies to the computer, which applies them.

Additionally, the agent uses the rumor or peer-to-peer functionality to coordinate with other agents installed on computers in the same group. The peer-to-peer functionality allows an agent to centrally download new signature files and updates for every computer on its network. Refer to Chapter 10: Protection updates for more information.

Dynamic proxy

The agents store a list with information about the computers on the network that have agents capable of sending messages to the Internet. These agents are called proxies.

To act as a proxy for other agents, a computer must meet the following requirements: it must have a direct connection to the Internet and at least 256 MB of RAM. Additionally, the installation sequence must have finished on the computer.

When the list of proxies is empty or none of the agents in the list respond (availability = 0), the agent sends a message via broadcast to the subnet asking “Who is proxy?" so that it can send a message to the Internet via a proxy.

While waiting for data about the list of valid proxies, the proxy's module will not attend other requests.

The list of proxies has a value associated to each proxy with a maximum number of attempts to connect to another agent before it is considered invalid.

By default the number is three, and when the value reaches zero the agent will be considered invalid as a proxy. If at any time all the proxies in a list are invalid, the list itself will be considered invalid and a search for new proxies will be launched through the message "Who is proxy?"

It is possible that the message is sent correctly to a proxy in the list, but the proxy then discovers that it does not have an Internet connection.

In this case, the remote agent will repeat the sequence described herein, resending the message to another proxy in its list, while responding to any other agents via TCP that it is not a proxy anymore and that it should be removed from their lists as it no longer has a connection to the Internet.

This process is repeated until the message is sent correctly to the Internet or it passes through a maximum number of proxies without being sent, in which case the message will be lost.

It is possible to configure the maximum number of proxies through which a message can pass. By default, it will only be sent to one and if the sending attempt fails the message is lost.

All messages contain a list of the proxies through which they have passed to avoid being sent twice to the same proxy without Internet connection.

Static proxy

If you want all access to the Internet to be made through a specific computer chosen by the administrator, instead of dynamically through certain computers, the communications agent gives the possibility of specifying which computer you want to act as a proxy.

The computer that acts as a static proxy must meet the following requirements:

1. It must have an agent installed
2. It must have direct Internet access
3. It must have at least 256 MB of RAM
4. It must have established a connection to the server in the last 72 hours.

If, at any time, the computer set to work as a static proxy ceases to meet some of the requirements to act as such, the static proxy setting will be disabled in the console, the name of the computer will disappear, and a message will be displayed indicating the requirement that was not fulfilled.

The administrator will then be able to select another computer to work as a static proxy. If a computer stops acting as a static proxy because it has been blacklisted, but is then whitelisted, it will have to be configured again as static proxy so that all communications with the server pass through it.

If an agent has to access the Internet, it will first try to communicate using the static proxy.

If communication through the static proxy is not possible, it will try to establish a connection using the usual sequence of communication procedures.

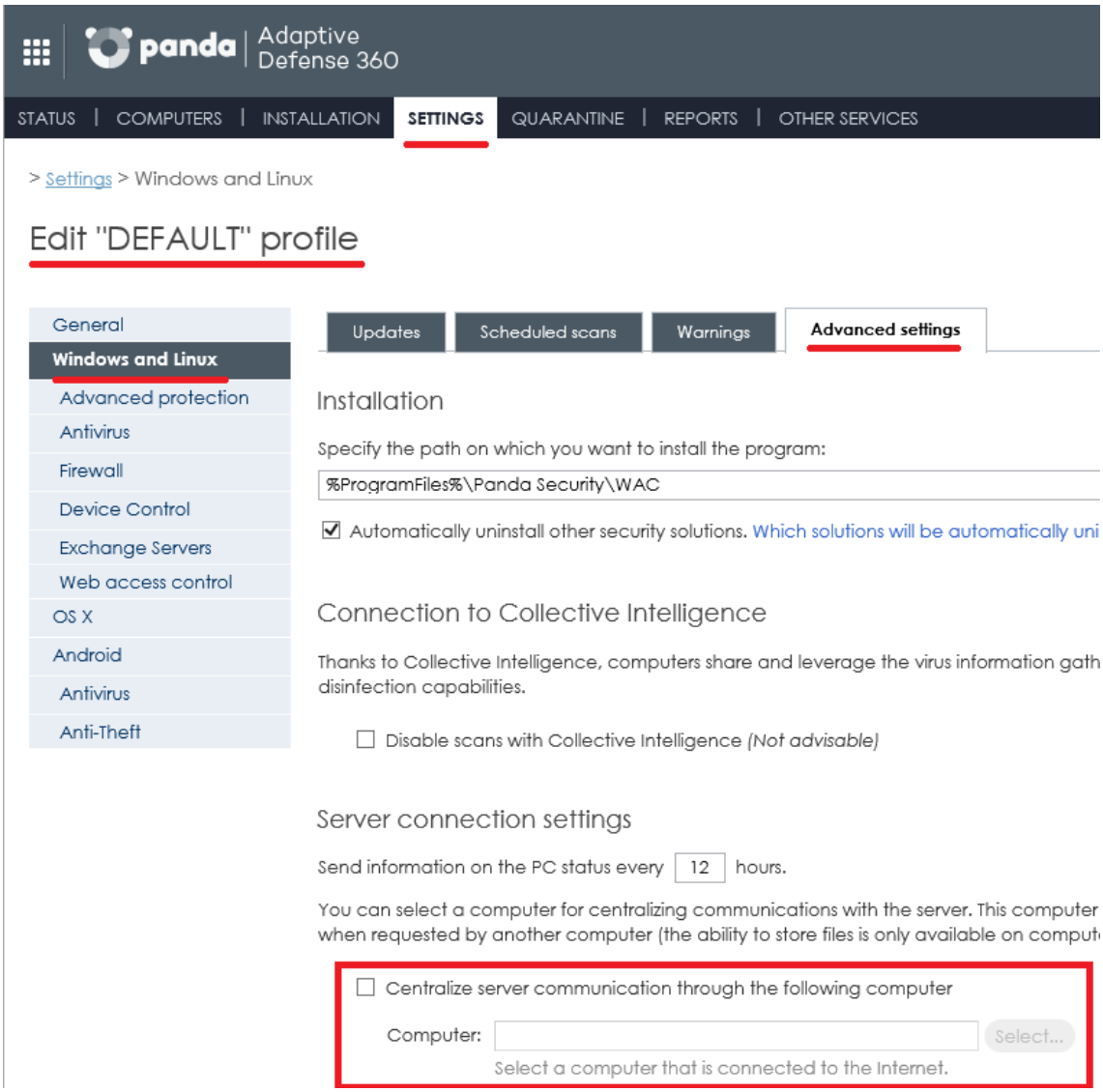
If it has a valid configuration stored, it will try to communicate using those settings.

Otherwise, it will try to connect directly to the Internet.

If it cannot connect directly, it will try to connect through a computer acting as a 'dynamic proxy', as described in the previous section.

When the computer acting as a proxy receives a request to access the Internet, it will try to connect directly. If the connection is successful, it will send the relevant reply to the agent requesting the connection.

To configure a static proxy, edit the properties of the profile that the installed agents belong to. To do that, go to the **Settings** window and select the profile to edit from the menu on the right. In the **Windows and Linux** menu, click **Advanced settings** and select the checkbox **Centralize server communication through the following computer**.



Protection module

This module contains the technologies that protect customers' computers. Adaptive Defense 360 combines in a single product all resources needed to detect targeted and next-generation malware (APTs), as well as remediation tools to disinfect compromised computers and assess the impact of intrusion attempts.

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

2.4.4. Logtrust accumulated knowledge server

Adaptive Defense 360 adds the option of including a storage service for all the knowledge generated by a customer's computers, with an entry for each action taken by the processes run on the customer's IT infrastructure, whether goodware or malware. This makes it possible to flexibly relate and visualize all the data gathered to get additional information about threats and about how users are using the company's IT resources.

The Logtrust service is accessible from the Web console dashboard.

Refer to Chapter 22 for information on configuring and using the knowledge analysis and advanced search service.

2.4.5. Third-party SIEM servers compatible with Adaptive Defense 360

Adaptive Defense 360 integrates with any third-party SIEM solution that customers may be using, transmitting data about the applications run on their computers. This information is sent to the SIEM server along with all the knowledge gathered by Adaptive Defense 360 and can then be leveraged by the customer's tools.

The SIEM systems compatible with Adaptive Defense 360 are:

QRadar

AlienVault

ArcSight

LookWise

Bitacora

Refer to Integration with SIEM products, for more information about how** Adaptive Defense 360 **integrates with third-party SIEM solutions.

2.4.6. Early Classification Service 24h and Early Classification Service 72h

Adaptive Defense 360 classifies every application run on the customer's network as malware or goodware. More than 99 percent of all processes seen on the network are known or are automatically classified in less than 24 hours. However, a small number of programs, in particular advanced malware specifically designed to go undetected, may require a manual analysis by our PandaLabs expert engineers.

Depending on the **Early Classification Service** that the customer selects, Panda Security will ensure that all programs run are classified within 24 or 72 hours of being detected, either automatically or manually.

The service level is assessed on a quarterly basis, and if the service terms and conditions are not met, Panda Security agrees to automatically extend the service free of charge for an additional quarter.

To implement the** Early Classification Service **successfully, a 1-month training period is required in which the solution will learn about the characteristics of the customer's network.

2.4.7. Samples Feed

This service serves as an essential complement to those companies that have their own malware analysis laboratory.

By using a REST API, Panda Security will provide the customer with normalized samples of the malware and goodware found on their network for analysis.

Panda Security will also deliver malware automations, that is, comprehensive execution reports detailing the actions taken by the malware found on the customer's network in Panda Security's sandbox infrastructures equipped with real machines.

2.4.8. IP Feeds

This is a subscription service where customers receive sets of IP addresses used by botnets detected and analyzed by Panda Security.

This information flow is delivered on a daily basis and can be leveraged by the customer's security devices to increase the protection level of their network.

3. The adaptive protection full cycle

3.1. Introduction

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

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

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

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

In view of this dramatic change in the malware landscape, Adaptive Defense 360 proposes a new security approach based on an **adaptive protection cycle**: a set of protection, detection, monitoring, forensic analysis and remediation services integrated and centralized within a single administration console to show the network security full cycle in real time.

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

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

3.2. The adaptive protection cycle

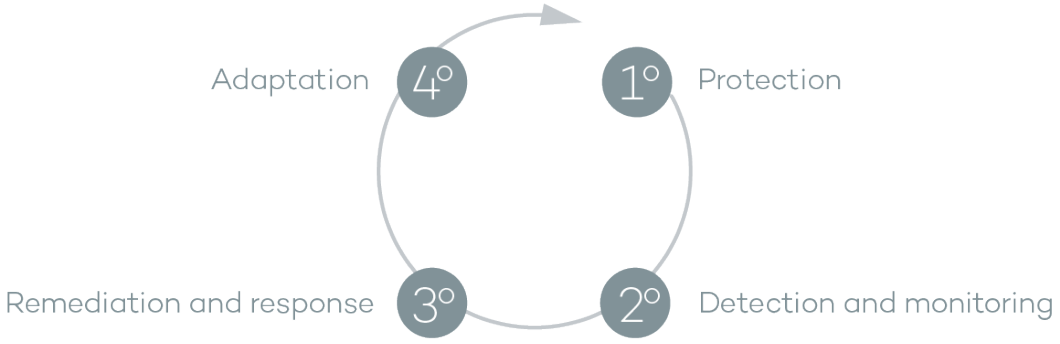
Adaptive Defense 360 is a managed service that frees administrators from the responsibility of deciding which files are dangerous and why.

Instead, the company's technicians are provided with the time and tools necessary to monitor and assess the security status of the network and the applications run by users.

The final objective is to allow organizations to adapt their security policies to respond to new threats, in a continuous fine-tuning process that results in a secure, productive IT environment for users.

Additionally, administrators are provided with forensic analysis and remediation tools to combat security threats, restore systems back to a normal condition after an intrusion attempt, and determine the scope of an intrusion in order to develop effective contingency plans.

The adaptive protection cycle adopted by Adaptive Defense 360 is illustrated in the graph below, which will be explained in the next sections.



3.3. 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. Adaptive Defense 360 is compatible with Windows, Linux and Mac OS X workstations and servers, as well as with Android smartphones and tablets.

Protection is a module traditionally developed by general security vendors that offer antivirus solutions to protect the infection vectors most commonly used by hackers. These antivirus products rely on the signatures files published by the security vendor, and downloaded by users to their local computers or accessed in real time from the cloud.

Adaptive Defense 360 complements these traditional means with a series of advanced technologies designed to prevent malware entry and unauthorized access:

Anti-exploit protection for vulnerable systems

Panda Security has developed a new technology that strengthens its security solutions and detects viruses that no other security company is able to detect. The aim is to protect even those systems that are recognized within the industry as vulnerable, having reached their EOL (End Of Life), like Windows XP for example. Those systems no longer receive security updates and may have vulnerabilities that can be taken advantage of through exploits.

Adaptive Defense 360 detects and neutralizes malware like Blackhole or Redkit that exploits zero-day vulnerabilities (in Java, Adobe, MS Office, etc.) to infect computers. It uses a three-layered detection/protection approach that analyzes how exploits behave instead of their morphology.

In the first layer, Adaptive Defense 360 provides passive protection against exploits by leveraging well-known technologies such as DEP, ASLR, SEHOP, Bottom Up Randomization and others.

In the second layer, the solution runs heuristic scans to find out if a process has been exploited by malware taking advantage of a software vulnerability. This layer is capable of detecting ROP, Stack pivot and other strategies used by exploits to bypass protection systems and run malicious code.

The third layer performs a behavioral analysis to detect the execution of malicious code by an exploited process. To do that, the solution performs contextual behavioral analyses locally by using the knowledge accumulated on Panda Security's Collective Intelligence platform.

This three layered approach allows Adaptive Defense 360 to effectively protect systems with known vulnerabilities.

Permanent antivirus protection and Collective Intelligence

Adaptive Defense 360's antivirus protection leverages **Collective Intelligence**, a security platform that provides high-level protection in real time, exponentially increasing the solution's detection capabilities.

Collective Intelligence has servers that automatically classify and process all the data provided by the user community about detections on their computers. Adaptive Defense 360 queries **Collective Intelligence** whenever required, ensuring maximum detection without negatively affecting resource consumption on computers.

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

Given the current context of increasing amounts of malware, Collective Intelligence and services hosted in the cloud are an essential complement to traditional updates to successfully combat the enormous amount of threats in circulation.

Refer to chapters 13, 14, 15 and 16 for more information on the Adaptive Defense 360 ***antivirus protection for the various supported platforms***

The Cloud

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.

Adaptive Defense 360 is served from the cloud, connecting to Collective Intelligence servers to protect your computers at all times, increasing its detection capabilities and not interfering with computer performance. Now, all knowledge is in the cloud, and thanks to Adaptive Defense 360, all users can benefit from it.

Protection against advanced stealth techniques and macro viruses

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

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

Finally, the service can also detect the latest fileless infection techniques, which inject the virus payload directly into the processes used to exploit system vulnerabilities. These attacks do not write files to the hard disk, so traditional security solutions are less likely to detect them.

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

Email and Web protection

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

Refer to chapter 13 for more information about how to configure the email and Web protection

Firewall and intrusion detection system (IDS)

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

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

*Refer to chapter 13 for more information about **how to configure the firewall** and the intrusion detection system*

Device control

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

Adaptive Defense 360 allows administrators to restrict the use of those devices on protected computers, blocking access to them or allowing them to be completely or partially used (read-only access).

*Refer to chapter 13 for more information about **how to configure the device control** feature*

Spam, virus and content filtering for Exchange servers

Adaptive Defense 360 scans for viruses, hacking tools and suspicious/potentially unwanted programs sent to the Exchange Server mailboxes.

Eliminating junk mail (spam) is a time-consuming task. And not only that, spam is also a frequent source of scams.

To tackle this, Adaptive Defense 360 provides anti-spam protection for Exchange Server. This feature helps companies improve user productivity and increase the security of network computers

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

- Mailbox protection

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

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

Additionally, the mailbox protection allows administrators to scan Exchange server user folders in the background, making the most of server idle times. This protection uses smart scans which do not re-scan already scanned items, as opposed to the typical scenario where both the mailboxes and the quarantine folder are scanned every time a new signature file is published.

- Transport protection

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

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

*Refer to chapter 13 for more information about **how to configure the protection for Microsoft Exchange***

Web access control

This protection allows network administrators to limit access to specific Web categories, and configure a list of URLs to allow or deny access to. This feature allows companies to optimize network bandwidth and increase business productivity.

Web pages are divided into 59 categories. Select the URL categories that you want to deny access to. You can modify them at any time.

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

*Refer to chapter 13 for more information about **how to configure the Web access control feature***

3.4. 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, Adaptive Defense 360 implements a number of novel technologies that allow the network administrator to pinpoint the problem.

Advanced permanent protection

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

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

Adaptive Defense 360 implements three blocking types for unknown (not yet classified) processes and processes classified as malware:

- Audit

In Audit mode, **Adaptive Defense 360** only reports on detected threats but doesn't block or disinfect the malware detected. This mode is useful for testing the security solution or checking that the installation of 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 Adaptive Defense 360 to gain sufficient information 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 Adaptive Defense 360 as goodware: They are allowed to run.
- Files classified by Adaptive Defense 360 as malware: They are sent to quarantine or disinfected.
- Unclassified files coming from external sources (Internet, email and others): They are prevented from running until a classification is returned. Once a classification is returned they will be allowed to run (goodware) or not (malware).

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

- Unclassified files that are installed on the user's computer before the implementation of Adaptive Defense 360: They will be allowed to run although their actions will be monitored

and sent to the server for analysis. Once classified, they will be allowed to run (goodware) or sent to quarantine(malware).

- Lock

In environments where security is the top priority, and in order to offer maximum security guarantees, Adaptive Defense 360 should be configured in **Lock** mode. In this mode, the software that is in the process of classification will be prevented from running. This means that only legitimate software will be allowed to run.

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

More than 99% of programs found on users' computers are already classified by Adaptive Defense 360***. Only a small minority of programs are prevented from running.***

Refer to chapter 13 for more information about how to configure the different blocking modes

Monitoring data files

Adaptive Defense360 monitors every access to the user's data files by the processes run on the computer. This way, if a malicious item manages to infect the computer, it will be possible to accurately determine which files were modified and when.

It will also be possible to determine if those files were sent out over the Internet, the target 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 and user certificate stores.

Digital Wallet stores.

Browser settings.

Firewall settings.

GPO settings.

Visibility of the network status

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

Some of these tools, like the reports, are already known, however, the important thing at this point is not only to determine if 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 Adaptive Defense 360 dashboard provides key information for that purpose:

- Information on which processes found on the network are unknown to Adaptive Defense 360, and which process are in the process of being classified by Panda Security, along with a preliminary assessment of their danger level.
- Detailed activity information through 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, both known malware trying to enter the network and neutralized by the Protection module, as well as 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 networks by preventing all unknown software to run, or adjust the blocking level to allow certain unknown programs to run.

Refer to chapter 17 for more information about the visibility and monitoring of computers and processes

3.5. Remediation and response

In the event of infection, administrators must be able to work in two lines of action: quickly restore affected computers to their original state, and assess the impact of the infection, that is, find out

whether there was a data leak, the extent of the attack, which computers were compromised, etc. The Remediation and Response phase provides tools for these two scenarios.

Response

Administrators have a Forensic Analysis tool that displays every action taken by malware, including the infection vector (the way the malware entered the network), information about any attempt to spread to other computers or access the user's hard disk to steal confidential information, and any connections made to external computers.

Additionally, the Logtrust accumulated knowledge server stores every action taken by the processes run by users. This makes it possible to extend the functionality of the forensic analysis module and perform advanced searches to generate activity graphs that aid data analysis and interpretation.

*Refer to chapter 21 for more information about how to use the **Forensic Analysis** tool*

Remediation

Adaptive Defense 360 provides several remediation tools, some manual and some automatic.

The automatic tools include the traditional disinfection module typical of antivirus solutions, along with the quarantine used to store suspicious or deleted items.

In the case of infections caused by advanced malware or very complex disinfections, administrators have the option to use a standalone disinfection tool developed by Panda Security from the administration console: **Cloud Cleaner.**

Additionally, they can also use remote desktop tools to connect to other computers remotely and troubleshoot issues caused by malware.

*Refer to chapter 20 for more information about how to use the **Remediation tools***

3.6. Adaptation

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

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

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

Changing the advanced protection settings

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

Changing the antivirus protection settings

Scheduling a larger number of scans or enabling the protection of infection vectors such as email or the Internet will help protect computers.

Restricting access to certain websites by category

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

Filtering out spam and phishing messages

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

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

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

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

The firewall is a tool designed to minimize malware exposure on computers, by preventing communications to and from programs that are not malicious in nature but may leave the door open for malware to enter the network. If malware is detected that infects the network via a chat or P2P application, configuring the firewall rules correctly can prevent those programs from communicating with the exterior.

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

4. Creating Panda Accounts

4.1. What is a Panda Account?

When you buy Adaptive Defense 360 you will receive an email from Panda Security. Click the link in the message to go to the website where you can create your Panda Account.

You must then activate your Panda Account using the link sent to you in another email message.

Finally, go to Panda Cloud. There you will find the shortcut to access the Adaptive Defense 360 Web console.

This new method aims to increase the security of your login credentials as, instead of receiving them via email, you yourself create and activate your Panda Account, the entry point to access the Adaptive Defense 360 Web console.

Panda Cloud lets you manage your cloud solutions quickly and easily and, if necessary, access information regarding other Panda Security solutions which will resolve all your network's protection needs.

4.2. How can I create a Panda Account?

After you purchase your licenses you will receive an email message. Now you can create your Panda Account. To do this, follow these steps:

1. Open the message and click the link included in it.
2. You will access a Web page to create your Panda Account.
3. Enter your email address and click **Create.**

Use the language menu if you want to display the page in a different language. You can also view the license agreement and the privacy policy by clicking the relevant links.

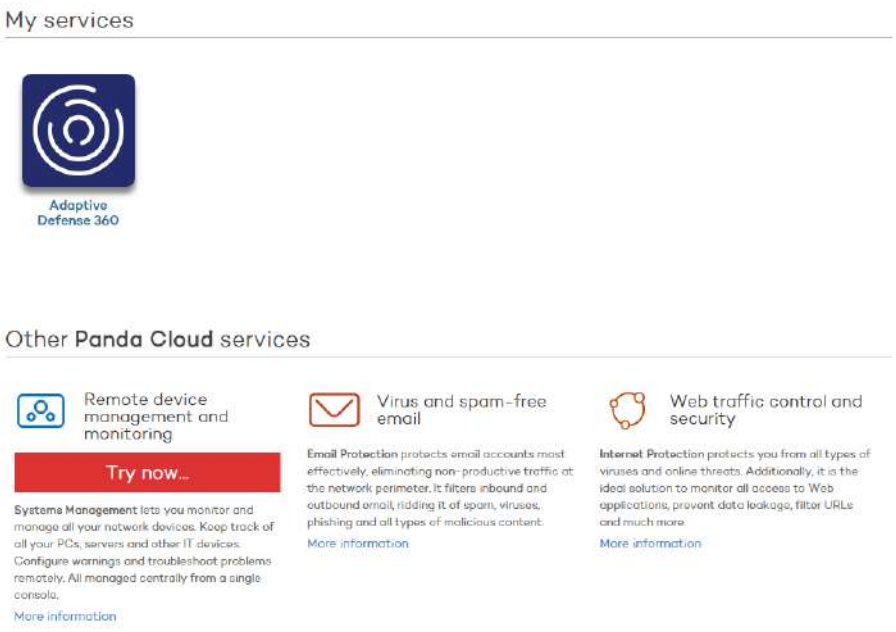
You will receive another message at the email address specified when creating your Panda Account. Use this message to activate your account.

4.3. How can I activate a Panda Account?

Once you have created your **Panda Account** you have to activate it. In order to do that, you will receive a message at the email address you specified when creating your Panda Account.

1. Go to your inbox and find the message.
2. Click the activation button. By doing that, you will validate the email address that you provided when creating your Panda Account. If the button doesn't work, copy and paste the URL included in the message into your browser.
3. The first time that you access your Panda Account you will be asked to set a password. Click **Activate Account**.
4. Enter the required data and click **Save data**. If you prefer to enter your data later, click **Not now**.
5. Accept the license agreement and click **OK**.

You will have successfully activated your Panda Account. You will then find yourself in the Panda Cloud site. From there, you will be able to access your Adaptive Defense 360 console. To do that, simply click the solution icon in the **My services** section.



5. The Web administration console

General structure of the Web administration console

5.1. Introduction

This chapter explains the general structure of the Web administration console.

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

A single tool for complete security management.

The Web administration console lets you distribute the protection agents to network computers, configure security settings and monitor the protection status of computers, as well as offering troubleshooting tools and forensic analysis in the event of problems. All these functions are available from a single console, facilitating integration of different tools and minimizing the complexity of using products from different vendors.

Centralized security management for all offices and mobile users

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

Security management from anywhere at any time

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

5.1.1. Web console requirements

The Web console can be accessed from the following link:

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

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

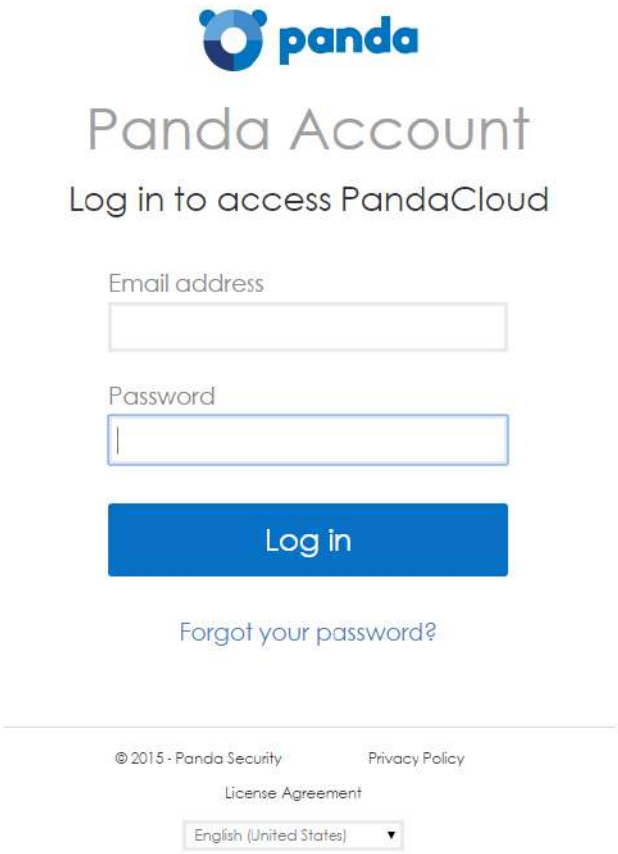
- You must have valid login credentials (user name and password). See Chapter 4 for more details on how to create a Panda account for accessing the Web console.
- A certified compatible browser (others may be compatible).
    - Internet Explorer 10 or later.
    - Firefox
    - Google Chrome

- Internet connection and communication through port 443.

5.1.2. IDP federation

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

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

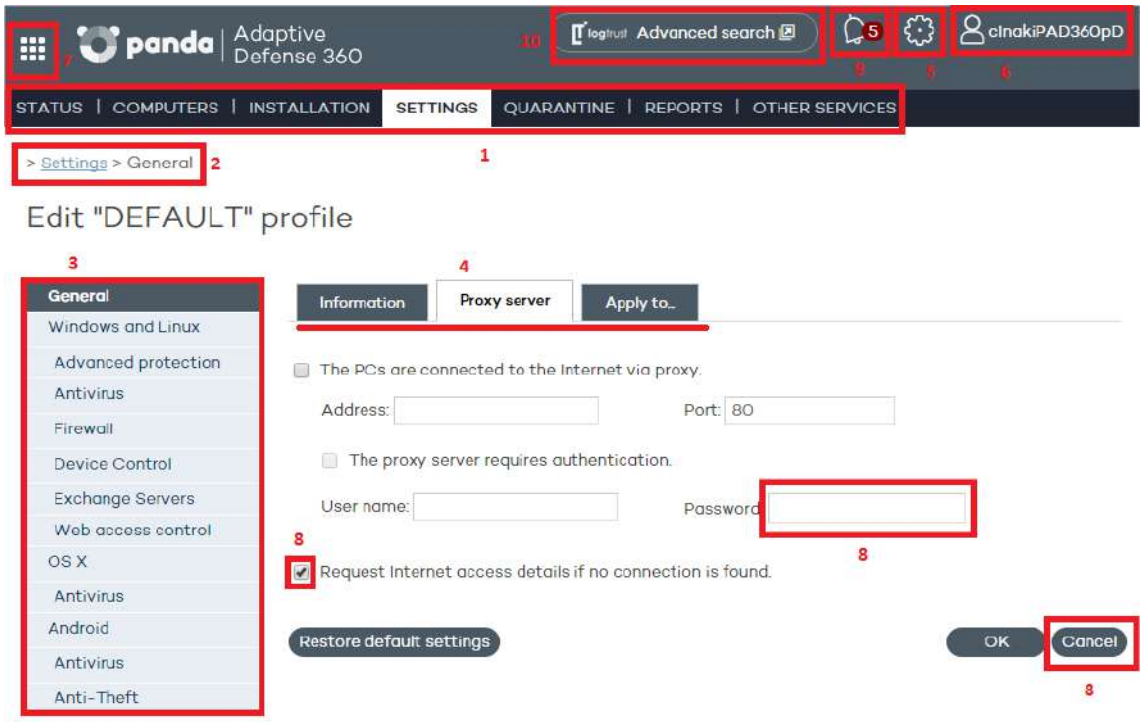


5.2. General structure of the Web administration console

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

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.

5.2.1. General view of the Web administration console

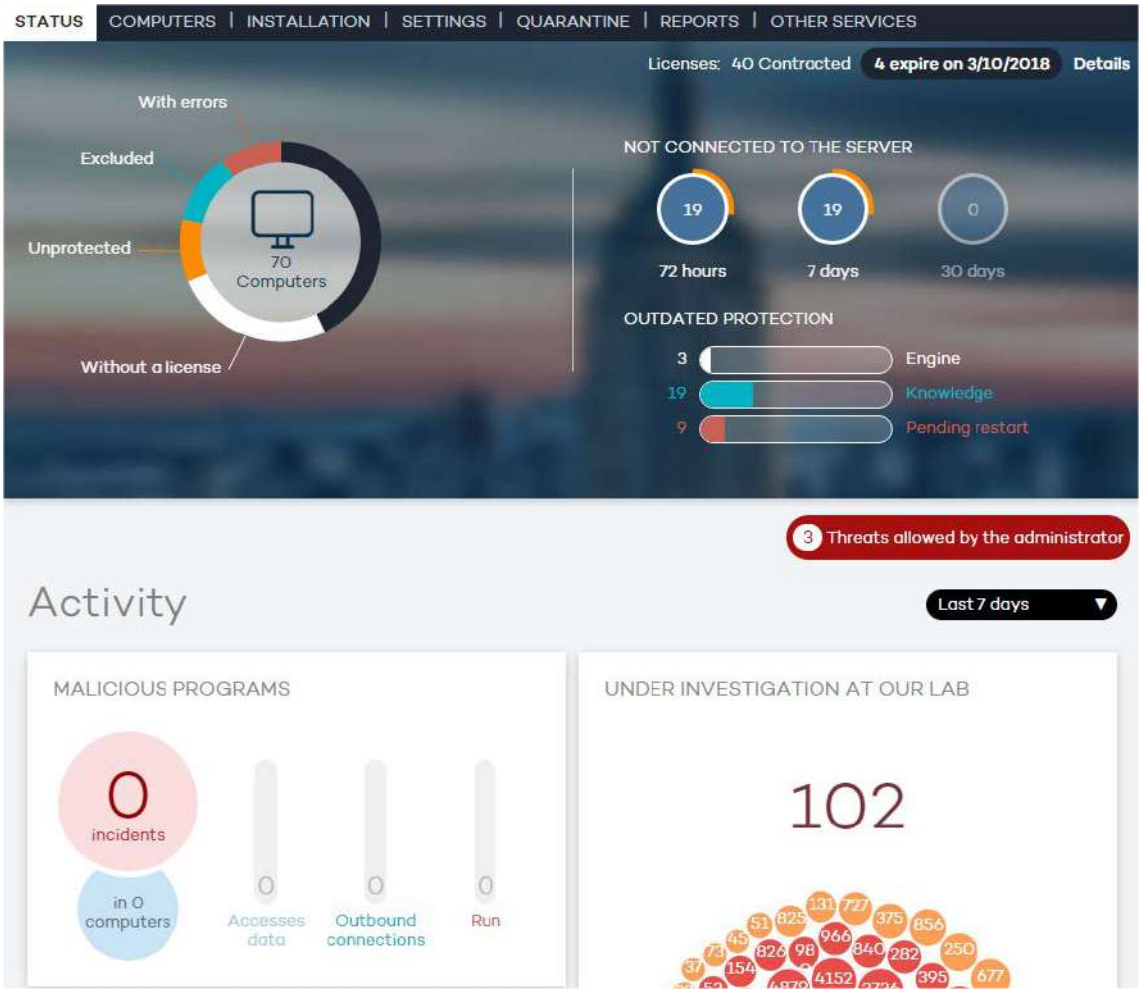


5.2.2. Top menu (1)

The top menu has seven windows, each with related tools and resources:

- **Status**
- **Computers**
- **Installation**
- **Settings**
- **Quarantine**
- **Reports**
- **Other services**

Status window



The **Status** window is the first one you see when accessing the console for the first time. It shows a number of counters with information about your licenses and the status of your protection.

If you haven't installed the protection on any of your computers, you'll be prompted to go to the **Computers** window to begin the installation.

The **Status** window has a number of panels with graphs describing the security status of the network and Adaptive Defense 360 licenses.

*See Chapter 6 **Licenses** for more details on license management in* Adaptive Defense 360. *See Chapter 17 **Visibility and monitoring** and Chapter 19 **Reports** for more real-time information on the network security status and consolidated reports.*

Computers window

This contains information about the status of network computers. The Computers window displays an installation wizard if there are still no computers on the network with the agent installed.

It is also possible from the Computers window to add agents, although this task can be carried out entirely from the Installation window.

Installation window

This contains all the tools you need for deploying Adaptive Defense 360 agents on the network.

*See Chapter 9 **Installing the protection** for more information about the process of installing Adaptive Defense 360 agents on network computers.*

Settings window

This lets you manage and configure groups and protection profiles.

*See Chapters 11 and 12 for more details on how to **create profiles** and **groups**, and Chapters 12, 13, 14, 15 and 16 for configuring protection profiles in accordance with the platform (**Windows, Linux**, **Mac OS X** and **Android**)*

Quarantine window

This contains a list of all the items discovered on the network that Adaptive Defense 360 considers suspicious and/or that have been deleted to prevent the risk of infection.

*See Chapter 18 **Quarantine** for more information*

Reports window

The reports let you send and receive static consolidated documents in several formats about specific areas of the security service.

*See Chapter 19 **Reports** for more information*

Other services window

This lets you contact the Panda Security technical department as well as send comments and suggestions regarding the service.

5.2.3. Browser path (2)

The browser path shows the full path for the current window.

This path comprises the names of the windows that have been passed through to get to the present location, separated by the “>” symbol.

The hyperlinks can be used to go directly back to any previous point, without having to retrace your steps.

5.2.4. Side menu (3)

The side menu is displayed in several windows, such as Installation or Settings. It contains a series of options that administrators can use to display additional settings. Clicking these options adds them to the browser path discussed above.

5.2.5. Tabs (4)

These are used to group common settings options across many of the windows in the console. Tabs are not added to the browser path when clicked.

5.2.6. General settings button (5)

This displays a drop-down menu with several general options described below:

Users

This lets you create new users with different access permissions to the Web console.

See Chapter 8 for more information about users and permissions.

Preferences

This includes general settings regarding the operation of the console:

- **Language**: Lets you choose between 13 console languages.
- **Email alerts**: Lets you send email alerts to administrators directly from the Adaptive Defense 360 platform. These alerts contain information about the items detected and blocked on Windows computers**.**

*For more information, refer to the **Windows protection profiles** section.*

- **Default view**: This determines how computers will be displayed in the console: by name or by IP address.

- **Group restrictions**: This lets you determine the maximum number of computers in any given group.

See Chapter 11 Groups for more information about creating and managing groups.

- **Remote access:** This lets you configure the credentials for accessing computers administered by Adaptive Defense 360 and which have any of the supported remote desktop applications installed (LogMeIn, TeamViewer and VNC). This access can be shared with the service provider in order to delegate management of the computers**.**

See Chapter 20 Remediation tools for more details.

- **Automatic management of suspicious files:** This lets you automatically send files classified as suspicious to Panda Security for analysis.
- **Account management:** This lets you merge accounts and delegate administration of computers.

See Chapter 7 Managing Accounts for more details.

Help

This is the console context-sensitive Help file. Click F1 to get the Help file for the current screen.

Advanced administration guide

This lets you download the advanced administration guide**.**

Tech Support

From here you can contact Panda Security's Support department**.**

Suggestions box

This lets you contact the Panda Security Product department to send comments and suggestions regarding the service**.**

License agreement

Here you can see the product EULA**.**

About

This displays the versions of the various service components.

5.2.7. Logged-in user (6)

This lets you log out of the console, and then displays the IDP (Identity Provider) screen in order to log in.

5.2.8. Panda Cloud button (7)

This button gives administrators access to Panda Cloud, where they can see at a glance all the Panda Security services they have contracted.

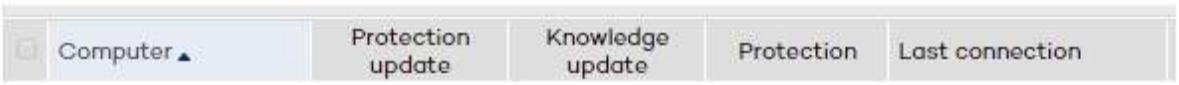
5.2.9. Settings components (8)

The Adaptive Defense 360 console uses standard settings components, such as:

- Drop-down menus
- Combo boxes
- Buttons
- Check boxes for activation
- Dialog boxes

In many cases, the console checks whether the text that has been entered is correct (if the "@" symbol is present in email addresses, numerical data, etc.).

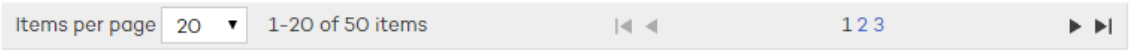
Adaptive Defense 360 uses a series of tables to present lists. All these tables have a header that lets you order the lists by different criteria. Click on a header category to order the list according to this category and click it again to reverse this order.



The direction of the arrow indicates whether the order is ascending or descending.

At the bottom of the table there is a pagination tool. This function varies depending on the type of table:

- Lines per page selector
- Shortcut to specific pages
- Next page
- Previous page
- Last page
- First page



5.2.10. Notifications (9)

The notifications icon includes a red number indicating the number of urgent messages that the system has to deliver to the administrator.

Here there is a color code -blue, red, orange- to indicate the importance of the message.

5.2.11. Access to the accumulated knowledge service (10)

This button takes you to the accumulated knowledge repository console. This repository provides detailed reports and lets you carry out advanced searches for applications on the network and their activity.

*See Chapter 22 **Accumulated Knowledge Server** for more details.*

6. Licenses

Contracting and renewing licenses

License status

Assigning and releasing licenses

License expiry alerts

6.1. Introduction

In order to use the service you must have licenses for Adaptive Defense 360 for Windows/Linux/Android or Adaptive Defense 360 for OS X if you need protection for OS X systems. Depending on the specific needs of each network, it may be necessary to install/uninstall the protection on computers, remove computers from the protected list, add new computers to the list, etc.

License usage is reflected in the number of available licenses.

> ***Licenses for** Adaptive Defense 360 **for Windows/Linux/Android can be used on any of these operating systems.***

> ***To protect computers and servers with OS X, you must get licenses specifically for this system, as the licenses are not the same as those for Linux/Windows/Android.***

6.2. Contracting and renewing licenses

To start using the service, you have to contract licenses for each of the computers you want to protect. An Adaptive Defense 360 license is assigned to a single computer (workstation or server).

> ***To contract or renew licenses contact your designated partner.***

6.2.1. License contracts

Licenses are grouped into license contracts. A license contract is a group of licenses listed with the following characteristics:

- **Product**: Adaptive Defense 360 or Adaptive Defense 360 + Logtrust.
- **Contracted**: Number of licenses contracted in the license contract.
- **Type**: Trial (30 days) or Release.
- **Expiry date**: Date when the licenses expire and the computers will cease to be protected.

The license contracts will vary depending on the platform:

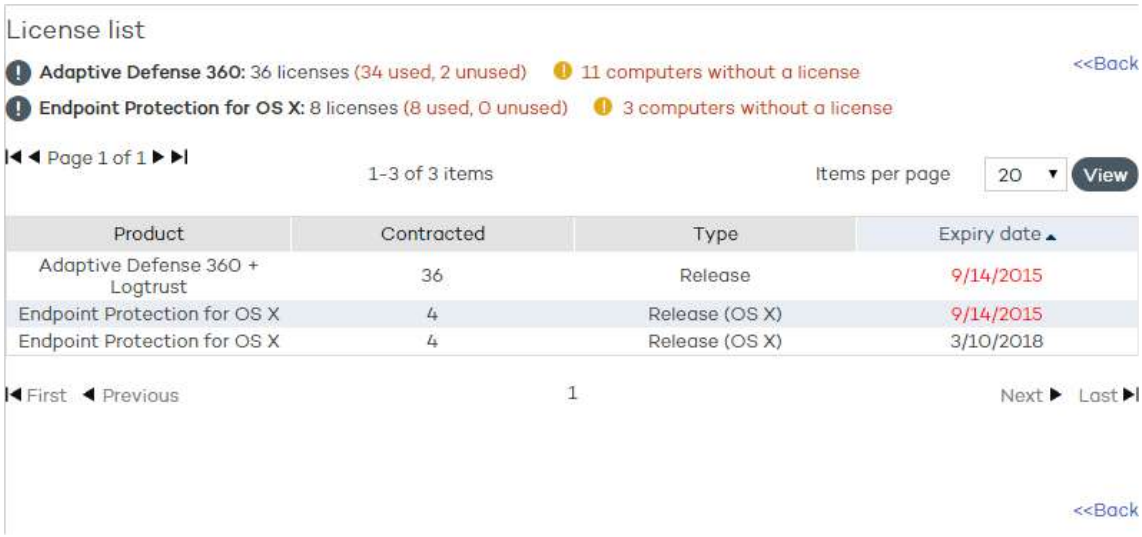
  - License contracts for Windows / Linux / Android: Licenses contracted for these platforms can be interchanged and used on any of these systems.

- License contracts for Mac OS X are specific to OS X.

At the top of the console you can see the total number of contracted licenses for all active license contracts along with the expiry date of the license contracts that will expire soonest and the corresponding number of licenses.

To view details of the license contracts click **Status** and **Details**.

You will see a **License list** comprising a list of license contracts and additional information.



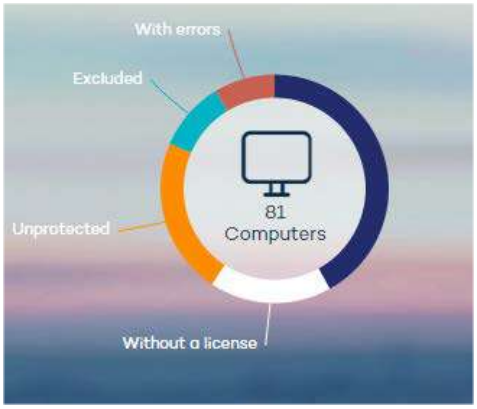
At the top you will see the status of the licenses split into two groups:

- Adaptive Defense 360: Number of contracted licenses (used, unused) and computers without a license.
- **Endpoint Protection for OS X**: Number of contracted licenses (used, unused) and computers without a license.

In the center of the screen you can see the various license contracts and their descriptions. Move the cursor over them to display more detailed information.

6.3. License status

The **Status** window includes the Adaptive Defense 360 dashboard which reflects the current status of network computers, in the form of a circle with colored segments and counters.



Move the cursor over each color to display a tooltip with the number of computers corresponding to each category.

Click the different areas of the panel to display more information about the license status.

6.3.1. Network computers

In the center of the license panel you can see all the computers discovered on the customer's network, regardless of their status (whether or not they have a valid license assigned, with errors etc.). This counter also includes the computers located by the discovery tool.

Click the counter to display the **Computers** window.

6.3.2. OK computers

The dark blue area of the circle corresponds to protected computers, i.e, computers with a valid Adaptive Defense 360 license and with no errors.

These computers are using a license.

6.3.3. Computers without a license

Computers without a license are those that are not protected because there are insufficient licenses to protect them, or because they belong to a group with a maximum number of licenses assigned by the administrator.

Click the white area to display the **Without a license** tab of the **Computers** screen with a list of the computers that don't have a license assigned.

These computers do not use up licenses.

6.3.4. Computers with errors

The red area displays the computers with errors, i.e. computers with a license assigned and on which the agent was installed correctly but the protection has returned an error.

These computers use licenses.

6.3.5. Excluded computers

The light blue area represents excluded computers. If there are less licenses contracted than the total number of computers that require protection, you can prioritize the computers to be protected first and the others will be excluded.

Excluded computers are those that the administrator has decided will temporarily not be protected. Excluded computers do not compete to obtain a spare license, they are not updated and their status is not reported to Adaptive Defense 360.

These computers do not use up licenses.

6.3.6. Unprotected computers

These are represented by the yellow segment of the circle. They are unprotected as the agent has not been correctly installed on the computer, they have been identified by the discovery tool or the agent has been uninstalled.

These computers do not use up licenses.

6.4. Assigning and releasing licenses

When the agent is installed on one computer, one license of Adaptive Defense 360 for Windows/Linux/Android or Adaptive Defense 360 for OS X will be subtracted from the total number of available licenses.

When a computer is removed from the list of protected computers, one license of Adaptive Defense 360 for Windows/Linux/Android or Adaptive Defense 360 for OS X will automatically be added to the total number of available licenses, depending on the operating system of the computer you remove.

When due to expiry the number of contracted licenses is reduced by 'X', the status will change to Without a license for as many Windows/Linux/Android or OS X computers and devices as licenses have expired.

6.4.1. Reassigning licenses

Where the number of contracted licenses is less than the number of computers to protect, this difference will be included in the **Without a license** tab. These computers will compete for any spare licenses that appear, as explained in the section Contracting and renewing licenses.

To prevent a computer without a license from competing for newly contracted licenses, you have to delete them from the console. To do this, go to the **Without a license** tab in the **Computers** screen, select the computers and click **Delete selected computers**.

If you want to release a license from a computer with a valid license, you have to exclude the computer. The license will then be released and assigned to a computer in the **Without license** list.

Note: You cannot just delete a computer with licenses, as the next time it communicates with the Adaptive Defense 360 server, it will be assigned a license once again. See Chapter 10 for more information about deleting computers.

6.5. License expiry notifications

The **Notification** area displays different alerts relating to the expiry date of your licenses: whether it has been exceeded, whether there are licenses expiring in the next 60 days, and whether you could be left with fewer licenses than those currently used.

These notifications are different depending on the operating system of the computers whose licenses are about to expire, i.e. warnings regarding licenses of Adaptive Defense 360 for Windows/Linux/Android, and Adaptive Defense 360 for OS X appear separately.

In both cases you can renew your licenses by contacting your usual reseller or sales advisor. Adaptive Defense 360 will display a reminder in the **Status** window.

See Chapter 5 for more information about the notifications.

7. Account management

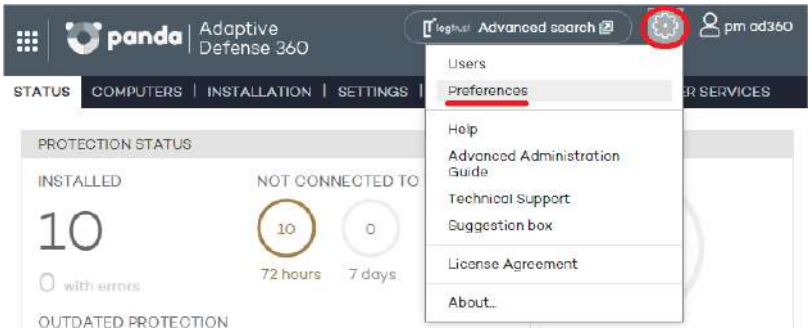
Delegating account management

Merging accounts

7.1. Introduction

Console users with total control permissions have access to the account management features provided by Adaptive Defense 360: delegating account management and merging accounts.

Both options can be found in the **Account management** window. To access it, go to **Preferences** and click **Manage accounts**.

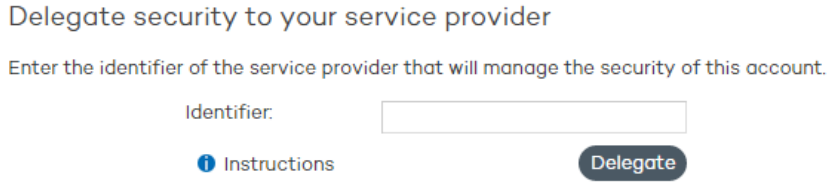


7.2. Delegating account management

This feature lets you delegate security management to a partner, or change the partner that takes care of managing your network security.

> ***To delegate account management to a partner, you will need the partner's Panda Security identifier.***

In the **Delegate security to your service provider** section, enter the partner's identifier.



7.2.1. Possible errors when delegating account management

The following errors may appear when trying to delegate account management:

Invalid identifier. Please try again and make sure you enter it correctly. Try again and make sure you enter the partner ID correctly.

You do not have licenses to perform this operation. Contact your usual sales advisor or reseller to renew them. If your licenses have expired you will not be able to access the account management feature. Please contact your reseller or sales advisor to renew your licenses.

Could not perform the operation. Please contact your reseller or sales advisor. It is possible that the characteristics of the services/licenses that you contracted do not allow you to use the management delegation feature. Please contact your reseller or sales advisor.

An error occurred: Could not register the request. Please try again. This error occurs when the process fails for an unknown reason. Please try again and if you cannot activate the service, contact Panda Security technical support.

7.3. Merging accounts

If a client has products in several accounts, they can merge them into a single one to facilitate centralized management of their computers' security. The process of merging accounts consists of transferring all of the data from a source account to a target account and delete the source account.

The process of transferring data is not immediate. It may take a short time before you can see the change reflected in the target account Web console.

Consequences of merging accounts

It is **VERY IMPORTANT** that before you merge accounts, you understand the consequences:

- The services associated with the source account will be moved to the target account. Those services will cease to be active in the source account, which will be deleted. Also, access to the source account Web console will be denied.
- The target account Web console will display data and information from the computers that were managed from the source account. To check this, just access the target account Web console.
- The protection installed on the computers managed from the source account will be reassigned automatically, and will be managed from the target account. It will not be necessary to reinstall the protection.

Requirements for merging accounts

Below we describe the necessary requirements to merge accounts successfully. If any of the following requirements is not met, the process will be interrupted and an error message will be displayed in the console.

- Both the source account and the target account must have the same version of Adaptive Defense 360.
- Neither the source account nor the target account may have expired licenses.
- Both the source account and the target account must belong to the same partner.
- The source account must have fewer than 10,000 licenses. The target account, however, can have more than 10,000 licenses.
- Both the source account and the target account must have the same additional services contracted.

7.3.1. How to merge accounts

Access the source account Web console (this is the account that will be canceled).

Click Manage accounts in the Preferences window. You will be taken to the Account management window.

Select Merge.

Enter the Login Email of a user with total control permissions on the account to transfer the data to, as well as the client number (identifier) provided in the welcome message.

If you're sure you want to merge the accounts, click Merge.

7.3.2. Effects of account merging on service configuration

Merging accounts involves transferring information about managed computers from a source account to a target account. More precisely, this is the information that the service transfers (or doesn't transfer) from one account to the other:

- **License information**: All data about active license contracts (that is, information about active licenses, start and end dates, types of licenses, etc.) will be transferred from the source account to the target account.
- **Configuration profiles:** All configuration profiles from the source account will be transferred to the target account. If there is already a profile with the same name in the target account (for example, Sales Profile), the profile from the source account will be renamed with a numeric suffix (Sales Profile-1).

The default profile (Default) from the source account will be transferred to the target account, but will be considered as just another profile and will lose the status of default profile.

- **Computer groups**: All computer groups in the source account will be added to the target account. In the case of groups with the same name, the same criteria will be applied as with profiles in the previous point.
- **Reports**: The settings of the reports generated in the source account will not be added to the target account.

- **Statistics**: All detection statistics will be transferred from the source account to the target account.
- **Quarantine**: All items found in the source account quarantine, including excluded and restored items, will be lost.
- **Users**: All users with access to the source account Web console (and their permissions) will be added to the target account, except the default user.

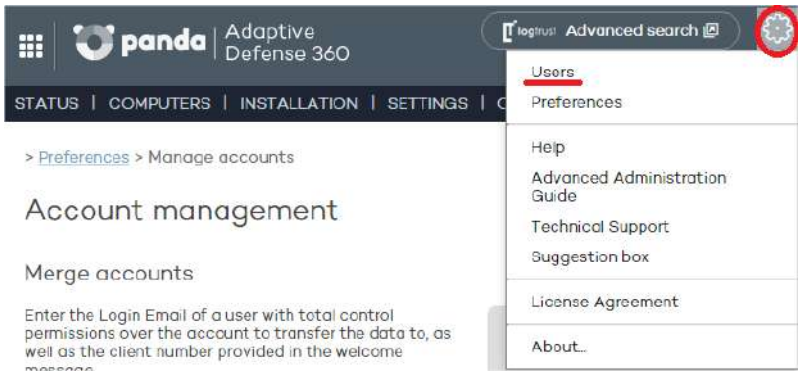
8. Users

8.1. Introduction

> ***In this chapter, the term "user" refers to the different accounts created to access the Web console, not the network users who work with computers protected with*** Adaptive Defense 360

Creating different users and assigning permissions to them makes it possible to share the Adaptive Defense 360 management tasks among various administrators with different access levels and technical profiles/roles.

To configure users and permissions, go to the **Users** menu.



The **Users** menu splits data into three columns: **Login Email**, **Name** and **Permissions**. As you create users, these will appear on the list, along with the type of permissions that you have given them.

8.2. Creating users

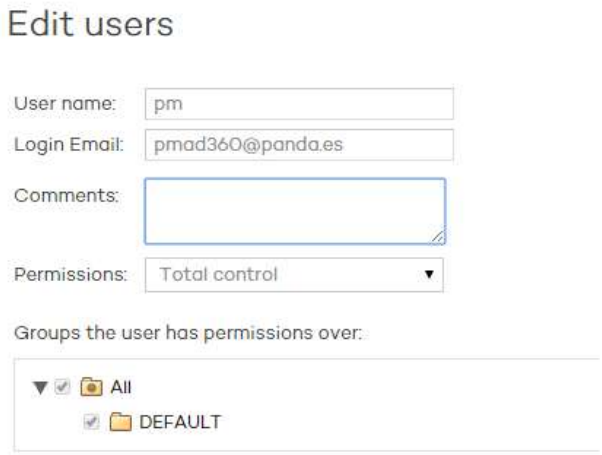
Follow these steps to create a user:

1. In the **Users** menu, click **Add user**.
2. Enter the **Login Email** and confirm it.
3. You can add additional information in the **Comments** section if you want to.
4. Select the permission to assign to the user. For more information, refer to the **Types of permissions** section.
5. In **Groups**, select the group/subgroup or groups/subgroups that the user will be able to act upon, based on the permissions assigned to them. Users with total control permissions will be able to act on all groups.

6. Click **Add**. A message will be displayed informing you that an email message has been sent to the address specified when creating the user.
7. After the user has been created, it will appear on the list available in the **Users** section.

8.3. Changing user details

To change a user's details, go to the **Users** section, and click the user's login email address to access the **Edit users** window.

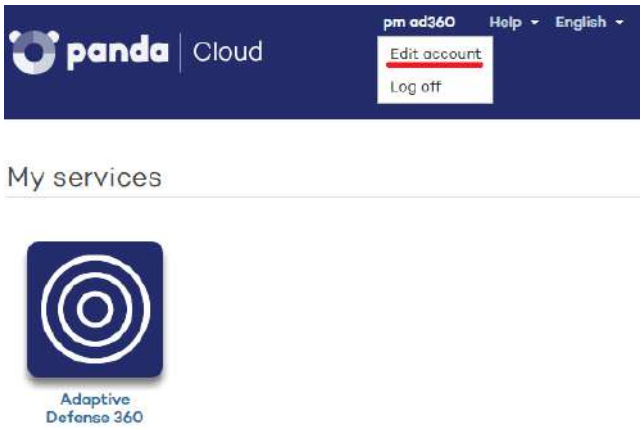


This window lets you change the user's comments, their permissions and the groups they can act upon, but not their name or login email address.

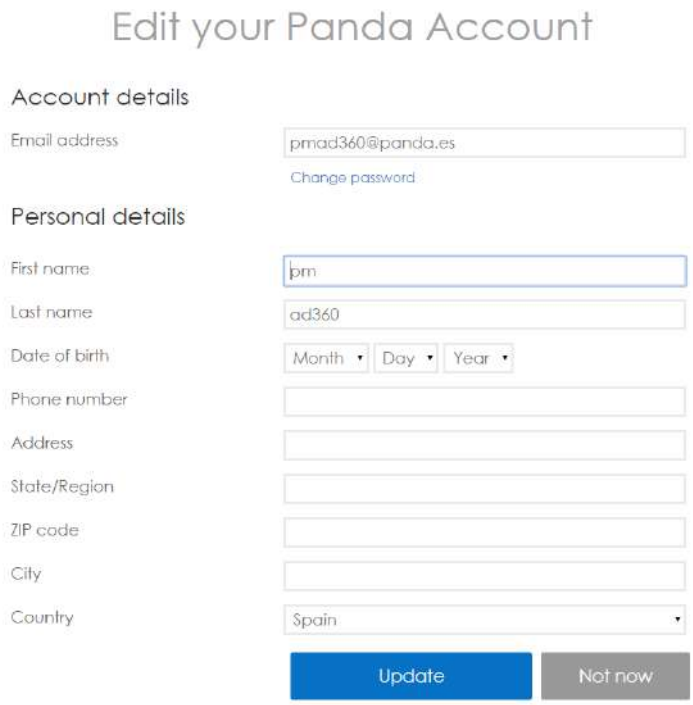
> ***In the case of the Default user, it is only possible to edit the Comments field.***

8.3.1. Changing user names

To change a user's name, access the Panda Cloud console through the icon in the upper left corner of the window, log in using the user's credentials and click the user's name. Then, click **Edit account**.



You will access the user's Panda Account, from which you will be able to change the user's details and password. Then click **Update**.



Once this is complete, both Web consoles (Panda Cloud and Adaptive Defense 360) will display the new user name.

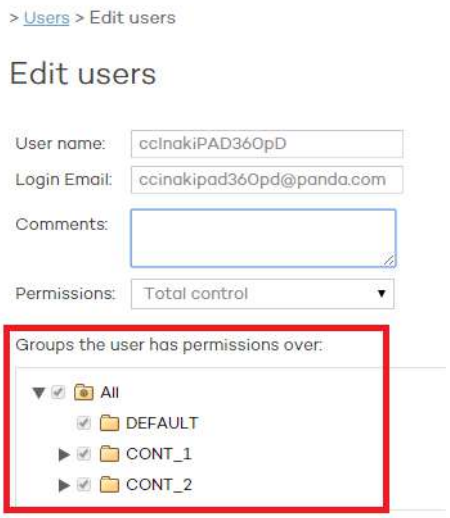
8.4. Deleting users

To delete a user, go to the **Users** menu. On the user list, select the checkbox next to the user that you want to delete. You can select all users at once by selecting the checkbox in the **Login Email** column header. Then, click **Delete**.

8.5. Assigning permissions to users and groups

Adaptive Defense 360 allows you to assign different access permissions for console users on one or several computer groups. This way, each user will only be able to manage the security of the computers belonging to the groups they have access to.

To assign permissions on groups, edit the user and select the groups of computers whose security the user can manage.



8.5.1. Permission inheritance

When giving permissions on a specific group, every subgroup in the group will inherit the assigned permissions. From then on, every newly created subgroup in the group will automatically inherit the permissions assigned on the parent group.

Otherwise, if you assign permissions on a parent group and some of its subgroups but not all, any new subgroup that may be added to the group won't inherit the permissions of the parent group.

8.6. Types of permissions

Adaptive Defense 360 includes three types of permissions. The permission assigned to a user will dictate which actions they can perform, and on which computers or groups.

The actions that a user can take affect various aspects of the basic and advanced protection settings, and include the creation and modification of their own user credentials, the configuration and assignment of user groups and profiles, the generation of different kinds of reports, etc.

The permissions that exist are:

Total control permission

Administrator permission

Monitoring permission

8.6.1. Total control permission

User management. Users can:

- View all users created on the system.
- Delete users.

Group and computer management. Users can:

- Create and delete groups/subgroups.
    - If a user has total control permissions on a group, they will also have them on all its subgroups.
    - If a user has total control permissions on a group, and later a subgroup is added to that group, the user will automatically have total control permissions on the newly created subgroup.
- Configure the protection profiles of all groups.
- Assign computers to all groups/subgroups.
- Move computers from one group/subgroup to another.
- Edit the **Comments** field in the **Computer details** window.
- Access any computer remotely.

Profile and report management. Users can:

- Copy profiles and view copies of any profile.
- Configure scheduled scans of specific paths for any profile.
- View reports (on-demand reports, not scheduled ones) on any group.
- Create tasks to send scheduled reports on any group.
- View all report sending tasks.

Search of unprotected computers. Users can:

- Configure searches for unprotected computers.
- View and/or delete any of the tasks created.

Protection uninstall. Users can:

- Configure protection uninstall tasks.

- View and/or delete any of the tasks created.

License and account management. Users can:

- Use the option to add licenses using an activation code.
- Use the option to merge accounts.
- Delegate security management to a partner.

8.6.2. Administrator permission

The actions that administrator users can perform (manage users, computers and groups, as well as configuring and uninstalling the protection), are restricted to those computers or groups they have created or have permissions on.

User management. Users can:

- Change their own credentials.
- Create users.

Search of unprotected computers. Users can:

- Create search tasks launched from computers on which they have permissions.
- View and/or delete any of the previously created search tasks, but only from computers in groups on which they have permissions.

Group and computer management. Users can:

- Create groups/subgroups (manual or automatic by IP address), and configure the protection profiles of the groups on which they have permissions. Administrator users cannot access a *child* group if they do not have access to the relevant *parent* group.
- Delete groups on which they have permissions. You can only delete groups that don't have any computers inside, that is, prior to deleting a group/subgroup you must assign or move its computers to another group/subgroup. Once you have emptied a group/subgroup, you can delete it.
- Edit the **Comments** field of those computers on which they have permissions, in the **Computer details** window.
- Remotely access computers that belong to groups on which they have permissions.

Protection uninstall. Users can:

- Configure uninstall tasks for those computers and groups on which they have permissions.
- View and/or delete uninstall taks, but only on computers belonging to groups on which they have permissions.

Profile and report management. Users can:

- Create and view new profiles.
- Create copies of profiles on which they have permissions and view them.

- Configure scheduled scans of specific paths for profiles on which they have permissions or which they have created.
- View reports (on-demand reports, not scheduled ones) on groups on which they have permissions, provided those permissions apply to all the groups covered in the report.
- Create tasks to send scheduled reports on groups they have permissions on.
- View tasks to send scheduled reports on groups they have permissions on, provided those permissions apply to all the groups covered in the report. Otherwise, they will not be able to view the report sending task.

8.6.3. Monitoring permission

Users can:

- Change their own credentials.
- View and monitor the protection of the groups/subgroups assigned to them.
    - If a user has monitoring permissions on a group, they will also have them on all its subgroups.
    - If a user has monitoring permissions on a group and later a subgroup is added to that group, the user will automatically have monitoring permissions on the newly created subgroup.
- View the profiles assigned to the groups/subgroups on which they have permissions.
- View searches for unprotected computers performed from computers belonging to groups/subgroups on which they have permissions.
- View uninstall tasks for groups/subgroups on which they have permissions.
- View reports (on-demand reports) on groups/subgroups on which they have permissions.
- View tasks to send reports on groups/subgroups they have permissions on, provided those permissions apply to all the groups/subgroups covered in the report. Otherwise, they will not be able to view the report sending task.

9. Installing the protection

9.1. Introduction

Installing the protection consists of deploying the software required to enable the advanced protection, monitoring and security management services to the network computers.

It is important to install the protection on every computer on the network to prevent security breaches that may be later exploited by attackers through malware designed to attack vulnerable systems.

Adaptive Defense 360 provides several tools to help administrators install the protection. These tools are available or not depending on the platform to install the protection on.

The table below shows the tools included in Adaptive Defense 360 and their availability for each platform.

Tool	Platform			
	Windows	Linux	Mac OS X	Android
Agent download from the console	YES	YES	YES	YES
Generation of download URL	YES	YES	YES	YES
Centralized distribution tool	YES	No	No	No
Search for unprotected computers	YES	No	No	No

9.1.1. Agent download from the console

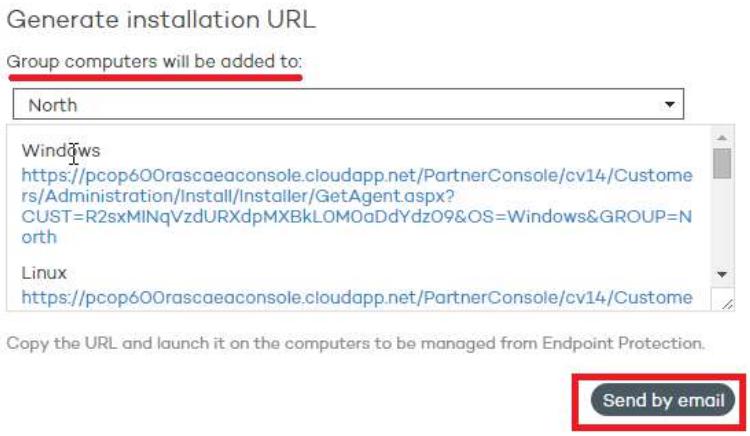
This consists of downloading the installation package directly from the administration console. To do that, select the platform to protect in the **Installation** window: Windows, Linux, Android and Mac OS X

Click the relevant icon to download the appropriate package. Bear in mind that despite the installation method is very similar for all operating systems (Windows, Linux, OS X and Android), it is advisable that you read later in this chapter the specific section for each of them to find out their peculiarities.

In both Linux and Windows, the installer is the same for 32-bit and 64-bit platforms. Before downloading the installer, don't forget to check the requirements that the computers/devices must meet.

9.1.2. Generating a download URL

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



Generate the URL and click the **Send by email** button.

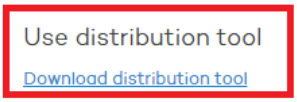
Also, the installation process lets you select the group that the computer whose protection you are installing will belong to. Select the relevant group from the drop-down menu displayed. By default, the computer will belong to the DEFAULT group.

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

9.1.3. Centralized distribution tool

The distribution tool lets you install and uninstall the protection centrally on Windows computers, avoiding manual intervention from end users throughout the process.

In the **Installation** window, click **Download distribution tool**.



In the download dialog box, select **Save**. Then, once it has downloaded, run the file from the directory you saved it to. A wizard will guide you through the installation process.

Adaptive Defense 360 also supports centralized installation using third-party tools such as Microsoft Active Directory.

The procedure to use the centralized distribution tool and install the protection with third-party tools is explained in ***Annex I: Centralized installation tools***

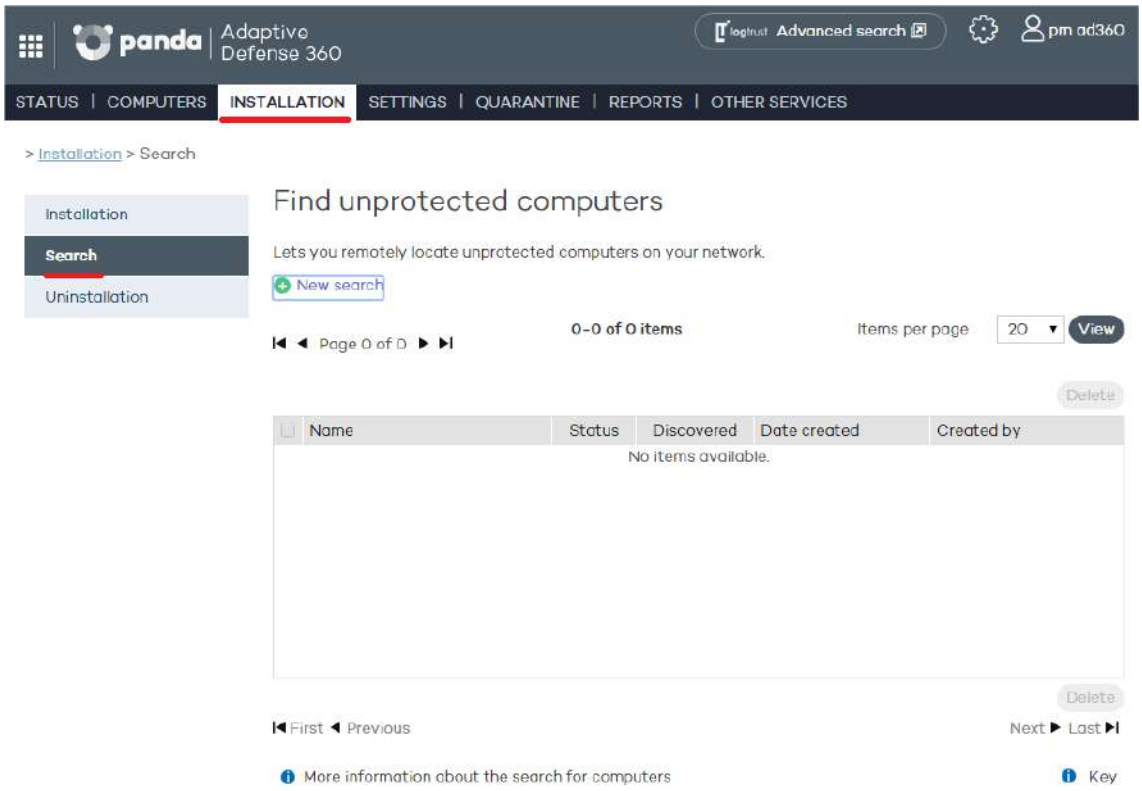
9.1.4. Searching for unprotected computers

Adaptive Defense 360 includes a computer search system that gives administrators a global vision of the unprotected computers on the network.

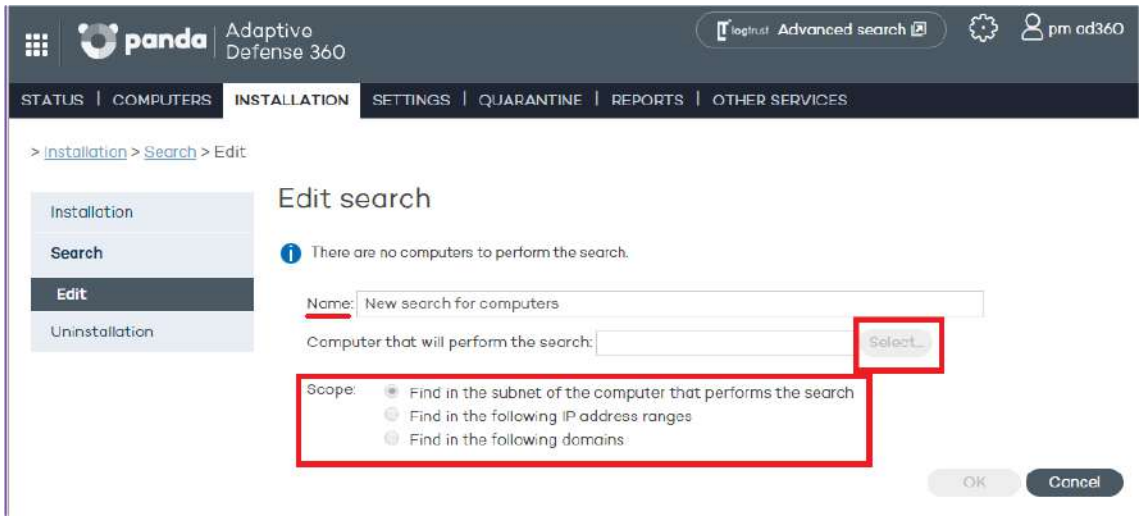
This system is based on configuring and running search tasks performed by a computer that must meet a series of requirements:

- It must have the agent and the protection installed, and be correctly integrated into the Adaptive Defense 360 server.
- It cannot appear on the **Excluded computers** tab, in the **Computers** window.
- It must have established a connection to the Adaptive Defense 360 server in the last 72 hours.
- It cannot be performing an uninstall task, that is, it cannot show any of the following statuses regarding an uninstall task:
    - **On hold**
    - **Starting**
    - **Uninstalling**
- It must have an Internet connection, either directly or through other computers ('proxy' feature).
- It must have an Internet connection, either directly or through other computers ('proxy' feature).

To configure a search task, go to the **Installation** window and click the **Search** menu.



This window displays a list of all previous searches. Click any of them to edit it. Additionally, click **New search** to access a new window to configure searches.



You'll need to enter the following information when configuring a search task:

- Task name (a maximum of 50 characters).
  - You cannot give two tasks the same name for the same customer.
  - You cannot use the following characters: <, >, “, ‘, &
- Computer from which to launch the search task. This computer must be selected from the list of protected computers.

Search types

Finally, you must select the scope of the search. Choose from the following options:

- The **subnet of the computer** that performs the search (the default option).

This option uses the subnet mask of the TCP/IP configuration of the computer that performs the search to limit its scope.

Subnet-based searches show all the devices found on the network, not only Windows computers.

- One or several **IP address ranges (IPv4)**.

If ranges are entered that have IP addresses in common, the relevant computers will be found only once.

Range-based searches show all the devices found on the network, not only Windows computers

- One or several **domains**.

Enumeration of the computers that belong to an Adaptive Defense 360 domain requires that the Windows Computer Browser service be running on the computer that performs the search. On each network segment, a Master Browser is elected from the group of computers located on the segment that are running the browser service.

There are two possible scenarios depending on whether the network is a workgroup or a domain:

- Network with Primary Domain Controller (PDC / BDC) or Active Directory (AD) installed

The PDC or AD server takes on the Domain Master Browser role and obtains from each Master Browser a full list of the computers found on each network segment. The administrator will see a single list in the Adaptive Defense 360 console with all the computers on the network.

- Network without Primary Domain Controller (PDC / BDC) or Active Directory (AD) installed

As there is no computer that acts as the Domain Master Browser, the Master Browser in each network segment will only contain the list of computers that belong to that segment. The Adaptive Defense 360 computer performing the search will only obtain the list of computers in its segment.

To obtain a complete result, it will be necessary to configure individual searches from the Adaptive Defense 360 ***console for each network segment.***

Search task statuses

- **On hold**: The computer that performs the search downloads the search command from the server. The server becomes aware of the action and changes the task status.

- **Starting**:
    - The computer that performs the search calculates the priority of the new task in relation to other tasks that might also be waiting to be run. The new task waits its turn according to the priority queue.
    - The computer that performs the search checks to see if it fulfills the requirements to run the task.
    - A message is sent to the server indicating that the task has started to run.
- **In progress**
    - The computer that performs the search starts scanning the network to find unprotected computers.

Search task action sequence

The action sequence will vary depending on the search type:

- By IP address (IP address and subnet ranges)
    - The system pings each IP address using the ICMP protocol
    - It waits for a response to the pings
    - It tries to resolve the names of the IP addresses that respond
- By domain
    - A list is made of all the computers that belong to the domain
    - The system checks to see if the computers on the list have the agent installed
    - A message is sent to the agent
    - The system waits for a response

Search task results

The computer that performs the search will send the server a list of all the unprotected computers on the network, even though the list may not have changed from the one previously sent from the same computer.

This list contains:

- Computers without an agent installed.
- Computers integrated into another Panda account: It is not possible to communicate with agents installed on computers belonging to other Panda accounts, therefore no response will be received and the system will interpret that the computers are unprotected.

The wait time for a response will be 3 sec x number of computers that responded to the ICMP ping + 30 sec (safety margin).

Blacklisted computers are not considered unprotected and will NOT appear as the result of a search task.

Details of unprotected computers

The following information is obtained about each unprotected computer found:

- IP address (always).
- Computer name, if the computer that performed the search could resolve it.

9.2. Protection deployment overview

The installation process comprises a series of steps that will vary depending on the status of the network at the time of deploying the protection 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:

1- Find out the number and characteristics of the unprotected devices on the network

Use the option to **search for unprotected computers** to find the unprotected Windows computers on the network.

2- Find out if you have sufficient licenses to deploy the protection

Compare the search results (don't forget to add all the devices with operating systems not supported by the search tool: Android, Mac OS X and Linux) to the number of free licenses. Take into account the peculiarities described in Chapter 6 Licenses.

3- Select the installation procedure

Depending on the total number of Windows computers, you might want to install the protection with the centralized distribution tool, a third-party tool, or **generate a download URL** and send it by email for manual installation.

4- Check whether the computers have another antivirus installed

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

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

Trial versions

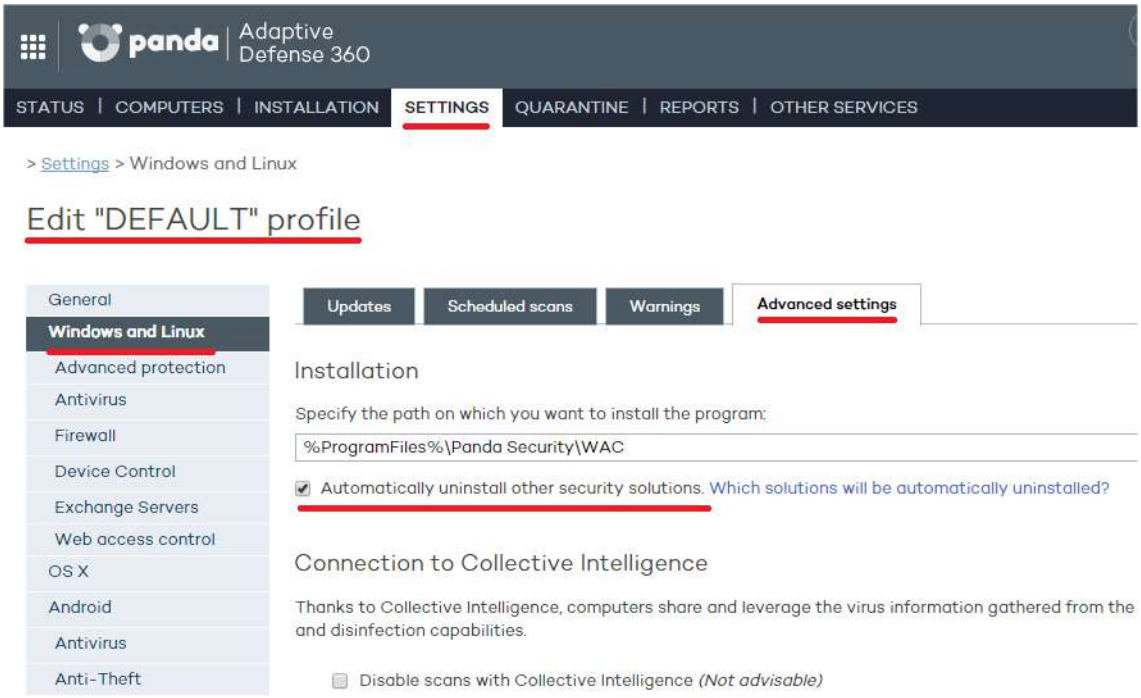
By default, trial versions of Adaptive Defense 360 can be installed on computers with a solution from another vendor. This allows users to evaluate Adaptive Defense 360 and see for themselves how it detects advanced threats that go undetected by the traditional antivirus installed.

Full versions

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

Refer to Annex 3 for a list of the antivirus solutions that Adaptive Defense 360 uninstalls automatically. If the solution you have to uninstall is not on the list, you'll have to uninstall it manually.

This behavior can be changed both for trial and full versions. Go to **Settings** / **(Click the profile to edit) / Windows and Linux / Advanced settings.**



Panda Security antivirus solutions

If the computer is already protected with **Endpoint Protection, Endpoint Protection Plus** or **Panda Fusion**, the protection will update without having to uninstall or reinstall it.

If the computer is already protected with **Admin Secure** (**Panda Security for Business**), the behavior is the same as with a competitor antivirus.

5- Check if the requirements for the target platform are met

The minimum requirements for each operating system are described later in this chapter, in the sections dealing with each platform.

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

All the protection services provided by Adaptive Defense 360, with the exception of the firewall and the intrusion detection system (IDS) on Windows computers, start working without having to restart the computers. If the firewall is required, it will be necessary to configure the network computers to restart.

It is possible that a restart of the client is required or a small micro cutting in connection with some earlier versions of Citrix occur.

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

Installing Adaptive Defense 360 causes a micro-interruption (less than 4 seconds) in the connections established by the programs running on the computer. All applications that do not incorporate security mechanisms to detect connection interruptions will need a restart. If a restart is not possible and there are applications that may not work properly after the micro-interruption, it is advisable to install the Adaptive Defense 360 agent outside office hours.

9.3. Installing the protection on Windows computers

You can install Adaptive Defense 360 on Windows computers manually by downloading the installer from the console or emailing the download URL to end users, or automatically using the centralized distribution tool (as explained in Annex I: Centralized installation tools).

9.3.1. Internet access requirements

For Adaptive Defense 360 to work correctly, the computers where the protection agent is to be installed must be able to access a number of URLs.

If you have a firewall, a proxy server or other network restrictions, allow access to the URLs below for Adaptive Defense 360 to work correctly.

During the installation process, the product automatically classifies the applications most frequently used by the user on the computer, without having to wait for each application to be run. This aims at speeding up the classification process and preventing applications from being blocked at system startup if it is not possible to connect to the Internet. For this reason, it is very important to make sure that all computers meet the Internet access requirements before installing Adaptive Defense 360*.*

Web administration console

- https://www.pandacloudsecurity.com/
- https://managedprotection.pandasecurity.com/

Updates and upgrades

- http://acs.pandasoftware.com/member/installers/
- http://acs.pandasoftware.com/member/uninstallers/
- http://enterprise.updates.pandasoftware.com/pcop/pavsig/
- http://enterprise.updates.pandasoftware.com/pcop/nano
- http://enterprise.updates.pandasoftware.com/pcop/sigfiles/sigs
- http://enterprise.updates.pandasoftware.com/pcop/files
- http://acs.pandasoftware.com/free/
- http://acs.pandasoftware.com/sigfiles
- http://acs.pandasoftware.com/pcop/uacat
- http://enterprise.updates.pandasoftware.com/pcop/uacat/
- http://enterprise.updates.pandasoftware.com/updates_ent/
- https://pcopsupport.pandasecurity.com

Quarantine

- http://hercules.pandasoftware.com/getqesi.aspx
- http://hercules.pandasoftware.com/getqesd.aspx

Communication with the server

- https://mp-agents-inst.pandasecurity.com
- http://mp-agents-inst.pandasecurity.com/Agents/Service.svc
- https://mp-agents-inst.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-sync.pandasecurity.com/Agents/Service.svc
- https://mp-agents-sync.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-async.pandasecurity.com/Agents/Service.svc
- https://agentscomp.pandasecurity.com/AgentsSecure/Service.svc
- https://pac100pacprodpcop.table.core.windows.net
- https://storage.accesscontrol.pandasecurity.com
- https://prws.pandasecurity.com
- https://rpuws.pandasecurity.com/frws

Communication with the Collective Intelligence servers

- http://cache.pandasoftware.com
- http://cache2.pandasecurity.com
- https://rpkws.pandasecurity.com/kdws/files
- http://proinfo.pandasoftware.com (OS X systems)
- http://proinfo.pandasoftware.com/connectiontest.html (If access to this URL fails, the product will try to reach http://www.iana.org)

- https://ims.pandasecurity.com/ProySRF
- http://statistics.pandasoftware.com

Inbound and outbound traffic (Anti-spam and URL Filtering)

- http://*.pand.ctmail.com
- http://download.ctmail.com

Communications with Cloud Cleaner

- http://beaglecommunity.appspot.com
- http://waspproxy.googlemail.com
- http://*.pandasecurity.com

For correct communication among the Adaptive Defense 360 communications agents, enable ports TCP 18226 and UDP 21226 (company intranet).

In peripheral devices, such as advanced firewalls that inspect and block communications based on their content type it is recommended to add additional rules that allow free traffic to the URLs mentioned

9.3.2. Hardware and software requirements

- Processor: Pentium 300 MHz or equivalent
- RAM: 256 MB
- Space for installation: 650 MB
- Browser: Internet Explorer 6.0 or later
- On computers with an operating system prior to Windows XP SP2 or Windows 2003 Server SP1:
  - Windows Installer 2.0 (Windows Installer 3.0 is recommended for remote uninstall)
  - Disable the Windows firewall or enable the **File and printer sharing exception (Start**, **Settings**, **Control Panel**, **Network connections**, **Local area connections**, (right button) **Properties, General**).
  - Disable **Use simple file sharing** (on Windows XP, **Tools**, **Folder Options**, **View**, **Use simple file sharing**).
- Workstations:
  - Operating systems: Windows 10, Windows 8.1, Windows 8, Windows 7 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows XP (32-bit and 64-bit) and Windows 2000 Professional.
  - RAM: For the antivirus protection: 64 MB, for the firewall: 128 MB.
- Servers
  - Operating systems: Windows 2000 Server, Windows Home Server, Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit)*, Windows Server 2008 R2*, Windows Server 2012 and Windows Server 2012 R2.
  - RAM: 256 MB.

Windows Server Core servers are not directly compatible with the product. However installing the graphics system will allow Adaptive Defense 360 *run smoothly.*

- Other supported applications:
  - VMWare ESX 3.x, 4.x, 5.x
  - VMWare Workstation 6.0, 6.5, 7.x, 8.x and 9.x
  - Virtual PC 6.x
  - Microsoft Hyper-V Server 2008 R2 and 2012 3.0
  - Citrix XenDesktop 5.x, XenClient 4.x, XenServer and XenApp 5.x and 6.x

To deploy the protection with the distribution tool to computers with Windows Server 2008 R2, select the option "Enable remote management of this server from other computers". This option, which is disabled by default, must be enabled and allowed by the firewall. To enable it, follow the instructions specified in the following Microsoft article: ***http://support.microsoft.com/kb/976839***.

9.4. Installing the protection on Windows computers with Microsoft Exchange

9.4.1. Internet access requirements

The Internet access requirements of the agent for Windows with Microsoft Exchange are the same as those for the agent for Windows.

9.4.2. Hardware and software requirements

The hardware requirements to install the Exchange Server protection are those of Exchange Server:

- Exchange 2003:
  http://technet.microsoft.com/es-es/library/cc164322(v=exchg.65).aspx
- Exchange 2007:
  http://technet.microsoft.com/es-es/library/aa996719(v=exchg.80).aspx
- Exchange 2010:
  http://technet.microsoft.com/es-es/library/aa996719(v=exchg.141).aspx
- Exchange 2013
  http://technet.microsoft.com/es-es/library/aa996719(v=exchg.150).aspx

The Microsoft Exchange Server versions supported by Adaptive Defense 360 are:

- Microsoft Exchange Server 2003 Standard (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2003 Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2003 included in Windows SBS 2003
- Microsoft Exchange Server 2007 Standard (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 Enterprise (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 included in Windows SBS 2008
- Microsoft Exchange Server 2010 Standard (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 included in Windows SBS 2011
- Microsoft Exchange Server 2013 Standard
- Microsoft Exchange Server 2013 Enterprise

Roles in which the Exchange Server protection is installed (in Exchange 2007 and Exchange 2010):

- Mailbox
- Hub Transport
- Edge Transport

Roles in which the Exchange Server protection is installed (in Exchange 2013):

- Mailbox

Operating systems supported:

- Exchange 2003: Windows Server 2003 (32-bit) SP1+ and Windows Server 2003 R2 (32-bit)
- Exchange 2007: Windows Server 2003 (64-bit) SP1+, Windows Server 2003 R2 (64-bit), Windows 2008 (64-bit) and Windows 2008 R2
- Exchange 2010: Windows 2008 (64-bit) and Windows 2008 R2
- Exchange 2013: Windows 2012

9.5. Installing the protection on Linux computers

You can install Adaptive Defense 360 on Linux devices manually by downloading the installer from the console, or emailing the download URL to end users.

9.5.1. Internet access requirements

The Linux agent must be able to access the following URLs:

- http://pcoplinux.updates.pandasecurity.com/updates/nanoupdate.phtml
- http://pcoplinux.downloads.pandasecurity.com/nano/pavsignano/nano_1/

9.5.2. Hardware and software requirements

Supported distributions

- Ubuntu (32-bit and 64-bit), version 12 or later
- Red Hat Enterprise (64-bit), version 6.0 or later
- Debian Squeeze (32-bit and 64-bit)
- OpenSuse (32-bit and 64-bit), version 12 or later
- Suse Enterprise Server (64-bit), version 11 SP2 or later
- CentOS 6.x or later

Prerequisites

The system must meet the following requirements for the product to work correctly:

- **The "lsb_release" utility must be installed (on RedHat and Debian).**
    - On Debian, download and install the following package:

      lsb-release_3.2-23.2squeeze1_all.deb
    - On RedHat, download and install the following package:

      redhat-lsb.i686
- **PavSL protection dependencies (all distributions)**
  The PavSL protection requires the installation of the following libraries to work properly:
    - libsoup-2.4.so.1 (HTTP client/server library for GNOME)
    - libgthread-2.0
    - libmcrypt.so.4 (MCrypt - encryption functions)
    - libz.so.1 (zlib compression and decompression library)

      Make sure the **/opt/PCOPAgent/PCOPScheduler/pavsl-bin/** directory contains all the PavSL protection dependencies
- **The AT/CRON services must be properly installed and enabled (in all distributions)**

  Make sure the AT and CRON services are properly installed and enabled in the system services.
- **The whiptail command must be available** to run the proxy configuration script.

9.6. Installing the protection on Mac OS X computers

You can install Adaptive Defense 360 on Mac OS X devices manually by downloading the installer from the console, or emailing the download URL to end users.

9.6.1. Internet access requirements

The Mac OS X agent must be able to access the following URLs:

- mp-agents-inst.pandasecurity.com
- mp-agents-sync.pandasecurity.com
- mp-agents-async.pandasecurity.com
- proinfo.pandasoftware.com
- http://www.netupdate2.intego.com
- https://www.netupdate2.intego.com
- http://www.integodownload.com
- http://www.intego.com

9.6.2. Hardware and software requirements

Supported operating systems

Adaptive Defense 360 supports the following OS X operating systems:

- Mac OS X 10.6 Snow leopard (Intel Core 2 Duo processor or later)
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite

Hardware

- Processor: Intel® Core 2 Duo
- Hard Disk: 1.5 GB free space
- Browser: Internet Explorer 5.5 or later, Firefox and Chrome

9.7. Installing the protection on Android devices

You can install Adaptive Defense 360 on Android devices manually by downloading the installer from the console or emailing the download URL to end users.

The process to install Adaptive Defense 360 on Android devices has the peculiarity that, once you have installed the protection, it is necessary to take the additional step of adding the Android device to a computer group in the Adaptive Defense 360 Web console**.**

This way, the Web console will be aware of the existence of the device and will show it on the list of protected computers.

Installing the protection by sending the download URL

In this case, the protection is installed from the Android device through an installation URL sent by email.

In the Adaptive Defense 360 Web console, select the group to which you want to add the device (the Default group is selected by default). Then, click **Send by email**.

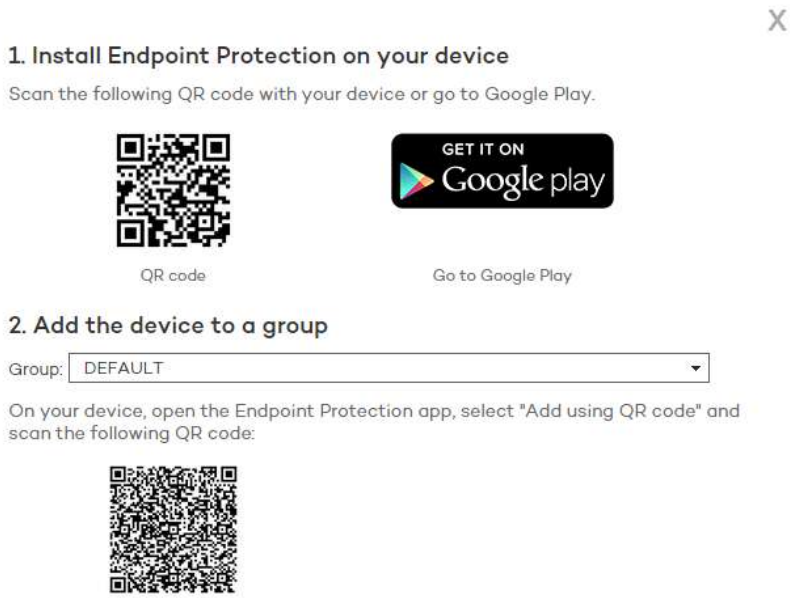
End users will automatically receive an email message with two URLs. The first one is the installation URL. Clicking it takes the user to the Adaptive Defense 360 page in Google Play to install the protection.

Once the protection has been installed, it will be necessary to open Adaptive Defense 360 from the device and click the second URL included in the email.

Installing the protection from the Web console

To install the protection from the console, the user must access the Adaptive Defense 360 console from their Android device and click the Android icon in the **Installation** menu. There, they can choose between installing the protection using a QR code or from the Google Play Store.

> *To read the QR code it is necessary to have a QR scanner such as Barcode Scanner installed on the device.*



After the Adaptive Defense 360 agent has been installed on the Android device, this will have to be linked to a specific group. To do that, it will be necessary to select in the console the relevant group using the **Group** drop-down menu, and tap **Add this device to the group** on the Android device to scan the second QR code displayed.

9.7.1. Internet access requirements

Communication with the server

- https://mp-agents-inst.pandasecurity.com
- http://mp-agents-inst.pandasecurity.com/Agents/Service.svc
- https://mp-agents-inst.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-sync.pandasecurity.com/Agents/Service.svc
- https://mp-agents-sync.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-async.pandasecurity.com/Agents/Service.svc
- https://agentscomp.pandasecurity.com/AgentsSecure/Service.svc
- https://pac100pacprodpcop.table.core.windows.net
- https://storage.accesscontrol.pandasecurity.com

- https://prws.pandasecurity.com
- https://rpuws.pandasecurity.com/frws
- https://managedprotection.pandasecurity.com/PartnerConsole/cv13/Customers/Administration/Install/Installer/GetAgent.aspx

DMP integration

- https://dmp.devicesmc.pandasecurity.com

Snap the Thief

- https://storage.accesscontrol.pandasecurity.com

Updates and upgrades

- http://acs.pandasoftware.com/member/installers/
- http://acs.pandasoftware.com/member/uninstallers/
- http://enterprise.updates.pandasoftware.com/pcop/pavsig/
- http://enterprise.updates.pandasoftware.com/pcop/nano
- http://enterprise.updates.pandasoftware.com/pcop/sigfiles/sigs
- http://acs.pandasoftware.com/free/
- http://acs.pandasoftware.com/sigfiles
- http://acs.pandasoftware.com/pcop/uacat
- http://enterprise.updates.pandasoftware.com/pcop/uacat/
- http://enterprise.updates.pandasoftware.com/updates_ent/
- https://pcopsupport.pandasecurity.com

Collective Intelligence

- https://rpuws.pandasecurity.com
- https://rpkws.pandasecurity.com/kdws/sigs
- https://prws.pandasecurity.com
- http://iext.pandasecurity.com/ProyIEXT/ServletIExt

Push notifications

- https://developers.google.com/cloud-messaging/http

For push notifications to work properly it will be necessary to open ports 5228, 5229 and 5230 to all IP addresses contained in the IP blocks listed in Google's ASN of 15169.

9.7.2. Hardware and software requirements

Adaptive Defense 360 is compatible with all Android devices with version 2.3 *Gingerbread* or later. The solution requires 15 MB of free space in the device's internal memory to work properly.

9.8. Uninstalling the protection

Adaptive Defense 360 provides three tools to uninstall the protection. The following table illustrates the availability of the different uninstall methods on each operating system.

Tool	Platform			
	Windows	Linux	Mac OS X	Android
Local uninstall	YES	YES	YES	YES
Uninstall using the centralized distribution tool	YES	No	No	No
Uninstall from the administration console	YES	No	No	No

9.8.1. Local uninstall

Adaptive Defense 360 can be uninstalled manually from the Windows Control Panel, provided the administrator has not **set an uninstall password** when configuring the security profile for the computer in question. If they have, you will need authorization or the necessary credentials to uninstall the protection.

Refer to chapter 13 Windows protection profiles for more information about the administrator password

On Windows 8 and later:

Control Panel > *Programs* > *Uninstall a program*.

Alternatively, type 'uninstall a program' at the Windows Start Screen.

On Windows Vista, Windows 7, Windows Server 2003, 2008 and 2012:

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

On Windows XP:

Control Panel > *Add or remove programs.*

On OS X:

Finder > *Applications* > Drag the icon of the application that you want to uninstall to the recycle bin.

On Android devices:

Go to *Settings*.

Security > Device administrators.

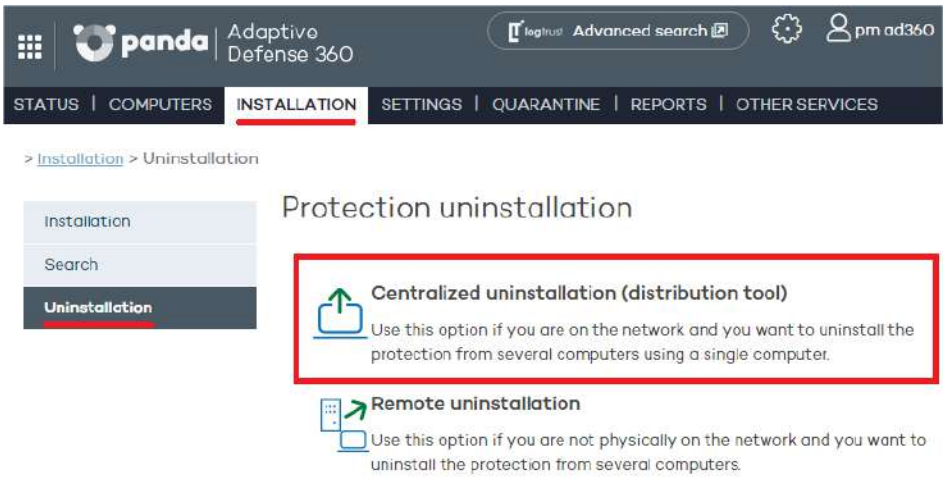
Clear the Adaptive Defense 360 checkbox. Then, tap *Disable* > *OK*.

Back in the Settings window, tap *Apps*. Click Adaptive Defense 360 > *Uninstall* > *OK*.

9.8.2. Uninstalling the protection using the centralized distribution tool

This option is only available for Windows computers.

In the Web console main window, click **Installation**. Then, click **Uninstallation** in the menu on the left. Select **Remote uninstallation**. You will be taken to the **Centralized uninstallation** window, where you will be able to download the centralized distribution tool**.**



*Refer to Annex 1 **Centralized installation tools** for more information*

9.8.3. Uninstalling the protection from the administration console

This option is only available for Windows computers

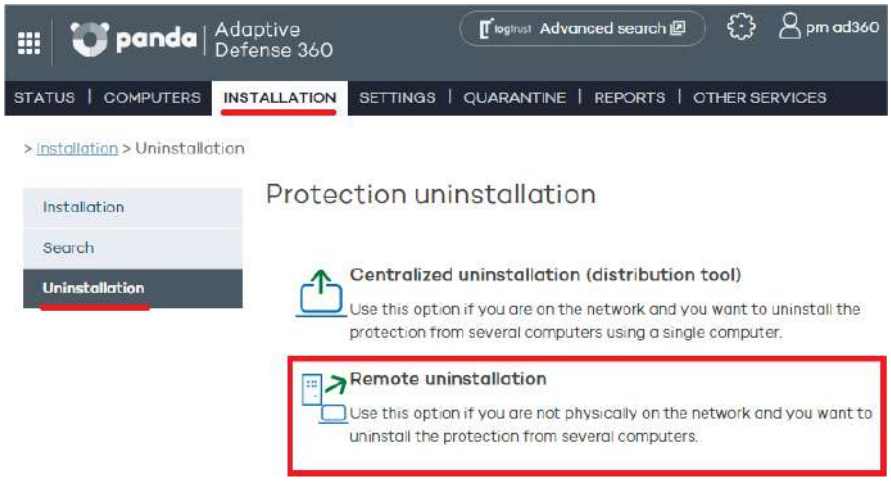
The remote uninstall feature allows administrators to uninstall the protection simply and effectively from the Web console, without having to physically go to each computer. This uninstall type therefore saves on costs and legwork.

The first step is to create and configure an uninstall task. To do that, the administrator must select the group and the computers in the group that will be affected by the task. After the process is complete, they will be able to check the results of the uninstall task on each computer.

Creating a remote uninstall task

1- In the main console window, click **Installation** and then **Uninstallation** in the menu on the left.

2- Select **Remote uninstallation**. This will take you to the **Remote uninstallation** window.

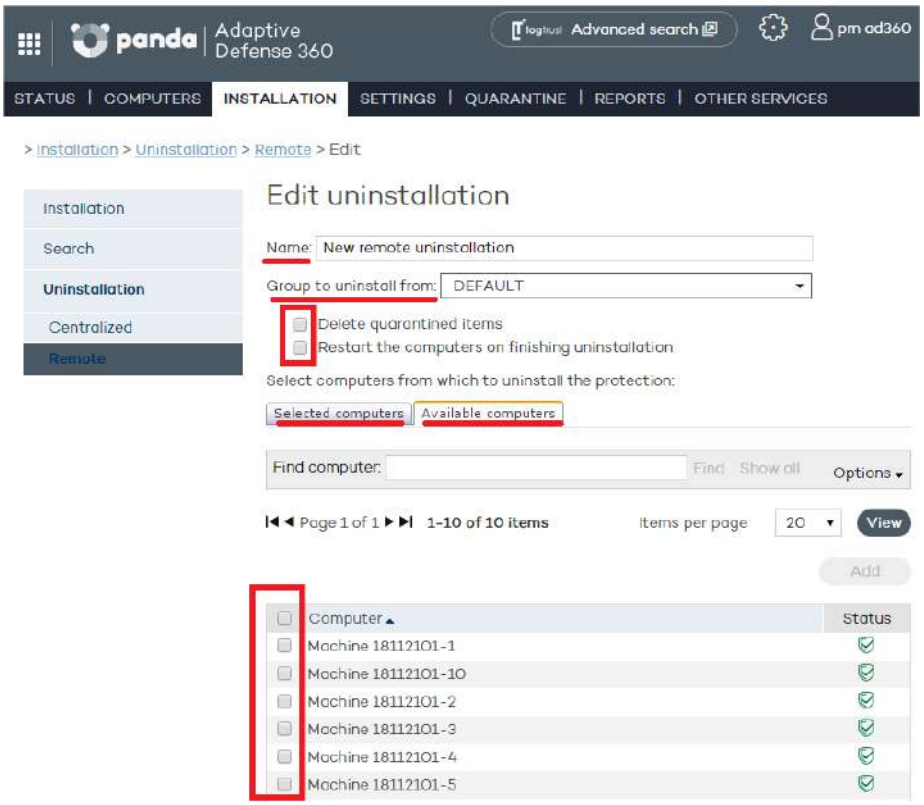


To configure uninstall tasks, the user that accesses the administration console must have total control or administrator permissions. For more information, refer to Chapter 8 Users.

3- To configure a new uninstall task, click **New uninstallation**. Then, in the **Edit uninstallation** window, name the task and select the group that contains the computers whose protection will be uninstalled. The groups displayed will be those on which you have permissions.

4- If the selected group has a configuration profile for which an uninstall password has been set, enter it in the **Password** field.

5- Select the computers from the computer list displayed on the **Available computers** tab, and click **Add**. After you select them, they will appear on the **Selected computers** tab.



Viewing remote uninstall tasks and their results

Uninstall tasks are listed in the **Remote uninstallation** window, from where you can also remove them by using the **Delete** button.

Information is organized into the following columns:

- **Name**: Shows the name given to the uninstall task when created.
- **Status**: The status icons indicate the status of the uninstall task.
- **Uninstalled protections**: Indicates the number of protections uninstalled.
- **Date created**: Date the uninstall task was created. **Created by**: User that created the task.

You will be able to create, view, or remove uninstall tasks depending on your permissions.

To see the results of any of the uninstall tasks, click on its name and you will go to the **Results** window.

Remote uninstall results

Click the name of an uninstall task in the **Remote uninstallation** window to see its results.

In addition to the name and the start and end date of the task, this window also shows information about the affected computers and their status.

If the status of the uninstall task is **On hold**, the start date will display a hyphen (-). The same applies to the end date if the task has not finished.

If you want to see the uninstall task settings, use the **View settings** link.

Incompatibility between searches for unprotected computers and remote uninstall tasks

If a computer is involved in an uninstall task (*On hold*, *Starting*, or *In progress*), **it is not possible** to create another uninstall task for it, or select it as the computer from which to launch searches for unprotected computers.

Likewise, if a computer is running a task for discovering unprotected computers, **it is not possible** to create an uninstall task for it.

10. Updating the protection

10.1. Introduction

Adaptive Defense 360 is a cloud-based managed service that doesn't require administrators to update servers or the back-end infrastructure that supports the protection service. However, it is necessary to update the agents installed on the customer's computers.

The components installed on users' computers are the following:

- Protection engine
- Signature file

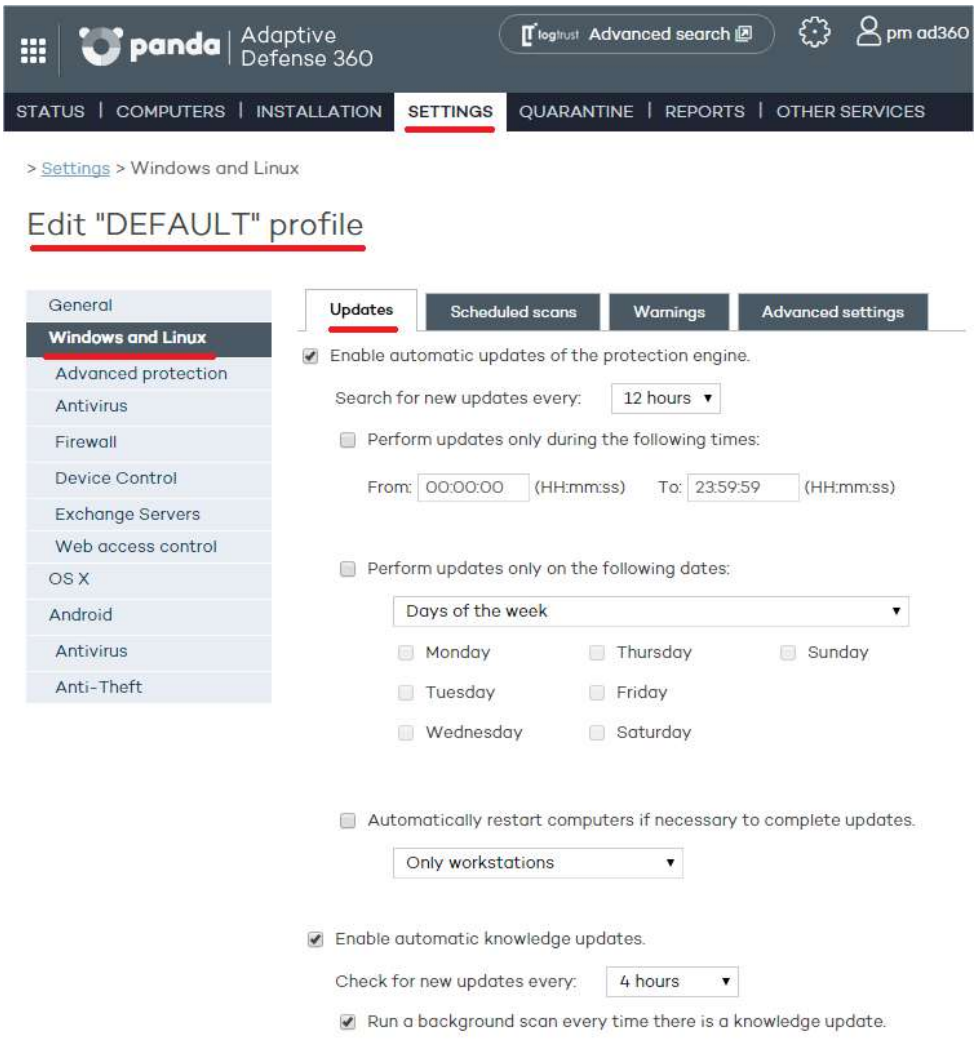
The update procedure and options will vary depending on the platform to update:

Module	Platform			
	Windows	**Linux**	**Mac OS X**	**Android**
Protection	Automatic and configurable	Local	Automatic	Automatic
Signature file	Automatic and configurable	Automatic	Automatic	Automatic

- Automatic and configurable: Updates can be configured through the console and deployment is remote.
- Automatic: Updates cannot be configured but deployment is remote.
- Local: Updates are performed manually or using third-party centralized distribution tools.

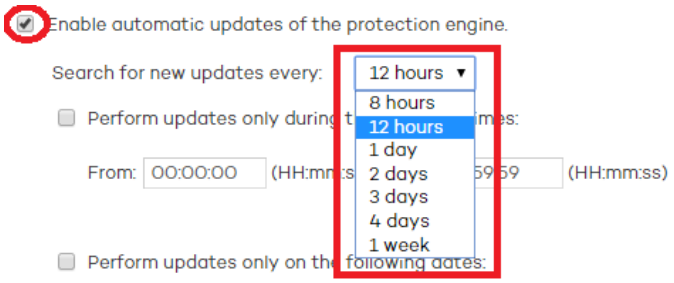
10.2. Updating the protection on Windows systems

The update settings are part of the configuration profile assigned to a computer. Therefore, to access the configuration settings, go to **the Settings** window and select the profile to edit. Once you have selected it, click **Windows and Linux** in the menu on the left, and click the **Updates tab.**



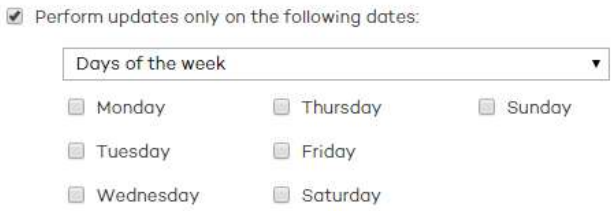
10.2.1. Updating the protection

- First, select the option to enable updates.
- Use the drop-down menu to select the frequency to search for updates.

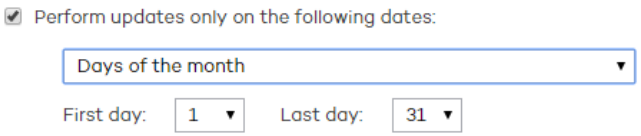


- You can also select a date and time for the automatic updates to take place. You can select:

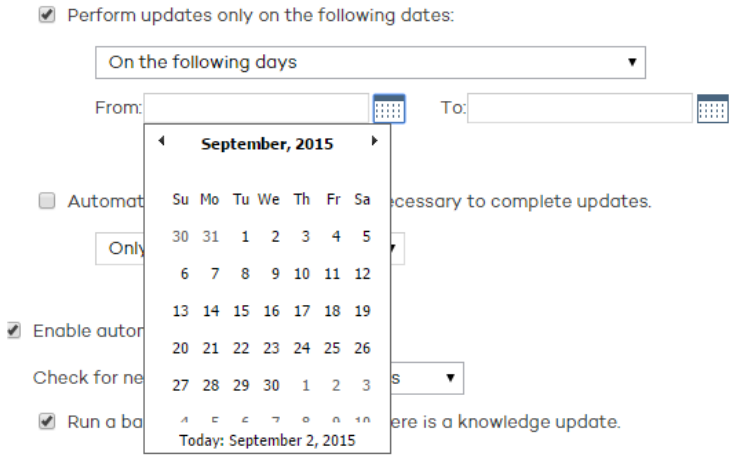
- The days of the week for the update to take place.



- The days of every month on which the update must take place.



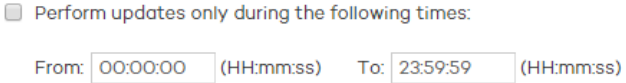
- A date range for the update to take place.



- Indicate which computer families must be automatically restarted after an update.

> ***An update will not be finished until the relevant computer has restarted. If the automatic restart option is not selected, and the computer is not manually restarted after 15 days, the agent will start showing messages to the user to restart the computer.***

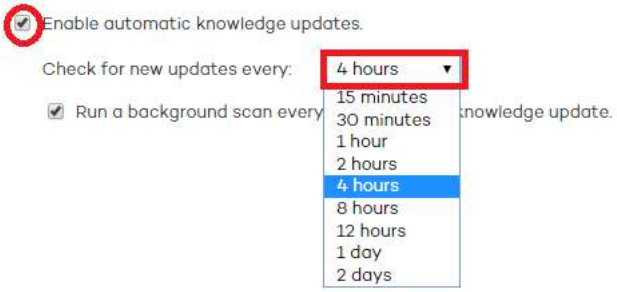
- Additionally, you can set the time interval at which to perform the update.



10.2.2. Updating the signature file

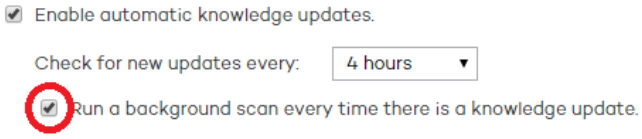
- Select the option to enable the automatic updates feature.

- Use the drop-down menu to select the frequency to search for updates.



- Select if you want a background scan to be run every time the signature file is updated.

> ⚠ ***It is advisable to clear this option in virtual environments since, as there are multiple computers concurrently running on the same physical hardware, updating the signature file simultaneously on all of them may lead to performance problems***



10.2.3. Peer-to-Peer or rumor functionality

The Peer-to-Peer (or 'rumor') functionality reduces Internet bandwidth usage, as those computers that have already updated a file from the Internet then share the update with the other connected computers. This prevents saturating Internet connections.

The P2P feature is very useful for deploying Adaptive Defense 360 and downloading the installation program. When one of the computers has downloaded the Adaptive Defense 360 installation program from the Internet, the others are informed by their communications agents.

Then, instead of accessing the Internet, they get the installation program directly from the computer that downloaded it and install the protection.

This functionality is also very useful when updating the protection engine and the signature files, and is implemented in the two local processes that need to download files from the Internet: **WalUpd** and **WalUpg**.

This functionality is enabled in the configuration files **walupd.ini** and **walupg.ini**, located in the **InstallDir** folder in the Adaptive Defense 360 **installation directory**:

```
WALUPD.ini

[GENERAL]

UPDATE_FROM_LOCAL_NETWORK=1

WALUPG.ini

[GENERAL]

UPGRADE_FROM_LOCAL_NETWORK=1
```

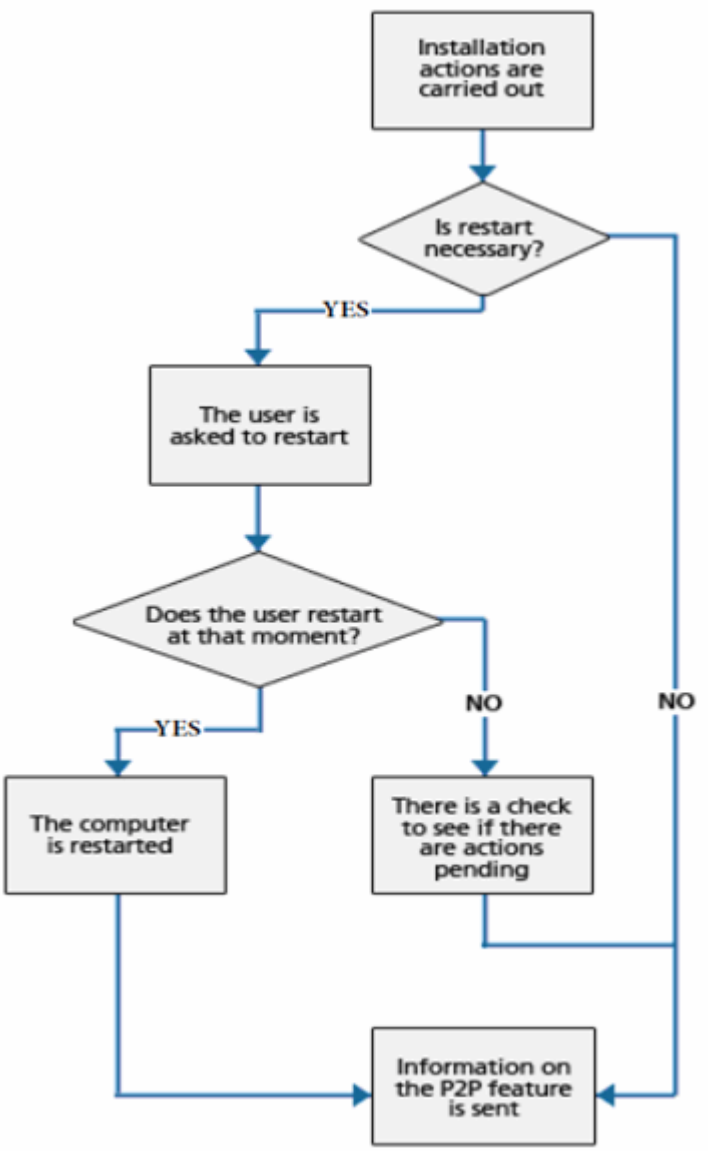
The P2P functionality works independently in each of these local processes. It may be enabled in one of them but not in the other.

The P2P functionality works as follows:

As soon as a computer has updated its signature files or any protection (or the agent itself), it sends a broadcast message with the information about the files that it has to the other computers on the network.

As for the information for the **WALUpg** process, if a restart is necessary after installing/upgrading the protection, and the user chooses to restart later, the information transmitted via the P2P functionality will be sent immediately instead of waiting for the restart.

This process is illustrated in the following diagram:



The computers save the information they receive, and use it when required.

If a computer needs a file, it will first check whether another computer on the network has it before downloading it from the Internet. If so, it will request the file from the other computer. The file will be received asynchronously and there is a maximum time that must elapse before retrying.

Once the computer that requested a file receives it, it will continue with the update or upgrade process.

10.3. Updating the protection on Linux systems

10.3.1. Updating the protection

In the case of Linux computers it is not possible to perform remote automatic updates. Therefore, when a new version of the protection is made available, it has to be manually installed on computers.

Seven days after the release of a version more recent than the protection installed on a Linux computer, this will appear as "out-of-date" in the **Status** window.

10.3.2. Updating the signature file

In the case of Linux computers, it is not possible to configure the frequency of the automatic updates of the signature file. These will always take place every 4 hours.

10.4. Updating the protection on Mac OS X systems

10.4.1. Updating the protection

The protection of OS X computers is updated automatically, even though you can disable this feature from the administration console.

72 hours after the release of a version more recent than the protection installed on a Mac OS X computer, this will appear as "out-of-date" in the **Status** window.

10.4.2. Updating the signature file

In the case of OS X computers, it is not possible to configure the frequency of the automatic updates of the signature file. It is updated every hour.

48 hours after the release of a version more recent than the file installed on a Mac OS X computer, this will appear as "out-of-date" in the **Status** window.

10.5. Updating the protection on Android systems

10.5.1. Updating the protection

Android protection updates are published on Google Play. The agent will display a notification for users to accept the update on their devices.

10.5.2. Updating the signature file

Signature files can be updated automatically. Additionally, you can choose to update the protection exclusively through Wi-Fi networks.

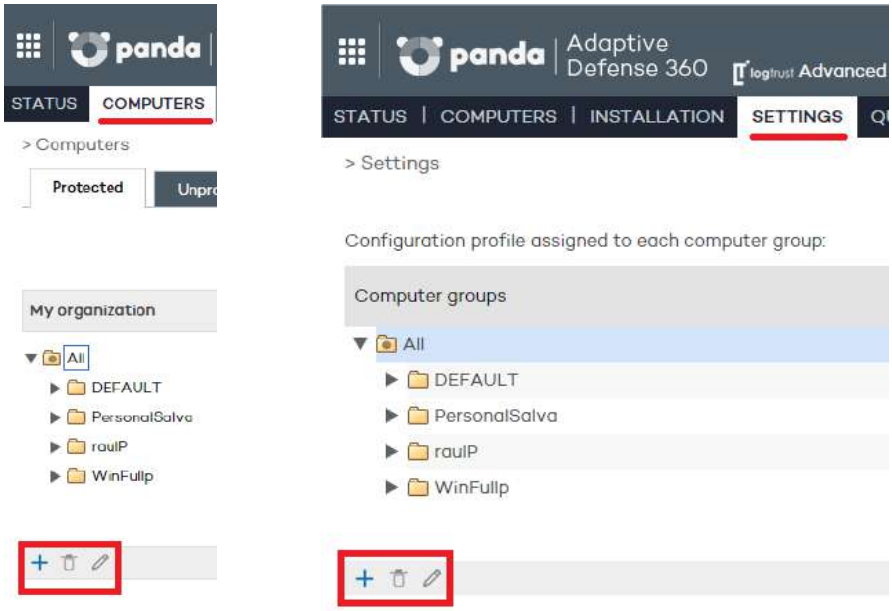
11. Groups

11.1. Introduction

Adaptive Defense 360 allows you to organize computers into groups with common protection and security characteristics.

This way, in networks with more than 10 PCs it is usual to create groups with those computers that have similar security requirements, for example all the PCs in the same department, computers managed by users within the same category or with the same IT knowledge, etc.

Groups are created and managed through the **Computers** window, or through the **Settings** window by means of the three icons located under the tree group**.**



Assigning computers to groups

In Adaptive Defense 360, a computer can only belong to one group at a time. Computers are assigned to groups in different ways:

- When installing the agent on a computer, as indicated in Chapter 9 Installing the protection
- By manually moving a computer to a group in the administration console. Refer to section **Manually moving computers to a group** in this chapter.
- Automatically, when a computer added to an automatic-type group is moved to the relevant subgroup. Refer to sections **Creating automatic groups arranged by IP address** and **Creating automatic groups based on Active Directory** in this chapter to configure rules that allow computers to be automatically assigned to groups.

11.2. Computer tree

The computer tree is a resource accessible from the **Computers** and **Settings** windows, and which allows you to see at a glance the group and subgroup hierarchy of the organization.

The parent node is at the top of the tree so that every group and subgroup created by the administrator hangs from it. Adaptive Defense 360 is delivered with a predetermined DEFAULT group. This group contains all of the devices with an agent installed.

The parent node is called **All** and is represented by the icon.

The parent node cannot be edited or deleted. Nor is it possible to assign a protection profile to it

Every node in the group tree displays an arrow next to it that allows you to expand it should it contain subgroups.

11.3. Group types

Manual groups

They are identified in the console with the icon.

These are static groups: The computers they contain will always belong to the same group unless they are manually moved by the administrator using the **Move** option. Refer to section **Moving computers manually**.

Automatic groups arranged by IP address

They are identified in the console with the icon.

This type of group comprises subgroups, and each subgroup contains rules configured by the administrator describing the IP address ranges of the computers that belong to it. When a computer is moved to an **automatic group arranged by IP address**, Adaptive Defense 360 checks the computer's IP address and moves the computer automatically to the subgroup whose rules fit in relation to that particular computer.

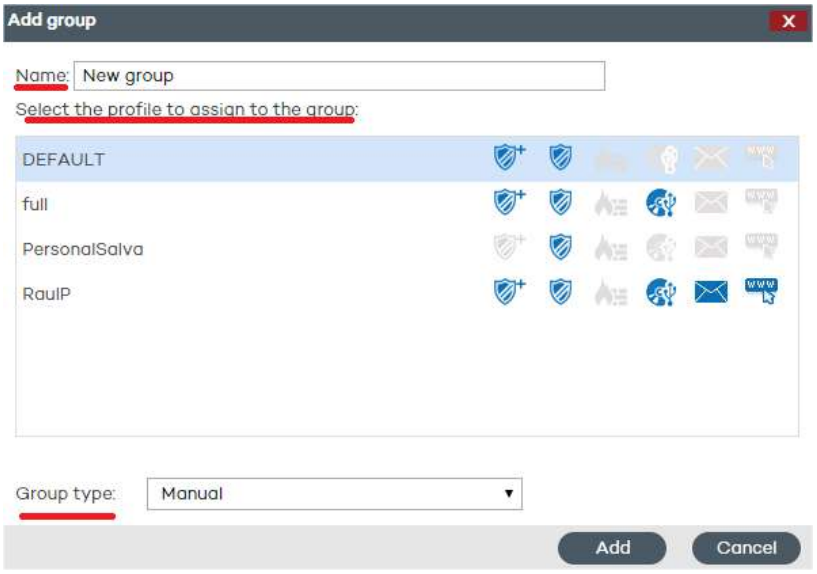
Automatic groups based on Active Directory

They are identified in the console with the icon.

This group type is designed to replicate the organization's Active Directory structure. When a computer is moved to a group based on Active Directory, Adaptive Defense 360 automatically creates in the console the subgroup structure required to move the computer to the group it occupies in Active Directory.

11.4. Creating a manual group

- Click the **Settings** tab.
- To create a subgroup, first select the parent group in the group tree. If you want to create a first-level group, select the **All** parent group.
- Then, click the icon. A window will open with the parameters to configure.



- Enter the name of the group and select the protection profile to assign to it. For more information about protection profiles, refer to chapter 12 Protection profiles.

Remember that you cannot have two groups with the same name at the same level

- Select the **Group type**: **Manual**.

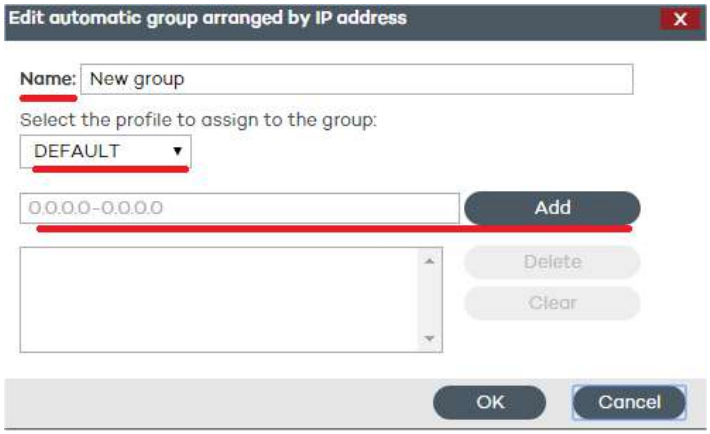
Click **Add**. The new group will be added to the group tree.

11.5. Creating an automatic group arranged by IP address

The group creation process is the same as for manual groups, the only difference being that you must select **Automatic (arranged by IP address)** in **Group type**.

Once you have created a group you will be taken to the edit window. This window lets you configure the automatic rules to apply to the group.

Click the  icon to display the rule creation window.



There, you will have to specify:

- The rule name
- The protection profile to assign to the rule
- The IP address range(s) that the rule will refer to

Once you finish configuring these options, click **OK** to finish creating the rule.

Every rule you create will automatically generate a subgroup in the **automatic group** that you have created in the previous step. Every computer added to an **automatic group arranged by IP address** will be automatically moved to the appropriate subgroup based on its IP address.

11.5.1. Importing rules from a .CSV file

You can configure the rules for an automatic group manually, or import them from a .CSV file. Click **Import** and then **Select** to find the .CSV file on your hard disk.

Format of the .CSV file to import

The .CSV file must have the following characteristics:

Each line must contain one to three data strings separated with tabs, and in the following order:

- **Group path** (from the source of the data to import, excluding the **All** group). For example: \Hall of Justice\Room1
- **IP range**. Two options are possible: IP-IP or IP-mask (this field is optional)
- **Profile**. (This field is optional)

If a profile instead of an IP address range is specified, use a **double tab** to separate the two visible fields (group path and profile):

\Hall of Justice JusticeP

Other examples:

\Hospital\Emergency Room\Ambulance1 10.10.10.10-10.10.10.19

\Hospital\Emergency Room

\Hospital\Emergency Room\Ambulance2 10.10.10.20-10.10.10.29 AmbulanceP

\Hospital\Areilza Clinic 10.10.20.10/22 ClinicProfile

\Hall of Justice\Court of Appeals 10.10.50.10/12 Justice2

If, when importing groups from a .CSV file, the information in one of the lines is incorrect, an error will be displayed indicating the line and string whose format is invalid. If there is an error in at least one of the lines, none of the groups in the .CSV file will be imported.

Once you have successfully imported groups from a .CSV file into an automatic group, it won't be possible to repeat the same operation for the same group.

11.5.2. How automatic groups arranged by IP address work

Computers are added to an automatic group arranged by IP address and automatically moved to the appropriate subgroup at the time of installing the agent on the computer. If then you decide to manually move the computer to another group, it will stay there, regardless of its IP address.

These groups take into account all of the computer's IP addresses (computers with network aliases or multiple physical network interfaces), and select the first match they find.

Groups are searched first by level and then by the order of creation. Groups are navigated in descending order. If no subgroup is found that fits a specific computer, the computer will be moved to the parent group.

11.6. Creating an automatic group based on Active Directory

The group creation process is the same as for manual groups, the only difference being that you must select **Automatic (based on Active Directory)** in **Group type**.

11.6.1. Automatic replication of the Active Directory structure

The process of generating and updating subgroups in an **automatic group based on Active Directory** takes place automatically for every computer that is assigned to that type of group. The action sequence is the following:

- The administrator moves a computer to an **automatic group based on Active Directory manually,** or assigns it to it when installing the protection.
- The Adaptive Defense 360 agent retrieves information from the Active Directory structure that the computer belongs to: Organizational unit, PC name, etc.
- This information is sent to the Adaptive Defense 360 server. On the server, the solution checks to see if the subgroup that corresponds to the organizational unit exists in the console:
    - If it doesn't, it creates it automatically and moves the computer to the newly created subgroup. The Default protection profile is assigned to the computer.
    - It it does, the computer is moved to it.

The subgroup tree that hangs from an **automatic group based on Active Directory** is automatically updated whenever a computer that belongs to it is moved to another Active Directory organizational unit. Adaptive Defense 360 will create the new subgroup if required and will move the computer to it.

No specific configuration is required in Active Directory, in the Adaptive Defense 360 agents installed, or in the administration console. Each agent retrieves the necessary information from the Active Directory structure that the computer belongs to, and sends it automatically to the Adaptive Defense 360 server, which updates the tree displayed in the console.

Changes are sent from the** Adaptive Defense 360 **agent to the server according to the configuration established in the Server connection settings section of the protection profile assigned to the computer. Refer to Chapter 13 for more information.

11.6.2. Manual replication of the Active Directory structure

It may be necessary to manually import the Active Directory structure in the following scenarios:

- Not all computers on the network have an Adaptive Defense 360 agent installed capable of reporting the organizational unit that they belong to. Despite this, the administrator needs to have the entire Active Directory structure replicated in the administration console.
- The administrator wants to have the entire group and subgroup structure from the start without having to start deploying the Adaptive Defense 360 agents.

After you create a group you are taken to the edit window.

Click **Import** to load a previously exported Active Directory structure in CSV format.

The file to import must have the following format:

- It must be a file with a .CSV extension
- Every line in the file must include the group and, optionally, the profile associated with the group. Both values must be tab-separated, for example: "Group Path" tab "Profile Name" [Optional]

Example of a .CSV file:

activedirectory.org ProfileName

activedirectory.org\Domain Controllers ProfileName

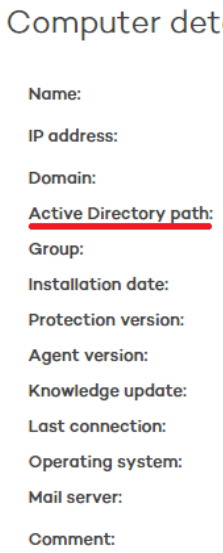
activedirectory.org\Computers ProfileName

activedirectory.org\OrganizationalUnit1 ProfileName
activedirectory.org\OrganizationalUnit1\Department1 ProfileName
activedirectory.org\OrganizationalUnit1\Department2 ProfileName

When importing the file, a link is displayed with information about how to create a .CSV file for import purposes.

11.6.3. Viewing a computer's Active Directory path information

In the **Computers** window, select the computer whose information you want so view. You will be taken to the **Details** window. Check the **Active Directory path** field.

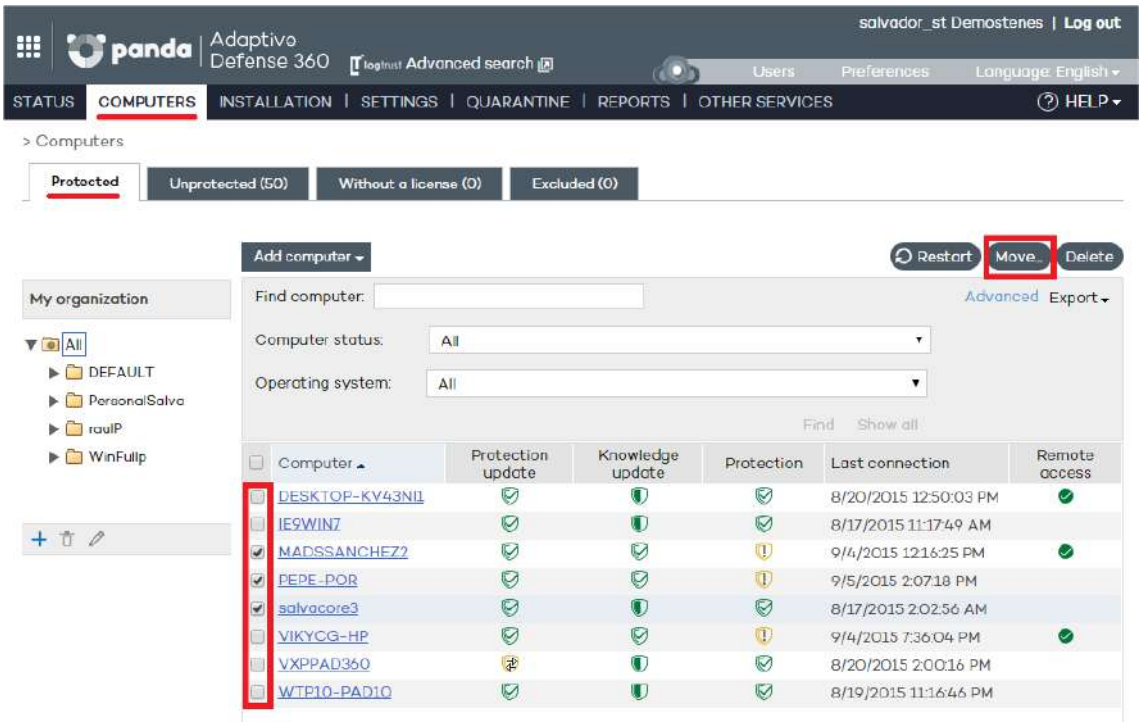


11.7. Adding a computer to a group

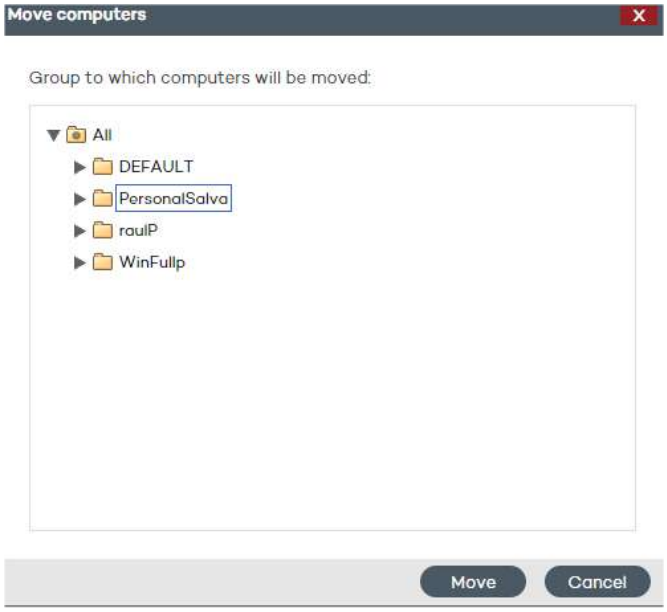
Manual integration

You can manually move a computer or computer group to any other group, regardless of whether this is a manual or automatic group (**arranged by IP address** or **based on Active Directory**).

- Go to the **Computers** window. On the **Protected** tab, select the computer or computers that you want to assign to a group.
- Click **Move**.



- In the **Move computers** window, select the group/subgroup to move the computer/computers to.
- Click **Move**.



You can't assign computers to a group if you only have monitoring permissions. Refer to Chapter 8 for more information about user permissions.

If you try to move one or several computers to a group that has reached the maximum number of allowed installations, a message will be displayed informing you that the operation cannot be performed. Refer to the **Group restrictions** section later in this chapter for more information.

11.8. Adding a computer to a group during installation

When installing the protection on a computer by downloading the installer, you must select the group that the computer will be added to once the installation is complete.

If the computer is added to an automatic group arranged by IP address, Adaptive Defense 360 will move the computer to the appropriate subgroup. If the computer does not fit into any defined subgroup, it will be moved to the parent group.

11.9. Creating and deleting a group

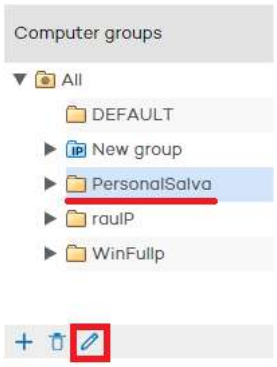
You can create, delete and edit a group from the **Computers** and **Settings** windows.

Groups are usually edited to change their name or the profile assigned to the group and/or the groups that hang from it.

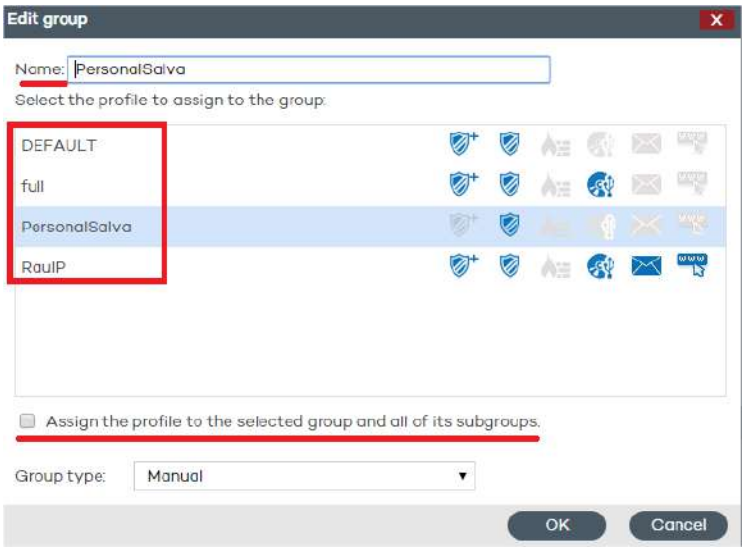
Note: Once a group is created it is not possible to change its type.

Editing a manual group

To edit a manual group, select it from the tree and click the  icon.



Then, you will be able to edit the group's name and assign a protection profile to it from the profile list displayed.

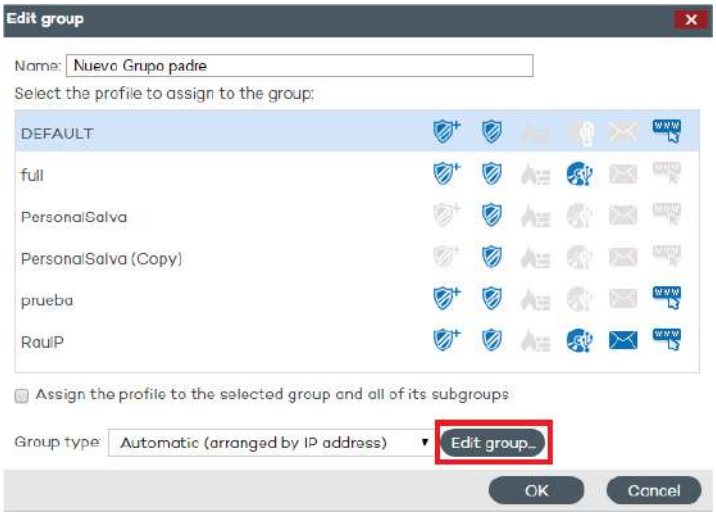


If the group contains subgroups, you can apply the selected profile to all of them. To do that, select the **Assign the profile to the selected group and all of its subgroups** checkbox and click **OK**.

Editing an automatic group arranged by IP address

Two scenarios are possible: Editing the parent group, and editing subgroups with associated IP addresses.

The first case is identical to editing a manual group. To edit subgroups, click the **Edit group** button in the group edition window.



The window that opens will display the IP address rules and the subgroups associated with the automatic group.

Editing an automatic group based on Active Directory

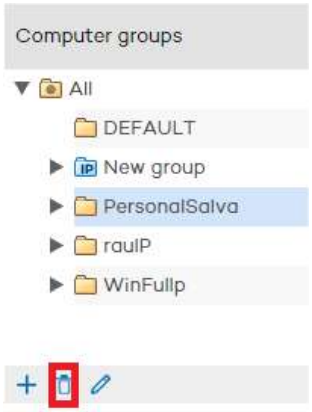
Two scenarios are possible: Editing the parent group, and editing subgroups with the company's Active Directory structure.

The first case is identical to editing a manual group. To edit subgroups, click the **Edit group** button in the group edition window.

> ***It is not possible to change the name of the subgroups included in an automatic group based on Active Directory, as any change would break the correspondence between the structure generated in the*** Adaptive Defense 360 ***console and the company's Active Directory structure. Any change made would be undone in the administration console, re-creating the subgroup whose name was changed and moving computers to it.***

Deleting a group

To delete a group, select it from the group tree and click the icon.



Remember that you cannot delete groups that contain other groups or subgroups. For that reason, before deleting a group you must move every computer it may contain to another group/subgroup.

When this is complete, you will be able to delete the relevant group/subgroup.

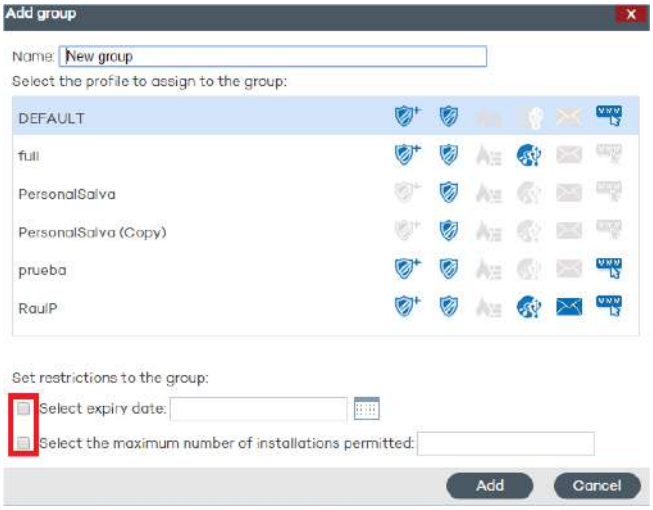
11.10. Group restrictions

Group restrictions are used to limit the number of computers that can belong to a group. This option is particularly useful for partners who want to assign a certain group to a specific customer. Administrators can set the total number of computers that can belong to a group at the same time and for how long.

Partners are advised to use our free product for partners [Panda Partner Center](#) to manage the entire customer life cycle. Contact your sales advisor if you want to have access to that service.

To enable group restrictions, go to the **Preferences** menu and select the **Assign restrictions to groups** checkbox in the **Group restrictions** section.

Once enabled, two new settings will appear in the group creation window:



- **Select expiry date**: Lets you set for how long a computer can belong to a group. After that date, the computer's status will change to **without a license**.
- **Select the maximum number of installations permitted**: Lets you set the maximum number of computers that can belong to the group.
    - If you try to move a computer to a group that has reached the maximum number of installations allowed, an error message will be displayed in the administration console.
    - If you try to install a computer's protection and add it to a group that has reached the maximum number of installations allowed, an error message will be displayed in the computer's local console.

12. Configuration profiles

Network protection overview and planning

Creating and managing protection profiles

Protection profile general settings

12.1. Introduction

This chapter provides an introduction to the configuration of security profiles.

The security profile is the main tool used in Adaptive Defense 360 to deploy the security policy defined by the administrator to the network computers with an agent installed.

A security profile contains the specific configuration of the protection modules, applied to one or several device groups.

A security profile may contain settings that affect different platform types, such as Windows or Mac OS X. This way, a single security profile can be used to configure the protection of all devices on the network, regardless of the device type that receives it.

12.2. Network protection overview and planning

To effectively deploy the security configuration, it is recommended that the administrator follows a series of general steps that will facilitate implementation of the security policy defined in the company, while at the same time minimizing the number and severity of security incidents.

12.2.1. Study and define the company's security policy

The first step the team responsible for ensuring corporate security has to take is create a series of documents that define the security framework required by the company.

This security framework must be compatible with users' needs with regard to network access and the tools required to do their daily tasks without problems.

The objective is to describe a safe and productive environment for the network computers, and for the integrity of the data handled by the company, protecting corporate assets from unauthorized access and preventing data leaks that may damage the company's reputation and lead to financial losses.

To be able to generate this documentation, the team responsible for ensuring corporate security must have a deep understanding of the security and suspicious behavior detection mechanisms to be implemented in the company in order to ensure a trusted, productive environment. The table below illustrates the features provided by Adaptive Defense 360 and their availability on the different operating systems and platforms

Features / Minimum platform	Windows 2000	Windows XP SP2+	Mac OS X	Linux	Android
Advanced permanent protection (Audit, Hardening, Lock)		x			
Data theft detection		x			
Protection of vulnerable systems		x			
Permanent antivirus protection	x	x	x		x
On-demand antivirus protection	x	x	x	x	x
Scheduled scans	x	x	x	x	x
Email protection	x	x			
Web protection	x	x			
Network firewall	x	x			
Application firewall	x	x			
Intrusion detection system	x	x			
URL filtering by category		x			
Device control		x			
Anti-theft protection					x

For file and email servers, Adaptive Defense 360 provides the following features:

Features / Minimum platform	Windows Server	Microsoft Exchange	Mac OS X	Linux
Advanced permanent protection (Audit, Hardening, Lock)	X*	X*		
Data theft detection	X*	X*		
Protection of vulnerable systems	X*	X*		
Permanent antivirus protection	x	x	x	
On-demand antivirus protection	x	x	x	x
Scheduled scans	x	x	x	x
Email mailbox protection		x		
Protection of traffic among email servers (transport)		x		
Anti-spam protection		x		
Content filtering		x		
Network firewall	x	x		
Application firewall	x	x		
Intrusion detection system	x	x		
URL filtering by category	x	x		
Device control	x	x		

(*) Technology compatible with Windows Server, Workstation and Exchange platforms. It requires the execution of the suspect PEs for operation.

12.2.2. Create a list of all the corporate devices to protect

The purpose of this point is to determine the corporate devices that will receive a security configuration from Adaptive Defense 360. To do that, it will be necessary to know each device's operating system, its role within the network (server, workstation, mobile device), and the profile of the user who will use it along with their department.

12.2.3. Make sure that every device on the list has an Adaptive Defense 360 agent installed

For computers to be integrated into the Adaptive Defense 360 console and protected, they must have an agent installed and a valid license assigned. Refer to Chapter 9 for information about installation procedures. Refer to Chapter 6 for information about how to check the status of your Adaptive Defense 360 **licenses.**

12.2.4. Group computers based on their common security requirements

Developing a clear device grouping strategy is key to managing corporate security. Given that the security configurations will be applied to one or several computer groups it will be necessary to find those computers that have the same security requirements.

To be able to segment the network into different groups you must first establish the grouping criteria to be used. Take into account the computer and user data obtained in the second point, that is, the profile of the user who will use the device, the device's operating system, etc.

12.2.5. Create security profiles

A security profile is a configuration template assigned to one or several device groups, and which defines the protection behavior.

The features that can be configured in a security profile include the scan type, the items to scan, access restrictions to the devices connected to the computer, how often the protection will be updated, and other parameters.

The administrator will have to create as many security profiles as security scenarios are required for the different computer groups.

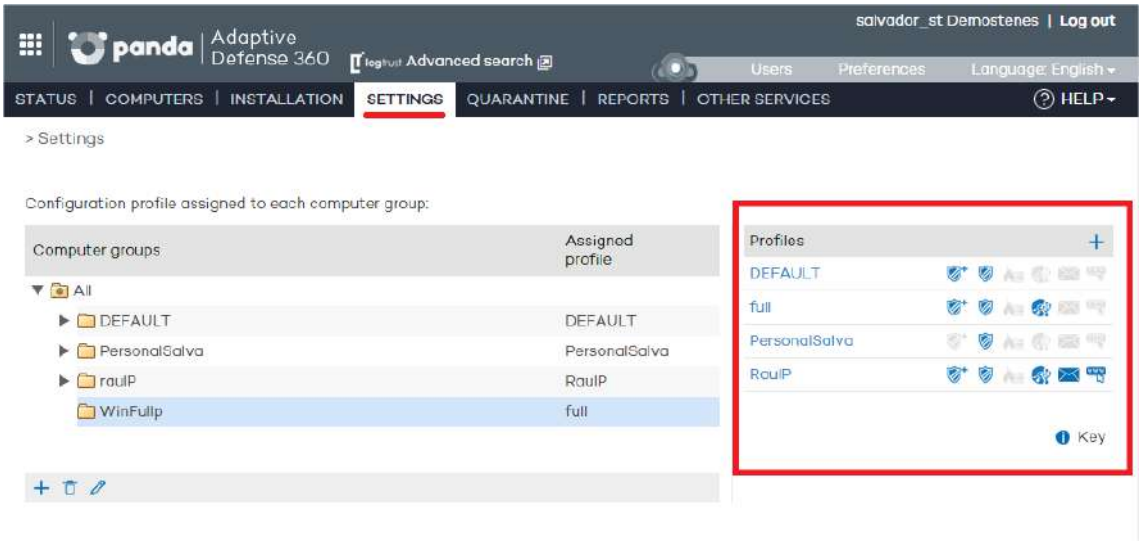
12.2.6. Assign security profiles to groups

There are several options when assigning profiles to groups: one single profile applied to several groups, each group with a different profile, or just one profile and one group in the case of very small or homogeneous networks.

Once you have applied a security profile to a group, every device in the group will be protected according to the protection behavior described in the security profile assigned to it.

12.3. Creating and managing protection profiles

To manage protection profiles, go to the **Settings** window.



12.3.1. Creating a protection profile

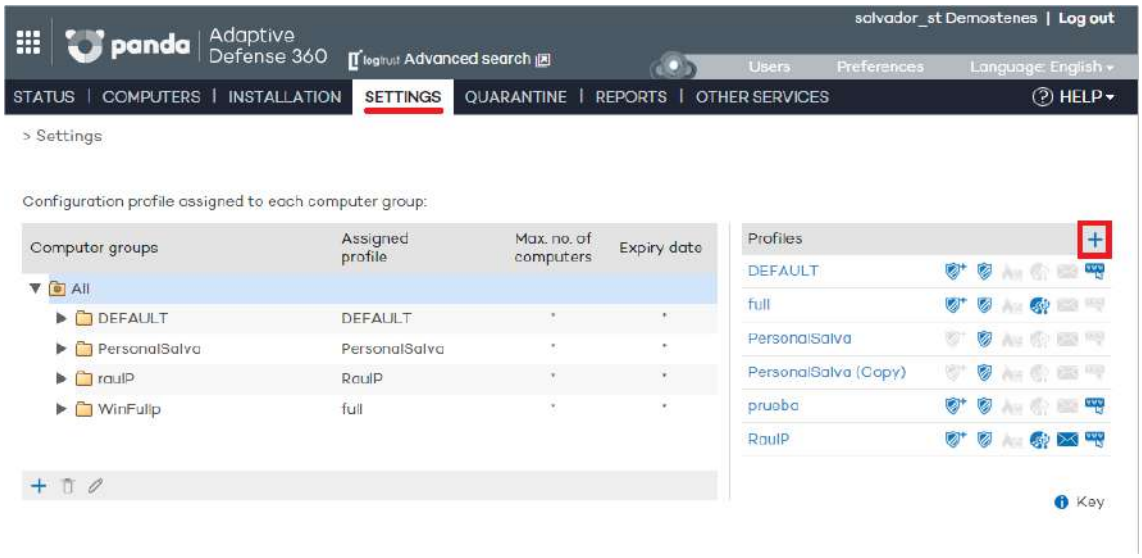
The new profiles you create will appear in the **Settings** window, next to the ***Default*** profile, with information about the protections they include.

You can edit a profile's settings at any time by clicking on its name and going to the **Edit profile** window.

You cannot assign the same name to two profiles. An error message would appear.

> ***If you cannot view an existing profile, you probably don't have the necessary permissions to do so. Refer to Chapter 8 Users for more information.***

To create a profile, click the + icon in the **Settings** window . You will be taken to the **Edit profile** window. From there you will be able to configure the new profile.



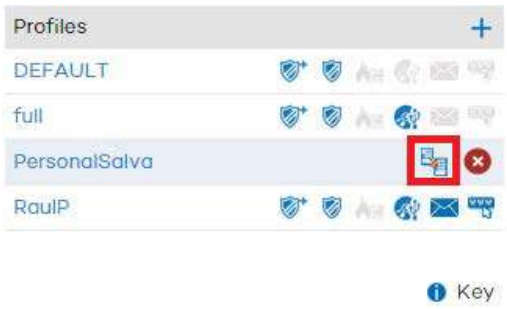
The process to configure a protection profile is explained later in this chapter.

12.3.2. Copying protection profiles

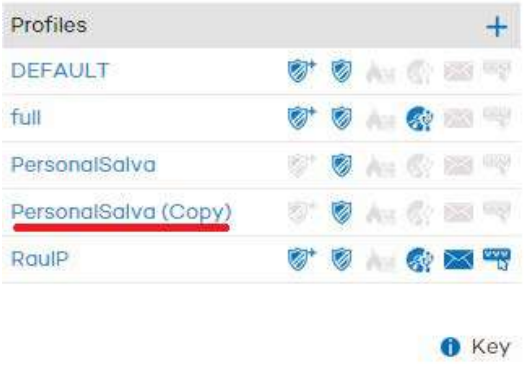
Adaptive Defense 360 gives you the option to make copies of existing profiles. This is useful when you think that the basic settings of a profile that you have created could be used for other computers as well.

This way, instead of having to create the basic settings every time, you can copy an existing profile and then adapt it to the specific circumstances as required.

In the **Settings** window, place the mouse pointer over the icons representing the active protections in the profile you want to copy, and click the  icon.



Once you have made a copy of an existing profile, this will appear under the original profile with the same name and the text *(copy)* at the end.

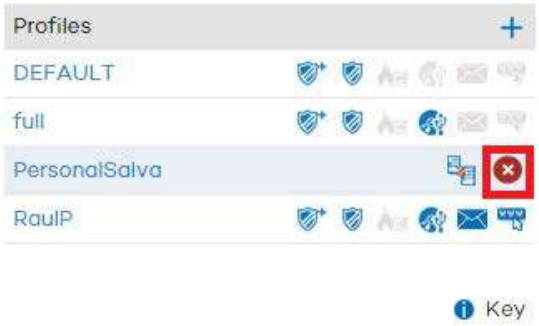


You can also make a copy of the **DEFAULT** profile, however, the copy will not have the status of default profile and will not be assigned automatically to any computer. The original **DEFAULT** profile will be the only predetermined one.

Profile copying is subject to the permissions that you have.

12.3.3. Deleting a protection profile

Click the  icon to delete the selected profile.



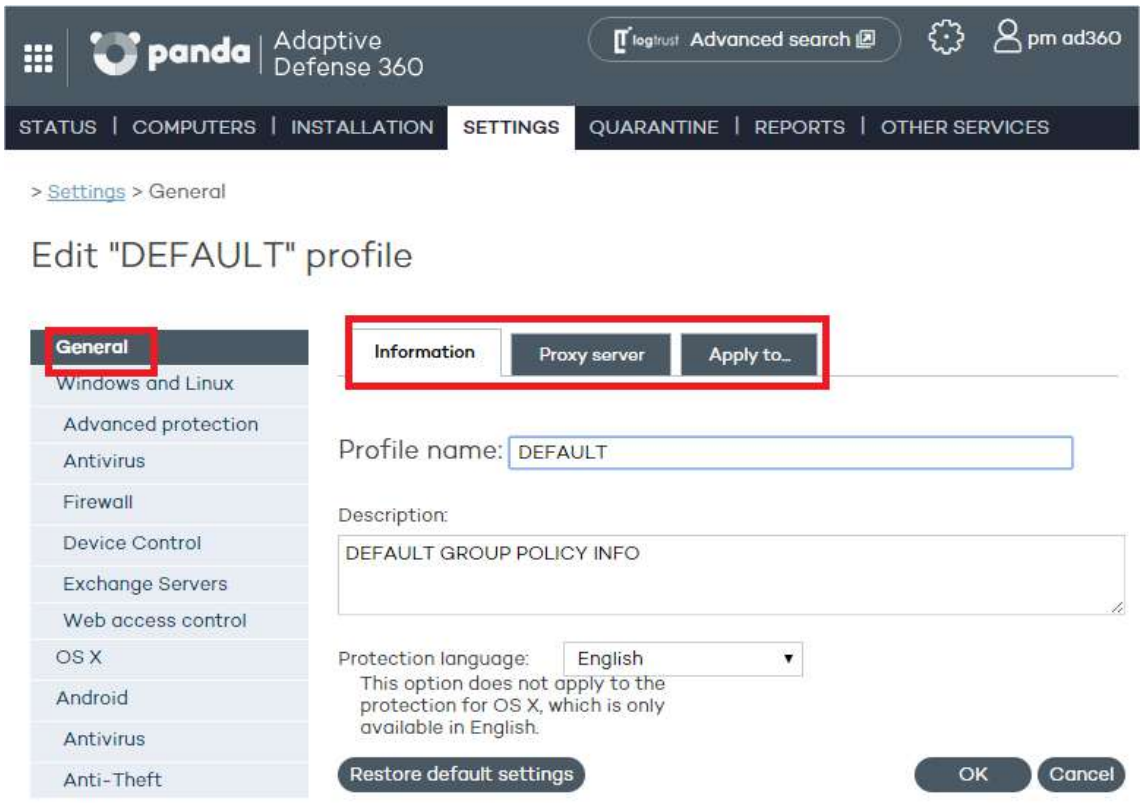
You can only delete a protection profile if the following conditions are met:

- The protection profile is not the **DEFAULT** one.
- You have the necessary permissions to do so.
- The profile is not assigned to any group of computers.

If any of the aforementioned conditions are not met, it will not be possible to delete the protection profile and an error message will be displayed in the administration console.

12.4. Protection profile general settings

Once you have created a profile you can configure it by clicking on it. A window will be displayed with a two-level side menu with the features to configure depending on the platform of the computer to protect (Windows, Linux, Mac OS X and Android).



The general settings are divided into three tabs:

Information tab

Click this tab to enter the name of the profile that you are creating, add a description to identify it, and select the language of the protection.

The protection language option only affects Windows computers, as Adaptive Defense 360 for OS X always installs in English. On Android devices, the protection will install in the language of the device, or in English if the relevant language is not supported by the protection.

Proxy server tab

Configure the network computers' Internet connection. Specify the way the computers connect to the Internet, if they use a proxy server, and if proxy authentication is required.

In the case of Linux computers, you'll have to configure the Internet connection settings locally from each computer using the command line.

Select the option **Request Internet access details if no connection is found.** This way, if the agent cannot access the Internet, a window will be displayed for the user to enter the connection data.

Apply to tab

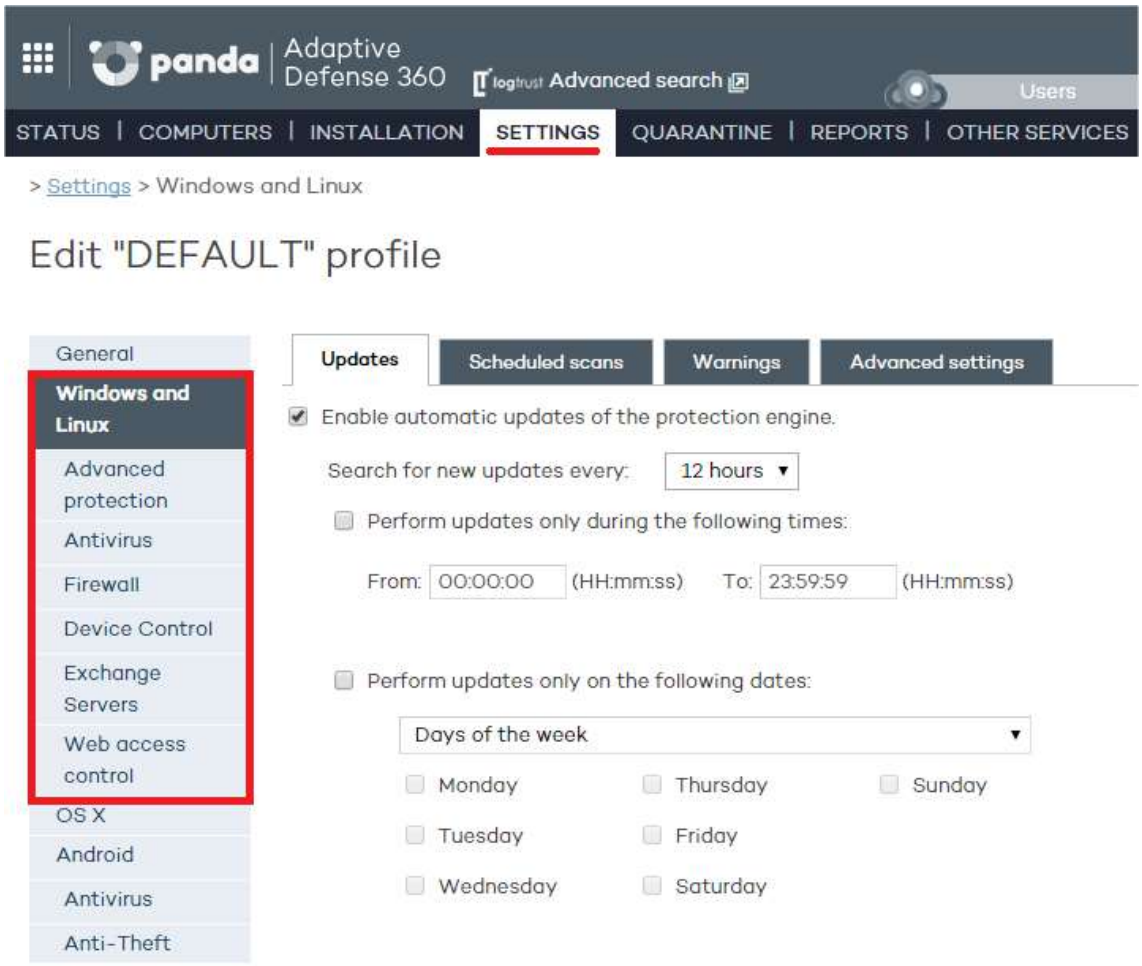
Click this tab to assign the profile to a group or groups of computers.

13. Windows protection profiles

13.1. Introduction

To configure the security profile for a Windows computer, go to the **Settings** window. Select the profile to configure from the **Profiles** panel, and then select **Windows and Linux** from the side menu.

Every protection module applicable to Windows computers has its own section in the side menu.



13.2. General settings

Click **Windows and Linux** in the side menu. A section will be displayed with four tabs to configure the agent's behavior with respect to updates, scheduled scans, warnings and advanced installation and connectivity settings.

Updates

Refer to Chapter 10 for more information about updates

Scheduled scans

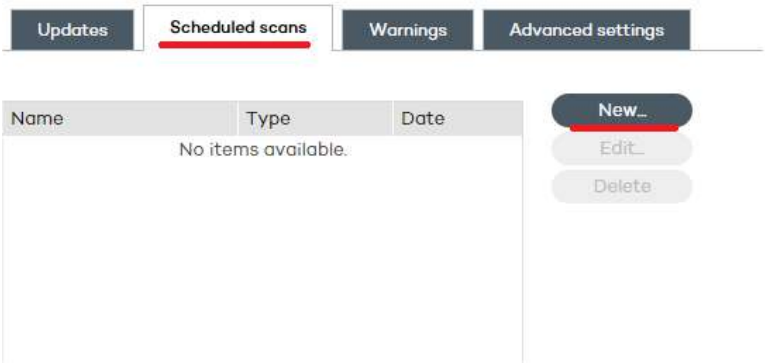
Select the **Scheduled scans** tab to create immediate, scheduled, or periodic scan tasks of the entire computer or just certain components.

You can schedule scans of your hard disks only, or indicate the specific paths of the files or folders that you want to scan.

As you create scan tasks, these will appear on the **Scheduled scans** tab in the **Edit profile** window, from which you can edit them or delete them if desired.

Next, we describe the steps to configure a new scan task:

- Click **New** to go to the **Edit profile – New scan job** window.



- In the window that opens, enter the following data:
  - **Name**: Choose a name for the scan task.
  - **Scan type**: Select the type of scan that you want to create:
    - Immediate scan: Once configured, the immediate scan will take place as soon as the computer connects to the Adaptive Defense 360 server, and the solution checks that the protection configuration has changed.
    - Scheduled scan: The scan will take place at the time and date you set in **Start date** and **Start time**. Use the drop-down menu to select if the scan start time refers to the Adaptive Defense 360 server or the user's computer.
    - Periodic scan: Set the start date and start time, and select the scan frequency in the **Repetition** menu.
  - **Scan**: Select an option from:
    - The whole computer: Scans all hard disks and USB drives
    - Hard disks
    - Other items: Use this option to scan specific items (files, folders, etc.). You'll have to enter the path of the item to scan. The path format must start with \\computer, \\IP address or (drive letter):\.

      Examples:

      \\computer\folder

      **c:\folder1\folder2*

      The permission that you have will dictate whether or not you'll be able to define specific paths to scan. The maximum number of paths to scan for each profile is 10.
- Click the **Advanced settings** option to access a window where you will be able to configure additional aspects of the scheduled scans:

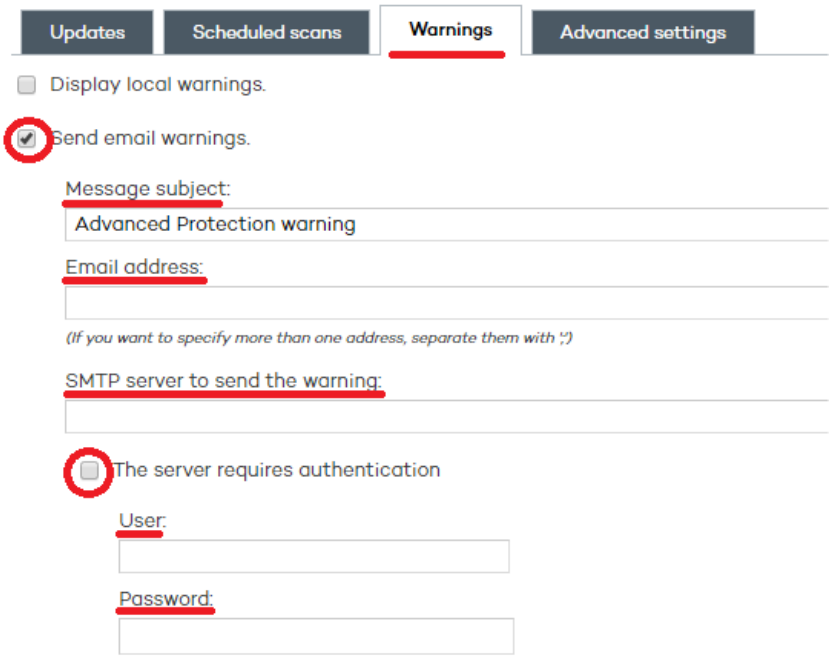
- Select the relevant checkbox to scan compressed files.
- Select the malicious software you want to scan for. The option to scan viruses will always be enabled.
- You can scan the entire computer or exclude certain folders or files with specific extensions from the scans. In the latter case, use the **Add**, **Delete** and **Clear** buttons to define the list of exclusions.

Warnings

This section lets you configure the two types of alerts generated by the AdaptiveDefense 360 local protection.

- Local alerts: These are the alerts displayed by the agent on the affected computer when malware, intrusion attempts or unallowed devices are detected.

- Email alerts: These are the alerts emailed to the administrator by the AdaptiveDefense 360 agent. These alerts contain information about the malware found on the affected computers as well as any violation of the policies defined in the device control module.



These are the alerts emailed to the administrator by the AdaptiveDefense 360 agent. These alerts contain information about the malware found on the affected computers as well as any violation of the policies defined in the device control module.

Select the Send email alerts checkbox to configure the alert message to be sent to the administrator**:**

- **Message subject**: Enter a message subject to allow administrators to add filters to their email client to sort the alert messages received.
- **Email address**: You can enter multiple email addresses separated with a semicolon character (;).
- **SMTP server to send the alert:** Enter the IP address of the company's mail server. This address must be accessible from theAdaptiveDefense 360 local protection.
- **The server requires authentication**: If the mail server is not an open relay for the company's internal IP addresses, it will be necessary to enter the appropriate credentials to send the alerts. These credentials are submitted via the ESMTP protocol, AUTH LOGIN extension.

The email sent by the local protection to the administrator will contain the following basic information:

- **Malware type**: Malware category.
- **Affected computer**: Name of the computer where the malware was found.
- **Path** (if applicable).
- **File** (if applicable): Name of the file where the threat was detected.
- **Action**: Remediation action taken automatically by the local protection.

An alert will be sent every time any of the following events occur:

- Malware detection.
- The Device Control module detects an unauthorized action on a device.

To avoid flooding the administrator's mailbox, Adaptive Defense 360 will enter 'epidemic mode' if it detects more that 20 events pertaining to the same malware or the same device in less than a minute. From then on, a single message will be sent every five minutes with a summary of the events detected. To exit the epidemic mode, it will be necessary that two or more events of the aforementioned type do not occur within the same minute.

Email alerts from the Adaptive Defense 360 **platform**

To prevent situations where the organization's internal mail server is down, cannot be accessed by the computer's local protection, or the client does not have an SMTP mail server, the Adaptive Defense 360 platform can also send email alerts directly to the administrator's account without passing through the organization's internal mail server.

This feature is independent of the profile configuration and can be set for the entire managed network by clicking the General settings button and then **Preferences.**

You can set the conditions under which an email alert will be sent:

- **Malware or PUP detection**: A maximum of 2 emails will be sent per file, computer and day to avoid flooding the administrator's mailbox. This option is selected by default.
- **Every time an item gets blocked**: A single email will be sent per file, computer and day to avoid flooding the administrator's mailbox. This option is disabled by default.
- **Every time a file allowed by the administrator is finally classified**: This alert is only sent if the administrator excluded a blocked item that was pending classification at the time of execution, and the item is finally classified as malware. Since this is a potentially dangerous situation, the system will send an alert to the administrator whenever a change is made to an excluded item's classification. The most typical case is the exclusion of a blocked unclassified item that Adaptive Defense 360 finally classifies as malware

Advanced settings

Here you can configure aspects related to the installation of the protection on computers, as well as the connection of these computers to the Internet and to the Adaptive Defense 360 servers. You can also configure options related to the suspicious file quarantine.

- Installation: Specify in which directory you want to install the protection. Adaptive Defense 360 will show a default path, which you can change if you want.
- Automatically uninstall other security solutions. This section lets you indicate if you want Adaptive Defense 360 to automatically uninstall any competitor product detected on the computer, or if you want both products to coexist on the same computer. Refer to Chapter 9 for more information.
- Connection to Collective Intelligence: Administrators can disable scans with Collective Intelligence. It is advisable to keep this option enabled if you want to benefit from the detection power provided by Collective Intelligence.
- Server connection settings: Establish how often you want computers to send information to the Adaptive Defense 360 servers about the status of the protection installed. This must be a value between 12 and 24 hours.

- **Centralize server communication through the following computer**: Specify the computer through which connections with the Adaptive Defense 360 server will be centralized. To do that, select the relevant checkbox and click **Select**. In the **Select computer** window, choose a computer or search for it using the **Find** button. Then click **OK**.

- Quarantine settings: Lets you indicate the path on the user's computer where detected suspicious items will be temporarily stored. By default, the Quarantine folder is located in the installation directory.
- Administrator password: The administrator password allows you to uninstall and configure the local protection in administrator mode. That is, it allows you to uninstall Adaptive Defense 360 from the network computers, or allow end users themselves to enable or disable their protection from the Adaptive Defense 360 local console. These options are not mutually exclusive, so you can select both at the same time.

13.3. Configuring the advanced protection

The advanced protection lets you establish different security modes to block unknown malware, and protect computers against APTs and advanced threats.

Mode

- Audit: In audit mode, **Adaptive Defense 360** only reports on detected threats but doesn't block or disinfect the malware detected.
- Hardening: Allows execution of the unknown programs already installed on users' computers. However, unknown programs coming from external sources (Internet, email, etc.) will be blocked until they are classified. Programs classified as malware will be moved to quarantine.
- Lock: Prevents all unknown programs from running until they are classified.
    - **Do not report blocking to the computer user**
    - **Report blocking to the computer user**: Users will see a message whenever an item is blocked, explaining why it was blocked.
    - **Report blocking and give the computer user the option to run the item:** Displays a message for 1 minute allowing users to run the detected item under their own responsibility. These exclusions are permanent until the administrator changes the configuration from the console.

Exclusions

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

This section allows you to configure items on the network computers that will not be scanned by Adaptive Defense 360

- **Extensions**: Allows you to specify file extensions that won't be scanned.
- **Folders**: Allows you to specify folders whose content won't be scanned.
- **Files**: Allows you to indicate specific files that won't be scanned.

Network usage

Every executable file found on users' computers that is not recognized by **Adaptive Defense 360** will be sent by the agent to our server for analysis. This is configured to have no impact on the performance of the customer's network (the maximum number of MB that can be transferred in an hour per agent is set by default to 50). Unknown files are sent only once for all the customers using Adaptive Defense 360. Additionally, bandwidth management mechanisms have been implemented in order to minimize the impact on the customer's network.

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

Privacy

To allow Adaptive Defense 360 to display the full name and path of the files sent for analysis in its reports and forensic analysis tools, select the relevant checkbox on the **Privacy** tab.

13.4. Configuring the antivirus protection

The **Files**, **Mail** and **Web** tabs let you configure the general behavior of the antivirus protection for the profile you are creating.

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

- Files identified as malware when disinfection is possible:

They are disinfected. The original file is deleted and replaced with a harmless, disinfected copy.

- Files identified as malware when disinfection is not possible

If disinfection is not possible, the file is moved to quarantine.

Files

Here you can configure the basic operation of the antivirus with respect to the file protection.

- Select **Enable permanent file protection**.
- If you want the protection to scan compressed files, select the relevant checkbox.

- Select the malicious software to detect.
    - **Viruses**: 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.
    - **Hacking tools and PUPs**: Programs that can be used by a hacker to carry out actions that cause problems for the user of the affected computer.

If the permanent file protection is enabled, it will not be possible to disable the virus detection option.

Next, select the behavioral detection technologies:

- Block malicious actions: Enables a set of anti-exploit technologies that scan the behavior of local processes looking for suspicious activity.

To define exclusions, click **Advanced settings**. You'll be taken to the **Exclusiones** tab, already explained in the **Configuring the advanced protection** section.

Mail

This window lets you configure how the email antivirus protection will operate in the profile you are creating.

- Indicate whether you want to enable the permanent email protection, as well as scanning compressed files.
- Select the malicious software to detect by ticking the relevant checkboxes.
    - Viruses
    - Hacking tools and PUPs
    - Suspicious items
    - Phishing: A technique for obtaining confidential information fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

Click **Advanced settings**. You'll be taken to the **Exclusiones** tab, where you will be able to configure attachment file name extensions that won't be scanned by the protection

For information about the advanced settings for the email protection feature, refer to the Exchange Server section later in this chapter.

Web

This tab lets you configure the Internet protection, which protects users against Internet-borne malware and phishing attacks.

This protection is disabled by default. To enable it, follow the steps below:

- Enable the permanent Internet protection for Windows workstations and/or servers.
- Select the option to detect phishing Web pages if you want to.

The virus detection option will always be enabled.

13.5. Configuring the firewall and intrusion detection features

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

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

The first thing you must do to configure the firewall protection is decide if the users to which the profile will be applied will be allowed to configure the firewall from their computers (firewall in user mode) or if you, as the administrator, will do it (firewall in administrator mode).

Firewall in user mode

Select the option that allows users to configure the firewall protection.

In this case, the end user will be able to access the firewall settings from the agent installed on their computer.

Firewall in administrator mode

If, otherwise, you want the firewall settings to be available only from the Web console, you, as the administrator, will establish the firewall restrictions, block rules, permissions, etc. to be applied to the computers you select.

In that case, keep the default option selected: **Apply the following settings to the firewall**.

You must also choose whether the firewall protection configuration will be applied to Windows workstations and/or Windows servers. Select the relevant checkboxes.

General

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

- **Public network**: This is the network type you find in Internet cafes, airports, etc. Visibility of computers is restricted on such networks, and there are restrictions on sharing files, resources and directories.
- **Trusted network**: In this case, we are generally talking about office or home networks. Your computer will be perfectly visible to the other computers on the network. Additionally, there are no limitations on sharing files, resources or directories.

Adaptive Defense 360 will behave differently and will apply different predetermined rules depending on the type of network. You can view these predetermined rules (Panda rules) by going to the Programsand System tabs.

Programs

This tab allows administrators to specify which of the user's programs can communicate with the network/Internet and which cannot.

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

1- Choose the default action from the **Default action** menu.

- **Allow access**: Allows communications for all programs with no specific rules assigned. This is the default, basic mode.

- **Deny access**: Denies connections for all programs with no specific rules assigned. This is an advanced mode, as it requires adding rules for every frequently used program. Otherwise, those programs will not be allowed to communicate, affecting their performance.

2- Click Add to define the way a specific application should behave:

- **Allow inbound and outbound connections**: The program can connect to the Internet/local network and allows other programs or users to connect to it. There are certain types of programs that need these permissions to work correctly: file swapping programs, chat applications, Internet browsers, etc.
- **Allow outbound connections**: The program can connect to the Internet/local network, but does not accept external connections from other users or applications.

- **Allow inbound connections**: The program accepts connections from programs or users from the Internet/local network, but it will not have outbound permissions to connect.
- **No connection**: The program cannot connect to the Internet or the local network.

Intrusion prevention

The intrusion detection module allows administrators to detect and reject malformed traffic designed to impact the security and performance of the computers to protect. This traffic type may cause malfunction of user programs, and lead to serious security issues, allowing remote execution of user applications by hackers, data theft, etc.

Adaptive Defense 360 provides protection against 15 types of generic patterns. This protection can be enabled and disabled by selecting and clearing the relevant checkboxes. Next is a description of the types of malformed traffic supported and the protection provided:

- **IP explicit path**: Rejects IP packets with an explicit source route field. These are IP packets that are not routed based on their target IP address, but the routing information is defined beforehand.
- **Land Attack**: Stops denial-of-service attacks by TCP/IP stack loops by detecting packets with identical source and destination addresses.
- **SYN flood**: This attack launches TCP connection attempts massively to force the targeted computers to commit resources for each connection. The protection establishes a maximum number of open TCP connections to prevent the computer under attack from becoming saturated.
- **TCP Port Scan**: Detects if a host tries to connect to several ports in a specific time period. It blocks the attack preventing replies to the suspicious host. In addition, it filters the replies so the sender doesn't even get closed port replies.
- **TCP Flags Check**: Detects TCP packets with invalid flag combinations. It acts as a complement to the protection against port scanning by blocking attacks of that type such as "SYN&FIN" and "NULL FLAGS". It also complements the protection against OS fingerprinting attacks as many of these are based on replies to invalid TCP packets.
- **Header Lengths**
  - **IP:** Rejects inbound packets with an IP header length that exceeds a specific limit.
  - **TCP:** Rejects inbound packets with a TCP header length that exceeds a specific limit.
  - **Fragmentation control:** Checks the status of the packet fragments to be reassembled at the destination, protecting the system against memory overflow attacks due to missing fragments, ICMP redirects masked as UDP and computer scanning.
- **UDP Flood**: Rejects UDP streams to a specific port if the number of UDP packets exceeds a preconfigured threshold in a particular period.
- **UDP Port Scan**: Protects the system against UDP port scanning attacks.
- **Smart WINS**: Rejects WINS replies that do not correspond to requests sent by the computer.
- **Smart DNS**: Rejects DNS replies that do not correspond to requests sent by the computer.
- **Smart DHCP**: Rejects DHCP replies that do not correspond to requests sent by the computer.

- **ICMP Attack**: This filter performs various checks.
    - **SmallPMTU**: By inspecting ICMP packets, the protection detects invalid MTU values used to generate a denial of service attack or slow down outbound traffic.
    - **SMURF:** The attack involves sending large amounts of ICMP (echo request) traffic to the network broadcast address with a source address spoofed to the victim's address. Most computers on the network will reply to the victim, multiplying traffic flows. The protection rejects unsolicited ICMP replies if they exceed a certain threshold in a specific time period.
    - **Drop unsolicited ICMP replies**: Rejects all unsolicited ICMP replies and ICMP replies that have expired due to timeout.
- **ICMP Filter echo request**: Rejects Echo requests.
- **Smart ARP**: Rejects ARP replies that do not correspond to requests sent by the protected computer to avoid ARP cache poisoning scenarios.
- **OS Detection**: Falsifies data in replies to the sender to trick operating system detectors. It prevents attacks aimed at taking advantage of vulnerabilities associated with the operating system detected. This protection complements the TCP Flag Checker.

System

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

The system rules let you establish connection rules that affect the entire system (regardless of the process that manages them). They have priority over the rules that govern the connection of programs to the Internet/local network.

To develop an effective protection strategy it is necessary to follow the steps below in the order listed: Set the firewall's default action. To do that, go to the Programs tab and:

1. Choose an action from the Default action menu:
    - **Allow access**: Allows communications for all programs with no specific rules assigned. This is the default, basic mode: all programs with no specific rules assigned can communicate with the Internet/local network.

    - **Deny access**: Denies connections for all programs with no specific rules assigned. This is an advanced mode, as it requires adding rules for every frequently used program. Otherwise, those programs will not be allowed to communicate, affecting their performance.

2. Click the Add button to add new connection rules as well as the action to take.

The order of the rules in the list is not random. They are applied in descending order, therefore, if you change the position of a rule, you will also change its priority.

Next we describe the fields found in a system rule:

- **Rule name**: The name of the rule. Two rules cannot have the same name.
- **Action to take**: Defines the action to be taken by Adaptive Defense 360 if the rule matches the examined traffic.
    - **Allow**: Allows traffic
    - **Deny**: Blocks traffic. It drops the connection.
- **Direction**: Sets the traffic direction for connection protocols such as TCP
        - **Oubound**: Outbound traffic
        - **Inbound**: Inbound traffic
    - **Zone**
    - **Protocol**: Allows you to specify the rule protocol. The local ports field will vary depending on the chosen protocol.
        - **TCP**
        - **UDP**
        - **ICMP**
        - **IP Types**
    - **Local ports / Services / Protocols**: A different field will be displayed depending on the type of protocol chosen:
        - **Local ports**: Allows you to specify the TCP and UDP local ports. A drop-down menu is displayed with the most common ports, as well as a **custom** field to add ports within the range 0-65535. If you enter several individual ports, separate them with a comma between entries. Use a hyphen if you want to enter a range of port numbers. (E.g. 80, 25, 120-134)
        - **Services**: Allows you to specify the ICMP message subtype.
        - **Protocols**: Allows you to specify the high-level protocol that will travel in the IP packet examined.

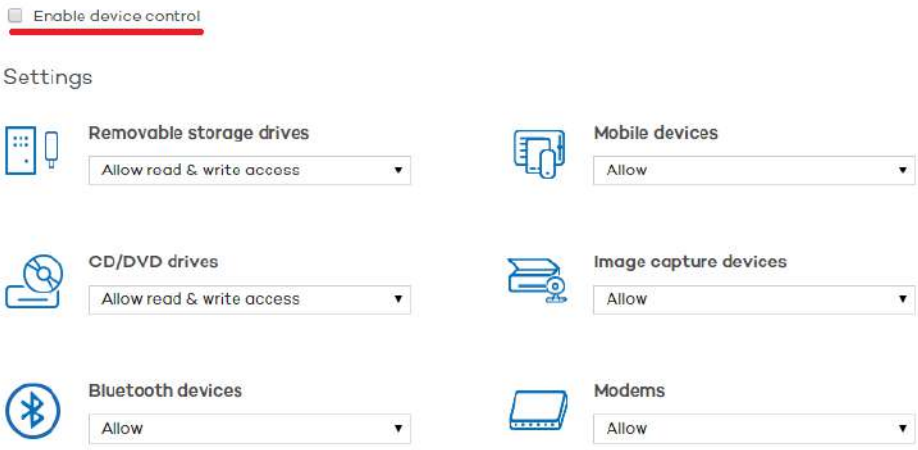
13.6. Configuring the device control feature

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

The device control settings allow you to configure the device control protection for the profile you are creating. Select the device or devices you want to authorize or block and specify their usage.

Follow the steps below to enable the device control feature:

- Select the **Enable device control** checkbox.
- In the relevant menu, select the authorization level for each device type.
    - In the case of USB flash drives and CD/DVD drives, you can choose among **Block**, **Allow read access** or **Allow read & write access**.
    - The options available for Bluetooth and imaging devices, USB modems and smartphones are **Allow** and **Block**.

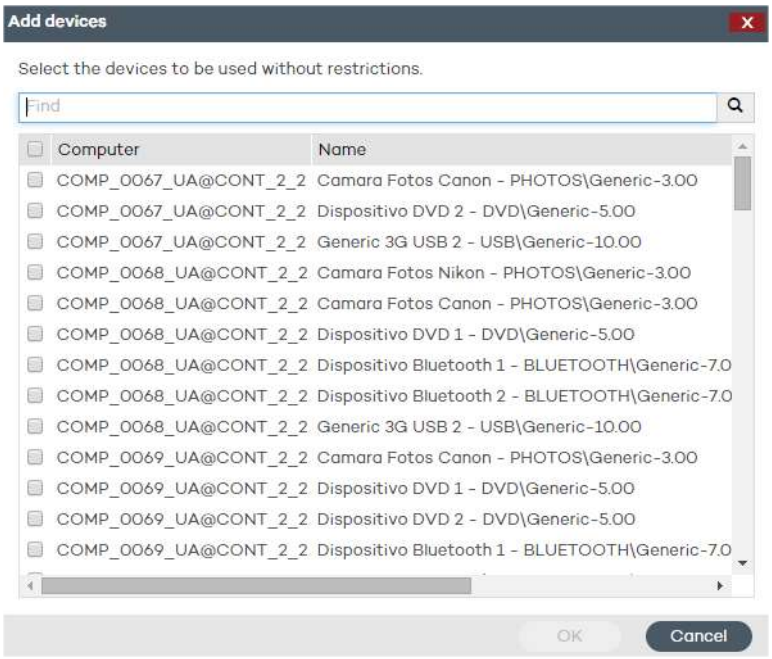


13.6.1. Device exclusions

Sometimes, you may need to block a certain category of devices but allow the use of some specific devices belonging to that category.

In that case you can create a whitelist, that is, a list of devices that will be allowed despite belonging to an unauthorized category.

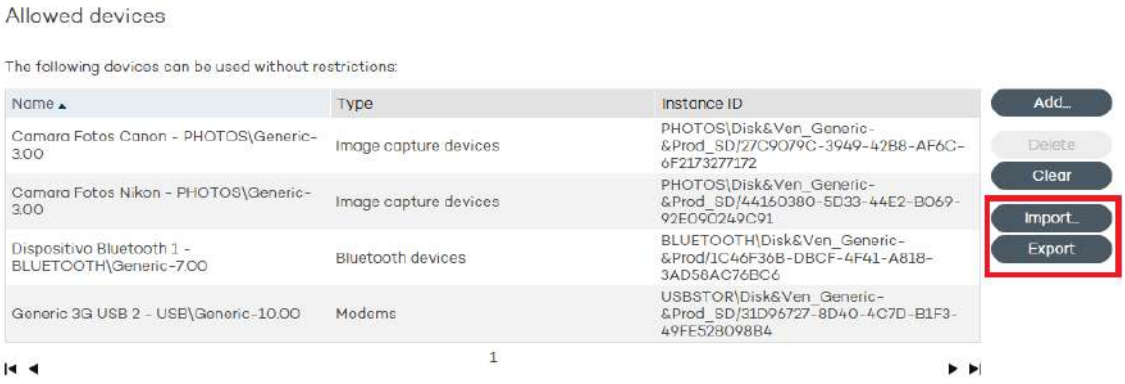
Adaptive Defense 360 shows a list of all the devices connected to each computer. Click **Add** in the **Allowed devices** section to display the list, and select the devices that you want to exclude from the general blocking options configured.



13.6.2. Exporting/importing a list of allowed devices

Once you have finished configuring your list of allowed devices, you can export it to a text file. You can also do the opposite, that is, create a text file with the devices that you want to allow, and import it to the Adaptive Defense 360 Web console.

Use the **Export** and **Import** buttons to export and import already configured exclusion lists.

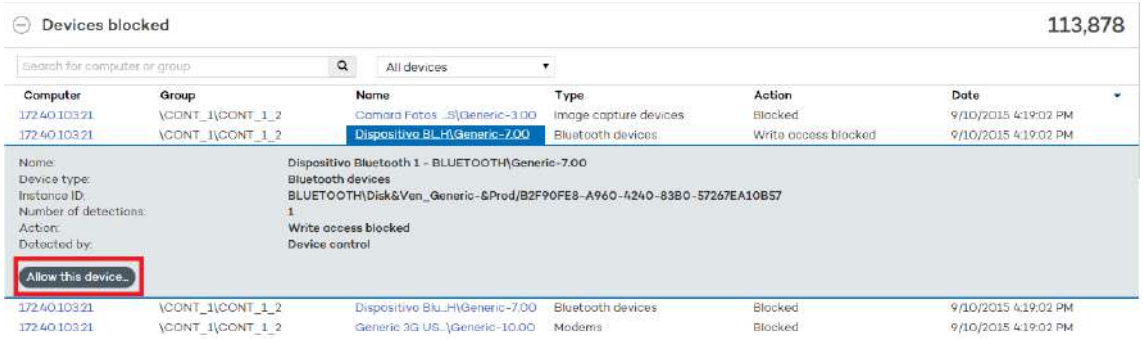


13.6.3. Allowing blocked devices

Every time that Adaptive Defense 360 detects an unauthorized device, it blocks it and logs the incident in the **Detection details** section.

To access the **Detection details** section, go to **Status** > **Detection origin** > **Detection details** > **Detected threats** > **Devices blocked**.

There you'll see a button called **Allow this device**.



Click the button and select the protection profiles to authorize the device for. The device will be included in the list of allowed devices for the selected profiles.

13.6.4. Finding a device's unique ID

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

- In the Windows Device Manager, access the properties of the USB device that you want to identify in order to exclude it.
- Go to the **Details** tab and select **Resources** from the **Property** menu. A value called CM_DEVCAP_UNIQUEID should be displayed.
- Next, select **Device Instance Path** from the **Property** menu to obtain the device's unique ID.

If no CM_DEVCAP_UNIQUEID value is displayed, it will not be possible to identify the device uniquely. You will have to use the device's hardware ID to identify it.

In the **Property** menu, select **Hardware ID**. This value will allow you to exclude every USB device of the same model as the detected one, as it won't be possible to differentiate one from the others.

Once you have the unique IDs of all the devices that you want to allow, you'll be able to create a whitelist and import it as explained in the previous section.

13.6.5. Warnings

The device control module shows different types of notifications to end users.

- Unallowed devices

If the protection detects that the user connects a device that is not allowed according to the security profile applied to the computer, a warning will be displayed informing them that they do not have permission to access it.

- Read-only devices

The device will appear in the My Computer directory, but a warning message will be displayed if the user double-clicks it. The message will indicate that the user does not have permission to write to it.

13.7. Configuring the protection for Exchange Server

Provided you have the necessary licenses, you can enable the protection for Exchange Server from the console and apply it to any Exchange servers that you are managing.

> *The protection for Exchange Server supports Exchange 2003, 2007, 2010, 2013 and 2016.*

The protection for Exchange Server includes three protection modules: **Antivirus**, **Anti-spam** and **Content filtering**.

Additionally, depending on the moment when Adaptive Defense 360 scans email traffic, there are two protection modes: mailbox protection and transport protection.

The table below illustrates the availability of these protection modes for the different protection modules and Exchange versions.

Mode / Module	Antivirus	Anti-spam	Content filtering
Mailbox	2003, 2007, 2010		
Transport	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016

- Mailbox protection

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

> *The mailbox protection is only available in the Antivirus module for Exchange 2003, 2007 and 2010*

- Transport protection

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

13.7.1. Antivirus

Adaptive Defense 360 scans for viruses, hacking tools and suspicious/potentially unwanted programs sent to the Exchange Server mailboxes.

The administrator has the option to enable/disable the mailbox and/or the transport protection by clicking the relevant checkboxes.

- Mailbox protection

The mailbox protection behaves differently depending on whether the Exchange server is Exchange Server 2013-2016 or a different version.

- Exchange 2013-2016 does not allow message manipulation: if a message contains a dangerous item, the entire message is moved to quarantine. Users protected with Adaptive Defense 360 will receive a message with the original subject but the body replaced with a warning text. This text prompts the user to contact the network administrator to recover the original message.
- In all other Exchange versions, Adaptive Defense 360 takes the action defined by Panda Security when a malware item is detected: disinfect the attachment if disinfection is possible, or send it to quarantine if disinfection is not possible. Therefore, the user will receive the original message with the clean attachments or, if disinfection was not possible, a replacement file called “security_alert.txt” with information about the reason for the detection.

13.7.2. Anti-spam

Select or clear the **Detect spam** checkbox to enable or disable this protection.

- **Actions to perform on spam messages**
  - **Let the message through**: The tag *Spam* will be added to the subject line of the message. This is the default option.
  - **Move the message to...:** You will have to specify the email address that the message will be moved to. In addition, the tag *Spam* will be added to the subject line of the message.
  - **Delete the message**
  - **Flag with SCL (Spam Confidence Level)**

SCL

The Spam Confidence Level (SCL) is a value from 0 to 9 assigned to a message that indicates the likelihood that the message is spam. A value of 9 indicates a extremely high likelihood that the message is spam. 0 is assigned to messages that are not spam. The SCL value can be used to configure a threshold in Active Directory above which you consider a message to be spam: the solution flags messages with the relevant SCL value and lets them through.

Then, it is the administrator who establishes the action to be taken on the message based on the threshold set in Active Directory.

Allowed/denied addresses and domains

Use the **Add**, **Delete** and **Clear** buttons to configure a list of addresses and domains whose messages will not be scanned by the anti-spam protection (*whitelist*), or a list of addresses and domains whose messages will always be intercepted and deleted by the protection (*blacklist*).

Keep in mind the following aspects when configuring these lists:

- If a domain is on the blacklist but an address in the domain is on the whitelist, the address will be allowed. However, all other addresses in the domain will be blocked.
- If a domain is on the whitelist but an address in the domain is on the blacklist, that address will be blocked. However, all other addresses in the domain will be allowed.
- If a domain (e.g.: domain.com) is on the blacklist and one of its subdomains (e.g.: mail1.domain.com) is on the whitelist, the addresses in the subdomain will be allowed. However, all other addresses in the domain or in any other of its subdomains will be blocked.
- If a domain is on the whitelist, all subdomains in the domain will also be whitelisted.

Content filtering

The Content Filtering feature allows administrators to filter email messages based on the extension of their attachments.

Once you have set a list of potentially suspicious files, configure the action to take on them.

You can also use the content filtering feature on email attachments with double extensions

- **Consider files with the following extensions dangerous**: Select this checkbox to classify certain extensions as dangerous. Then, use the **Add**, **Delete**, **Clear** and **Restore** buttons to set the list of extensions to block.
- **Consider attachments with double extensions dangerous, except for the following**: Select this option to block all messages containing files with double extensions, except for the ones you allow. Use the **Add**, **Delete**, **Clear** and **Restore** buttons to configure the list of double extensions to allow.
- **Action to take**: Select whether you want to delete files with dangerous attachments or move them to a specific folder. This can very useful to store and analyze those files in order to make the appropriate adjustments to the list of dangerous extensions.

Detection log

Every detection that takes place on an Exchange server is logged locally in a CSV file. This allows network administrators to obtain additional information when a message does not reach the intended recipient.

This file is called ExchangeLogDetections.csv and can be found in the following folder:

%AllUsersProfile%\Panda Security\Panda Cloud Office Protection\Exchange

The file content is shown in tabular form with the following fields:

- Date: Date when the message arrived at the Exchange server.
- From: Message sender.
- To: Message recipient.
- Subject: Email subject.
- Attachments: List of the message attachments.
- Protection
- Action

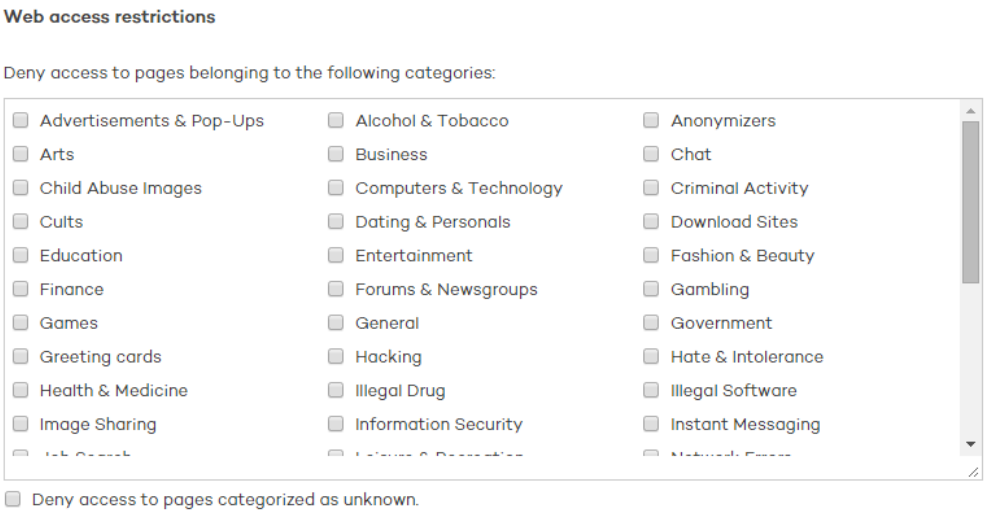
13.8. Configuring the Web access control

This protection allows network administrators to limit access to specific Web categories, and configure a list of URLs to allow or deny access to. This feature lets companies optimize network bandwidth and increase business productivity.

Denying access to specific Web pages

Web pages are divided into 59 categories. Select the URL categories that you want to deny access to. You can modify them at any time.

Select the relevant checkbox to enable the Web access control feature for Windows workstations, Windows servers or both. Then, select the categories that you want to deny access to.



If a user tries to access a Web page belonging to a blocked category, an access denied notification will be displayed.

If you make a change to the list of allowed or denied categories, it can take up to 15 minutes for the network computers to receive the new configuration. During this time, the Web access control feature will behave in exactly the same way as it did before the modification.

Denying access to pages categorized as unknown

You can deny access to pages categorized as unknown simply by selecting the relevant checkbox.

Bear in mind that internal and intranet sites that connect on ports 80 or 8080 may be categorized as unknown, resulting in users not being able to access them. To avoid that, administrators can add any unknown pages that they want to the exclusion while list explained below.

List of allowed/denied addresses and domains

You can set a list of pages that will always be allowed (whitelist) or blocked (blacklist).

You can edit these lists at any time.

- Enter the URL of the relevant address or domain in the text box.
- Click **Add**.
- Use the **Delete** and **Clear** buttons to edit the list according to your needs.
- Finally, click **OK** to save the settings.

Database of URLs accessed from computers

Each computer keeps a database of the URLs accessed from it. This database can only be consulted locally, that is, from the computer itself, for a period of 30 days.

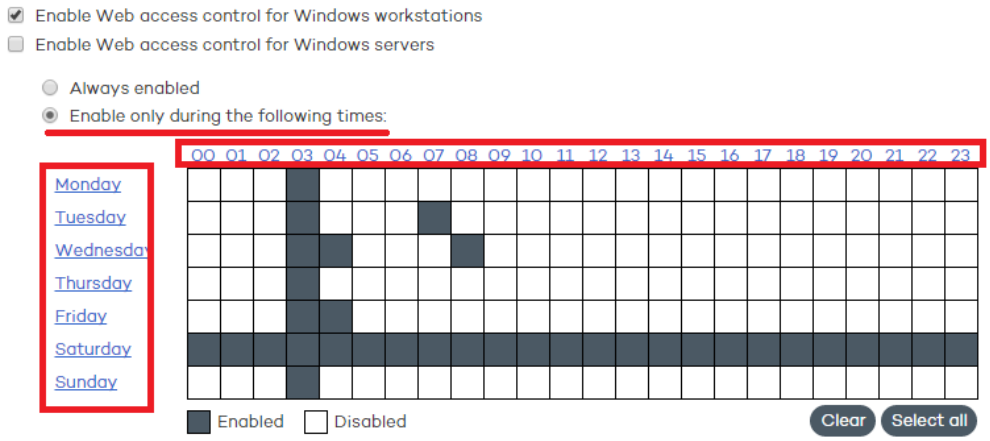
The data collected in this database is:

- User ID.
- Protocol (HTTP or HTTPS).
- Domain.
- URL.
- Returned category.
- Action (Allow/Deny).
- Access date.
- Access counter (by category and by domain).

Configuring time periods for the Web access control feature

This feature allows you to limit access to certain Web page categories and blacklisted sites during working hours, and authorize it during non-working hours or weekends.

To configure Internet access time limits, select the **Enable only during the following times** option



Then, select the times at which you want the Web access control to be enabled. Use the time grid to do so.

- To select whole days, click the relevant day of the week.
- To select the same time period for every day of the week, click the relevant hours.

> ***Bear in mind that the system will use the local time on each computer, not the server time.***

14. Linux protection profiles

General settings

Configuring the antivirus protection

14.1. Introduction

To configure the security profile for a Linux computer, go to the **Settings** window. Select the profile that you want to configure from the **Profiles** panel, and click **Windows and Linux** from the side menu.

This chapter only covers those settings supported for Linux systems.

14.2. General settings

Updates

In the case of Linux computers it is not possible to perform automatic updates. Therefore, when a new version of the protection is made available, it has to be manually installed on computers.

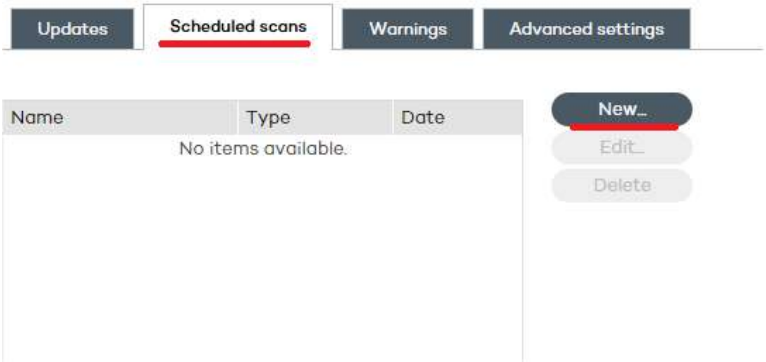
Seven days after the release of a version more recent than the protection installed on a Linux computer, this will appear as "out-of-date" in the **Status** window. The administrator will then have to install the new protection on the computer.

Also, in the case of Linux computers, it is not possible to configure the frequency of the automatic updates of the signature file.

Scheduled scans

Next, we describe the steps to configure a new scan task:

- Click **New** to go to the **Edit profile – New scan job** window.



- In the window that opens, enter the following data:
  - **Name**: Choose a name for the scan task.
  - **Scan type**: Select the type of scan that you want to create:
    - Immediate scan: Once configured, the immediate scan will take place as soon as the computer connects to the Adaptive Defense 360 server, and the solution checks that the protection configuration has changed.

        - Scheduled scan: The scan will take place at the time and date you set in **Start date** and **Start time**. Use the drop-down menu to select if the scan start time refers to the Adaptive Defense 360 server or the user's computer.
        - Periodic scan: Set the start date and start time, and select the scan frequency in the **Repetition** menu.
    - **Scan**: Select an option from:
        - The whole computer: Scans all hard disks and USB drives
        - Hard disks
        - Other items: Use this option to scan specific items (files, folders, etc.). You'll have to enter the path of the item to scan. The path must start with /
          Example: /root/documents
- Click the **Advanced settings**link to access a new window where you'll be able to configure additional aspects of the scheduled scans:
    - Select the relevant checkbox to scan compressed files.
    - Select the malicious software you want to scan for. The **Hacking tools and PUPs** and **Viruses** options will always be enabled.
    - You can scan the entire computer or exclude certain folders or files with specific extensions from the scans. In the latter case, use the **Add**, **Delete** and **Clear** buttons to define the list of exclusions.

Warnings

This option is not supported for Linux computers.

Advanced settings

- **Installation**: On Linux computers, the protection is installed in a default folder that cannot be changed.
- **Connection to Collective Intelligence**: On Linux computers it is not possible to disable the connection to Collective Intelligence. Therefore, as long as a computer is connected to the Internet, the installed protection will query Collective Intelligence.
- **Server connection settings:** This option is not available for Linux computers.
- **Quarantine settings**: The quarantine is not supported for Linux computers
- **Administrator password**: This option is not available for Linux computers.

14.3. Configuring the antivirus protection

The permanent file protection is not supported for Linux computers. Therefore, to protect your Linux computers you must run on-demand scans or schedule periodic scans.

15. Mac OS X protection profiles

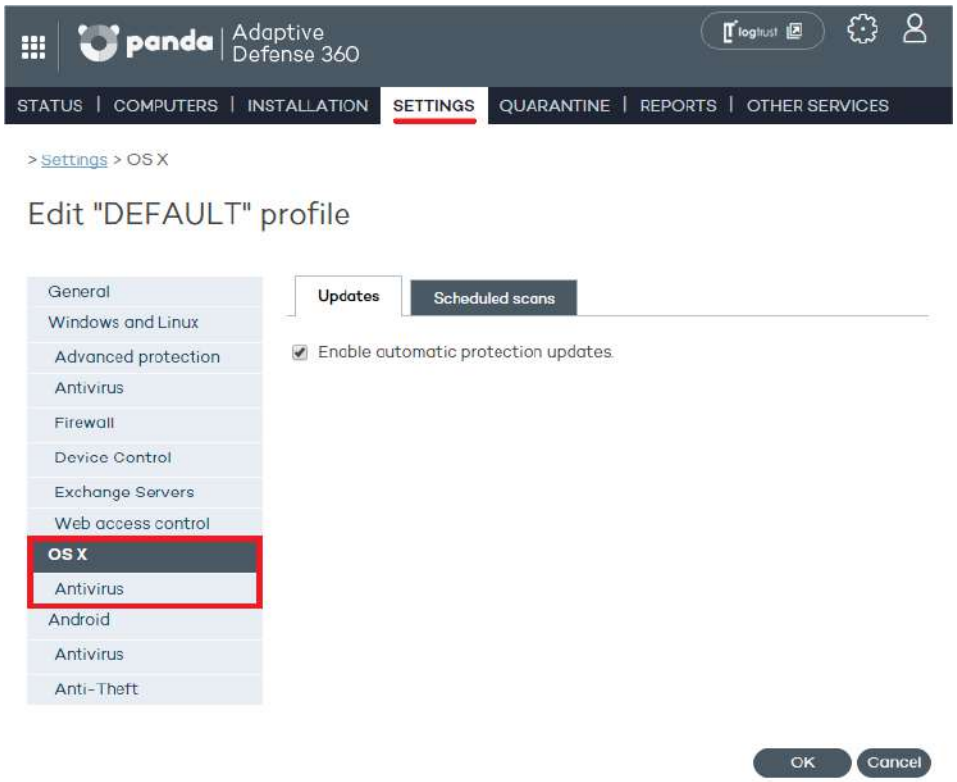
Specific characteristics of the protection for Mac OS X

General protection settings

Configuring the antivirus protection

15.1. Introduction

To configure a security profile for a Mac OS X computer, go to the **Settings** window. Select the profile to configure from the **Profiles** panel, and select **OS X** from the side menu.



15.2. Specific characteristics of the protection for Mac OS X

The protection for OS X has a series of unique characteristics that set it apart from the protection for Windows/Linux systems. These are as follows:

Configuring updates on OS X computers

In the case of OS X computers, it is not possible to configure the frequency of the automatic updates of the signature file. The signature file is updated every hour.

48 hours after the release of a version more recent than the file installed on a Mac OS X computer, this will appear as "out-of-date" in the **Status** window.

Frequency of protection updates on OS X computers

The protection for OS X computers is updated with the following frequency:

- Signature file: Updated every hour
- Protection settings: The agent checks for changes every 4 hours
- Detection information: Updated every 6 hours

- Computer status information: Updated every 12 hours

Automatic updates of the protection engine (upgrades)

The protection of OS X computers is updated automatically, even though you can disable this feature from the administration console.

72 hours after the release of a version more recent than the protection installed on a Mac OS X computer, this will appear as "out-of-date" in the **Status** window.

During the installation process you will have to uninstall the previous version and install the new one.

15.3. General protection settings

Click **OS X** in the menu on the left to access the general protection settings.

Scheduled scans

Select the **Scheduled scans** tab to create immediate, scheduled and periodic scan tasks of the entire computer or just certain components.

You can schedule scans of your hard disks only, or indicate the specific paths of the files or folders that you want to scan.

As you create scan tasks, these will appear on the **Scheduled scans** tab in the **Edit profile** window, from which you can edit them or delete them if desired.

Next, we describe the steps to configure a new scan task:

- Click **New** to go to the **Edit profile – New scan job** window.
- In the window that opens, enter the following data:
    - **Name**: Choose a name for the scan task.
    - **Scan type**: Select the type of scan that you want to create:
        - Immediate scan: Once configured, the immediate scan will take place as soon as the computer connects to the Adaptive Defense 360 server, and the solution checks that the protection configuration has changed.
        - Scheduled scan: The scan will take place at the time and date you set in **Start date** and **Start time**. Use the drop-down menu to select if the scan start time refers to the Adaptive Defense 360 server or the user's computer.
        - Periodic scan: Set the start date and start time, and select the scan frequency in the **Repetition** menu.
    - **Scan**: Select an option from:
        - Hard disks

          Other items: Use this option to scan specific items (files, folders, etc.). You'll have to enter the path of the item to scan.

          The path must start with /: *Example: /root/documents*

The permission that you have will dictate whether or not you'll be able to define specific paths to scan. The maximum number of paths to scan for each profile is 10.

- Click the **Advanced settings** link to access a window where you will be able to configure additional aspects of the scheduled scans:
    - Select the relevant checkbox to scan compressed files.
    - Select the malicious software you want to scan for. The option to scan viruses will always be enabled.
    - You can scan the entire computer or exclude certain folders or files with specific extensions from the scans. In the latter case, use the **Add**, **Delete** and **Clear** buttons to define the list of exclusions.

15.4. Configuring the antivirus protection

Select the **Enable permanent file protection** checkbox to protect the file system on your Mac OS X computers.

Exclusions

This section allows you to configure items, folders, etc. that will not be scanned by Adaptive Defense 360

16. Android protection profiles

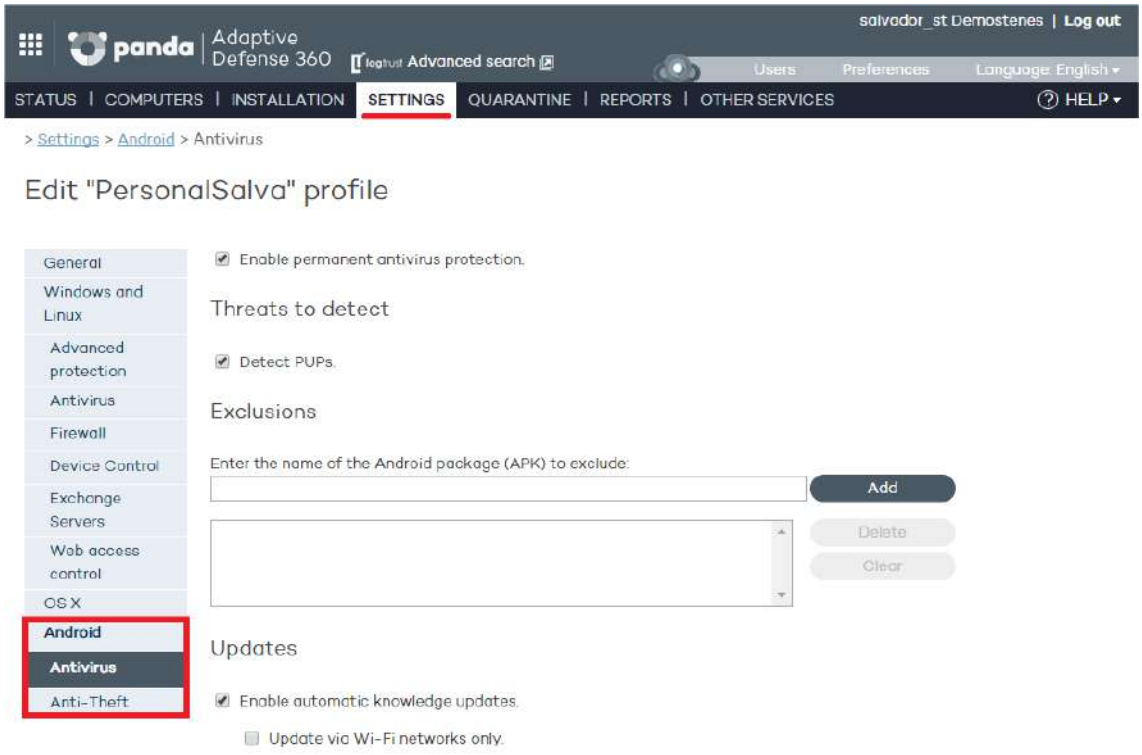
Configuring the antivirus protection

Configuring the Anti-Theft protection

16.1. Introduction

To configure the security profile for an Android tablet or smartphone, go to the **Settings** window. Select the profile to configure from the **Profiles** panel, and click **Android** from the side menu.

The Android protection module is divided into two sections: Antivirus and Anti-Theft.



16.2. Configuring the antivirus protection

The antivirus protection for Android smartphones protects corporate devices against the installation of malware-infected apps and PUPs, scanning both the devices and their SD memory cards on access and on demand.

Select the **Enable permanent antivirus protection** checkbox to enable malware detection. Additionally, select the **Detect PUPs** checkbox to also detect potentially unwanted programs.

Exclusions

The Android protection allows you to exclude installed apps from the scans. To do this, follow the steps below:

- Enter the name of the Android package (.apk) that you want to exclude, and click **Add**.
- Use the **Delete** and **Clear** buttons to clear or edit the contents of the list of exclusions.

Updates

To update the signature file automatically, select **Enable automatic knowledge updates**. Additionally, you can choose to update the protection exclusively through Wi-Fi networks to avoid extra data charges.

Scheduled scans

To schedule a scan, click the **New** button.

Use the options in the **New scan job** window to configure the scan type: immediate, scheduled or periodic.

As you create scan tasks, these will appear on the list of scheduled scans for the profile whose antivirus protection you are configuring. You can edit or delete them from there.

- **Immediate scan**: Once you have configured the scan, it will take place as soon as the device connects to the Adaptive Defense 360 server.
- **Scheduled scan**: The scan will take place at the configured date and time. For that to happen, you need to configure the scan sufficiently in advance. If there is no connection to the Adaptive Defense 360 server at the scheduled date and time, the scan will take place as soon as the connection is re-established.
- **Periodic scan**: The scan will take place at the date and time that you set in the corresponding fields with the corresponding frequency. As with scheduled scans, it is advisable to configure periodic scans sufficiently in advance to ensure there is connection with the Adaptive Defense 360 server. Otherwise, the scan will take place as soon as the connection is re-established.

16.3. Configuring the Anti-Theft protection

The Anti-Theft protection included in Adaptive Defense 360 will give you total control over the company's Android devices, and will allow you to take a series of actions in case of loss or theft.

Namely, you will be able to locate, lock and wipe the devices, take a picture of the thief, and send it by email to an address of your choice.

To enable this feature, select the **Enable Anti-Theft protection** checkbox.

- **Report the device's location**: Select this checkbox If you want the protection to automatically report the device's location.

- **Take a picture after three failed unlock attempts and email it to the following addresses**: Select this checkbox if you want to receive an email when there is activity on a stolen device. Then, enter the email address(es) that the picture of the potential thief will be sent to. Use a semicolon (;) to separate them. If, together with the option to snap a picture of the thief, you select the option to report the device's location, the email received will include a photo plus a map showing its location.

Once you have finished configuring the protection, go to the **Computer details** window to track the location of the device, lock it, and change the email address for the **Snap the thief** feature.

Privacy mode

Administrators can allow end users to use their devices in privacy mode. This allows the end user to disable the options to automatically report the device's location and take a picture of the thief, which will be password-protected.

When enabling the privacy mode, the Adaptive Defense 360 agent will prompt the end user to set a personal 4-digit access code. Then, the administrator will have to enter this code in the administration console if they want to make use of the device location and snap the thief features.

17. Visibility and monitoring

Dashboard

Detections

Lists of incidents and malware detected

Network computer status

17.1. Introduction

Adaptive Defense 360 offers network administrators four major groups of tools to view the security status of their IT resources:

- The dashboard with real-time information.
- Lists of incidents and malware detected.
- Lists of computers and network devices.
- Consolidated reports with data compiled over time.

The consolidated reports are discussed in Reports chapter.

These four tools enable administrators to accurately appraise the risk of infection to the managed computers.

The end goal of the viewing and monitoring tools is to be able to determine the impact of any security breaches and to take any necessary action, either to mitigate the effects or to prevent similar situations in the future.

17.2. Dashboard

The Adaptive Defense 360 dashboard is available in the **Status** window and is divided into two main areas: **Activity** and **Detections**. Each section contains a series of panels with information that enables administrators to get an immediate picture of the security status of their network.

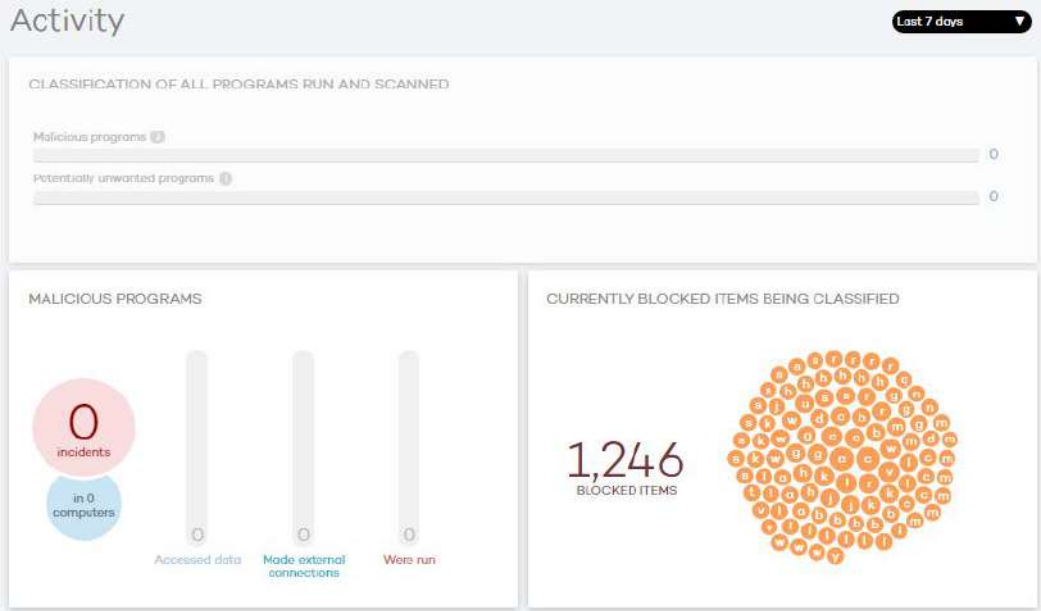
The panels displayed in the dashboard are generated in real time and are interactive: move the mouse pointer over the items to display tooltips with further information and click the items to open windows with detailed information.

The dashboard displays information for the time period established by the administrator using the tool at the right of the **Status** window. The options are:

- **Last 24 h**
- **Last 7 days**
- **Last month**
- **Last year**

Below we describe the various panels and their purpose.

17.2.1. Activity section



The **Activity** section shows a classification of all of the programs run and scanned on the network's Windows computers, as well as the security incidents detected and the number of currently blocked items being classified by the system.

Adaptive Defense 360 reports an incident in the **Activity** section for each computer-threat-threat type triplet found. If the cause of a specific incident does not disappear, a maximum of two detections will be reported every 24 hours for each computer-threat-threat type triplet that requires the administrator's attention.

The **Activity** section is divided into the following areas:

- **Malicious programs**
- **Potentially unwanted programs**
- **Under investigation at our lab**

17.2.2. Classification of all programs run and scanned

The purpose of this panel is to quickly display the percentage of goodware and malware items seen and classified on the client's network during the time period selected by the administrator. The panel displays three horizontal bars, along with the number of events associated to each item category and a percentage over the total number of events.

> ***The data in this panel corresponds to the entire IT network, not only to those computers that the administrator has permissions on based on the credentials used to log in to the console. Unclassified items are not shown in the panel.***

- Trusted programs: Applications seen on the client's network which have been scanned and classified as goodware.
- Malicious programs: Applications seen on the client's network which have been scanned and classified as malware.
- Potentially unwanted programs: Applications seen on the client's network which have been scanned and classified as PUP.

Clicking any item displays the **Malware Status** or **PUP Status** windows, discussed later in this chapter.

17.2.3. Malicious programs and potentially unwanted programs

The information displayed in these panels refers to those computers that the administrator has permissions on based on the credentials used to log in to the console. If the administrator does not have permissions on all computers on the network, a warning will be displayed at the top of the panel.

- Number of incidents/alerts detected
- Number of computers with incidents detected
- Accessed data: Number of alerts that include one or more attempts to access information on users' hard disks.
- Outbound connections: Number of incidents that involve connections to external computers.
- Run: Number of malware samples that have been run.

Malicious programs and potentially unwanted programs show data with a maximum interval of 1 month. In the event that the administrator set a longer period explanatory text at the top of the panel is displayed.

Clicking these items will take you to the **Status - Malware** or **Status - PUP** windows.

17.2.4. Currently blocked items being classified

This panel shows every unknown process detected on the network that requires further analysis by Panda Security Labs in order to be classified as goodware or malware. Depending on the way the protection has been configured (Lock, Hardening or Audit), these item may be blocked during the time it takes to classify them.

The information displayed in this section is a history of all the items that have been blocked and are pending classification since the service was implemented on the customer's network until the current time, and is not affected by the time period selected by the administrator.

The total number of temporarily blocked items indicates the different applications (different MD5) that are being blocked. This number is independent of the number of run attempts performed by each blocked application. Some bubbles may have the same malware name. This is typical of malware that uses polymorphic techniques to avoid being detected by signature-based traditional antivirus solutions. Every variant of the same malware that has a different MD5 is shown independently.

Each application is counted once only. That is, even if an application tries to run several times on the same computer, it will only be counted once. The size of each bubble is an indicator of the number of computers where the malware was found and blocked.

Example:

Suppose the dashboard displays a total of eight currently blocked items pending classification. Each item will be represented with a circle.

Suppose one of the applications tried to run thirty times on the same computer on the same day. As all those attempts took place on the same computer and on the same day, they will count as only one of the eight detections shown in the panel.

Blocked applications are indicated with a color code:

- Orange: For applications with a medium probability of being malware.
- Dark orange: For applications with a high probability of being malware.
- Red: For applications with a very high probability of being malware.

Move the mouse pointer over a circle to display the application's full name and a series of icons representing key actions:

- Folder: The program has read data from the user's hard disk.
- Globe: The program has connected to another computer.

Click the number of blocked items or any of the circles in the panel to access detailed information.

17.3. Detections section

The Detections section displays all of the intrusion attempts managed by Adaptive Defense 360 in the selected period.

The data shown corresponds to all infection vectors and all supported platforms so that the administrator can have specific information (volume, type, attack method) on the malware found on their computes over a specific period of time.

The Detections section is divided into the following panels:

17.3.1. Detected threats

This panel includes two sections: a line graph and a list.

The line graph displays the evolution of threats detected on the network divided into malware types.

- **Viruses and spyware**
- **Hacking tools and PUPs**
- **Suspicious items**
- **Phishing**
- **Other**

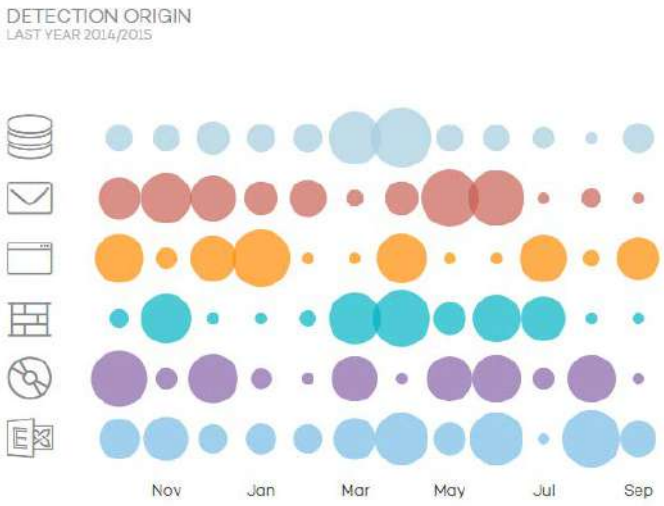
The Y axis shows the number of incidents and the X axis the date.

To simplify the content of the panel, move the mouse pointer over each category at the bottom of the graph and the others will disappear.

The list on the right shows the actions which, although not directly related with the malware detected, are nevertheless important in drawing administrators' attention to potentially dangerous situations.

- **Intrusion attempts blocked**: These are attacks blocked by the firewall and the intrusion prevention system.
- **Devices blocked**: Devices blocked by the device control module.
- **Dangerous actions blocked**: Detections made by the local behavior analysis.
- **Tracking cookies**: Cookies detected that monitor users' Internet movements.
- **Malware URLs blocked:** Web addresses that point to pages containing malware.

17.3.2. Detection origin



This panel displays the infection vectors used by the malware discovered on the network.

The Y axis contains a series of icons displaying the infection vector:

- **File system**
- **Local email**
- **Internet**
- **Firewall / Intrusion detection system**
- **Device control**
- **Exchange server**

The X axis shows the date of the selected period.

This graph contains a series of different sized circles of different colors. The size of the circle reflects the number of detections. Move the mouse pointer over the circle to see a tooltip to see the number of detections for a certain date and infection vector.

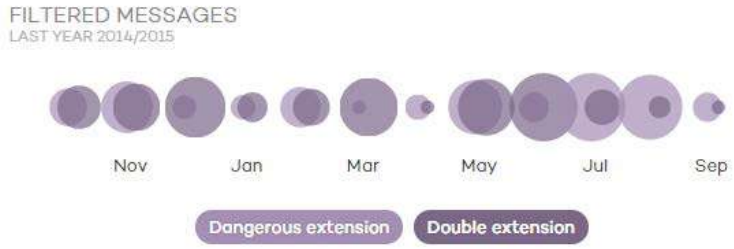
17.3.3. Detected spam

This panel shows the amount of spam detected in the Exchange server.

The X axis shows the dates of the selected period.

This graph contains a series of different sized circles. The size of the circle reflects the number of detections. Move the mouse pointer over the circle to see a tooltip to see the number of detections for a certain date.

17.3.4. Filtered messages

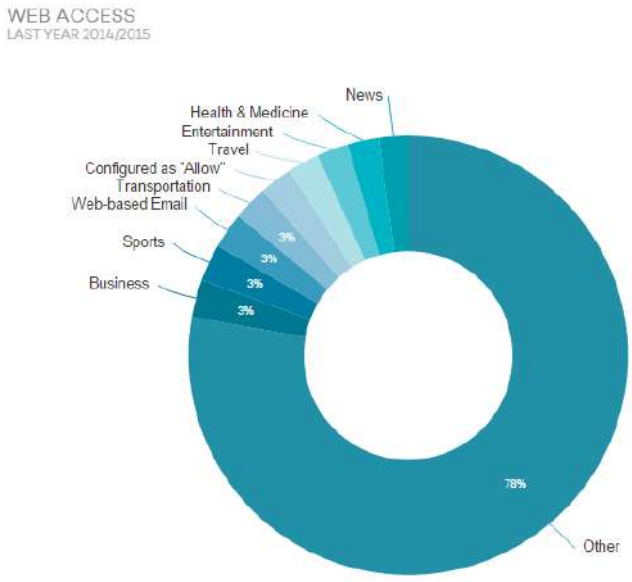


This panel shows the number of messages that were filtered by the Exchange server content filter.

The X axis shows the dates of the selected period.

This graph contains a series of different sized circles. The size of the circle reflects the number of detections. Move the mouse pointer over the circle to see a tooltip to see the number of events for a certain date.

17.3.5. Web access



This panel shows a pie graph representing the Web page categories requested by network users. Pass the mouse pointer over each segment to see the number of requests for each category.

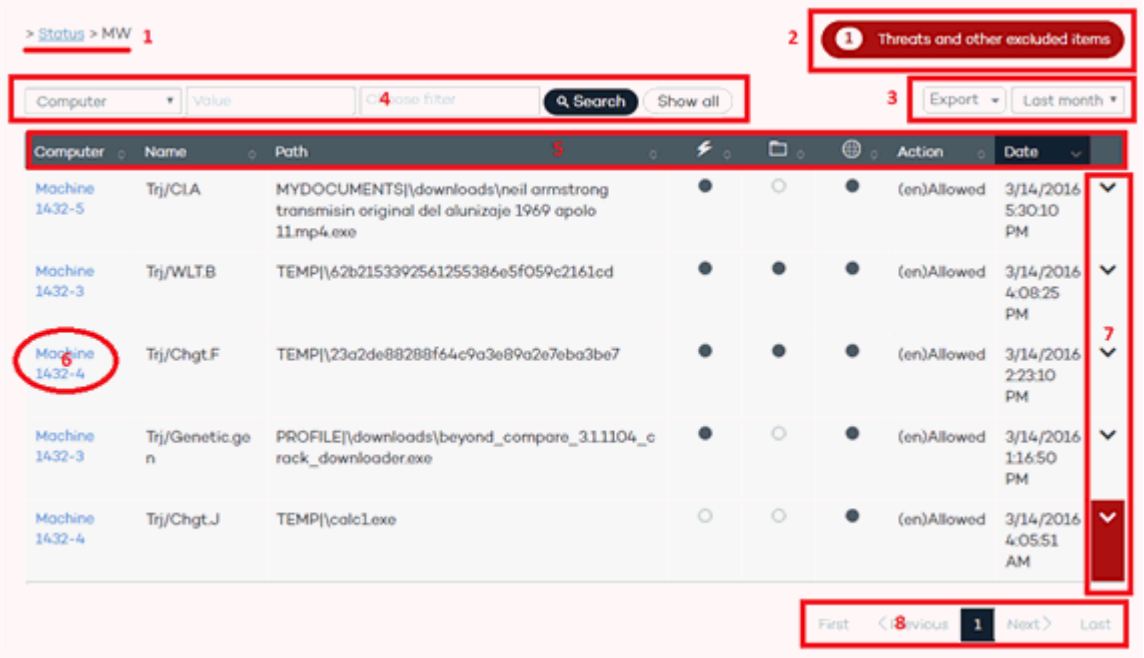
17.4. Lists of Activity section

Click the different panels in the **Activity** section to display reports and detailed lists of the malware or software under analysis found on the client's network.

The purpose of these lists is to provide administrators with the necessary information to find the source of a problem, assess the severity of an incident and, if required, take the necessary remediation measures to update the company's security policies.

These lists also allow administrators to add exclusions and unblock blocked items under analysis. See later in this document for more information about the exclusion and unblock operations supported by the solution.

All of these lists have the same structure:



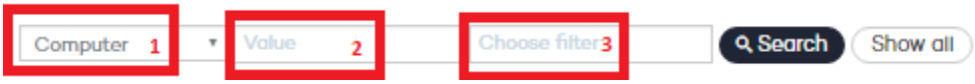
1. List name. Notification regarding the existence of files classified as malware by Adaptive Defense 360 and which have been allowed to run by the administrator.
2. Time interval combo box and list export tool. The time period combo box allows the administrator to apply the following time filters to the list: last 24 hours, last day, and last month. The export tool allows administrators to save the list to an Excel or CSV file.
3. Filter tool. Each list incorporates its own filters based on the data it contains. These are explained in the relevant sections.
4. You can sort the data in the tables by clicking the column headers.
5. Click a computer's name for extended information.
6. Drop-down arrow with information about the malware actions. Refer to chapter **Forensic analysis** for more information about the actions performed by the detected malware.
7. Refer to chapter **Remediation tools** for more information about the remediation tools provided by Adaptive Defense 360.
8. Pagination controls for easier browsing.

17.4.1. MW list

Click any of the items in the **Malicious programs** panel, or **Malicious programs in the Classification of all programs run and scanned** panel, to view a list of the threats found on the computers protected with Adaptive Defense 360.

The screen provides different filters to filter the information displayed.

At the top there is a search tool:



Filter 1 restricts the search indicated in the text box to its right:

- **Computer**: The search string will be applied to the computer name.
- **Name**: The search string will be applied to the malware name.
- **Date**: The search string will be applied to the date of detection.

Filter 3 shows those threats that match the selected criteria:

- **Run**: The malware was run and the computer is infected.
- **Not run**: Malware detected by the vulnerability protection.
- **Blocked**: Malware identified by Adaptive Defense 360 and prevented from running.
- **Allowed by the end user**: Malware identified by Adaptive Defense 360 and allowed to run by the user.
- **Access to data files**: The malware accessed the disk to collect information from the computer, or to create the files and resources necessary for its execution.
- **Communications**: The malware created sockets for communicating with other computers, including localhost.
- **Deleted.**
- **Disinfected:** The file was disinfected by the antivirus.
- **Quarantined:** The file cannot be disinfected and was sent to quarantine.

The table fields are as follows:

- **Computer**: Computer where the detection took place.
- **Name**: Malware name.
- **Path**: Full path to the infected file.
- **Was run**: The malware was run and the computer might be infected.
- **Accessed data**: Indicates whether the threat sent or received data from other computers.
- **Made external connections**: The threat has communicated with remote computers to send or receive data.
- **Action**: Action taken on the malware (block, allow, quarantine, delete, disinfect, allow by the user, etc.).
- **Date**: Date when the malware was detected on the computer.

17.4.2. Currently blocked items being classified

This panel shows a list of those files in which Adaptive Defense 360 has detected risks despite their classification is not fully complete.

These files are blocked during the time it takes to fully classify them.

At the top of the screen there is a search tool:

Section 1 allows you to display every item that was blocked since Adaptive Defense 360 was installed on the network (blocking history) or only those that are currently blocked.

Filter 2 restricts the search indicated in the text box to its right:

- **Computer**: The search string will be applied to the computer name.
- **Name**: The search string will be applied to the name of the blocked file.
- **Date**: The search string will be applied to the date when the item was blocked.
- **MD5:** The search string will be applied to the digest value of the blocked file.

Filter 4 filters the items on the list by the protection mode in which Adaptive Defense 360 was configured when blocking the item, as well as the actions taken by the file (only if the file was allowed to run before being blocked and its actions were logged by the system).

The **Currently blocked** table fields are as follows:

- **Computer.**
- **Name**: Malware name.
- **Path:** Full path to the item.
- **Accessed data**: Indicates whether the threat sent or received data from other computers.
- **Made external connections**: The threat has communicated with remote computers to send or receive data.
- **Protection mode**: Specifies the mode that the protection was configured in at the time of blocking the item.
- **Likelihood of being malicious**: Medium, high, very high.
- **Date.**

The **History** table fields are as follows:

- **Computer.**
- **Name**: Malware name.
- **Path:** Full path to the item.
- **Action.**
- **Accessed data**: Indicates whether the threat sent or received data from other computers.

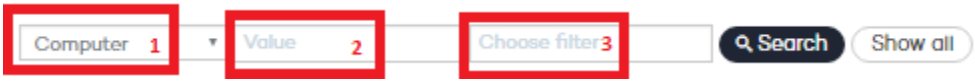
- **Made external connections**: The threat has communicated with remote computers to send or receive data.
- **Protection mode**: Specifies the mode that the protection was configured in at the time of blocking the item.
- **Excluded**: Indicates whether or not the item was excluded from monitoring.
- **Likelihood of being malicious**: Medium, high, very high.
- **Date.**

17.4.3. PUP list

Click any of the items in the **Potentially Unwanted Programs (PUP)** panel to view a list of the threats found on the computers protected with Adaptive Defense 360.

The screen provides different filters to filter the information displayed.

At the top there is a search tool:



Filter 1 restricts the search indicated in the text box to its right:

- **Computer**: The search string will be applied to the computer name.
- **Name**: The search string will be applied to the PUP name.
- **Date**: The search string will be applied to the date of detection.

Filter 3 shows those threats that match the selected criteria:

- **Run**: The PUP was run and the computer is infected.
- **Not run**: PUP detected by the protection against vulnerabilities.
- **Blocked**: PUP identified by Adaptive Defense 360 and prevented from running.
- **Allowed**: PUP identified by Adaptive Defense 360 and allowed to run by the user.
- **Access to data files**: The PUP accessed the disk to collect information from the computer, or to create the files and resources necessary for its execution.
- **Communications**: The PUP created sockets for communicating with other computers, including localhost.

The table fields are as follows:

- **Computer**: Computer where the detection took place.
- **Name**: PUP name.
- **Path**: Full path to the PUP file.

- **Was run**: The PUP was run and the computer might be infected.
- **Accessed data**: Indicates whether the PUP sent or received data from other computers.
- **Made external connections**: The PUP has communicated with remote computers to send or receive data.
- **Action**: Action taken on the PUP (block, allow, quarantine, delete, disinfect, allow by the user, etc.).
- **Date**: Date when the PUP was detected on the computer.

17.4.4. Detection details list

This list offers consolidated and complete information about all detections on all platforms and from all supported infection vectors used by hackers.

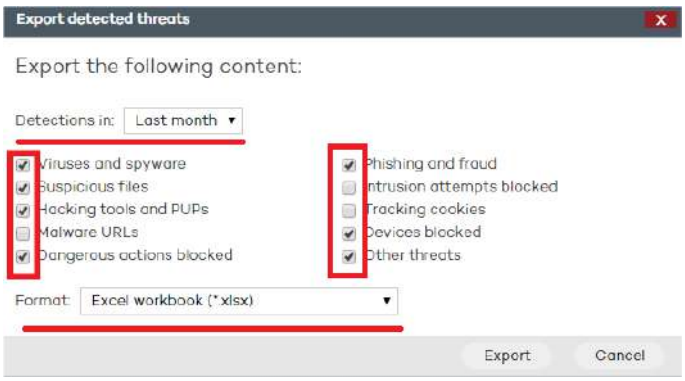
To display this list, click the Detected threats or Detection origin panels, in the Detections area of the dashboard.

The information is presented in three lists:

- **Detected threats**
- **Computers with most threats**
- **Most detected malware**

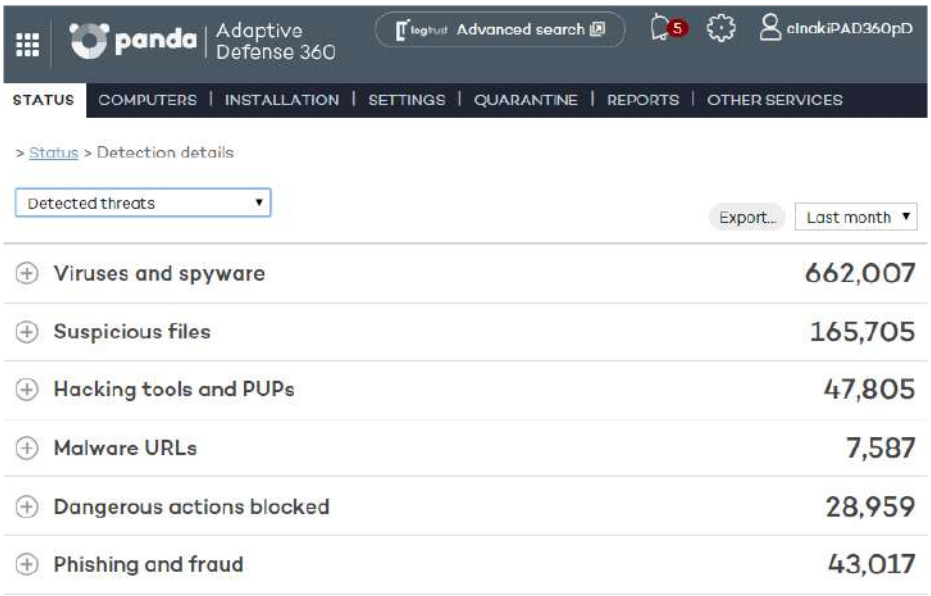
The top toolbar lets you choose the list to display, set the time period and export the data to a file. Click Export to display a window from which you can choose:

- The type of event to export
- File format (Excel, CSV)
- Time period (last 24 hours, last month, last year)



List of detected threats

This displays a list of threats and dangerous events seen on the network and grouped by type:

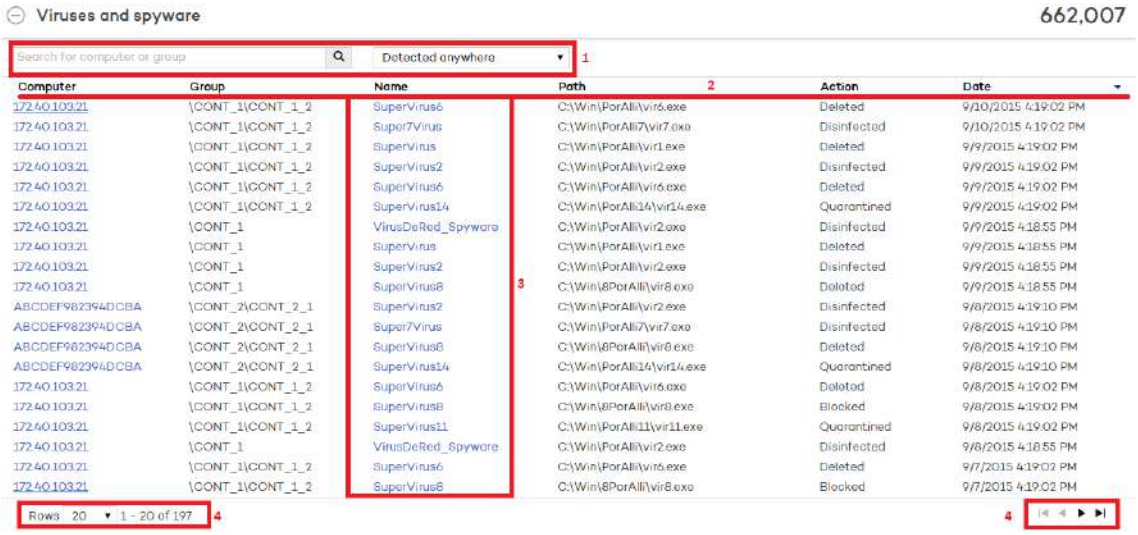


The groups are as follows:

- **Viruses and spyware**
- **Suspicious files**: This displays the files classified as suspicious by the Adaptive Defense 360 heuristic analysis.
- **Hacking tools and PUPs**
- **Malware URLs**: URL pointing to a page containing malware.
- **Dangerous actions blocked**: This displays the files classified as suspicious by the behavior analysis techniques.
- **Phishing and fraud**
- **Intrusion attempts blocked**: Detections of malformed traffic.
- **Tracking cookies**: Displays the cookies used to spy on users browsing habits.
- **Devices blocked**: Peripheral devices connected to a user's computer that have been blocked by the administrator.
- **Other threats**: Detection of malware not classified within the above categories (Jokes, etc.)

There is a counter for each group with the number of events during the chosen time period and the type of malware.

Click the ⊕ icon of a specific group to display the content as illustrated below.



1- Tools for filtering the information in a group:

The controls displayed will depend on the type of group:

- Group or computer search
- Place where the item was detected:
  - **Anywhere**
  - **In the file system**
  - **In Exchange server**
  - **In email**
- Type of device:
  - **All devices**
  - **Removable storage drives**
  - **Imaging devices**
  - **CD/DVD drives**
  - **Bluetooth devices**
  - **Modems**
  - **Mobile devices**
- Number of rows to display
- Pagination tool

2- Information about detected items.

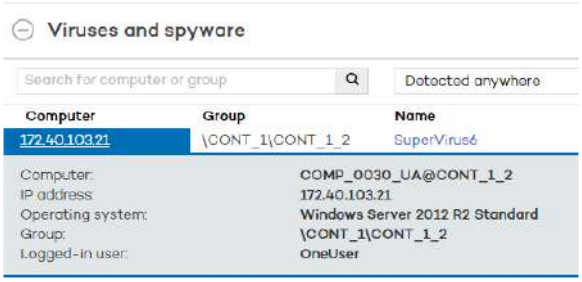
The columns displayed will depend on the type of group

- **Computer**: Name of the computer where the detection took place.
- **Group**: Group to which the computer belongs.
- **Name**: Name of the threat.
- **Path**: Path of the file system where the threat was detected.
- **Action**: Action taken by Adaptive Defense 360**.**
  - **Deleted**: The malware could not be disinfected and has been deleted.

- **Disinfected**
- **Quarantined**
- **Blocked:** The malware has been blocked
- **Process ended:** The malware was running and Adaptive Defense 360 killed the process.

3- Information about specific items

Clicking any item displays further information.

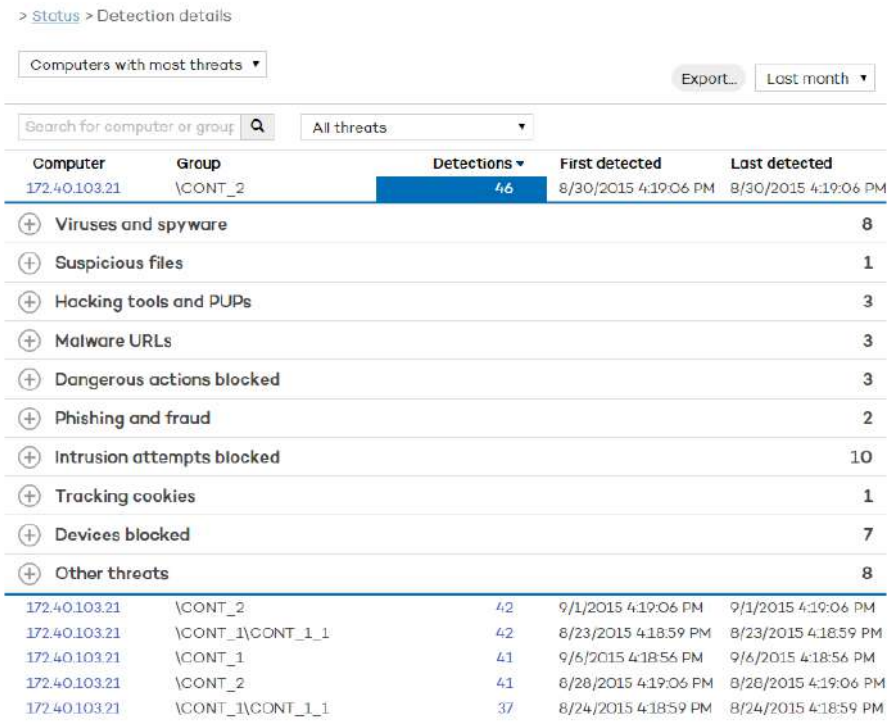


4- Pagination tool

This lets you establish the number of lines to display in the group and lets you move between pages.

Computers with most threats

This list adds another level with respect to the **Detected threats** list, as it first displays the computers with most detections and, by clicking each computer, then displays a breakdown of the types of detections, like the list of **Detected threats**.

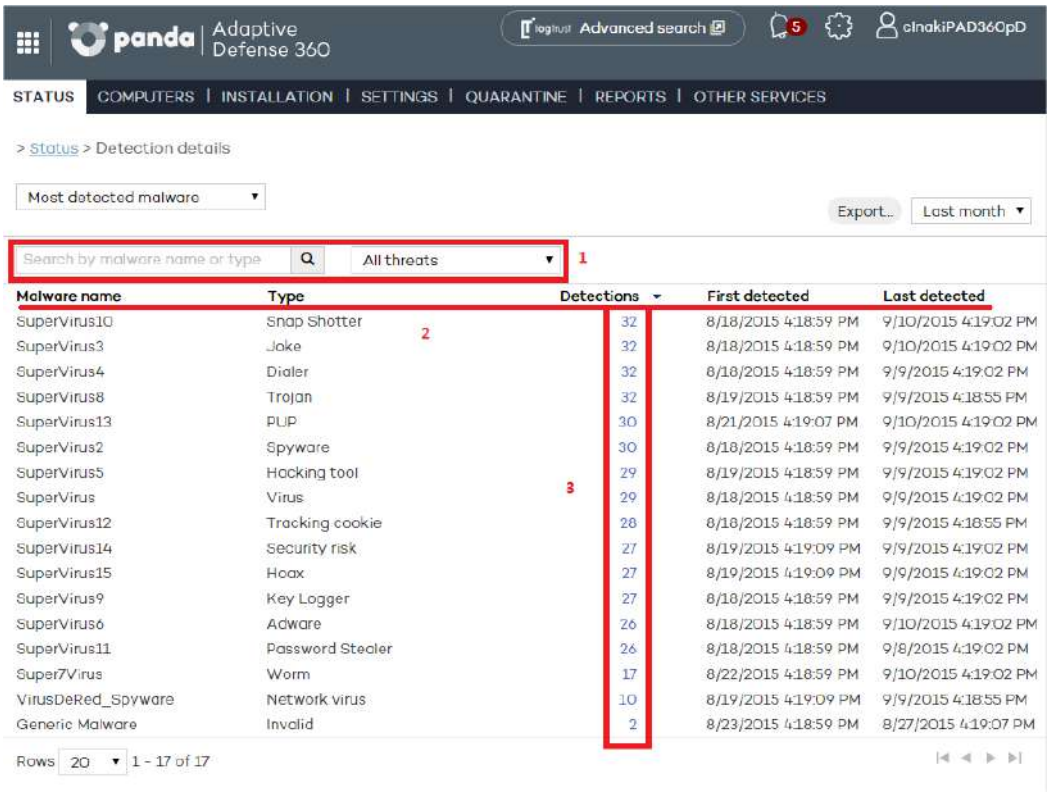


1- Information for the detected items.

- **Computer**
- **Group**
- **Detections**
- **First detected**: Date of the first detection during the period
- **Last detected**: Date of the last detection during the period

Most detected malware

This displays a list of the malware most frequently encountered on the customer's network.



1- Tools for filtering the information in the list

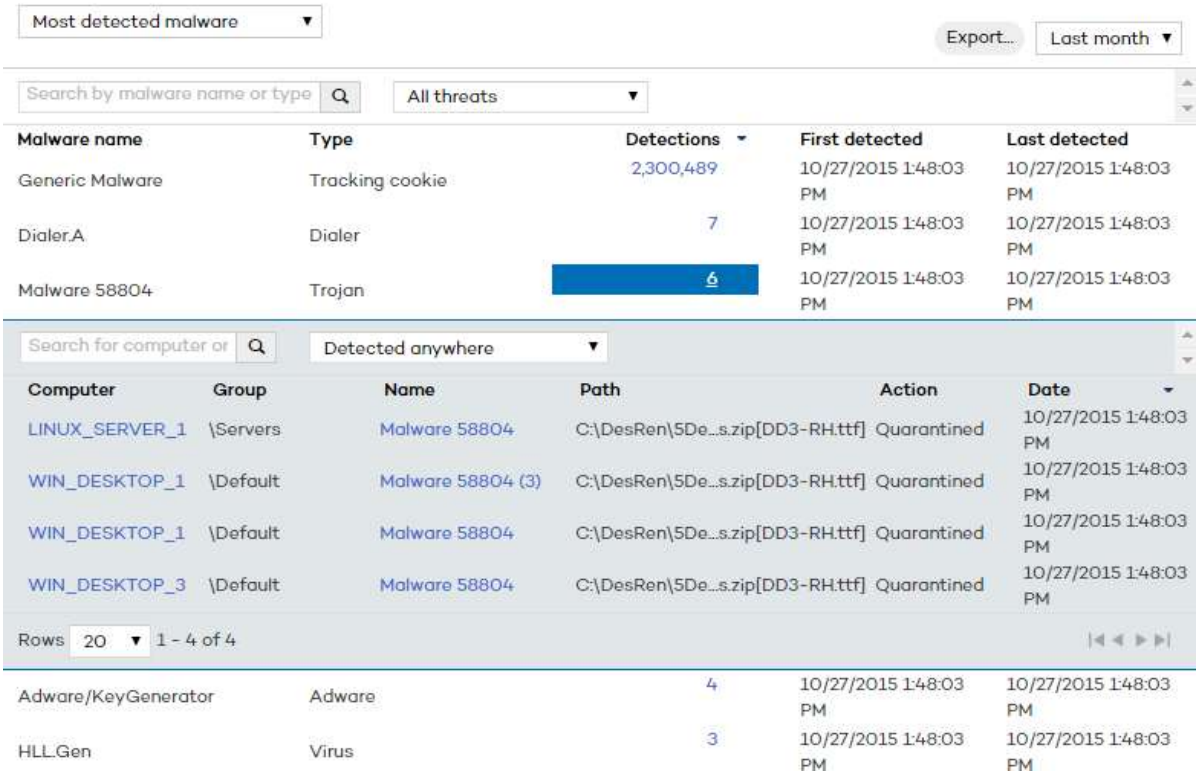
- Name or type of threat: Enter the name or type of threat.
- Type of threat: Select the type of threat from the list.
    - **Viruses and Spyware**
    - **Hacking tools and PUPs**
    - **Tracking cookies**
    - **Other threats**

2- Information about detected items

- **Malware name**
- **Type**
- **Detections**
- **First detected**
- **Last detected**

3- Information about specific items

Click the number of detections of a specific threat to display the list of **Detected threats.**



17.4.5. Web access list

Click the **Web access** panel to display a list with consolidated and complete information on users' access to Web page categories.

This list is divided into four panels:

- Most accessed categories (top 10)
- Computers with most access attempts (top 10)
- Most blocked categories (top 10)
- Computers with most access attempts blocked (top 10)

Each panel has a **See full list** link which displays the full list for each category.

17.5. Network computers status

The dashboard provides a brief summary of the protection status of the entire network.

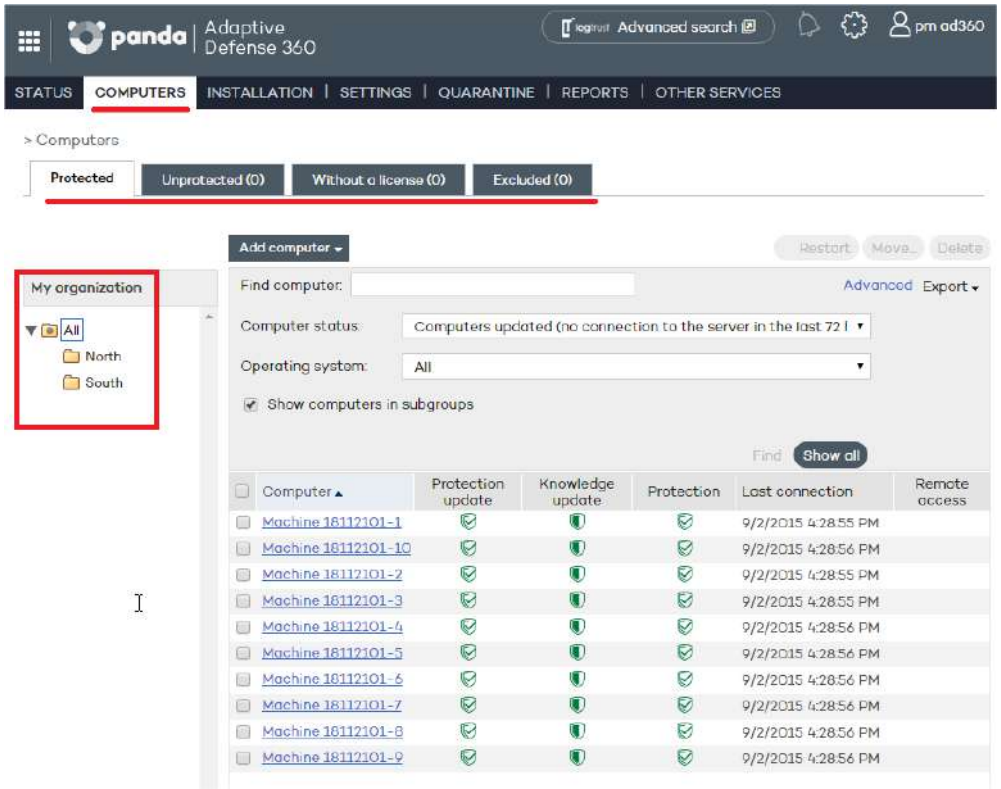
This section displays the computers that require the administrator's attention:

- Computers that have not connected to the server in the last 72 hours, 7 days and 30 days.
- Computers with outdated protection: the engine, the signature file and those that need a restart to apply an update to the engine of the downloaded protection.

Click the various items in the panel to display the **Protected** tab in the **Computers** window, which is explained below.

The following items are displayed in the **Computers** window to improve monitoring of the IT resources and enable searches for devices:

- The group tree
- Status tabs
- Search tools
- A window with details of the computer or device



17.5.1. Group tree

The group tree on the left-hand side of the window lets you move through the different group levels and see the computers included in each group. Click **All** to obtain the list of all network computers.

17.5.2. Tabs

There are four groups each reflecting the protection status of the computers:

Protected

Unprotected

Without a license

Excluded

Protected

Computers with the Adaptive Defense 360 agent correctly installed and with a valid license assigned, although they could have outdated protection or an error in the protection.

Unprotected

This includes cases where the agent is in the process of installation or removal, the protection has been uninstalled, as well as computers that have been discovered with the discovery tool.

Without a license

These are computers that had a valid license assigned in the past but the corresponding license contract has expired and consequently they are unprotected. This also includes computers that belong to a group with restrictions on the maximum number of licenses or on the expiry date and the computer has not met these conditions.

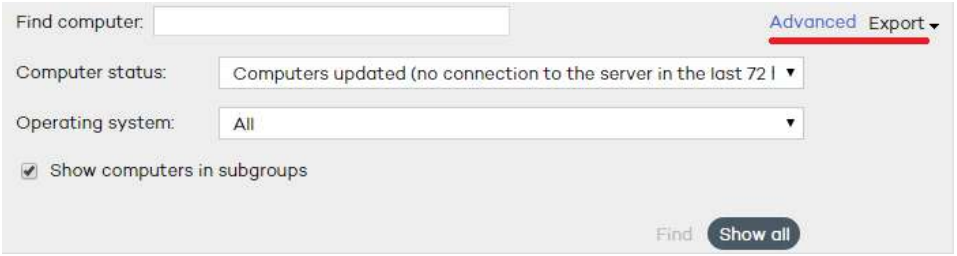
Excluded

These are computers with an Adaptive Defense 360 agent installed but that don't compete for a valid license. Administrators can manually exclude computers when the number of valid licenses contracted is lower than the number of computers on the network to protect.

17.5.3. Search tools

The list of computers can be filtered using various criteria depending on the selected tab.

In some tabs, moreover, there is an **Advanced** button. Click this to show or hide other search criteria.



There is also a **Show all** button, which overrides any filters and displays all computers in the selected tab.

Below you can see the search options and criteria for each of the tabs.

Protected tab

- **Find computer**: Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'
- **Computer status**:
  - **All**
  - **Computers with all protections enabled**
  - **Computers with all protections disabled**
  - **Computers with up-to-date protection**
  - **Computers with out-of-date protection**
  - **Computers with partially enabled protection:** Computers with any of the protection modules disabled.
  - **Computers with protection errors**
  - **Computers pending restart**
  - **Computers with up-to-date knowledge**
  - **Computers with out-of-date knowledge**
  - **Updated computers (no connection to the server in the last 72 hours)**
  - **Updated computers (no connection to the server in the last 7 days)**
  - **Updated computers (no connection to the server in the last 30 days**)
- **Operating system**:
  - **All**
  - **Windows**
  - **Linux**
  - **Mac OS X**
  - **Android**
- **Show computers in subgroups**: Search in the group selected from the group tree and all its subgroups.

Unprotected tab

- **Find computer**: Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'
- **Computer status**:

- **All**
- **Unprotected computers**
- **Unmanaged computers:** Computers on the network without an agent installed and discovered by the discovery tool.
- **Computers installing the protection**
- **Computers uninstalling the protection**
- **Computers with errors during installation**
- **Computers with errors during uninstallation**
- **Computers with unknown name**

- **Operating system**:
  - **All**
  - **Windows**
  - **Linux**
  - **Mac OS X**
  - **Android**
- **Show computers in subgroups**: Search in the group selected from the group tree and all its subgroups.

Without a license tab

- **Find computer**: Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'

Excluded tab

- **Find computer**: Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'

17.5.4. Lists of computers

Once the search criteria is established, a list is displayed with the computers that meet the criteria.

This list is displayed as a table with a series of columns, which will vary depending on the tab describing the status of the computer.

Protected tab

- **Computer**: This shows the list of protected computers, presented either by their name or by their IP address. If different computers have the same name and IP address, they will be displayed as different computers in the Web console provided that their MAC address and administration agent identifier are different. If you want to change the way they are presented, go to the Preferences section (select the  icon at the top of the Web console). See Chapter 5: The Web administration console for more information.

- **Protection update**: This indicates the protection status. Move the mouse pointer over the icon to display the meaning of the icon and the protection version.
  -  Updated
  -  Not updated
  -  Awaiting restart
- **Knowledge update**: This indicates the status of the signature file. Move the mouse pointer over the icon to display the meaning of the icon and the update date.
  -  Updated
  -  Hasn't connected in the last 72 hours
  -  Not updated
- **Protection:** Indicates the protection level of the computer. Move the mouse pointer over the icon to display the protections enabled.
  -  All available protections are enabled
  -  Some of the available protections are disabled
  -  Systems with on-demand or scheduled protections
  -  One or more of the protections has an error
- **Last connection**: Date on which the computer last connected to the Adaptive Defense 360 server.
- **Remote access**: It means that the computer has at least one remote access tool installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer. If the computer has multiple tools installed, place the mouse pointer over the icon to display all of them. Select one to access the computer remotely. See Chapter 20 Remediation tools for more information.

Unprotected tab

- **Computer**: This shows the list of unprotected computers, presented either by their name or by their IP address. If different computers have the same name and IP address, they will be displayed as different computers in the Web console provided that their MAC address and administration agent identifier are different. If you want to change the way they are presented, go to the Preferences section (select the  icon at the top of the Web console). See Chapter 5: The Web administration console for more information.
- **Status**: This shows the status of the protection through a series of icons.
  -  Installed
  -  Uninstalled
  -  Uninstallation error

- o Installation error
- o Protection successfully uninstalled

- **Details**: Specifies the reason for the computer status. For example, if the status is **Installation error**, in **Details** you will see the error code. If the **Status** column shows **Unprotected**, the **Details** column will display **Protection uninstalled**.
- **Last connection**: This shows the date and time of the last connection with the computer.
- **Remote access**: If an icon is displayed in this column, it means that the computer has at least one remote access tool installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer.

Without a license tab

- **Computer**: This shows the list of computers without a license, presented either by their name or by their IP address. If different computers have the same name and IP address, they will be displayed as different computers in the Web console provided that their MAC address and administration agent identifier are different. If you want to change the way they are presented, go to the Preferences section (select the icon at the top of the Web console). See Chapter 5: The Web administration console for more information.
- **O.S.**: This shows the operating system and service pack version (in the case of Windows).
- **Reason**: This gives the reason why the computer doesn't have a license: insufficient valid licenses or the computer doesn't meet the restrictions of the group it belongs to.

Excluded tab

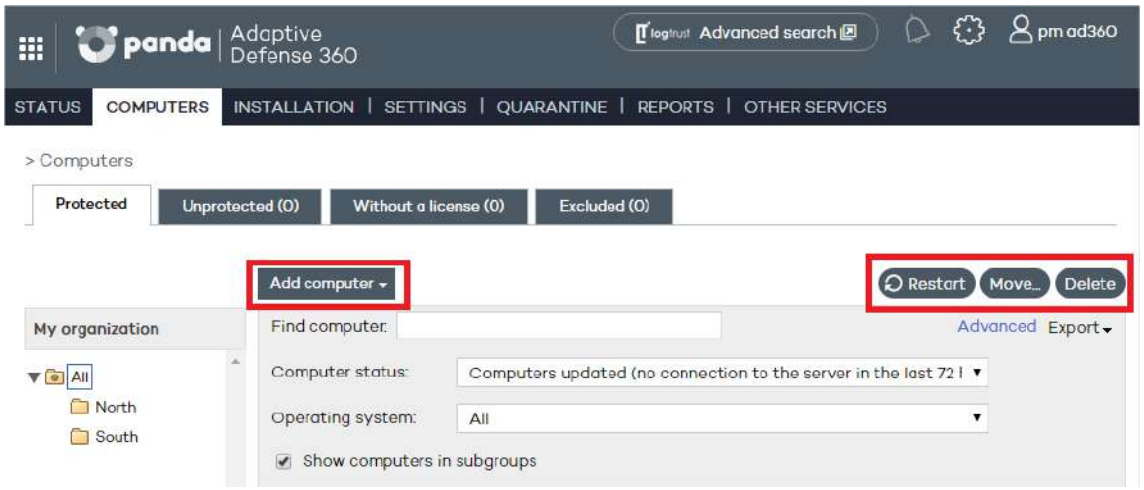
- **Computer**: This shows the list of excluded computers, presented either by their name or by their IP address. If different computers have the same name and IP address, they will be displayed as different computers in the Web console provided that their MAC address and administration agent identifier are different. If you want to change the way they are presented, go to the Preferences section (select the icon at the top of the Web console). See Chapter 5: The Web administration console for more information.
- **Group**

17.5.5. Actions on selected computers

All the lists have an initial selection column. Click the box at the top to select (or unselect) all items in the list.

At the foot of the table there is a pagination tool to ease navigation through the pages.

Select one or more computers in the table to take the actions available on the relevant tab.



Protected tab

- **Add computer**: This shows the Adaptive Defense 360 agent installation wizard for adding new computers to the administration console.
- **Restart**: This restarts the selected computers.
- **Move**: This lets you move the selected computers to another group.
- **Delete**: This option removes the computer from the Adaptive Defense 360 database, although if the agent is not deleted, it will reappear after the next connection.
- **Remote access:** This indicates that the computer has a remote access tool installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer. If the computer has multiple tools installed, place the mouse pointer over the icon to display all of them. Select one to access the computer remotely. See Chapter 20 Remediation tools for more information.

Unprotected tab

- **Delete selected computers:** The selected computers will be removed from the Adaptive Defense 360 database.
- **Delete all computers**
- **Exclude selected computers**

Without a license tab

- **Delete selected computers**
- **Delete all computers**
- **Exclude selected computers**

Excluded tab

- **Delete selected computers**
- **Delete all computers**

17.5.6. Details of Windows, Linux and Mac OS X computers

If you want to access detailed information about a computer, click on it. You will be taken to the **Computer details** window, where you will find information about the computer's status regardless of whether it is protected or not.

Computer details

- **Name**
- **IP address**
- **Domain**: Only in Windows computers
- **Active Directory path**: Only if the computer belongs to an Active Directory.
- **Group**
- **Installation date**
- **Protection version**
- **Agent version**
- **Knowledge date**: Signature file date
- **Last connection**
- **Operating system**
- **Mail server**
- **Comments**: Use the **Comments** field if you want to add additional information to identify the computer. If you are a user with monitoring permissions, you will not be able to use this field.

Protection

See Chapters 13, 14, 15 and 16 for more information about the protections provided by Adaptive Defense 360.

This displays the status of the protection modules (**Enabled**, **Disabled**, **Not applicable**).

- **Advanced protection.** This indicates the protection mode: **Monitor**, **Hardening**, **Lock**. It applies to Windows XP SP2 and later and Windows 2003 Server SP1and later.
- **File protection.**
- **Mail protection.**
- **Internet browsing protection**.
- **Firewall protection**.
- **Device control**.
- **Antivirus protection for Exchange Server**.
- **Anti-spam protection for Exchange Server**.
- **Content filtering for Exchange Server**.
- **Web Access control**.

Tools available

See Chapter 20 for more information about the Adaptive Defense 360 ***remediation tools***.

- **Disinfect computer:** Adaptive Defense 360 automatically disinfects malware detected. Computers compromised by advanced malware have the possibility to use **Panda Cloud Cleaner.** Click **Disinfect computer** to use it.
- **Report problem with this computer**: Use this option if you want to report a computer problem to Panda Security's qualified technicians.
- **Restart computers**: Use this to restart those computers which, for some reason, appear on the list of protected computers as requiring a restart.
- **Delete from database**: If you want to delete those computers that have not connected to the server for a long time, use the **Delete from database** option. You won't be able to access them or view any information about them.
- **Exclude**: Excluded computers will be shown in the list of excluded computers in the **Computers** window. No information or alerts will be displayed about them anywhere else in the console. You can undo these exclusions at any time.

17.5.7. Details of Android devices

In the case of Android devices, the **Computer details** window displays information about the device, and the status of its antivirus and Anti-Theft protection. See Chapter 20 for more information about the Adaptive Defense 360 remediation tools for Android.

If the Anti-Theft feature is enabled for a device, a map will be displayed showing its location and the options provided by the protection: wipe, lock, snap the thief and locate.

If any of the protections displays an error, click the **How to fix errors** link to view a series of troubleshooting instructions to help you resolve the issue.

Computer details

The details here are the same as for Windows computers, except:

- **IP address**: Not displayed
- **Domain**: Not displayed
- **Active Directory Path**: Not displayed
- **Device ID**: Character string identifying the device in Adaptive Defense 360

Protections

This displays the protection modules enabled:

- **Antivirus protection**
- **Anti-Theft protection**

Tools available

- **Wipe device**: Use the **Wipe** button to erase all the data on the device and restore its original factory settings.
- **Lock device**: Click the **Lock device** button to prevent access to it. Enter a four-digit unlock code.
- **Snap the thief:** This feature automatically takes a picture of anyone interacting with a stolen device. Enter the email address to send the picture to.
- **Privacy mode:** Administrators can allow end users to use their devices in privacy mode. This allows the user to disable the options to automatically report the device's location and take a picture of the thief, which will be password-protected.
- **Task list:** Shows a list of the tasks run on the device from the Web console. For more information, refer to the **Task list** section.

Task list

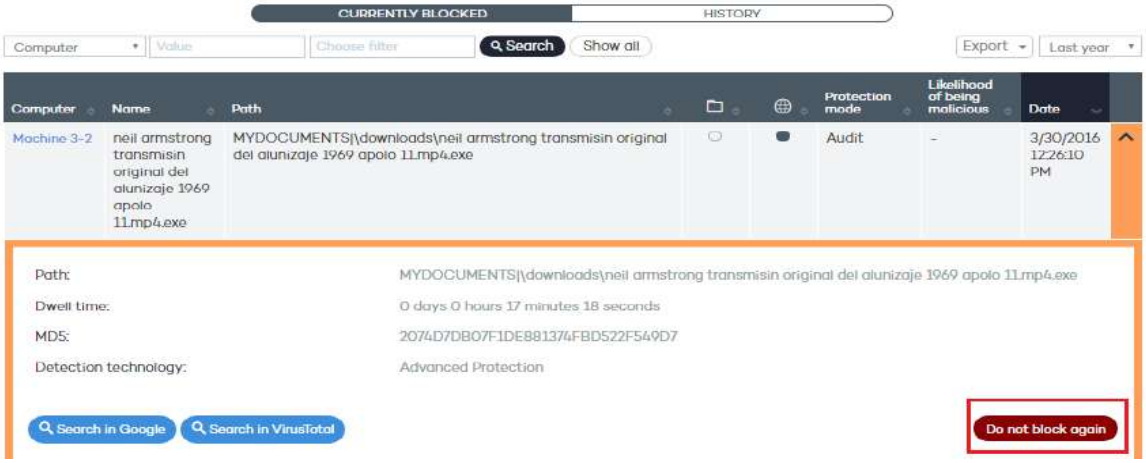
The **Computer details** window shows a list of every task (theft alerts, wipe and locate) sent from the Web console to be run on the Android device.

The list shows a status for each task. For example: If there are three theft alert tasks, one of them will appear as **Run**, another one will appear as **Received** and the third one will be **Pending**. As the first task finishes and is removed from the list, the **Received** task will change its status to **Run** and the **Pending** task will change to **Received**.

- **Pending:** Tasks will appear as **Pending** during the time that elapses between the moment that the task is configured in the Web console and the moment that it is received at the device. Bear in mind that if the device is turned off or offline, the task will also appear as **Pending**.
- **Received:** In this case, the device has received the task but has not run it yet or the task is in progress and has not finished. For example, in the case of a locate task, the task will appear as **Received** until the device is effectively located. In the case of a snap the thief task, it will appear as **Received** as long as no picture is actually taken. That is because the task is not considered to be run until the thief triggers it, that is, touches the device screen.
- **Run:** A task will appear as **Run** once the device reports that it has been completed (successfully or not).

17.6. Managing exclusions and blocked items

Adaptive Defense 360 will block unclassified programs depending on the protection mode selected. However, if users cannot wait for the system to automatically unblock a file once it has been classified, the administrator can use the button **Do not block again** in the **Currently blocked items being classified** window.



It is very important that you don't unblock any items unless you are completely sure that they are not harmful.

Bear in mind that should an item be finally classified as malware, unblocking it before being categorized will allow it to perform the malicious actions that it was designed for.

Follow the steps below to unblock a currently blocked item that is being analyzed for classification:

1. In the list of blocked items, find the item that you want to unblock and click the arrow that appears next to the **Date** column.
2. Click the **Do not block again** button.
3. If you are sure you want to unblock the selected item, respond affirmatively to the confirmation message.

After you unblock a currently blocked item, it will disappear from the **Currently blocked** list in section **Currently blocked items being classified**. By doing that, you are allowing it to run under your own responsibility. The item will appear in the **Excluded items** list and in the history of blocked item, indicating that it has been excluded.

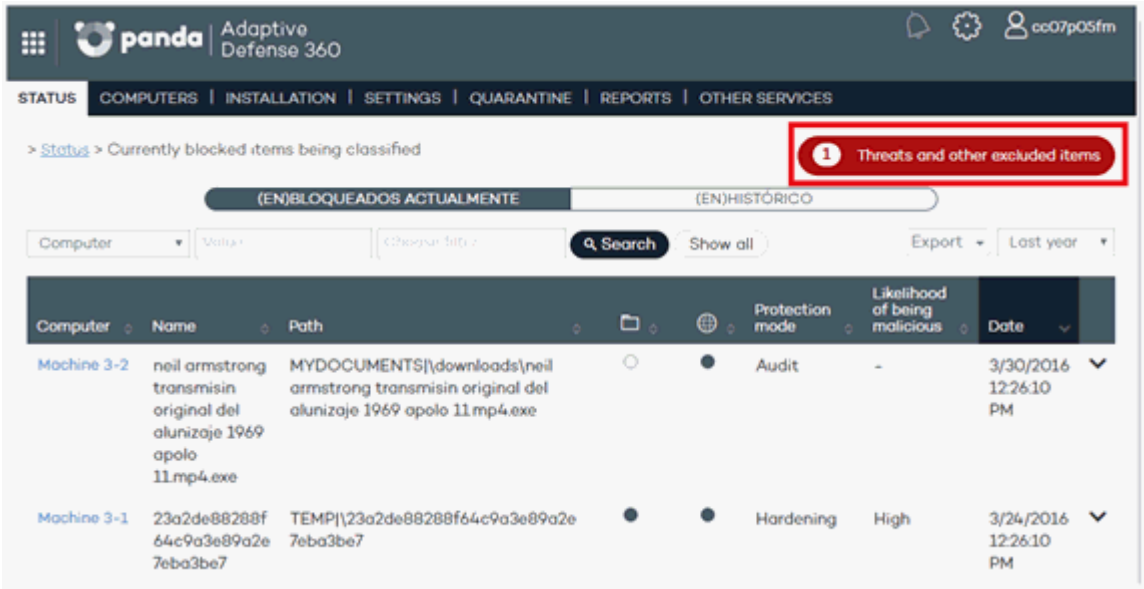
Excluding items classified as malware or PUPs

Excluding an item classified as malware from scans is equivalent to unblocking a blocked item that is pending classification, although in the former case you are allowing the execution of a program that Adaptive Defense 360 has already classified as harmful or dangerous.

It is very important that before you exclude a malware or PUP from scans you consider the consequences very seriously.

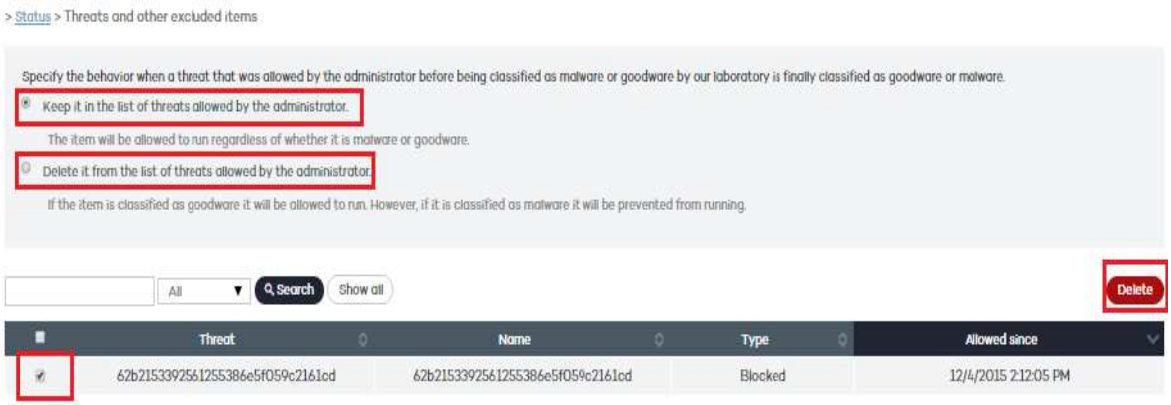
Viewing excluded items

To view the list of excluded items, use the button displayed in the Adaptive Defense 360 status window, or at the top of the malware/PUP/currently blocked items windows.



Managing excluded items

The **Threats and other excluded items** window lets you specify the solution's behavior with excluded or unblocked items.



To do it, follow the steps below:

- Select the checkbox next to a particular item.

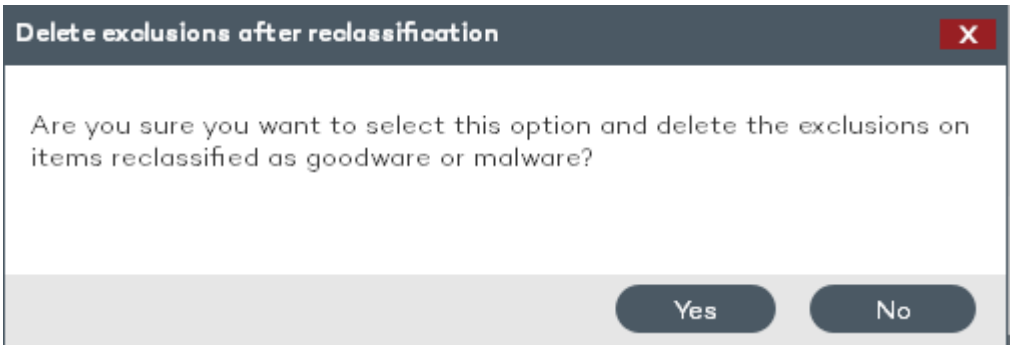
If you choose to keep it in the list of allowed threats, it will be allowed to run regardless of whether it is finally classified as malware or goodware. It won't be scanned again.

However, if you choose to remove it from the list of allowed threats:

- If the item is finally classified as goodware, it will be allowed to run.

- If the item is finally classified as malware, it will be prevented from running and will be added to the relevant counter in the dashboard. This is the default option.
- Respond affirmatively to the confirmation message.

Selecting the option **Delete it from the list of threats allowed by the administrator** will display a confirmation message.



17.6.1. Reviewing malware actions performed prior to being blocked

The service lets you access information about the number of times a malicious item has been detected on your network and the actions it carried out before being blocked by Adaptive Defense 360. To view that information, click the arrow to the right of the Date column.

Unblocking an item

In the list of blocked items, use the Do not block again button to prevent items from being blocked by Adaptive Defense 360 again. Refer to the Excluding blocked items section for more information.

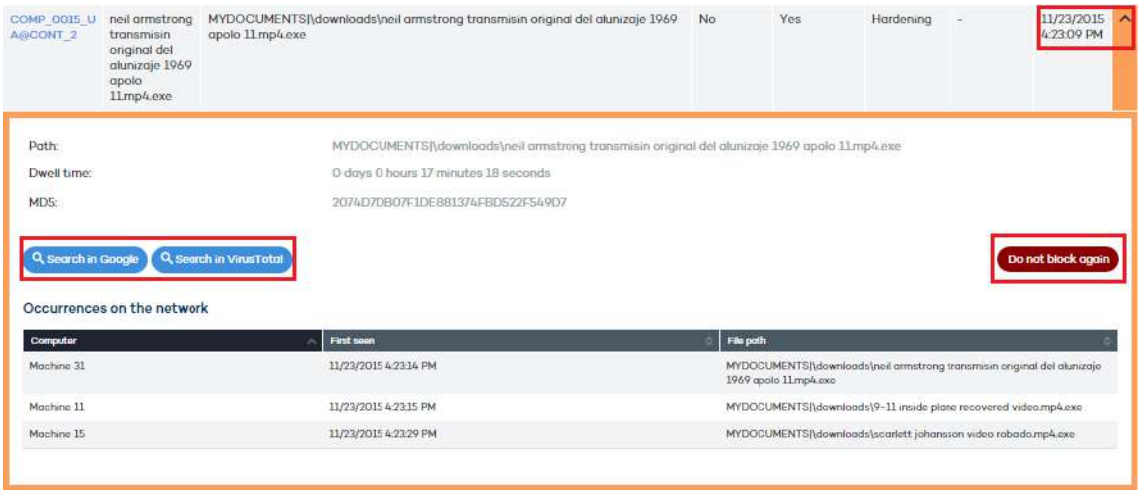
IMPORTANT: Do not exclude items unless you are absolutely certain you don't want to have them blocked ever again. Please refer to the Excluding blocked items section for more information.

Accessing additional information

To find out more about a specific item, use the Search in Google or Search in VirusTotal options.

Accessing activity graphs

If the item managed to take any actions before being blocked, the View activity graph button will be displayed. Click it to access an activity graph with detailed information about the actions performed by the item.


COMP_0015_UA@CONT_2
neil armstrong transmisin original del alunizaje 1969 apolo 11.mp4.exe
MYDOCUMENTS|\downloads\neil armstrong transmisin original del alunizaje 1969 apolo 11.mp4.exe
No
Yes
Hardening
-
11/23/2015 4:23:09 PM
Path:
MYDOCUMENTS|\downloads\neil armstrong transmisin original del alunizaje 1969 apolo 11.mp4.exe
Dwell time:
0 days 0 hours 17 minutes 18 seconds
MD5:
2074D7DB07F1DE881374FBD522F549D7
Search in Google
Search in VirusTotal
Do not block again
Occurrences on the network
Computer
First seen
File path
Machine 31
11/23/2015 4:23:14 PM
MYDOCUMENTS|\downloads\neil armstrong transmisin original del alunizaje 1969 apolo 11.mp4.exe
Machine 11
11/23/2015 4:23:15 PM
MYDOCUMENTS|\downloads\9-11 inside plane recovered video.mp4.exe
Machine 15
11/23/2015 4:23:29 PM
MYDOCUMENTS|\downloads\scarlett johansson video robado.mp4.exe

18. Reports

Report types

Generating and sending reports

18.1. Introduction

Adaptive Defense 360 lets you generate reports about the security status of your network and any detections made over a given period of time. You can also select the content that will appear in the report, whether you want more detailed information, and if you want graphs. All of these options are quick and simple to manage.

18.2. Report types

Adaptive Defense 360 provides four types of reports:

- **Executive report**
- **Status report**
- **Detection report**
- **Threat reportt**

18.2.1. Executive report

This report provides a summary of the three main aspects of network security:

Status of the protection installed on the network

Detections and infection attempts on the network

Service status

Below is a description of the information provided in the Executive report:

- Status of the protection installed, and items detected over the last 24 hours, the last seven days and the last month.
- Top 10 computers with most malware detected and attacks blocked, respectively.
- Top 10 computers with most devices blocked.
- Information about the status of the licenses contracted.
- Number of computers on which the protection is being installed at the time of generating the report (including computers with installation errors).
- Number of spam messages detected.
- Top 10 accessed websites sorted by category.
- Top 10 computers with most Internet access attempts.
- Top 10 computers with most Internet access attempts blocked.

18.2.2. Status report

This report gives an overview of the protection and update status of all computers at the time of report generation. It also reports the number of computers on which the protection is being installed at the time of generating the report (including computers with installation errors).

18.2.3. Detection report

This report shows the detections made during the last 24 hours, the last 7 days, and the last month. It indicates the computer, the group, the type of detection, the number of detections made, the action taken, and the date when the detection took place.

18.2.4. Threat report

This report shows the threats detected by the advanced protection in the selected date range.

It also displays the computers that represent the greatest risk, that is, those computers where most infections have been detected.

Finally, it provides detailed information about each detected threat:

- Malicious programs
- Potentially unwanted programs (PUPs)
- Programs under investigation in our lab

For each of these you can see the total number of infections, the number of devices on which they have been detected, whether they have been run, if they have made an external connection and if they have accessed data.

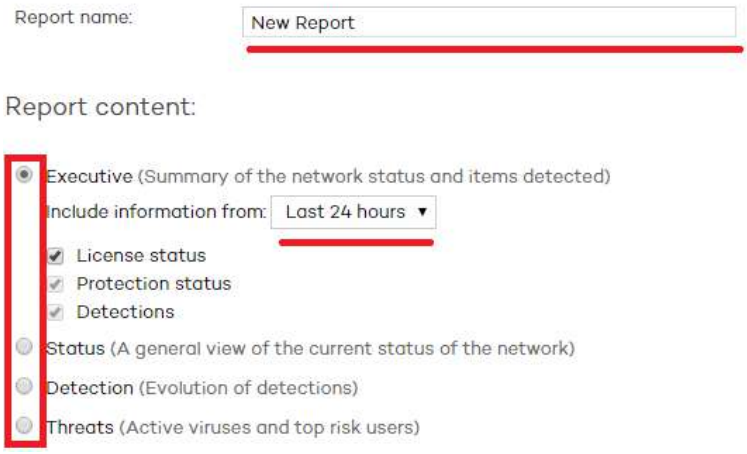
18.3. Generating and sending reports

In the Web console main window, click **Reports**. A new window will open, divided into the following sections:

- **Report name and content**
- **Report scope**
- **Schedule sending by email**

18.3.1. Report name and content

Select the name, type and period covered by the report (last 24 hours, last week or last month). The latter option only applies to the Executive, Detection and Threat reports.



18.3.2. Report scope

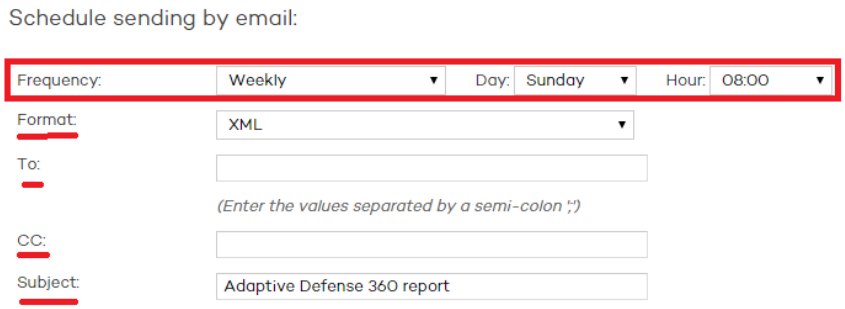
Select the computers covered in the report. Computers are selected by groups.

18.3.3. Schedule sending by email

If you don't need to schedule and send the report, but want to view it immediately, click **Show report** . Set the **Frequency** field to **Do not send**. The report will be immediately generated, and will appear on the report list in the left-hand side of the window.

You can save a limitless number of reports. To access a report, simply click its name on the list that appears on the left side of the **Reports** window.

You can schedule tasks to send reports by email to selected recipients in different formats.



To do that, enter the following data:

Frequency: The frequency of sending the report. Depending on the option you choose you will be able to select a day of the week, the time of the day or the day of the month on which the report will be sent:

Monthly

Weekly

Daily

The 1st of the month

Format: The report format

XML

CSV

IFF

PDF

Web

Excel

To: The recipient's email address

CC: Use this field if you want to 'carbon copy' another recipient

Subject: The subject line of the message

You can schedule up to 27 report send tasks. If you reach that limit, you will need to delete a previous task to create a new one.

19. Remediation tools

Automatic file disinfection

On-demand file scanning and disinfection

Advanced computer disinfection

Remote desktop access

Anti-Theft protection

19.1. Introduction

Adaptive Defense 360 provides several remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle presented in chapter 3.

Some of these tools are automatic and don't require administrator intervention, whereas other require the execution of certain actions through the Web console.

All of the remediation tools included in Adaptive Defense 360 can be used from the Web console without having to physically go to the affected user's computer, thus saving time and travel costs.

The table below illustrates the tools available for each platform and their type (manual or automatic).

Remediation tool	Platform	Type	Purpose
Automatic file disinfection	Windows, Mac OS X, Android	Automatic	To disinfect or quarantine malware at the time of infection.
On-demand file scanning and disinfection	Windows, Mac OS X, Linux, Android	Automatic (scheduled) / Manual	To scan, disinfect and quarantine malware at the time chosen by the administrator or at scheduled times.
Computer disinfection	Windows	Manual	To disinfect computers affected by both conventional and advanced malware particularly resilient to removal.
On-demand restart	Windows	Manual	Restarts computers to apply updates, finish manual disinfection tasks and fix protection errors.
Remote desktop access	Windows	Manual	Remote control tools to access infected computers.
Anti-Theft protection	Android	Manual	Tools that help you locate stolen devices and identify the potential thief.

19.2. Automatic file disinfection

Automatic disinfection is performed by the real-time advanced protection and the antivirus protection.

Upon detecting malware, Adaptive Defense 360 automatically cleans the affected item provided there is a disinfection method available. Otherwise, the item is moved to quarantine, as explained in chapter 18.

Automatic disinfection does not require administrator intervention, however, the **Enable permanent file protection** checkbox must be selected in the Antivirus section.

Refer to chapter 13 for more information about the blocking modes available in Adaptive Defense 360 *and the antivirus settings.*

Advanced protection mode	Antivirus protection	Behavior
Audit	Enabled	Detection, disinfection, quarantine
Hardening, Lock	Enabled	Detection, blocking of unknown items, disinfection, quarantine
Audit	Disabled	Detection
Hardening, Lock	Disabled	Detection, blocking of unknown items

19.3. On-demand file scanning and disinfection

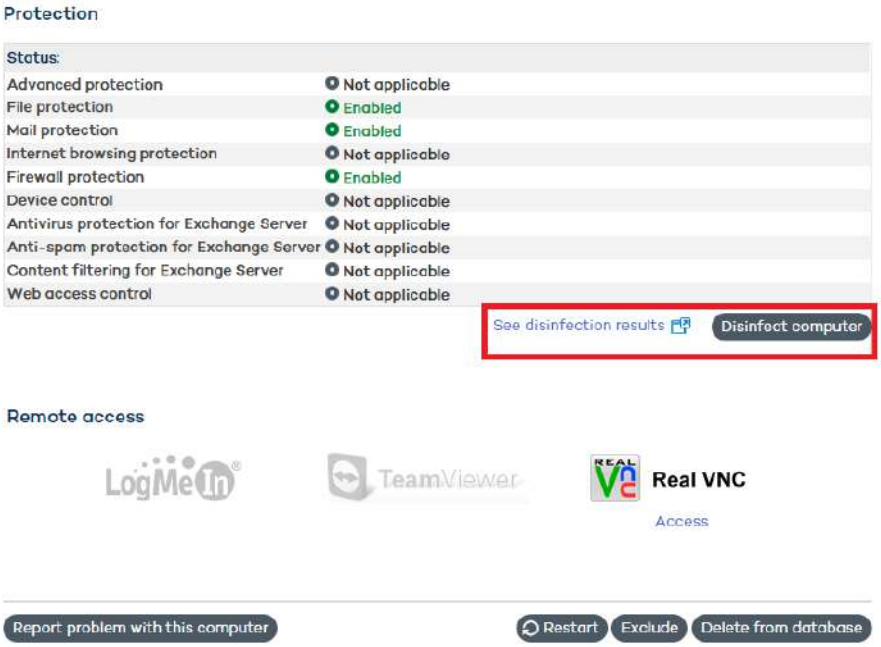
To disinfect files on demand you must create scheduled scan tasks, as explained in chapters 13 to 16, or run individual on-demand scans.

19.4. Advanced computer disinfection

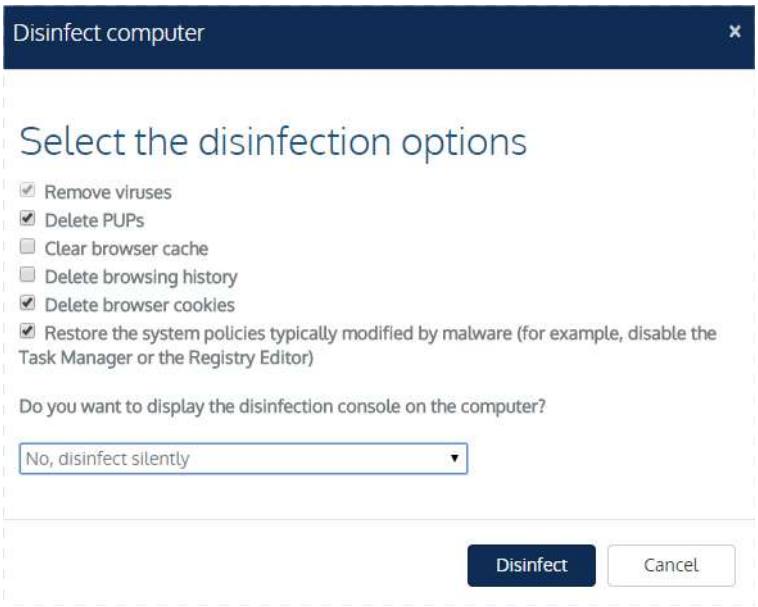
Automatic disinfection may fail on computers infected with advanced malware or PUPs, as these threats are much harder to neutralize. These computers can be easily identified by administrators as they will cause new incidents to be constantly reported in the dashboard's**Activity** panel. Only in those cases will it be necessary to use the advanced disinfection tool.

Once the infected computers have been located, the network administrator can launch our **Cloud Cleaner** disinfection tool remotely from the administration console. To do that, click the **Malicious programs** or **Potentially unwanted programs** panel (depending on the nature of the incident) in the **Activity** area. Click the specific incident and then click **Disinfect computer**.

You can also disinfect a computer from the **Computer details** window (go to the **Computers** tab, click **Protected**, click the relevant computer and finally click **Disinfect computer**).



You will then be shown a quick setup window.



The disinfection menu options are as follows:

Remove viruses: This checkbox is always enabled and cleans the viruses found on the computer.

Delete PUPs: Deletes potentially unwanted programs.

Clear browser cache: Cleans the cache of the Web browser installed on the computer (Internet Explorer, Firefox or Chrome).

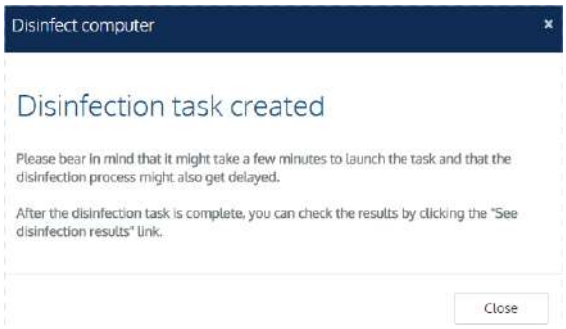
Delete browsing history: Cleans the Web browsing history.

Delete browser cookies: Deletes browser cookies.

Restore the system policies typically modified by malware: Restores access to the task manager, shows file extensions, and generally restores all the system policies that the malware may have changed preventing their restoration to the original configuration chosen by the customer.

Do you want to display the disinfection console on the computer? If the answer is yes, it shows the Cloud Cleaner console along with the disinfection results.

Once configured, a disinfection task will be created.



After running the task, you'll be able to see the results by clicking the **See disinfection results** link.

For more information about Cleaner Monitor, see the product's Web help or the link ***http://pcopdocuments.azurewebsites.net/Help/pccm/es-ES/index.htm***

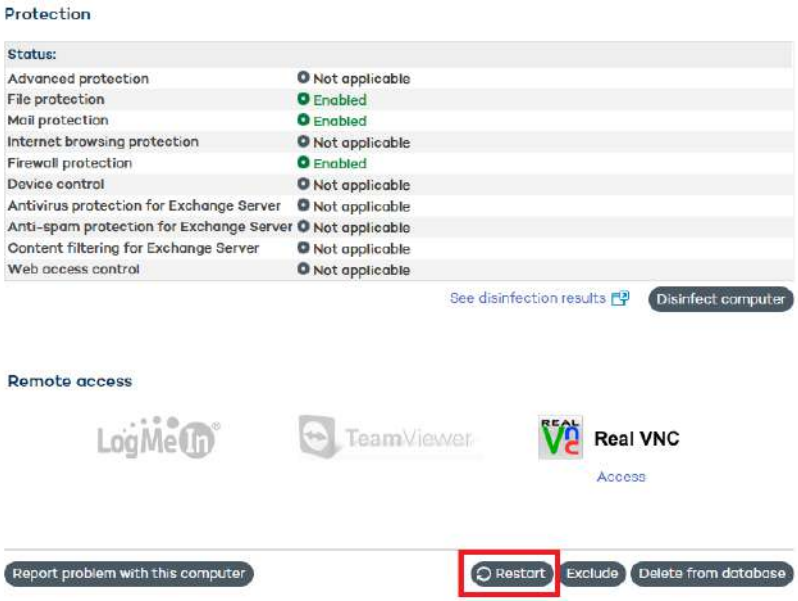
If you have problems disinfecting a PC, we advise you to manually download and run the most up-to-date version of Panda Cloud Cleaner from ***http://pandacloudcleaner.pandasecurity.com***

19.5. Restarting computers

The Web console lets administrators restart computers remotely. This is very helpful if you have computers whose protection you need to update or protection problems to fix. Only those computers listed on the list of protected computers can be restarted remotely.

To do that, go to the **Computers** window / **Protected** tab, select the checkbox next to the computer or computers that you want to reboot, and click **Restart**.

Alternatively, you can also click a computer's name, access the **Computer details** window and click the **Restart** button.



19.6. Remote desktop access

19.6.1. Viewing computers with remote access tools installed

The remote access feature lets you access your network computers from the administration console without physically having to be in front of them.

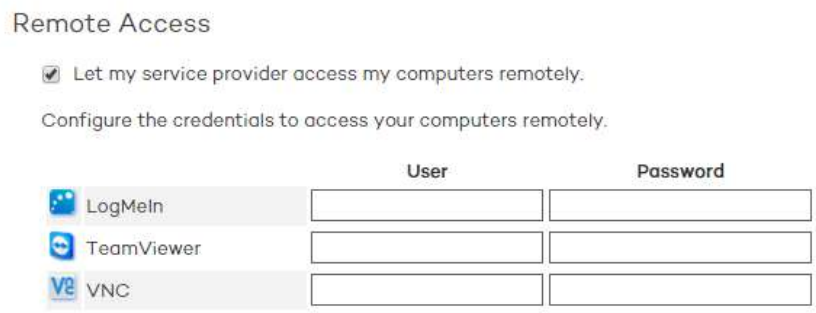
Adaptive Defense 360 lets you access your network computers using any of the following remote access tools:

- TeamViewer
- RealVNC
- UltraVNC
- TightVNC

- LogMeIn.

A small icon will be displayed in the **Computers** window for any computer with any of these tools installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer.

You can enter the credentials from the **Computers** window or in the **Preferences** window accessible through the  icon located at the top of the console.



If the computer has multiple tools installed, placing the mouse pointer over the icon will display all of them. Select one to access the computer remotely.

If a computer has different VNC tools installed, you will only be able to access it through one of them, in the following order of priority: 1-RealVNC, 2-UltraVNC, 3-TightVNC.

You will be able to access more or fewer computers depending on whether you have total control or administrator permissions.

> ***If you only have monitoring permissions, you will not be able to access any computers, and the icon in the Remote access column will be grayed out.***

19.6.2. How to get remote access to another computer

Remote access from the Computers window

The first time that you access the **Computers** window, a warning will be displayed indicating that the network computers don't have any remote access tools installed. If you want to install a remote access tool on them, click the link in the warning.

Remote access from the Computer details window

You can also use the remote access feature from the **Computer details** window, provided the selected computer has a remote access tool installed. If so, click the icon belonging to the remote access tool that you want to use.

To access other computers remotely, install one of the supported remote access tools on them: TightVNC, UltraVNC, RealVNC, TeamViewer or LogMeIn.

If a computer has multiple VNC tools installed, remember that you will only be able to access it using one of the tools in the specified order of priority.

19.6.3. How to use the remote access tools

VNC tools

These tools can only be used to access computers on the same local network as the customer.

Depending on the authentication settings established, you might be able to access them without having to enter any credentials in the console, or otherwise you may have to enter a password, or a user name and a password to establish a remote connection.

For an administrator to be able to access computers using VNC they must allow execution of a Java applet on their computer, otherwise, they will not be able to access them.

TeamViewer

This tool can be used to access computers outside the customer's local network.

To access computers through TeamViewer you will only need to enter the computer password. The "user" field can be left blank.

The password you must enter to access a computer through TeamViewer is the computer's TeamViewer password or the password for unattended access to computers. It is not the customer's TeamViewer account password.

It is advisable to have the same TeamViewer password on all computers.

The administrator's computer (the computer from which the Adaptive Defense 360 Web console is accessed) must have TeamViewer installed (it is not enough to have it in "run without installation" mode).

LogMeIn

This tool can be used to access computers outside the customer's local network.

To access computers via LogMein, you need to enter the LogMeIn account user name and password.

19.7. Anti-Theft protection

The Anti-Theft protection included in Adaptive Defense 360 will give you total control over your company's Android devices, and will allow you to take a series of actions in case of loss or theft.

Namely, you will be able to locate, lock and wipe your company's devices, take a picture of the thief, and send it by email to an address of your choice.

19.7.1. Enabling the Anti-Theft protection

In the Web console main window, click **Settings**. Then, click the name of the profile you want to configure the Anti-Theft protection for.

In the menu on the left, click the **Anti-Theft** option under Android.

If you want Adaptive Defense 360 to automatically report the device location, select the relevant checkbox.

Additionally, if you want to receive an email when there is activity on a stolen device, select the relevant checkbox. Then, enter the email address(es) that the picture of the potential thief will be sent to. Use a semicolon (;) to separate them.

If, together with the option to snap a picture of the thief, you select the option to report the device's location, the email received will include a photo plus a map showing its location.

Once you have finished configuring the protection, go to the **Computer details** window to track the location of the device, lock it, and change the email address for the **Snap the thief** feature.

Privacy mode

Administrators can allow end users to use their devices in privacy mode. This allows the user to disable the options to automatically report the device's location and take a picture of the thief, which will be password-protected.

However, it will still be possible to use those options on demand, but only if you have the password entered by the user.

To re-enable the options to automatically report the device's location and snap the thief, it will be necessary to disable the privacy mode.

20. Forensic analysis

20.1. Introduction

When the Adaptive Defense 360 dashboard displays an infection, it needs to be determined to what extent the network has been compromised and how to protect it from future attacks.

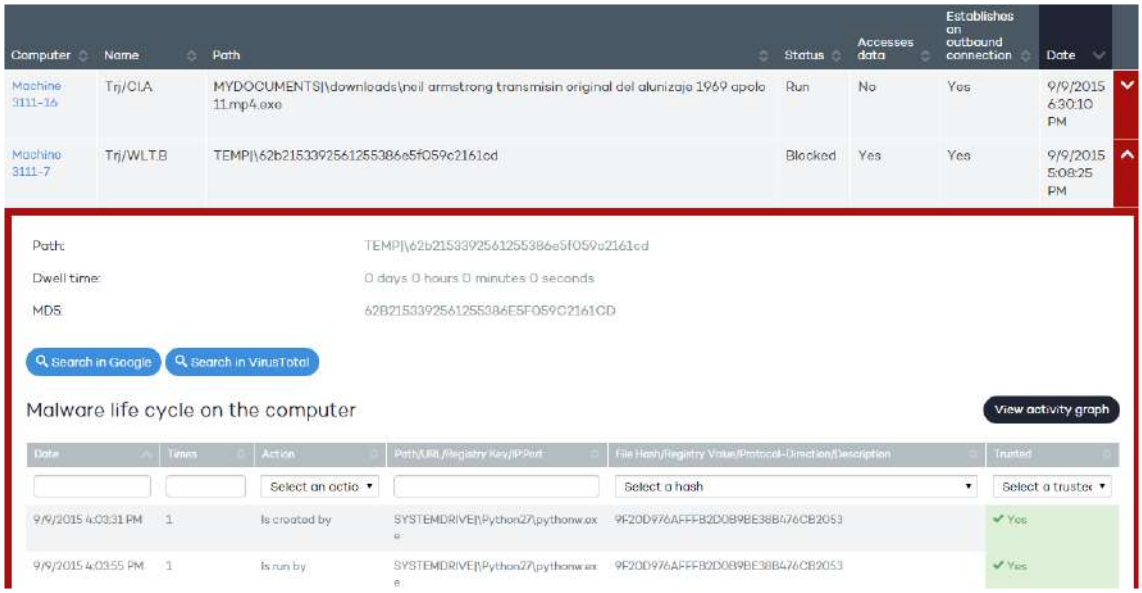
New generation malware is characterized by going undetected for long periods of time, taking advantage of this to access sensitive data or company intellectual property. Its objective is economic gain, either through blackmail by encrypting company documents or selling the information obtained to the competition, among other strategies common to these types of attacks.

Whatever the case, it is vital to determine the actions that the malware performed on the network in order to take appropriate measures. Adaptive Defense 360 is able to continuously monitor all actions triggered by threats and store them to show their path, from their initial appearance on the network until their neutralization.

Adaptive Defense 360 visually displays this type of information in two ways: through action tables and graphs.

20.2. Forensic analysis using the action tables

The **Status** window lets you access lists of the threats detected on the network by clicking the panels available in the **Activity** section. Click any of the threats to obtain a table with detailed information about their activity.



The fields included to generally describe the threat are:

MD5: Adaptive Defense 360 shows the malware hash for subsequent checking in VirusTotal or Google.

Malware path: Path of the executable that contains the malware.

Dwell time: Time that the threat has remained in the system without being classified.

Malware life cycle on the computer: This is a table that details each of the actions triggered by the threat.

Additionally, there are two buttons to search for further information on the Internet using Google and the VirusTotal website.

20.2.1. Action table

The action table for the threat includes only relevant events, because the amount of actions triggered by a process is so high that it would prevent the extraction of useful information for a forensic analysis.

The table content is initially presented in date order, making it easier to follow the development of the threat.

The fields included in the action table are detailed below:

Date: Date of the action

Times: Number of times the action was executed. A single action executed several times consecutively only appears once in the list of actions.

Action: Action implemented. Below is a list of the actions that can appear in this field:

- File download
- Socket used
- Accesses data
- Is run by
- Runs
- Is created by
- Creates
- Is modified by
- Modifies
- Is loaded by
- Loads
- Is installed by
- Installs
- Is mapped by
- Maps
- Is deleted by
- Deletes
- Is renamed by

- Renames
- Is killed by
- Kills process
- Remote thread created by
- Creates remote thread
- Kills process
- Remote thread created by
- Creates remote thread
- Comp opened by
- Opens comp
- Comp created by
- Creates comp
- Creates Reg Key to exe file
- Modifies Reg Key to exe file

Path/URL/Registry key/IP:port: Action entity. Depending on the action type it can contain:

- **Registry key**: For all actions that involve modifying the Windows registry
- **IP:port**: For all actions that involve communicating with a local or remote computer
- **Path**: For all actions that involve access to the computer hard disk
- **URL**: For all actions that involve access to a URL

File Hash/Registry Value/Protocol-Direction/Description: This field complements the entity. Depending on the action type it can contain:

- **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. The possible values are:
  - TCP
  - UDP
  - Bidirectional
  - UnKnown
- **Description**
- **Trusted**: The file is digitally signed

To locate actions of most interest in the list, there is a series of filters in the table header.

Some of the fields are text type fields and others are drop-down menus with all the various occurrences given in the selected column. Text searches are flexible and do not require the use of wildcards to search within the text string.

20.2.2. Subject and predicate in the actions

To correctly understand the format used to present the information in the action list, a parallel needs to be drawn with the natural language:

All actions have as the subject the file classified as malware. This subject is not indicated in each line of the action table because it is common throughout the table.

All actions have a verb which relates the subject (the classified threat) with an object, called the entity. The entity is indicated in the Path/URL/Registry key/IP:port field of the table.

The entity is complemented with a second field which adds information to the action, which is the Hash/Registry Value/Protocol-Direction/Description field.

The example below illustrates two actions carried out by the same hypothetical malware:

Date	Times	Action	Path/URL/Registry key/IP:port	Hash/Registry Value/Protocol-Direction/Description	Trusted
3/30/2015 4:38:40 PM	1	Connects to	54.69.32.99:80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Loads	PROGRAM_FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL	9994BF035813FE8EB6BC98ECCBD5B0E1	NO

The first action indicates that the malware (subject) **connects to (action)** the IP address 54.69.32.99:80 (entity) through the TCP-bidirectional protocol.

The second action indicates that the malware (subject) **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 Adaptive Defense 360:

Active: These are predicative actions (with a subject and predicate) related by an active verb. In these actions, the verb of the action relates the subject, which is always the process classified as a threat, and a direct object, the entity, which can be multiple according to the type of action.

Passive: These are actions where the subject (the process classified as malware) becomes the passive subject (which receives rather than executes the action), and the verb is passive (to be + participle). In this case, the passive verb relates the passive subject which receives the action with the entity, which performs the action.

Examples of active actions are:

Connects to

Loads

Creates

Examples of passive actions are:

Is created by

Is downloaded from

An example of a passive action is:

Date	Times	Action	Path/URL/Registry key/IP:port	Hash/Registry Value/Protocol-Direction/Description	Trusted
3/30/2015 4:51:46 PM	1	Is run by	WINDOWS| \ explorer.exe	7522F548A84ABAD8FA516DE5AB3931EF	NO

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 malware. By contrast, passive actions usually reflect the infection vector used by the malware (which process run it, which process copied it to the user's computer, etc.).

20.3. Forensic analysis using the activity graphs

Execution graphs visually display the information shown in the action tables, emphasizing the temporal aspect.

The graphs are initially used to provide, at a glance, a general idea of the actions triggered by the threat.

20.3.1. Diagrams

The string of actions in the execution graph view is represented by two items:

Nodes: They mostly represent actions or information items

Lines and arrows: They unite the action and information nodes to establish a temporal order and assign each node the role of "subject" or "predicate".

20.3.2. Nodes

The nodes show the information through their associated icon, color and descriptive panel on the right of the screen when selected with the mouse.

The color code used is as follows.

- **Red**: Untrusted item, malware, threat.
- **Orange**: Unknown item, unclassified.
- **Green**: Trusted item, goodware.

Listed below are action-type nodes with a brief description:

Symbol	Node Type	Description
	Action	- File downloaded - Compressed file created
	Action	- Socket / communication used
	Action	- Monitoring initiated

	Action	- Process created
	Action	- Executable file created - Library created - Key created in the registry
	Action	- Executable file modified - Registry key modified
	Action	- Executable file mapped for write access
	Action	- Executable file deleted
	Action	- Library loaded
	Action	- Service installed
	Action	- Executable file renamed
	Action	- Process stopped or closed
	Action	- Thread created remotely
	Action	- Compressed file opened

Listed below are descriptive-type nodes with a brief description:

Symbol	Node Type	Description
	Final Node	- File name and extension o Green: Goodware o Orange: Unclassified o Red: Malware/PUP
	Final Node	- Internal computer (it is on the corporate network) o Green: Trusted o Orange: Unknown o Red: Untrusted
	Final Node	- External computers o Green: Trusted o Orange: Unknown o Red: Untrusted
	Final Node	- Country associated with the IP address of an external computer
	Final Node	- File and extension
	Final Node	- Registry key

20.3.3. Lines and arrows

The lines of the graphs relate the different nodes and help to establish the order in which the actions performed by the threat were executed.

The two attributes of a line are:

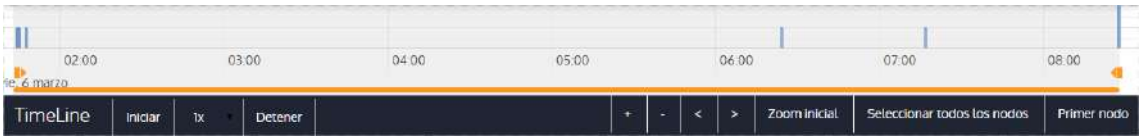
Line thickness: The thickness of a line which joins two nodes indicates the number of occurrences that this relationship has had in the graph. The greater number of occurrences, the greater the size of the line

Arrow: Marks the direction of the relationship between the two nodes

20.3.4. The timeline

The timeline helps control the display of the string of actions carried out by the threat over time. Using the buttons at the bottom of the screen you can position yourself at the precise moment where the threat carried out a certain action and retrieve extended information that can help you in the forensic analysis processes.

The timeline of the execution graphs looks like this:



Initially, you can select a specific interval on the timeline dragging the interval selectors to the left or right to cover the timeframe of most interest to you.

After selecting the timeframe, the graph will only show the actions and nodes that fall within that interval. The rest of the actions and nodes will be blurred on the graph.

The actions carried out by the threat are represented on the timeline as vertical bars accompanied by the timestamp, which marks the hour and minute when they occurred.

20.3.5. Zoom in and Zoom out

The + and – buttons of the time bar allow you to zoom in or zoom out for higher resolution if there are many actions in a short time interval.

20.3.6. Timeline

To view the string of actions run by the threat, the following controls are used:

Start: Starts the execution of the timeline at a constant speed of 1x. The graphs and lines of 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.***

20.3.7. Filters

The controls for filtering the information shown are at the top of the graph.

The filtering criteria available are:

Action: Drop-down menu which lets you select an action type from all those executed by the threat. This way, the graph only shows the nodes that match the action type selected and the adjacent nodes associated with this action

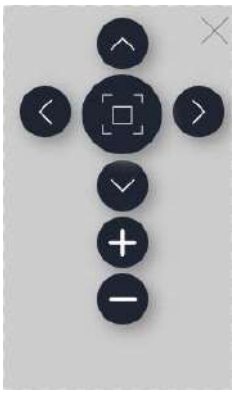
Entity: Drop-down menu which lets you choose an entity (the content of the field Path/URL/Registry key/IP:port)

20.3.8. Node movement and general zoom

To move the graph in four directions and zoom in or zoom out, you can use the controls in the top right of the graph.

> ***To zoom in and zoom out more easily, you can use the mouse scroll wheel.***

The X symbol allows you to leave the graph view.



If you would rather hide the timeline button zone to use more space on the screen for the graph, you can select the  symbol situated in the bottom right of the graph.

Finally, the behavior of the graph when it is displayed on screen or dragged by one of its nodes can be configured using the panel shown below, accessible by selecting the button in the top left of the graph

20.4. Interpreting the action tables and activity graphs

Certain technical knowledge is required to correctly interpret the action tables and activity graphs, as both resources are representations of the dumping of the evidence collected, which must be interpreted by the company's network administrator.

In this chapter, some basic interpretation guidelines are offered through several real malware examples.

> ***The name of the threats indicated here can vary among different security vendors. You should use the hash ID to identify specific malware.***

20.4.1. Example 1: Display of the actions executed by the malware Trj/OCJ.A

The top of the alerts table shows critical information about the malware found. In this case the important data is as follows:

Date: 06/04/2015 3:21:36

Computer: XP-BARCELONA1

Name: Trj/OCJ.A

Type: MW

Status: Run

Malware path: TEMP | \Rar$EXa0.946\appnee.com.patch.exe

Status

The malware status is **Run** due to the fact that the Adaptive Defense 360 mode configured was **Hardening**: The malware already resided on the computer when Adaptive Defense 360 was installed and was unknown at the time of running.

Hash

The hash string can be used to obtain more information on sites such as VirusTotal to gain a general idea of the threat and how it works.

Malware path

The path where the malware was detected for the first time on the computer belongs to a temporary directory and contains the RAR string. Therefore, it comes from a RAR file temporarily uncompressed in the directory, and which gave the appnee.com.patch.exe executable as the result.

Action table

Step	Date	Action	Path
1	3:17:00	Created by	PROGRAM_FILES|\WinRAR\WinRAR.exe
2	3:17:01	Is run by	PROGRAM_FILES|\WinRAR\WinRAR.exe
3	3:17:13	Creates	TEMP|\bassmod.dll
4	3:17:34	Creates	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifies	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Deletes	PROGRAM_FILES|\ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK
7	3:17:41	Creates	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifies	PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll
9	3:17:59	Runs	PROGRAM_FILES|\Google\Chrome\Application\chrome.exe

Steps 1 and 2 indicate that the malware was uncompressed by WinRar.Exe and run from that program. The user opened the compressed file and clicked its binary.

Once run, in step 3 the malware created a DLL file (bassmod.dll) in a temporary folder, and another one (step 4) in the installation directory of the Adobe Acrobat 11 program. In step 5, it also modified an Adobe DLL file, to take advantage perhaps of some type of program vulnerability.

After modifying other DLL files, it launched an instance of Chrome which is when the timeline finishes. Adaptive Defense 360 classified the program as a threat after that string of suspicious actions and stopped its execution.

The timeline shows no actions on the registry, so it is very likely that the malware is not persistent or has not been executed up to the point of surviving a restart of the computer.

The Adobe Acrobat 11 software has been compromised so a reinstall is recommended; however, thanks to the fact that Adaptive Defense 360 monitors both goodware and malware executables, the

execution of a compromised program will be detected when it triggers dangerous actions, and ultimately be blocked.

20.4.2. Example 2: Communication with external computers by BetterSurf

BetterSurf is a potentially unwanted program that modifies the Web browser installed on the user's computer and injects ads in the Web pages that they visit.

The top of the alerts table shows critical information about the malware found. The following data is provided in this case:

Date: 3/30/2015

Computer: MARTA-CAL

Name: PUP/BetterSurf

Type: MW

Malware path: PROGRAM_FILES | \VER0BLOCKANDSURF\N4CD190.EXE

Dwell time: 11 days 22 hours 9 minutes 46 seconds

Dwell time:

In this case, the dwell time was very long: the malware was dormant on the customer's network for almost 12 days. This is increasingly normal behavior and may be for various reasons: perhaps because the malware has not carried out any suspicious action until very late, or simply because the user downloaded the file but did not run it at the time.

Action table

Step	Date	Action	Path / IP	Hash / Protocol
1	08/03/2015 11:16	Created by	TEMP | \08c3b650-e9e14f.exe	EB0C9D2E28E1EE
2	03/18/2015 11:16	Is run by	SYSTEM | \services.exe	953DF73048B8E8
3	03/18/2015 11:16	Loads	PROGRAM_FILES | \VER0BLOF\N4Cd190.dll	CE44F5559FE618
4	03/18/2015 11:16	Loads	SYSTEM | \BDL.dll	D7D59CABE1270
5	03/18/2015 11:16	Socket used	127.0.0.1:13879	0-UnKnown
6	03/18/2015 11:16	Socket used	37.58.101.205:80	0-Bidirectional
7	03/18/2015 11:17 AM	Socket used	5.153.39.133:80	0-Bidirectional
8	03/18/2015 11:17 AM	Socket used	50.97.62.154:80	0-Bidirectional
9	03/18/2015 11:17 AM	Socket used	50.19.102.217:80	0-Bidirectional

Here it can be seen how the malware established communication with several different IP addresses. The first of them (step 5) is the computer itself, and the rest are external IP addresses to which it connects via port 80 and from which the advertising content is probably downloaded.

The main prevention measure in this case will be to block those IP addresses in the corporate firewall.

Before adding rules to block IP addresses in the corporate firewall, you should consult the IP addresses to be blocked in the associated RIR (RIPE, ARIN, APNIC, etc.) to see the network to which they belong. In many cases, the remote infrastructure used by the malware is shared with legitimate services housed in providers such as Amazon and similar, so blocking IP addresses would be the same as blocking access to normal Web pages.

20.4.3. Example 3: Access to the registry by PasswordStealer.BT

PasswordStealer.BT is a Trojan that records the user's activity on the computer and sends the information obtained to the exterior. Among other things, it is able to capture the user's screen, record the keystrokes and send files to a C&C (Command & Control) server.

The top of the alerts table shows critical information about the malware found. The following data is provided in this case:

Malware path: APPDATA | \microsoftupdates\micupdate.exe

The name and location of the executable indicate that the malware poses as a Microsoft update. This particular malware is not able to infect computers by itself; it requires the user to run the virus manually.

Status

The malware status is **Run** due to the fact that the Adaptive Defense 360 mode configured was **Hardening**: The malware already resided on the computer when Adaptive Defense 360 was installed and was unknown at the time of running.

Action table

Step	Date	Action	Path	Path / Hash
1	03/31/2015 23:29	Is run by	PROGRAM_FILESX86 | \internet explorer\iexplore.exe	7477021D17D781B24
2	03/31/2015 23:29	Created by	INTERNET_CACHE | \Content.IE5\QGV8PV80\ index[1].php	C9D4C32DF27B3CDEF
3	03/31/2015 23:30	Creates Reg Key to exe file	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\ CurrentVersion \Run?MicUpdate	C:\Users\vig03\AppData\ Roaming\ MicrosoftUpdates\ MicUpdate.exe
4	03/31/2015 23:30	Runs	SYSTEMX86 | \notepad.exe	D378BFFB70864AA61C

5	03/31/2015 23:30	Remote thread created by	SYSTEMX86|\notepad.exe	D378BFFB70864AA61C

In this case the malware is created in step 2 by a Web page and run by Internet Explorer.

The order of actions has a granularity of 1 microsecond. For this reason, several actions executed within the same microsecond may not appear in order in the timeline, as in step 1 and step 2.

Once run, the malware becomes persistent in step 3 adding a branch in the registry which will launch the program when the computer starts up. It then starts to execute 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 this malware by deleting the registry entry. It is quite possible that on an infected computer the malware prevents you from editing that entry; depending on the case, you would have to either start the computer in safe mode or with a bootable CD to delete that entry.

20.4.4. Example 4: Access to confidential data by Trj/Chgt.F

Trj/Chgt.F was published 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 action table to show you the behavior of this advanced threat.

Action table

Step	Date	Action	Path	Info
1	4/21/2015 2:17:47 PM	Is run by	SYSTEMDRIVE|\Python27\pythonw.exe	9F20D976AFFFB2D0B9BE38B476CB2053
2	4/21/2015 2:18:01 PM	Accesses data	#.XLS	Access to Office Excel document
3	4/21/2015 2:18:01 PM	Accesses data	#.DOC	Access to Office Word document
4	4/21/2015 2:18:03 PM	Creates	TEMP|\doc.scr	4DBD8393522CD5DA7364ACEA35E80719
5	4/21/2015 2:18:06 PM	Runs	TEMP|\doc.scr	4DBD8393522CD5DA7364ACEA35E80719
6	4/21/2015 2:18:37 PM	Runs	PROGRAM_FILES|\Microsoft Office\Office12\WINWORD.EXE	CEAA5817A65E914AA178B28F12359A46
7	4/21/2015	Connects to	192.168.0.1:2042	TCP-Bidirectional

8:58:02 PM

The malware is initially run by the Python interpreter (step 1) to later access an Excel and Word document (steps 2 and 3). In step 4, a file with a .SCR extension is run, probably a screensaver with some type of flaw or error that causes an anomalous situation in the computer and which might be exploited by the malware.

A TCP type connection occurs in step 7. The IP address is private, so the malware would be connecting to the customer's network.

In this case, the content of the files accessed must be checked to assess the loss of information, although looking at the timeline the information accessed seems to not have been extracted from the customer's network.

Adaptive Defense 360 will disinfect the threat, and automatically block subsequent executions of the malware for that customer and other customers.

21. Accumulated knowledge server

Accessing the Logtrust environment

Adaptive Defense 360 table description

21.1. Introduction

> ***The Logtrust environment is an optional module of*** Adaptive Defense 360***. If you do not have access to this environment contact your sales representative.***

Logtrust is a real-time service aimed at exploiting accumulated knowledge. The service imports and automatically analyzes in real time all information generated by Adaptive Defense 360.

Logtrust facilitates information searches on the safety of the customer's IT resources and helps generate colorful graphics to interpret the data registered by the Adaptive Defense 360 agents.

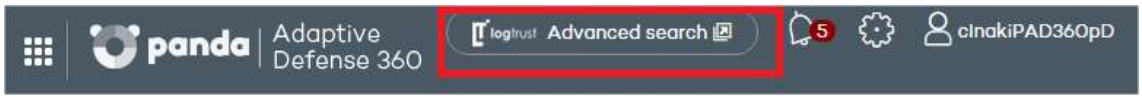
This chapter will show in detail the organizational scheme designed to store the information generated by Adaptive Defense 360, and the procedures necessary to use this information.

The objective of the Logtrust platform is to complement the information offered by Adaptive Defense 360 when it comes to establishing new remediation protocols, and assist in the forensic analysis techniques shown in Chapter 21.

> ***The Logtrust environment includes an online help accessible from the top panel Help.***

21.2. Accessing the Logtrust environment

To access the Logtrust environment you need to select the **Advanced Search** link on the Adaptive Defense 360 dashboard.



21.3. Adaptive Defense 360 table description

Adaptive Defense 360 sends all the information collected from the agents installed on the customer's computers to the Logtrust service, which will organize it into easy-to-read tables. This information covers every process run on the network, whether goodware or malware.

Each line of a table is an event monitored by Adaptive Defense 360. The tables contain a series of specific fields as well as common fields that appear in all of them, and which offer information such as when the event occurred, the computer where it was registered, its IP address, etc.

Many fields use prefixes that help refer to the information shown. The two most used prefixes are:

Parent: The fields that begin with the Parent tag (parentPath, parentHash, parentCompany...) reflect the content of a characteristic or attribute of the parent process.

Child: The fields that begin with the Child tag (childPath, childHash, childCompany...) reflect the content of a characteristic or attribute of a child process created by the parent process.

Besides these prefixes, many fields and values use abbreviations; knowing their meaning helps interpret the field in question:

Sig: Digital signature

Exe: Executable

Prev: Prevalence

Mw: Malware

Sec: Seconds

Op: Operation

Cat: Category

PUP: Potentially Unwanted Program

Ver: Version

SP: Service Pack

Cfg: Configuration

Svc: Service

Op: Operation

PE: Executable program

Cmp and comp: Compressed file

Dst: Destination

Listed below are the available tables indicating the type of information they contain and their specific fields.

21.3.1. Alert table

This table corresponds to the alerts shown on the Adaptive Defense 360 dashboard (**Activity** panel).

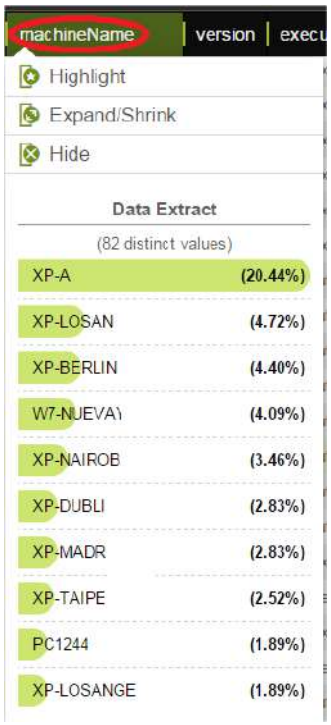
It contains a line for each threat detected on the customer's network with information on the computer involved, type of alert, timestamp and result of the alert.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
machineIP	IP address of the customer's computer that triggered the alert	IP address
date	Date when the event is received on the Adaptive Defense 360 server	Date
alertType	Category of the threat that triggered the alert	Malware, PUP
machineName	Name of the customer's computer	String
version	Version of the Adaptive Defense 360 agent installed on the computer	String in x.x.x format
executionStatus	The threat was run or not	Run or Not Run
dwellTimeSecs	Time in seconds from the first time the threat was seen on the customer's network	Seconds
itemHash	Hash of the detected threat	String
itemName	Name of the detected threat	String
itemPath	Full path of the file that contains the threat	String

Since the **Alerts** table is a transposition of the **Activity** panel in the Adaptive Defense 360 console, it is easy to obtain statistics of the most affected computers:

10 most attacked and infected computers

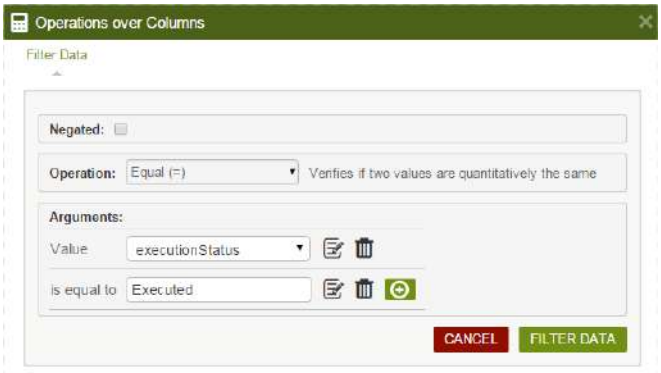
Click the header of the **machineName** or **manicheIP** columns to obtain a list of the 10 most attacked computers.



This list covers from the time when Adaptive Defense 360 first started to work on the customer's network; if you want to reduce the range, you can simply narrow the interval with the **Search limits** controls.

These lists include both malware blocking and executions; if you want to only show infected computers, you will need to add a filter by clicking the icon in the toolbar

You will also need to configure a data filter using the **executionStatus** field and equaling it to **Executed**, as shown in the image.



10 most viewed threats

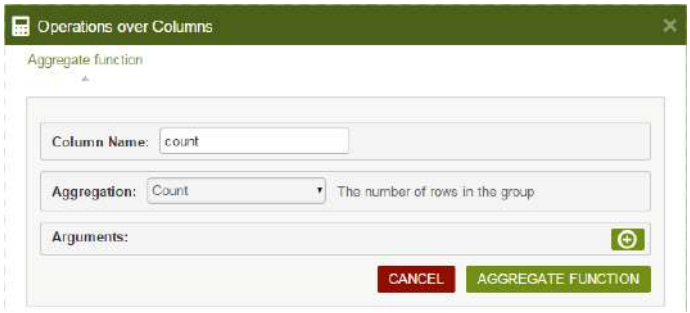
Similarly, by clicking the **itemHash** or **itemName** columns you can display quick statistics on the 10 most viewed threats on the customer's network.

Another way of obtaining far more visual information is to generate a graph of the most viewed malware. The name of the malware is shown on the coordinate axis and the number of occurrences on the abscissa axis.

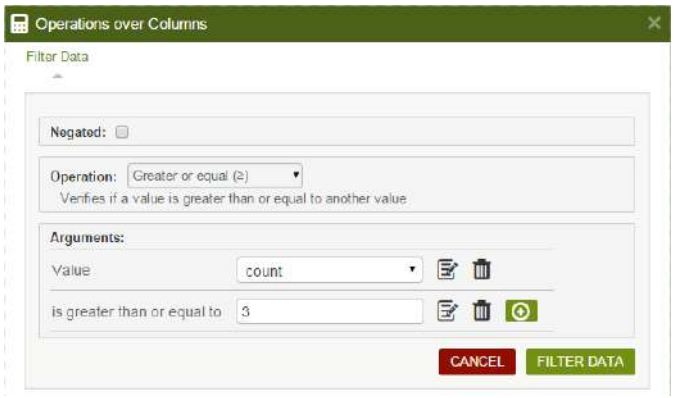
For this, you need to follow the steps below:

Add an aggrupation to the itemName field without any time limit (No temporal aggrupation).

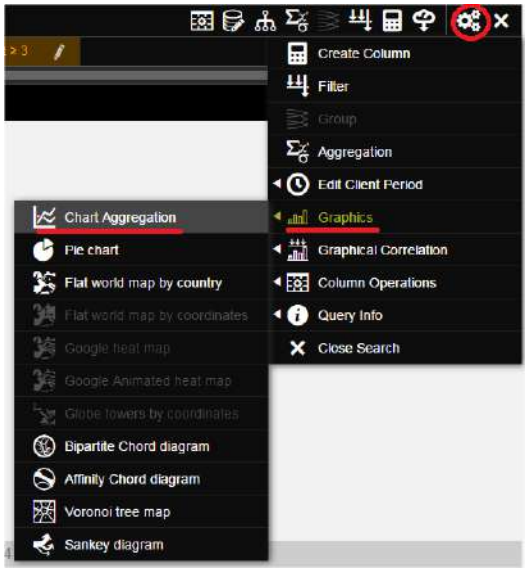
Add a counter function to determine how many occurrences there are in each itemName group.



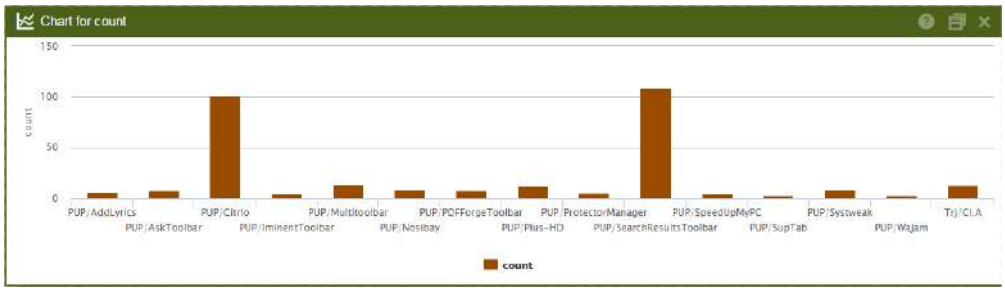
Add a filter to determine the aggrupation of 2 or fewer occurrences. This will clean the graph of those threats that have only been viewed twice



Add a Chart Aggregation type graphic and use the Count column as a parameter.



At this point, there is already a list of alerts grouped by threat and with the number of occurrences for each threat. You can create a simple graph with this data:



Other useful information

There are several interesting fields in the **Alerts** table that can be used to extract valuable information on the attacks received on the customer's network:

Eventdate: Grouping by this field you can see the number of daily attacks and determine if there is an ongoing epidemic.

dwellTimeSecs: This field provides the detection window of the threats received, i.e. the time from when the threat was first seen on the customer's network to its classification.

itemHash: Given that the name of the threat varies among security vendors, the hash field can be used to group threats instead of the itemName. This also helps to distinguish malware that is labeled with the same name.

21.3.2. Drivers table

This table logs all operations performed on drivers that are detected in the processes run on the user's computers.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIp	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	User name of the process that performs the operation on the driver	String
muid	Internal identifier of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
op	Operation performed by the process on the driver	Open Creation
hash	File hash/digest	String
driveType	Type of drive where the process that triggered the operation on the driver resides	Fixed, Remote, Removable
path	Path of the process that triggered the operation on the driver	String
validSig	Digitally signed process	Boolean
company	Content of the Company attribute of the process metadata	String
imageType	Internal architecture of the executable	EXEx32, EXEx64, DLLx32, DLLx64
exeType	Type of executable	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
prevalence	Historical prevalence on Panda Security's systems	HIGH, LOW, MEDIUM
prevLastDay	Previous-day prevalence on Panda Security's systems	HIGH, LOW, MEDIUM
cat	Category of the file that performed the operation on the driver	Goodware, Malware, PUP, Unknown, Monitoring
mwName	Malware name if the file is classified as a threat	String, (Null if the item is not malware)
serviceDriveType	Type of drive where the process that receives the operation resides	Fixed, Remote, Removable
servicePath	Path of the driver that received the operation	String

This table indicates the operations performed by all processes on the drivers installed. Since the malware that creates or modifies drivers is considered particularly dangerous because it attacks basic elements of the system, the ideal solution in this case is to filter the **Cat** field and dismiss anything that is classified as "Goodware" or "Monitoring".

21.3.3. Filesdwn Table

This table contains information on the HTTP downloads performed by the processes seen on the customer's network (URL, downloaded file data, computers that performed the downloads, etc.).

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
muid	Internal identifier of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
type	Type of downloaded file	Zip, Exe, Cab, Rar
url	Download URL	URI resource
hash	Digest/hash of the downloaded file	String
validSig	Digitally signed downloaded file	Boolean
company	Content of the company attribute of the process metadata	String
imageType	Internal architecture of the downloaded file	EXEx32, EXEx64, DLLx32, DLLx64

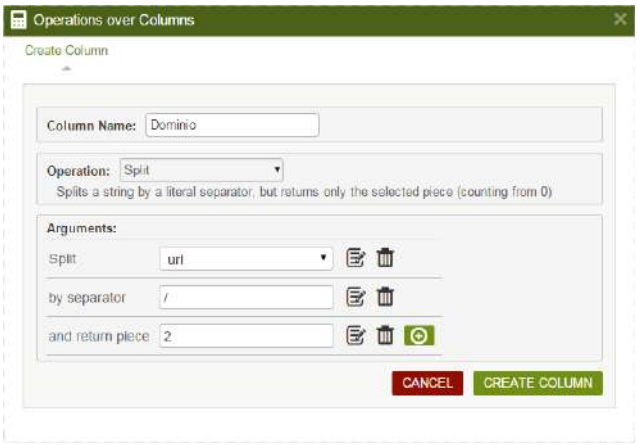
exeType	Type of executable of the downloaded file	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
prevalence	Historical prevalence on Panda Security's systems	HIGH, LOW, MEDIUM
prevLastDay	Previous-day prevalence on Panda Security's systems	HIGH, LOW, MEDIUM
cat	Category of the downloaded file	Goodware, Malware, PUP, Unknown, Monitoring
mwName	Malware name if the downloaded file is classified as a threat	String, (Null if the item is not malware)

Since this table shows all downloads performed by network users irrespective of whether they are malware or goodware, apart from locating with a simple filter the download information in the case of malware, it will also be possible to graphically display the domains that receive most downloads.

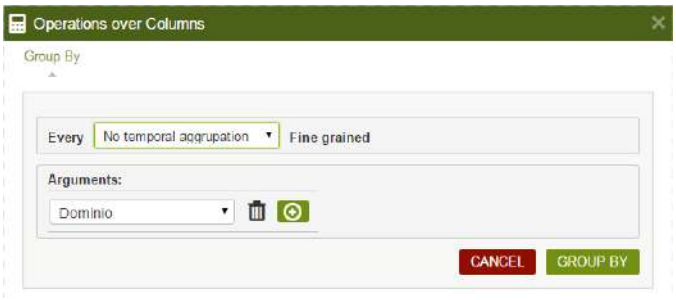
Domains that receive most downloads

To show this type of information, you need to manipulate the content of the **URL** field to remove the part of the string not of interest to you and end up with the domain.

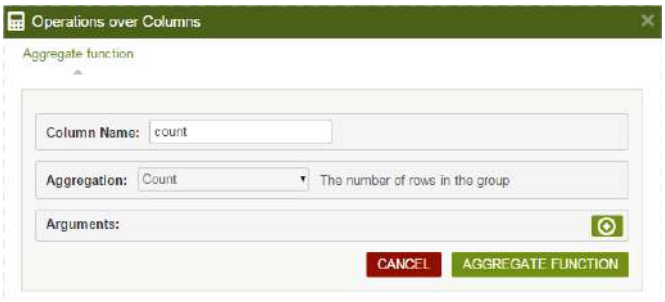
Create a new column with the Split operation on the URL field.



Group by different URL selecting No temporal aggrupation

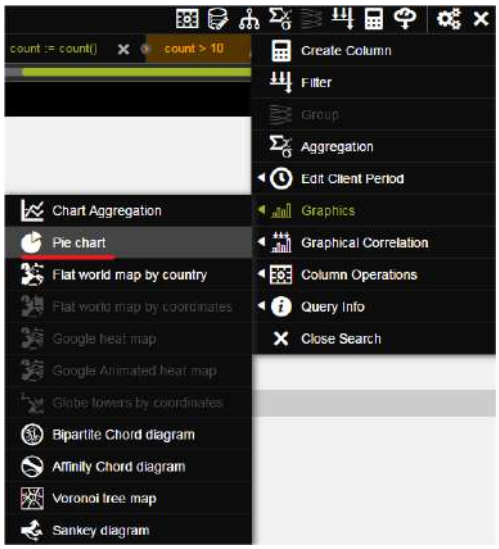


Add a count type aggregation column

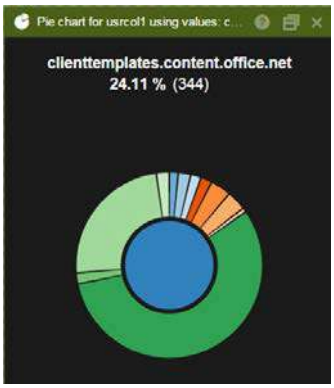


This way, you will obtain a list for each grouped domain and the number of occurrences of each domain within each group. With this information, you can easily obtain a graph with the most visited domains for downloading purposes.

In this case, a pie chart, simpler to interpret for the type of information shown here. For this, pre-filter the groups of 10 or fewer occurrences to be able to look in more detail at the rest of the domains.



In pie charts, the different sections are active so when you pass the mouse over them they show the percentages and name of the items represented.



Other useful information

Similarly, other fields can be combined to enhance or filter the lists and obtain more refined tables. You can use the following fields:

Machine or machineIP: Grouping by these fields you can see the computers on the customer's network that start the most downloads.

Cat: Filtering by this field you can clear the table and only show what is classified as malware. You can therefore obtain the domains considered as malware emitters to block them in a layer 7 firewall.

21.3.4. Hook table

This table logs all the hook creation and manipulation operations detected on the user's system

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
muid	Internal identifier of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
hooktype	Type of hook made by the process	Keyboard_ll, mouse_ll, keyboard, mouse
hash	Digest of the process that makes the hook	String

	on the system	
driveType	Type of drive where the process that makes the hook resides	Fixed, Remote, Removable
path	Path of the process that makes the hook	String
validSig	Process that makes the digitally signed hook	Boolean
company	Content of the Company attribute in the metadata of the process that makes the hook	String
imageType	Architecture of the file that makes the hook	EXEx32, EXEx64, DLLx32, DLLx64
exeType	Type of executable of the process that makes the hook	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
prevalence	Historical prevalence of the process that makes the hook on Panda Security's systems	HIGH, LOW, MEDIUM
prevLastDay	Previous-day prevalence of the process that makes the hook on Panda Security's systems	HIGH, LOW, MEDIUM
cat	Category of the process that makes the hook on the system	Goodware, Malware, PUP, Unknown, Monitoring
mwName	Malware name if the process that makes the hook on the system is classified as a threat	String, (Null if the item is not malware)
hookPEhash	Digest/hash of the hooked process	String
Hook	Type of drive where the hooked process resides	Fixed, Remote, Removable
hookPEpath	Path of the hooked process	String
hookPEvalidSig	Digitally signed hooked process	Boolean
hookPEcompany	Content of the company attribute of the hooked process metadata	String
hookPEimageType	Internal architecture of the hooked	EXEx32, EXEx64, DLLx32,

	process file	DLLx64
hookPEexeType	Type of executable of the hooked process	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
hookPEprevalence	Historical prevalence of the hooked process on Panda Security's systems	HIGH, LOW, MEDIUM
hookPEprevLastDay	Previous-day prevalence of the hooked process on Panda Security's systems	HIGH, LOW, MEDIUM
hookPEcat	Category of the hooked process	Goodware, Malware, PUP, Unknown, Monitoring
hookPEmwName	Malware name if the hooked process is classified as a threat	String

This table shows the operations performed by all the processes that make hooks. Since the malware that performs this type of operation is considered particularly dangerous because it intercepts communications, the ideal solution in this case is to filter the **Cat** field and dismiss anything that is classified as "Goodware" or "Monitoring".

21.3.5. Install table

This table logs all the information generated during installation of the Adaptive Defense 360 agents on the customer's computers.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
machineIP1	IP address of an additional network card if it is installed	IP address
machineIP2	IP address of an additional network card if it is installed	IP address
machineIP3	IP address of an additional network card if it is installed	IP address
machineIP4	IP address of an additional network card if it is installed	IP address

machineIP5	IP address of an additional network card if it is installed	IP address
ver	Version of the Adaptive Defense 360 agent	String
op	Operation performed	Install, Uninstall, Upgrade
osVer	Operating system version	String
osSP	Service Pack version	String
osPlatform	Operating System platform	WIN32, WIN64

Agent uninstall

Apart from the lists of uninstalled agents shown in the **Computers** window (**Unprotected** tab), it may be very useful to quickly locate computers that have uninstalled their agent in a given time period.

For this, you need to select the date and simply add a filter to the **op** field to select all the rows that have the "Uninstall" string. This will allow you to obtain a list of all the computers whose protection has been uninstalled and are therefore vulnerable to threats.

21.3.6. Monitoredopen table

This table logs the data files accessed by the applications run on the user's computer, and the processes that accessed the data

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
muid	Internal identifier of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentHash	Digest/hash of the file that accesses data	String
parentPath	Path of the process that accesses data	String
parentValidSig	Process that accesses digitally signed data	Boolean

parentCompany	Content of the Company attribute in the metadata of the file that accesses data	String
parentBroken	The file that accesses data is corrupted/defective	Boolean
parentImageType	Type of internal architecture of the file that accesses data	EXEx32, EXEx64, DLLx32, DLLx64
parentExeType	Type of executable that accesses data	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
parentPrevalence	Historical prevalence of the file that accesses data on Panda Security's systems	HIGH, LOW, MEDIUM
parentPrevLastDay	Previous-day prevalence of the file that accesses data on Panda Security's systems	HIGH, LOW, MEDIUM
parentCat	Category of the file that accesses data	Goodware, Malware, PUP, Unknown, Monitoring
parentMWName	Malware name if the file that accesses data is classified as a threat	String, (Null if the item is not malware)
parentPid	ID number of the process that accesses data on the customer's computer	String
childPath	Name of the data file accessed by the process. By default, only the file extension is indicated to preserve the privacy of the customer's data	String
loggedUser	User logged in on the computer at the time of file access	String

Access to user documents

As this table shows the files accessed by all processes run on the user's computer, it is quite simple to locate an information leak in case of infection.

Filter by the **parentCat** field to distinguish goodware from other possibilities. This way, you will obtain a list of accesses to data files by unclassified processes or processes classified as malware, which will allow you to see at a glance the impact of data leakage and take the necessary measures.

21.3.7. Notblocked table

This table logs the items that Adaptive Defense 360 has not scanned due to exceptional situations such as service timeout on startup, configuration changes, etc.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
muid	Internal identifier of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentHash	Digest/hash of the parent file	String
parentValidSig	Digitally signed parent process	Boolean
parentCompany	Content of the Company attribute of the parent process metadata	String
parentBroken	The parent file is corrupted or invalid	Boolean
parentImageType	Internal architecture of the parent process	EXEx32, EXEx64, DLLx32, DLLx64
parentExeType	Type of executable of the parent process	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
parentPrevalence	Historical prevalence **of the parent process** on Panda Security's systems	HIGH, LOW, MEDIUM
parentPrevLastDay	Previous-day prevalence of the parent process on Panda Security's systems	HIGH, LOW, MEDIUM
parentCat	Category of the parent file	Goodware, Malware, PUP, Unknown, Monitoring
ParentmwName	Malware name if the parent file is classified as a threat	String, (Null if the item is not malware)
childHash	Digest/hash of the child file	String
childValidSig	Digitally signed child process	Boolean

childCompany	Content of the company attribute of the child process metadata	String
childBroken	The child file is corrupted or invalid	Boolean
childImageType	Internal architecture of the child process	EXEx32, EXEx64, DLLx32, DLLx64
childExeType	Type of executable of the child process	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
childPrevalence	Historical prevalence of the child file on Panda Security's systems	HIGH, LOW, MEDIUM
childPrevLastDay	Previous-day prevalence of the child file on Panda Security's systems	HIGH, LOW, MEDIUM
childCat	Category of the child process	Goodware, Malware, PUP, Unknown, Monitoring
childmwName	Malware name if the child file is classified as a threat	String, (Null if the item is not malware)
cfgSvcLevel	Agent service configuration	• Learning: The agent allows the execution of unknown processes • Hardening: The agent prevents the execution of processes classified as threats • Block: The agent prevents the execution of processes classified as threats and unknown processes
realSvcLevel	Agent operation mode. The agent may temporarily have a configuration established that is different from the configuration being used for reasons attributable to the execution environment. Eventually, cfgSvcLevel and realSvcLevel must coincide.	• Learning: The agent allows the execution of unknown processes • Hardening: The agent prevents the execution of processes classified as threats • Block: The agent prevents the execution of processes classified as threats and unknown processes

responseCat	File category returned by the cloud	Unknown = 0 Goodware = 1 Malware = 2 Suspicious = 3 Compromised =4 GoodwareNotConfirmed = 5 PUP = 6 GoodwareUnwanted = 7
numCacheClassifiedElements	No. of classified items in the agent cache	Numeric

21.3.8. Ops Table

This table logs all operations performed by the processes seen on the customer's network.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
op	Operation performed	CreateDir, Exec, KillProcess, CreatePE, DeletePE, LoadLib, OpenCmp, RenamePE, CreateCmp
muid	Internal identifier of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentHash	Digest/hash of the parent file	String

parentPath	Parent process path	String
parentValidSig	Digitally signed parent process	Boolean
parentCompany	Content of the Company attribute of the parent file metadata	String
parentImageType	Type of internal architecture of the parent file	EXEx32, EXEx64, DLLx32, DLLx64
parentExeType	Type of the parent executable	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
parentPrevalence	Historical prevalence of the parent file on Panda Security's systems	HIGH, LOW, MEDIUM
parentPrevLastDay	Previous-day prevalence of the parent file on Panda Security's systems	HIGH, LOW, MEDIUM
parentCat	Category of the parent file	Goodware, Malware, PUP, Unknown, Monitoring
parentMWName	Name of the malware found in the parent file	String, (Null if the item is not malware)
childHash	Digest/hash of the child file	String
childPath	Child process path	String
childValidSig	Digitally signed child process	Boolean
childCompany	Content of the Company attribute of the child file metadata	String
childImageType	Type of internal architecture of the child file	EXEx32, EXEx64, DLLx32, DLLx64
childExeType	Type of child executable	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
childPrevalence	Historical prevalence of the child file on Panda Security's systems	HIGH, LOW, MEDIUM
childPrevLastDay	Previous-day prevalence of the child file on Panda Security's systems	HIGH, LOW, MEDIUM
childCat	Category of the child file	Goodware, Malware, PUP, Unknown, Monitoring
childMWName	Name of the malware found in the child file	String, (Null if the item is not malware)

ocsExec	Software considered as vulnerable was run or not	Boolean
ocsName	Name of the software considered vulnerable	String
ocsVer	Version of the software considered vulnerable	String
peCreationSource	Creation source of the executable process. Equivalent to the DriveType field	String
params	Run settings of the executable process.	String
toastResult	Result of the pop-up message shown	• OK • Timeout • Angry • Block • Allow
clientCat	Item category in the agent cache	Goodware, Malware, PUP, Unknown, Monitoring
action	Action performed	Allow, Block, BlockTimeout
serviceLevel	Agent mode	• Learning: The agent allows the execution of unknown processes • Hardening: The agent prevents the execution of processes classified as threats • Block: The agent prevents the execution of processes classified as threats and unknown processes
winningTech	Technology that triggered the action	• Unknown • Cache • Cloud • Context • Serializer • User • Legacyuser • Netnative • certifUA

21.3.9. Tabla ProcessNetBytes

This table logs the data usage of the processes seen on the customer's network. A log per process is sent every four hours approximately with the amount of data transferred since the last log was sent. The total amount of bytes sent and received per process will be the sum of all quantities received.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event was received by the Adaptive Defense 360 server	Date
machineName	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
version	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
muid	Internal ID of the customer's computer	String in the following format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
path	Program path and name	String
pid	Process ID	Numeric
bytesSent	Number of bytes sent by the process since the last event was generated	Numeric
bytesReceived	Number of bytes received by the process since the last event was generated	Numeric

Graphical representation of the applications that use the most data

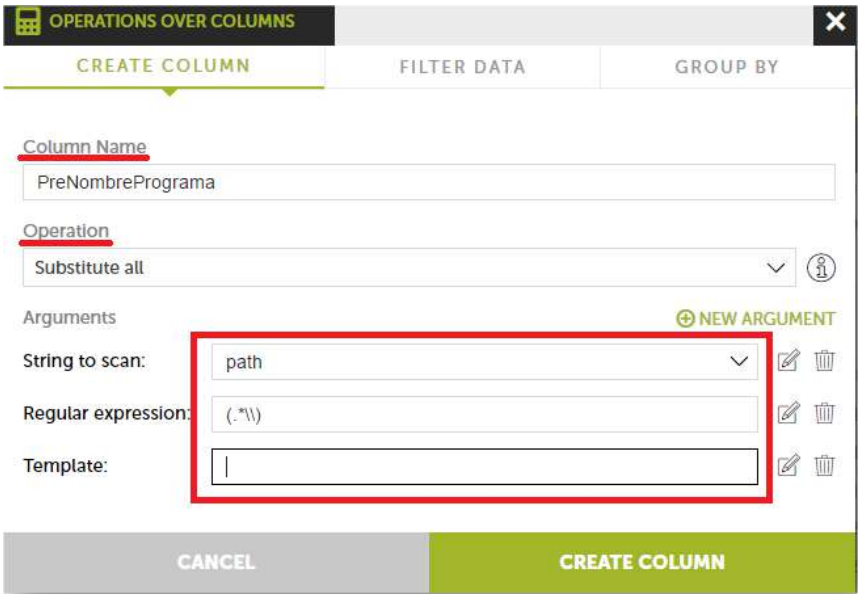
This table is most typically used to see which programs on the network computers use the most data. It is worth noting that this table doesn't differentiate between internal data and external data usage. That is, the total amount of data used by a process may be a mixture of data requested over the Internet and data obtained from the company's internal servers (mail servers, Intranet Web servers, files shared among workstations, etc.).

To be able to easily determine which network applications use the most data, a Voronoi diagram will be generated with the data received by each application run on the customer's network.

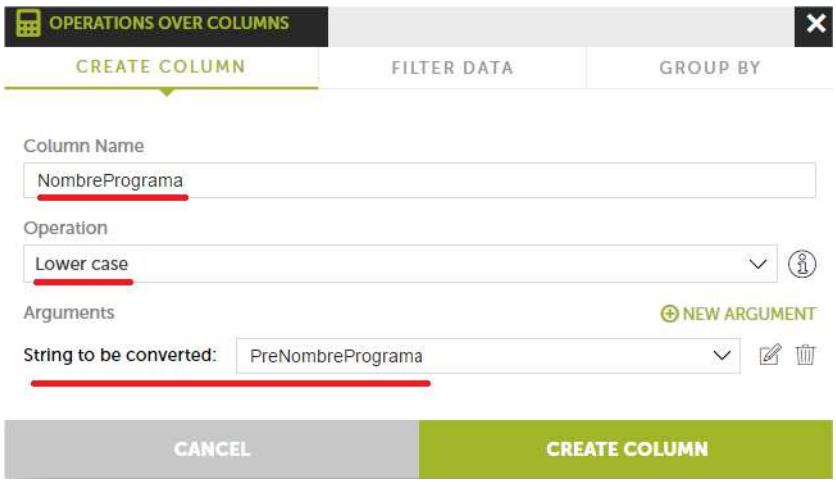
- Extract the name of the program run

As the name of each application run is logged in the **Path** field with its full path, the first step will be to extract the application name. To do that, create a new column named **ProgramName1** with the **Substitute All** operation and the following arguments:

- **String to scan:** Path column
- **Regular Expression:** (.*\ \)
- **Template:** (empty)



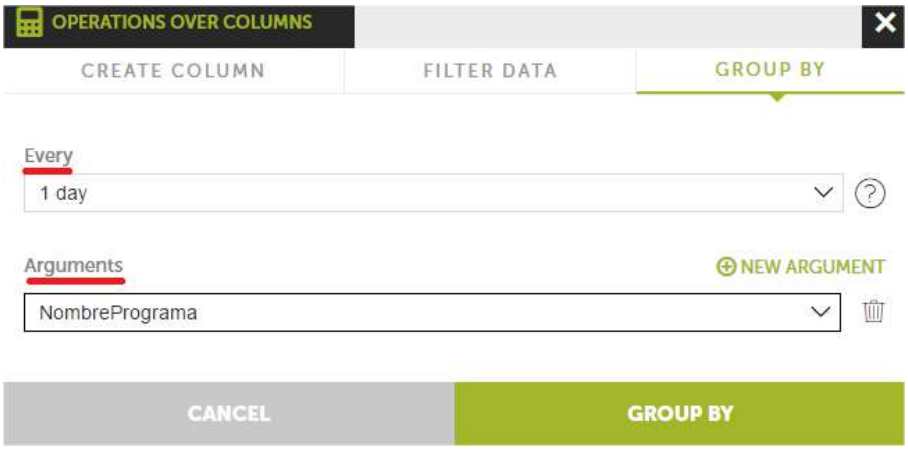
Then, filter by **null** to avoid processing wrong entries, and create another column -**ProgramName**- with the **Lower Case** operation over the previously created column (ProgramName1). This way, you'll get the names of all programs run in lowercase letters and without errors.



Another simpler method would be to use the table's hash field to identify running processes. This method, however, may result in a higher number of unique processes as each version of a program has its own hash value, which will make reading the diagram generated in the last step more difficult.

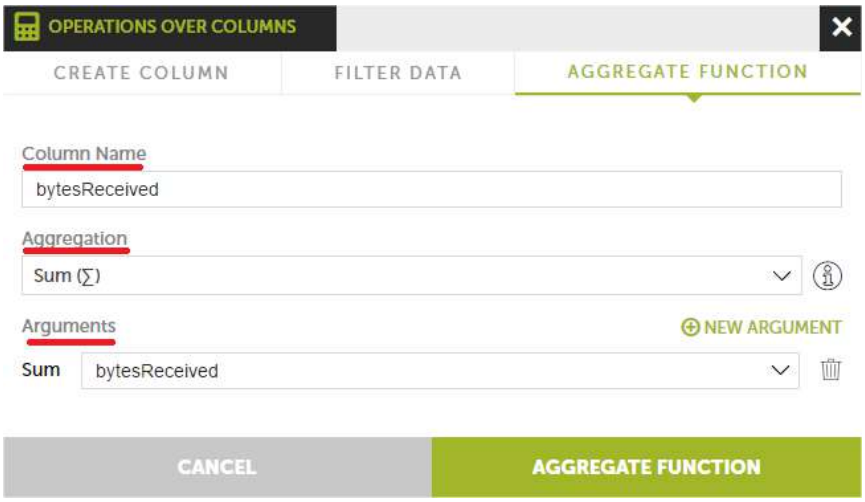
- Add a daily aggregation

Add an aggregation based on the number of days to cover (a daily aggregation in our example) along with the **ProgramName** field.



- Add a sum function

Add a sum function over the **bytesReceived** field to sum the total number of bytes received by each process.

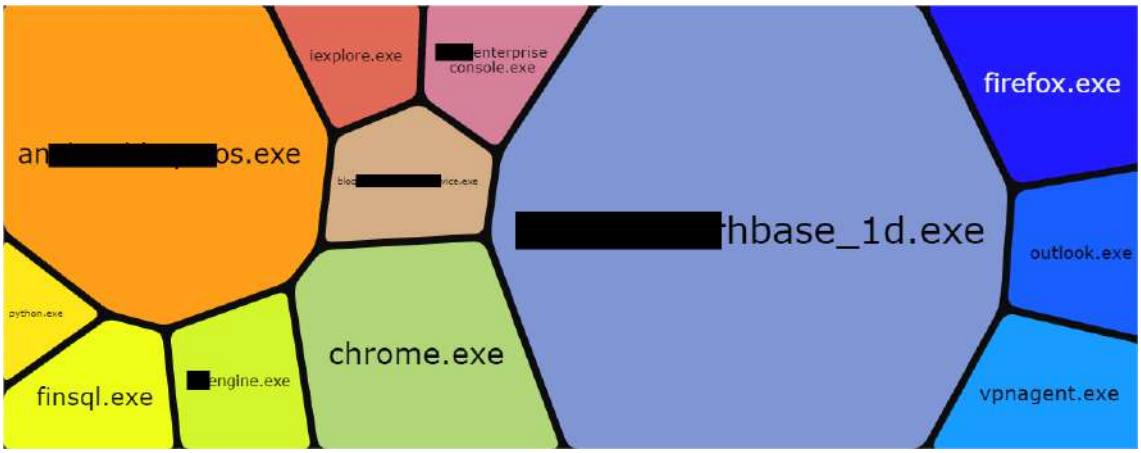


- Add a data filter

In order to see only the processes that have used more than a certain amount of data and simplify the diagram, you can filter the results by a figure: for example 100 megabytes (104857600 bytes).

- Create the Voronoi diagram

In **Signals**, drag the **ProgramName** field. Then, in **Value**, drag the **bytesReceived** field.



21.3.10. Registry table

This table logs all the operations performed by the processes seen on the customer's network on each computer's registry.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	User name of the process that modified the registry	String
op	Operation performed on the computer registry	ModifyExeKey, CreateExeKey
hash	Digest/hash of the process that modifies the registry	String
muid	Internal identifier of the customer's computer	String in the following format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
targetPath	Path of the executable that the registry modification points to	Type of drive where the process that accesses the registry resides

regKey	Registry key	String
driveType	Type of drive where the process that accesses the registry resides	String
path	Path of the process that modifies the registry	String
validSig	Registry key	Boolean
company	Registry key	String
imageType	Architecture of the file that accesses the registry	String
exeType	Type of executable	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
Prevalence	Historical prevalence of the process on Panda Security's systems	HIGH, LOW, MEDIUM
prevLastDay	Previous-day prevalence of the process on Panda Security's systems	HIGH, LOW, MEDIUM
Cat	Process category	Goodware, Malware, PUP, Unknown, Monitoring
mwName	Malware name if the process is classified as a threat	String, (Null if the item is not malware)

Persistence of installed threats

As this table shows registry access by all processes run on the user's computer, it is quite simple to see which malware managed to run and achieve persistence on the system.

There are many different registry branches that allow a program to be run at startup but the most used by Trojans and other types of threats are:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

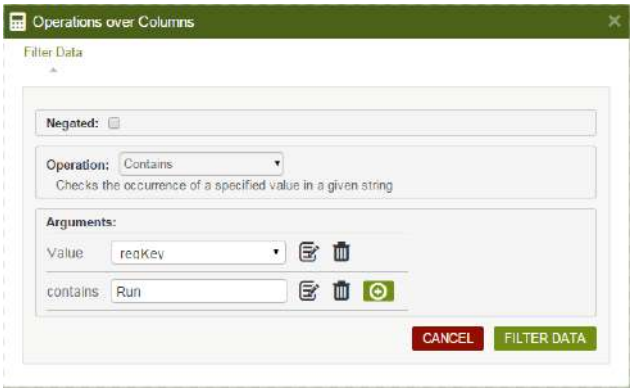
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

Almost all of those keys share the “Run” branch, so by filtering by the regKey field and searching for the “Run” substring you will be able to view all the information about the processes that added or removed startup branches.



After filtering the processes that manipulate the boot system, you can then apply subsequent filters that refine the initial search, using the **Cat** field to remove all programs classified as goodware from the list, as shown in the previous examples.

21.3.11. Socket table

This table logs all network operations performed by the processes seen on the customer's network.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
hash	Digest/hash of the process that makes the connection	String
muid	Internal identifier of the customer's computer	String in the following format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
driveType	Type of drive where the process that makes the connection resides	Fixed, Remote, Removable
path	Path of the process that makes the	String

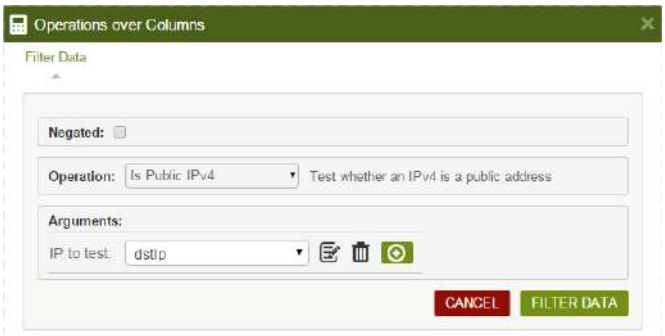
	connection	
protocol	Communications protocol used by the process	TCP, UDP, ICMP, ICMPv6,IGMP, RF
port	Communications port used by the process	0-65535
direction	Communication direction	Upload, Download, Bidirectional, Unknown
dstIp	Destination IP address	IP address
dstPort	Destination port	0-65535
dstIp6	IP v6 destination address	IP address
validSig	File that makes the digitally signed connection	Boolean
company	Content of the Company attribute in the metadata of the file that makes the connection	String
imageType	Internal architecture of the process that makes the connection	EXEx32, EXEx64, DLLx32, DLLx64
exeType	Type of executable of the process that makes the connection	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
prevalence	Historical prevalence on Panda Security's systems	HIGH, LOW, MEDIUM
prevLastDay	Previous-day prevalence on Panda Security's systems	HIGH, LOW, MEDIUM
cat	Category of the process that makes the connection	Goodware, Malware, PUP, Unknown, Monitoring
mwName	Malware name if the process that makes the connection is classified as a threat	String, (Null if the item is not malware)

Programs that most connect to the exterior

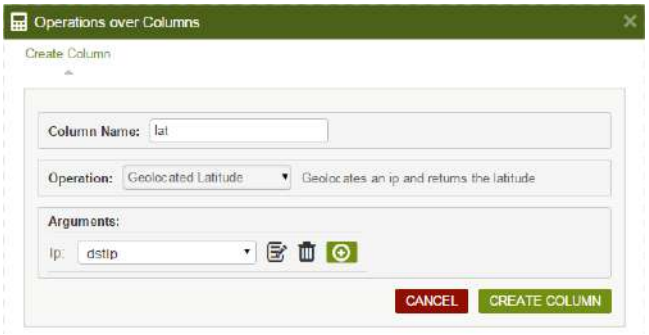
Similarly to the graphs in the console that geolocate the destinations of the connections made by the malware installed on the customer's network, you can obtain the destinations most connected by the legitimate software run on computers. For this, you need to follow the steps below:

Add a filter that removes all programs that are not considered legitimate. **For this, you need to set the Cat field to "Goodware"**

Add a filter that removes all connections to private IP addresses. For this, you need to create a column with the Is Public IPv4 function on the dstIp field, as shown in the figure



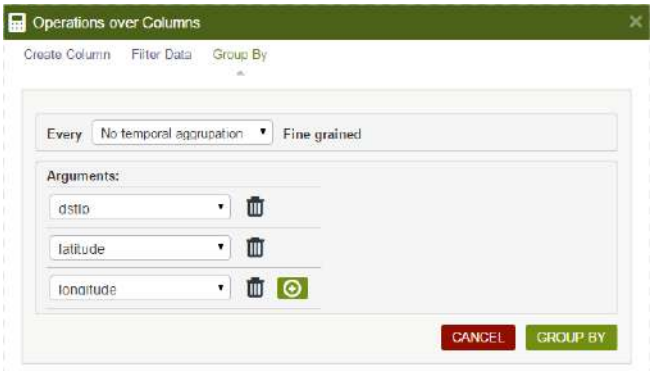
Add both latitude and longitude columns that extract the longitude and latitude from the dstIP field with the functions Geolocated Latitude/Longitude.



At this point, you'll have a list of connections from legitimate software to public IP addresses, and the latitude and longitude of each IP address. The coordinates obtained will be shown on the map-type graph as dots.

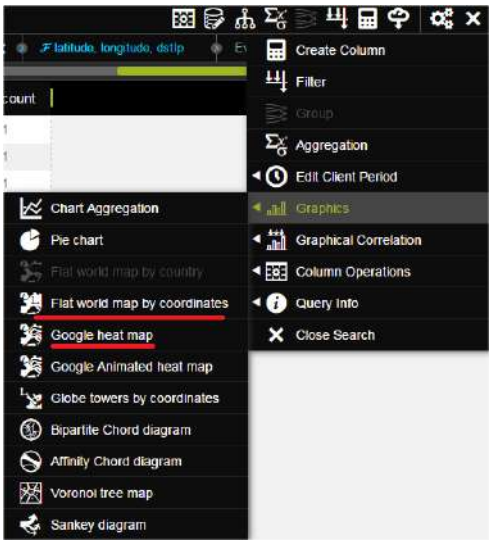
As the intention is to show the number of connections to the same IP address, you will need to form an aggrupation and add a counter to obtain the number of IP addresses repeated in an aggrupation.

Add an aggrupation with the arguments dstIP, latitude and longitude, without time limit (No temporal aggrupation).

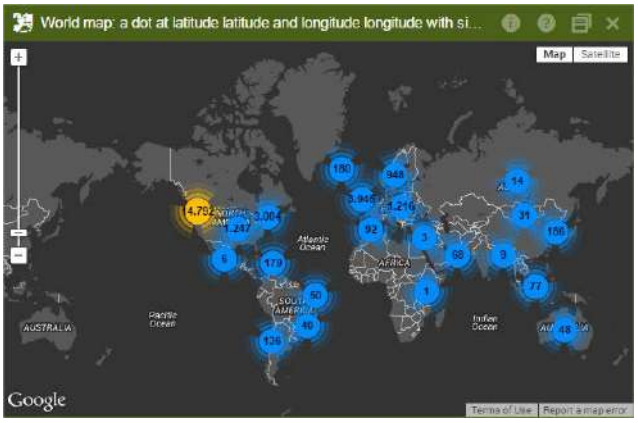


Add a counter type function.

Add a Flat world map by coordinates or Google heat map type graph using the count, latitude and longitude columns as data.



When dragging the columns to the relevant boxes, the selected map will be shown with the data represented by dots in different colors and sizes



21.3.12. Toast table

The Toast table logs an entry every time the agent shows a message to the customer

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event is received on the Adaptive Defense 360 server	Date
machine	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
ver	Version of the Adaptive Defense 360 agent	String
user	Process user name	String
muid	Internal identifier of the customer's computer	String in the following format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentHash	Digest/hash of the parent file	String
parentPath	Parent process path	String
parentValidSig	Digitally signed parent process	Boolean
parentCompany	Content of the Company attribute of the parent file metadata	String
parentImageType	Type of internal architecture of the parent file	EXEx32, EXEx64, DLLx32, DLLx64
parentExeType	Type of parent executable	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
parentPrevalence	Historical prevalence of the parent file on Panda Security's systems	HIGH, LOW, MEDIUM
parentPrevLastDay	Previous-day prevalence of the parent file on Panda Security's systems	HIGH, LOW, MEDIUM
parentCat	Category of the parent file	Goodware, Malware, PUP, Unknown, Monitoring
parentMWName	Name of the malware found in the parent file	String, (Null if the item is not malware)
childHash	Digest/hash of the child file	String
childPath	Path of the child process	String
childValidSig	Digitally signed child process	Boolean

childCompany	Content of the Company attribute of the child file metadata	String
childImageType	Type of internal architecture of the child file	EXEx32, EXEx64, DLLx32, DLLx64
childExeType	Type of child executable	Delphi, DOTNET, VisualC, VB, CBuilder, Mingw, Mssetup, Setupfactory, Lcc32, Setupfactory, Unknown
childPrevalence	Historical prevalence of the child file on Panda Security's systems	HIGH, LOW, MEDIUM
childPrevLastDay	Previous-day prevalence of the child file on Panda Security's systems	HIGH, LOW, MEDIUM
childCat	Category of the child file	Goodware, Malware, PUP, Unknown, Monitoring
clientCat	Item category in the agent cache	Goodware, Malware, PUP, Unknown, Monitoring
childMWName	Name of the malware found in the child file	String, (Null if the item is not malware)
serviceLevel	Agent mode	Learning: The agent allows the execution of unknown processes Hardening: The agent prevents the execution of processes classified as threats Block: The agent prevents the execution of processes classified as threats and unknown processes
winningTech	Technology that triggered the action	Unknown Cache Cloud Context Serializer User Legacyuser Netnative certifUA
cloudAccessOk	The cloud infrastructure is accessible to the agent	Boolean
SonFirstSeen	First time that the system saw the process that caused the pop-up warning to appear	Date
SonLastQuery	Last time that the process that caused the pop-up warning launched a query to the cloud	Date
PrevoiusClientCat	Previous category of the item that caused the pop-up warning	Numeric

ToastResult	Result of the pop-up warning	OK: The customer accepts the message Timeout: The pop-up warning disappears due to non-action by the user Angry: The user rejects the blocking Block Allow

21.3.13. VulnerableAppsFound table

This table logs all of the vulnerable application found on each computer on the customer's network. Unlike the **Ops** table, whose **ocsExec**, **ocsName** and **ocsVer** fields show the vulnerable applications that have been run on the network, this table shows all of the vulnerable applications that reside on computers.

Once every day, a log is sent per each detected application. If an application is deleted, the solution will stop sending the relevant event.

Name	Explanation	Values
eventdate	Date of the event on the customer's computer	Date
serverdate	Date when the event was received by the Adaptive Defense 360 server	Date
machineName	Name of the customer's computer	String
machineIP	IP address of the customer's computer	IP address
Ver	Version of the Adaptive Defense 360 agent	String
criticalSoftEventType	Indicates the existence of vulnerable software	Present
itemHash	Digest value of the vulnerable program found on the computer	String
Filename	Name of the vulnerable file	String
File path	Full path to the vulnerable file	String
Size	Size of the vulnerable file	Numeric
internalName	Content of the Name attribute of the vulnerable file metadata	String
companyName	Content of the Company attribute of the vulnerable file metadata	String
fileVersion	Content of the Version attribute of the vulnerable file metadata	String
productVersion	Content of the ProductVersion attribute of the vulnerable file metadata	String
filePlatform	Operating system platform	WIN32, WIN64

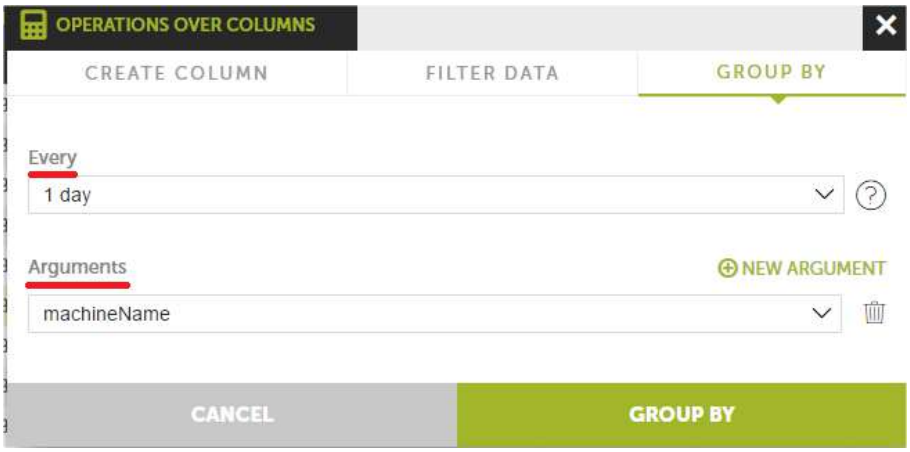
Computers with most vulnerable applications

This table is typically used to determine which computers on the network have most vulnerable applications.

In this example, no distinction is made between installed applications and applications that have simply been copied to the computer's hard disk. Also, bear in mind that an application copied N times to a computer doesn't count as one, but as N.

Add a 1-day aggregation

As vulnerable software events are generated on a daily basis, you can select to group all rows every day with the **machineName field as argument.** However, bear in mind that those computers that have not connected to the server on a particular day won't generate any events.



Add a **Count** function.

As each vulnerable program found on a computer generates one event per day, it will be enough to count the number of times that each computer appears in the aggregation.

Add a filter.

If the values obtained are too disperse, you may want to set a filter that excludes those computers that don't reach a certain threshold. To do that, simply add a **Greater or equal** filter with the appropriate value. Below that threshold there will be no computers on the list.

Generate a Voronoi diagram.

Use the **MachineName** field as **Signal** and the **Count** field as **Value** to generate a diagram that shows the most vulnerable computers on the network.

22. Integration with SIEM products

If you need integration with another SIEM system, please contact your sales advisor or service provider.

22.1. Introduction

Adaptive Defense 360 integrates with SIEM solutions, adding detailed information about the activity of the applications running on protected endpoints.

The information sent to the customer's SIEM system comes from the Adaptive Defense 360 server, which is why it is pre-prepared information (category, prevalence, etc.), and not simply raw data collected from the agents installed on users' computers.

Listed below are the SIEM systems compatible with Adaptive Defense 360:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora

QRadar

Adaptive Defense 360 integrates with **QRadar**, supporting logs in LEEF format.

AlienVault and ArcSight

Integration with **AlienVault** and **ArcSight** feeds data to the SIEM system in CEF (Common Event Format).

LookWise and the former Bitacora

LookWise and the former **Bitacora** can receive alert events and prevalence information from Adaptive **Defense 360**, i.e., information on when and on which computers of the IT infrastructure the detected malware has been seen.

22.2. Integration and bandwidth consumption

Integration with the customer's SIEM platform takes place using the SFTP protocol. Adaptive Defense 360 writes compressed files to the folder indicated by the customer. These files log network activity in the selected format.

On average, 1 MB of data is sent to the SIEM platform per day and per protected computer.

Integration with new SIEM platforms is a process that is undertaken on demand, so there is a possibility of integration with manufacturers such as **Splunk** and others.

23. Annex I: Centralized installation tools

Installation using Active Directory

Installation using the distribution tool

23.1. Introduction

Adaptive Defense 360 allows administrators to centrally install the Windows agent on small and medium-sized networks by using the centralized distribution tool (included free of charge) or third-party tools.

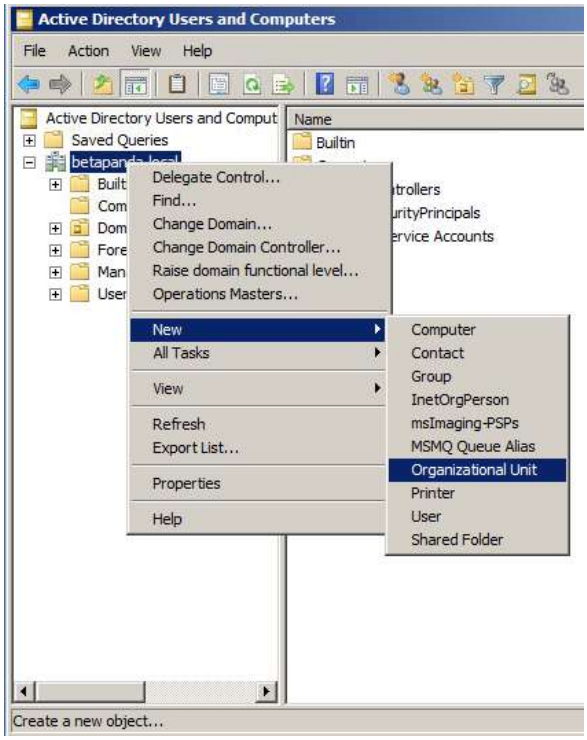
This chapter explains how to install the Adaptive Defense 360 agent on a Windows network with Active Directory and with the distribution tool included in the solution.

23.2. Installation using Active Directory

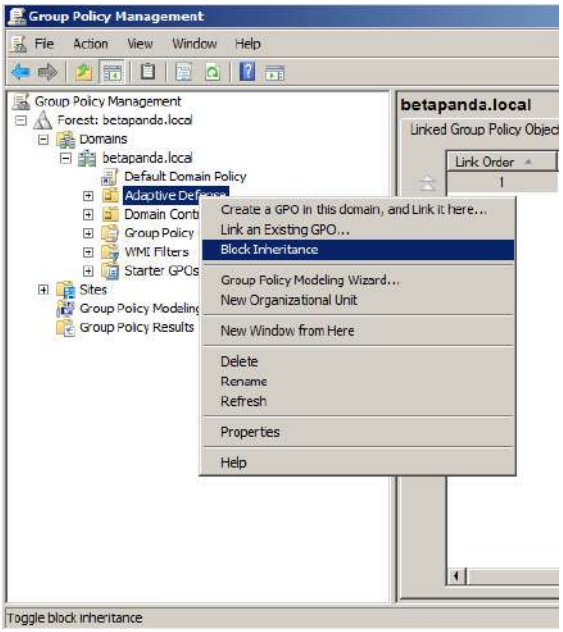
Below we detail the steps for installation using GPO (Group Policy Object).

Download and share the Adaptive Defense 360 installer: Move the Adaptive Defense 360 installer to a shared folder which is accessible to all the computers that are to receive the agent.

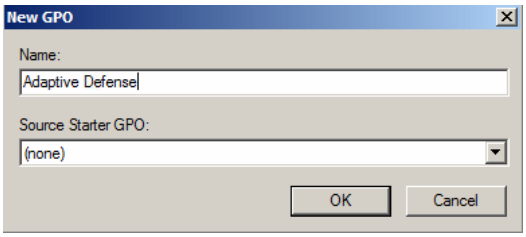
Open the "Active Directory Users and Computers" applet and create a new OU (Organizational Unit) called "Adaptive Defense".

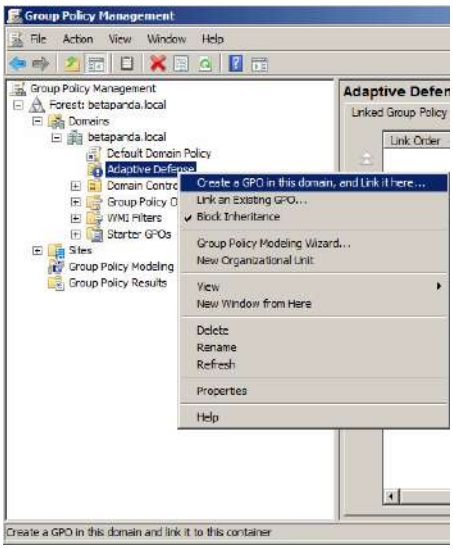


Open the Group Policy Management snap-in, and in Domains select the newly created OU to block inheritance.

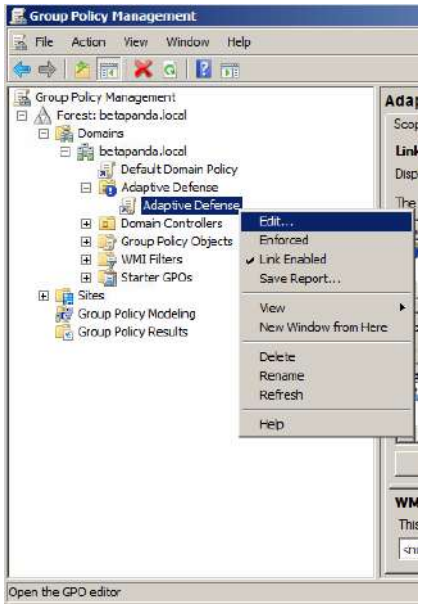


Create a new GPO in the "Adaptive Defense" OU.

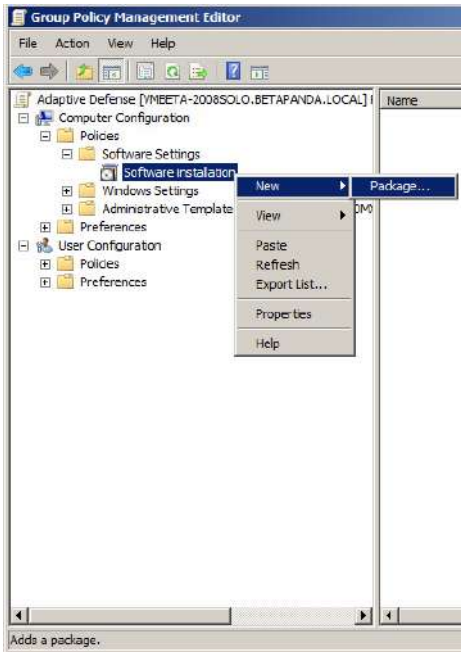


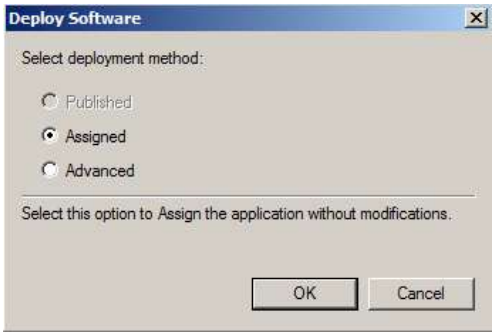


Edit the GPO.

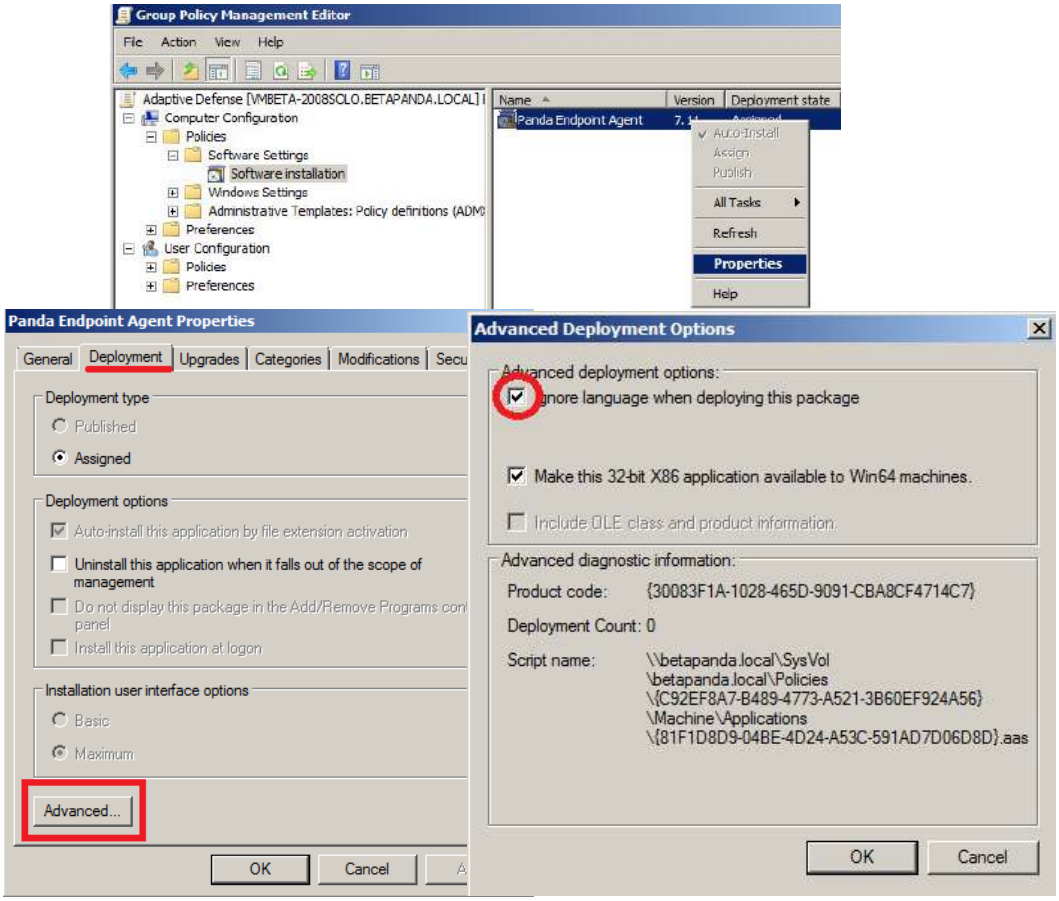


Add a new installation package which contains the Adaptive Defense 360 agent. To do this, you will be asked to add the installer to the GPO.





Once it has been added, go to Properties, Deployment, Advanced, and select the checkbox that bypasses checking the target operating system against the one defined in the installer.



Finally, in the previously created Adaptive Defense OU in "Active Directory Users and Computers", add all the network computers to which the agent will be sent.

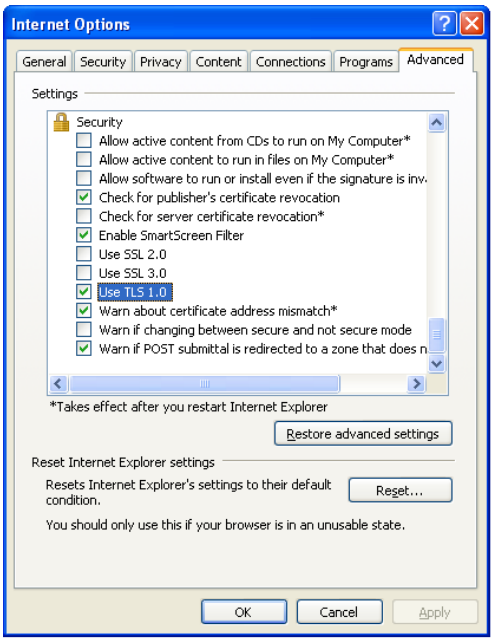
23.3. Installation using the distribution tool

23.3.1. Minimum requirements

Installing the agent with the distribution tool requires a Windows computer that meets the following minimum requirements:

- Operating system: Windows, 10, Windows 8.1, Windows 8, Windows 7 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows XP Professional (32-bit and 64-bit), Windows 2000 Professional, Windows Server 2000, Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2, Windows Home Server, Windows Server 2012 and Windows Server 2012 R2.
- Memory: 64 MB
- Hard disk: 20 MB
- Processor: Pentium II 300 MHz or equivalent
- Windows Installer 2.0 (Windows Installer 3.0 is recommended for remote uninstallation)
- Browser: Internet Explorer 6.0 or later
- Other:
    - Access to the Admin$ resource on the computers to which the protection will be distributed.
    - A user with administrator rights on the computers to which the protection will be distributed.

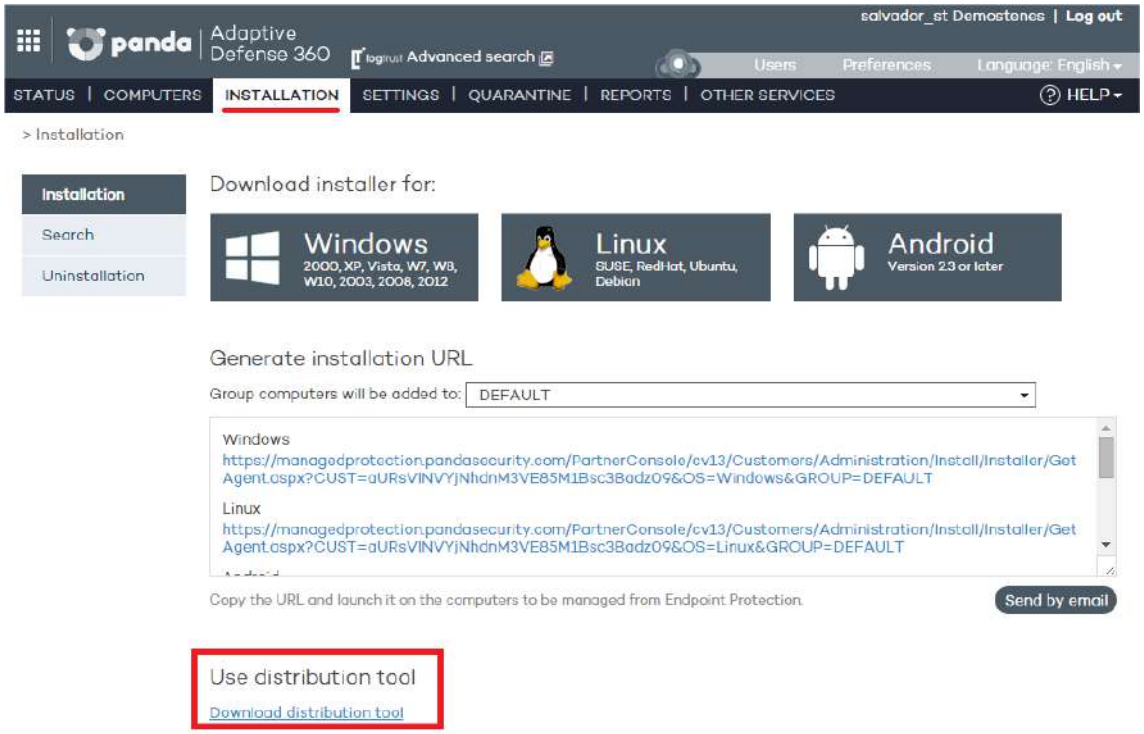
For the tool to work properly in Internet Explorer, you will need to disable the use of SSL in the Advanced Security Settings and enable the use of TSL:



23.3.2. How to deploy the agent

Follow the steps below to install the protection using Panda Security's distribution tool.

To download the distribution tool, go to the Installation window and click the Download distribution tool link.



Run the DistributionTool.msi file on the computer from which you will distribute the Adaptive Defense 360 agent to all computers on the network.

Once installed, run the tool from the Windows Start menu. The Protection installation screen will open, which will allow you to distribute the protection in two ways:

Distribution by domain

- Enter the group the computers whose protection you are going to install will be added to. This will determine the protection profile to be applied to those computers.
- In the network tree, select the domains or computers on which you want to install the protection.
- Use a user name and password with administrator permissions to carry out the installation. The user name must be entered in the domain\user name format.
- Once you have entered the credentials, click **Install** to generate the installation tasks.

Distribution by IP address or computer name

- Enter the group the computers whose protection you are going to install will be added to. This will determine the protection profile to be applied to those computers.
- Add the names or IP addresses of the computers whose protection you are going to install, separated by commas. You can also select IP address ranges (use the "-" symbol for ranges, e.g. 172.18.15.10 – 172.18.15.50).
- Use a user name and password with administrator permissions to carry out the installation. The user name must be entered in the domain\user name format.
- Click **Install** to generate the installation tasks.

- Check the console to see whether the installation task has been created successfully.
- After that, the protection installation will begin, completely transparently to end users.
- Restart the computer if prompted.

23.3.3. How to uninstall Adaptive Defense 360 centrally

The Adaptive Defense 360 distribution tool lets you uninstall the protection centrally, avoiding manual intervention from end users throughout the process. To do this, follow the steps below:

- In the tool's console, select **Uninstall protection**. You will be taken to the **Protection uninstallation** window, which allows you uninstall the protection in two ways:

Uninstall by domain

- In the network tree, select the computers or domains from which you want to uninstall the protection.
- Enter the uninstall password created during the installation process. If no password was created, leave this field blank.
- Use a user name and password with administrator permissions to perform the uninstall. The user name must be entered in the domain\user name format.
- If you want items removed from quarantine during the uninstall process, and computers to be automatically restarted after uninstall, select the relevant checkboxes.
- Once the data is entered, click **Uninstall** to generate the uninstall tasks.

Uninstall by IP address or computer name

- Enter the names or IP addresses of the computers whose protection you want to uninstall, separated by commas. You can also select IP address ranges (use the "-" symbol for ranges, e.g. 172.18.15.10 – 172.18.15.50).
- Enter the uninstall password created during the installation process. If no password was created, leave this field blank.
- Use a user name and password with administrator permissions to perform the uninstall. The user name must be entered in the domain\user name format.
- If you want items removed from quarantine during the uninstall process, and computers to be automatically restarted after uninstall, select the relevant checkboxes.
- Click **Uninstall** to generate the uninstall tasks.

  - Check the console to see whether the uninstall task has been created successfully.
  - After that, the uninstall process will begin, completely transparently to end users.
  - Restart the computers when prompted.

24. Appendix II: Communication with endpoints

Endpoint communication with the Internet

Bandwidth usage

Communication and stored data security

24.1. Introduction

This appendix describes the communication between the agents and the Adaptive Defense 360 server.

24.2. Endpoint communication with the Internet

24.2.1. Communication periods

The Adaptive Defense 360 agents installed on network computers communicate with the server at regular intervals. These intervals will depend on the type of communication being transmitted. The figures below indicate the **maximum** time that can elapse before an event that must be transmitted to the server is actually sent.

- **Check for settings changes in the console**: Every 15 minutes.
- **Changes to the computer settings** (name, IP address, MAC address, OS version, Service pack, etc.): Every 12 hours.
- **Computer settings** (no changes): Every 24 hours
- **Check for new signature file**: 4 hours by default. See Chapter 13 to change this setting.
- **Check for updates to the protection engine**: 12 hours by default. See Chapter 13 to change this setting.

24.2.2. Internet access

The following table shows a summary of how endpoints protected with Adaptive Defense 360 access the Internet for tasks that require communication over the Internet.

Endpoint Status	Communication with the server	Signature file updates	Product installation and upgrades	Access to Collective Intelligence (CI)
Connected to the Internet	From the endpoint or another endpoint configured for such purpose.	It shares signature files downloaded by other networked endpoints thanks to Adaptive Defense 360's P2P technologies. It only downloads signature files provided no other endpoint has	It shares upgrade packages downloaded by other networked endpoints thanks to Adaptive Defense 360's P2P technologies. It only downloads upgrade packages provided no other endpoint has done it previously. It is possible to specify an endpoint to download upgrade	Connections to Collective Intelligence are established from each endpoint.*

		done it previously. It is possible to specify an endpoint to download signature files from the server. This endpoint will also act as a signature repository, so that signature files will not be downloaded again when requested by another computer.	packages from the server.	
Not connected to the Internet (but at least one networked endpoint has an Internet connection)	From the endpoint with the Internet connection or the endpoint configured to channel all communications with the server.	Updates take place from the endpoint with the Internet connection, or the endpoint configured to channel all communications with the server.	Upgrades take place from the endpoint with the Internet connection, or the endpoint configured to channel all communications with the server.	It is not possible to access Collective Intelligence from endpoints without an Internet connection*.

* If endpoints access the Internet using a corporate proxy server, Adaptive Defense 360 will use it as well. The proxy server to use can be configured in the Adaptive Defense 360 settings.

24.3. BANDWIDTH USAGE SUMMARY TABLE

The following table shows a summary of the bandwidth used by Adaptive Defense 360 for each type of communication.

Communication	Approximate bandwidth usage
Product installation	8.18 MB: Installer and communications agent 60.5 * MB: Endpoint protection package
Communication with the server	240 KB every 12 hours (190 KB in messages sent every 15 minutes to check for configuration changes, and 50 KB in status, settings and reports messages)
Signature file updates**	25 MB the first time only, after installing the protection.

	200-300 KB every 24 hours for signature file patches.
Sending of the actions triggered by each running process	1 MB per day and per endpoint
Product upgrades**	8.18 MB: Communications agent 60.5 MB: Endpoint protection package A product upgrade takes place every 6 months approximately.
Queries to Collective Intelligence	Real-time, on-access protection 500 KB: Bandwidth used on the first day, when the cache is empty. 35-100 KB: Bandwidth used after the first day, once the information is cached. Full scan of the computer 200-500 KB: First full scan of the computer. 50-200 KB: Subsequent full scans of the computer.

* 46.2 MB for the 64-bit installer

** Signature file and product updates are downloaded by a single endpoint on the network, and shared by the other networked endpoints thanks to Adaptive Defense 360's P2P technologies.

The signature file patches will be different depending on how outdated the signature files are. For example, if an endpoint has a two-day old signature file and another one has a one-day old signature file, the patches to download will be different.

If you select a computer to act as a proxy/repository server, all communications except queries to Collective Intelligence will take place through that computer. Additionally, signature files will be stored in the computer selected as the repository (it will not be necessary to download them again if requested by another computer on the network).

ESTIMATING BANDWIDTH USAGE

Suppose you have a local network consisting of N interconnected computers, and you install Adaptive Defense 360 on them.

The bandwidth usage will be approximately as follows.

Communication type	Internet bandwidth consumption by N PCs	Local network bandwidth consumption by N PCs
Product installation (1 time only)	8.18 MB for the communications agent & the installer **x N computers** + 60.5 MB for the endpoint protection package	8.18 MB del instalador y agente de comunicaciones x **N computers** 60.5 MB for the endpoint protection package
Communication with the server	240 KB every 12 hours **x N computers**	240 KB every 12 hours **x N computers**

Sending of the actions triggered by each running process	1 MB per day **x N computers**	1 MB per day **x N computers**
Signature file updates	25 MB the first time only, after installing the protection **x N computers** + 160 KB every 24 hours for signature file patches **x N computers**	25 MB the first time only, after installing the protection + 160 KB every 24 hours for signature file patches
Product upgrades (approx. every 6 months)	8.18 MB for the communications agent & the installer **x N computers** + 60.5 * MB for the endpoint protection package	8.18 MB for the communications agent & the installer **x N computers** + 60.5 * MB for the endpoint protection package
Queries to Collective Intelligence	500 KB the first time **x N computers** + 35-100 KB every day **x N computers**	500 KB the first time **x N computers** + 35-100 KB every day **x N computers**

* 46.2 MB for the 64-bit installer

24.4. Security of communications and stored data

The new Adaptive Defense 360 protection model requires information about the actions taken by applications installed on customers' computers.

The collection of data by Adaptive Defense 360 is strictly in accordance with the guidelines set out below:

The only information collected is that regarding Windows executable files, (.exe, .dll, etc.) that are run or loaded on the user's computer. No information is gathered about data files.

The file attributes are normalized, deleting any information referring to the logged in user. So, for example, the file paths are normalized as LOCALAPPDATA\name.exe instead of c:\Users\USER_NAME \AppData \Local\name.exe)

The only URLs collected are those from which executable files are downloaded. The URLs visited by users are not collected.

There is no relation between the data and the user in the data collected.

Under no circumstances will Adaptive Defense 360 send personal information to the cloud.

As essential information to support the new protection model, Adaptive Defense 360 sends information about the actions taken on each computer.

Attribute	Data	Description	Example
File	Hash	Hash of the file to which the event refers.	N/A
URL	URL	Address from where an executable file was downloaded.	http://www.malware.com/executable.exe
Path	Path	Normalized path of the file to which the event refers	APPDATA\
Registry	Key / Value	Windows registry key and its corresponding content.	HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\Panda Research\Minerva\ Version = 3.2.21
Operation	Operation ID	Identifier of the operation (creation/modification/loading/etc. of an executable, downloading of an executable, communication, etc.)	'0' type events indicate the execution of an executable
Communication	Protocol /Port/ Address	The communication event of a process (not its content) along with the protocol and address	Malware.exe sends data by UDP on port 4865
Software	Software installed	The list of software installed on the endpoint according to the Windows API.	Office 2007, Firefox 25, IBM Client Access 1.0

25. Appendix III List of Uninstallers

On installing Adaptive Defense 360, other security products might be detected on the computer. In that case, the following products will be automatically uninstalled before installing Adaptive Defense 360:

VENDOR	PRODUCT NAME
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32-bit Edition) AVG Internet Security 2013 (64-bit Edition) AVG AntiVirus Business Edition 2013 (32-bit Edition) AVG AntiVirus Business Edition 2013 (64-bit Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32-bit* AVG Internet Security Business Edition 2011 64-bit (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVG Free v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir Personal Edition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir Personal Edition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x
CA	CA Total Defense for Business Client V14 (32-bit Edition) CA Total Defense for Business Client V14 (64-bit Edition) CA Total Defense R12 Client (32-bit Edition) CA Total Defense R12 Client (64-bit Edition)
Bitdefender	BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32-bit) Check Point Endpoint Security 8.x (64-bit)
ESET	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32-bit) ESET NOD32 Antivirus 4.X (32-bit) ESET NOD32 Antivirus 4.X (64-bit) ESET NOD32 Antivirus 5 (32-bit) ESET NOD32 Antivirus 5 (64-bit)

	ESET NOD32 Antivirus 6 (32-bit) ESET NOD32 Antivirus 6 (64-bit) ESET NOD32 Antivirus 7 (32-bit) ESET NOD32 Antivirus 7 (64-bit)
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
Kaspersky	Kaspersky Endpoint Security 10 for Windows (32-bit Edition) Kaspersky Endpoint Security 10 for Windows (64-bit Edition) Kaspersky Endpoint Security 8 for Windows (32-bit Edition) Kaspersky Endpoint Security 8 for Windows (64-bit Edition) Kaspersky Anti-Virus 2010 9.0.0.459* Kaspersky® Business Space Security Kaspersky® Work Space Security Kaspersky Internet Security 8.0, 7.0, 6.0 (with Windows Vista + UAC, you must disable UAC) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (with Windows Vista + UAC, you must disable UAC) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee SaaS Endpoint Protection 6.x, 5.X McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0 McAfee Internet Security Suite 2007 McAfee Total Protection Service 4.7* McAfee Total Protection 2008
Norman	Norman Security Suite 10.x (32-bit Edition) Norman Security Suite 10.x (64-bit Edition) Norman Security Suite 9.x (32-bit Edition) Norman Security Suite 9.x (64-bit Edition) Norman Endpoint Protection 8.x/9.x Norman Virus Control v5.99
Norton	Norton Antivirus Internet Security 2008* Norton Antivirus Internet Security 2007 Norton Antivirus Internet Security 2006
Microsoft	Microsoft Security Essentials 1.x Microsoft Forefront EndPoint Protection 2010 Microsoft Security Essentials 4.x Microsoft Security Essentials 2.0 Microsoft Live OneCare Microsoft Live OneCare 2.5*
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205

PC Tools	Spyware Doctor with AntiVirus 9.x
Sophos	Sophos Anti-virus 9.5 Sophos Endpoint Security and Control 10.2 Sophos Endpoint Security and Control 9.5 Sophos Anti-virus 7.6 Sophos Anti-virus SBE 2.5* Sophos Security Suite
Symantec	Symantec.cloud - Endpoint Protection.cloud 21.x (32-bit) Symantec.cloud - Endpoint Protection.cloud 21.x (64-bit) Symantec EndPoint Protection 12.x (32-bit) Symantec EndPoint Protection 12.x (64-bit) Symantec EndPoint Protection 11.x (32-bit) Symantec EndPoint Protection 11.x (64-bit) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
Trend Micro	Trend Micro Worry-Free Business Security 8.x (32-bit Edition) Trend Micro Worry-Free Business Security 8.x (64-bit Edition) Trend Micro Worry-Free Business Security 7.x (32-bit Edition) Trend Micro Worry-Free Business Security 7.x (64-bit Edition) Trend Micro Worry-Free Business Security 6.x (32-bit Edition) Trend Micro Worry-Free Business Security 6.x (64-bit Edition) Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x
Comodo AntiVirus	Comodo Antivirus V 4.1 32-bit
Panda Security	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX and later
	Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX and later
	Panda Global Protection 2015* Panda Internet Security 2015* Panda Antivirus Pro 2015* Panda Gold Protection* Panda Free Antivirus
	Panda Global Protection 2014* Panda Internet Security 2014* Panda Antivirus Pro 2014* Panda Gold Protection*
	Panda Global Protection 2013* Panda Internet Security 2013*

	Panda Antivirus Pro 2013*
	Panda Global Protection 2012* Panda Internet Security 2012* Panda Antivirus Pro 2012*
	Panda Global Protection 2011* Panda Internet Security 2011* Panda Antivirus Pro 2011* Panda Antivirus for Netbooks (2011)*
	Panda Global Protection 2010 Panda Internet Security 2010 Panda Antivirus Pro 2010 Panda Antivirus for Netbooks
	Panda Global Protection 2009 Panda Internet Security 2009 Panda Antivirus Pro 2009
	Panda Internet Security 2008 Panda Antivirus + Firewall 2008 Panda Antivirus 2008
	Panda Internet Security 2007 Panda Antivirus + Firewall 2007 Panda Antivirus 2007

* * Panda 2015, 2014, 2013, 2012 products need a reboot to get uninstalled.

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

F-Secure PSB for Workstations 9.00: During the installation process of the Adaptive Defense 360 agent in Windows 7 and Windows Vista, the user will be prompted to select the Allow option.

*AVG Internet Security Business Edition 2011 32-bit *: During the Adaptive Defense 360 agent installation process, the user will be prompted to select the Allow option in several windows.

AVG Internet Security Business Edition 2011 64-bit (10.0.1375) - During the Adaptive Defense 360 agent installation process, the user will be prompted to select the Allow option in several windows.

* Kaspersky Anti-Virus 6.0 for Windows Workstations:

During the Adaptive Defense 360 agent installation process in 64-bit platforms, the user will be prompted to select the Allow option in several windows.

In order to uninstall the protection, the Kaspersky protection should not be password protected.

While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* F-Secure PSB for Workstations 9.00: During the Adaptive Defense 360 agent installation process, the user will be prompted to select the Allow option in two windows.

* AVG Anti-Virus Network Edition 8.5: During the Adaptive Defense 360 agent installation process, the user will be prompted to select the Allow option in two windows.

* Panda Antivirus 2011 products do not uninstall correctly on Windows Vista 64-bit. While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* Panda Cloud Antivirus 1.4 Pro and Panda Cloud Antivirus 1.4 Free: While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

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

* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically with Windows Vista x86 with UAC enabled*

*ESET NOD32 Antivirus 3.0.XX (2008) does not uninstall automatically on 64-bit platforms.

*ESET Smart Security 3.0 does not uninstall automatically on 64-bit platforms.

* ESET NOD32 Antivirus 2.7: After installation of the Adaptive Defense 360 agent on the computer, it will restart automatically without displaying any notification or asking for user confirmation.

ESET NOD332 Antivirus 2.70.39: After installation of the Adaptive Defense 360 agent on the computer, it will restart automatically without displaying any notification or asking for user confirmation.

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

* eTrust Antivirus 7.1 does not uninstall correctly on 64-bit platforms (Windows 2003 64-bit and Windows XP 64-bit).

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

* BitDefender Free Edition 2009 12.0.12.0. On Windows Vista and UAC enabled, while the program is being uninstalled, the user will be prompted to select the option Allow in the UAC window.

* Kaspersky Anti-Virus 2010 9.0.0.459. On systems with UAC enabled, while the program is being uninstalled, the user will be prompted to select the option Allow in the UAC window.

* Kaspersky Anti-Virus 8. On Windows Vista and UAC enabled, while the program is being uninstalled, the user will be prompted to select the option Allow in the UAC window.

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

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

If you have a program not included on this list, contact the corresponding vendor to find out how to uninstall it before installing Adaptive Defense 360.

26. Appendix IV: Key concepts

Remote access

Technology that enables someone to connect and interact remotely with a user's computer**.**

Network adapter

The network adapter allows communication between devices connected to each other, and also allows resources to be shared between two or more computers. It has a unique identifier.

Adware

Program that automatically runs, displays or downloads advertising to the computer.

Agent

The agent is responsible for communication between the managed computers and the Adaptive Defense 360 servers, as well as managing local processes.

Alert

A message concerning the protection activity of Adaptive Defense 360 when it may require action on the part of the user or administrator. Administrators receive alerts via email, and users receive alerts generated by the agent which appear on the device desktop.

Forensic analysis

A series of actions and processes carried out by network administrators with special tools in order to track a malicious program and evaluate the consequences when malware has managed to infect a network computer.

Heuristic analysis

Heuristic analysis analyzes hundreds of characteristics of a software file.

This determines the potential of the software to carry out malicious or damaging actions when run on a computer, and whether it is a virus, spyware, a Trojan, a worm, etc.

Antivirus

Program designed to detect and eliminate viruses and other threats.

APT (Advanced Persistent Threat)

A set of processes controlled by hackers and aimed at infecting customers' networks through diverse infection vectors simultaneously and designed to go undetected by traditional antivirus programs for long periods of time. The main aim of these threats is financial (theft of confidential information, intellectual property, etc.).

Signature file

The file that allows the antivirus to detect threats.

ARP (Address Resolution Protocol)

Protocol used for the resolution of network layer addresses into link layer addresses. On IP networks it translates IP addresses to physical MAC addresses.

Audit

An Adaptive Defense 360 mode that lets you see the processes run on the protected network computers without taking any remedial action (disinfection or blocking).

Notices

Also called **Incidents**, these show on the Web console the activity of malicious programs detected by the Adaptive Defense 360 advanced protection.

Block

This prevents the running of programs cataloged as malware or unclassified, according to the configuration of Adaptive Defense 360 set by the administrator.

Broadcast

Broadcasting of packets across data networks. One data packet can reach all computers on the same subnet. Broadcast packets don't go through routers and use different addressing methodology to differentiate them from unicast packets.

Adaptive protection cycle

A new security focus based on the integration of a group of services providing protection, detection, monitoring, forensic analysis and problem resolution. All these are centralized in a single administration console accessible from anywhere at any time.

Malware life cycle

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.

Web console

Tool for configuring the protection, as well as distributing and managing the agent across all the computers on your network. You can also see the security status of your network and generate and print the reports you want.

Quarantine

Repository of files that are suspected of being malicious or that cannot be disinfected, as well as the spyware and hacking tools detected.

Disinfectable

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

DHCP

Service that assigns IP addresses to new computers on the network.

Dialer

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

IP address

Number that identifies a device interface (usually a computer) on a network that uses the IP protocol.

MAC address

Hexadecimal, 48-bit unique identifier of a network card or interface. It is individual: each device has its own MAC address.

Active Directory

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed service for finding a range of information on network environments.

Linux distribution

Set of software packets and libraries that comprise an operating system based on the Linux kernel.

DNS (Domain Name System)

Service that translates domain names to different types of information, generally IP addresses.

Domain

Windows network architecture where the management of shared resources, permissions and users is centralized in a server called a Primary Domain Controller or Active Directory.

Excluded computers

Computers selected by the user which are not protected by the solution. Excluded computers are only displayed in the Excluded section, they are not shown anywhere else in the console. No warnings about them are displayed either. Bear in mind that you can undo these exclusions at any time.

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 will be automatically removed from the list of computers without a license as soon as new licenses are purchased.

Master Browser

The role of a computer on a Windows network that keeps a list of all devices that connect to that network segment.

Exploit

A known software flaw exploited by malware to cause a series of errors to the advantage of the malware that initiates the action.

Firewall

This is a barrier that can protect information on a system or network when there is a connection to another network, for example, the Internet.

URL filter by category

Control over the URLs requested by Internet users, denying or granting permission to access pages based on a URL database divided into subjects or categories.

Fragmentation

On data transmission networks, when the MTU of the underlying protocol is less than the size of the transmitted packet, routers divide the packet into smaller segments (fragments) which are routed independently and assembled at the destination.

Peer To Peer (P2P) funcionality

A Peer-to-Peer network is a network without fixed client or servers, but a series of nodes that work simultaneously as clients and servers for the other nodes on the network. This is a legal way of sharing files, similar to sending them via email or instant messaging, but more efficient.

In the case of Adaptive Defense 360, the P2P feature reduces Internet bandwidth consumption, as computers that have already updated a file from the Internet then share the update with other connected computers. This prevents saturating Internet connections.

Proxy funcionality

This feature allows Adaptive Defense 360 to operate in computers without Internet access, accessing the Web through an agent installed on a computer on the same subnet.

Geolocation

Geographical positioning of a device on a map from its coordinates.

Goodware

A file which after analysis has been classified as legitimate and safe.

Group

In Adaptive Defense 360, a group is a set of computers to which the same protection configuration profile is applied. Adaptive Defense 360 includes an initial group -*Default group*- to which the administrator can add all the computers to protect. New groups can also be created.

Workgroup

Architecture in Windows networks where shared resources, permissions and users can be independently managed from each computer.

Hardening

An Adaptive Defense 360 mode that blocks unknown programs downloaded from the Internet as well as all files classified as malware.

Distribution tool

Once downloaded from the Internet and installed on the administrator's PC, the distribution tool lets the administrator remotely install and uninstall the protection on selected network computers. In Adaptive Defense 360, the distribution tool can only be used to deploy the protection to Windows computers.

Hacking tool

Programs that can be used by a hacker 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.).

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

ICMP (Internet Control Message Protocol)

Error notification and monitoring protocol used by the IP protocol on the Internet.

IDP (Identity Provider)

Centralized service for managing user identity verification.

IP (Internet Protocol)

Principal Internet protocol for sending and receiving datagrams generated on the underlying link level.

Joke

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

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.

Notifications

Alerts for administrators about important issues concerning the Adaptive Defense 360 platform such as new versions of the endpoint protection, licenses about to expire, etc.

Lock

An Adaptive Defense 360 mode that blocks unknown programs and those classified as malware.

Machine learning

This is a branch of artificial intelligence whose aim is to develop technologies that can create programs from unstructured information delivered in the form of examples.

Malware Freezer

A function of the quarantine whose goal is to prevent the loss of data due to false positives. All files classified as malware or suspicious are sent to quarantine, thereby avoiding deleting and losing data if the classification is wrong.

MD5 (Message-Digest Algorithm 5)

This is a cryptographic hash function producing a 128-bit value that represents data input. The MD5 hash calculated on a file can unequivocally identify it or check that it has not been tampered with.

MTU (Maximum transmission unit)

Maximum packet size that a given protocol can transmit.

Cloud

Cloud computing is a technology that allows services to be offered across the Internet. In IT circles, the word *'cloud'* (or 'the cloud') is used as a metaphor for 'the Internet'.

OU (Organizational Unit)

Hierarchical method for classifying and grouping objects stored in directories.

Partner

A company that offers Panda Security products and services.

Profile

A profile is a specific protection configuration. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

Phishing

A technique for obtaining confidential information fraudulently. The information targeted includes passwords, credit card numbers and bank account details.

Local process

Local processes are responsible for performing the tasks necessary to implement and manage the protection on computers.

Potentially Unwanted Programs

A program that may be unwanted, despite the possibility that users consented to download it.

They are usually installed legitimately as part of another program.

Protocol

System of regulations and specifications used for exchanging data. One of the most commonly used is TCP-IP.

Proxy

A proxy server acts as an intermediary between an internal network (an intranet, for example) and an external connection to the Internet. This allows a connection for receiving files from Web servers to be shared.

Port

A numeric ID assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Responsive / Adaptable Web design (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.

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.

Rootkits

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is not malicious in itself, but is used by hackers to cover their tracks in previously compromised systems. There are types of malware that use rootkits to hide their presence on the system.

SCL (Spam Confidence Level)

The spam confidence level (SCL) is the normalized value assigned to a message that indicates the likelihood that the message is spam, based on the characteristics of a message (such as the content, message header, etc.).

Accumulated knowledge server

A service that stores and relates the knowledge collected by Adaptive Defense 360 from the customer's network in real time. It enables searches to be run and advanced graphs to be generated to interpret the information.

Exchange server

Mail server developed by Microsoft. Exchange Servers store inbound and/or outbound emails and distribute them to users' email inboxes. To connect to the server and download their email, users must have an email client installed on their computers.

SMTP server

Server that uses SMTP -simple mail transfer protocol- to exchange email messages between computers.

SIEM (Security Information and Event Management)

Software that provides storage and real-time analysis of the alerts generated by network devices and the applications on the network.

Suspicious file

A file with a high probability of being malware after having been analyzed by the Adaptive Defense 360 protection on the user's computer.

Spam

This refers to unsolicited email messages that normally contain advertising and are generally sent out massively and can have a range of negative effects on the recipient.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data on a network.

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignation and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Spyware

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and which collects personal data.

TCO (Total Cost of Ownership)

Financial estimate of the total direct and indirect costs of owning a product or system.

TLS (Transport Layer Security)

New version of protocol SSL 3.0

Network topology

Physical or logical map of network nodes.

Trojans

Programs that reach computers disguised as harmless programs that install themselves on computers and carry out actions that compromise user confidentiality.

Public network

This is the type of network you find in Internet cafes, airports, etc. Visibility of computers is restricted on such networks, and there are restrictions on sharing files, resources and directories.

Trusted network

In this case we are generally talking about office or home networks. Your computer will be perfectly visible to the other computers on the network. There are no limitations on sharing files, resources or directories.

SYN

Flag in the TOS field of TCP packets that identifies them as the start of the connection.

TCP (Transmission Control Protocol)

The main transport-layer Internet protocol aimed at connections for exchanging IP packets.

UDP (User Datagram Protocol)

A transport-layer protocol which is not trustworthy and not aimed at connections for exchanging IP packets.

Environment variable

This is a string of environment information such as a drive, path or file name that 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.

Window of opportunity

Time it takes between the first computer (in the world) being infected with new malware and its analysis and inclusion by antivirus companies in signature files to protect computers from infection. This is the period when malware can infect computers without the antivirus being aware of its existence.

Virus

Viruses are 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.