



Endpoint Protection



Endpoint Protection Plus

Guide for Network Administrators

Table of contents

1. PREFACE	10
1.1. INTRODUCTION	11
1.2. WHO IS THIS GUIDE AIMED AT?	11
1.3. ENDPOINT PROTECTION / ENDPOINT PROTECTION PLUS	11
1.4. ICONS	11
2. INTRODUCTION	13
2.1. INTRODUCTION	14
2.2. MAIN BENEFITS OF ENDPOINT PROTECTION / PLUS ON AETHER.	14
2.3. MAIN BENEFITS OF ENDPOINT PROTECTION PLUS ON AETHER.	15
2.4. AETHER PLATFORM: KEY FEATURES	16
2.4.1 KEY BENEFITS OF AETHER	16
2.4.2 AETHER ARCHITECTURE	18
2.4.3 AETHER ON USERS' COMPUTERS	18
2.5. ENDPOINT PROTECTION / PLUS ARCHITECTURE: KEY COMPONENTS	20
2.5.1 COLLECTIVE INTELLIGENCE SERVERS	21
2.5.2 MANAGEMENT CONSOLE WEB SERVER.....	21
2.5.3 COMPUTERS PROTECTED WITH ENDPOINT PROTECTION / PLUS	22
2.6. ENDPOINT PROTECTION / PLUS ON AETHER: USER PROFILE	22
2.7. ENDPOINT PROTECTION / PLUS ON AETHER: SUPPORTED DEVICES AND LANGUAGES.....	22
2.8. AVAILABLE RESOURCES AND DOCUMENTATION.....	23
3. ENDPOINT PROTECTION / PLUS TECHNOLOGIES	25
3.1. INTRODUCTION	26
3.2. TECHNICAL RESOURCES IMPLEMENTED IN ENDPOINT PROTECTION / PLUS.....	26
3.2.1 ANTI-EXPLOIT PROTECTION	27
3.2.2 PERMANENT ANTIVIRUS PROTECTION AND COLLECTIVE INTELLIGENCE	27
3.2.3 PROTECTION AGAINST ADVANCED STEALTH TECHNIQUES AND MACRO VIRUSES.....	28
3.2.4 EMAIL AND WEB PROTECTION.....	28
3.2.5 FIREWALL AND INTRUSION DETECTION SYSTEMS (IDS)	28
3.2.6 DEVICE CONTROL	29
3.2.7 SPAM, VIRUS AND CONTENT FILTERING FOR EXCHANGE SERVERS	29
3.2.8 WEB ACCESS CONTROL	30
3.2.9 NETWORK STATUS VISIBILITY.....	30
3.2.10 DISINFECTION TECHNIQUES.....	30
3.3. ADAPTATION PHASE	31
4. THE MANAGEMENT CONSOLE.....	33
4.1. INTRODUCTION	34
4.1.1 WEB CONSOLE REQUIREMENTS.....	34
4.1.2 IDP FEDERATION	35
4.2. GENERAL CHARACTERISTICS OF THE CONSOLE.....	35

4.3. GENERAL STRUCTURE OF THE WEB MANAGEMENT CONSOLE	35
4.3.1 TOP MENU (1)	36
4.3.2 SIDE MENU (2).....	38
4.3.3 WIDGETS (3)	38
4.3.4 TAB MENU	39
4.3.5 FILTERING AND SEARCH TOOLS	39
4.3.6 BACK BUTTON	40
4.3.7 SETTINGS ELEMENTS (8).....	40
4.3.8 CONTEXT MENUS	40
4.3.9 LISTS	41
 5. <u>LICENSES</u>.....	43
 5.1. INTRODUCTION	44
5.2. DEFINITIONS AND KEY CONCEPTS FOR MANAGING LICENSES	44
5.2.1 LICENSE CONTRACTS	44
5.2.2 COMPUTER STATUS	44
5.2.3 LICENSE STATUS AND GROUPS	45
5.2.4 TYPES OF LICENSES.....	45
5.2.5 LICENSE MANAGEMENT	45
5.2.6 LICENSE RELEASE	46
5.2.7 PROCESSES FOR ASSIGNING AND RELEASING LICENSES.....	47
5.3. CONTRACTED LICENSES.....	47
5.3.1 WIDGET	48
5.3.2 LICENSE LIST	49
5.4. EXPIRED LICENSES.....	52
5.4.1 EXPIRY NOTIFICATIONS	52
5.4.2 WITHDRAWAL OF EXPIRED LICENSES	52
5.5. ADDING TRIAL LICENSES TO COMMERCIAL LICENSES	53
5.6. SEARCHING FOR COMPUTERS BASED ON THE STATUS OF THEIR LICENSES	53
 6. <u>INSTALLING THE ENDPOINT PROTECTION / PLUS SOFTWARE</u>	55
 6.1. INTRODUCTION	56
6.2. PROTECTION DEPLOYMENT OVERVIEW	56
6.3. INSTALLATION REQUIREMENTS	59
6.3.1 REQUIREMENTS FOR EACH SUPPORTED PLATFORM.....	59
6.3.2 NETWORK REQUIREMENTS.....	60
6.4. MANUALLY DOWNLOADING AND INSTALLING THE ENDPOINT PROTECTION / PLUS SOFTWARE	60
6.4.1 DOWNLOADING THE INSTALLATION PACKAGE FROM THE WEB CONSOLE	60
6.4.2 GENERATING A DOWNLOAD URL	61
6.4.3 MANUALLY INSTALLING THE ENDPOINT PROTECTION / PLUS SOFTWARE	62
6.5. AUTOMATIC COMPUTER DISCOVERY AND REMOTE INSTALLATION.....	63
6.5.1 REQUIREMENTS FOR INSTALLING ENDPOINT PROTECTION / PLUS	64
6.5.2 COMPUTER DISCOVERY.....	64
6.5.3 DISCOVERY SCOPE.....	65
6.5.4 SCHEDULING COMPUTER DISCOVERY TASKS.....	65
6.5.5 LIST OF DISCOVERED COMPUTERS.....	66
6.5.6 DETAILS OF A DISCOVERED COMPUTER	70

6.5.7	INSTALLING THE PROTECTION ON COMPUTERS.....	72
6.6.	INSTALLATION WITH CENTRALIZED TOOLS	73
6.7.	INSTALLATION USING IMAGE GENERATION	76
6.8.	UNINSTALLING THE SOFTWARE	77
7.	<u>MANAGING COMPUTERS AND DEVICES</u>	<u>79</u>
7.1.	INTRODUCTION	80
7.1.1	REQUIREMENTS FOR MANAGING COMPUTERS FROM THE MANAGEMENT CONSOLE	80
7.2.	THE COMPUTERS AREA	80
7.2.1	THE COMPUTERS TREE PANEL	81
7.2.2	THE COMPUTERS LIST PANEL	83
7.2.3	COMPUTERS LIST	84
7.3.	FILTERS TREE.....	86
7.3.1	WHAT IS A FILTER?	86
7.3.2	GROUPS OF FILTERS	87
7.3.3	PREDEFINED FILTERS.....	87
7.3.4	CREATING AND ORGANIZING FILTERS	88
7.3.5	FILTER SETTINGS.....	90
7.3.6	FILTER RULES	90
7.3.7	LOGICAL OPERATORS	91
7.3.8	GROUPS OF FILTER RULES	91
7.4.	GROUPS TREE	92
7.4.1	WHAT IS A GROUP?	92
7.4.2	GROUP TYPES	93
7.4.3	GROUPS STRUCTURE.....	93
7.4.4	ACTIVE DIRECTORY GROUPS	93
7.4.5	CREATING AND ORGANIZING GROUPS	94
7.4.6	MOVING COMPUTERS FROM ONE GROUP TO ANOTHER	95
7.5.	COMPUTER DETAILS	96
7.5.1	GENERAL SECTION (1)	97
7.5.2	COMPUTER NOTIFICATIONS SECTION (2)	97
7.5.3	DETAILS SECTION (3)	98
7.5.4	HARDWARE SECTION (4)	99
7.5.5	SOFTWARE SECTION (5)	99
7.5.6	SETTINGS SECTION (6).....	100
7.5.7	FORCE SYNCHRONIZATION (7).....	100
7.5.8	CONTEXT MENU	100
8.	<u>MANAGING SETTINGS.....</u>	<u>101</u>
8.1.	INTRODUCTION	102
8.2.	WHAT ARE SETTINGS?	102
8.3.	OVERVIEW OF ASSIGNING SETTINGS TO COMPUTERS	102
8.3.1	IMMEDIATE DEPLOYMENT OF SETTINGS.....	103
8.3.2	MULTI-LEVEL TREES.....	103
8.3.3	INHERITANCE.....	103
8.3.4	MANUAL SETTINGS	103
8.3.5	DEFAULT SETTINGS	103
8.4.	MODULAR VS MONOLITHIC SETTINGS PROFILES.....	104

8.5. OVERVIEW OF THE FOUR TYPES OF SETTINGS.....	106
8.6. CREATING AND MANAGING SETTINGS.....	107
8.7. MANUAL AND AUTOMATIC ASSIGNING OF SETTINGS TO GROUPS OF COMPUTERS	108
8.7.1 ASSIGNING SETTINGS DIRECTLY/MANUALLY	108
8.7.2 INDIRECT ASSIGNING OF SETTINGS: THE TWO RULES OF INHERITANCE.....	110
8.7.3 INHERITANCE LIMITS.....	111
8.7.4 OVERWRITING SETTINGS	112
8.7.5 DELETING MANUALLY ASSIGNED SETTINGS AND RESTORING INHERITANCE	116
8.7.6 MOVING GROUPS AND COMPUTERS.....	117
8.8. VIEWING THE ASSIGNED SETTINGS	117
 9. AGENT AND LOCAL PROTECTION SETTINGS.....	 120
 9.1. INTRODUCTION	 121
9.2. CONFIGURING THE PANDA AGENT ROLE.....	121
9.2.1 PROXY ROLE	121
9.2.2 CACHE/REPOSITORY ROLE	122
9.2.3 DISCOVERY COMPUTER ROLE	123
9.3. CONFIGURING INTERNET ACCESS VIA A PROXY SERVER.....	123
9.4. CONFIGURING REAL-TIME COMMUNICATION	125
9.5. CONFIGURING THE AGENT LANGUAGE	125
9.6. CONFIGURING THE ANTI-TAMPER PROTECTION AND PASSWORD	126
9.6.1 ANTI-TAMPER PROTECTION.....	126
9.6.2 PASSWORD-PROTECTION OF THE AGENT.....	126
 10. SECURITY SETTINGS FOR WORKSTATIONS AND SERVERS	 128
 10.1. INTRODUCTION.....	 129
10.2. INTRODUCTION TO THE SECURITY SETTINGS FOR WORKSTATIONS AND SERVERS	129
10.3. GENERAL SETTINGS	130
10.3.1 UPDATES.....	130
10.3.2 UNINSTALL OTHER SECURITY PRODUCTS	130
10.3.3 EXCLUSIONS	130
10.4. ANTIVIRUS	131
10.4.1 THREATS TO DETECT	131
10.4.2 FILE TYPES.....	131
10.5. FIREWALL (WINDOWS DEVICES)	131
10.5.1 OPERATIONAL MODE	132
10.5.2 NETWORK TYPE	132
10.5.3 PROGRAM RULES	132
10.5.4 CONNECTION RULES	134
10.5.5 BLOCK INTRUSIONS.....	136
10.6. DEVICE CONTROL (WINDOWS DEVICES).....	137
10.6.1 ALLOWED DEVICES	137
10.6.2 EXPORTING/IMPORTING A LIST OF ALLOWED DEVICES	138
10.6.3 OBTAINING A DEVICE'S UNIQUE ID.....	138
10.7. WEB ACCESS CONTROL	139
10.7.1 CONFIGURING TIME PERIODS FOR THE WEB ACCESS CONTROL FEATURE	139
10.7.2 DENYING ACCESS TO SPECIFIC WEB PAGES	140
10.7.3 LIST OF ALLOWED/DENIED ADDRESSES AND DOMAINS.....	140

10.7.4 DATABASE OF ALL URLS ACCESSED FROM COMPUTERS	140
10.8. ANTIVIRUS FOR EXCHANGE SERVERS	141
10.9. ANTI-SPAM FOR EXCHANGE SERVERS	142
10.9.1 ACTIONS TO PERFORM ON SPAM MESSAGES	142
10.9.2 ALLOWED ADDRESSES AND DOMAINS	143
10.9.3 SPAM ADDRESSES AND DOMAINS	143
10.10. CONTENT FILTERING FOR EXCHANGE SERVERS	143
<u>11. ANDROID SECURITY SETTINGS</u>	<u>145</u>
11.1. INTRODUCTION.....	146
11.2. INTRODUCTION TO THE SECURITY SETTINGS FOR ANDROID DEVICES	146
11.3. UPDATES.....	146
11.4. ANTIVIRUS	146
<u>12. SOFTWARE UPDATES</u>	<u>147</u>
12.1. INTRODUCTION.....	148
12.2. CONFIGURING PROTECTION ENGINE UPDATES	148
12.2.1 UPDATES.....	149
12.3. CONFIGURING COMMUNICATIONS AGENT UPDATES	150
12.4. CONFIGURING KNOWLEDGE UPDATES.....	150
12.4.1 WINDOWS, LINUX AND MAC DEVICES	150
12.4.2 ANDROID DEVICES.....	150
12.5. UPDATE CACHE/REPOSITORY.....	150
12.5.1 CONFIGURING A COMPUTER AS A REPOSITORY	151
12.5.2 REQUIREMENTS AND LIMITATIONS OF COMPUTERS WITH THE CACHE ROLE.....	151
12.5.3 DISCOVERY OF CACHE NODES.....	151
<u>13. TASKS</u>	<u>152</u>
13.1. INTRODUCTION.....	153
13.2. TASK CREATION	153
13.2.1 TASK RECIPIENTS	153
13.2.2 TASK SCHEDULE AND FREQUENCY.....	153
13.3. TASK PUBLICATION	155
13.4. TASK MANAGEMENT	155
<u>14. MALWARE AND NETWORK VISIBILITY</u>	<u>158</u>
14.1. INTRODUCTION.....	159
14.2. OVERVIEW OF THE STATUS MENU	159
14.3. AVAILABLE PANELS/WIDGETS.....	161
14.3.1 PROTECTION STATUS	161
14.3.2 OFFLINE COMPUTERS.....	163
14.3.3 OUTDATED PROTECTION	164
14.3.4 THREATS ALLOWED BY THE ADMINISTRATOR	165
14.3.5 THREATS DETECTED BY THE ANTIVIRUS.....	166
14.3.6 CONTENT FILTERING FOR EXCHANGE SERVERS.....	168

14.3.7 WEB ACCESS.....	169
14.3.8 TOP 10 MOST ACCESSED CATEGORIES.....	170
14.3.9 TOP 10 MOST ACCESSED CATEGORIES BY COMPUTER.....	172
14.3.10 TOP 10 MOST BLOCKED CATEGORIES	173
14.3.11 TOP TEN MOST BLOCKED CATEGORIES BY COMPUTER	174
14.4. INTRODUCTION TO THE LISTS	175
14.4.1 TEMPLATES, SETTINGS AND VIEWS	175
14.4.2 MY LISTS PANEL.....	177
14.4.3 CREATING CUSTOM LISTS	177
14.4.4 DELETING A LIST	179
14.4.5 CONFIGURING A CUSTOM LIST	179
14.5. AVAILABLE LISTS	180
14.5.1 COMPUTER PROTECTION STATUS LIST	180
14.5.2 LIST OF THREATS ALLOWED BY THE ADMINISTRATOR	183
14.5.3 HISTORY OF THREATS ALLOWED BY THE ADMINISTRATOR LIST	185
14.5.4 LIST OF THREATS DETECTED BY THE ANTIVIRUS.....	187
14.5.5 WEB ACCESS BY CATEGORY LIST	189
14.5.6 WEB ACCESS BY COMPUTER LIST	191
14.5.7 'BLOCKED DEVICES' LIST	192
14.5.8 LICENSES LIST	194
14.5.9 'UNMANAGED COMPUTERS DISCOVERED' LIST	194
14.6. DEFAULT LISTS	195
 <u>15. MANAGING QUARANTINED AND EXCLUDED ITEMS</u>	 <u>196</u>
 15.1. INTRODUCTION.....	 197
15.2. TOOLS FOR MANAGING EXCLUSIONS.....	197
15.3. EXCLUDING ITEMS	198
15.3.1 EXCLUDING ITEMS CLASSIFIED AS A THREAT	198
15.4. MANAGING EXCLUDED ITEMS.....	199
15.5. MANAGING THE BACKUP/QUARANTINE AREA	199
15.5.1 VIEWING QUARANTINED ITEMS	200
15.5.2 RESTORING QUARANTINED ITEMS	200
 <u>16. REMEDIATION TOOLS</u>	 <u>201</u>
 16.1. INTRODUCTION.....	 202
16.2. AUTOMATIC COMPUTER DISINFECTION.....	202
16.3. ON-DEMAND COMPUTER SCANNING AND DISINFECTION.....	203
16.3.1 SCHEDULED SCAN TASKS.....	203
16.3.2 IMMEDIATE SCANS.....	204
16.4. COMPUTER RESTART	204
16.5. REPORTING A PROBLEM	205
16.6. ALLOWING EXTERNAL ACCESS TO THE WEB CONSOLE	205
 <u>17. ALERTS.....</u>	 <u>206</u>
 17.1. INTRODUCTION.....	 207
17.2. EMAIL ALERTS	207
17.2.1 CONFIGURING EMAIL ALERTS	207

17.2.2 ACCESS PERMISSIONS AND ALERTS	207
17.2.3 ALERT TYPES	207
18. REPORTS.....	210
18.1. INTRODUCTION.....	211
18.2. ON-DEMAND GENERATION OF EXECUTIVE REPORTS	211
18.2.1 INFORMATION REQUIRED TO GENERATE AN ON-DEMAND REPORT	211
18.3. SCHEDULED SENDING OF EXECUTIVE REPORTS	212
18.3.1 INFORMATION REQUIRED TO GENERATE A SCHEDULED REPORT.....	212
19. CONTROLLING AND MONITORING THE MANAGEMENT CONSOLE	214
19.1. INTRODUCTION.....	215
19.2. WHAT IS A USER ACCOUNT?	215
19.2.1 USER ACCOUNT STRUCTURE	215
19.2.2 WHAT IS THE MAIN USER?	215
19.3. WHAT IS A ROLE?	216
19.3.1 ROLE STRUCTURE	216
19.3.2 WHY ARE ROLES NECESSARY?	216
19.3.3 FULL CONTROL ROLE	217
19.3.4 MONITORING ROLE	217
19.4. WHAT IS A PERMISSION?	217
19.4.1 UNDERSTANDING PERMISSIONS.....	218
19.5. ACCESSING THE USER ACCOUNT AND ROLE SETTINGS	221
19.6. CREATING AND CONFIGURING USER ACCOUNTS	222
19.7. CREATING AND CONFIGURING ROLES	222
19.8. USER ACCOUNT ACTIVITY LOG	223
19.8.1 ACTION LOG	223
19.8.2 SESSION LOG	226
20. APPENDIX 1: ENDPOINT PROTECTION / PLUS REQUIREMENTS	228
20.1. REQUIREMENTS FOR WINDOWS PLATFORMS.....	229
20.1.1 SUPPORTED OPERATING SYSTEMS	229
20.1.2 HARDWARE REQUIREMENTS	229
20.2. REQUIREMENTS FOR WINDOWS EXCHANGE PLATFORMS	229
20.2.1 SUPPORTED OPERATING SYSTEMS	229
20.2.2 SOFTWARE AND HARDWARE REQUIREMENTS	229
20.2.3 SUPPORTED EXCHANGE VERSIONS	230
20.3. REQUIREMENTS FOR MACOS PLATFORMS	230
20.3.1 SUPPORTED OPERATING SYSTEMS	230
20.3.2 HARDWARE REQUIREMENTS	230
20.4. REQUIREMENTS FOR LINUX PLATFORMS	231
20.4.1 SUPPORTED 64-BIT DISTRIBUTIONS.....	231
20.4.2 SUPPORTED KERNEL VERSION	231
20.4.3 SUPPORTED FILE MANAGERS.....	231
20.4.4 HARDWARE REQUIREMENTS	231
20.4.5 INSTALLATION PACKAGE DEPENDENCIES	231
20.5. ANDROID PLATFORM REQUIREMENTS.....	231

20.5.1	SUPPORTED OPERATING SYSTEMS	231
20.5.2	HARDWARE REQUIREMENTS	232
20.5.3	NETWORK REQUIREMENTS.....	232
20.6.	WEB CONSOLE ACCESS.....	232
20.7.	ACCESS TO SERVICE URLS.....	232
21.	<u>APPENDIX 2: CREATING AND MANAGING A PANDA ACCOUNT.....</u>	<u>234</u>
21.1.	INTRODUCTION.....	235
21.2.	CREATING A PANDA ACCOUNT	235
21.3.	ACTIVATING YOUR PANDA ACCOUNT	235
22.	<u>APPENDIX 3: LIST OF UNINSTALLERS</u>	<u>237</u>
23.	<u>APPENDIX 4: KEY CONCEPTS</u>	<u>244</u>

1. Preface

Who is this guide aimed at?

Icons

1.1. Introduction

This guide contains basic information and procedures for making the most out of **Endpoint Protection** / **Endpoint Protection Plus on Aether**.


1.2. Who is this guide aimed at?

This guide is aimed at network administrators who need to manage the security of their organization's computers, find out the extent of the security problems detected, and define cyber-attack response and prevention plans.

Endpoint Protection / Plus is a managed service that delivers security without requiring active, constant intervention from the network administrator. It offers highly detailed information about the security status of the IT network thanks to the new **Aether** platform developed by Panda Security. **Aether** is a scalable and efficient platform for the centralized management of Panda Security solutions, addressing the needs of key accounts and MSPs. **Aether** facilitates the real-time presentation of information generated by **Endpoint Protection / Plus** about processes, the programs run by users and the devices installed, in a coordinated and highly detailed manner.

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

1.3. Endpoint Protection / Endpoint Protection Plus

This guide covers the products **Endpoint Protection** and **Endpoint Protection Plus**. Since both products share multiple features and work on the new **Aether** platform, this guide refers to both solutions with the names **Endpoint Protection / Plus** and **Endpoint Protection / Plus on Aether**. Those features that are only available in **Endpoint Protection Plus** are indicated with the icon .

1.4. Icons

The following icons are used in this guide:



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



Suggestions and recommendations



Important advice regarding the use of features in **Endpoint Protection / Plus**



Additional information available in other chapters or sections of the guide



Feature only available in **Endpoint Protection Plus**

2. Introduction

Key product features
Key platform features
Key components of the platform architecture
Services
Product user profile
Supported devices and languages
Resources and documentation

2.1. Introduction

Endpoint Protection and **Endpoint Protection Plus** are two security solutions that leverage multiple protection technologies, allowing organizations to replace the *on-premises* or *standalone* antivirus solution installed on their network with a complete, cloud-based managed security service.

Both products combine an extremely lightweight security software installed on network computers with a single Web management console accessible at anytime, anywhere and from any device.

Additionally, **Endpoint Protection Plus** allows organizations to monitor and control user productivity, preventing access to Web resources not linked to the company's activity and filtering corporate mail to eliminate spam-related performance problems.

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

Finally, both are cloud-based cross-platform products compatible with Windows, Mac OS X, Linux and Android devices. With **Endpoint Protection** and **Endpoint Protection Plus**, you'll only need one tool to ensure the security of all devices in your organization.

2.2. Main benefits of Endpoint Protection / Plus on Aether.

Endpoint Protection is a product that allows organizations to manage the security of all computers across the network, without negatively impacting device performance and at the lowest possible cost of ownership. It provides the following key benefits:

- **Lightweight product**

All operations are performed in the cloud, with almost no impact on computer performance.

- **Low memory usage:** the size of the locally stored signature files has been reduced thanks to Panda Security's use of real-time queries to collective intelligence. This has allowed us to move the malware database from the user's computer to the cloud.
- **Low network usage:** the number of required downloads has been reduced to the minimum.
- **Ability to share signature files among endpoints:** signature files are downloaded once and shared across the network.
- **Low processor usage:** the detection intelligence has been moved to the cloud, thereby requiring fewer processor resources on users' computers.

- **Cross-platform security**

Covers all infection vectors on Windows, Linux, Mac OS X and Android devices.

- **Security for all infection vectors:** web browsing, email, file system and all external devices connected to the PC.
- **Security against unknown threats:** anti-exploit technology to prevent malware from leveraging unknown security flaws in software in order to infect computers.
- **Behavior-based protection:** to detect unknown malware.
- **Cross-platform security:** windows, Linux, Mac OS X, Android and virtual engines (VMware, Virtual PC, MS Hyper-V, Citrix).

- **Easy to manage**

Easy-to-manage solution which doesn't require maintenance or additional infrastructure on the customer's network.

- **Easy to maintain:** no specific infrastructure is required to host the solution, allowing the IT team to spend their time on more productive tasks.
- **Easy protection for remote users:** each computer with **Endpoint Protection / Plus** installed communicates directly with the cloud; roaming users and remote offices are protected quickly and easily without specific installations or VPN configurations.
- **Easy to deploy:** provides multiple deployment methods and automatic uninstallers to remove competitor products and migrate easily from a third-party solution.
- **Soft learning curve:** simple and intuitive Web-based interface. Often-used options are one click away.

2.3. Main benefits of Endpoint Protection Plus on Aether.

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

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

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

Endpoint Protection Plus allows organizations to easily manage the security of every computer on the corporate network, without negatively impacting device performance and with low total cost of ownership. **Endpoint Protection Plus** adds the following benefits to those already provided by **Endpoint Protection**:

- **Maximum productivity**

Monitors and filters Web traffic and spam so that companies can focus on their core business and forget about employees' unproductive behavior.

- **Web monitoring and filtering:** increases corporate productivity by tracking users' Internet activities and preventing access to dangerous or unproductive websites during working hours. Supports any Web browser.
- **No more flooded mailboxes:** reduce the risk of attacks on your Exchange servers with the content filter feature. Improve end-user productivity and protection by filtering unwanted and malicious messages with the anti-malware and anti-spam engines.

2.4. Aether Platform: key features

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

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

Endpoint Protection / Plus operates completely transparently on **Aether** for administrators and users alike, as it has been designed from the bottom up.

This design means that it is not necessary to install new agents or products on customers' endpoints. This way, all Panda Security products that run on **Aether** share the same agent on customers' endpoints as well as the same Web management console, facilitating product management and minimizing resource consumption.

2.4.1 Key benefits of Aether

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

- **Cloud management platform**

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

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

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

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

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

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

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

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

- **Flexible and granular settings**

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

- **Complete and customized information**

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

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

2.4.2 Aether architecture

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

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

Figure 1 shows a high-level diagram of **Aether Platform**.

2.4.3 Aether on users' computers

Network computers protected by **Endpoint Protection / Plus on Aether** have a software program installed, made up of two independent yet related modules, which provide all the protection and management functionality:

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

- **Panda real-time communications agent**

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

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

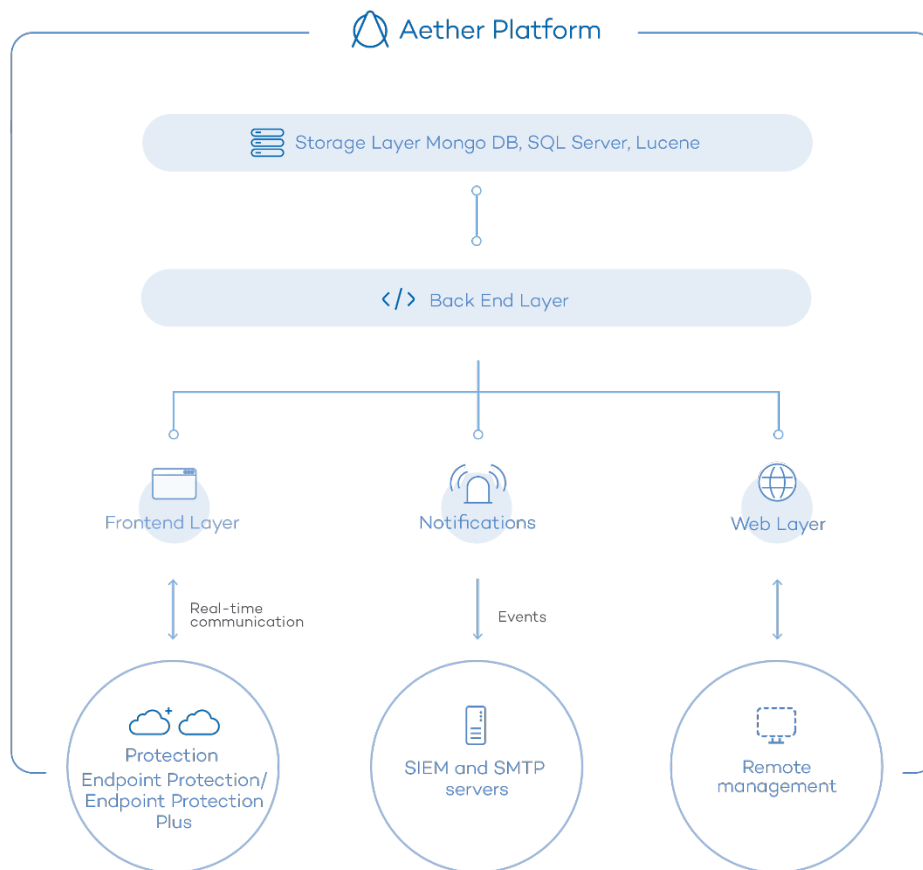


Figure 1: logical structure of **Aether Platform**

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

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

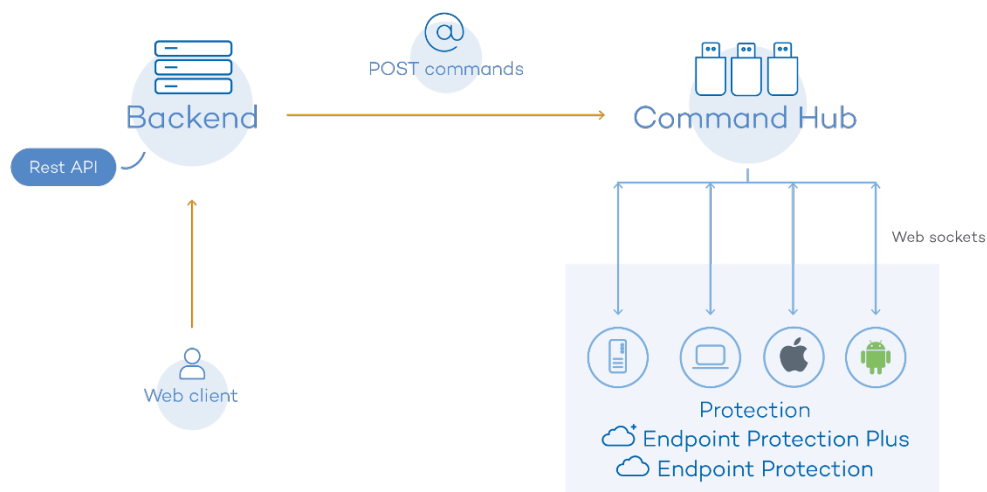


Figure 2: flowchart of the commands entered via the management console

2.5. Endpoint Protection / Plus architecture: key components

Endpoint Protection / Plus is a cloud security service that moves security intelligence and most scanning tasks to the IT infrastructure deployed in Panda Security's Data Processing Centers. This results in an extremely lightweight security software with low resource usage and low requirements to run in organizations.

Figure 3 shows the general structure of **Endpoint Protection / Plus** and its components:

Endpoint Protection / Plus is made up of the following components:

- Collective Intelligence servers
- **Endpoint Protection / Plus** agent installed on the device to protect
- **Endpoint Protection / Plus** protection installed on the device to protect
- Signature file
- Administrator console

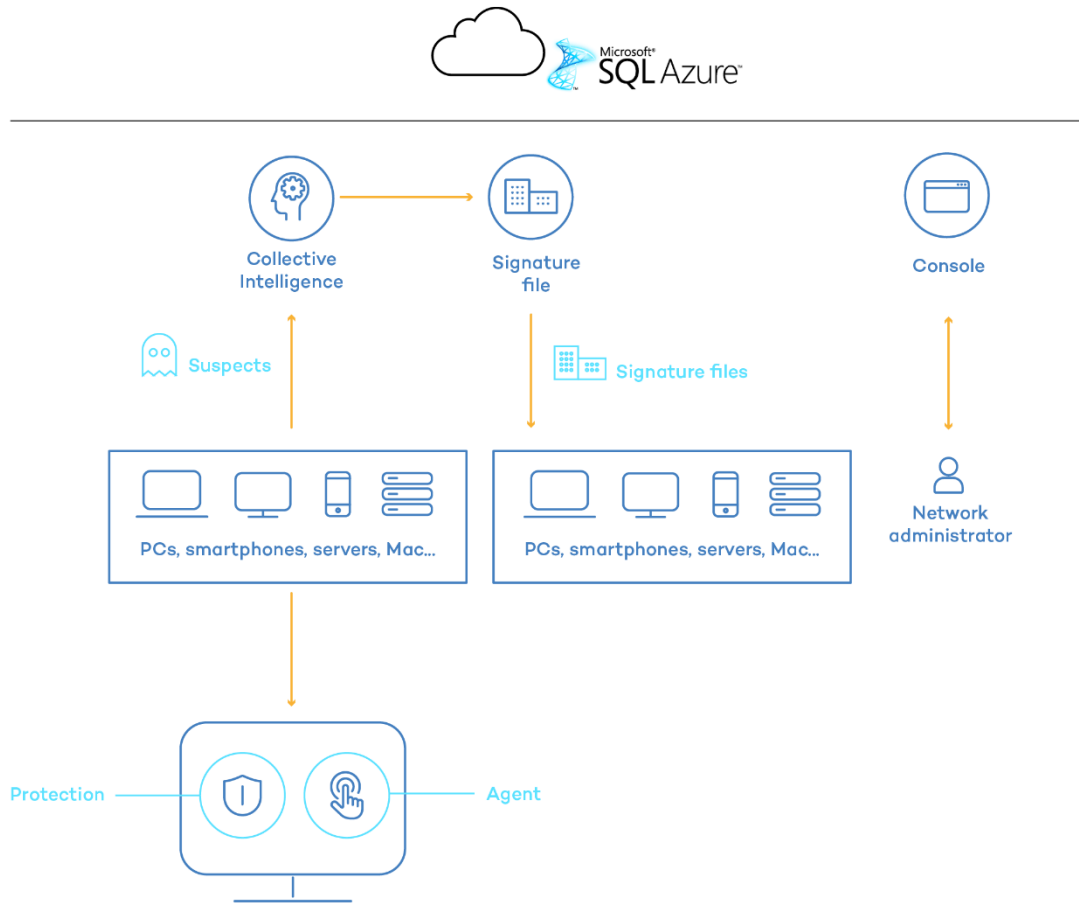


Figure 3: **Endpoint Protection / Plus** general structure

Below we describe the roles of each of these components.

2.5.1 Collective Intelligence servers

Collective Intelligence has servers that automatically classify and process all the data provided by the user community about the detections made on customers' systems. These servers belong to Panda Security's cloud-based infrastructure. Apart from this, the **Endpoint Protection / Plus** protection installed on computers queries Collective Intelligence only when required, ensuring maximum detection power without negatively affecting resource consumption.

2.5.2 Management console Web server

Endpoint Protection / Plus is managed entirely through the Web console accessible to administrators from <https://www.pandacloudsecurity.com/PandaLogin/>

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



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

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

2.5.3 Computers protected with Endpoint Protection / Plus

Endpoint Protection / Plus requires the installation of a small software component called **agent** on all computers on the network susceptible of having security problems.

This component is made up of two modules: the **Panda** communications agent and the **Endpoint Protection / Plus** protection module.

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



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

2.6. Endpoint Protection / Plus on Aether: user profile

Even though **Endpoint Protection / Plus** is a managed service that offers security without intervention from the network administrator, it also provides clear and detailed information about the malware activity detected across the entire corporate network. This data can be used by administrators to clearly assess the impact of security problems, and adapt the company's protocols to prevent similar situations in the future.

2.7. Endpoint Protection / Plus on Aether: supported devices and languages



Refer to Appendix 1: endpoint Protection / Plus requirements, for a full description of the platforms supported by Endpoint Protection / Plus on Aether and its requirements.

Endpoint Protection / Plus supports the following operating systems:

- Windows Workstation

- Windows Server
- Linux
- Mac OS X
- Android smartphones and tablets

Additionally, the management console supports the following Web browsers:

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

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

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

2.8. Available resources and documentation

Below is a list of the available resources for **Endpoint Protection / Plus on Aether**.

Guide for Network Administrators

<http://resources.pandasecurity.com/enterprise/solutions/endpointprotection/ENDPOINTPROTECTIONNoAP-guide-3.20.0-EN.pdf>

Product Page

<http://www.pandasecurity.com/uk/enterprise/solutions/cloud-office-protection/>

Product Support Page

<http://www.pandasecurity.com/uk/support/cloud-office-protection.htm>

3. Endpoint Protection / Plus technologies

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

3.1. Introduction

In recent years, the use of the Internet and all types of mobile devices has become universal in all fields. Laptops, servers, smartphones, tablets, removable storage drives and numerous other devices are now widely used in corporate environments. The business world has benefited enormously from these changes, increasing productivity and efficiency, and also improving internal and external communication.

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

In this scenario, the cloud has become an element of paramount importance: the high number of discovered threats would require enormous resources on the computers to protect, with a huge impact on device performance.

That's why Panda Security has launched **Endpoint Protection / Plus**, a security product for users' computers based on Collective Intelligence: an automatic system for detecting and disinfecting malware which is fed with the shared knowledge from millions of users. Thanks to Collective Intelligence, the computers that make up the Panda community instantly share and benefit from all the malware information which is stored and continuously updated in the cloud.

Panda Security was the first company with the infrastructure, the technology, the knowledge and the experience to apply the Collective Intelligence model to its products on the market. This way, Panda Security gives customers maximum protection with minimal impact on endpoints.

This chapter provides an overview of the technologies implemented in **Endpoint Protection / Plus** to manage the security of a company's network in the aforementioned malware scenario.

3.2. Technical resources implemented in Endpoint Protection / Plus

The aim of **Endpoint Protection / Plus** is to enable the IT Department to create a space where they can define and establish corporate security policies that respond rapidly and adequately to the new types of threats that are continuously emerging. This space is partly the product of the removal of responsibilities from the company's technical team of deciding which files are safe and which are dangerous, and for what reason. **Endpoint Protection / Plus** detects all kinds of threats automatically, without requiring active intervention from the network administrator or continuous monitoring of the security status of the network, saving time and resources.

On the other hand, the IT Department will also receive a set of tools for viewing the security status of the network and resolving malware-related problems.

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

3.2.1 Anti-exploit protection

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

Our anti-exploit technology detects and neutralizes malware such as Blackhole or Redkit that exploits zero-day vulnerabilities (in Java, Adobe, MS Office, etc.), before it infects the computer. The key is to use heuristic technologies with powerful detection capabilities. In particular, the new anti-exploit protection provided by **Endpoint Protection / Plus** analyzes how exploits behave instead of their morphology.

Endpoint Protection / Plus uses multiple sensors to send Collective Intelligence information about the behavior of those suspicious files that try to exploit 0-day vulnerabilities in order to infect PCs. This information allows Panda Security to keep the proactive technologies included in its products constantly up-to-date (via on-the-fly updates from the cloud).

In short, **Endpoint Protection / Plus** is designed to detect and neutralize this type of malware before it has been identified (and even created), protecting users against new malware variants.

3.2.2 Permanent antivirus protection and Collective Intelligence

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

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

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

Whenever a new malware specimen is detected on a computer in the user community, **Endpoint Protection / Plus** sends the relevant information to our **Collective Intelligence** servers in the cloud,

automatically and anonymously. This information is processed by our servers, delivering the solution to all users in the community in real time.

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



Refer to chapters 10 and 11 (Security settings for workstations and servers, and Android security settings) for more information about Endpoint Protection / Plus's antivirus service for the different supported platforms

3.2.3 Protection against advanced stealth techniques and macro viruses

In addition to the traditional detection strategy based on comparing the payload of scanned files to its signature files, **Endpoint Protection / Plus** uses several detection engines that scan the behavior of processes locally.

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

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

3.2.4 Email and Web protection

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

3.2.5 Firewall and intrusion detection systems (IDS)

Endpoint Protection / Plus provides three basic tools to filter the network traffic that protected computers send and receive:

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

3.2.6 Device Control

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

Endpoint Protection / Plus allows administrators to restrict the use of those devices on protected computers, blocking access to them or allowing complete or partial use only (read-only access).

3.2.7 Spam, virus and content filtering for Exchange servers



Feature only available in Endpoint Protection Plus.

Endpoint Protection / Plus scans Exchange servers for viruses, hacking tools and suspicious/potentially unwanted programs directed to users' mailboxes.

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

Endpoint Protection / Plus protects Exchange email servers by using two different technologies:

- **Mailbox protection**

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

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

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

- **Transport protection**

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

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

3.2.8 Web access control



Feature only available in Endpoint Protection Plus.

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.

Web pages are divided into 64 categories. Select the URL categories that you want to deny access to. You can modify them at any time.

Additionally, **Endpoint Protection / Plus** allows administrators to set time restrictions to limit access to certain Web page categories and blacklisted sites during working hours, or authorize it during non-business hours or weekends.

3.2.9 Network status visibility

Endpoint Protection / Plus provides a number of resources that allow administrators to assess the security status of their corporate network at a glance, using the activity panels displayed in the solution's dashboard.

The **Endpoint Protection / Plus** dashboard provides key information about the detections made in the different infection vectors used by malware.



Refer to chapter 14 Malware and network visibility for more information about how to view and monitor computers and processes.

3.2.10 Disinfection techniques

In the event of a security breach, the administrator must be able to quickly restore the affected computers to their original state.

To make that possible, **Endpoint Protection / Plus** provides advanced disinfection tools along with a quarantine to store suspicious and deleted items.



Refer to chapter 16 Remediation tools for more information.

3.3. Adaptation phase

After resolving a security incident with the Remediation tools, the administrator will have to adjust the company's security policies to prevent any such situation from occurring again.

Endpoint Protection / Plus can be used to strengthen endpoint security in a number of ways:

- **Changing the antivirus protection settings**

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

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



Feature only available in Endpoint Protection Plus.

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**



Feature only available in Endpoint Protection Plus.

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

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

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

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

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

The firewall and the IDS can also be used to prevent malware from propagating once the first computer has been infected.

4. The management console

General characteristics of the console
General structure of the Web management
console

4.1. Introduction

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

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

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

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

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

- **Service management from anywhere at anytime**

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

4.1.1 Web console requirements

The Web console can be accessed from the following link:

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

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

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



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

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

4.1.2 IDP federation

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

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

4.2. General characteristics of the console

Endpoint Protection / Plus's management console allows administrators to interact with the service, and provides the following benefits:

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

4.3. General structure of the Web management console

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

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

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

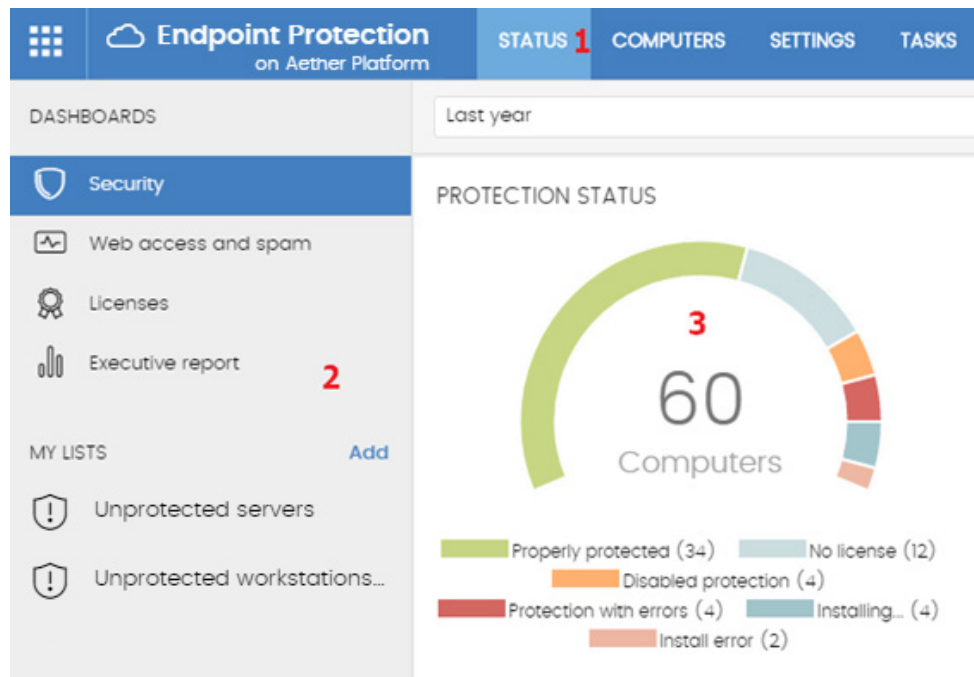



Figure 4: overview of the *Endpoint Protection / Plus* management console

4.3.1 Top menu (1)

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

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

Panda Cloud button

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

Status menu

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



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

Computers menu

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

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



Refer to chapter 8 Managing settings for more information.

Settings menu

Lets you define different types of settings:

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



Refer to chapter 19 Controlling and monitoring the management console for more information.

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



Refer to chapter 10 Security settings for workstations and servers for more information.

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



Refer to chapter 11 Android security settings for more information.

Tasks menu

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



Refer to chapter 13 Tasks for more information.

General Settings menu

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

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

User Account menu

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

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

4.3.2 Side menu (2)

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

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

4.3.3 Widgets (3)

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



Refer to chapter 14 Malware and network visibility for more information.

4.3.4 Tab menu

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

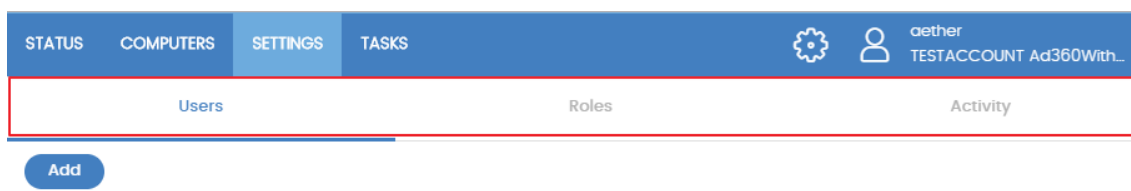


Figure 5: tab menu

4.3.5 Filtering and search tools

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

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

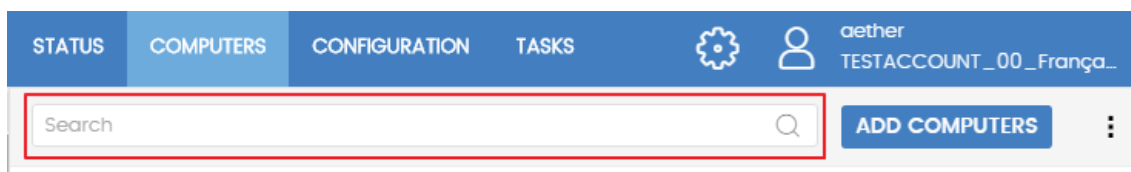


Figure 6: search tool

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

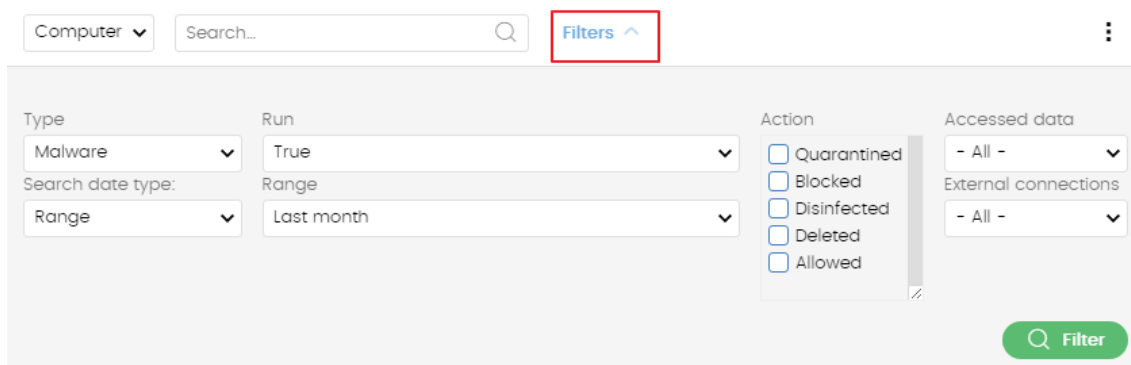


Figure 7: filtering tool for data lists

4.3.6 Back button

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

4.3.7 Settings elements (8)

The **Endpoint Protection / Plus** Web console uses standard settings elements, such as:

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

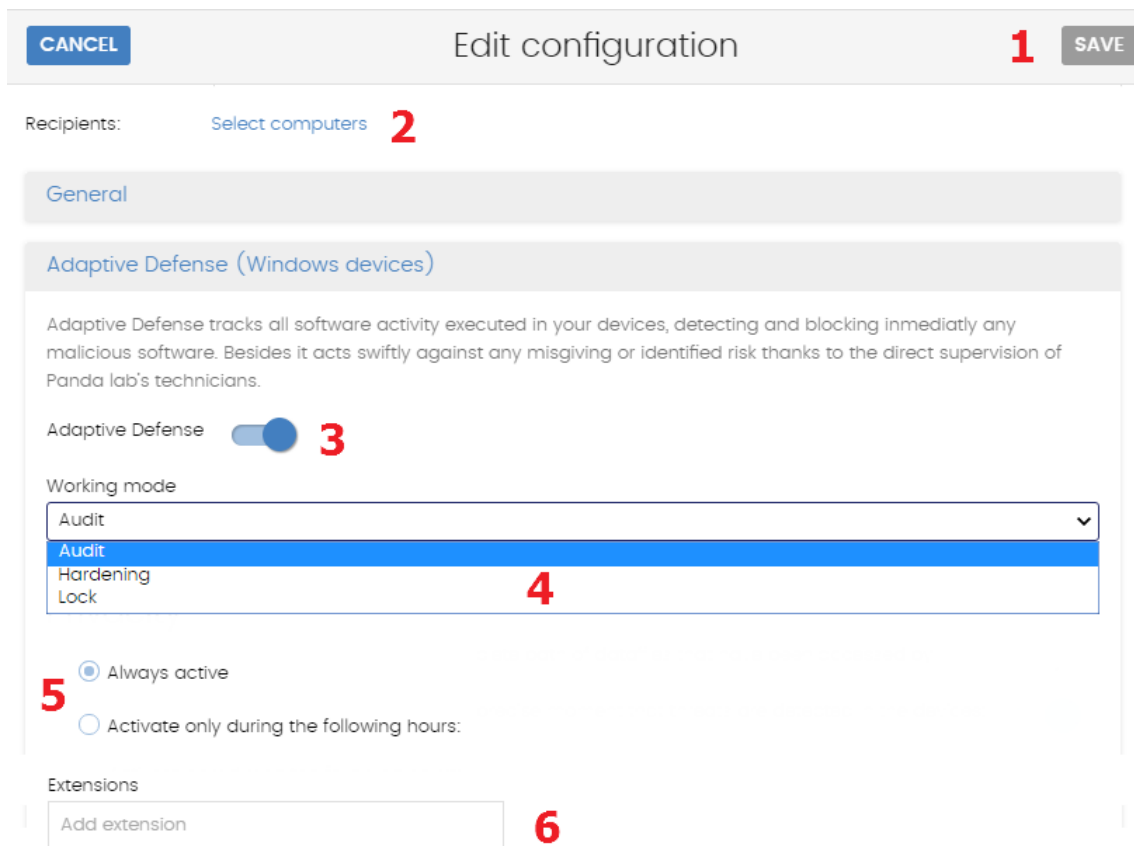



Figure 8: controls for using the management console

4.3.8 Context menus

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

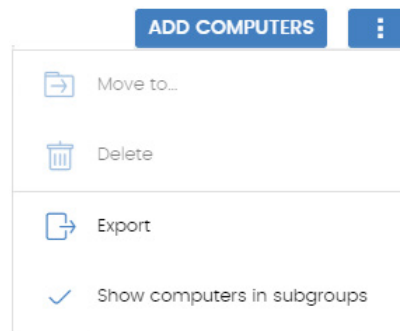


Figure 9: context menu

4.3.9 Lists

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

Executed malware **1**

2 Filters ^

3

4

Type: Malware

Date search type: Range

Range: Last month

Search: Host Name

Run: True

Action:

- ☐ Moved quarantine
- ☐ Blocked
- ☐ Cleaned
- ☐ Deleted
- ☐ Allowed

Accessed data: - All -

External connections: - All -

5 FILTER

Host Name	Threat	File path				Action	Date
Machine_Cus tomer_1_Id38	Malware Nam e 2	Malware Path Sample 2	●	●	○	Deleted	3/10/2017 1:00: 00 AM
Machine_Cus tomer_1_Id38	Malware Nam e 14	Malware Path Sample 14	●	●	○	Allowed	3/15/2017 12:1 8:00 AM
Machine_Cus tomer_1_Id38	Malware Nam e 8	Malware Path Sample 8	●	●	○	Cleaned	3/14/2017 9:2 4:00 PM
Machine_Cus tomer_1_Id38	Malware Nam e 10	Malware Path Sample 10	●	●	○	Blocked	3/14/2017 10:2 2:00 PM
Machine_Cus tomer_1_Id38	Malware Nam e 4	Malware Path Sample 4	●	●	○	Blocked	3/14/2017 7:28: 00 PM

6

7 10 entries

8 1 to 10 of 2140

9 <<

10 <

11 1

12 2

13 3

14 4



15 5

16 >

17 >>

Figure 10: items in lists

- **List name (1):** lets you identify the information on the list.
- **Filtering and search tool link (2):** click it to display a panel with search and filtering controls.
- **Context menu (3):** displays a drop-down menu with export options.
- **Filtering and search parameters (4):** let you refine the data displayed on the list.

- **Sort order (5):** you can change the sort order of the list by clicking the column headers at the top of the list view. Click the same header a second time to switch between ascending and descending order. This is indicated with arrows ( for ascending and  for descending).
- **Pagination (6):** at the bottom of the table there are pagination tools to help you navigate easier and faster.
 - Rows per page selector **(7)**
 - Number of pages/rows displayed out of the total number of pages/rows **(8)**
 - First page link **(9)**
 - Previous page link **(10)**
 - Links to the next 5 pages **(11)**
 - Next page link **(12)**
 - Last page link **(13)**

5. Licenses

- License management
- Definitions and key concepts
- License status summary
 - Contracted licenses
 - Expired licenses
 - Trial licenses
- Computer search based on license status

5.1. Introduction

To benefit from **Endpoint Protection / Plus**'s advanced security services you need to purchase licenses of the product and assign them to the computers to protect, according to your organization's security needs.

This chapter explains how to manage your **Endpoint Protection / Plus** licenses, as well as how to assign them to your computers, release them and check their status.

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



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

5.2. Definitions and key concepts for managing licenses

The following is a description of terms required to understand the graphs and data provided by **Endpoint Protection / Plus** to show the status of computer licenses.

5.2.1 License contracts

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

- **Product type**: Endpoint Protection / Plus, Endpoint Protection / Plus with Advanced Reporting Tool.
- **Contracted licenses**: number of licenses contracted in the license contract.
- **License type**: nFR, Trial, Commercial, Subscription.
- **Expiry**: license expiry date and the computers that will cease to be protected.

5.2.2 Computer status

Endpoint Protection / Plus makes a distinction between three different license statuses on network computers:

- **Computers with a license**: the computer has a valid license in use.
- **Computers without a license**: the computer doesn't have a valid license in use, but is eligible to have one.
- **Excluded**: computers for which it has been decided not to assign a license. These computers won't be protected by **Endpoint Protection / Plus**, although they will be displayed in the console and some management features will be valid for them. To exclude a computer, you have to release the license manually.



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

5.2.3 License status and groups

There are two possible status types for contracted licenses:

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

Licenses are separated into two groups according to their status:

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

5.2.4 Types of licenses

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

5.2.5 License management

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

Automatic assignment of licenses

Once you install **Endpoint Protection / Plus** on a computer on the network, and provided there are unused **Endpoint Protection / Plus** licenses, the system will assign a free license to the computer automatically.

Manual assignment of licenses

Follow the steps below to manually assign an **Endpoint Protection / Plus** license to a network computer.

- Go to the **Computers** menu at the top of the console. Find the device to assign the license to. You can use the folder tree, the filter tree or the search tool.
- Click the computer to access its details screen.

- Go to the **Details** tab. The **Licenses** section will display the status '**No licenses**'. Click the



icon to assign a free license to the computer automatically.

5.2.6 License release

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

Automatic release

When the **Endpoint Protection / Plus** software is uninstalled from a network computer, the system automatically recovers a license and returns it to the group of licenses available for use.

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

Manual release

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

Follow the steps below to manually release an **Endpoint Protection / Plus** license:

- Go to the **Computers** menu at the top of the console. Find the device whose license you want to release. You can use the folder tree, the filter tree or the search tool.
- Click the computer to access its details screen.
- Go to the **Details** tab. The **Licenses** section will display the status '**Endpoint Protection / Plus**'.



Click the icon to release the license and send it back to your group of unused licenses.

5.2.7 Processes for assigning and releasing licenses

Case 1: excluded computers and those with assigned licenses

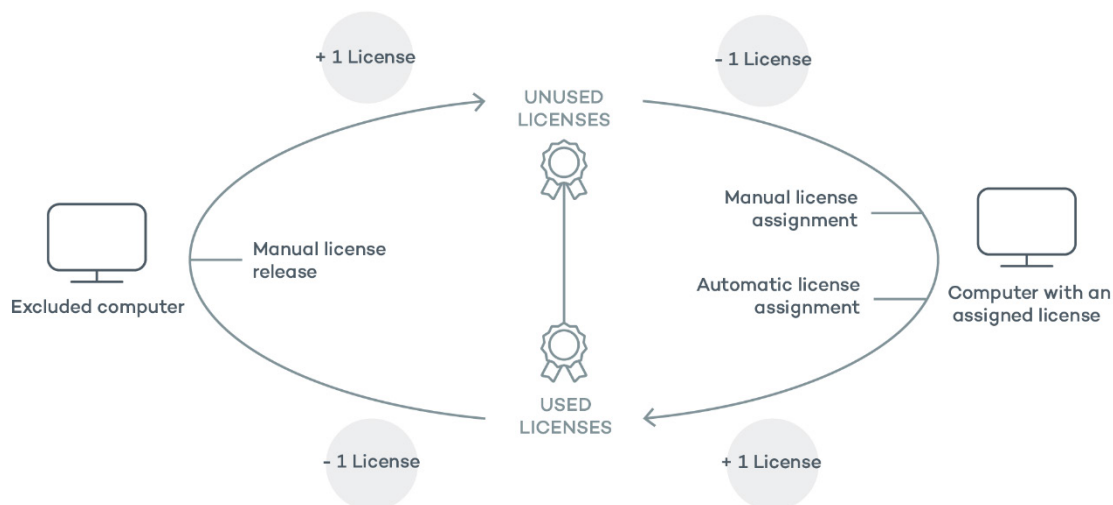


Figure 11: modification of license groups with excluded computers and those with licenses assigned

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

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

Case 2: computers without an assigned license

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

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

5.3. Contracted licenses

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

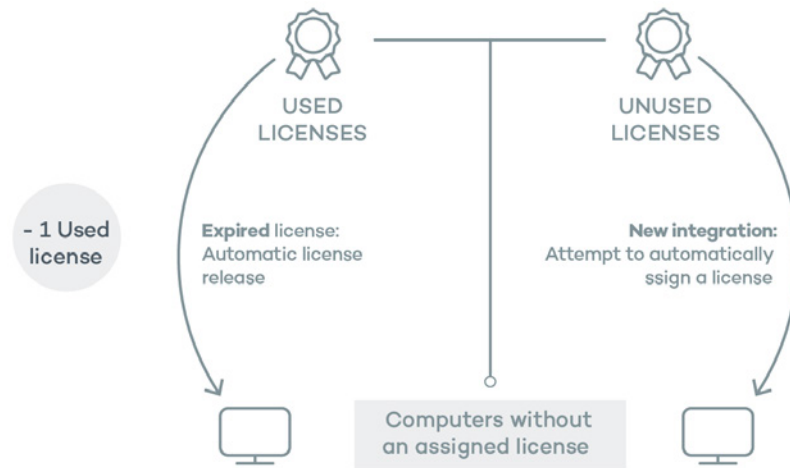


Figure 12: computers without an assigned license due to expiry of the license contract and because the group of unused licenses is empty.

5.3.1 Widget

The panel shows how the contracted product licenses are distributed.

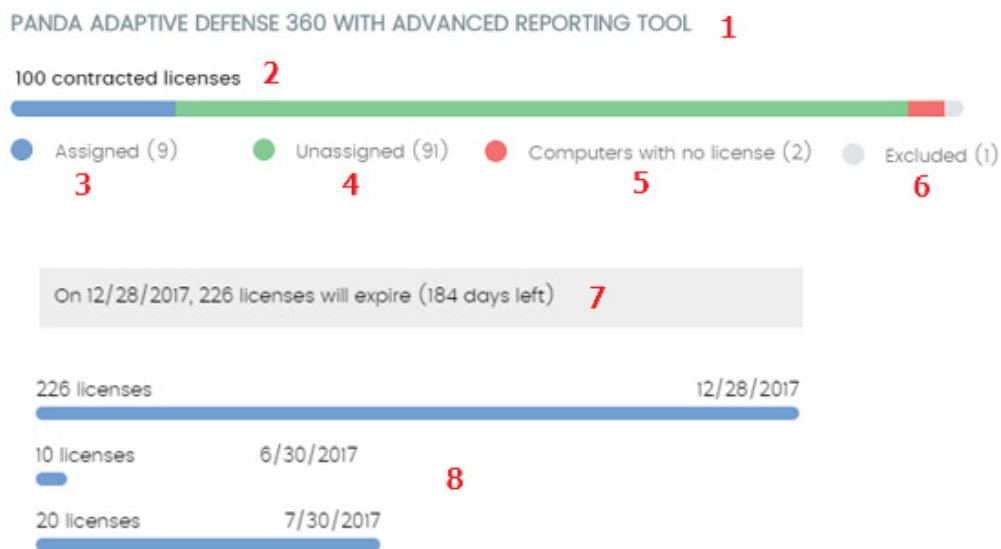


Figure 13: license panel with three license contracts

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

- License contract expiry (8)

Name of the contracted product (1)

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

Total number of contracted licenses (2)

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

Assigned (3)

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

Unassigned (4)

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

Computers without a license (5)

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

Excluded computers (6)

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

License expiry (7)

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

License contract expiry (8)

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

5.3.2 License list

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

Filed	Comment	values
Computer	Computer name	Character string




Filed	Comment	values
Group	Folder within the Endpoint Protection / Plus group tree to which the computer belongs	Character string
License status		 Assigned  Computers with no license  Excluded computers
Last connection	Date that the computer status was last sent to the Panda Security cloud	Date

Table 1: protected computer list fields

Fields displayed in the exported file

Campo	Comentario	Valores
Customer	Customer account that the product belongs to.	Character string
Computer type		Workstation Laptop Mobile device Server
Computer	Computer name	Character string
Operating system	Operating system installed, internal version and patch status.	Character string
Platform	Operating system installed on the computer.	Windows Linux MacOS Android
Active Directory	Path in the company's Active Directory tree where the computer is found	Character string
Exchange server	Version of the mail sever installed.	Character string
Virtual machine	Indicates whether the computer is physical or virtual	Boolean
Agent version		Character string

Campo	Comentario	Valores
Protection version		Character string
System boot date		Date
Installation date	Date that the Endpoint Protection / Plus software was successfully installed.	Date
Last connection date	Date that the computer status was last sent to the Panda Security cloud	Date
License status		Assigned Unassigned Excluded
Group	Folder within the Endpoint Protection / Plus group tree to which the computer belongs	Character string
IP address	Primary IP address of the computer.	Character string
Domain	Windows domain that the computer belongs to	Character string
Description		Character string

Table 2: fields in the Licenses exported file

Filter tool

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

Table 3: filter fields for the Licenses list

Lists accessible from the panel



Figure 14: hotspots in the Contracted licenses panel

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

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

5.4. Expired licenses

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

5.4.1 Expiry notifications

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

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



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

5.4.2 Withdrawal of expired licenses

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

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

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



This logic for withdrawing expired licenses affects all compatible devices with Endpoint Protection / Plus and with licenses assigned

5.5. Adding Trial licenses to Commercial licenses

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

- A new trial license contract is created for the trial period and with the same amount of licenses as previously available and the licenses contracted for the trial.
- Commercial license contracts appear temporarily disabled during the trial period, though the expiry and renewal cycle is unaffected.
- The corresponding product functionality is enabled for the trial with no need to update the computers.
- **Endpoint Protection / Plus** will, by default, be enabled in Audit mode. If you do not want to enable **Endpoint Protection / Plus** on all computers or you want to set a different protection mode, this can be configured accordingly.

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

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

Endpoint Protection / Plus's filter tree lets you search for computers based on the status of their licenses.



Refer to chapter 7 Managing computers and devices for more information about how to create an Endpoint Protection / Plus filter

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

- **Property – License status:** you can create filters based on the following license status:
 - **Assigned:** lists those computers with an **Endpoint Protection / Plus** license assigned.

- **Not assigned:** lists those computers that don't have an **Endpoint Protection / Plus** license assigned.
- **Unassigned manually:** lists those computers whose **Endpoint Protection / Plus** license was released by the network administrator.
- **Unassigned automatically:** lists those computers whose **Endpoint Protection / Plus** license was automatically released by the system.
- **Property - License name:** finds every computer with an **Endpoint Protection / Plus** license assigned.
- **Property – Type:** lists those computers with a specific type of **Endpoint Protection / Plus** license.
 - **Release:** lists computers with commercial licenses of Endpoint Protection / Plus.
 - **Trial:** lists computers with trial licenses of Endpoint Protection / Plus.

6. Installing the Endpoint Protection / Plus software

- Protection deployment overview
 - Installation requirements
 - Manual installation
 - Discovery and remote installation
 - Installation with centralized tools
 - Installation using image generation
 - Software uninstall

6.1. Introduction

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

It is important to install the **Endpoint Protection / Plus** software on every computer on the network to prevent security breaches that may be later exploited by attackers through malware designed to attack vulnerable systems.

Endpoint Protection / Plus provides several tools to help administrators install the protection. These tools are discussed later in this chapter.

6.2. Protection deployment overview

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

Identify the unprotected devices on the network

The administrator must find those computers on the network without protection installed or with a third-party security product that needs replacing or complementing with **Endpoint Protection / Plus**.

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



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

Check if the minimum requirements for the target platform are met

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

Select the installation procedure

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

- Centralized distribution tool
- Manual installation using the **Send URL by email** option

- Placing an installer in a shared folder accessible to all users on the network
- Remote installation from the management console

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

Computers with no protection installed won't need to be rebooted to install the protection services provided by **Endpoint Protection / Plus**.



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

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



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

The default behavior will vary depending on the **Endpoint Protection / Plus** version to install.

- **Trial versions**

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

- **Commercial versions**

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



Refer to Appendix 3: list of uninstallers for a list of the antivirus solutions that Endpoint Protection / Plus uninstalls automatically. If the solution that needs to be removed is not on the list, it will have to be removed manually.

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



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

- **Panda Security antivirus products**

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

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

Table 4 summarizes the necessary conditions for a computer restart.

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

Table 4: probability of a restart when installing Endpoint Protection / Plus on Aether

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

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

Determine the computers' default settings

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

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

6.3. Installation requirements



For a full description of the necessary requirements for each platform, refer to [Appendix 1: endpoint Protection / Plus requirements](#).

6.3.1 Requirements for each supported platform

Windows platforms

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

MacOS platforms

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

Linux platforms

- **64-bit operating systems:** Ubuntu 14.04 LTS and later, Fedora 23 and later.
- **Supported kernel:** up to version 4.10 (64-bit).
- **Free space for installation:** 100 MB.
- **Ports** 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware and URL filtering to work.

Android platforms

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



Refer to our support website for more information about the last Linux kernel version supported by Endpoint Protection / Plus. Any later version won't be supported.

6.3.2 Network requirements

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

6.4. Manually downloading and installing the Endpoint Protection / Plus software

6.4.1 Downloading the installation package from the Web console



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

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

- Go to the **Computers** menu, click **Add computers**, and select the platform to protect: windows, Linux, Android or MacOS (Figure 15).
- Select the group that the computer will integrate into (Figure 16):
 - To integrate the computer into a native group, click **Add computers to this group (1)** and select a destination in the folder tree displayed.
 - To integrate the computer into an Active Directory group, click **Add computers to their Active Directory path (2)**.

- Next, you must select the proxy and language settings **(3)** to apply to the computer. If the computer is to be integrated into a native group, it will automatically inherit the settings of the folder where it will reside. However, if you choose to integrate it into an Active Directory group, you'll have to manually select the proxy and language settings from those displayed in the drop-down menu. If the automatic selection does not meet your needs, click the drop-down menu and select one of the available options.

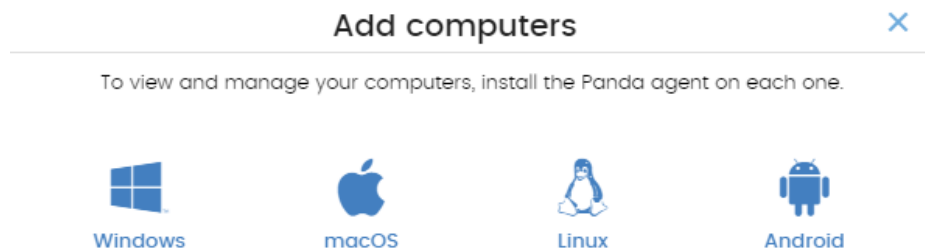


Figure 15: platform selection window

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

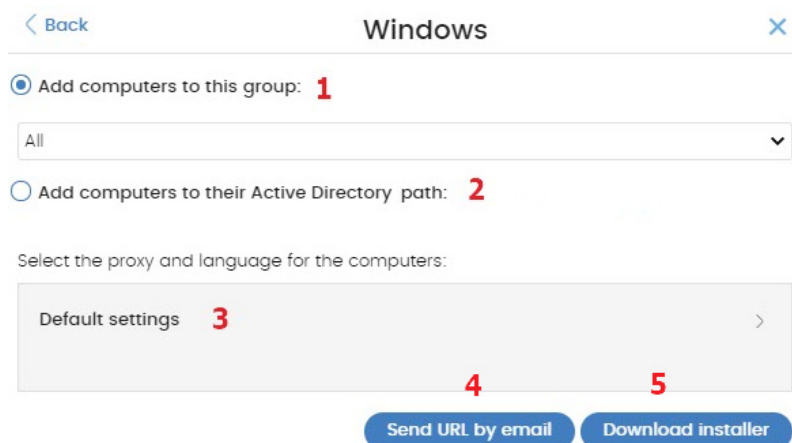


Figura 16: configuring the download package

6.4.2 Generating a download URL

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

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

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

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

6.4.3 Manually installing the Endpoint Protection / Plus software



Administrator permission is required to install the Endpoint Protection / Plus software on users' computers.

Installing Endpoint Protection / Plus on Windows platforms

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

Installing Endpoint Protection / Plus on Linux platforms

Open a terminal in the folder with the downloaded package and run the following command:

```
sudo sh "package name"
```

Installing Endpoint Protection / Plus on MacOS platforms

Open a terminal in the folder with the downloaded package and run the following command:

```
sudo sh "package name"
```

Installing Endpoint Protection / Plus on Android platforms



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

< Back
Android
×

Add computers to this group:

All

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

QR code

Go to Google Play

Send URL by email

Figure 17: platform selection screen

- **Add computers to this group (1):** this lets you specify the group within the folder tree to which the device will be added once the **Endpoint Protection / Plus** software is installed.
- **QR code (2):** the QR code that contains the link to download the software from Google Play.
- **Go to Google Play (3):** a direct link to download the **Endpoint Protection / Plus** software from Google Play.
- **Send URL by email (4):** the email message with the link ready to send to the user of the devices that will be protected by **Endpoint Protection / Plus**.

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

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



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

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

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

6.5. Automatic computer discovery and remote installation

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



Remote installation is only compatible with Windows platforms.

6.5.1 Requirements for installing Endpoint Protection / Plus

For you to be able to install **Endpoint Protection / Plus** remotely, the following requirements must be met:

- **To discover an unmanaged computer:** UDP port 137 must be accessible to the *System* process.
- **To install the protection remotely on the computer:** TCP port 445 must be accessible to the *System* process.



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

6.5.2 Computer discovery

Computers are discovered by means of another computer with the role of '*Discovery computer*'.

Requirements for finding unprotected computers on your network

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

- Reply to pings (echo request, echo reply)
- Return the computer's NetBIOS name (NetBios Name Service running on TCP/UDP port 137)
- Have not been hidden by the administrator
- Are not currently managed by **Panda Endpoint Protection / Plus** on **Aether Platform**



*All computers that meet the aforementioned requirements will appear on the list of discovered computers, regardless of whether their operating system or device type supports the installation of **Panda Endpoint Protection / Plus***

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

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

Characteristics of a discovery computer

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

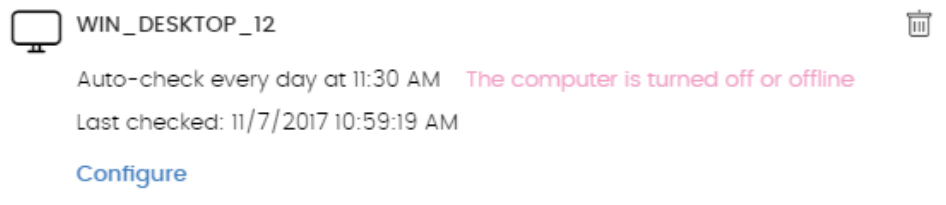


Figure 18: access to the discovery task settings window

Computer name

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

6.5.3 Discovery scope

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

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

6.5.4 Scheduling computer discovery tasks

Scheduling a task

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

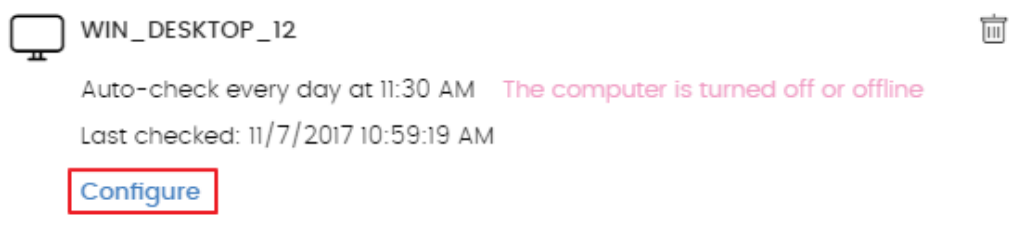


Figure 19: access to the discovery task settings window

- **Automatic execution of discovery tasks**

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

- **Manual execution of discovery tasks**

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

6.5.5 List of discovered computers

Displays the unmanaged devices found by **Panda Endpoint Protection / Plus**.

There are two ways to access this list:

- From the Protection status widget
- From My lists

- **Protection status widget**

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

PROTECTION STATUS



Figure 20: access to the list of discovered computers from the **Protection status** widget

- **My lists**

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

Description of the list of discovered computers

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

Field	Comments	Values
by		
Last seen	Date when the computer was last discovered	Date

Table 5: fields in the list of discovered computers

Next is a description of the possible error messages:

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

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer	Name of the discovered computer	Character string
IP	The computer's primary IP address	Character string

Field	Comments	Values
MAC address	The computer's physical address.	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card	Character string
Domain	Windows domain the computer belongs to	Character string
First seen	Date when the computer was first discovered	Character string
First seen by	Name of the discovery computer that first saw the workstation/server	Character string
Last seen	Date when the computer was last discovered	Date
Last seen by	Name of the discovery computer that last saw the workstation/server	Character string

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

Filter tool

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

Table 7: filters available in the list of discovered computers

Hidden computers

To avoid generating too long lists of discovered computers that may contain computers not eligible for **Endpoint Protection / Plus** installation, it is possible to hide computers selectively by following the steps below:

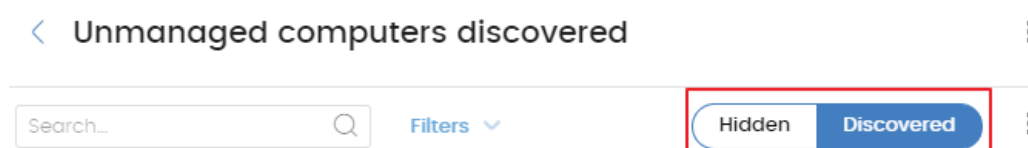


Figura 21: discovered/Hidden computer list selector

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

Deleted computers

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

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

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



A deleted computer that is not physically removed from the network will appear again in the next discovery task. Only delete those computers that will never be accessible again.

6.5.6 Details of a discovered computer

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

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

1

Computer details

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

2

Discovered by

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

3

Figura 22: details of a discovered computer

Computer alerts

- **Error installing the Panda agent:** this message specifies the reason why the agent installation failed.
 - Wrong credentials. Launch the installation again using credentials with sufficient privileges to perform the installation.
 - Discovery computer not available.
 - Unable to connect to the computer. Make sure the computer is turned on and meets the remote installation requirements.
 - Unable to download the agent installer. Make sure the computer is turned on and meets the remote installation requirements.
 - Unable to copy the agent installer. Make sure the computer is turned on and meets the remote installation requirements.
 - Unable to install the agent. Make sure the computer is turned on and meets the remote installation requirements.
 - Unable to register the agent. Make sure the computer is turned on and meets the remote installation requirements.
- **Installing Panda agent:** once the installation process is complete, the computer will no longer appear on the list of discovered computers.
- **Hidden computer.**
- **Unmanaged computer:** the computer doesn't have the Panda agent installed.

Computer details

- **Computer name**

- **Description:** lets you assign a description to the computer, even though it is currently not managed.
- **First seen:** date/time when the computer was first discovered.
- **Last seen:** date/time when the computer was last discovered.
- **IP address**
- **Physical addresses (MAC)**
- **Domain:** windows domain the computer belongs to.
- **NIC manufacturer:** manufacturer of the computer's network interface card.

Last discovery computer

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

6.5.7 Installing the protection on computers

To remotely install the **Endpoint Protection / Plus** software on one or more computers on your network follow the steps below:

From the list of discovered computers

- Go to the list of discovered computers. There are three ways to do this:
 - Go to **My lists** on the left-hand side menu and click the **Add** link. From the drop-down menu, select the **Unmanaged computers discovered** list.
 - Go to the Status menu at the top of the console. In the Protection status widget, click the link **XX computers have been discovered that are not being managed by Panda Endpoint Protection / Plus**.
 - Go to the **Computers** menu at the top of the console. Click **Add computers** and select **Discovery and remote installation**. A wizard will be displayed. Click the link **View unmanaged computers discovered**.
- From the list of discovered computers, select **Discovered** or **Hidden** depending on the status of the relevant computers (1).
- Select the checkboxes that correspond to the computers that you want to install the software on.
- To install it on multiple computers simultaneously, click the general context menu and select **Install Panda agent**.
- To install it on a single computer, click the computer's context menu and then click **Install Panda agent**.
- Configure the installation by following the steps described in section 6.4
- You can enter one or multiple installation credentials. Use the local administrator account of the target computer or the domain that it belongs to in order to install the software successfully.

From the computer details window

Click a discovered computer to display its details window. At the top of the screen you'll see the button **Install Panda agent**. Follow the steps detailed in section 6.4.

6.6. Installation with centralized tools

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

1 Download and share the Endpoint Protection / Plus installer

- Move the **Endpoint Protection / Plus** installer to a shared folder which is accessible to all the computers that are to receive the software.

2 Create a new OU (Organizational Unit) called "Endpoint Protection"

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

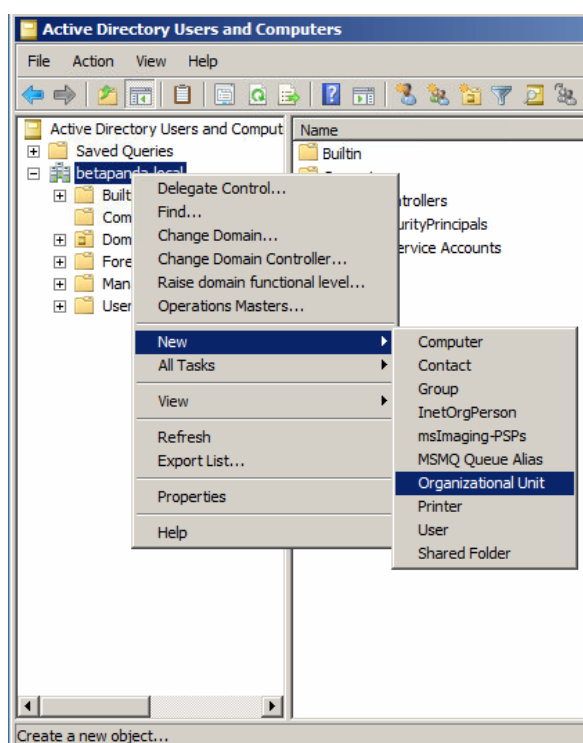


Figure 23: create an Organizational Unit

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

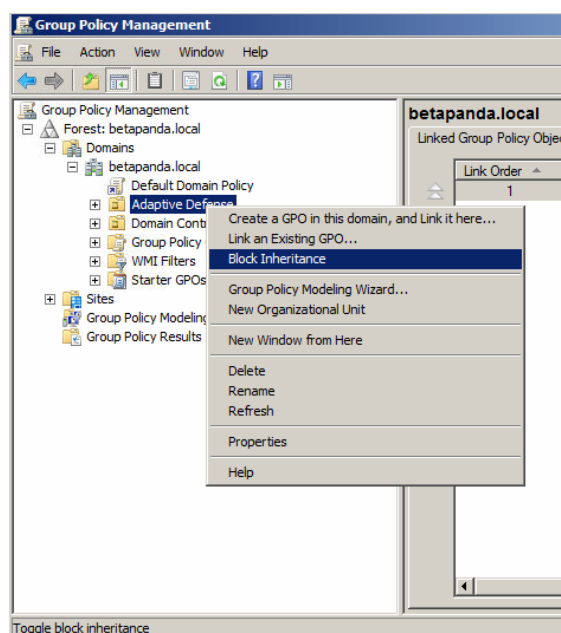


Figure 24: block inheritance

- Create a new GPO in the "Endpoint Protection" OU.

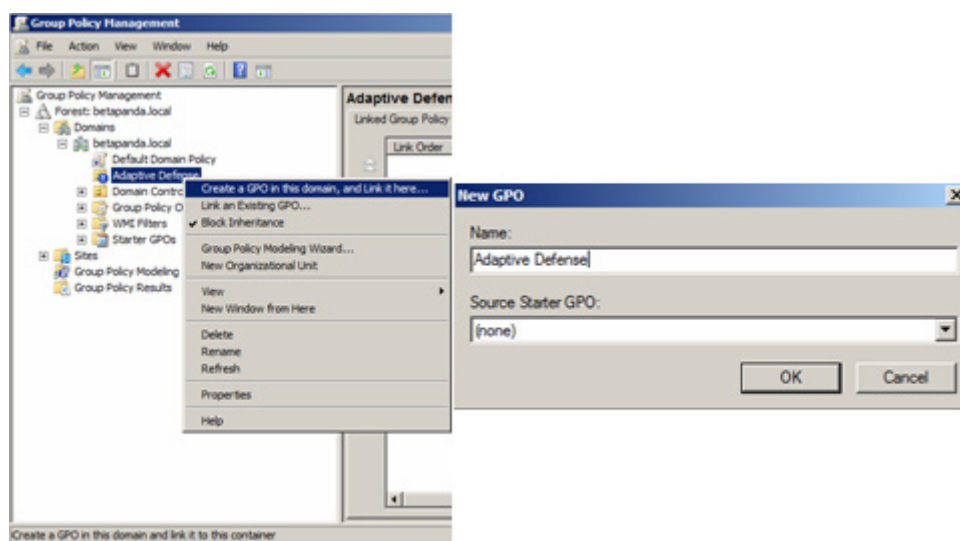


Figure 25: create a GPO

3 Add a new installation package to the newly created GPO

- Edit the GPO.

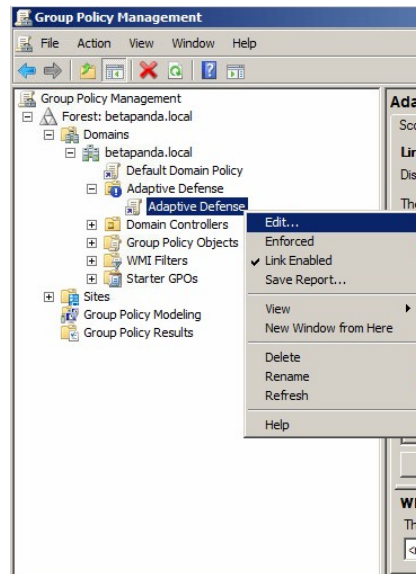


Figure 26: edit the newly created GPO

- Add a new installation package which contains the **Endpoint Protection / Plus** software. To do this, you will be asked to add the installer to the GPO.

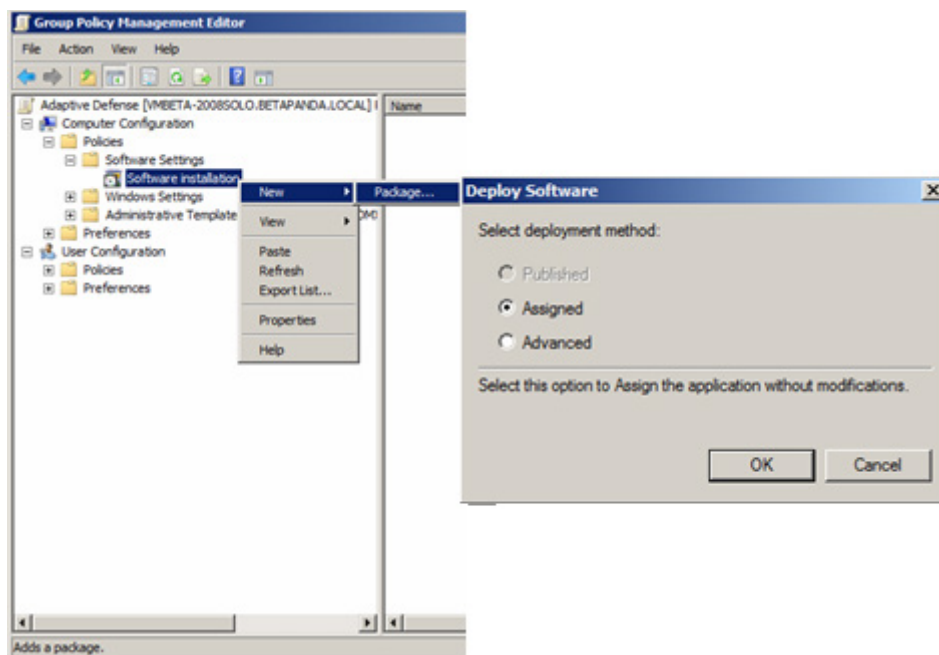


Figure 27: assign a new deployment package

4 Edit the deployment properties

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

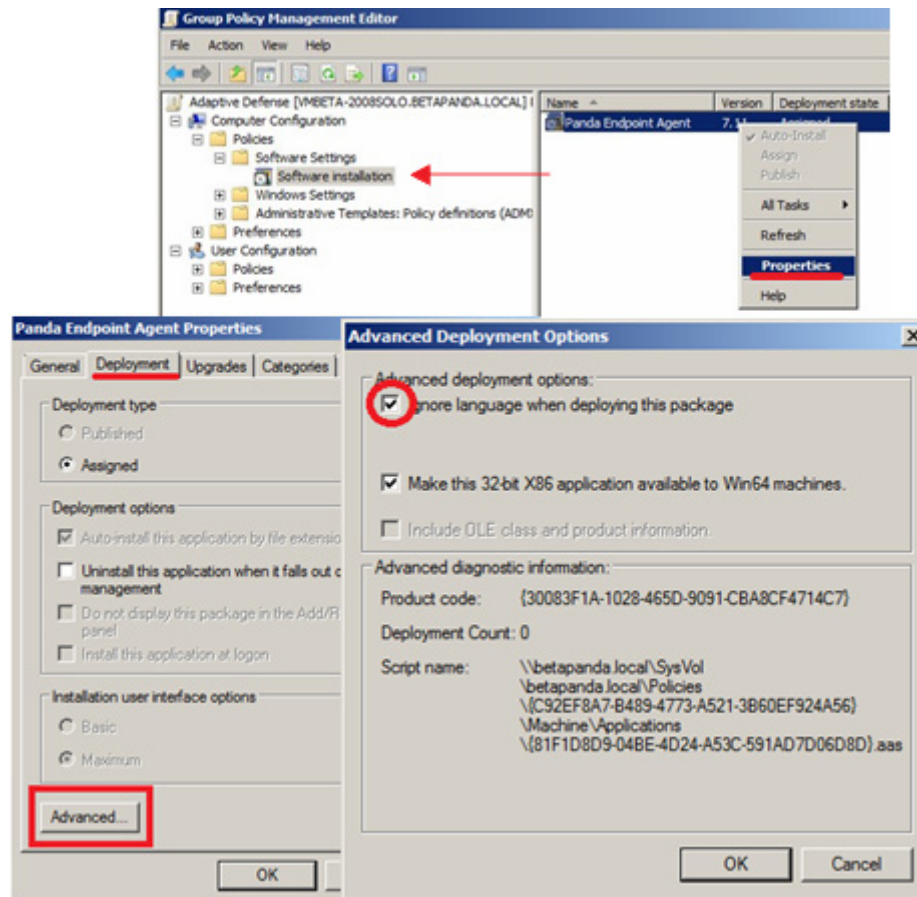


Figure 28: configure the deployment package

- Finally, in the Endpoint Protection OU you created in "Active Directory Users and Computers", add all the network computers to which the software will be sent.

6.7. Installation using image generation

In large networks made up of many homogeneous computers, it is possible to automate the process to install the operation system and the tools that accompany it.

This automation consists of creating a base image (also known as master image, golden image or clone image), by installing on a virtual or physical computer an up-to-date operating system and every software that the users may need, including security tools. Once ready, a copy of the computer's hard disk is extracted which is then copied to the other computers on the network, substantially reducing deployment times.

If the network administrator uses this automated deployment procedure and **Endpoint Protection / Plus** is part of the base image, it will be necessary to take some additional steps for the procedure to be successful.

Installing the **Endpoint Protection / Plus** software on a computer entails automatically assigning a unique ID to it. This ID is used by Panda Security to show and identify the computer in the management console. If, later, a golden image is generated with the **Endpoint Protection / Plus** software installed on it, and the image is then cloned to other computers, every computer that receives the image will inherit the same **Endpoint Protection / Plus** ID and, consequently, the console will only display a computer.

To avoid this, a program is required that deletes the ID generated when installing the software on a computer. This program is called `reintegra.zip` and can be downloaded from Panda Security's support website.

<http://www.pandasecurity.com/uk/support/card?id=500201>

Refer to the website for specific instructions on how to install the **Endpoint Protection / Plus** agent on a golden or master image.

6.8. Uninstalling the software

Endpoint Protection / Plus can be uninstalled manually from the operating system's 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.

On Windows 8 and later:

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

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

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

On Windows XP:

- Control Panel > Add or remove programs.

On macOS:

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

On Android devices:

- Go to Settings. Security > Device administrators.
- Clear the **Endpoint Protection / Plus** checkbox. Then, tap Disable > OK.
- Back in the Settings window, tap Apps. Click **Endpoint Protection / Plus** > Uninstall > OK.

On Linux

- **Fedora:** activities > Software > Installed
- **Ubuntu:** ubuntu software> Installed

7. Managing computers and devices

The Computers area
The Filters tree
The Groups tree
Computer details

7.1. Introduction

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

7.1.1 Requirements for managing computers from the management console

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

As with other Panda Security products based on **Aether**, **Endpoint Protection / Plus** delivers the Panda agent in the installation package for all compatible platforms.

Devices without an **Endpoint Protection / Plus** license but with Panda agent installed will appear in the management console, although the protection will be uninstalled and scan tasks or other **Endpoint Protection / Plus** resources won't be run.



Computers with expired licenses will still be scanned for threats, but the signature file won't be updated. In this condition, Endpoint Protection / Plus won't be an effective solution to combat threats. Panda Security strongly recommends that organizations renew the contracted services in order to keep their network protected.

7.2. The Computers area

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

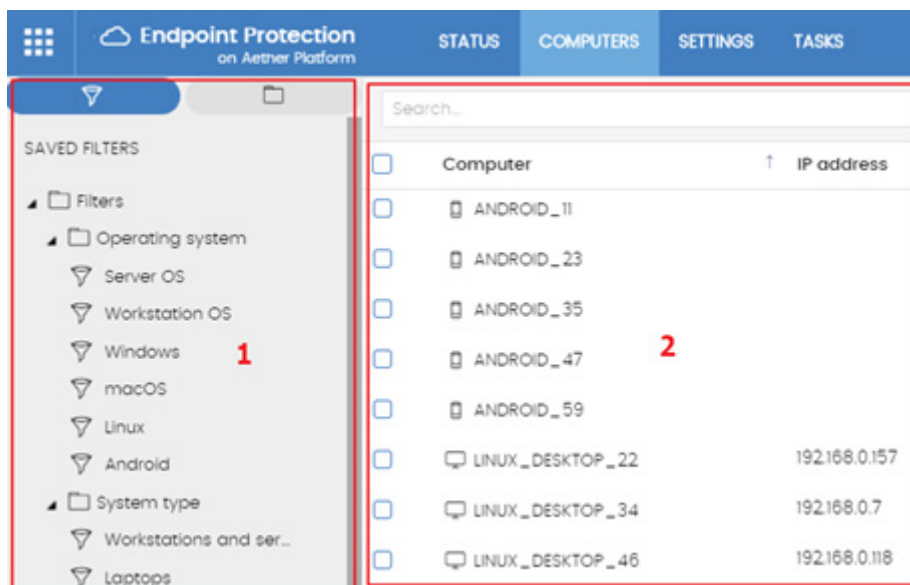


Figure 29: general view of the panels in the Computers area

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

Display computers in subgroups

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

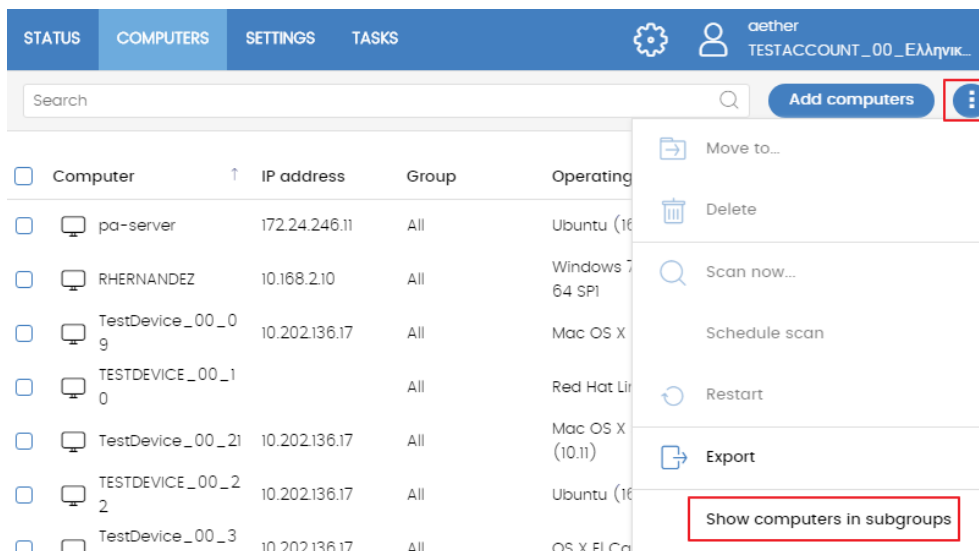


Figure 30: show computers in subgroups

7.2.1 The Computers tree panel

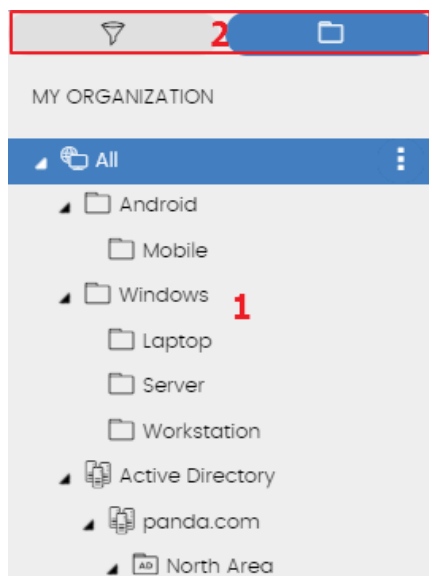




Figure 31: the Computers tree panel

Endpoint Protection / Plus displays the computers through the Computers tree (2), which offers three independent views or trees (1):

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

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

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



To locate unprotected computers or those with certain security criteria or protection status, see Chapter 14 Malware and network visibility. To assign security settings profiles, see Chapter 8 Managing settings. To run troubleshooting tasks, see chapter 16 Remediation tools.

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

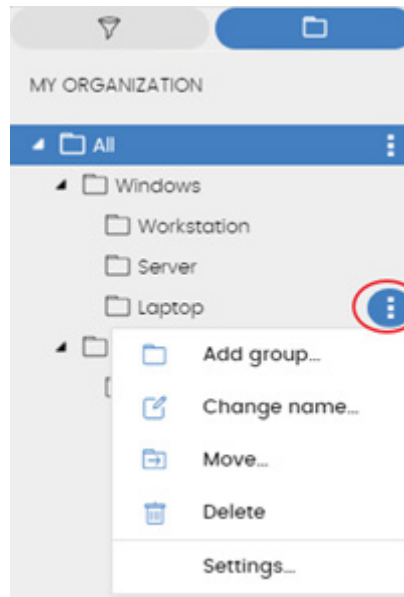


Figure 32: pop-up menu with all available operations for the selected branch

7.2.2 The Computers list panel

This screen displays the following information:

<div> <input type="text" value="Search"/> 2 + Add computers 3 </div>						
<input type="checkbox"/>	Computer	IP address	Group	Operating system	Last connection	
<input type="checkbox"/>	pa-server	172.24.246.11	All	Ubuntu (16.4)	4/24/2017 10:54:29 AM	⋮
<input type="checkbox"/>	RHERNANDEZ	10.168.2.10	All	Windows 7 Professional 64 SP1	4/24/2017 10:48:01 AM	⋮
<input type="checkbox"/>	TestDevice_00_09	10.202.136.17	All	Mac OS X Lion (10.11)	4/13/2017 8:49:41 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_10		All	Red Hat Linux (16.10)	4/24/2017 2:49:44 AM	⋮
<input type="checkbox"/>	TestDevice_00_21	10.202.136.17	All	Mac OS X Snow Leopard (10.11)	4/20/2017 8:50:21 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_22	10.202.136.17	All	Ubuntu (16.10)	4/24/2017 2:50:25 AM	⋮
<input type="checkbox"/>	TestDevice_00_33	10.202.136.17	All	OS X El Capitan (10.11)	4/24/2017 2:51:01 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_34	10.202.136.17	All	Red Hat Linux (16.10)	4/24/2017 2:51:04 AM	⋮
<input type="checkbox"/>	TestDevice_00_45	10.202.136.17	All	OS X Mavericks (10.11)	4/13/2017 8:51:41 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_46		All	Ubuntu (16.10)	4/24/2017 2:51:45 AM	⋮

Figure 33: the Computers list panel

- (1) List of computers belonging to the selected branch.

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

7.2.3 Computers list

You will see the following details for each computer:








Field	Comments	Values
Computer	Computer name and type	Character string  Desktop computer (Windows, Linux or MacOS workstation or server)  Laptop computer  Mobile device (Android smartphone or tablet)
IP address	The computer's primary IP address	Character string
Group	Folder in the Endpoint Protection / Plus Groups tree to which the computer belongs, and its type	Character string  Group  Active Directory domain or root group  Organizational Unit  Groups tree root
Operating system		Character string
Last connection	Date when the computer status was last sent to Panda Security's cloud	Date

Table 8: fields in the Computers list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Computer name	Character string

Field	Comments	Values
IP addresses	List of the IP addresses of the cards installed on the computer	Character string
Physical addresses (MAC)	List of the physical addresses of the cards installed on the computer	Character string
Domain	Windows domain to which the computer belongs	Character string
Active Directory	Path in the company's Active Directory tree where the computer is found	Character string
Group	Folder in the Endpoint Protection / Plus Groups tree to which the computer belongs	Character string
Agent version		Character string
System boot date		Date
Installation date	Date when the Endpoint Protection / Plus software was successfully installed on the computer	Date
Last connection date	Last time the computer connected to the cloud	Date
Platform	Type of operating system installed	Windows Linux MacOS Android
Operating system	Operating system installed on the computer, internal version and patches applied	Character string
Virtual machine	Indicates whether the computer is physical or virtual	Boolean
Exchange Server	Version of the mail server installed	Character string
Protection version		Character string
Last update on	Date the protection was last updated	Date
Licenses	Licensed product	Endpoint Protection / Plus
Proxy and language settings	Name of the proxy and language settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer has inherited the proxy and language settings	Character string
Security settings for workstations and servers	Name of the security settings applied to the workstation or server	Character string

Field	Comments	Values
Settings inherited from	Name of the folder from which the computer has inherited its settings	Character string
Security settings for Android devices	Name of the security settings applied to the mobile device	Character string
Settings inherited from	Name of the folder from which the device has inherited its settings	Character string
Per-computer settings	Name of the settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer has inherited its settings	
Description		Character string

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

Herramientas de filtrado

Field	Comments	Values
Computer	Computer name	Character string

Table 10: filters available on the Computers list screen

7.3. Filters tree

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

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

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

7.3.1 What is a filter?

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



A computer can belong to more than one filter.

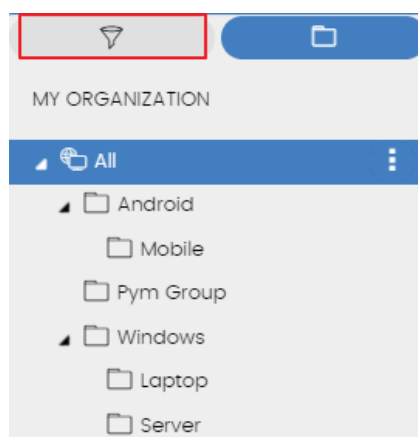


Figure 34: how to access the Filters tree

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

7.3.2 Groups of filters

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

7.3.3 Predefined filters

Endpoint Protection / Plus includes a series of commonly used filters that administrators can use to organize and locate network computers. Predefined filters can also be edited or deleted.



A predefined filter that has been deleted cannot be recovered.

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

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

Table 11: List of predefined filters

7.3.4 Creating and organizing filters

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

Creating filters

To create a filter, follow the steps below:

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



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

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

Creating folders

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



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

Deleting filters and folders

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



You cannot delete the 'Filters' root node.

Moving and copying filters and folders

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

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



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

Renaming filters and folders

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

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



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

7.3.5 Filter settings

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

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

A filter has four sections:

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

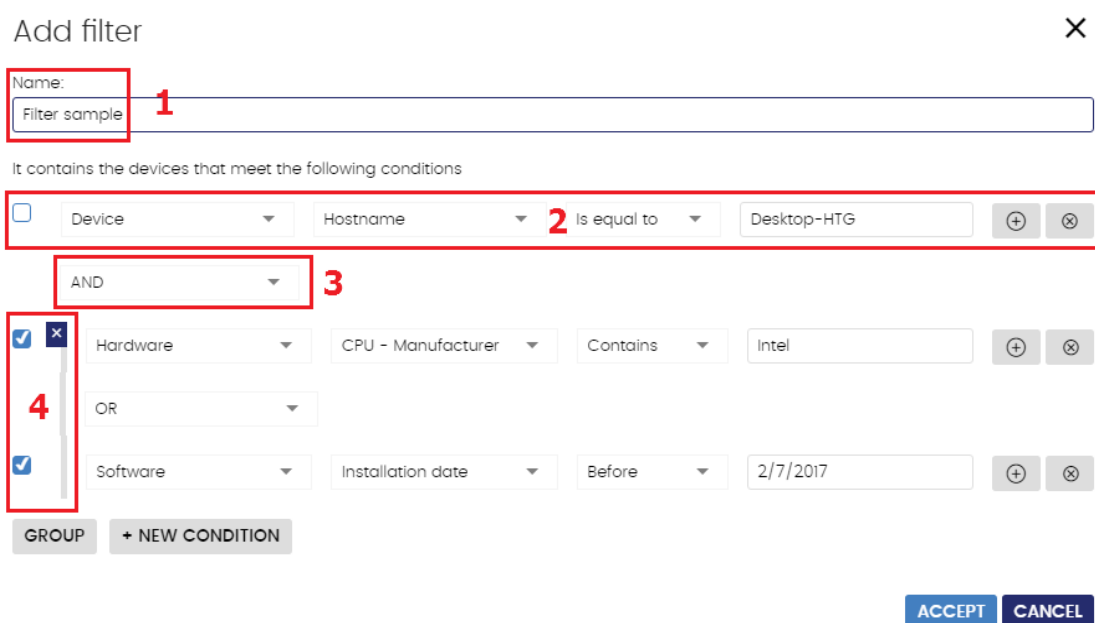


Figure 35: general view of the filter settings

7.3.6 Filter rules

A filter rule comprises the items described below:

- **Category (1)**: this groups the properties in sections to make it easy to find them.
- **Property (2)**: the characteristic of a computer that determines whether it belongs to a filter.
- **Operation (3)**: this determines the way in which the computer's characteristics are compared to the values set in the filter.
- **Value (4)**: the content of the property. Depending on the type of property, the value field will change to reflect entries such as 'date', etc.



Figure 36: components of a filter rule

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

7.3.7 Logical operators

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

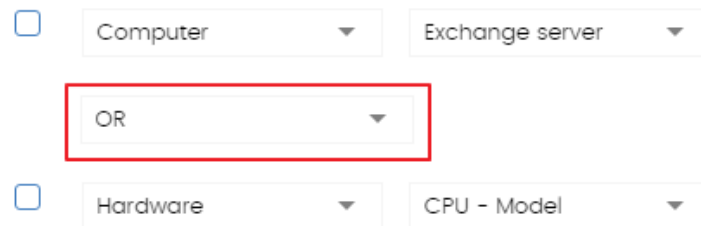


Figure 37: logical operator OR

7.3.8 Groups of filter rules

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

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

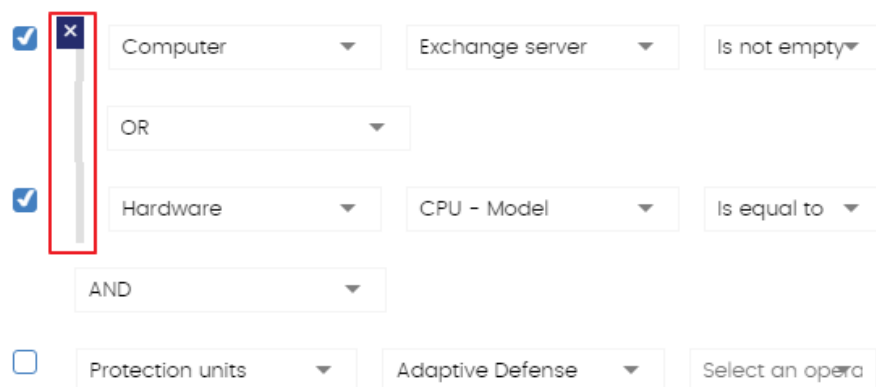


Figure 38: group of filter rules equivalent to (Rule 1 OR Rule 2) AND Rule 3

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

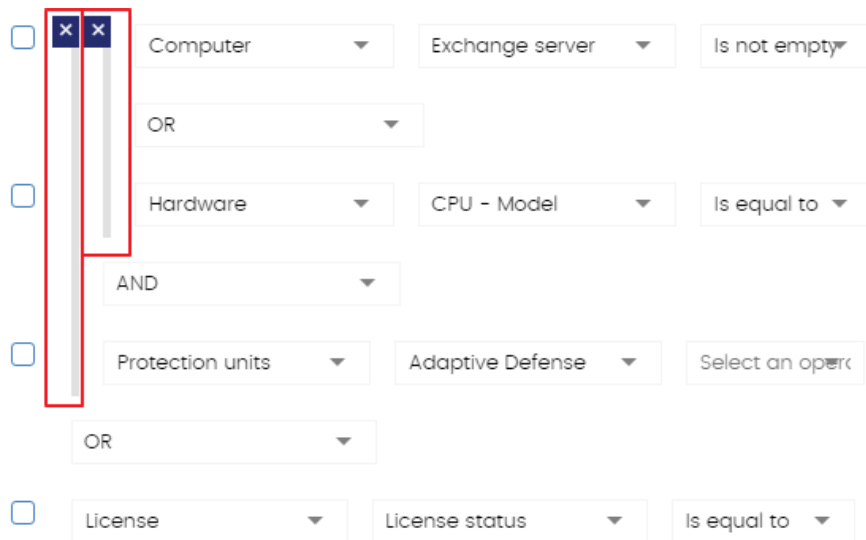


Figure 39: nested group equivalent to ((Rule 1 AND Rule 2) AND Rule 3) OR Rule 4

7.4. Groups tree

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

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

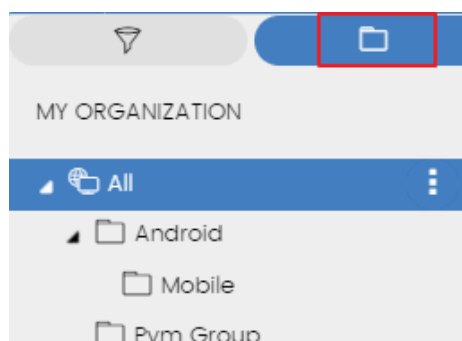


Figure 40: accessing the Groups tree

By clicking the different items in the tree, the panel on the right is updated, presenting all the computers in the selected group and its subgroups.






7.4.1 What is a group?

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



The maximum number of levels in a group is 10.

7.4.2 Group types

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


7.4.3 Groups structure

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



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

7.4.4 Active Directory groups

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

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

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

7.4.5 Creating and organizing groups

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

Creating groups

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



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

Deleting groups

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



The All root node cannot be deleted

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

Moving groups

To move a group, follow the steps below:

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



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

Renaming groups

To rename a group, follow the steps below:

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




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

7.4.6 Moving computers from one group to another

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


Moving groups of computers to groups

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

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

Moving a single computer to a group

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

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

Moving computers from an Active Directory group

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

Moving computers to an Active Directory group

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

Returning multiple computers to their Active Directory group

To return multiple computers to their original Active Directory group, click the context menu of the group where they are and select **Move computers to their Active Directory path**. All computers that

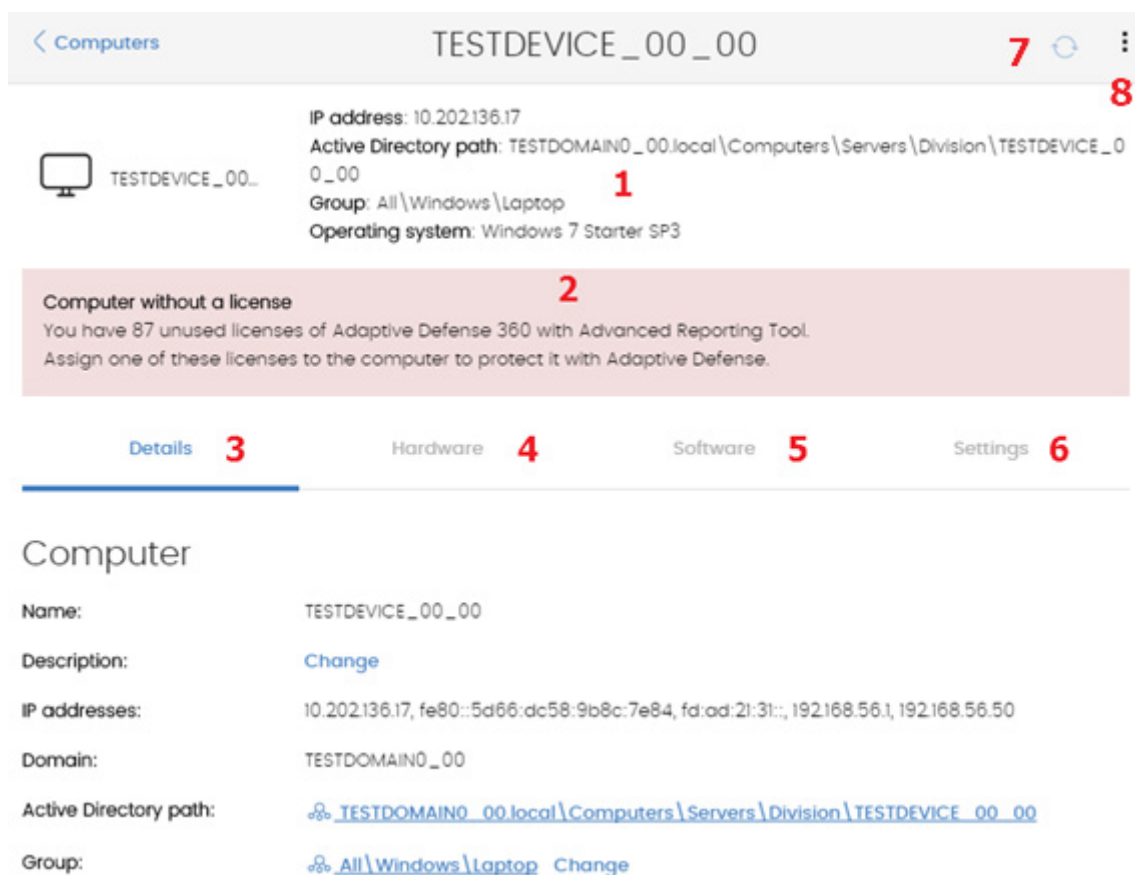
belong to a group in the company's Active Directory and which have been moved by the administrator to other groups in the **Endpoint Protection / Plus** console will be restored to their original Active Directory location.

7.5. Computer details

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

The Details window is divided into 6 sections:

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



TESTDEVICE_00_00

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

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

Details | Hardware | Software | Settings

Computer

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

Figure 41: general view of the computer details

7.5.1 General section (1)

This contains the following information:

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

7.5.2 Computer notifications section (2)

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

Unprotected computer:

- **Protection disabled**: a message is displayed stating that the antivirus or the Exchange protection is disabled. You are advised to assign protection settings to the computer with the protections enabled. See Chapter 8 for assigning security settings and Chapter 9 for creating security settings.
- **Protection with errors**: a message is displayed stating that the antivirus protection or the Exchange protection has an error. Restart the computer or reinstall the software. See Chapter 6 to install the software on the computer and Chapter 17 to restart the computer.
- **Installation error**: the computer is unprotected because there was an error during installation. See Chapter 6 to reinstall the software on the computer.
- **Installation in progress**: the computer is unprotected because the installation of **Endpoint Protection / Plus** is incomplete. Wait a few minutes until the installation is complete.

Out-of-date computer:

- **Computer pending restart**: the update for the security engine has been downloaded but the computer needs to be restarted for it to be applied. See Chapter 17 to restart the computer remotely.
- **Protection updates disabled**: the software won't receive any improvements. This will jeopardize the security of the computer in the future. See Chapter 8 to create and assign 'Per-computer settings' that allow the software to be updated.
- **Knowledge updates disabled**: the software won't receive any updates to the signature file. This will jeopardize the security of the computer in the short-term. See Chapters 10 and 11 to create security settings that allow the signature file to be updated.
- **Knowledge update error**: the download of the signature file failed. There is an explanation in this chapter of how to check the free space on your hard disk. See Chapter 16 to restart the computer. See Chapter 6 to reinstall software on the computer.

Offline since...

The computer has not connected to the Panda Security cloud in several days. Check the connectivity of the computer and the firewall settings. See chapter 10 Security settings for workstations and servers to check whether the connectivity requirements are fulfilled. See Chapter 6 to reinstall the software.

Pending restart

The administrator has requested a restart which has not yet been applied.

7.5.3 Details section (3)

The information in this tab is divided into two sections: **computer** with information about the device settings provided by the Panda agent, and **Security**, with the status of the **Endpoint Protection / Plus** protection.

- **Computer**
 - **Name:** computer name.
 - **Description:** descriptive text provided by the administrator.
 - **Physical addresses (MAC):** physical addresses of the network interface cards installed.
 - **IP addresses:** list of all the IP addresses (main and alias).
 - **Domain:** windows domain that the computer belongs to. This is empty if it does not belong to a domain.
 - **Active Directory path:** the path of the computer in the company's Active Directory tree.
 - **Group:** the group within the Groups tree to which the computer belongs. To change the computer's group, click **Change**.
 - Operating system
 - **Mail server:** version of Microsoft Exchange server installed on the computer.
 - **Virtual machine:** this indicates whether the computer is physical or virtual.
 - **Licenses:** the Panda Security product licenses installed on the computer. For more information, see Chapter 5.
 - **Agent version**
 - **System boot date**
 - **Installation date**
 - **Last connection** of the agent to the Panda Security infrastructure. The communications agent will connect at least every four hours.
- **Security:** this section indicates the status (Enabled, Disabled, Error) of the **Endpoint Protection / Plus** technologies.
 - **File Antivirus**
 - **Mail Antivirus**
 - **Web Browsing Antivirus**
 - **Firewall protection**

- **Device Control**
- **Web Access Control** (in Endpoint Protection Plus only)
- **Protection version**
- **Knowledge update date:** date when the signature file was last updated.



For more information about the security details of the protected computers, see chapter 14 Malware and network visibility.

7.5.4 Hardware section (4)

This contains the following information:

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

7.5.5 Software section (5)

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

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



Search tool

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

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

Change log

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

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

7.5.6 Settings section (6)

The **Settings** section displays the profiles associated with the computer and which are described in Chapter 8 Managing settings.

7.5.7 Force synchronization (7)

Sends all pending changes from the computer to the cloud.

7.5.8 Context menu

Shows the different actions you can take on the computer:

- **Move to:** moves the computer to a standard group.
- **Move to Active Directory group:** moves the computer to its original Active Directory group.
- **Delete:** frees up the **Endpoint Protection / Plus** license and deletes the computer from the Web console.
- **Disinfect:** lets you run a disinfection task immediately. Refer to chapter 16 Remediation tools for more information.
- **Scan now:** lets you run a scan task immediately. Refer to chapter 16 Remediation tools for more information.
- **Schedule scan.** Lets you schedule a scan task. Refer to chapter 16 Remediation tools for more information.
- **Restart:** restarts the computer immediately. Refer to chapter 16 Remediation tools for more information.
- **Report a problem:** opens a support ticket for Panda Security's support department. Refer to chapter 16 Remediation tools for more information.

8. Managing settings

What are settings?

Overview of assigning settings

Modular vs monolithic settings profiles

Overview of the four types of settings

Creating and managing settings

Manual and automatic assigning of settings

Viewing assigned settings

8.1. Introduction

This chapter looks at the resources implemented in **Endpoint Protection / Plus** for managing the settings of network computers.

8.2. What are settings?

Settings, also called “settings profiles” or simply “profiles”, offer administrators a simple way of establishing the security, productivity and connectivity parameters on the computers managed through **Endpoint Protection / Plus**.

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

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

8.3. Overview of assigning settings to computers

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

- 1 **Creation of groups of similar computers or with identical connectivity and security requirements**
- 2 **Assigning computers to a corresponding group**
- 3 **Assigning settings to groups**
- 4 **Immediate and automatic pushing out of settings to network computers**

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

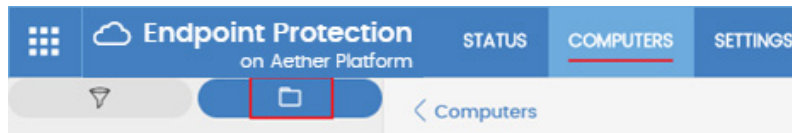


Figure 42: access to the Groups tree

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



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

8.3.1 Immediate deployment of settings

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



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

8.3.2 Multi-level trees

In medium-sized and large organizations, there could be a wide range of settings. To facilitate the management of large networks, **Endpoint Protection / Plus** lets you create group trees with various levels.

8.3.3 Inheritance

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

8.3.4 Manual settings

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

8.3.5 Default settings

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

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

- Default settings (Proxy and language)
- Default settings (Per-computer settings)
- Default settings (Workstations and servers settings)
- Default settings (Android devices settings)

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

8.4. Modular vs monolithic settings profiles

Endpoint Protection / Plus uses a modular format for creating and distributing settings to computers. As such, there are four independent profiles covering four settings areas.

The four types of profiles are as follows:

- Proxy and language settings
- Per-computer settings
- Workstation and servers settings
- Android devices settings

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

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

Case study: creating settings for several offices

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

Network of a company formed by several offices:



If **Endpoint Protection / Plus** implemented all the configuration parameters in a single monolithic profile, the company would require 15 different settings profiles ($5 \times 3 = 15$) to adapt to the needs of all three departments in the company's offices.

Monolithic profile



However, as **Endpoint Protection / Plus** separates the proxy settings from the security settings, the number of profiles needed is reduced ($5 \text{ proxy profiles} + 3 \text{ department profiles} = 8$) as the security

profiles for each department in one of the offices can be reused and combined with the proxy profiles in other offices.

Proxy and Language modular profile



Security modular profile



8.5. Overview of the four types of settings



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

Proxy and language settings

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

Per-computer settings

Let you define several settings pertaining to the Panda agent:

- Update frequency of the **Endpoint Protection / Plus** software installed on computers. Refer to chapter 12 Software updates.

- Password required to install the agent on end users' computers.
- Anti-Tamper protection.

Workstation and server settings

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

Android device settings.

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

8.6. Creating and managing settings

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

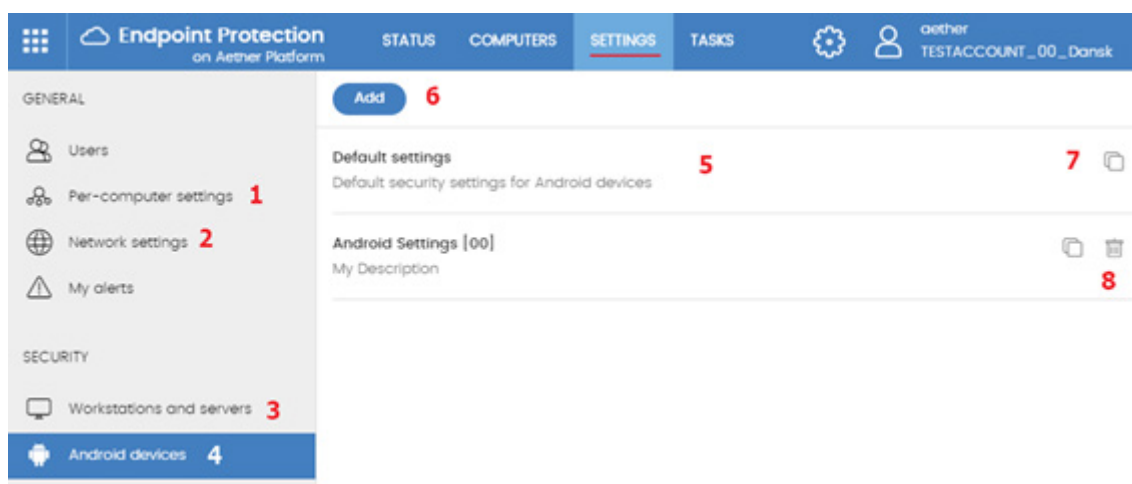


Figure 43:Screen for creating and managing settings profiles

Creating settings

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

Copying and deleting settings

Use the icons (7) and (8) to copy and delete a settings profile, although if it has been assigned to one or more computers, you won't be able to delete it until it has been freed up. Click the settings profile in order to edit it.



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

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

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

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

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

8.7.1 Assigning settings directly/manually

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

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

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



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

From the Groups tree

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

- Click the group's context menu.
- Click **Settings**. A window will open with the profiles already assigned to the selected group and the type of assignment:
 - **Manual/Direct assignment**: the text will read **Directly assigned to this group**.
 - **Inherited/Indirect assignment**: the text will read **Settings inherited from**, followed by the name and full path of the group the settings were inherited from.

- Select the new settings and click **OK** to assign the settings to the group.
- The settings will immediately be deployed to all members of the group and sub-groups.
- The changes will immediately apply to all corresponding computers.

From the computer list panel

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

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

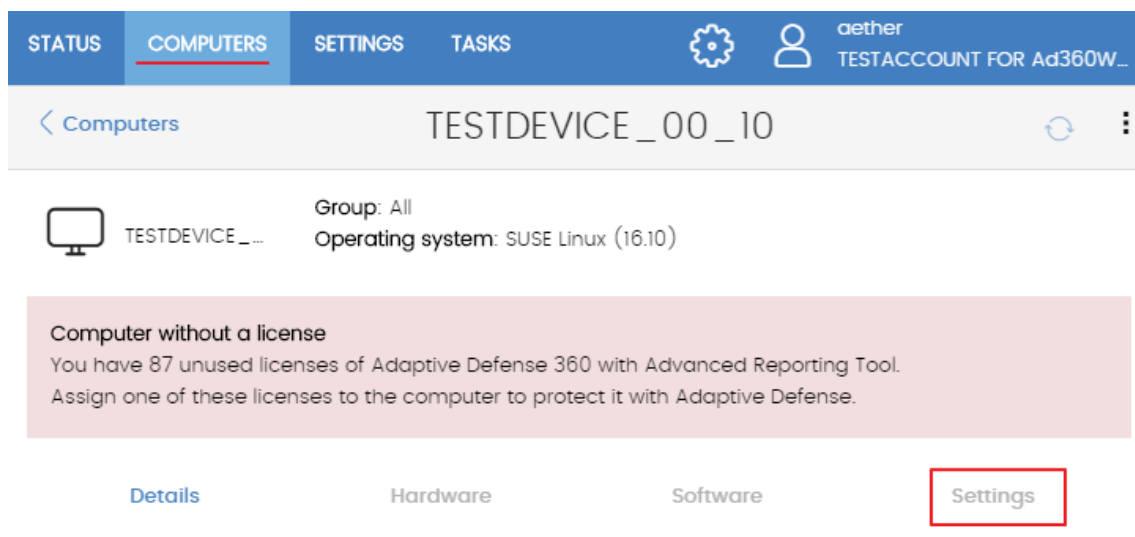



Figure 44: access to settings from the computer details tab.

- Select the new settings. They will be applied automatically to the computer.

From the settings profile itself

If you want to assign settings to one or more computers without the need for them to belong to a group, follow the steps below:

- In the **Settings** menu, click the type of profile you want to assign in the left-hand panel.
- Select the settings and then click **Select computers**. The computers with profiles assigned will be displayed.
- Click  to add the computers you want to add.
- Click **Add**. The profile will be assigned to the selected computers and the new settings will be immediately applied.



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

8.7.2 Indirect assigning of settings: the two rules of inheritance

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

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

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

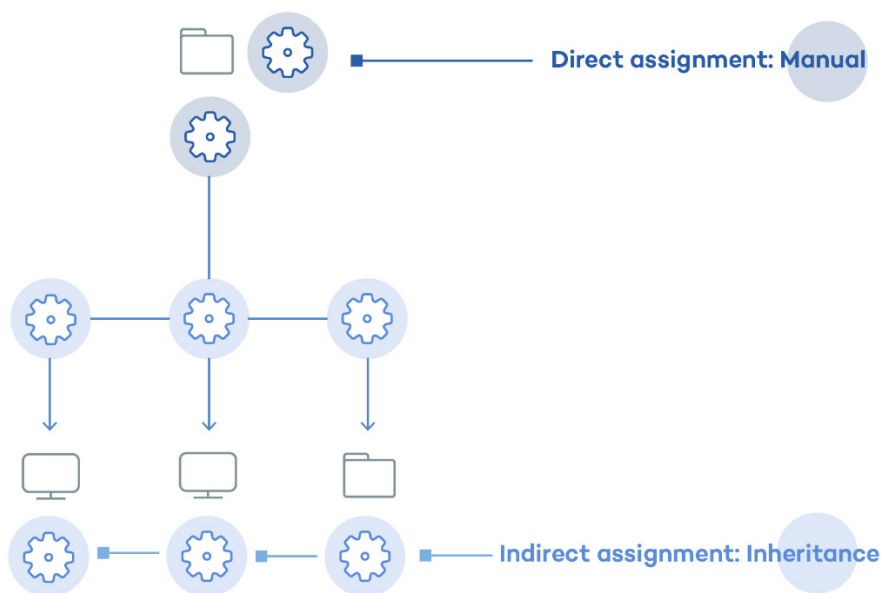


Figure 45: example of inheritance/indirect assigning. The parent group receives the settings that are then pushed out to the child nodes.

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

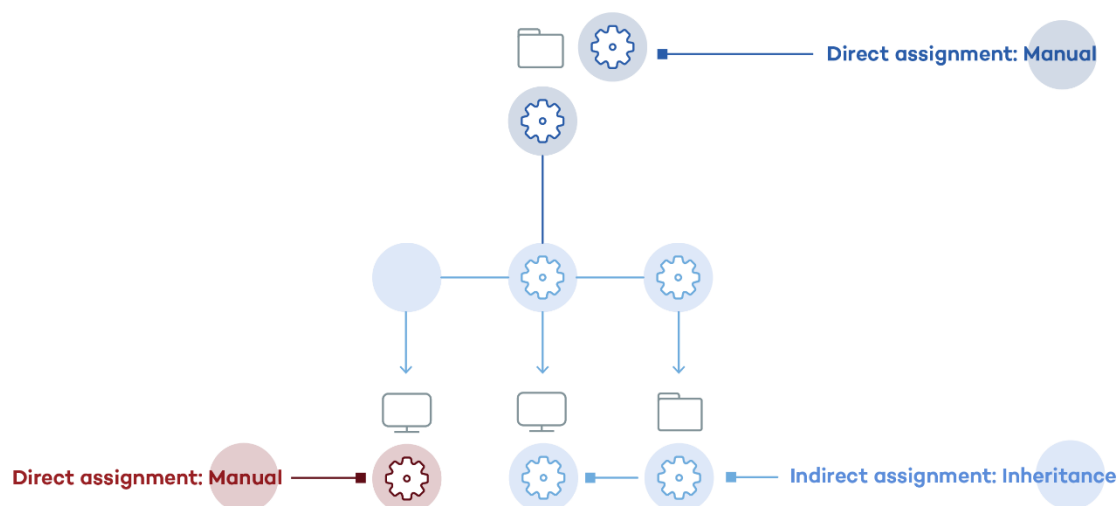


Figura 46: example of the priority of direct assigning over indirect. The inherited settings are overwritten with the manually assigned ones

8.7.3 Inheritance limits

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

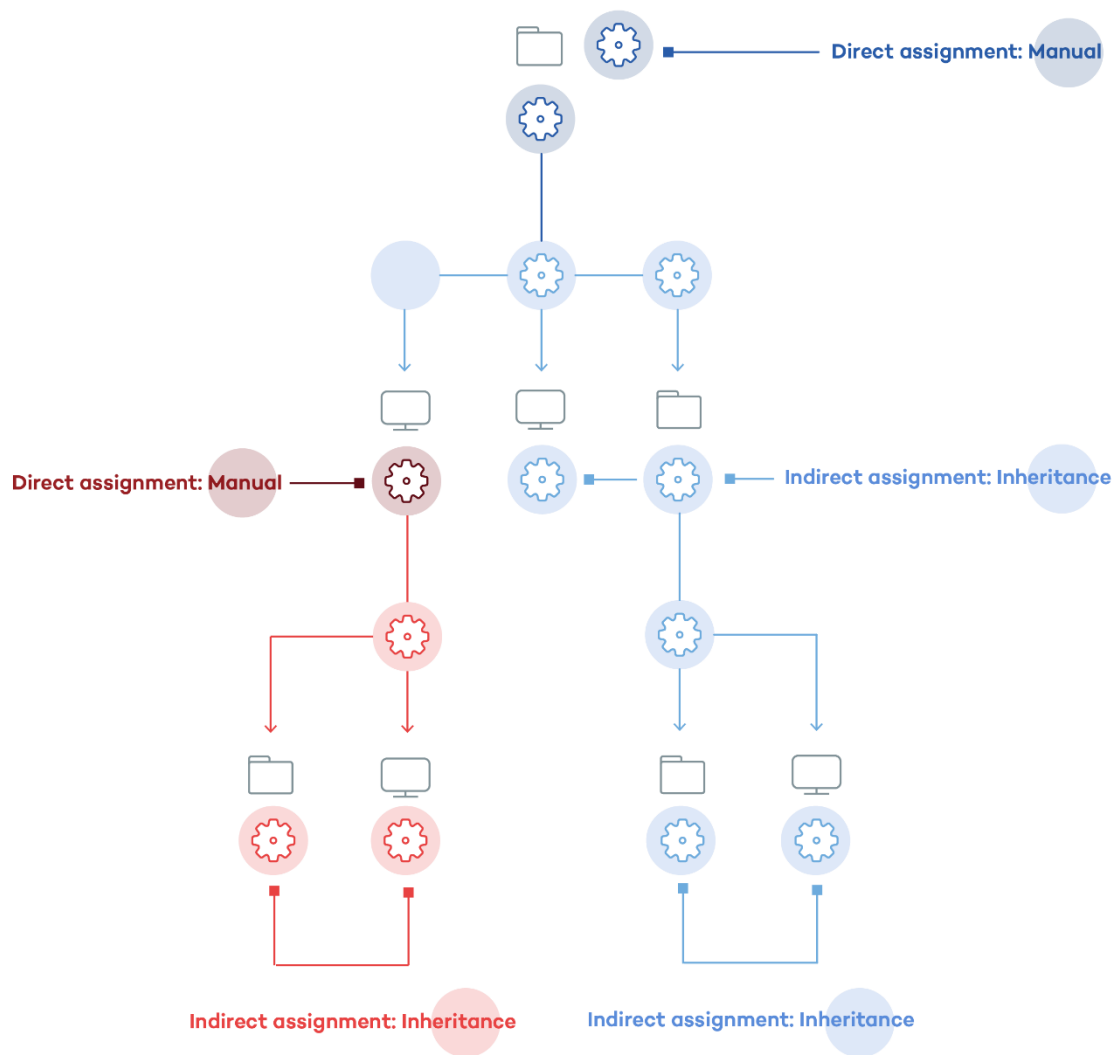


Figure 47: example of inheritance restricted by manual/direct assignment of settings. The parent node settings are passed on to the dependent branches of the tree but stop once manually assigned settings are found.

8.7.4 Overwriting settings

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

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

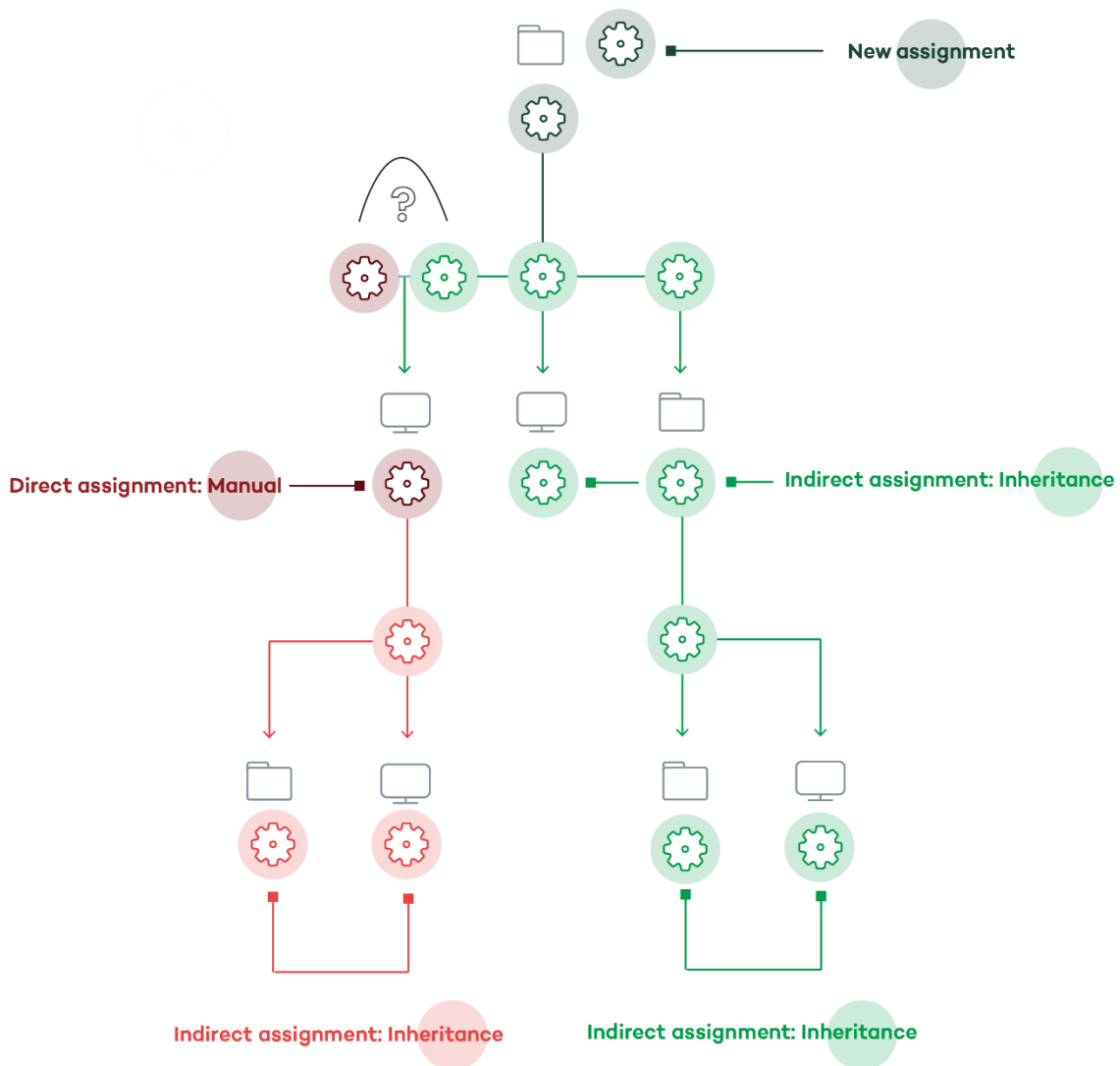


Figure 48: change to the inherited settings in a node that affects the manually applied settings of items lower down

In this case, **Endpoint Protection / Plus** asks the administrator if the previously set manual settings are to be kept or overwritten with the inheritance:

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

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

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

Keep all settings

Make all inherit these settings

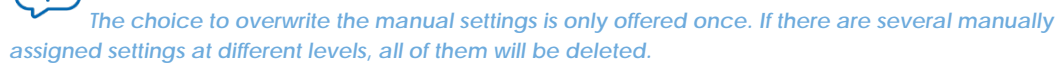
Figure 49: window for selecting the way that settings changes are applied to a branch containing groups configured manually

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

Make all inherit these settings



Be careful when choosing this option as it is not reversible! All manually applied settings below the node will be lost, and the inherited settings will be applied immediately to the computers. This could change the way Endpoint Protection / Plus acts on many computers.



Keep all settings

115

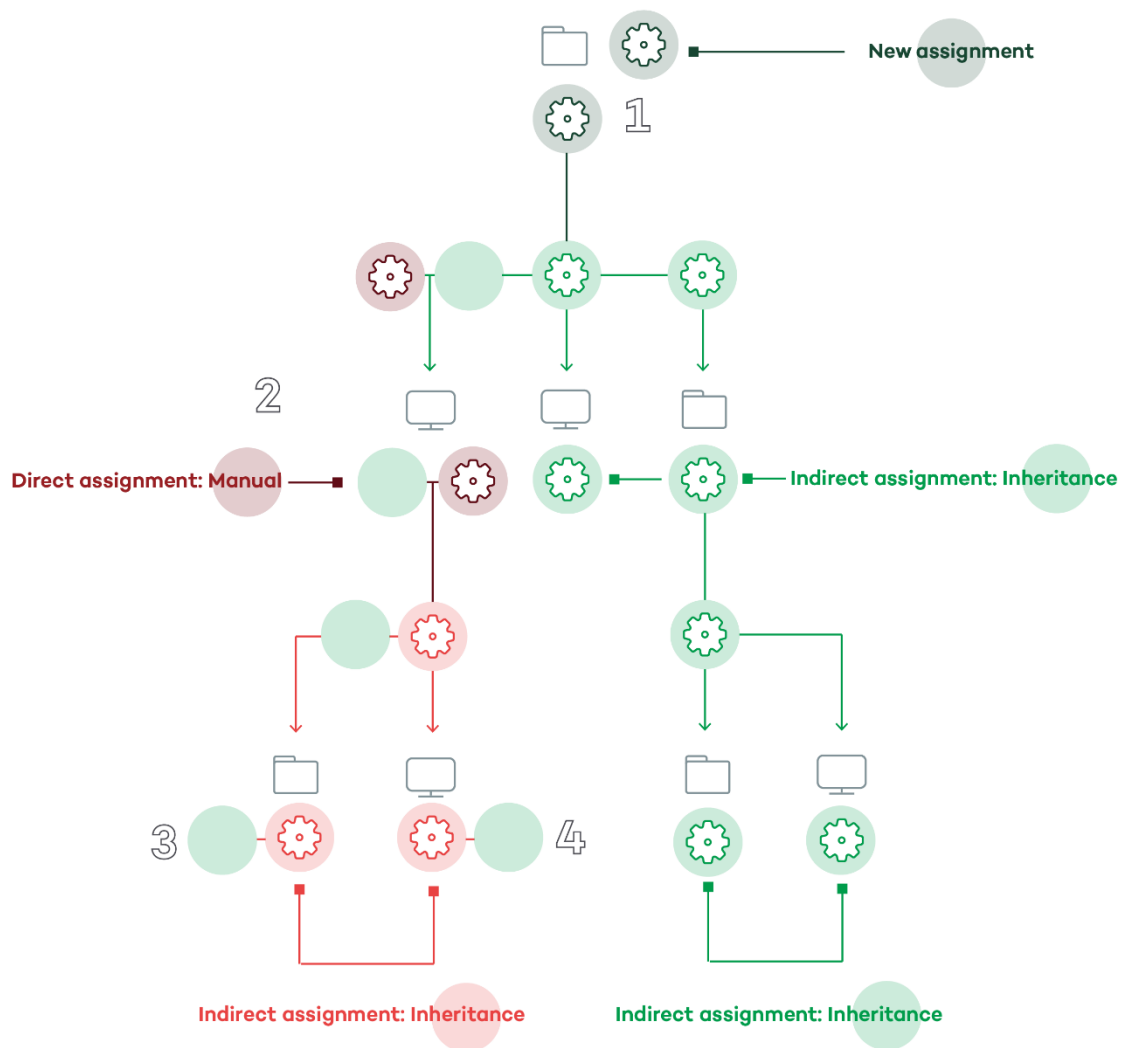


Figure 51: manually applied settings are maintained

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

8.7.5 Deleting manually assigned settings and restoring inheritance

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

- In the **Computers** menu, click the group with the manually assigned settings to delete in the Groups tree in the panel on the left.
- Click the context menu icon and select **Settings**. A pop-up window will appear with the profiles assigned. Select the manually assigned profile you want to delete.

- A list will appear with all the available profiles that can be assigned manually. At the end of the list you will see the button **Inherit from parent group** along with the settings that will be inherited if you click the button and the group from which they will be inherited.

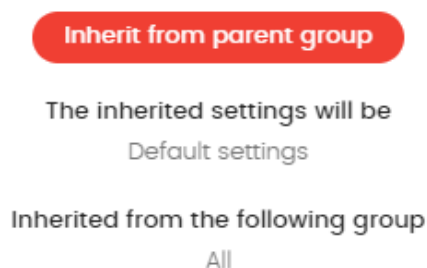


Figure 52: button for deleting manual settings and re-establishing inheritance

8.7.6 Moving groups and computers

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

Moving individual computers

In the case of moving individual computers, **Endpoint Protection / Plus** respects the manual settings that are established on the devices moved, and automatically overwrites the inherited settings with the settings established in the new parent group.

Moving groups

In the case of moving groups, **Endpoint Protection / Plus** displays a window with the question "Do you want the settings inherited by this computer to be replaced by those in the new group?"

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

8.8. Viewing the assigned settings

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

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

Groups tree

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

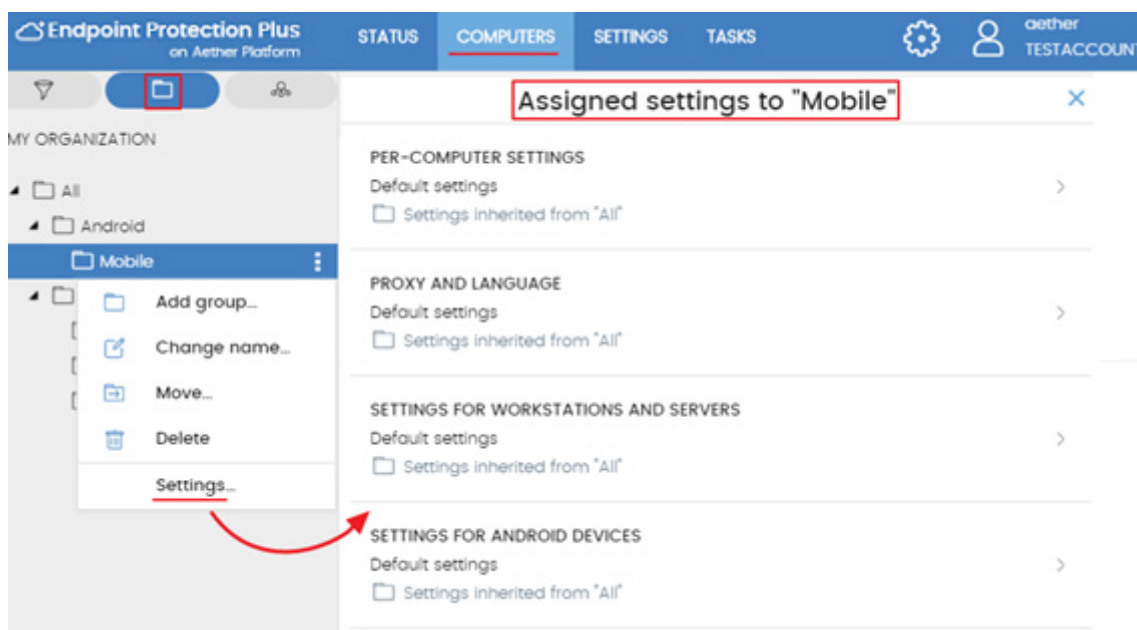




Figura 53: settings assigned from the Groups tree

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

- **Type of settings:**
 - Proxy and language settings
 - Per-computer settings
 - Settings for workstations and servers
 - Settings for Android devices
- **Name of the settings:** name given by the administrator when creating the settings.
- **Inheritance type**
 - **Settings inherited from...:**  The settings were assigned to the specified parent folder. Every computer on the branch inherits them.
 - **Directly assigned to this group:**  The settings applied to the computers are those that the administrator assigned to the folder manually.

Computer settings tab

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

Exporting the list of computers

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

The CSV file includes the following information fields:

- Proxy and language settings
- Settings inherited from
- Security settings for workstations and servers
- Settings inherited from
- Security settings for Android devices
- Settings inherited from
- Per-computer settings
- Settings inherited from

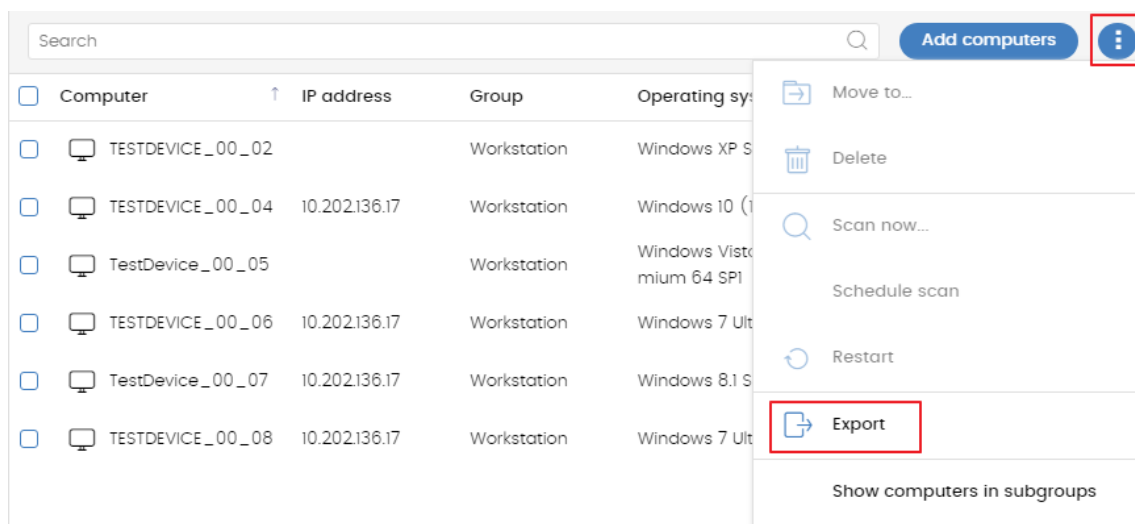


Figure 54: exporting the list of computers in CSV format



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

9. Agent and local protection settings

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

9.1. Introduction

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

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

9.2. Configuring the Panda agent role

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

- Proxy
- Discovery computer
- Cache

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

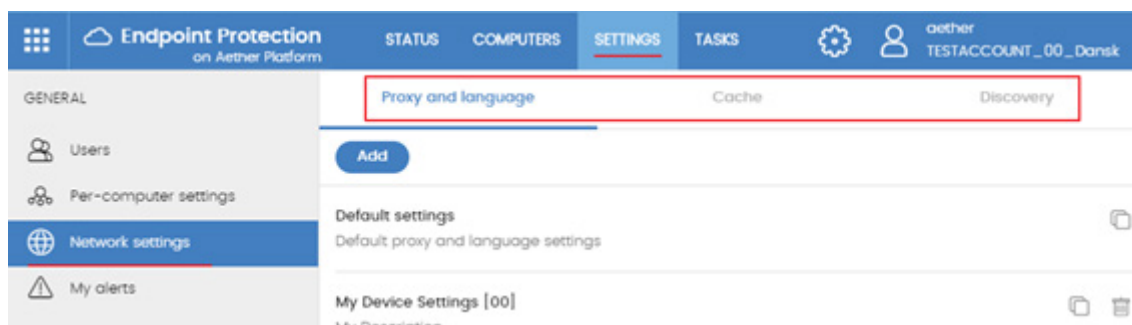


Figure 55: access to the role settings window


9.2.1 Proxy role

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

Configuring a computer as a proxy server

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

Revoking the proxy role

- Click the **Proxy and language** tab. Select an existing **Proxy and language** settings profile or create a new one.
- Expand the Proxy section and select Endpoint Protection / Plus proxy.
- Click Select computer...
- Click the  icon of the computer that you want to stop acting as a proxy.

9.2.2 Cache/repository role


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

Configuring a computer as a cache

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

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

Revoking the cache role

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

Requirements and limitations of computers with the cache role

- At most 2 GB of additional disk space to store downloads.
- The scope of the computer with the cache role is restricted to the network segment to which its network interface is connected. If a cache computer has several network interface cards, it can serve as a repository for each network segment to which it is connected.



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

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

Discovery of cache nodes

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

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

9.2.3 Discovery computer role

The **Discovery** tab is directly related to the installation and deployment of **Endpoint Protection / Plus** across the customer's network. Refer to chapter 6 for more information about the **Endpoint Protection / Plus** discovery and installation processes.

9.3. Configuring Internet access via a proxy server

Configuring proxy usage

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

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

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

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

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

To configure the sending of data via a **Panda Endpoint Protection / Plus** proxy, click the link **Select computer** to display a list of the available computers that have the proxy role on the network.



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

Fallback mechanism

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

- If the Internet connection is configured via corporate proxy or **Panda Endpoint Protection / Plus** proxy and there is no response, an attempt is made to connect directly.

- Internet Explorer: the Panda agent tries to recover the Internet Explorer proxy settings with the profile of the user logged in to the computer.
 - If the configuration of the proxy credentials is defined explicitly, this method can't be used.
 - If the Internet Explorer proxy settings use PAC (Proxy Auto-Config) the URL is obtained from the settings file, provided that the protocol is HTTP or HTTPS.
- WinHTTP / WinInet: the default proxy settings are read.
- WPAD (Web Proxy Auto-discovery Protocol): a request is sent to the network via DNS or DHCP to get the URL that points to the PAC settings file.

9.4. Configuring real-time communication

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

Disabling real-time communication

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

If you disable real-time communication, your computers will communicate with the **Endpoint Protection / Plus** server every 15 minutes.

9.5. Configuring the agent language

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

- Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Proxy and language** tab.
- Select an existing **Proxy and language** settings profile or create a new one.
- Select a language from the list:
 - English
 - Spanish

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



If the language is changed while the Endpoint Protection / Plus local console is open, the system will prompt the user to restart the console. This process does not affect the security of the computer.

9.6. Configuring the Anti-Tamper protection and password

9.6.1 Anti-Tamper protection

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

Enabling the Anti-Tamper protection

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

9.6.2 Password-protection of the agent

Administrators can set up a password to prevent users from changing the protection features or completely uninstalling the **Endpoint Protection / Plus** software from their computer.

Setting up the password

- Click the **Settings** menu at the top of the console. Then, click **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.

- Expand section Security against unauthorized protection tampering:
 - Request password to uninstall Panda agent from computers: this is to prevent users from uninstalling the Endpoint Protection / Plus software.
 - **Allow the protections to be temporarily enabled/disabled from the computers' local console:** this allows administrators to manage a computer's security from its local console. Enabling this option requires setting up a password.

10. Security settings for workstations and servers

Introduction to the security settings for workstations and servers

General settings

Antivirus

Firewall

Device Control

Web Access Control

Antivirus for Exchange servers

Anti-Spam for Exchange servers

Content Filtering for Exchange servers

10.1. Introduction

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

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

10.2. Introduction to the security settings for workstations and servers

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

- **General:** lets you configure the updates, the removal of competitor products, and file exclusions from scans.
- **Antivirus:** lets you configure the general parameters that control the traditional anti-malware protection against viruses and threats.
- **Firewall (Windows devices):** lets you configure the general parameters that control the firewall and IDS against network attacks.
- **Device Control (Windows devices):** lets you configure the general parameters that control user access to the peripheral devices connected to their computers.
- **Web Access Control (Endpoint Protection Plus only):** lets you restrict access to certain Web content categories.
- **Antivirus for Exchange servers (Endpoint Protection Plus only):** scans the inbound and outbound email that goes through your Exchange mail servers, searching for threats.
- **Anti-Spam for Exchange servers (Endpoint Protection Plus only):** scans the inbound and outbound email that goes through your Exchange mail servers, searching for unwanted email.
- **Content Filtering for Exchange servers (Endpoint Protection Plus only):** restricts the content types that can reach your Exchange servers.

Feature	Windows	Mac OS X	Linux	Windows Exchange
Antivirus	X	X	X	X
Firewall & IDS	X			
Email Protection	X			
Web Protection	X	X	X	
Device Control	X			

Web Access Control	X	X	X
Anti-Spam			X
Content Filtering			X

Table 12: security features per platform

10.3. General settings

The general settings let you configure how **Endpoint Protection / Plus** behaves regarding updates, the removal of competitor products, and file and folder exclusions from the scans performed by the traditional antivirus.

10.3.1 Updates

Refer to chapter 12 Software updates for more information about how to update the agent, the protection, and the software signature file installed on users' computers.

10.3.2 Uninstall other security products

Refer to chapter 6 Installing the Endpoint Protection / Plus software for more information about what to do with competitor products when installing **Endpoint Protection / Plus**.



Refer to Appendix 3: list of uninstallers for a list of the competitor products that Endpoint Protection / Plus can automatically uninstall from users' computers.

10.3.3 Exclusions

The **Exclusions** section lets you select the computer items that won't be scanned for malware.

Disk files

Lets you select the files on the hard disk of protected computers that won't be scanned by **Endpoint Protection / Plus**.

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

Exclude the following email attachments:

Lets you specify the extensions of email file attachments that **Endpoint Protection / Plus** won't scan.

10.4. Antivirus

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

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

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

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

10.4.1 Threats to detect

Lets you configure the types of threats that **Endpoint Protection / Plus** will search for and remove from the file system, mail client and Web client installed on users' computers.

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

10.4.2 File types

This section lets you specify the types of files to be scanned by **Endpoint Protection / Plus**:

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

10.5. Firewall (Windows devices)

Endpoint Protection / Plus provides three basic tools to filter the network traffic that protected computers send and receive:

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

10.5.1 Operational mode

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

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

10.5.2 Network type

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

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

Endpoint Protection / Plus will behave differently and will apply different predetermined rules depending on the type of network. You can view these predetermined rules (**Panda rules**) in the **Program rules** and **Connection rules** sections.

10.5.3 Program rules

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

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

1 Set the default action

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

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

2 Enable Panda's rules

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

3 Add rules to define the specific behavior of your applications

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



Figure 56: edit controls for program rules

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

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

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

10.5.4 Connection rules

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

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

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

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

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

2 Enable Panda's rules

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

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

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



Figure 57: edit controls for connection rules

The order of the rules on the list is important. They are applied in descending order, therefore, if you change the position of a rule, you will also change its priority.

Next, we describe the fields found in a connection rule:

- **Name**
- **Description**
- **Action:** indicates the action that **Endpoint Protection / Plus** will take if the examined traffic matches the rule.
 - **Allow:** allows the traffic.
 - **Deny:** blocks the traffic. It drops the connection.
- **Direction:** specifies the direction of the traffic for connection protocols such as TCP.
 - **Outbound:** outbound traffic.
 - **Inbound:** inbound traffic.
- **Zone**
- **Protocol:** Lets you specify the rule protocol. The options displayed will vary depending on the option you select:
 - **TCP, UDP, TCP/UDP:** lets you define TCP and/or UDP rules, including local and remote ports.
 - **Local ports:** lets you specify the connection port used on the user's computer. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).
 - **Remote ports:** lets you specify the connection port used on the remote computer. Select **Custom** to enter multiple ports separated by commas (,). To specify a range, use a hyphen (-).
 - **ICMP:** lets you create rules that describe ICMP messages, along with their type and subtype.
 - **IP Types:** lets you create rules for the IP protocol and other higher-level protocols.
- **IP addresses:** lets you specify the traffic's source and destination IP addresses.
- **MAC addresses:** lets you specify the traffic's source and destination MAC addresses.



The source and destination MAC addresses are overwritten every time the traffic goes through a proxy, router, etc. Therefore, the data packets will reach their destination with the MAC address of the last device that handled traffic.

10.5.5 Block intrusions

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

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

- **IP Explicit Path:** rejects IP packets that contain an explicit source route field. These packets are not routed based on their target IP address, but the routing information is defined beforehand.
- **Land Attack:** stops denial-of-service attacks that use TCP/IP stack loops by detecting packets with identical source and target addresses.
- **SYN Flood:** this attack launches TCP connection attempts massively to force the targeted computer to commit resources for each connection. The protection establishes a maximum number of open TCP connections to prevent the computer under attack from becoming saturated.
- **TCP Port Scan:** detects if a host tries to connect to several ports on the protected computer in a specific time period. The solution filters both the requests to open ports and the replies to the malicious computer. This prevents the attacking computer from obtaining information about the status of the ports.
- **TCP Flags Check:** detects TCP packets with invalid flag combinations. It acts as a complement to the protection against port scanning by blocking attacks of that type such as "SYN&FIN" and "NULL FLAGS". It also complements the protection against OS fingerprinting attacks as many of these are based on replies to invalid TCP packets.
- **Header Lengths**
 - **IP:** rejects inbound packets with an IP header length that exceeds a specific limit.
 - **TCP:** rejects inbound packets with a TCP header length that exceeds a specific limit.
 - **Fragmentation overlap:** checks the status of the packet fragments to be reassembled at the destination, protecting the system against memory overflow attacks due to missing fragments, ICMP redirects masked as UDP, and computer scanning.
- **UDP Flood:** rejects UDP streams to a specific port if the number of UDP packets exceeds a preconfigured threshold in a particular period.
- **UDP Port Scan:** protects the system against UDP port scanning attacks.
- **Smart WINS:** rejects WINS replies that do not correspond to requests sent by the computer.
- **Smart DNS:** rejects DNS replies that do not correspond to requests sent by the computer.
- **Smart DHCP:** rejects DHCP replies that do not correspond to requests sent by the computer.

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

10.6. Device Control (Windows devices)

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

The Device Control feature lets you configure the way the protected computer will behave when connecting or using a removable or mass storage device. Select the device or devices you want to authorize or block, and specify their usage.

Follow the steps below to enable the Device Control feature:

- Select the **Enable device control** checkbox **(1)**.
- From the drop-down menu, select the authorized usage level for each type of device **(2)**
 - In the case of USB flash drives and CD/DVD drives, you can choose among **Block**, **Allow read access** or **Allow read & write access**.
 - The options available for Bluetooth and imaging devices, USB modems and smartphones are **Allow** and **Block**.

10.6.1 Allowed devices

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

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

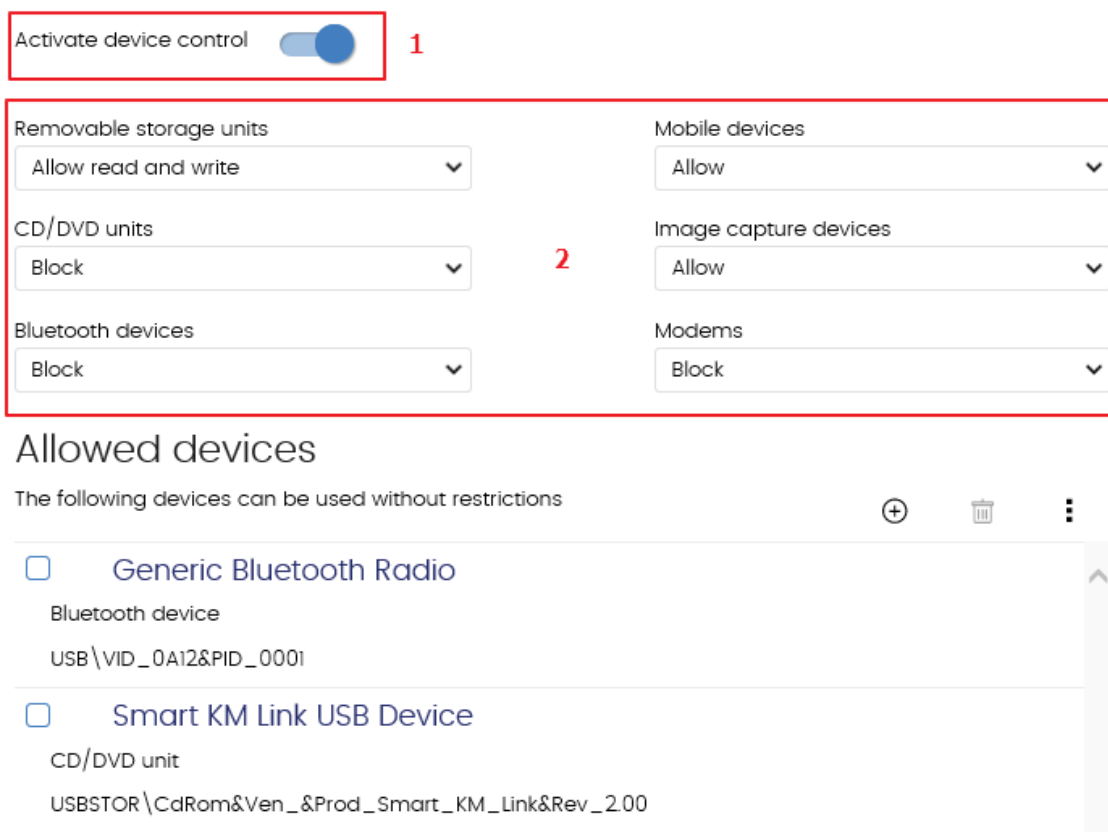




Figure 58: device Control settings

Endpoint Protection / Plus lists all devices connected to each computer. Click the  icon in the **Allowed devices** section to display the list of all devices connected to the computers on your network. Use this list to select those devices that you want to exclude from the general block rules defined for each type of device. Finally, use the  button to delete existing exclusions.

10.6.2 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 **Endpoint Protection / Plus** Web console.

To export and import exclusion lists, use the **Export** and **Import** options from the context menu .

10.6.3 Obtaining a device's unique ID

If you want to exclude a device from the Device Control feature without having to wait for the user to connect it and then exclude it manually, obtain the device's ID. To do this, follow the steps below:

- In the Windows Device Manager, access the properties of the USB device that you want to identify in order to exclude it.

- Go to the Details tab and select Resources from the Property menu. A value called CM_DEVCAP_UNIQUEID should be displayed.
- Next, select Device Instance Path from the Property menu to obtain the device's unique ID.

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

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

Once you have the unique IDs of all the devices that you want to allow, you can create your whitelist and import it as explained in the previous section.

10.7. Web Access Control



Feature only available in Endpoint Protection Plus.

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

To enable and disable it, click the **Enable Web access control** option.

10.7.1 Configuring time periods for the Web Access Control feature

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

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

Next, select the times at which you want the Web Access Control to be enabled. To enable it only during certain times, select the relevant box and use the time grid to select the times that you want.

- To select whole days, click the relevant day of the week.
- To select the same time period for every day of the week, click the relevant hours.
- To select every day of the month, click the **Select all** button.
- To deselect your selection and start over, click the **Clear** button.

10.7.2 Denying access to specific Web pages

Endpoint Protection / Plus groups Web pages into 64 categories. All you have to do is select those categories that you want to deny access to.

Use the available category list to do so. If a user visits a Web page that belongs to one of the forbidden categories, a warning Web page will be displayed indicating that access is denied and the reason.

Denying access to pages categorized as unknown

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



Bear in mind that internal and intranet sites accessible on ports 80 and 8080 may be categorized as unknown, resulting in users not being able to access them. To avoid this, you can add any pages you want to the exclusion whitelist explained below.

10.7.3 List of allowed/denied addresses and domains

You can set a list of pages that will always be allowed (whitelist) or blocked (blacklist), regardless of the category that they belong to.

You can edit these lists at any time.

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

As soon as a website coincides with one of the whitelisted/blacklisted sites (either wholly or partially), it will be allowed/blocked. In the case of long URLs, it will be enough to enter the beginning of the URL in the appropriate box.

10.7.4 Database of all URLs accessed from computers

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

The data displayed is as follows:

- User ID
- Protocol (HTTP or HTTPS)
- Domain
- URL

- Returned category
- Action (Allow/Deny)
- Date accessed
- Access counter (by category and domain)

10.8. Antivirus for Exchange servers



Feature only available in Endpoint Protection Plus.

Provided you have the necessary licenses, you'll be able to enable the protection for Exchange servers from the management console, and assign licenses to any Exchange server on your network.

The protection for Exchange servers supports Exchange 2003, 2007, 2010, 2013 and 2016, and consists of the following three modules:

- Antivirus
- Anti-spam
- Content filter

Additionally, and depending on the moment when **Endpoint Protection / Plus** scans the email traffic, we can differentiate between two protection modes: mailbox protection and transport protection.

Tabla 13 shows the Exchange versions supported by each protection module and scan mode.

Scan mode/Protection module	Antivirus	Anti-Spam	Content Filtering
Mailbox	2003, 2007, 2010		
Transport	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016

Tabla 13: exchange versions supported by each protection module and scan mode

Mailbox protection

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

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

Transport protection

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

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

You can enable/disable the mailbox and/or the transport protection by clicking the relevant checkboxes.

Mailbox protection

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

Exchange 2013-2016 does not allow message manipulation. That is, if a message contains a dangerous item, the entire message will be moved to quarantine. In such a case, the end user protected with **Endpoint Protection / Plus** will receive a message with the original subject but the message body replaced with a warning text. This text will prompt the user to contact the network administrator to recover the original message.

With all other versions of Exchange Server, **Endpoint Protection / Plus** will take the action defined by Panda Security when a malware item is detected: disinfect the attachment if disinfection is possible, or send it to quarantine if disinfection is not possible. That is, the end user will receive the original message with the clean attachments or, if disinfection is not possible, a replacement file called "security_alert.txt" with information about the reason for the detection.

10.9. Anti-spam for Exchange servers



Feature only available in Endpoint Protection Plus.

Use the **Detect spam** button to enable or disable this protection.

Upon enabling the anti-spam protection, **Endpoint Protection / Plus** will show a pop-up message offering the possibility to add a series of exclusion rules to improve the performance of your mail servers.

10.9.1 Actions to perform on spam messages

Specify what to do with spam messages:

- **Let the message through:** the tag *Spam* will be added to the subject line of the message. This is the default option.

- **Move the message to...** You will have to specify the email address that the message will be moved to. In addition, the tag *Spam* will be added to the subject line of the message.
- **Delete the message**
- **Flag with SCL** (Spam Confidence Level)

SCL

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

Then, the administrator will establish the action to be taken on each message based on the threshold set in Active Directory.

10.9.2 Allowed addresses and domains

This is a whitelist of trusted email addresses and domains whose messages won't be scanned by the anti-spam protection.

If you want to specify more than one address/domain, separate them with ",".

10.9.3 Spam addresses and domains

This is a blacklist of email addresses and domains whose messages will be intercepted and deleted by the protection.

Keep in mind the following aspects when configuring these lists:

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

10.10. Content Filtering for Exchange servers



Feature only available in Endpoint Protection Plus.

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

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

You can also filter email attachments with double extensions.

- **Action to take:** select whether you want to delete files with dangerous attachments or move them to a specific folder. This can be very helpful if you want to analyze those files at a later stage.
- **Consider attachments with the following extensions dangerous:** enter the extensions of those files you want to consider dangerous. You can use the **Add**, **Delete**, **Clear** and **Restore** buttons to configure the list to your needs.
- **Consider attachments with double extensions dangerous, except for the following:** select this option to block all messages containing files with double extensions, except for the ones you allow. Use the **Add**, **Delete**, **Clear** and **Restore** buttons to configure the list of double extensions to allow.

Detection log

All detections that take place on an Exchange server are logged locally in a CSV file. This allows network administrators to obtain additional information when a message does not reach the intended recipient.

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

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

The CSV file contains the following fields arranged in a tabular form:

- **Date:** date when the message arrived at the Exchange server.
- **From**
- **To**
- **Subject**
- **Attachments:** list of message attachments.
- **Protection**
- **Action**

11. Android security settings

Settings for Android devices
Updates
Antivirus

11.1. Introduction

Endpoint Protection / Plus's Settings menu provides the parameters required to configure the security settings for smartphones and tablets. Click the **Android devices** panel on the left-hand menu to display a list of the security configurations already created.

This chapter explains the available security settings for Android devices, and gives recommendations to protect smartphones and tablets.

11.2. Introduction to the security settings for Android devices

The settings options for Android devices are divided into three sections. Click each of them to display a drop-down menu with the associated options. Below we offer a brief explanation of each section:

- **Updates:** lets you define the type of connection to be used by the device to download updates from Panda Security's cloud.
- **Antivirus:** lets you configure the antivirus protection.
- **Anti-Theft:** lets you enable or disable the anti-theft features included in **Endpoint Protection / Plus**.

11.3. Updates

The update options are described in chapter 12 Software updates.

11.4. Antivirus

The antivirus protection for Android devices protects smartphones and tablets against the installation of malware-infected apps and PUPs, scanning both your devices and their SD memory cards on access and on demand.

Select the **Enable permanent antivirus protection** checkbox to enable malware detection.

Exclusions

The Android protection allows you to exclude any of the installed apps from the scans. To do that, enter the names of the packages to exclude, separated with commas.

To look up an app's package name, find the app in the Google Play app store using a Web browser. The package name will be listed at the end of the URL after the '?id='.

12. Software updates

- Protection engine updates
- Communications agent updates
- Knowledge updates
- Update cache

12.1. Introduction

Endpoint Protection / Plus is a cloud-based managed service that doesn't require customers to update the back-end infrastructure that supports the protection service. However, it is necessary to update the software installed on the customer's computers.

The components installed on users' computers are the following:

- Panda communications agent
- **Endpoint Protection / Plus** protection engine
- Signature file for the traditional antivirus protection

The update procedure and options will vary depending on the operating system of the computer to update, as indicated in Table 14:

Module	Platform			
	Windows	Mac OS X	Linux	Android
Panda agent	On-demand			
Endpoint Protection / Plus protection	Configurable	Configurable	Configurable	No
Signature file	Enable/Disable	Enable/Disable	Enable/Disable	No

Table 14: update procedures based on platform and module

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

12.2. Configuring protection engine updates

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

12.2.1 Updates

To enable the automatic updates of the **Endpoint Protection / Plus** protection module, select the **Automatically update Aether on devices** checkbox. This will enable all other settings options on the screen. If that option is cleared, the protection module will never be updated.



It is not advisable to disable the protection engine updates. Computers with outdated protection will be more vulnerable to malware and advanced threats over time.

Running updates at specific time intervals

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

- Start time
- End time

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

Running updates on specific days

Use the drop-down menu to specify the day the update should be run:

- **Any day:** the updates will run when they are available.
- **Days of the week:** use the checkboxes to select the days of the week when the **Endpoint Protection / Plus** updates will run. If an update is available, it will run on the first day of the week that coincides with the administrator's selection.
- **Days of the month:** use the menus to set the days of the month when the **Endpoint Protection / Plus** updates will run. If an update is available, it will run on the first day of the month that coincides with the administrator's selection.
- **On the following days:** use the menus to set a specific date range for the **Endpoint Protection / Plus** updates. This option lets you select update intervals that won't be repeated over time. After the specific date, no updates will be run. This option forces the administrator to constantly establish a new update interval as soon as the previous one has expired.

Computer restart

Endpoint Protection / Plus lets you define a logic for computer restarts, if needed, by means of the drop-down menu at the bottom of the settings window:

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

12.3. Configuring communications agent updates

The Panda agent is updated on demand. **Endpoint Protection / Plus** will display a notification in the management console indicating the availability of a new agent version. From then on, the administrator will be able to launch the update whenever they want to.

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

12.4. Configuring knowledge updates

To configure **Endpoint Protection / Plus's** signature file updates, go to the security configuration profile assigned to the computer, depending on its type.

12.4.1 Windows, Linux and Mac devices

Go to **Settings**, and select **Workstations and servers** from the left-hand menu.

Go to **General**. There you will see the following options:

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



It is not advisable to disable the automatic knowledge updates. A computer with out-of-date protection will be more vulnerable to threats.

- **Run a background scan every time there is a knowledge update:** lets you automatically run a scan every time a signature file is downloaded onto the computer. These scans will have minimum priority so as not to interfere with the user's work.

12.4.2 Android devices

Go to **Settings**, and select **Android devices** from the left-hand menu.

Endpoint Protection / Plus lets you restrict software updates so that they don't consume mobile data.

Select this option to restrict updates to those occasions when there is an available Wi-Fi connection for your smartphone or tablet.

12.5. Update cache/repository

Endpoint Protection / Plus lets you designate one or more computers on the network with the cache role. These computers automatically download and store all files required so that other computers

with **Endpoint Protection / Plus** installed can update the signature file, the agent and the protection engine without having to access the Internet. This saves bandwidth, as computers will not have to independently download the updates.

12.5.1 Configuring a computer as a repository

- Click Settings, then Cache and Add cache computer.
- Select a computer from the list and click **OK**.

From then on, the selected computer will have the cache role and will start downloading all necessary files, keeping the repository synchronized automatically. The rest of the computers on the network will contact the cache computer for updates.

12.5.2 Requirements and limitations of computers with the cache role

- At most, 2 GB of additional disk space to store the downloads.
- The environment of the computer with the cache role is restricted to the network segment to which its network interface is connected. If a cache computer has several network interfaces, it can serve as a repository for each network segment to which it is connected.



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

- The other computers will automatically discover the presence of the cache node and will redirect their update requests.
- A protection license has to be assigned to the cache node in order for it to operate.
- The firewall settings must allow SSDP (uPnP) traffic on UDP port 21226.

12.5.3 Discovery of cache nodes

Computers designated with the cache role will broadcast to the network segments to which their interfaces connect at the time the new role is assigned. Network computers will receive the publication of the service and will connect to the most appropriate node based on the amount of free resources, should there be more than one designated cache node on the same network segment.

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

13. Tasks

Task creation
Task publication
Task management

13.1. Introduction

Tasks are a resource implemented in **Endpoint Protection / Plus** that allows administrators to launch security scans on computer groups on demand or scheduled for a specific date/time.

The process of launching a task is divided into three steps:



- **Task creation and configuration:** select the computers to be scanned, the characteristics of the scan task, the time/date, the scan frequency, and the way it will behave in the event of an error.
- **Task publication:** once you create a task, you must activate it by entering it in the **Endpoint Protection / Plus** task scheduler. Activated tasks will be run on the scheduled day/time.
- **Task execution:** the task will be run when the configured conditions are met.

13.2. Task creation

To create a task, click the **Tasks** menu at the top of the console. A window will appear where you will see all created tasks, and their status. To create a new task, click **Add** and select **Scheduled scan** from the drop-down menu. A window will be displayed with the task details, divided into four areas:

- **Overview:** task name and description.
- **Recipients:** computers that will receive the task.
- **Schedule:** task schedule (day and time).
- **Scan options:** on-demand scan parameters.

13.2.1 Task recipients

Click **Recipients**. A window will open for you to select the computers that will receive the configured task. Click  to add a new computer, and  to remove computers.



To access the computer selection window you must first save the task.

13.2.2 Task schedule and frequency

You can configure the following schedule options:

- **Starts:** indicates the task start time/date.
- **Maximum run time:** indicates the maximum time that the task can take to complete. After that time the task will be canceled if it is not completed.
- **Repeat:** indicates the frequency of the task from the time/date indicated in the **Starts** field.

Starts:

- **As soon as possible (enabled):** the task will be launched immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified if the computer is **turned off**.
- **As soon as possible (disabled):** the task will run on the date selected in the calendar. Specify whether to take into account the computer's local time or the **Endpoint Protection / Plus server time**.
- **If the computer is turned off:** if the computer is turned off or cannot be accessed, the task won't run. The task scheduler lets you establish the task's expiration date, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available).
- **Do not run:** the task is immediately canceled if the computer is not available at the scheduled time.
- **Run the task as soon as possible, within:** lets you define the time interval during which the task will be run if the computer becomes available.
- **Run when the computer is turned on:** there is no time limit. The system waits for the computer to be available to launch the task.

Maximum run time

- **No limit:** there is no time limit for the task to complete.
- **1, 2, 8 or 24 hours:** there is a time limit for the task to complete. After that time interval, the task will be canceled returning an error.
- **Repeat:** indicates a repeat interval (every day, month or day) from the date specified in the **Starts** field.

Scan options

The scan options let you configure the scan engine parameters in order to scan the computers' file system. The following options are available:

- **Scan type**
 - **The entire computer:** runs an in-depth scan of the computer, including every connected storage device.
 - **Critical areas:** quick scan of the following directories:
 - %WinDir%\system32
 - %WinDir%\SysWow64
 - Memory
 - Boot system
 - Cookies
 - **Specific items:** lets you enter the full path of massive storage devices. This option supports environment variables. The solution will scan the specified path and every folder and file it may contain.
- **Detect viruses:** detects programs that enter computers with malicious purposes. This option is always enabled.

- **Detect hacking tools and PUPs:** detects potentially unwanted programs, as well as programs that can be used by hackers to carry out actions that cause problems for the user of the affected computer.
- **Detect suspicious files:** in scheduled scans, the computer software is scanned statically, that is, running items are not scanned. Therefore it may be necessary to enable heuristic scanning algorithms to detect all types of threats.
- **Scan compressed files**
- **Exclude the following files from scans**
 - Do not scan files excluded from the permanent protections: the files whose execution was allowed by the administrator won't be scanned. These files will always run, along with any file globally excluded from the console.
 - Extensions
 - Files
 - Directories

13.3. Task publication

Once you have created and configured a task, it will be added to the list of configured tasks. However, the task will not be active until it is published. To publish a task, click the **Publish now** button.

As soon as you publish a task, it will be added to the **Endpoint Protection / Plus** task scheduler, which will launch the task based on its settings.

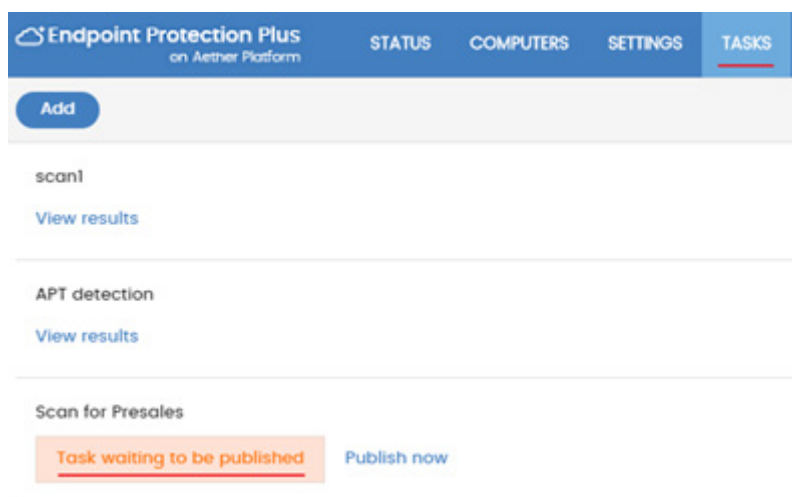


Figure 59: task publication

13.4. Task management

Administrators can delete, copy, cancel or view tasks by clicking the icons mentioned below.

Modifying a published task

Click a task's name to display its settings window. There you will be able to edit any of the task's settings.




You can only change the name and description of a published task. To modify a published task, you must copy it.

Canceling a published task

To cancel a published task, click the **Cancel** link. The task will be canceled, but it won't be deleted from the task window so you will still be able to view its results.


Deleting a task

Executed tasks are not deleted automatically. To delete them, you must click the  icon.



Deleting a task also deletes its results.

Copying tasks

Click a task's  icon to copy it. The new task will have the same settings as the original one.

Viewing a task's results

You can view the current results of any published task by clicking the **View results** link. A window with the results will appear, along with some filters for you to search for specific information.

Table 15 shows the fields in the task table:

Field	Comment	Values
Computer	Name of the computer where the scheduled scan took place	Character string
IP address	The computer's primary IP address	Character string
Status	<p>Pending: the task tried to launch the scan, but the target computer was not accessible. A wait period starts based on the task settings.</p> <p>In progress: the scan is underway</p> <p>Success: the scan finished successfully</p> <p>Failed: the scan failed, returning an error</p> <p>Expired: the task didn't even start as the configured period expired.</p> <p>Canceled: the task was manually canceled</p>	Character string

Field	Comment	Values
Start date	Scan start date	Date
End date	Scan end date	Date
Detections	Number of detections	Numeric value

Table 15: filtering parameters for task results

Table 16 displays the available search filters:

Field	Comment	Values
Date	Drop-down menu with the date when the task became 'Active' based on the configured schedule. An active task will launch a scan immediately, or wait until the target machine is available. This date is specified in the Date column.	Date
Detections	Lets you specify whether to display computers with detections or clean computers.	Binary value
Status	Pending: the task has not been run yet as the execution window has not been reached In progress: the scan is underway Success: the scan finished successfully Failed: the scan failed and returned an error Canceled (the task could not start at the scheduled time) Canceled: the task was manually canceled Canceled (maximum run time exceeded) Canceled	Enumeration

Table 16: task search filters

14. Malware and network visibility

- Overview of the Status menu
 - Available panels/widgets
 - Introduction to the lists
 - Available lists
 - Default lists

14.1. Introduction

Endpoint Protection / Plus offers administrators three large groups of tools for viewing the security status and the networks they manage:

- The dashboard, with real-time, up-to-date information.
- Custom lists showing incidents, detected malware and managed devices along with their status.
- Networks status reports with information collected and consolidated over time.



For information about the consolidated reports, see Chapter 18 Reports.

Visualization and monitoring tools determine in real time the network security status as well as the impact of any possible security breaches in order to facilitate the implementation of appropriate security measures.

14.2. Overview of the Status menu

The **Status** menu includes the main visualization tools and has several sections, which you can see below:



Figure 60: the Status window with the dashboard and access to the lists

Accessing the dashboard (1)

You can access the dashboard through the **Status** menu at the top of the screen. From the dashboard you can access different widgets, as well as the lists.

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

Time period selector (2)

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

- Last 24 h
- Last 7 days
- Last month
- Last year



Not all information panels offer information for the last year. Those that don't support this option have a notice at the top of the screen to this effect.

Dashboard selector (3)

- **Security**: security status of the IT network.
- **Web access and spam**: blocking and filtering of Internet contents and unsolicited email on Microsoft Exchange servers.
- **Licenses**: refer to chapter 5 for more information about license management.
- **Executive report**: refer to chapter 18 for more information about how to configure and generate reports.

This chapter deals with the resources provided in sections **Security** and **Web and spam access**.

My lists (4)

The lists are data tables with the information presented in the panels. This includes highly detailed information and has search tools to locate the information you need.

Information panels/widgets (5)

The dashboard has a series of widgets related to a specific aspect of network security.

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

All the graphs have a key explaining the meaning of the data, and have hotspots that can be selected to display lists with predefined filters.

THREATS DETECTED BY THE ANTIVIRUS

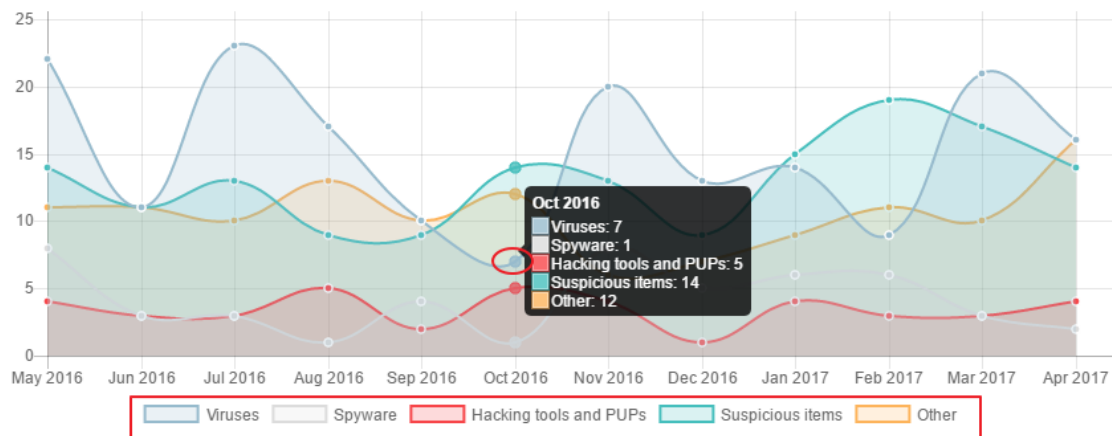


Figure 61: tooltips with detailed information and keys about the data shown

Endpoint Protection / Plus uses several types of graphs to display information in the most practical way based on the type of data displayed:

- Pie charts
- Histograms
- Bar charts

Click the items in the graphs to display more detailed lists.

14.3. Available panels/widgets

Below is a description of the different widgets displayed in the **Endpoint Protection / Plus** dashboard, their areas and hotspots, as well as their tooltips and their meaning.

14.3.1 Protection status

Protection status shows those computers where **Endpoint Protection / Plus** is working properly and those where there have been errors or problems installing or running the protection module. The status of the network computers is represented with a circle with different colors and associated counters.

The panel offers a graphical representation and percentage of those computers with the same status.



The sum of all computers can be more than 100% as the status types are not mutually exclusive.

PROTECTION STATUS



Figure 62: protection status' panel

- **Meaning of the different status types**

- **Properly protected:** indicates the percentage of computers where **Endpoint Protection / Plus** installed without errors and is working properly.
- **Installing:** this indicates the percentage of computers on which **Endpoint Protection / Plus** is currently being installed.
- **No license:** computers without a license are those that are not protected because there are insufficient licenses or because an available license has not been assigned to the computer.
- **Disabled protection:** these are computers that don't have the antivirus protection enabled.
- **Protection with errors:** this includes computers with **Endpoint Protection / Plus** installed, but for one reason or another the protection module is not responding to the requests from the Panda Security server.
- **Install error:** this indicates the computers on which the installation of the protection has not been properly completed.
- **Center:** the center of the pie chart indicates the total percentage of unprotected computers out of all of those visible to **Endpoint Protection / Plus**. For a computer to be visible it must have the Panda agent installed.

- Lists accessible from the panel

PROTECTION STATUS



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

Figure 63: hotspots in the Unprotected computers panel

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

- (1) Computer protection status list filtered by Protection status = Properly protected
- (2) Computer protection status list filtered by Protection status = Protection with errors
- (3) Computer protection status list filtered by Protection status = Installing
- (4) Computer protection status list filtered by Protection status = Disabled protection
- (5) Computer protection status list filtered by Protection status = No license
- (6) Computer protection status list filtered by Protection status = Install error
- (7) Computer protection status list without any filters

14.3.2 Offline computers

OFFLINE COMPUTERS

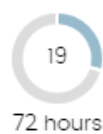


Figure 64: offline computers panel

Offline computers displays the computers that have not connected to the Panda Security cloud for a certain amount of time. Such computers are susceptible to security problems and require special attention from the administrator.

- **Meaning of the pie charts displayed**
 - **72 hours:** number of computers that have not reported their status in the last 72 hours.
 - **7 days:** number of computers that have not reported their status in the last 7 days.
 - **30 days:** number of computers that have not reported their status in the last 30 days.
- **Lists accessible from the panel**

OFFLINE COMPUTERS

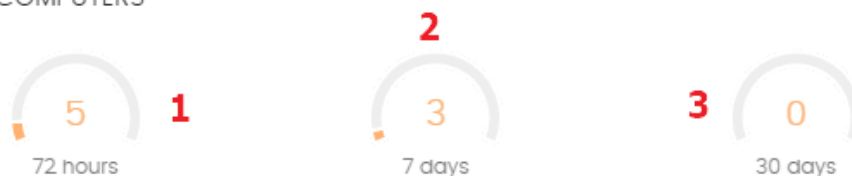


Figure 65: hotspots in the Offline computers panel

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

- (1) **Offline computers** list filtered by **Last connection** = More than 72 hours ago
- (2) **Offline computers** list filtered by **Last connection** = More than 7 days ago
- (3) **Offline computers** list filtered by **Last connection** = More than 30 days ago

14.3.3 Outdated protection

OUTDATED PROTECTION



Figure 66: outdated protection panel

Outdated protection displays the computers on which the latest version of the signature file is more than three days older than the latest one released by Panda Security. It also displays the computers on which the latest version of the antivirus engine is more than seven days older than the latest one released by Panda Security. Such computers are therefore vulnerable to attacks from threats.

- **Meaning of the bars**

The panel shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts:

- **Protection:** for at least seven days the computer has had a version of the antivirus engine older than the latest one released by Panda Security.
- **Knowledge:** it has been at least three days since the computer has updated the signature file.
- **Pending restart:** the computer requires a restart to complete the update.

- **Lists accessible from the panel**

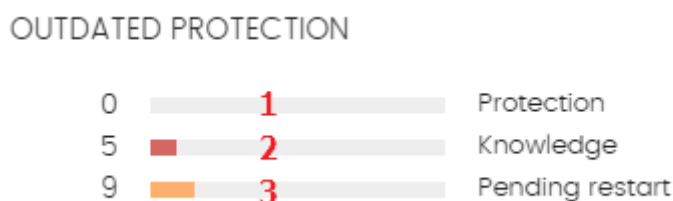


Figure 67: hotspots in the Outdated protection panel

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

- (1) Computer protection status list filtered by Updated protection = No
- (2) Computer protection status list filtered by Knowledge = No
- (3) Computer protection status list filtered by Updated protection = Pending restart

14.3.4 Threats allowed by the administrator

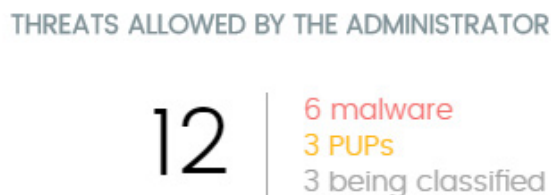


Figure 68: threats allowed by the administrator panel

Endpoint Protection / Plus automatically deletes or disinfects, if possible, all programs classified as malware.

If the administrator wants to allow the execution of an item already classified as a threat, **Endpoint Protection / Plus** has tools to restore deleted files.

- Meaning of the information displayed in the panel

The panel represents the total number of items excluded from blocking, broken down into three types:

- Malware
- PUP
- Being classified

- Lists accessible from the panel

THREATS ALLOWED BY THE ADMINISTRATOR



Figure 69: hotspots in the 'Threats allowed by the administrator' panel

- (1) Threats allowed by the administrator list with no filters
- (2) Threats allowed by the administrator list filtered by **Current classification** = Malware
- (3) Threats allowed by the administrator list filtered by **Current classification** = PUP
- (4) Threats allowed by the administrator list filtered by **Current classification** = Being classified (blocked and suspicious items)

14.3.5 Threats detected by the antivirus

THREATS DETECTED BY THE ANTIVIRUS

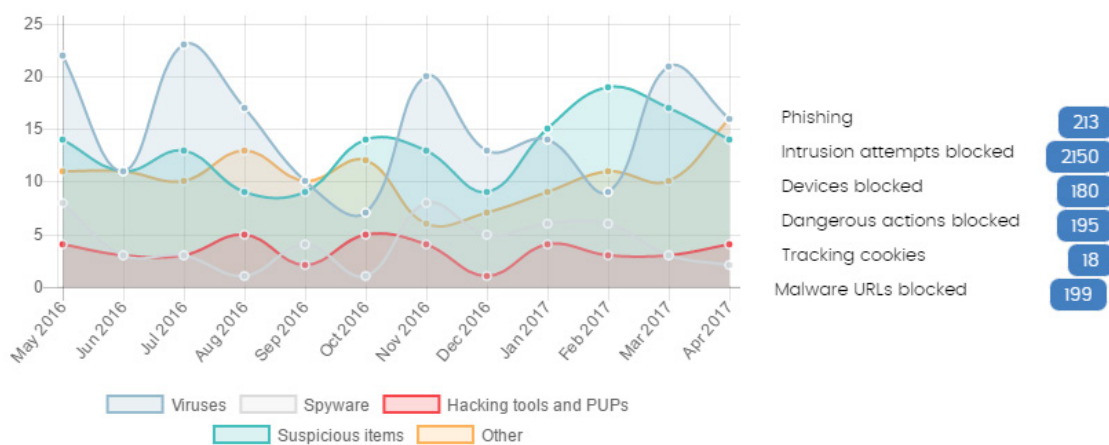


Figure 70: 'Threats detected by the antivirus' panel

Threats detected by the antivirus consolidates all the intrusion attempts that **Endpoint Protection / Plus** has dealt with in the selected time period.

The data covers all infection vectors and all supported platforms, so administrators are able to get specific data (volume, type, form of attack) related to the malware that reached the network during a selected period of time.

- **Meaning of the information displayed in the panel**

This panel comprises two sections: a line chart and a summarized list.

The line chart represents detections on the network over time, split into malware categories:

- **Viruses and spyware**
- **Hacking tools and PUPs**
- **Suspicious items**
- **Phishing**
- **Other**

The Y axis shows events and the X axis dates.

The list on the right shows the events that the administrator may want to review in order to look for symptoms or potentially dangerous situations.

- **Intrusion attempts blocked:** these are attacks that are blocked by the firewall and the intrusion prevention system.
- **Devices blocked:** peripheral devices blocked by the device control feature.
- **Dangerous operations blocked:** detections made by scanning local behavior.
- **Tracking cookies:** detection of cookies used to track users' Web activity.
- **Malware URLs blocked:** web addresses that lead to pages containing malware.

- **Lists accessible from the panel**

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

THREATS DETECTED BY THE ANTIVIRUS

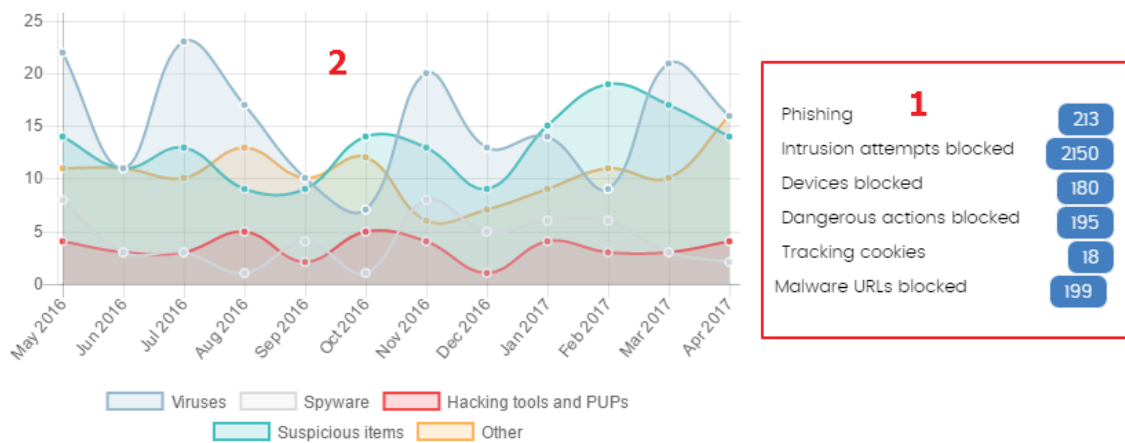


Figure 71: hotspots in the 'Threats detected by the antivirus' panel

- (1) Threats detected by the antivirus list filtered by Threat type = (Phishing OR Intrusion attempts blocked OR Devices blocked OR Dangerous operations blocked OR Tracking cookies OR Malware URLs).
- (2) Threats detected by the antivirus list with no filters.

14.3.6 Content filtering for Exchange servers



Feature only available in Endpoint Protection Plus.

CONTENT FILTERING FOR EXCHANGE SERVERS

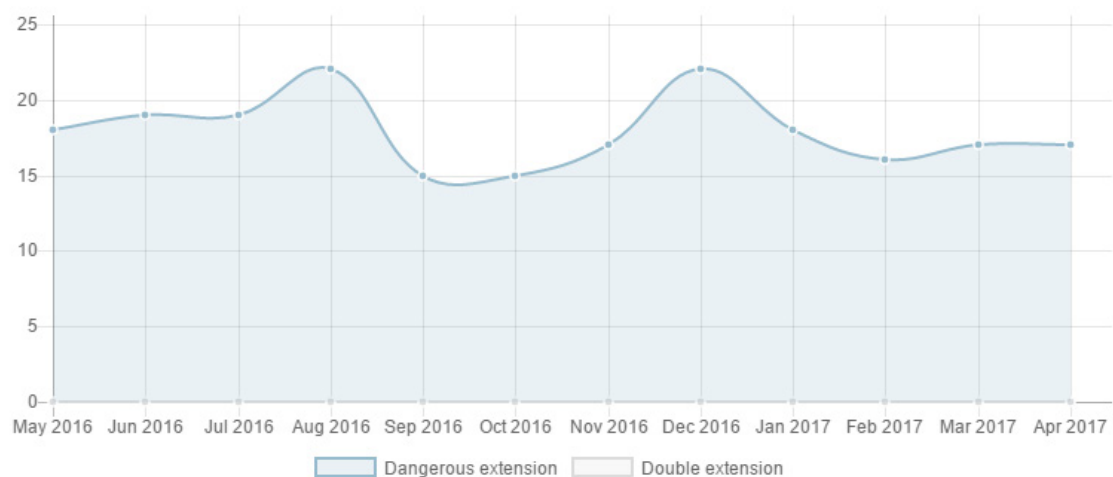


Figure 72: 'Content filtering for Exchange servers' panel

This panel shows the number of messages blocked by the Exchange Server content filter.

- **Meaning of the information displayed in the panel**

This shows two types of data: the number of messages filtered for having a dangerous extension, and for having a double extension.

Hover the mouse pointer over the chart to display a tooltip with the following information:

- **Dangerous extension:** the number of messages filtered for having an attachment with a dangerous extension.
- **Double extension:** the number of messages filtered for having an attachment with a double extension.

14.3.7 Web access



Feature only available in Endpoint Protection Plus.

WEB ACCESS

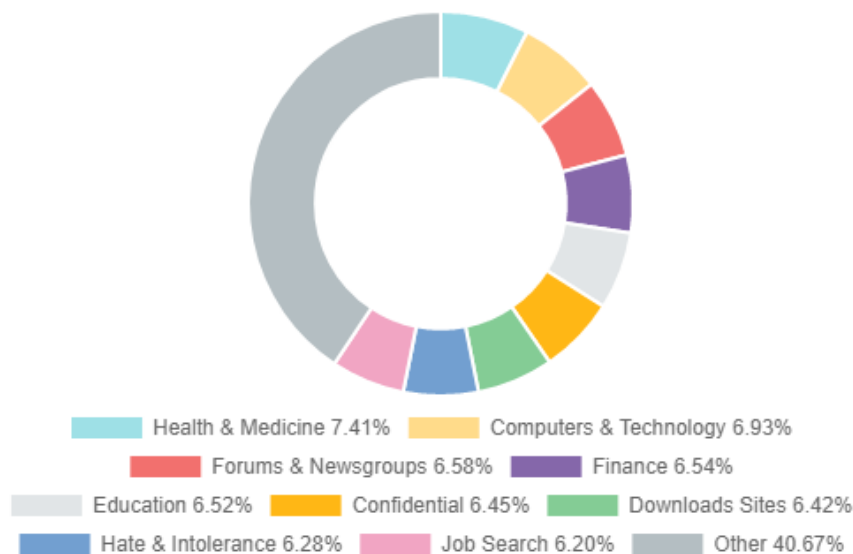


Figure 73: web access panel

This panel displays a pie chart with the different Web page categories requested by network users.

- **Meaning of the information displayed in the panel**

The pie chart shows the 10 most important Web page categories that **Endpoint Protection / Plus** identifies when categorizing the pages visited by network users:

- **Hate and intolerance**
- **Criminal activity**

- Job search
- Dating and personals
- Finance
- Confidential
- Entertainment
- Government
- Illegal drugs
- Other

The pie chart key shows the percentage of Web page requests for each category.

- Lists accessible from the panel

WEB ACCESS

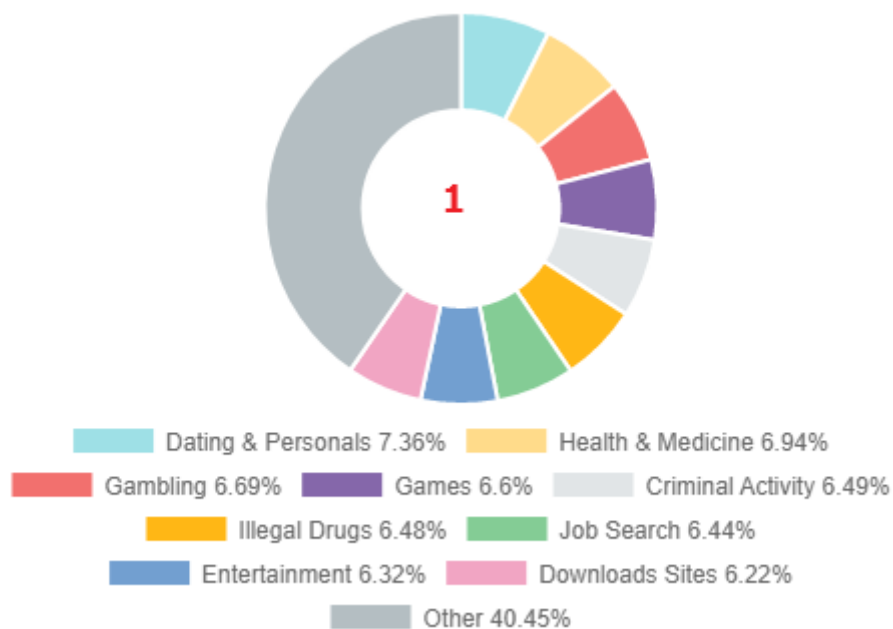


Figure 74: hotspots in the 'Web access' panel

- (1) Web access by computer list filtered by **Category** = Selected category

14.3.8 Top 10 most accessed categories



Feature only available in Endpoint Protection Plus.

Top 10 most accessed categories		
Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60
See full report		

Figure 75: most accessed categories panel

This displays the number of visits and the number of computers that have accessed the ten most visited Web page categories.

Each category gives the total number of visits in the selected date range, and the number of computers that have accessed one or more times.

- Lists accessible from the panel

Top 10 most accessed categories		
Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60
See full report		

Figure 76: hotspots in the 'Top ten most accessed categories' panel

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

- (1) Web access by computer list filtered by **Category** = Selected category
- (2) Web access by computer list with no filters

14.3.9 Top 10 most accessed categories by computer



Feature only available in Endpoint Protection Plus.

Top 10 most accessed categories by computer		
Computer	Category	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

[See full report](#)

Figure 77: 'Top 10 most accessed categories by computer' panel

This displays the number of Web page visits, ordered by category, of the ten computers that have used the Web most.

- Lists accessible from the panel

Top 10 most accessed categories by computer		
Computer 1	Category 2	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

[See full report](#)

Figure 78: hotspots in the 'Top 10 most accessed categories by computer' panel

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

- (1) Web access by computer list filtered by **Computer** = Selected computer
- (2) Web access by computer list filtered by **Category** = Selected category

14.3.10 Top 10 most blocked categories



Top 10 most blocked categories		
Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

[See full report](#)

Figure 79: top ten most blocked categories panel

This panel indicates the ten most frequently blocked Web page categories, along with the number of access attempts blocked, and the number of computers that attempted to access and were blocked.

- Lists accessible from the panel

Top 10 most blocked categories		
Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

[See full report](#)

Figure 80: hotspots in the 'Top 10 most blocked categories' panel

- (1) Web access by computer list filtered by Computer = Selected computer

14.3.11 Top ten most blocked categories by computer



Feature only available in Endpoint Protection Plus.

Top 10 most blocked categories by computer		
Computer	Category	Denied access attempts
TESTDEVICE_00_00	Games	194
TESTDEVICE_00_14	Entertainment	171
TestDevice_00_45	Entertainment	163
TESTDEVICE_00_28	Illegal Drugs	157
TestDevice_00_23	Downloads Sites	156
TestDevice_00_51	Job Search	156
TESTDEVICE_00_30	Health & Medicine	154
TestDevice_00_59	Computers & Technology	149
TESTDEVICE_00_48	Entertainment	147
TestDevice_00_31	Finance	146

[See full report](#)

Figure 81: top 10 most blocked categories by computer panel

This panel shows the computer-category combinations with the most Web page visits blocked, indicating the name of the computer, the category, and the number of access attempts denied for each computer-category combination.

- Lists accessible from the panel

Top 10 most blocked categories by computer		
Computer	Category	Denied access attempts
TESTDEVICE_00_00	Games	194
TESTDEVICE_00_14	Entertainment	171
TestDevice_00_45	Entertainment	163
TESTDEVICE_00_28	Illegal Drugs	157
TestDevice_00_23	Downloads Sites	156
TestDevice_00_51	Job Search	156
TESTDEVICE_00_30	Health & Medicine	154
TestDevice_00_59	Computers & Technology	149
TESTDEVICE_00_48	Entertainment	147
TestDevice_00_31	Finance	146

[See full report](#)

Figure 82: hotspots in the 'Top ten most blocked categories by computer' panel

- (1) Web access by computer list filtered by **Computer name** = Selected computer
- (2) Web access by computer list filtered by **Category** = Selected category

14.4. Introduction to the lists

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

14.4.1 Templates, settings and views

The **Endpoint Protection / Plus** lists are, in effect, *templates*, that allow one or more *settings*. A list can be thought of as the source of data about a specific area.

Settings are values specifically assigned to the search tools and filters associated to each template.

The *settings* of a *template* result in a list which the administrator can edit and consult later. This way, administrators can save time defining searches and filters about *Lists* which they can use again later.

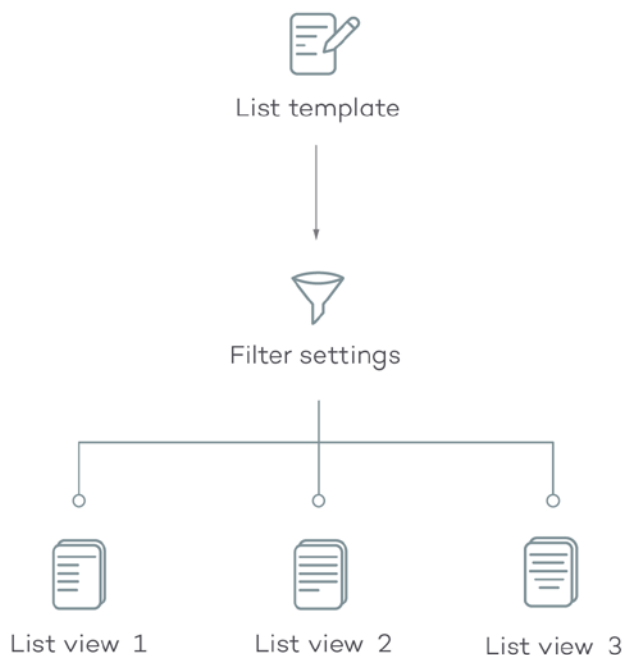


Figura 83: generating three lists from the same template/data source

List templates

There are 8 templates that correspond to the types of information displayed below:

- Threats detected by the antivirus
- Intrusion attempts blocked
- Devices blocked
- Access to Web pages by category (**Endpoint Protection Plus** only)
- Access to Web pages by computer (**Endpoint Protection Plus** only)
- Computer protection status
- Licenses
- Unmanaged computers discovered

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

Settings

In the context of lists, the settings represent a data filter specified by the administrator and associated to a template. Each template has different filters according to the type of data displayed.

Administrators can establish as many filter settings for a template as they wish, in order to enable different views of the same source of data.

Views of lists

The combination of a *template* and *settings* results in a specific view of the list. A template can have several associated views if the administrator has created various settings for the same template.

14.4.2 My lists panel

All created lists are displayed on the left-hand side panel **My lists**, on the **Status** main screen.

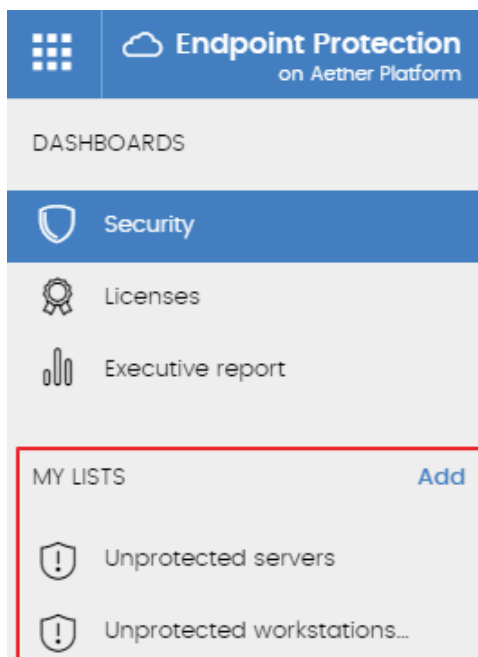


Figure 84: 'My lists' side panel

14.4.3 Creating custom lists

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

- **From the My lists side menu**

Click **Add** in the panel on the left to display a window with a drop-down menu with the eight available templates (Figure 86).

- **From a dashboard panel**

- Click a widget on the dashboard to open its associated template.
- Click its context menu **(6)** and select **Copy**. A new list will be created.
- Edit the list filters, name and description and click **Save (5)**.

Computer	Threat	Path	Status	Action	Date
Machine_Customer_1_014a	Malware Name 14	Malware Path Sample 14	●	Blocked	4/24/2017 2:18:00 AM
Machine_Customer_1_014a	Malware Name 12	Malware Path Sample 12	●	Blocked	4/24/2017 1:20:00 AM
Machine_Customer_1_014a	Malware Name 10	Malware Path Sample 10	●	Deleted	4/24/2017 12:22:00 AM

Figura 85: overview of a list

- From an existing list
 - You can copy an existing list by clicking its context menu (6) and clicking **Copy**.

Figura 86: available lists

- From the context menu of the My lists panel

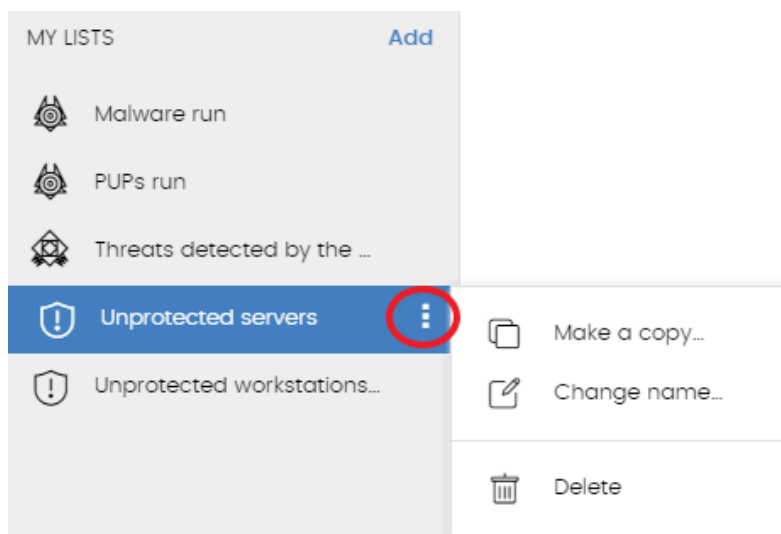



Figura 87: context menu of the lists available in the 'My lists' panel

- Click the context menu of the list you want to copy.
- Click Make a copy.
- A new view will be created which you can edit according to your preferences.


14.4.4 Deleting a list

There are two different ways to delete a list:

- From the My lists panel

- From the **My lists** panel, click the context menu of the list you want to delete.
- Click the  icon.

- From the list itself

- Click the list's context menu (6)
- Click the  icon from the drop-down menu displayed.

14.4.5 Configuring a custom list

To define a new list, follow the steps below:

- Assign a new name to the list (1). By default, the console creates a new name for the list by adding the string "New" to the type of list, or "Copy" if the list is a copy of a previous one.
- Assign a description (2): this step is optional.
- Click the link **Filters** (3) to display the settings and search section.

- Set the data filter **(4)** to display the relevant details.
- Click **Filter (7)** to apply the configured filter in order to check if it meets your needs. The search result will be displayed in the list **(8)**.
- Click **Save (5)**. The list will be added to the panel on the left under **My lists**, and can be accessed by clicking on the name.

Also, in the menu button **(6)** there is an option to export the list in CSV format and to make a copy of it.











Exporting a list in CSV format adds additional fields with respect to the list displayed in the Web console. These fields are documented later on in each list.

14.5. Available lists

14.5.1 Computer protection status list

This list displays all the network computers in detail, with filters that let you locate those workstations or mobile devices that are not protected due to one of the reasons displayed in the panel.

Field	Comments	Values
Computer	Name of the unprotected computer	Character string
Antivirus	Status of the antivirus protection	<div>  Not installed </div> <div>  Error </div> <div>  Enabled </div> <div>  Disabled </div> <div>  No license </div>
Updated protection	<p>This indicates whether the installed protection module has the latest version released.</p> <p>Hover the mouse pointer over the field to see the version of the protection installed.</p>	<div>  Updated </div> <div>  Not updated (7 days without updating since last release) </div> <div>  Pending restart </div>



Field	Comments	Values
Knowledge	This indicates whether the signature file installed on the computer is the latest version.	 Updated
	Hover the mouse pointer over the field to see the date of the latest version installed.	 Not updated (3 days without updating since last release)
Last connection	Date of the last time that the Endpoint Protection / Plus status was sent to the Panda Security cloud.	Date

Tabla 17: fields in the Computer protection status list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account of the service	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Computer name	Character string
IP address	Primary IP address of the computer	Character string
Domain	Windows domain to which the computer belongs	Character string
Description		Text
Group	Folder in the Endpoint Protection / Plus folder tree to which the computer belongs	Character string
Agent version		Character string
Installation date	Date on which the Endpoint Protection / Plus software was successfully installed on the computer	Date

Field	Comments	Values
Last update on	Date of the last update of the signature file	Date
Platform	Operating system installed on the computer	Windows Linux MacOS Android
Operating system	Operating system on the computer, internal version and patches applied	Character string
Exchange Server	Version of the mail server installed	Character string
Protection updated	Indicates whether the installed protection has the latest version released	Binary value
Protection version		Character string
Updated knowledge	Last version of the signature file downloaded on the device	Binary
Knowledge updated	Indicates whether the signature file installed on the computer is the latest version	Binary value
File antivirus Mail antivirus Web browsing antivirus Firewall protection Device control Exchange server antivirus Exchange server anti-spam Web access control	Status of the corresponding protection	Not installed Error Enabled Disabled No license

Table 18: fields of the 'Computer protection status' exported file

Filter tool

Field	Comments	Values
Computer type	Type of device	Workstation Laptop Mobile device Server
Find computer	Computer name	Character string
Last connection	The last time that the Endpoint Protection / Plus status was sent to the Panda Security cloud	All More than 72 hours More than 7 days More than 30 days
Updated protection	This indicates whether the installed protection module has the latest version released.	All Yes No Pending restart
Platform	Operating system installed on the computer.	All Windows Linux Mac Android
Knowledge	Update status of the signature file of the antivirus protection	Binary
Reason		Not installed Protection with errors Enabled Protection disabled No license No protection

Table 19: filter fields for the Computer protection status list

14.5.2 List of Threats allowed by the administrator

This list shows in detail all the items being classified or classified as threats which the administrator has allowed to be run.



This list can only be accessed from the Threats allowed by the administrator widget

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Type	Type of file	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware


Field	Comments	Values
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Allowed by	Console user that created the exclusion	Character string
Allowed since	Date that the administrator created the file exclusion	Date
Delete 	This lets you revoke the file exclusion	

Table 20: fields in the Threats allowed by the administrator list

Fields in the exported file

Fields	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Current type	Type of file at the time the list is accessed	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
Original type	Type of file at the time it was first allowed to be blocked	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Allowed by	Console user that created the exclusion	Character string
Allowed since	Date that the administrator created the file exclusion	Date

Table 21: fields in the 'Threats allowed by the administrator' exported file

Filter tool

Field	Comments	Values
Search	Threat: name of the malware or PUP Allowed by: console user that created	Character string

Field	Comments	Values
	the exclusion File: name of the file containing the threat Hash: string that identifies the file	
Current classification	File classification at the time the list is accessed	Malware PUP Goodware Being classified (Blocked and suspicious)
Original classification	File classification at the time it was first blocked	Malware PUP Blocked Suspicious

Table 22: filter fields in the Threats allowed by the administrator list

14.5.3 History of Threats allowed by the administrator list

This displays a history of all events that have taken place with respect to the threats and unknown files that the administrator has allowed to run.

This list doesn't have a corresponding panel in the dashboard. To access it, click the **History** link in the **Threats allowed by the administrator** window.

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Type	Type of threat allowed to run	Malware PUP Blocked Suspicious
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Action	Action taken on the allowed item	Exclusion removed by the user Exclusion removed after reclassification Exclusion added by the user Exclusion kept after reclassification
User	User account under which the relevant action was taken	Character string

Field	Comments	Values
Date	Date the event took place	Date

Table 23: fields in the History of threats allowed by the administrator list

Fields included in the exported file

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Current type	Type of threat the last time it was allowed to run.	Malware PUP Blocked Suspicious
Original type	File type when the event occurred.	
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Action	Action taken	Exclusion removed by the user Exclusion removed after reclassification Exclusion kept by the user Exclusion kept after reclassification
User	User account of the user that allowed the threat	Character string
Date	Date the event took place	Date

Table 24: fields in the History of threats allowed by the administrator list

Filter tool




Field	Comments	Values
Search	<p>User: user account of the user that allowed the threat</p> <p>File: name of the file containing the threat</p> <p>Hash: string identifying the file</p>	Character string

Field	Comments	Values
Current classification	File classification at the time the list is accessed	Malware PUP Goodware Being classified (Blocked and suspicious)
Original classification	File classification at the time it was first blocked	Malware PUP Blocked Suspicious
Action	Action taken on the allowed item	Exclusion removed by the user Exclusion removed after reclassification Exclusion kept by the user Exclusion kept after reclassification

Table 25: filter fields for the History of threats allowed by the administrator list

14.5.4 List of Threats detected by the antivirus

The list of detections offers consolidated and complete information about all the detections made on all supported platforms, and from all infection vectors scanned that are used by hackers to infect computers on the network.

Field	Comment	Values
Computer	Name of the computer on which the threat was detected	Character string
IP address	Primary IP address of the computer	Character string
Group	Group within the Endpoint Protection / Plus group tree that the computer belongs to	Character string  'All' group  Native group  Active Directory group
Path	File system path of the threat	Character string
Threat type	Type of threat detected	Virus Spyware PUPs and hacking tools Phishing Suspicious item Dangerous operation Tracking cookies Malware URLs Other

Field	Comment	Values
Action	Action taken by Endpoint Protection / Plus	Deleted Disinfected Quarantined Blocked Process terminated
Date	Date of detection	Date

Table 26: fields in the Threats detected by the antivirus list

Fields displayed in the exported file

Field	Comment	Values
Customer	Customer account to which the service belongs	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Name of the computer on which the file was detected	Character string
Malware name	Name of the threat detected	Character string
Threat type	Type of threat detected	Viruses Spyware Hacking tools and PUPs Phishing Suspicious items Dangerous actions blocked Tracking cookies Malware URLs Others
Malware type	Threat subclass	Character string
Number of detections	Number of times that Endpoint Protection / Plus detected the threat on the selected date	Number
Action	Action taken by Endpoint Protection / Plus	Deleted Blocked Process terminated
Detected by	Indicates the protection engine that made the detection	Antivirus: the threat was detected by the antivirus engine.
Detection path	File system path of the threat	Character string
Excluded	The threat has been excluded from scans by the administrator so it can be run	Binary

Field	Comment	Values
Date	Date of the detection	Date
Group	Group in the Endpoint Protection / Plus Group tree to which the computer belongs	Character string
IP address	Primary IP address of the computer where the detection was made	Character string
Domain	Windows domain to which the computer belongs	Character string
Description		Character string

Table 27: fields in the 'Threats detected by the antivirus' exported file

Filter tool

Field	Comments	Values
Search date type	Range: this lets you set the time period, from the current moment back Custom date: this lets you choose a specific date from a calendar	Last 24 hours Last 7 days Last month Last year
Computer type	Type of device	Workstation Laptop Mobile device Server
Threat type	Type of threat detected	Viruses Spyware Hacking tools and PUPs Phishing Suspicious items Dangerous actions blocked Tracking cookies Malware URLs Others
Computer	Name of the computer on which the file was detected	Character string

Tabla 28: filter fields in the Threats detected by the antivirus list

14.5.5 Web access by category list



Feature only available in Endpoint Protection Plus.

Field	Comments	Values
Category	Category that the Web page belongs to	List of all supported categories
Allowed access attempts	Number of visits allowed to the category specified in the Category field	Number
Allowed computers	Number of computers allowed to visit the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number
Denied computers	Number of computers denied to access the category specified in the Category field	Number

Table 29: fields in the Web access by category list

Fields in the exported file

Field	Comments	Values
Category	Category that the Web page belongs to	List of all supported categories
Allowed access attempts	Number of visits allowed to the category specified in the Category field	Number
Allowed computers	Number of computers allowed to visit the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number
Denied computers	Number of computers denied to access the category specified in the Category field	Number

Table 30: fields in the 'Web access by category' exported file

Filter tool

Field	Comments	Values
Search date type	<p>Range: this lets you set the time period, from the current moment back</p> <p>Custom date: this lets you choose a specific date from a calendar</p>	<p>Last 24 hours</p> <p>Last 7 days</p> <p>Last month</p> <p>Last year</p>

Field	Comments	Values
Category	Category that the Web page belongs to	List of all supported categories

Table 31: filter fields in the Web access by category list

14.5.6 Web access by computer list



Feature only available in Endpoint Protection Plus.

The Web access by computer list shows all the computers on the network and the visits allowed or denied to Web pages (sorted by category).

Field	Comments	Values
Computer	Name of the computer	Character string
IP address	Primary IP address of the computer	Character string
Category	Category that the Web page belongs to	List of the categories included
Group	Group within the Endpoint Protection / Plus group tree that the computer belongs to	Character string
Allowed access attempts	Number of visits allowed to the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number

Table 32: fields in the Web access by computer list

Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Group	Group within the Endpoint Protection / Plus group tree that the computer belongs to	Character string

Field	Comments	Values
Domain	Windows domain the computer belongs to	Character string
Computer	Name of the computer	Character string
IP address	Primary IP address of the computer	Character string
Category	Category that the Web page belongs to	List of the categories included
Allowed access attempts	Number of visits allowed to the category specified in the Category field	Number
Denied access attempts	Number of access attempts denied to the category specified in the Category field	Number
Description		Character string

Table 33: fields in the 'Web access by computer' exported file

Filter tool

Field	Comments	Values
Search date type	<p>Range: this lets you set the time period, from the current moment back</p> <p>Custom date: this lets you choose a specific date from a calendar</p>	<p>Last 24 hours</p> <p>Last 7 days</p> <p>Last month</p> <p>Last year</p>
Category	Category that the Web page belongs to	List of all supported categories
Computer type	Type of device	<p>Workstation</p> <p>Laptop</p> <p>Mobile device</p> <p>Server</p>
Computer	Name of the computer	Character string

Table 34: filter fields in the Web access by computer list

14.5.7 'Blocked devices' list

This list provides details of the network computers that have restricted access to peripherals.

Field	Comments	Values
Computer	Name of the computer	Character string




Field	Comments	Values
IP address	The computer's primary IP address	Character string
Group	Folder in the Endpoint Protection folder tree to which the computer belongs	Character string  'All' group  Native group  Active Directory group
Type	Type of device affected by the security settings	Removable storage drive Imaging device CD/DVD drive Bluetooth device Modem Mobile device
Action	Action taken on the device	Block Allow read access Allow read & write access
Date	Date and time when the action was taken	Date

Table 35: Fields in the 'Blocked devices' list

Fields displayed in the exported file

Fields	Comments	Values
Customer	Customer account that the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Mobile device Server
Computer	Computer name	Character string
Name	Name of the peripheral connected to the computer and affected by the security settings	Character string
Instance ID	ID of the affected device	Character string
Number of detections	Number of times a disallowed action has been detected on the device	Numeric value
Action	Action taken on the device	Block Allow read access Allow read & write access
Detected by	Module that detected the disallowed operation	Device Control
Date	Date when the disallowed operation was detected	Date

Fields	Comments	Values
Group	Folder in the Endpoint Protection folder tree to which the computer belongs	Character string
IP address	The computer's primary IP address	Character string
Domain	Windows domain the computer belongs to	Character string

Table 36: fields in the 'Blocked devices' exported file

Filter tool

Campo	Comentario	Valores
Computer type	Type of device	Workstation Laptop Mobile device Server
Find computer	Computer name	Character string
Search date type	<p>Range: lets you set the time period, from the current moment back</p> <p>Custom range: lets you choose a specific date from a calendar</p>	Last 24 hours Last 7 days Last month
Device type	Type of device affected by the security settings	Removable storage drive Imaging device CD/DVD drive Bluetooth device Modem Mobile device

Tabla 37: filters available in the 'Blocked devices' list

14.5.8 Licenses list

The **Licenses** list is covered in chapter 5 Licenses.

14.5.9 'Unmanaged computers discovered' list

The **Unmanaged computers discovered** list is covered in chapter 6.

14.6. Default lists

The management console includes two lists generated by default:

- Unprotected workstations and laptops
- Unprotected servers

Unprotected workstations and laptops

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

- Computers on which the **Endpoint Protection / Plus** software is currently being installed or that have an installation problem.
- Computers with the protection disabled or with errors.
- Computers without a license assigned or with expired licenses.

Unprotected servers

This list lets you locate all servers, regardless of the operating system installed, that may be vulnerable to threats due to a problem with the protection:

- Servers on which the **Endpoint Protection / Plus** software is currently being installed or that have an installation problem.
- Servers with the protection disabled or with errors.
- Servers without a license assigned or with expired licenses

15. Managing quarantined and excluded items

[Tools for managing excluded items](#)

[Excluding items](#)

[Managing excluded items](#)

[Quarantine management](#)

15.1. Introduction

Endpoint Protection / Plus provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This balance is achieved through the use of several configurable tools:

- Tools for managing the execution of processes classified as threats
- Tools for managing the backup/quarantine area

Considerations about managing processes classified as malware

In other cases, the administrator may want to allow the execution of certain types of malware which, despite posing a potential threat, provide features valued by users. This is the case of PUPs, for example. These include toolbars that offer search capabilities but also collect users' private data and confidential corporate information for advertising purposes.

Considerations about quarantine management

Finally, administrators may want to have access to items classified as threats and deleted from users' computers.

15.2. Tools for managing exclusions

Administrators can manage exclusions from different areas within the management console. Below we provide a reference guide to find these tools quickly.

All of these tools are accessible from the **Status (1)** menu at the top of the console. Click the relevant widget in the dashboard.

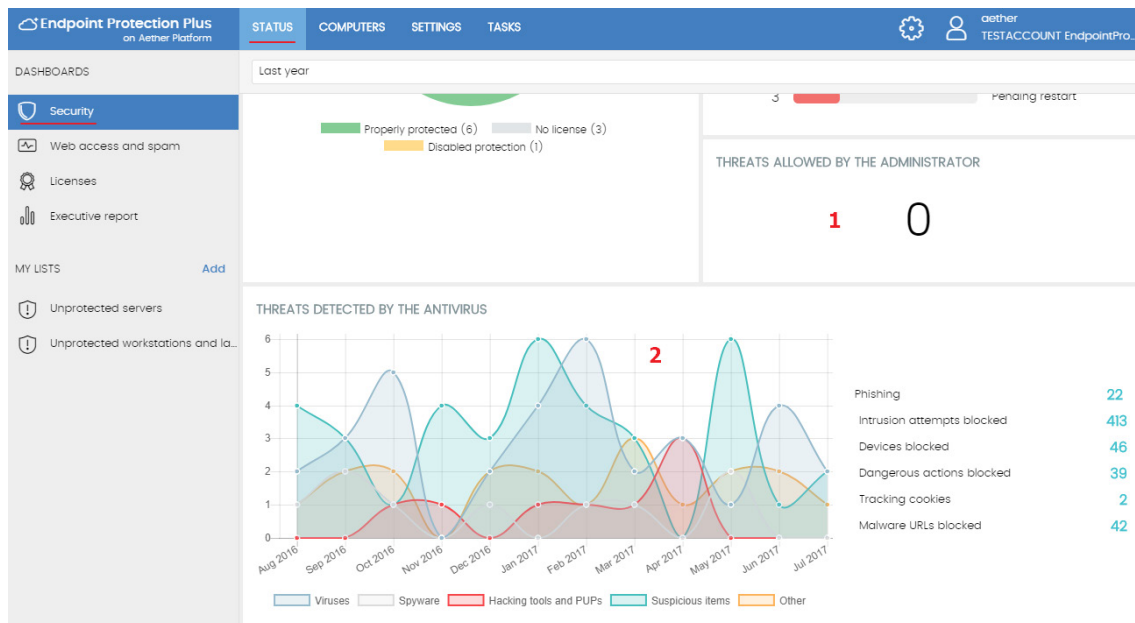



Figure 88: dashboard tools to manage exclusions

Lists

- **To get a list of currently excluded items:** go to the Threats allowed by the administrator panel (1).
- **To get a history of excluded items:** Go to the Threats allowed by the administrator panel (1), History context menu.
- **To see the state changes of excluded items:** go to the Threats allowed by the administrator panel (1), History context menu.

Adding and removing exclusions

- **To add a threat exclusion:** go to the Threats detected by the antivirus panel (2), select a threat, and click **Restore and do not detect again**.
- **To remove an exclusion:** Go to the Threats allowed by the administrator panel (1), select a threat and click the icon .

15.3. Excluding items

To allow the execution of a file classified as a threat, go to the **Threats detected by the antivirus** panel.

15.3.1 Excluding items classified as a threat

Excluding an item classified as malware from the scans is equivalent to allowing the execution of a program that **Endpoint Protection / Plus** has effectively classified as harmful or dangerous.

To do that, go to the **Threats detected by the antivirus** panel, select a threat and click the **Restore and do not detect again** button.

Go to the **Malware/PUP activity** panel, select a threat, and click the **Do not detect again** button to allow it to run.

Once excluded from the scans, the item in question will be added to the **Threats and other excluded items** list, as explained in the next section.

15.4. Managing excluded items

To manage excluded items, as well as to configure the solution's behavior when a suspicious item or a known classified item is reclassified, go to the **Threats allowed by the administrator** panel.

This panel lets you view and manage currently allowed files, as well as access a history of all excluded items.

List of currently excluded items

Threats allowed by the administrator displays items with an active exclusion. Every item on the list is allowed to run.

History

Click the context menu to display a history of all files excluded in **Endpoint Protection / Plus** and the actions taken on them. This list allows you to view all the states that a file has gone through (allowed or blocked), from the time it entered the **Threats allowed by the administrator** list until it exited it.

15.5. Managing the backup/quarantine area

Endpoint Protection / Plus's quarantine is a backup area that stores the items deleted after being classified as a threat.

Quarantined items are stored on each user's computer, in the Quarantine folder located in the software installation directory. This folder is encrypted and cannot be accessed by any other process. Thus, it is not possible to directly access or run any quarantined items, unless you do it using the Web console's restore tool.



The quarantine is compatible with Windows, Mac OS X and Linux. Android is not supported.

Endpoint Protection / Plus also quarantines suspicious files automatically, provided they meet the conditions established by Panda Security's PandaLabs department.

Once a suspicious item has been quarantined for further analysis, there are four possible scenarios:

- The item is classified as malicious but there is a disinfection routine for it: it is disinfected and restored to its original location.
- The item is classified as malicious, and there is no disinfection routine for it: it is quarantined for seven days.
- The item is identified as harmless: it is restored to its original location.
- Suspicious items are quarantined for a maximum of 30 days. If they finally turn out to be goodware, they are automatically restored to their original location.



Endpoint Protection / Plus doesn't delete files from users' computers. All removed files are actually sent to the backup area.

15.5.1 Viewing quarantined items

Administrators can view quarantined items through the **Threats detected by the antivirus** widget and list.

Use the filtering tools to view quarantined items (use the **Action** filter: "Quarantined" or "Deleted").

15.5.2 Restoring quarantined items

To restore a quarantined item, select it and click **Restore and do not detect again**. This will copy the item to its original location and restore its original permissions, owner, the registry keys associated with the file and any other information.

16. Remediation tools

Automatic computer disinfection
On-demand file scanning and disinfection
Computer restart
Reporting computer problems
External access to the console

16.1. Introduction

Endpoint Protection / Plus provides several remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle.

Some of these tools are automatic and don't require administrator intervention, whereas other require the execution of certain actions through the Web console.

The Table 38 illustrates the tools available for each platform and their type (manual or automatic).

Remediation tool	Platform	Type	Purpose
Automatic computer disinfection	Windows, Mac OS X, Linux 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 immediately or at scheduled times
On-demand restart	Windows	Manual	Forces a computer restart to apply updates, finish manual disinfection tasks and fix protection errors.

Table 38: endpoint Protection / Plus remediation tools

16.2. Automatic computer disinfection

Infected computers are disinfected automatically and in real time by the antivirus protection.

That is, upon detecting malware, **Endpoint Protection / Plus** will automatically clean the affected item provided there is a disinfection method available. Otherwise, the item will be quarantined.

Automatic disinfection does not require administrator intervention. However, the **File protection** checkbox must be selected in the security settings assigned to the computer.



Refer to chapter 10 Security settings for workstations and servers for more information about the block modes available in Endpoint Protection / Plus and the antivirus protection settings.

16.3. On-demand computer scanning and disinfection

There are two ways to scan and disinfect files on demand: one is to create a scheduled scan task and the other is to run an immediate scan.

16.3.1 Scheduled scan tasks

Scheduled scan tasks can be created in three different ways from the management console:

- From the **Tasks** menu at the top of the console
- From the **Computers** menu at the top of the console
- From a computer's **Details** tab



Refer to chapter 13 Tasks for more information about how to create a scheduled scan task from the Tasks menu.

Creating a scheduled scan task from the Computers menu

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- To schedule a task scan on a single computer, click the computer's context menu on the computer list (1).
- To schedule a task scan on multiple computers, use the checkboxes to select the computers to scan, and click the global context menu (2).
- Select the option **Schedule scan** from the drop-down menu.

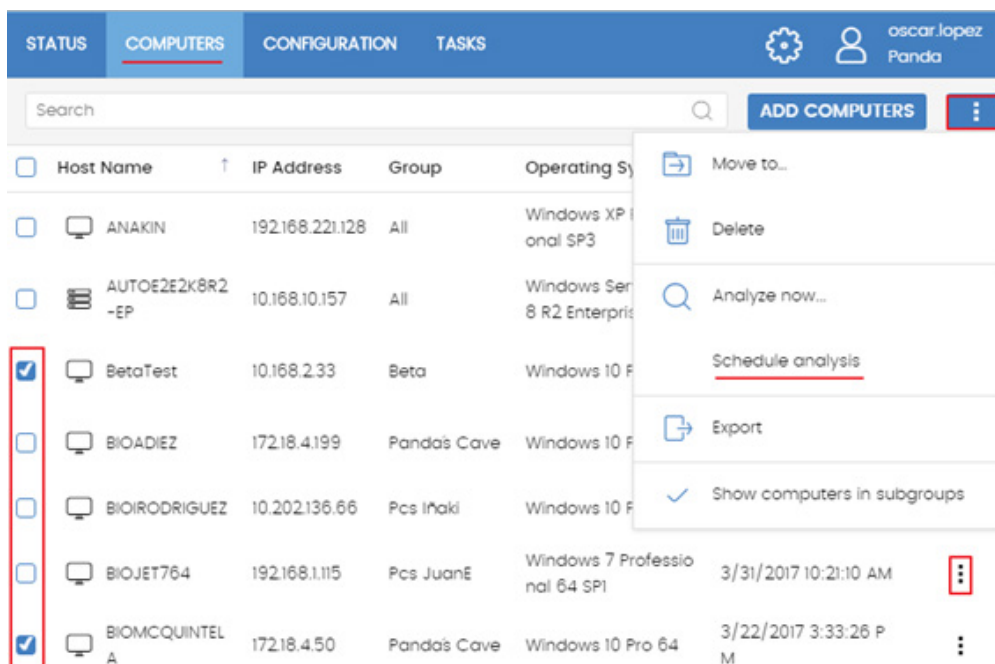


Figura 89: creating scheduled tasks from the Computers menu

Creating a scheduled scan task from a computer's Details screen

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- Click the computer to scan to view the **Details** screen.
- From the context menu, select **Schedule scan**.

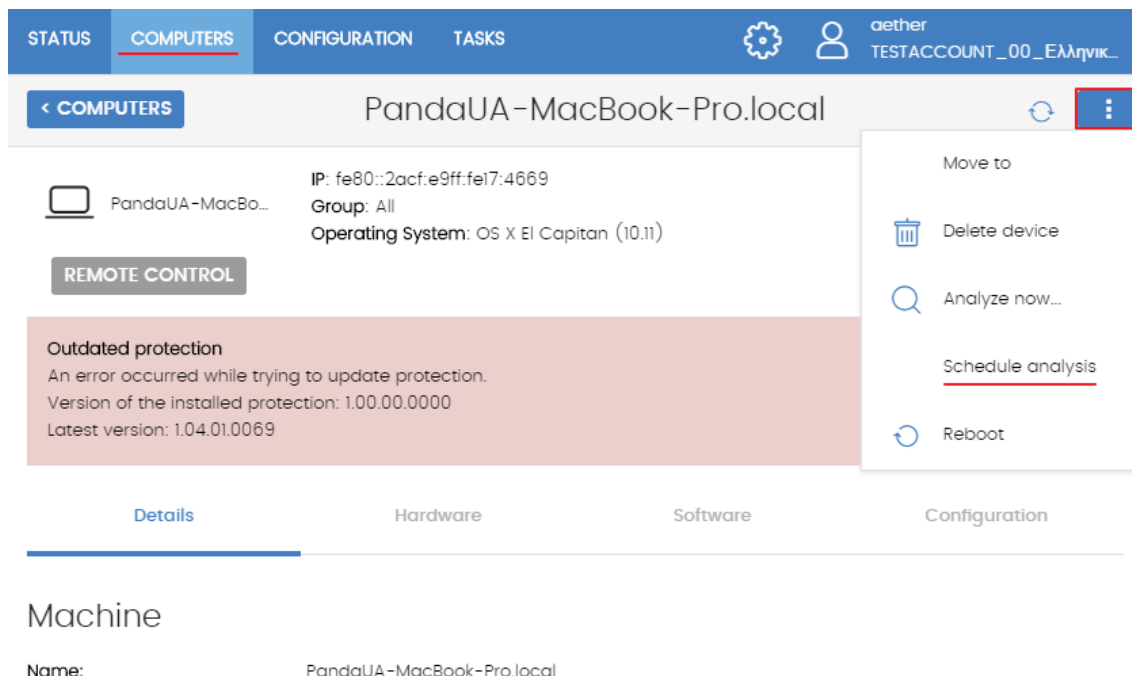


Figura 90: creating a scheduled scan from a computer's Details screen

16.3.2 Immediate scans

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- To launch an immediate scan on a single computer, click the computer's context menu on the computer list.
- To launch an immediate scan on multiple computers, use the checkboxes to select the computers to scan, and click the global context menu.
- From the drop-down menu, select the option **Scan now**.

16.4. Computer restart

The Web console lets administrators restart computers remotely. This is very helpful if you have computers whose protection needs updating or if there are protection problems to fix.

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- To restart a single computer, click the computer's context menu on the computer list.

- To restart multiple computers, use the checkboxes to select the computers to restart, and click the global context menu.
- From the drop-down menu, select **Restart**.

16.5. Reporting a problem

It is possible that the **Endpoint Protection / Plus** software may occasionally function incorrectly. Some symptoms could include:

- Errors reporting the computer status.
- Errors downloading knowledge or engine updates.
- Engine errors.

If **Endpoint Protection / Plus** functions incorrectly on some network computers, you can contact Panda Security's support department through the console and automatically send all the information required for diagnosis. To do this, click **Computers**, select the computers with errors, and click the context menu. A menu will appear entitled **Report a problem**.

16.6. Allowing external access to the Web console

If the administrator finds problems they can't resolve, they can grant Panda Security's support team access to their console. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- On the Users tab, click Allow the Panda Security S.L. team to access my console.

17. Alerts

Email alerts

17.1. Introduction

The alert system is a tool provided by **Endpoint Protection / Plus** to quickly notify administrators of important situations to ensure the proper operation of the security service.

Namely, an alert will be sent to the administrator every time one of the following events occur:

- There is a change in the license status
- There are install errors or a computer is unprotected

17.2. Email alerts

Email alerts are messages sent by **Endpoint Protection / Plus** to the administrator's email account. As previously explained, the system will send a message to the configured recipients' email accounts when certain events occur.

17.2.1 Configuring email alerts

Go to the **Settings** menu at the top of the Web console. Then click **Alerts** from the left-hand menu.

This screen lets administrators specify the email addresses to send messages to (**Send the alerts to the following address:**). You can also enable and disable each of the alert types to send.

17.2.2 Access permissions and alerts

Alerts are defined independently for each user of the Web console. The contents displayed in an alert will vary depending on the managed computers that are visible to the recipient's role.

17.2.3 Alert types

Protection and installation errors

These alerts have the following characteristics:

- An alert is generated for each unprotected computer found on the network
- An alert is generated for each computer with a protection or install error

The alert message will contain the following information:

- Name of the unprotected computer
- Group to which the computer belongs
- Computer information (name, description, operating system, IP address, group, Active Directory path, domain)

- Detection date and time (in UTC format)
- Reason: **protection with errors** or **Install error**.

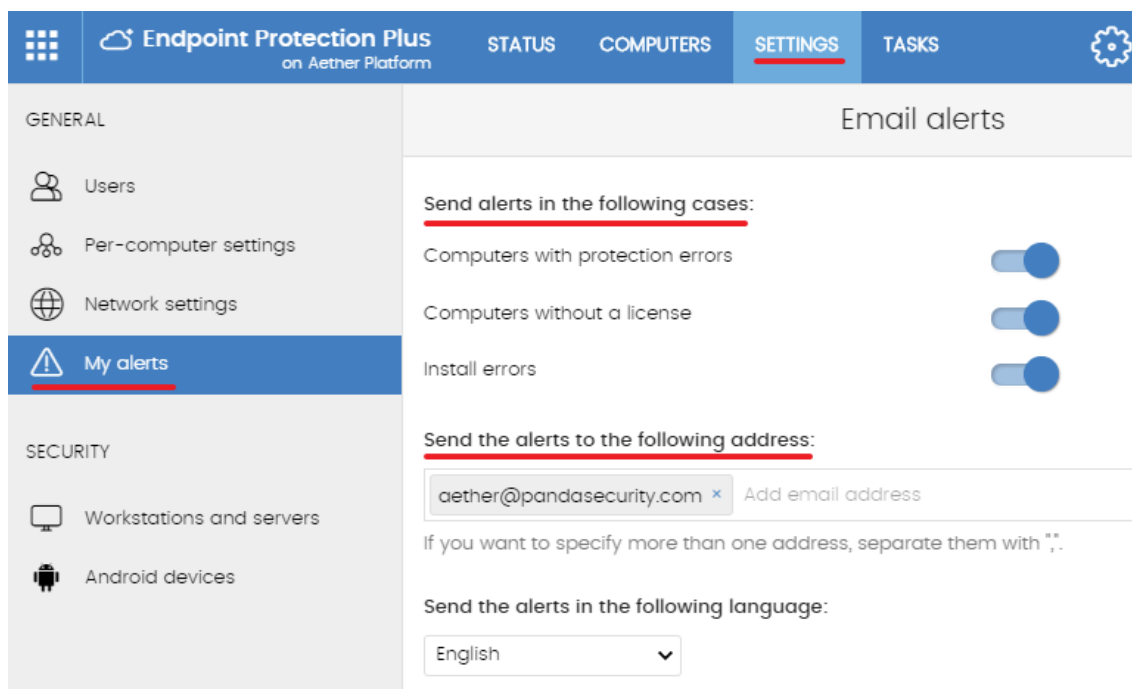


Figure 91: alert settings screen

Computers without a license

These alerts have the following characteristics:

- An alert is generated every time the solution fails to assign a license to a computer due to lack of sufficient free licenses

The alert message will contain the following information:

- Name of the unprotected computer
- Group to which the computer belongs
- Computer information (name, description, operating system, IP address, group, Active Directory path, domain)
- Detection date and time (in UTC format)
- Reason: **computer without a license**

Additionally, an alert will also be generated under the following circumstances:

- Every time a license contract expires

The alert message will contain the following information:

- Number of computers that are left without a license
- Number of expired licenses
- Product whose licenses have expired
- License contract expiration date

18. Reports

Roles and report generation

On-demand generation of executive reports

Scheduled sending of executive reports

18.1. Introduction

Endpoint Protection / Plus allows administrators to generate and send, automatically or manually, executive reports that consolidate all the information collected by the solution in the selected period.

18.2. On-demand generation of executive reports

Go to the **Status** menu at the top of the console, and click the **Executive report** option from the left-hand menu. This will open the report settings window. This window is divided into two tabs: **view** and **Schedule**. Click the **View** tab to configure the executive report to display.

18.2.1 Information required to generate an on-demand report

The following information will be required:

- **Information for the following dates:** specify the time interval to be covered by the report
 - **Last month**
 - **Last 7 days**
 - **Last 24 hours**
- **Information for the following computers:** specify the computers to extract information from
 - **All computers**
 - **Selected computers:** displays the group tree. Use the checkboxes to select the groups you want.
- **Include the following content:** lets you select the type of information to be included in the report.
 - **License status:** shows the number of contracted and used licenses. For more information, refer to chapter 5 Licenses.
 - **Network status:** shows the way the **Endpoint Protection / Plus** software is working on those computers where it is installed. It includes information from the following dashboard widgets: **unprotected computers** and **Outdated protection**.
 - **Detections:** shows all threats detected across the network. It includes information from the following dashboard widgets: **threats detected by the antivirus** and **Content filtering for Exchange servers (Endpoint Protection Plus only)**.
 - **Web access and spam (Endpoint Protection Plus only):** shows the users' Internet activity. It includes information from the following dashboard widgets: **web access**, **Top 10 most accessed categories**, **Top 10 most accessed categories by computer**, **Top 10 most blocked categories**, **Top 10 most blocked categories by computer** and **Spam detected on Exchange servers**.

Once you have finished configuring the settings, click the **View** button to display the report in a new window.




Check that neither your Internet browser nor any installed extension blocks the display of pop-ups.

18.3. Scheduled sending of executive reports

Go to the **Status** menu at the top of the console, and click the **Executive report** option from the left-hand menu. This will open the report settings window. This window is divided into two tabs: **view** and **Schedule**. Click the **Schedule** tab to configure a scheduled executive report.

18.3.1 Information required to generate a scheduled report

The scheduled reports window displays a list of all configured reports. Click **Add** to add a new scheduled report. To delete a configured report, click the  icon. To edit a configured report, click its name.

To configure a scheduled report, enter the following information:

- **Name:** name of the scheduled report that will be displayed on the list of configured reports.
- **Send automatically:** lets you schedule the sending of the executive report, or save the settings without sending the report.
- **Date and frequency:** lets you specify the day when the report will be sent and its frequency. Select **Every day**, **Every week** or **Every month**. The content of the drop-down menus will vary depending on your selection.
- **The following information:** this section displays the following settings: **dates**, **Computers** and **Content**. Click the arrow to the right to configure the following options:
 - **Information for the following dates:** specify the time interval to be covered by the report
 - **Last month**
 - **Last 7 days**
 - **Last 24 hours**
 - **Information for the following computers:** specify the computers to extract information from
 - **All computers**
 - **Selected computers:** displays the group tree. Use the checkboxes to select the groups you want.
 - **Include the following content:** lets you select the type of information to be included in the report
 - **License status:** shows the number of contracted and used licenses. For more information, refer to chapter 5 Licenses.
 - **Network status:** shows the way the **Endpoint Protection / Plus** software is working on those computers where it is installed. It includes information from the following dashboard widgets: **unprotected computers** and **Outdated protection**.

- **Detections:** shows all threats detected across the network. It includes information from the following dashboard widgets **Threats detected by the antivirus** and **Content filtering for Exchange servers (Endpoint Protection Plus only)**. Refer to chapter 14 Malware and network visibility for more information.
 - **Web access and spam (Endpoint Protection Plus only):** shows the users' Internet activity. It includes information from the following dashboard widgets: web access, Top 10 most accessed categories, Top 10 most accessed categories by computer, Top 10 most blocked categories, Top 10 most blocked categories by computer and Spam detected on Exchange servers.
- **To:** enter the email address that the report will be sent to. You can enter multiple addresses separated by commas.
 - **CC:**
 - **BCC:** use this field to send a copy of the report to a recipient without notifying other recipients that this was done.
 - **Subject:** specify the email subject line.
 - **Format:** select the format of the email attachment (the report): PDF, Excel, or Word.
 - **Language:** select the language of the report.

19. Controlling and monitoring the management console

What is a user account?

What is a role?

What is a permission?

Accessing the user account and role settings

Creating and configuring user accounts

Creating and configuring roles

Activity log

19.1. Introduction

This chapter describes the resources implemented in **Endpoint Protection / Plus** to control and monitor the actions taken by the network administrators that access the Web management console.

These resources are as follows:

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

19.2. What is a user account?

A user account is a resource managed by **Endpoint Protection / Plus**, comprising a set of information that the system uses to regulate administrator access to the Web console and define the actions that administrators can take on users' computers.

User accounts are only used by the administrators that access the **Endpoint Protection / Plus** console. In general, each administrator will have a unique personal account, and it is possible to create as many accounts as necessary.



Unlike the rest of this manual, where the word "user" refers to the person that uses a computer or device, in this chapter "user" refers to the account used by the administrator to access the Web console

19.2.1 User account structure

A user account comprises the following items:

- **Account login name:** this is assigned when the account is created and the aim is to identify the administrator accessing the account.
- **Account password:** this is assigned once the account is created and is designed to control access to the account.
- **Assigned role:** this can be selected once the user account is created. It lets you determine which computers the account user will be able to manage and the action they will be able to take.

19.2.2 What is the main user?

The main user is the user account provided by Panda Security to the customer when providing the **Endpoint Protection / Plus** service. This account has the **Full control** role, which is explained below.

The settings of the main user cannot be edited or deleted.

19.3. What is a role?

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

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

19.3.1 Role structure

A role is made up of the following:

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

19.3.2 Why are roles necessary?

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

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

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

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

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

Depending on its purpose, a computer may be assigned to a technician specialized in this field. For example, Exchange mail servers may be assigned to a group of specialized technicians, and other systems, such as Android devices, may not be visible to this group of technicians.

- The knowledge or expertise of the technician.

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

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

19.3.3 Full Control role

The **Endpoint Protection / Plus** license comes with the **Full Control** role predefined. The default administration account belongs to this role, and with this it is possible to take almost all actions that are available in the console.

The **Full Control** role cannot be deleted, edited or viewed, and any user account can belong to this role if it is assigned through the console.

19.3.4 Monitoring role

The **Monitoring role** is especially designed for network administrators responsible for monitoring networks, but without sufficient permissions to take actions such as editing settings or launching on-demand scans.

The permissions enabled in the **Monitoring Role** are as follows:

- View security settings for workstations and servers
- View security settings for Android devices
- View detections and threats
- View access to Web pages and spam (**Endpoint Protection Plus** only).
- Access to advanced reports

19.4. What is a permission?

A permission regulates access to a particular aspect of the management console. There are 15 types of permissions that provide access to many aspects of the **Endpoint Protection / Plus** console. A specific configuration from all available permissions generates a role, which can be assigned to one or more user accounts.

The **Endpoint Protection / Plus** permissions are as follows:

- Manage users and roles
- Assign licenses
- Modify computer tree
- Add, discover and delete computers
- Configure proxies and language
- Modify per-computer settings (updates, passwords, etc.)
- Restart computers
- Configure security settings for workstations and servers
- View security settings for workstations and servers
- Configure security settings for Android devices
- View security settings for Android devices
- View detections and threats
- View access to Web pages and spam (**Endpoint Protection Plus** only)
- Launch scan and disinfection tasks
- Exclude threats temporarily (malware, PUPs and blocked items)

19.4.1 Understanding permissions

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

Manage users and roles

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

Assign licenses

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

Modify the computer tree

- **Enabled:** the account user has complete access to the Groups tree, and can create and delete groups, as well as move computers to groups that have been created.
- **Disabled:** the account user can view the Groups tree and the settings assigned to each group, but cannot create new groups or move computers. They can change the group settings, as this action is governed by the permissions **Configure security for workstations and servers**, or **Configure security for Android devices**.

Add and delete computers

- **Enabled:** the account user can distribute the installer to network computers and include computers with **Endpoint Protection / Plus** installed in the console. They can also delete computers from the console.
- **Disabled:** the account user cannot download the installer, nor distribute it to computers. They cannot delete computers from the console.

Add, discover and delete computers

- **Enabled:** the account user can distribute the installer to their network computers and integrate them into the **Endpoint Protection / Plus** console. They can also delete computers from the console and configure all aspects related to the discovery of unmanaged computers: assign and revoke the 'discovery computer' role, edit discovery settings, launch an immediate discovery task, and install the Panda agent remotely from the list of discovery computers.
- **Disabled:** the account user cannot download the installer, nor distribute it to computers. They cannot delete computers from the console or access the computer discovery feature.

Configure proxies and languages

- **Enabled:** the account user can create new **Proxy and language** settings, edit or delete existing ones and assign them to computers in the console.
- **Disabled:** the account user cannot create new **Proxy and language** settings, nor edit or delete existing ones.



Given that moving a computer in the Groups tree can change the assigned Proxy and language settings, when you disable Configure Proxies and languages you also have to disable the permission Modify Groups tree.

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

- **Enabled:** the account user can create new **Per-computer settings**, edit or delete existing ones and assign them to computers in the console.
- **Disabled:** the account user cannot create new **Per-computer settings**, nor edit or delete existing ones.



Given that moving a computer in the Groups tree can change the assigned Per-computer settings, when you disable Modify per-computer settings you also have to disable the permission Modify Groups tree.

Restart computers

- **Enabled:** the account user can restart computers by going to the **Computers** menu and selecting **Restart** from the context menu (Windows workstations and servers, Linux and MacOS).
- **Disabled:** the account user cannot restart computers.

Configure security settings for workstations and servers

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



Given that moving a computer in the Groups tree can change the assigned Workstations and servers settings, when you disable Configure security for workstations and servers you also have to disable the permission Modify Groups tree.

When you disable this permission, you will see the permission **View security settings for workstations and servers**.

View security settings for workstations and servers



This permission can only be accessed when you disable Configure security for Workstations and servers.

- **Enabled:** the account user can only see the security settings created as well as the settings of a computer or group.
- **Disabled:** the account user won't be able to see the security settings created nor access the settings assigned to each computer.

Configure security settings for Android devices

- **Enabled:** the user account can create, edit, delete and assign settings for Android devices.
- **Disabled:** the user account will not be able to create, edit, delete or assign settings for Android devices.



Given that moving a computer in the Groups tree can change the assigned Android device settings, when you disable Configure security for Android devices you also have to disable the permission Modify Groups tree.

When you disable this permission, you will see the permission **View security settings for Android devices**, which is explained below.

View security settings for Android devices



This permission can only be accessed when you disable the permission Configure security for Android devices.

- **Enabled:** the account user will be able to see the settings created for Android devices as well as the settings for a specific Android device or group.
- **Disabled:** the account user won't be able to see the settings created for Android devices nor the settings for a specific Android device or group.

View detections and threats

- **Enabled:** the account user will be able to see the panels and lists in the **Security** section of the **Status** menu, and create new lists with custom filters.
- **Disabled:** the account user won't be able to see the panels and lists in the **Security** section of the **Status** menu, nor create new lists with custom filters.



Access to features related to excluding and unblocking threats and unknown items is determined through the permission Exclude threats temporarily (Malware, PUPs and blocked items).

View access to Web pages and spam



Feature only available in Endpoint Protection Plus.

- **Enabled:** the account user will be able to access the panels and lists in the **Web access and spam** section of the **Status** menu.
- **Disabled:** the account user won't be able to access the panels and lists in the **Web access and spam** section of the **Status** menu.

Launch scan and disinfection tasks

- **Enabled:** the account user will be able to create, edit and delete scan tasks.
- **Disabled:** the account user won't be able to create, edit or delete scan tasks. They will only be able to list the tasks and view the settings.

Exclude threats temporarily (Malware, PUPs and blocked items)

- **Enabled:** the account user can restore and prevent the detection of known classified threats. Similarly, they can also choose to stop allowing permitted threats.
- **Disabled:** the account user won't be able to restore known classified threats or stop allowing permitted threats.



It is necessary to enable View detections and threats in order to fully implement Exclude threats temporarily (Malware, PUPs, and blocked items).

19.5. Accessing the user account and role settings

In the **Settings** menu, when you click the **Users** panel, there are two sections associated with the management of roles and user accounts:

- **Users:** this lets you create new user accounts and define the roles they belong to.

- **Roles:** this lets you create and edit settings for accessing **Endpoint Protection / Plus** resources.

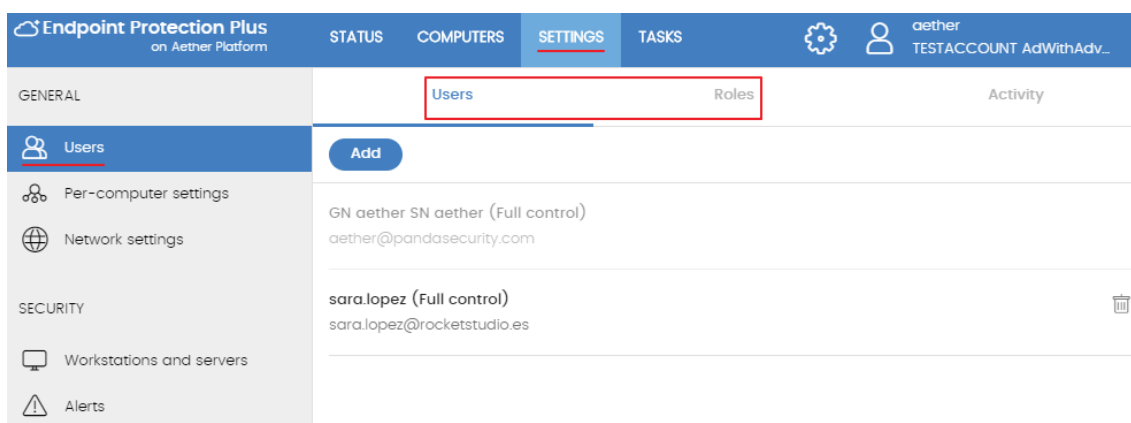



Figure 92: accessing the role and user settings

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

19.6. Creating and configuring user accounts



In the **Settings** menu, in the panel on the left, click **Users** and then the tab **Users** and you will be able to take all necessary actions related to the creation and editing of user accounts.

- **Add new user account:** click **Add** to add a new user, set the email account for accessing the account, the role to which it belongs, and a description of the account. The system will send an email to the account to generate the login password.
- **Edit a user account:** click the name of the user to display a window with all the account details that can be edited.
- **Delete or disable user accounts:** click the  icon of a user account to delete it. Click a user account and select the button **Block this user** to temporarily block access to the Web console from this account. If the account is currently logged in it will be blocked immediately.

19.7. Creating and configuring roles

In the **Settings** menu, click **Users** in the left-hand panel and then **Roles**, and you will be able to take all necessary actions related to the creation and editing of roles.

- **Add new role:** click **Add**. You will be asked for the name of the role, a description (optional), to select from the available computers, and a specific configuration of permissions.
- **Edit a role:** click the name of the role to display a window with all the settings that can be edited.

- **Copy a role:** click the  icon to display a window with a new role with exactly the same settings as the original one.
- **Delete role:** click the  icon of a role to delete it. If, when you delete a role, it already has user accounts assigned, the process of deleting it will be canceled.

19.8. User account activity log

Endpoint Protection / Plus logs every action taken by network administrators in the Web management console. This way, it is very easy to find out who made a certain change, when and on which object.

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

19.8.1 Action log

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

Fields displayed in the Actions list

Field	Comment	Values
Date	Date and time that the action was carried out	Date
User	User account that performed the action	Character string
Action	Type of action	Access Add scheduled report Assign license Block Delete Change 'Per-computer settings' Change 'Security settings' Change group Change parent group Change 'Proxy and language' Cancel Configure discovery Create Unassign license Stop allowing Unblock Discover now Designate cache computer Designate discovery computer Designate Panda proxy Edit Edit description Edit scheduled report

		Edit name Delete Delete scheduled report Inherit 'Per-computer settings' Inherit 'Security settings' Inherit 'Proxy and language' Install Locate Move to Active Directory path Move computers to their Active Directory path Hide Allow Publish Restart computers Restore communications Revoke cache computer Revoke discovery computer Revoke Panda proxy Sync group Make visible
Item type	Type of console object the action was performed on	Threat Settings Android device Computer Unmanaged computer Filter Group Device group Executive report Advanced reports List Preference for sending emails Role Task - Security scan User
Item	Console object the action was performed on	Character string

Table 39: fields in the Action log

Fields displayed in the exported file

Field	Comment	Values
Date	Date and time that the action was carried out	Date
User	User account that performed the action	Character string
Action	Type of action	Access Add scheduled report Assign license Block Delete Change 'Per-computer settings' Change 'Security settings' Change group Change parent group

Field	Comment	Values
		Change 'Proxy and language' Cancel Configure discovery Create Unassign license Stop allowing Unblock Discover now Designate cache computer Designate discovery computer Designate Panda proxy Edit Edit description Edit scheduled report Edit name Delete Delete scheduled report Inherit 'Per-computer settings' Inherit 'Security settings' Inherit 'Proxy and language' Install Locate Move to Active Directory path Move computers to their Active Directory path Hide Allow Publish Restart computers Restore communications Revoke cache computer Revoke discovery computer Revoke Panda proxy Sync group Make visible
Item type	Type of console object the action was performed on	Threat Settings Android device Computer Unmanaged computer Filter Group Device group Executive report Advanced reports List Preference for sending emails Role Task - Security scan User
Item	Console object the action was performed on	Character string

Table 40: fields in the 'Action log' exported file

Filter tool

Field	Comment	Values
From		Date
To		Date
Users		List of all user accounts that have been created in the management console

Table 41: filter fields in the Action log

19.8.2 Session log

The **Sessions** section displays a list of all accesses to the management console, and allows you to export the information to an Excel file and filter the information.

Fields displayed in the Sessions list

Field	Comment	Values
Date	Date and time that the access took place	Date
User	User account that accessed the console	Character string
Activity		Log in Log out
IP address	IP address from which the console was accessed	Character string

Table 42: fields in the Sessions list

Fields displayed in the exported file

Field	Comment	Values
Date	Date and time that the access took place	Date
User	User account that accessed the console	Character string
Activity		Log in Log out
IP address	IP address from which the console was accessed	Character string

Table 43: fields in the 'Sessions' exported file

Filter tool

Field	Comment	Values
From		Date
To		Date
Users		List of all user accounts that have been created in the management console

Table 44: filter fields in the Sessions list

20. Appendix 1: endpoint Protection / Plus requirements

Windows platforms
Windows Exchange platforms
MacOS platforms
Linux platforms
Android platforms
Web console access
Access to service URLs

20.1. Requirements for Windows platforms

20.1.1 Supported operating systems

Workstations

- Windows XP SP3 (32 bits)
- Windows Vista
- Windows 7
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)

Servers

- Windows 2003 (32-bit, 64-bit and R2) SP2 and later
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 and 2016

20.1.2 Hardware requirements

- Processor: pentium 1 GHz
- RAM: 1 GB
- Free space disk for the installation: 650 MB

20.2. Requirements for Windows Exchange platforms

20.2.1 Supported operating systems

- Exchange 2003: windows Server 2003 (32- bit) SP2+ and Windows Server 2003 R2 (32- bit)
- Exchange 2007: windows Server 2003 (64-bit) SP2+, Windows Server 2003 R2 (64-bit), Windows 2008 (64-bit) and Windows 2008 R2
- Exchange 2010: windows 2008 (64-bit) and Windows 2008 R2
- Exchange 2013: windows Server 2012 and Windows Server 2012 R2
- Exchange 2016: windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

20.2.2 Software and hardware requirements

The hardware requirements to install the protection on Exchange server are the ones determined by the Exchange server:

- Exchange 2003:

[http://technet.microsoft.com/en-us/library/cc164322\(v=exchg.65\).aspx](http://technet.microsoft.com/en-us/library/cc164322(v=exchg.65).aspx)

- Exchange 2007:

[http://technet.microsoft.com/en-us /library/aa996719\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us /library/aa996719(v=exchg.80).aspx)

- Exchange 2010:

[http://technet.microsoft.com/en-us /library/aa996719\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us /library/aa996719(v=exchg.141).aspx)

- Exchange 2013

[http://technet.microsoft.com/en-us /library/aa996719\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us /library/aa996719(v=exchg.150).aspx)

- Exchange 2016

[https://technet.microsoft.com/en-us /library/aa996719\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us /library/aa996719(v=exchg.160).aspx)

20.2.3 Supported Exchange versions

- Microsoft Exchange Server 2003 Standard and Enterprise (SP1/SP2)
- Microsoft Exchange Server 2007 Standard and Enterprise (SP0/SP1/SP2/SP3)
- Microsoft Exchange Server 2007 included in Windows SBS 2008
- Microsoft Exchange Server 2010 Standard and Enterprise (SP0/SP1/SP2)
- Microsoft Exchange Server 2010 included in Windows SBS 2011
- Microsoft Exchange Server 2013 Standard and Enterprise
- Microsoft Exchange Server 2016 Standard and Enterprise

20.3. Requirements for MacOS platforms

20.3.1 Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- MacOS 10.13 High Sierra

20.3.2 Hardware requirements

- **Processor:** Intel Core 2 Duo.
- **RAM:** 2 GB.
- **Free space disk for installation:** 400 MB.
- **Ports:** ports 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware and URL filtering to work.

20.4. Requirements for Linux platforms

20.4.1 Supported 64-bit distributions

- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS and 16.10
- Fedora 23, 24 and 25

20.4.2 Supported kernel version

From version 3.13 up to version 4.10

20.4.3 Supported file managers

- Nautilus
- PCManFM
- Dolphin

20.4.4 Hardware requirements

- **Processor:** pentium 1 GHz.
- **RAM:** 1.5 GB.
- **Free space disk for installation:** 100 MB.
- **Ports:** ports 3127, 3128, 3129 and 8310 must be accessible for the Web anti-malware and URL filtering to work

20.4.5 Installation package dependencies

debconf (>= 0.5) debconf-2.0	libfreetype6 (>= 2.3.5)	libpng12-0 (>= 1.2.13-4)	libxcb1
dkms (>= 1.95)	libgcc1 (>= 1:4.1.1)	libsm6, libssl1.0.0 (>= 1.0.0)	libxrender1
libc6 (>= 2.17)	libgl1-mesa-glx libgl1	libstdc++6 (>= 4.6)	make
libc6-dev	libice6 (>= 1:1.0.0)	libstdc++6:i386	notify-osd
libcurl3:i386	libltdl7 (>= 2.4.2)	libuuid1 (>= 2.16)	notification-daemon
libcups2	libnl-3-200 (>= 3.2.7)	libuuid1:i386	python-nautilus (>= 1.1-4)
libdbus-1-3 (>= 1.1.1)	libnl-genl-3-200 (>= 3.2.7)	libx11-6	zlib1g (>= 1:1.1.4)
libfontconfig1 (>= 2.9.0)	libnotify-bin (>= 0.7.6)	libx11-xcb1	

Table 45: required libraries for installation

20.5. Android platform requirements

20.5.1 Supported operating systems

- Ice Cream Sandwich 4.0

- Jelly Bean 4.1 - 4.2 - 4.3
- KitKat 4.4
- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0

20.5.2 Hardware requirements

A minimum of 10 MB of internal memory is required. Depending on the model, it is possible that the required space be larger.

20.5.3 Network requirements

For the push notifications to work correctly from the company's network, it is necessary to open ports 5228, 5229 and 5230 to the whole set of ASN 15169 IP addresses belonging to Google.

20.6. Web console access

The **Endpoint Protection / Plus** management console can be accessed with the latest version of the following compatible browsers.

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

20.7. Access to service URLs

In order to install and operate **Endpoint Protection / Plus** correctly, you need to allow access to the following URLs.

- https://*.pandasecurity.com
- http://*.pandasecurity.com
- https://*.windows.net
- <https://pandasecurity.logtrust.com>
- http://*.pandasoftware.com

Inbound and outbound traffic (anti-spam and URL filtering)

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

- <http://download.ctmail.com>

Ports

- Port 80 (HTTP, websocket)
- Port 443 (HTTPS)

21. Appendix 2: creating and managing a Panda Account

Creating a Panda Account
Activating your Panda Account

21.1. Introduction

A Panda Account provides administrators with a safer mechanism to register and access the Panda Security services purchased by the organization, than the old method of receiving the relevant access credentials by email.

With a Panda Account, it is the administrator who creates and activates the access credentials to the **Endpoint Protection / Plus** Web console.

21.2. Creating a Panda Account

Follow the steps below to create a Panda Account.

Open the email message received from Panda Security

- After purchasing **Endpoint Protection / Plus**, you will receive an email message from Panda Security.
- Click the link in the message to access a site from which you will be able to create your Panda Account.

Fill out the form

- Fill out the form with the relevant data.
- Use the drop-down menu in the bottom-right corner if you want to change the language of the form.
- You can view the license agreement and privacy policy by clicking the corresponding links.
- Click **Create** to receive a message at the email address entered in the form. Follow the instructions in that message to activate your account.

21.3. Activating your Panda Account

Once you have created your Panda Account you will need to activate it. You can do this through the email message that you will receive at the email address you specified when creating your Panda Account.

- Find the message in your Inbox.
- Click the activation button. By doing that you will validate the email address that you provided when creating your Panda Account. If the button doesn't work, copy and paste the URL included in the message into your browser.
- The first time that you access your Panda Account you will be asked to confirm your password. Then, click **Activate account**.
- Enter the required data and click **Save data**. If you prefer to enter your data later, click **Not now**.
- Accept the terms and conditions of the License Agreement and click **OK**.

Once your Panda Account has been successfully activated, you will be taken to the Panda Cloud site home page. There, you will be able to access your **Endpoint Protection / Plus** Web console. To do that, simply click the solution's icon in the **My Services** section.

22. Appendix 3: list of uninstallers

On installing **Endpoint Protection / Plus**, other security products might be detected on the computer. In that case, Table 45 shows the products that will be automatically uninstalled before installing **Endpoint Protection / Plus** across the network.

Vendor	Product name
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32bit- Edition) AVG Internet Security 2013 (64bit- Edition) AVG AntiVirus Business Edition 2013 (32bit- Edition) AVG AntiVirus Business Edition 2013 (64bit- Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32bits* AVG Internet Security Business Edition 2011 64bits (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVGFree v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir PersonalEdition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x
CA	CA Total Defense for Business Client V14 (32bit- Edition) CA Total Defense for Business Client V14 (64bit- Edition) CA Total Defense R12 Client (32bit- Edition) CA Total Defense R12 Client (64bit- Edition)
Bitdefender	BitDefender Endpoint Protection 6.x BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32 bits) Check Point Endpoint Security 8.x (64 bits)
Eset	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32 bits) ESET NOD32 Antivirus 4.X (32 bits) ESET NOD32 Antivirus 4.X (64 bits) ESET NOD32 Antivirus 5 (32 bits) ESET NOD32 Antivirus 5 (64 bits) ESET NOD32 Antivirus 6 (32 bits) ESET NOD32 Antivirus 6 (64 bits) ESET NOD32 Antivirus 7 (32 bits)

	ESET NOD32 Antivirus 7 (64 bits)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
iSheriff	iSheriff Endpoint Security 5.x
Kaspersky	Kaspersky Endpoint Security 10 for Windows (32bit- Edition) Kaspersky Endpoint Security 10 for Windows (64bit- Edition) Kaspersky Endpoint Security 8 for Windows (32bit- Edition) Kaspersky Endpoint Security 8 for Windows (64bit- 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 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee LiveSafe 2016 x86 / x64 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 (32bit- Edition) Norman Security Suite 10.x (64bit- Edition) Norman Security Suite 9.x (32bit- Edition) Norman Security Suite 9.x (64bit- 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	eScan Corporate for Windows 9.0.824.205

Technologies	
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 22.x Symantec.cloud - Endpoint Protection.cloud 21.x (32bits) Symantec.cloud - Endpoint Protection.cloud 21.x (64bits) Symantec EndPoint Protection 14.x (32bits) Symantec EndPoint Protection 14.x (64bits) Symantec EndPoint Protection 12.x (32bits) Symantec EndPoint Protection 12.x (64bits) Symantec EndPoint Protection 11.x (32bits) Symantec EndPoint Protection 11.x (64bits) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
Trend Micro	Trend Micro Worry-Free Business Security 8.x (32bit- Edition) Trend Micro Worry-Free Business Security 8.x (64bit- Edition) Trend Micro Worry-Free Business Security 7.x (32bit- Edition) Trend Micro Worry-Free Business Security 7.x (64bit- Edition) Trend Micro Worry-Free Business Security 6.x (32bit- Edition) Trend Micro Worry-Free Business Security 6.x (64bit- Edition) Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x Trend Micro OfficeScan 11.x
Comodo AntiVirus	Comodo Antivirus V 4.1 32bits
Panda Security	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX and earlier versions
	Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX and earlier versions
	Panda Global Protection 2017* Panda Internet Security 2017* Panda Antivirus Pro 2017* Panda Gold Protection 2017*
	Panda Global Protection 2016* Panda Internet Security 2016*

Panda Antivirus Pro 2016*
Panda Gold Protection 2016*
Panda Global Protection 2015*
Panda Internet Security 2015*
Panda Antivirus Pro 2015*
Panda Gold Protection*
Panda Free Antivirus
Panda Global Protection 2014*
Panda Internet Security 2014*
Panda Antivirus Pro 2014*
Panda Gold Protection*
Panda Global Protection 2013*
Panda Internet Security 2013*
Panda Antivirus Pro 2013*
Panda Global Protection 2012*
Panda Internet Security 2012*
Panda Antivirus Pro 2012*
Panda Global Protection 2011*
Panda Internet Security 2011*
Panda Antivirus Pro 2011*
Panda Antivirus for Netbooks (2011)*
Panda Global Protection 2010
Panda Internet Security 2010
Panda Antivirus Pro 2010
Panda Antivirus for Netbooks
Panda Global Protection 2009
Panda Internet Security 2009
Panda Antivirus Pro 2009
Panda Internet Security 2008
Panda Antivirus+Firewall 2008
Panda Antivirus 2008
Panda Internet Security 2007
Panda Antivirus + Firewall 2007
Panda Antivirus 2007

Table 46: list of uninstallers

* Panda 2017, 2016, 2015, 2014, 2013, 2012 products need a reboot to be uninstalled successfully.

* Comodo Antivirus V4.1 (32-bit) - Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

*F-Secure PSB for Workstations 9.00 - During the installation process of the Endpoint Protection agent on Windows 7 and Windows Vista systems, the user will be prompted to select the Allow option.

*AVG Internet Security Business Edition 2011 (32-bit) - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in several windows.

*AVG Internet Security Business Edition 2011 (64-bit) (10.0.1375) - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in several windows.

* Kaspersky Anti-Virus 6.0 for Windows workstations:

During the installation process of the Endpoint Protection agent on 64-bit platforms, the user will be prompted to select the Allow option in several windows.

To be able to uninstall the protection, the Kaspersky protection must not be password-protected.

Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* F-Secure PSB for Workstations 9.00 - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in two windows.

* AVG Anti-Virus Network Edition 8.5 - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in two windows.

* Panda Antivirus 2011 products do not uninstall correctly on 64-bit platforms. Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* Panda Cloud Antivirus 1.4 Pro and Panda Cloud Antivirus 1.4 Free - Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically on Windows Vista x64 systems.

* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically on Windows Vista x64 systems with UAC enabled.

* ESET NOD32 Antivirus 3.0.XX (2008) does not uninstall automatically on Windows Vista x64 systems.

* ESET NOD32 Antivirus 2.7*: after installing the Endpoint Protection agent on the computer, the system will restart automatically without displaying any notifications or asking for user confirmation.

* ESET NOD32 Antivirus 2.70.39*: after installing the Endpoint Protection agent on the computer, the system will restart automatically without displaying any notifications or asking for user confirmation.

* ESET Smart Security 3.0 does not uninstall automatically on Windows Vista x64 systems.

* Sophos Anti-virus SBE 2.5 does not uninstall correctly on Windows 2008 systems.

* eTrust Antivirus 7.1 does not uninstall correctly on 64-bit platforms.

* Norton Antivirus Internet Security 2008 does not uninstall correctly if the Windows Vista UAC is enabled.

* BitDefender Free Edition 2009 12.0.12.0: on Windows Vista systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

* Kaspersky Anti-Virus 2010 9.0.0.459: on systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

* Kaspersky Anti-Virus 8: on Windows Vista systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

* McAfee Total Protection Services 4.7. The uninstaller does not run correctly if UAC is enabled. Furthermore, 32-bit platforms require user intervention.

* Microsoft Live OneCare 2.5 does not uninstall correctly on Windows Small Business Server 2008.

If you have a program not included on this list, contact the relevant vendor to find out how to uninstall it before installing **Endpoint Protection / Plus on Aether**.

23. Appendix 4: key Concepts

Active Directory

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed directory service for finding a range of information on network environments.

Adware

Program that automatically runs, displays or downloads advertising to the computer.

Alert

See Incident.

Anti-spam

Technology that searches for unwanted email based on its contents.

Anti-Tamper protection

A set of technologies aimed at preventing tampering of the **Endpoint Protection / Plus** processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, anti-exploit techniques, etc.), to detect and remove computer viruses and other threats.

ARP (Address Resolution Protocol)

A telecommunication protocol used for resolution of Internet layer addresses into link layer addresses. On IP networks, this protocol translates IP addresses into physical MAC addresses.

Automatic assignment of settings

See Inheritance.

Backup

Storage area for non-disinfectable malicious files, as well as the spyware items and hacking tools detected on your network. All programs classified as threats and removed from the system are temporarily moved to the backup/quarantine area for a period of 7/30 day based on their type.

Broadcasting

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network simultaneously, without the need to send it individually to each device. Broadcast packets don't go through routers and use different addressing methodology to differentiate them from unicast packets.

Cache/Repository (role)

Computers that automatically download and store all files required so that other computers with **Endpoint Protection / Plus** installed can update their signature file, agent and protection engine

without having to access the Internet. This saves bandwidth as it won't be necessary for each computer to separately download the updates they need. All updates are downloaded centrally for all computers on the network

Cloud (Cloud computing)

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

Computers without a license

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers are not protected, but are displayed in the Web management console.

Device control

Module that allows organizations to define the way protected computers must behave when connecting a removable or mass storage device to them.

DHCP

Service that assigns an IP address to each computer on a network

Dialer

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

Discovery computer (role)

Computers capable of finding unmanaged workstations and servers on the network in order to remotely install the **Endpoint Protection / Plus** agent on them.

Disinfectable file

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

Domain

Windows network architecture where the management of shared resources, permissions and users is centralized in a server called a Primary Domain Controller (PDC) or Active Directory (AD).

Domain Name System (DNS)

Service that translates domain names into different types of information, generally IP addresses.

Dwell time

Length of time that a threat has remained undetected on the network.

Endpoint Protection / Plus software

Program installed on the computers to protect. It consists of two modules: the Panda agent and the protection.

Environment variable

A string consisting of environment information such as a drive, path or file name, which is associated with a symbolic name that Windows can use. You can use the System applet in the Control Panel or the 'set' command at the command prompt to set environment variables.

Exchange server

Mail server developed by Microsoft. Exchange servers store inbound and/or outbound emails and distribute them to users' email inboxes.

Excluded program

Programs that were initially deleted as they were classified as malware or PUP, but have been selectively and temporarily allowed by the administrator, who excluded them from the scans performed by the solution.

Exploit

Generally speaking, an exploit is a sequence of specially crafted data aimed at causing a controlled error in the execution of a vulnerable program. Once the error occurs, the compromised process will mistakenly interpret certain parts of the data sequence as executable code, taking malicious actions that may compromise the security of the target computer.

Filter

A dynamic-type computer container that automatically groups together those items that meet the conditions defined by the administrator. Filters simplify the assignment of security settings, and facilitate management of all computers on the network.

Filter tree

Collection of filters grouped into folders, used to organize all computers on the network and facilitate the assignment of settings.

Firewall

Technology that blocks the network traffic that coincides with certain patterns defined in rules established by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

Folder tree

Hierarchical structure consisting of static groups, used to organize all computers on the network and facilitate the assignment of settings.

Fragmentation

On data transmission networks, when the MTU of the underlying protocol is not sufficient to accommodate the size of the transmitted packet, routers divide the packet into smaller segments (fragments) which are routed independently and assembled in the right order at the destination.

Geolocation

Geographical positioning of a device on a map from its coordinates.

Goodware

A file which, after analysis, has been classified as legitimate and safe.

Group

Static container that groups one or more computers on the network. Computers are assigned to groups manually. Groups simplify the assignment of security settings, and facilitate management of all computers on the network.

Hacking tool

Programs used by hackers to carry out actions that cause problems for the user of the affected computer (allowing the hacker to control the computer, steal confidential information, scan communication ports, etc.).

Heuristic scanning

Static scanning that employs a set of techniques to inspect suspicious programs based on hundreds of file characteristics. It can determine the likelihood that a program may take malicious actions when run on a user's computer.

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

ICMP (Internet Control Message Protocol)

Error notification and monitoring protocol used by the IP protocol on the Internet.

IDP (Identity Provider)

Centralized service for managing user identity verification.

Indirect assignment of settings

See Inheritance.

Infection vector

The means used by malware to infect users' computers. The most common infection vectors are Web browsing, email and pen drives.

Inheritance

A method for automatically assigning settings to all subsets of a larger, parent group, saving management time. Also referred to as 'automatic assignment of settings' or 'indirect assignment of settings'.

IP address

Number that identifies a device interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

IP Feeds

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

IP (Internet Protocol)

Principal Internet communications 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.

Linux distribution

Set of software packets and libraries that comprise an operating system based on the Linux kernel.

MAC address

48-bit hexadecimal number that uniquely identifies a network card or interface.

Malware

This term is used to refer to all programs that contain malicious code (MALicious softWARE), whether it is a virus, Trojan, worm or any other threat to the security of IT systems. Malware tries to infiltrate or damage computers, often without users knowing, for a variety of reasons.

Malware Freezer

A feature of the quarantine/backup module whose goal is to prevent data loss due to false positives. All files classified as malware or suspicious are sent to the quarantine/backup area, thereby avoiding deleting and losing data if the classification is wrong.

Manual assignment of settings

Direct assignment of a set of settings to a group, as opposed to the automatic or indirect assignment of settings, which uses the inheritance feature to assign settings without administrator intervention.

MD5 (Message-Digest Algorithm 5)

A cryptographic hash function producing a 128-bit value that represents data input. The MD5 hash value calculated for a file is used to identify it unequivocally or check that it has not been tampered with.

MTU (Maximum Transmission Unit)

Maximum packet size (in bytes) that the transport will transmit over the underlying network.

Network adapter

Hardware that allows communication among different computers connected through a data network. A computer can have more than one network adapter installed, and is identified in the system through a unique identifier.

Network topology

Physical or logical map of network nodes.

OU (Organizational Unit)

Hierarchical method for classifying and grouping objects stored in directories.

Panda agent

One of the modules included in the **Endpoint Protection / Plus** software. It manages communications between computers on the network and Panda Security's cloud-based servers, in addition to managing local processes.

Partner

A company that offers Panda Security products and services.

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Peer to Peer (P2P) functionality

Information transfer mechanism that uses the network bandwidth more efficiently on networks with nodes that work simultaneously as clients and servers, establishing a direct two-way communication.

Endpoint Protection / Plus implements P2P connections to reduce bandwidth usage, as those computers whose signature file has been already updated will share the update locally with those computers that also need to update it.

Phishing

A technique for obtaining confidential information from a user fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

Port

Unique ID number assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

Potentially Unwanted Program (PUP)

A program that may be unwanted, despite the possibility that users consented to download it. Potentially unwanted programs are often downloaded inadvertently along with other programs.

Protection (module)

One of the two components of the **Endpoint Protection / Plus** software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the **Endpoint Protection / Plus** cloud.

Proxy functionality

This feature allows **Endpoint Protection / Plus** to operate on computers without Internet access, accessing the Web through an agent installed on another computer on the same subnet.

Public network

Networks in public places such as airports, coffee shops, etc. These networks require that you establish some limitations regarding computer visibility and usage, especially with regard to file, directory and resource sharing.

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Quarantine

See Backup.

RIR (Regional Internet Registry)

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

Role

Specific permission configuration applied to one or more user accounts, and which authorizes users to view and edit certain resources of the console.

Rootkit

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is used by attackers to hide evidence and utilities on previously compromised systems.

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.

Samples Feed

A service for delivering normalized malware and automations through a REST API to companies with their own anti-malware laboratory.

SCL (Spam Confidence Level)

Normalized value assigned to a message that indicates the likelihood that the message is spam, based on its characteristics (content, headers, etc.)

Settings

See Settings profile.

Settings profile

Specific settings governing the protection or any other aspect of the managed computer. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

Signature file

File that contains the patterns used by the antivirus to detect threats.

SMTP server

Server that uses SMTP (Simple Mail Transfer Protocol) to exchange email messages between computers.

Spam

This term refers to unsolicited email messages that usually contain advertising and are generally sent out massively. Spam can have a range of negative effects on the recipient.

Spyware

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and collects personal data.

Suspicious item

A program with a high probability of being malware after having been scanned by the **Endpoint Protection / Plus** protection installed on the user's computer.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

SYN

Flag in the TOS (Type Of Service) field of TCP packets that identifies them as connection start packets.

Task

Set of actions scheduled for execution at a configured frequency during a specific period of time.

TCO (Total Cost of Ownership)

Financial estimate of the total direct and indirect costs of owning a product or system.

TCP (Transmission Control Protocol)

The main transport-layer Internet protocol, aimed at connections for exchanging IP packets.

TLS (Transport Layer Security)

New version of protocol SSL 3.0.

Trojans

Programs that reach computers disguised as harmless software to install themselves on computers and carry out actions that compromise user confidentiality.

Trusted network

Networks in private places such as offices and households. Connected computers are generally visible to the other computers on the network, and there is no need to establish limitations on file, directory and resource sharing.

UDP (User Datagram Protocol)

A transport-layer protocol which is unreliable and unsuited for connections for exchanging IP packets.

User (console)

Information set used by **Endpoint Protection / Plus** to regulate administrator access to the Web console and establish the actions that administrators can take on the network's computers.

User (network)

A company's workers using computing devices to do their job.

User account

See User.

Virus

Programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

VPN (Virtual Private Network)

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

Web access control

Technology that allows organizations to control and filter the URLs requested by the network's Internet browsers in order to allow or deny access to them, taking as reference a URL database divided into content categories.

Web console

Tool to manage the advanced security service **Endpoint Protection / Plus**, accessible anywhere, anytime through a supported Internet browser. The Web console allows administrators to deploy the security software, push security settings, and view the protection status.

Widget (Panel)

Panel containing a configurable graph representing a particular aspect of network security. **Endpoint Protection / Plus's** dashboard is made up of different widgets.

Workgroup

Architecture in Windows networks where shared resources, permissions and users are managed independently on each computer.



Endpoint Protection



Endpoint Protection Plus

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

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

© Panda Security 2017. All rights reserved..