



 Adaptive Defense 360

# Guide for Network Administrators

---

## Table of contents

<b>1. PREFACE.....</b>	<b>9</b>
1.1. INTRODUCTION .....	10
1.2. WHO IS THE GUIDE AIMED AT? .....	10
1.3. ICONS .....	10
<b>2. INTRODUCTION.....</b>	<b>11</b>
2.1. INTRODUCTION .....	12
2.2. KEY FEATURES OF ADAPTIVE DEFENSE 360.....	12
2.3. ADAPTIVE DEFENSE 360 USER PROFILE.....	13
2.4. ADAPTIVE DEFENSE 360 ARCHITECTURE: KEY COMPONENTS .....	13
2.4.1 ADAPTIVE DEFENSE 360 CLOUD SERVER FARM.....	14
2.4.2 MANAGEMENT CONSOLE WEB SERVER .....	15
2.4.3 COMPUTERS PROTECTED WITH ADAPTIVE DEFENSE 360.....	15
2.5. ADAPTIVE DEFENSE 360 SERVICES.....	19
2.5.1 ADVANCED REPORTING TOOL SERVICE.....	19
2.5.2 SIEMFEEDER SERVICE: INTEGRATION WITH THE CUSTOMER'S SIEM SERVICE .....	19
2.5.3 SAMPLES FEED.....	20
2.5.4 IP FEEDS.....	20
2.5.5 REMOTE CONTROL MODULE .....	20
2.6 ADAPTIVE DEFENSE 360: SUPPORTED DEVICES.....	20
2.7 AVAILABLE RESOURCES AND DOCUMENTATION.....	21
<b>3. THE ADAPTIVE PROTECTION FULL CYCLE .....</b>	<b>22</b>
3.1. INTRODUCTION .....	23
3.2. THE ADAPTIVE PROTECTION CYCLE .....	23
3.3. PHASE 1: COMPLETE PROTECTION OF THE IT NETWORK.....	24
3.3.1 ANTI-EXPLOIT PROTECTION .....	24
3.3.2 PERMANENT ANTIVIRUS PROTECTION AND COLLECTIVE INTELLIGENCE .....	25
3.3.3 PROTECTION AGAINST ADVANCED STEALTH TECHNIQUES AND MACRO VIRUSES .....	25
3.3.4 EMAIL AND WEB PROTECTION .....	26
3.3.5 FIREWALL AND INTRUSION DETECTION SYSTEM (IDS) .....	26
3.3.6 DEVICE CONTROL .....	26
3.3.7 SPAM, VIRUS AND CONTENT FILTERING FOR EXCHANGE SERVERS .....	26
3.3.8 WEB ACCESS CONTROL.....	27
3.3.9 PROTECTION FOR VULNERABLE SYSTEMS .....	27
3.4. PHASE 2: DETECTION AND MONITORING.....	27
3.4.1 ADVANCED PERMANENT PROTECTION.....	28
3.4.2 MONITORING DATA FILES .....	29
3.4.3 VISIBILITY OF THE NETWORK STATUS.....	30
3.5. PHASE 3: REMEDIATION AND RESPONSE .....	30
3.6. PHASE 4: ADAPTATION.....	31
<b>4. CREATING PANDA ACCOUNTS .....</b>	<b>33</b>
4.1. INTRODUCTION .....	34
4.2. CREATING A PANDA ACCOUNT .....	34

<b>4.3. ACTIVATING YOUR PANDA ACCOUNT .....</b>	<b>35</b>
<b><u>5. THE WEB MANAGEMENT CONSOLE.....</u></b>	<b><u>36</u></b>
<b>5.1. INTRODUCTION .....</b>	<b>37</b>
5.1.1 WEB CONSOLE REQUIREMENTS.....	37
5.1.2 IDP FEDERATION .....	38
<b>5.2. GENERAL STRUCTURE OF THE WEB MANAGEMENT CONSOLE .....</b>	<b>38</b>
5.2.1 TOP MENU (1).....	38
5.2.2 BROWSER PATH (2) .....	41
5.2.3 SIDE MENU (3) .....	41
5.2.4 TABS (4).....	41
5.2.5 GENERAL SETTINGS BUTTON (5) .....	41
5.2.6 LOGGED-IN USER (6) .....	43
5.2.7 PANDA CLOUD BUTTON (7) .....	43
5.2.8 SETTINGS COMPONENTS (8).....	43
5.2.9 NOTIFICATIONS (9).....	44
5.2.10 ACCESS TO THE ADVANCED REPORTING TOOL SERVICE (10) .....	44
<b><u>6. LICENSES .....</u></b>	<b><u>45</u></b>
<b>6.1. INTRODUCTION .....</b>	<b>46</b>
<b>6.2. CONTRACTING AND RENEWING LICENSES.....</b>	<b>46</b>
6.2.1 LICENSE CONTRACTS .....	46
<b>6.3. PROTECTION STATUS .....</b>	<b>48</b>
<b>6.4. ASSIGNING AND RELEASING LICENSES .....</b>	<b>49</b>
<b>6.5. LICENSE EXPIRY NOTIFICATIONS.....</b>	<b>50</b>
<b><u>7. ACCOUNT MANAGEMENT .....</u></b>	<b><u>51</u></b>
<b>7.1. INTRODUCTION .....</b>	<b>52</b>
<b>7.2. DELEGATING ACCOUNT MANAGEMENT .....</b>	<b>52</b>
7.2.1 POSSIBLE ERRORS WHEN DELEGATING ACCOUNT MANAGEMENT.....	53
<b>7.3. MERGING ACCOUNTS .....</b>	<b>53</b>
7.3.1 CONSEQUENCES OF MERGING ACCOUNTS.....	53
7.3.2 REQUIREMENTS FOR MERGING ACCOUNTS.....	54
7.3.3 HOW TO MERGE ACCOUNTS .....	54
7.3.4 EFFECTS OF ACCOUNT MERGING ON SERVICE CONFIGURATION .....	54
7.3.5 POSSIBLE ERROR MESSAGES WHEN MERGING ACCOUNTS .....	55
<b><u>8. USERS .....</u></b>	<b><u>56</u></b>
<b>8.1. INTRODUCTION .....</b>	<b>57</b>
<b>8.2. CREATING USERS .....</b>	<b>57</b>
<b>8.3. CHANGING USER DETAILS .....</b>	<b>58</b>
<b>8.4. DELETING USERS.....</b>	<b>59</b>
<b>8.5. ASSIGNING PERMISSIONS TO USERS AND GROUPS .....</b>	<b>60</b>
8.5.1 PERMISSION INHERITANCE .....	60
<b>8.6. TYPES OF PERMISSIONS.....</b>	<b>60</b>
8.6.1 TOTAL CONTROL PERMISSION .....	61
8.6.2 ADMINISTRATOR PERMISSION .....	62
8.6.3 MONITORING PERMISSION.....	63

<b>9.</b>	<b><u>INSTALLING THE PROTECTION</u></b>	<b>64</b>
9.1.	<b>INTRODUCTION</b>	<b>65</b>
9.1.1	AGENT DOWNLOAD FROM THE CONSOLE	65
9.1.2	GENERATING A DOWNLOAD URL	66
9.1.3	CENTRALIZED DISTRIBUTION TOOL	66
9.1.4	SEARCHING FOR UNPROTECTED COMPUTERS	67
9.2.	<b>PROTECTION DEPLOYMENT OVERVIEW</b>	<b>71</b>
9.3.	<b>INSTALLING THE PROTECTION ON WINDOWS COMPUTERS</b>	<b>73</b>
9.3.1	INTERNET ACCESS REQUIREMENTS	73
9.3.2	HARDWARE AND SOFTWARE REQUIREMENTS	75
9.4.	<b>INSTALLING THE PROTECTION ON WINDOWS COMPUTERS WITH MICROSOFT EXCHANGE</b>	<b>76</b>
9.4.1	INTERNET ACCESS REQUIREMENTS	76
9.4.2	HARDWARE AND SOFTWARE REQUIREMENTS	76
9.5.	<b>INSTALLING THE PROTECTION ON LINUX COMPUTERS</b>	<b>77</b>
9.5.1	INTERNET ACCESS REQUIREMENTS	77
9.5.2	HARDWARE AND SOFTWARE REQUIREMENTS	77
9.6.	<b>INSTALLING THE PROTECTION ON MAC OS X COMPUTERS</b>	<b>78</b>
9.6.1	INTERNET ACCESS REQUIREMENTS	78
9.6.2	HARDWARE AND SOFTWARE REQUIREMENTS	79
9.7.	<b>INSTALLING THE PROTECTION ON ANDROID DEVICES</b>	<b>79</b>
9.7.1	INTERNET ACCESS REQUIREMENTS	81
9.7.2	HARDWARE AND SOFTWARE REQUIREMENTS	81
9.8.	<b>INTRODUCTION TO INSTALLATION USING IMAGE GENERATION</b>	<b>81</b>
9.9.	<b>UNINSTALLING THE PROTECTION</b>	<b>82</b>
9.9.1	LOCAL UNINSTALL	83
9.9.2	UNINSTALLING THE PROTECTION USING THE CENTRALIZED DISTRIBUTION TOOL	83
9.9.3	UNINSTALLING THE PROTECTION FROM THE MANAGEMENT CONSOLE	84
<b>10.</b>	<b><u>UPDATING THE PROTECTION</u></b>	<b>87</b>
10.1.	<b>INTRODUCTION</b>	<b>88</b>
10.2.	<b>UPDATING THE COMMUNICATIONS AGENT</b>	<b>88</b>
10.3.	<b>UPDATING THE PROTECTION ON WINDOWS SYSTEMS</b>	<b>89</b>
10.3.1	UPDATING THE PROTECTION	89
10.3.2	UPDATING THE SIGNATURE FILE	91
10.3.3	PEER-TO-PEER OR RUMOR FUNCTIONALITY	91
10.4.	<b>UPDATING THE PROTECTION ON WINDOWS SERVER CORE SYSTEMS</b>	<b>93</b>
10.5.	<b>UPDATING THE PROTECTION ON LINUX SYSTEMS</b>	<b>93</b>
10.5.1	UPDATING THE PROTECTION	93
10.5.2	UPDATING THE SIGNATURE FILE	93
10.6.	<b>UPDATING THE PROTECTION ON MAC OS X SYSTEMS</b>	<b>93</b>
10.6.1	UPDATING THE PROTECTION	93
10.6.2	UPDATING THE SIGNATURE FILE	93
10.7.	<b>UPDATING THE PROTECTION ON ANDROID SYSTEMS</b>	<b>94</b>
10.7.1	UPDATING THE PROTECTION	94
10.7.2	UPDATING THE SIGNATURE FILE	94
<b>11.</b>	<b><u>GROUPS</u></b>	<b>95</b>
11.1.	<b>INTRODUCTION</b>	<b>96</b>
11.1.1	ASSIGNING COMPUTERS TO GROUPS	96
11.2.	<b>COMPUTER TREE</b>	<b>96</b>

<b>11.3. GROUP TYPES .....</b>	<b>97</b>
<b>11.4. CREATING A MANUAL GROUP .....</b>	<b>98</b>
<b>11.5. CREATING AN AUTOMATIC GROUP ARRANGED BY IP ADDRESS .....</b>	<b>98</b>
11.5.1 IMPORTING RULES FROM A .CSV FILE .....	99
11.5.2 HOW AUTOMATIC GROUPS ARRANGED BY IP ADDRESS WORK .....	100
<b>11.6. CREATING AN AUTOMATIC GROUP BASED ON ACTIVE DIRECTORY .....</b>	<b>100</b>
11.6.1 AUTOMATIC REPLICATION OF THE ACTIVE DIRECTORY STRUCTURE .....	100
11.6.2 MANUAL REPLICATION OF THE ACTIVE DIRECTORY STRUCTURE .....	101
11.6.3 VIEWING A COMPUTER'S ACTIVE DIRECTORY PATH INFORMATION .....	102
<b>11.7. ADDING A COMPUTER TO A GROUP.....</b>	<b>103</b>
11.7.1 MANUAL INTEGRATION .....	103
11.7.2 ADDING A COMPUTER TO A GROUP DURING INSTALLATION .....	104
<b>11.8. CREATING AND DELETING A GROUP .....</b>	<b>104</b>
<b>11.9. GROUP RESTRICTIONS.....</b>	<b>106</b>
<b><u>12. PROTECTION PROFILES.....</u></b>	<b><u>108</u></b>
<b>12.1. INTRODUCTION .....</b>	<b>109</b>
<b>12.2. NETWORK PROTECTION OVERVIEW AND PLANNING .....</b>	<b>109</b>
<b>12.3. CREATING AND MANAGING PROTECTION PROFILES .....</b>	<b>112</b>
12.3.1 CREATING A PROTECTION PROFILE .....	113
12.3.2 COPYING PROTECTION PROFILES .....	113
12.3.3 DELETING A PROTECTION PROFILE .....	114
<b>12.4. PROTECTION PROFILE GENERAL SETTINGS .....</b>	<b>114</b>
<b><u>13. WINDOWS PROTECTION PROFILES .....</u></b>	<b><u>117</u></b>
<b>13.1. INTRODUCTION .....</b>	<b>118</b>
<b>13.2. GENERAL SETTINGS .....</b>	<b>118</b>
<b>13.3. CONFIGURING THE ADVANCED PROTECTION.....</b>	<b>122</b>
13.3.1 BEHAVIOR.....	122
13.3.2 ANTI-EXPLOIT .....	122
13.3.3 EXCLUSIONS .....	124
13.3.4 NETWORK USAGE.....	124
13.3.5 PRIVACY .....	125
<b>13.4. CONFIGURING THE ANTIVIRUS PROTECTION .....</b>	<b>125</b>
<b>13.5. CONFIGURING THE FIREWALL AND INTRUSION DETECTION FEATURES .....</b>	<b>126</b>
<b>13.6. CONFIGURING THE DEVICE CONTROL FEATURE .....</b>	<b>130</b>
13.6.1 DEVICE EXCLUSIONS.....	131
13.6.2 EXPORTING/IMPORTING A LIST OF ALLOWED DEVICES .....	132
13.6.3 ALLOWING BLOCKED DEVICES .....	132
13.6.4 FINDING A DEVICE'S UNIQUE ID .....	132
13.6.5 ALERTS.....	133
<b>13.7. CONFIGURING THE PROTECTION FOR EXCHANGE SERVERS .....</b>	<b>133</b>
13.7.1 ANTIVIRUS .....	134
13.7.2 ANTI-SPAM .....	134
<b>13.8. CONFIGURING THE WEB ACCESS CONTROL PROTECTION.....</b>	<b>136</b>
<b>13.9. CONFIGURING TIME PERIODS FOR THE WEB ACCESS CONTROL FEATURE.....</b>	<b>138</b>
<b><u>14. LINUX PROTECTION PROFILES.....</u></b>	<b><u>139</u></b>
<b>14.1. INTRODUCTION .....</b>	<b>140</b>

14.2.	GENERAL SETTINGS .....	140
14.3.	CONFIGURING THE ANTIVIRUS PROTECTION .....	141
<b>15.</b>	<b><u>MAC OS X PROTECTION PROFILES .....</u></b>	<b>142</b>
15.1.	INTRODUCTION .....	143
15.2.	SPECIFIC CHARACTERISTICS OF THE PROTECTION FOR MAC OS X.....	143
15.3.	GENERAL PROTECTION SETTINGS .....	144
15.4.	CONFIGURING THE ANTIVIRUS PROTECTION .....	145
<b>16.</b>	<b><u>ANDROID PROTECTION PROFILES .....</u></b>	<b>146</b>
16.1.	INTRODUCTION .....	147
16.2.	CONFIGURING THE ANTIVIRUS PROTECTION .....	147
16.3.	CONFIGURING THE ANTI-THEFT PROTECTION .....	148
<b>17.</b>	<b><u>MALWARE VISIBILITY AND MONITORING .....</u></b>	<b>150</b>
17.1.	INTRODUCTION .....	151
17.2.	DASHBOARD.....	151
17.3.	ACTIVITY SECTION .....	151
17.4.	DETECTIONS SECTION .....	155
17.5.	ACTIVITY SECTION LISTS.....	159
17.5.1	MALICIOUS PROGRAMS AND EXPLOITS LIST .....	160
17.5.2	CURRENTLY BLOCKED ITEMS BEING CLASSIFIED .....	163
17.5.3	PUP LIST .....	165
17.5.4	DETECTION DETAILS LIST.....	166
17.6.	MANAGING EXCLUSIONS AND BLOCKED ITEMS.....	171
17.6.1	KNOWN FILES .....	172
17.6.2	UNKNOWN FILES.....	172
17.6.3	UNBLOCKING UNKNOWN ITEMS PENDING CLASSIFICATION .....	173
17.6.4	EXCLUDING ITEMS CLASSIFIED AS MALWARE OR PUP.....	174
17.6.5	EXCLUDED ITEMS MANAGEMENT WINDOW .....	175
17.6.6	CURRENTLY ALLOWED ITEMS .....	176
17.6.7	HISTORY .....	178
<b>18.</b>	<b><u>COMPUTER VISIBILITY AND MONITORING .....</u></b>	<b>181</b>
18.1.	INTRODUCTION .....	182
18.2.	NETWORK COMPUTER STATUS .....	182
18.3.	COMPUTER VISIBILITY .....	182
18.3.1	SEARCH TOOLS.....	184
18.3.2	LISTS OF COMPUTERS .....	185
18.3.3	ACTIONS ON SELECTED COMPUTERS .....	187
18.3.4	DETAILS OF WINDOWS, LINUX AND MAC OS X COMPUTERS .....	188
18.3.5	DETAILS OF ANDROID DEVICES.....	190
<b>19.</b>	<b><u>REPORTS .....</u></b>	<b>192</b>
19.1.	INTRODUCTION .....	193
19.2.	REPORT TYPES.....	193

- 19.2.1 EXECUTIVE REPORT ..... 193
- 19.2.2 STATUS REPORT ..... 194
- 19.2.3 DETECTION REPORT ..... 194
- 19.2.4 THREATS REPORT ..... 194
- 19.2.5 CONSOLE ACCESS AUDIT REPORT ..... 195
- 19.2.6 COMPUTER STATUS REPORT ..... 196
- 19.3. GENERATING AND SENDING REPORTS ..... 196**
- 19.3.1 REPORT NAME AND CONTENT ..... 196
- 19.3.2 REPORT SCOPE ..... 197
- 19.3.3 SCHEDULED REPORTS ..... 197

**20. REMEDIATION TOOLS ..... 199**

- 20.1. INTRODUCTION ..... 200**
- 20.2. AUTOMATIC FILE DISINFECTION ..... 200**
- 20.3. EXPLOIT BLOCKING ..... 201**
- 20.4. ON-DEMAND FILE SCANNING AND DISINFECTION ..... 202**
- 20.5. ADVANCED COMPUTER DISINFECTION ..... 202**
- 20.6. COMPUTER RESTART ..... 203**
- 20.7. REMOTE DESKTOP ACCESS ..... 203**
- 20.7.1 VIEWING COMPUTERS WITH REMOTE ACCESS TOOLS INSTALLED ..... 204
- 20.7.2 HOW TO GET REMOTE ACCESS TO ANOTHER COMPUTER ..... 205
- 20.7.3 HOW TO USE THE REMOTE ACCESS TOOLS ..... 205
- 20.8. ANTI-THEFT PROTECTION ..... 206**
- 20.8.1 ENABLING THE ANTI-THEFT PROTECTION ..... 206

**21. QUARANTINE ..... 208**

- 21.1. INTRODUCTION ..... 209**
- 21.2. QUARANTINE ON LINUX AND ANDROID DEVICES ..... 209**
- 21.3. QUARANTINE AND MALWARE FREEZER BEHAVIOR ..... 209**
- 21.3.1 STORING SUSPICIOUS FILES ..... 209
- 21.3.2 SENDING SUSPICIOUS ITEMS TO QUARANTINE ..... 209
- 21.4. QUARANTINE MANAGEMENT ..... 210**
- 21.4.1 SEARCHING FOR QUARANTINED ITEMS ..... 210
- 21.4.2 RESTORING QUARANTINED ITEMS ..... 210
- 21.4.3 LIST OF QUARANTINED ITEMS ..... 211
- 21.4.4 FILES EXCLUDED FROM SCANS ..... 211

**22. FORENSIC ANALYSIS ..... 212**

- 22.1. INTRODUCTION ..... 213**
- 22.2. FORENSIC ANALYSIS USING THE ACTION TABLES ..... 213**
- 22.2.1 MALWARE DETAILS ..... 213
- 22.2.2 EXPLOIT DETAILS ..... 214
- 22.2.3 ACTION TABLE ..... 215
- 22.2.4 SUBJECT AND PREDICATE IN ACTIONS ..... 216
- 22.3. FORENSIC ANALYSIS USING THE ACTIVITY GRAPHS ..... 218**
- 22.3.1 DIAGRAMS ..... 219
- 22.3.2 NODES ..... 219
- 22.3.3 LINES AND ARROWS ..... 221
- 22.3.4 THE TIMELINE ..... 221

22.3.5	ZOOM IN AND ZOOM OUT .....	222
22.3.6	TIMELINE .....	222
22.3.7	FILTERS.....	223
22.3.8	NODE MOVEMENT AND GENERAL ZOOM .....	223
<b>22.4.</b>	<b>INTERPRETING THE ACTION TABLES AND ACTIVITY GRAPHS .....</b>	<b>224</b>
22.4.1	EXAMPLE 1: VIEWING THE ACTIONS EXECUTED BY THE MALWARE TRJ/OCJ.A .....	224
22.4.2	EXAMPLE 2: COMMUNICATION WITH EXTERNAL COMPUTERS BY BETTERSURF .....	226
22.4.3	EXAMPLE 3: ACCESS TO THE REGISTRY BY PASSWORDSTEALER.BT .....	227
22.4.4	EXAMPLE 4: ACCESS TO CONFIDENTIAL DATA BY TRJ/CHGT.F .....	228
<b>23.</b>	<b><u>APPENDIX 1: CENTRALIZED INSTALLATION TOOLS .....</u></b>	<b><u>230</u></b>
<b>23.1.</b>	<b>INTRODUCTION .....</b>	<b>231</b>
<b>23.2.</b>	<b>INSTALLATION USING ACTIVE DIRECTORY .....</b>	<b>231</b>
<b>23.3.</b>	<b>INSTALLATION USING THE DISTRIBUTION TOOL.....</b>	<b>234</b>
23.3.1	MINIMUM REQUIREMENTS .....	234
23.3.2	HOW TO DEPLOY THE AGENT .....	235
23.3.3	HOW TO UNINSTALL ADAPTIVE DEFENSE 360 CENTRALLY .....	235
<b>24.</b>	<b><u>APPENDIX 2: COMMUNICATION WITH ENDPOINTS .....</u></b>	<b><u>237</u></b>
<b>24.1.</b>	<b>INTRODUCTION .....</b>	<b>238</b>
<b>24.2.</b>	<b>ENDPOINT COMMUNICATION WITH THE INTERNET .....</b>	<b>238</b>
24.2.1	COMMUNICATION PERIODS.....	238
24.2.2	INTERNET ACCESS .....	238
<b>24.3.</b>	<b>BANDWIDTH CONSUMPTION SUMMARY TABLE .....</b>	<b>239</b>
<b>24.4.</b>	<b>SECURITY OF COMMUNICATIONS AND STORED DATA.....</b>	<b>240</b>
<b>25.</b>	<b><u>APPENDIX 3: LIST OF UNINSTALLERS.....</u></b>	<b><u>242</u></b>
<b>26.</b>	<b><u>APPENDIX 4: KEY CONCEPTS.....</u></b>	<b><u>250</u></b>

# 1. Preface

---

Who is the guide aimed at?

Icons

## 1.1. Introduction

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

## 1.2. Who is the guide aimed at?

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

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

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

## 1.3. Icons

The following icons appear in the guide:



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



Suggestions and recommendations.



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



See another chapter or section in the guide for more information

# 2. Introduction

---

Key features

User profile

General architecture

Adaptive Defense 360 architecture: Key components

Adaptive Defense 360 Services

## 2.1. Introduction

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

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

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

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

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

## 2.2. Key features of Adaptive Defense 360

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

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

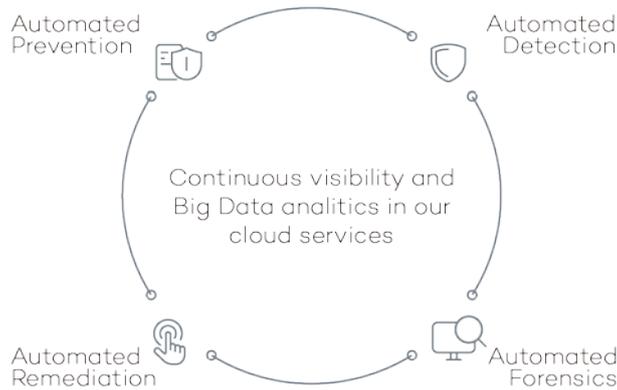


Figure 1: The four pillars of **Adaptive Defense 360**'s advanced protection

### 2.3. Adaptive Defense 360 user profile

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

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

### 2.4. Adaptive Defense 360 architecture: Key components

**Adaptive Defense 360** is based on monitoring the behavior of all processes run in the customer's IT infrastructure. The information collected is analyzed using machine learning techniques in Big Data environments hosted in the cloud, so customers don't have to install additional hardware or resources on their premises.

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

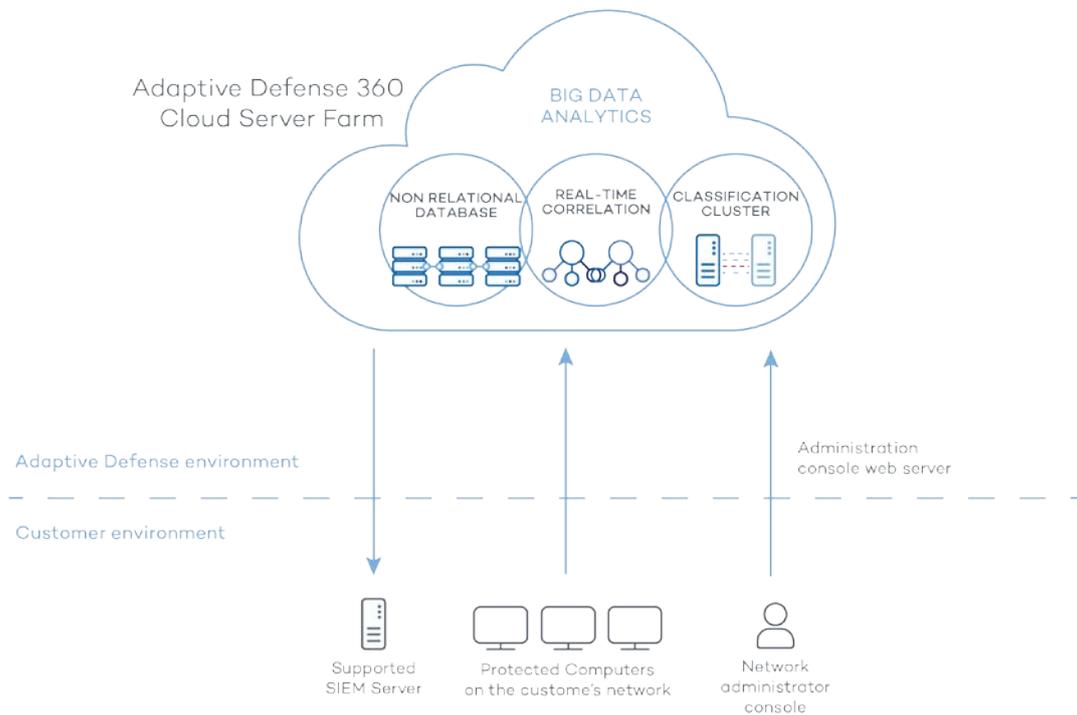


Figure 2: General structure of **Adaptive Defense 360**

**Adaptive Defense 360** comprises several components:

- Cloud server farm
- Management console Web server
- Computers protected by the **Adaptive Defense 360** software
- Computer of the network administrator that accesses the Web console
- ART (Advanced Reporting Tool) server
- Compatible SIEM server
- Protection module installed on the network computers

Below we describe the roles of the architecture components.

### 2.4.1 Adaptive Defense 360 cloud server farm

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

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

There are several advantages to this new model of analyzing processes in the cloud as opposed to

traditional techniques based on sending samples to the antivirus vendor and manual analysis:

- The success rate when classifying a process run on multiple endpoints over time is 99.9991% (less than 1 error for every 100,000 files scanned,) so the number of false positives and false negatives is virtually zero.
- Every process run on the computers protected by **Adaptive Defense 360** is monitored and analyzed, which eliminates the uncertainty provided by traditional antivirus solutions, which recognize malware items but cannot identify other applications.
- The delay in classifying processes seen for the first time (the malware window of opportunity) is minimal, as the **Adaptive Defense 360** agent relays in real time the actions triggered by each process to the server, which analyzes them looking for suspicious behavior. This drastically reduces the customer's exposure when dealing with threats and targeted attacks. In addition, the executable files found on users' computers that are not recognized by the **Adaptive Defense 360** platform are sent by the agent to Panda Security's server farm for analysis.



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

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

## 2.4.2 Management console Web server

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

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

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

## 2.4.3 Computers protected with Adaptive Defense 360

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

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



*Even though in this chapter we make a difference between "agent" and "protection", these are two modules that install at the same time and are necessary to correctly manage the security of the computer to*

*protect. This way, both terms -“agent” and “protection”- are used indistinctly to refer to the software component installed on each user's computer.*

- **Communications agent**

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

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

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

- The administrator makes a configuration change in the Web console.
- The server sends a notification to inform the affected computers that a configuration change has been made.
- Each computer checks for new notifications every 15 minutes. If there is a new notification:
  - The computer asks the **Adaptive Defense 360** server for the new configuration policies.
  - The server delivers the policies to the computer, which applies them.

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

### Dynamic proxy

Each agent stores a list with information about the computers on the network that have agents installed capable of sending messages to the Internet. These agents are called proxies.



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

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

While waiting for data about the list of valid proxies, the proxy's module will not attend other requests. The list of proxies has a value associated to each proxy with a maximum number of attempts to connect to another agent before it is considered invalid.

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

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

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

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

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

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

### **Static proxy**

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

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

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

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

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

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

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

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

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

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

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

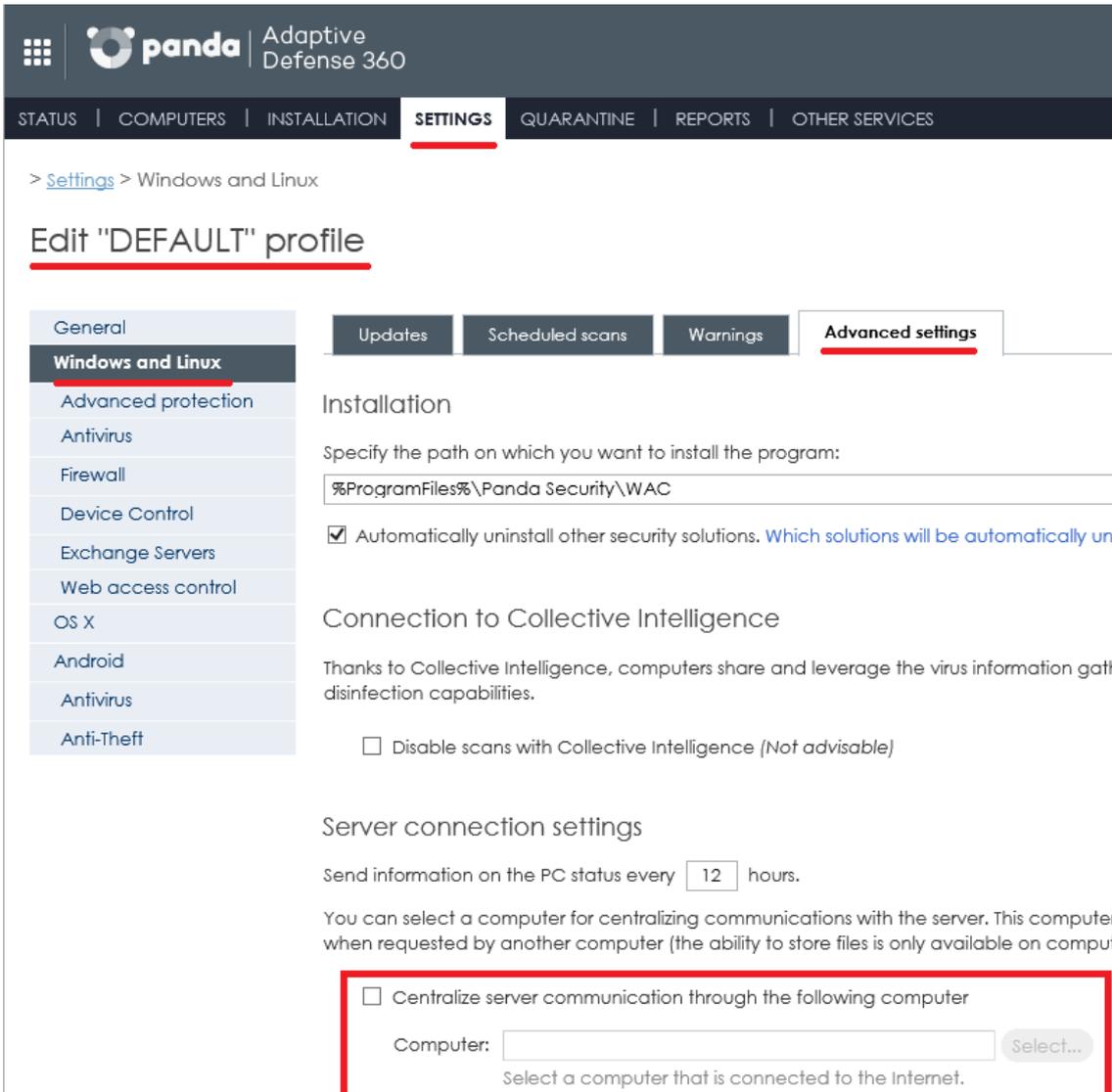


Figure 3: Configuring a proxy computer

- **Protection module**

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



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

## 2.5. Adaptive Defense 360 services

### 2.5.1 Advanced Reporting Tool service

**Adaptive Defense 360** allows all the information collected from customers' computers to be automatically and seamlessly sent to Advanced Reporting Tool, a service designed to store and exploit the knowledge generated on the customer's network.

**Adaptive Defense 360** monitors all processes run across the IT network, whether goodware or malware, sending their actions to Advanced Reporting Tool, a platform capable of flexibly and visually relating all the data collected in order to extract security intelligence and obtain additional information on threats and the way users are using corporate computers.

The **Advanced Reporting Tool** service can be accessed directly from the **Adaptive Defense 360** Web console dashboard.



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

### 2.5.2 SIEMFeeder service: Integration with the customer's SIEM service

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

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

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora



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

### 2.5.3 Samples Feed

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

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

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

### 2.5.4 IP Feeds

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

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

### 2.5.5 Remote Control module

**Adaptive Defense 360** offers customers a cloud-based remote control module that facilitates remote troubleshooting. This module provides network administrators with a number of tools, including remote desktop and remote command line, to remove malware and check that their computers are working properly.

All of the tools provided by the Remote Control module are run from the cloud, and can be accessed anywhere, anytime, from the **Adaptive Defense 360** console using any of the supported Web browsers.



*Refer to the Remote Control Administrator's Guide for more information about this module.*

## 2.6 Adaptive Defense 360: Supported devices

**Adaptive Defense 360** supports the following operating systems:

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

The management console supports the following Web browsers:

- Chrome
- Internet Explorer
- Microsoft Edge\* (we recommend that you disable SmartScreen Filter)
- Firefox

## 2.7 Available resources and documentation

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

### **Guide for Network Administrators**

<http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADAPTIVEDEFENSE360-manual-EN.pdf>

### **Advanced Reporting Tool Guide**

<http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADVANCEDREPORTING TOOL-Guide-EN.pdf>

### **SIEMFeeder Guide**

<http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-EN.PDF>

### **Product Support Page**

<http://www.pandasecurity.com/usa/support/adaptive-defense-360-aether.htm>

### **Product Page**

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

# 3. The adaptive protection full cycle

---

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

### 3.1. Introduction

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

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

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

Consequently, every security strategy must be based on minimizing malware dwell time, that is, the time lapse between when an unknown threat enters the customer's network and when it is identified as malware. Today, malware dwell time is an estimated 259 days for the increasingly common targeted attacks, whose main objectives are industrial espionage and data theft.

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

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

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

### 3.2. The adaptive protection cycle

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

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

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

The adaptive protection cycle implemented by companies with the help of **Adaptive Defense 360** is illustrated in Figure 4.

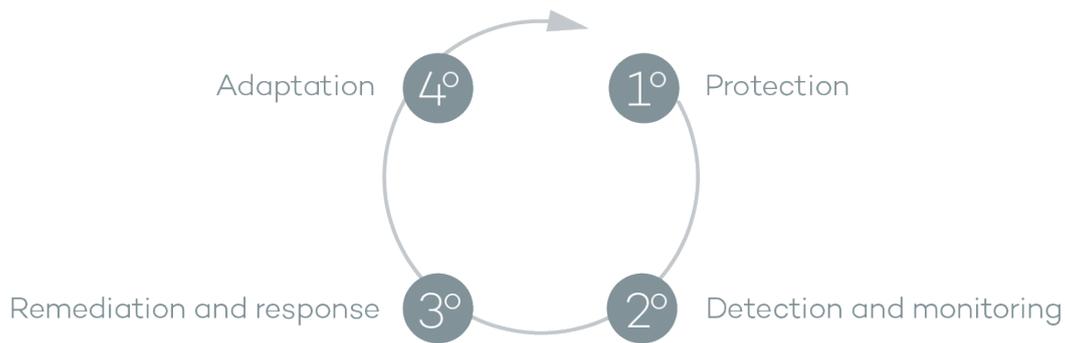


Figure 4: Adaptive protection cycle

### 3.3.Phase 1: Complete protection of the IT network



Refer to chapters 13 14 and 15 for more information about the Adaptive Defense 360 protection features covered in this section

The first phase in the adaptive protection cycle involves the necessary tools to effectively protect and defend the IT network against attacks and infection attempts. **Adaptive Defense 360** is compatible with Windows, Linux and Mac OS X workstations and servers, as well as with Android smartphones and tablets.

#### 3.3.1 Anti-exploit protection

**Adaptive Defense 360** implements technologies to protect network computers against threats capable of leveraging bugs in installed software (exploits). These bugs can cause anomalous behaviors in compromised applications, leading to security failures on customers' networks.

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

In order to achieve these high levels of protection and immediate response, **Adaptive Defense 360** implements new hooks in the operating system, using them to locally and continually monitor all

actions taken by the processes run on users' computers.

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

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

### 3.3.2 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 and 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 Adaptive Defense 360's antivirus protection is primarily based on Collective Intelligence, a cloud-based knowledge platform that exponentially increases detection capabilities.

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

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

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

### 3.3.3 Protection against advanced stealth techniques and macro viruses

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

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

Finally, the service can also detect the latest fileless infection techniques, which inject the virus

payload directly into the processes used to exploit system vulnerabilities. These attacks do not write files to the hard disk, so traditional security solutions are less likely to detect them.

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

### 3.3.4 Email and Web protection

**Adaptive Defense 360** goes beyond the traditional email and Web security approach based on plug-ins that add the relevant protection features to certain email clients and Web browsers.

Instead, it works by intercepting at low level every communication that uses common protocols such as HTTP, HTTPS or POP3. This way, the solution is able to provide permanent, homogeneous protection for all email and Web applications past, present and future, without the need for specific configurations or updates as email and Web service providers release new products incompatible with the previous plug-ins.

### 3.3.5 Firewall and intrusion detection system (IDS)

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

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

### 3.3.6 Device control

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

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

### 3.3.7 Spam, virus and content filtering for Exchange servers

**Adaptive Defense 360** scans all messages sent to your Exchange Server mailboxes for spam, viruses, hacking tools and suspicious/potentially unwanted programs.

To do this, it implements both anti-spam and antivirus protection for Exchange servers.

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

- Mailbox protection

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

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

Additionally, the mailbox protection is configured to have no impact on the way the Exchange server works upon receiving a new signature file. The protection will scan the entire server in the background, making the most of server idle times.

- **Transport protection**

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

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

### 3.3.8 Web access control

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

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

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

### 3.3.9 Protection for vulnerable systems

**Adaptive Defense 360** protects even those systems that are recognized within the industry as vulnerable, having reached their EOL (End Of Life), like Windows XP for example. Those systems no longer receive security updates and may have vulnerabilities that can be taken advantage of through exploits.

## 3.4.Phase 2: Detection and monitoring

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

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

### 3.4.1 Advanced permanent protection

Adaptive Defense 360's advanced protection is a new, ground-breaking technology that continuously monitors every process run on the customer's Windows computers. **Adaptive Defense 360** collects all actions taken by the processes run on the network and sends them to Panda Security's cloud, where they are analyzed applying automatic Machine Learning techniques in Big Data environments. The service returns a classification (goodware or malware) with 99.9991 accuracy (less than 1 error for every 100,000 files scanned), preventing false positives.

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

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

- **Audit**

In Audit mode, **Adaptive Defense 360** only reports on detected threats but doesn't block or disinfect the malware detected. This mode is useful for testing the security solution or checking that the installation of the product doesn't have a negative effect on computer performance.

- **Hardening**

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

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

- Files classified by **Adaptive Defense 360** as goodware: They are allowed to run.
- Files classified by **Adaptive Defense 360** as malware: They are sent to quarantine or disinfected.
- Unclassified files coming from external sources (Internet, email and others): They are prevented from running until a classification is returned. Once a classification is returned they will be allowed to run (goodware) or not (malware).



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

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

- **Lock**

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

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



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

### 3.4.2 Monitoring data files

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

It will also be possible to determine if those files were sent out over the Internet, the target IP addresses, and other information that may be useful for the subsequent forensic analysis or remediation actions.

Below we list the types of data files that are monitored:

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

### 3.4.3 Visibility of the network status

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

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

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

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

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

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



*Refer to chapter 17 Malware visibility and monitoring for more information*

### 3.5.Phase 3: Remediation and response

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

- **Response**

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



*Refer to chapter 22 Forensic analysis for more information about how to use this tool*

- **Remediation**

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

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

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

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



*Refer to chapter 20 Remediation tools for more information*

### 3.6. Phase 4: Adaptation

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

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

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

- **Changing the advanced protection settings**

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

- **Changing the antivirus protection settings**

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

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

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

- **Filtering out spam and phishing messages**

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

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

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

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

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

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

# 4. Creating Panda Accounts

---

Creating a Panda Account  
Activating your Panda Account

## 4.1. 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 **Adaptive Defense 360** Web console.

## 4.2. Creating a Panda Account

Follow the steps below to create a Panda Account.

### Open the email message received from Panda Security

- After purchasing **Adaptive Defense 360**, you will receive an email message from Panda Security.
- Click the link in the message to access a site from which you will be able to create your Panda Account.



## Create your Panda Account

Creating an account is all you need to access all of your Panda services.

Email address

Confirm your email address

**Create**

Figure 5: Creating a 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.
- Once you have finished entering the relevant data, click **Create**. You will receive a message at the email address entered in the form. Follow the instructions in that message to activate your account.

### 4.3. 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 **Adaptive Defense 360** Web console. To do that, simply click the solution's icon in the My Services section.

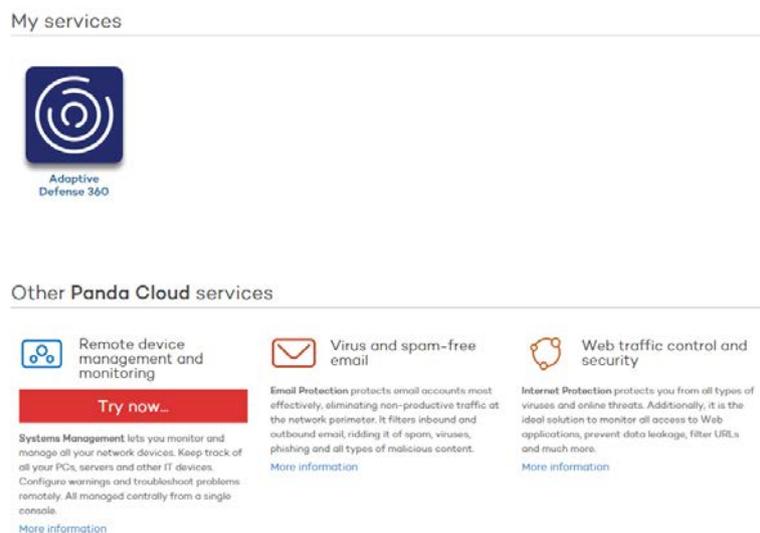


Figure 6: Panda Cloud screen showing the services available for the created account

# 5. The Web management console

---

General structure of the Web management console

## 5.1. Introduction

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

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

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

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

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

- **Security management from anywhere at any time**

The Web 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.

### 5.1.1 Web console requirements

The Web console can be accessed from the following link:

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

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

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



*See Chapter 4 Creating Panda Accounts for more details on how to create a Panda account for accessing the Web console*

- Latest version of a compatible Internet browser:
  - Internet Explorer
  - Firefox
  - Google Chrome
- Internet connection and communication through port 443.

### 5.1.2 IdP federation

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

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



## 5.2. General structure of the Web 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 troubleshooting and forensic analysis.

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

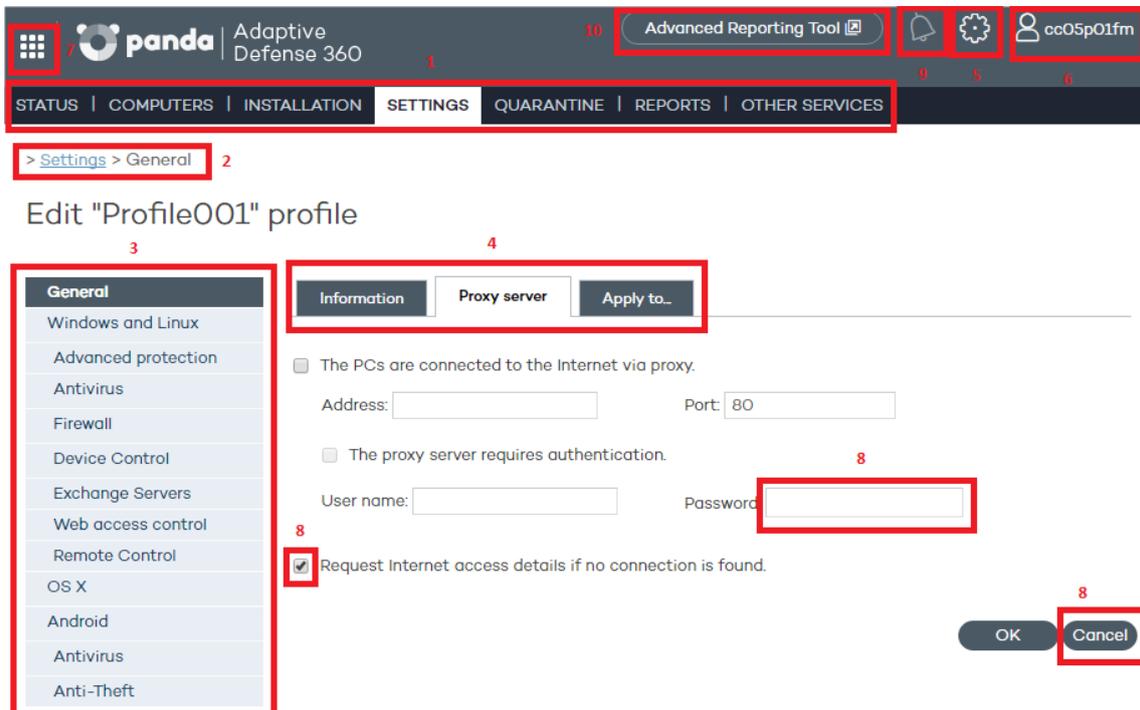


Figure 7: Overview of the management console

### 5.2.1 Top menu (1)

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

Status

- Computers

- Installation
- Settings
- Quarantine
- Reports
- Other services

### Status window

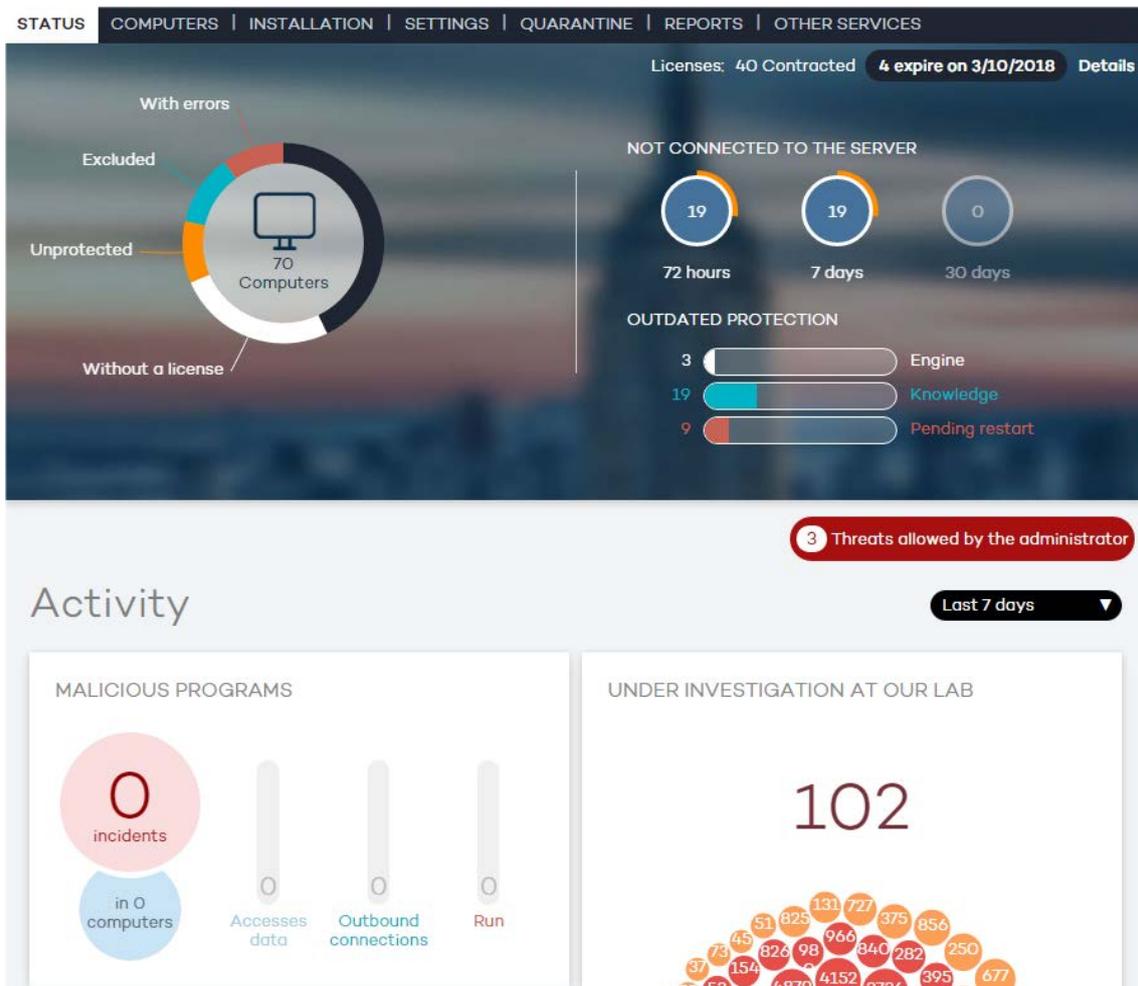


Figure 8: Status window

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

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

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



See chapter 6 Licenses for more details on license management in Adaptive Defense 360. See chapter 17 Malware visibility and monitoring, and chapter 19 Reports, for more information about the real-time monitoring of your network security and the consolidated reports.

### Computers window

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

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

### Installation window

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



See chapter 9 Installing the protection for more information about how to install the Adaptive Defense 360 agents on your network computers.

### Settings window

This lets you manage and configure groups and protection profiles.



See chapter 11 Groups and chapter 12 Protection profiles for more details on how to create profiles and groups. See chapters 13, 14 and 15 for more information on how to configure the protection profiles based on the platform to protect (Windows, Linux, Mac OS X and Android)

### Quarantine window

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



See chapter 21 Quarantine for more information

### Reports window

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



See chapter 19 Reports for more information

### Other services window

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

### 5.2.2 Browser path (2)

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

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

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

### 5.2.3 Side menu (3)

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

### 5.2.4 Tabs (4)

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

### 5.2.5 General settings button (5)

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

#### Users

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



*See chapter 8 Users for more information about users and permissions*

#### Preferences

This includes general settings regarding the operation of the console:

- **Language:** Lets you choose between 13 console languages.
- **Email alerts:** To prevent situations where the organization's internal mail server is down, cannot be accessed by the computer's local protection, or the customer does not have an SMTP mail server, the Adaptive Defense platform can also send email alerts directly to the administrator's account without passing through the organization's internal mail server. These alerts contain information about the items detected and blocked on Windows computers.

## Email alerts

Send alerts when the following events occur:

- Malware detected.
- PUP detected.
- An item gets blocked.
- A file allowed by the administrator is classified.

Send the alerts to the following address:

email@example.com

(If you want to specify more than one address, separate them with ";")

Alert language:

English ▾

Figure 9: Alert configuration settings

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

- **Every time a malware specimen or PUP is detected:** A maximum of 2 emails will be sent per file, computer and day to avoid flooding the administrator's mailbox. This option is selected by default.
- **Every time an exploit is detected:** The service will send as many email alerts as detections are made, without limitation. This option is selected by default.
- **Every time an item gets blocked:** A single email will be sent per file, computer and day to avoid flooding the administrator's mailbox. This option is disabled by default.
- **Every time a file allowed by the administrator is finally classified:** This alert is sent in those cases in which the administrator excludes a blocked item that is pending classification, and the item is finally classified as malware (or goodware). Since this is a potentially dangerous situation, the system will send an alert to the administrator whenever a change is made to an excluded item's classification. The most typical case is the exclusion of a blocked unclassified item that **Adaptive Defense 360** finally classifies as malware
- **Default view:** This determines how computers will be displayed in the console: by name or by IP address.
- **Group restrictions:** This lets you determine the maximum number of computers in any given group.
- **Remote access:** This lets you configure the credentials for accessing computers administered by Adaptive Defense 360 and which have any of the supported remote desktop applications installed (LogMeIn, TeamViewer and VNC). This access can be shared with the service provider in order to delegate management of the computers.



The Remote Access feature allows integration of Adaptive Defense 360 with a number of compatible third-party remote access tools. Additionally, Adaptive Defense 360 offers Panda Remote Control, a proprietary troubleshooting tool that doesn't require third-party products or specific configurations. Contact your sales representative if you want to purchase Panda Remote Control licenses. Refer to the Panda Remote Control Administrator's Guide for more information

- **Automatic management of suspicious files:** This lets you automatically send files classified as suspicious to Panda Security for analysis.

- **Account management:** This lets you merge accounts and delegate administration of computers.



*See chapter 7 Account management for more details*

## Help

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

## Advanced administration guide

This lets you download the advanced administration guide.

## Tech Support

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

## Suggestions box

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

## License agreement

Here you can see the product EULA.

## About

This displays the versions of the various service components.

### 5.2.6 Logged-in user (6)

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

### 5.2.7 Panda Cloud button (7)

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

### 5.2.8 Settings components (8)

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

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

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

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



Figure 10: Sort arrows in table headers

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

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

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

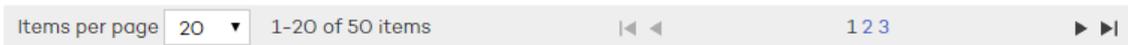


Figure 11: Pagination controls in the table footer

### 5.2.9 Notifications (9)

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

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

### 5.2.10 Access to the Advanced Reporting Tool service (10)

Click this button to access the Advanced Reporting Tool Web management console. Advanced Reporting Tool is a service that enables administrators to obtain detailed reports and perform advanced searches on the network applications and their activity.



*Refer to the Advanced Reporting Tool User's Guide for more information.*

# 6. Licenses

---

Contracting and renewing licenses

License status

Assigning and releasing licenses

License expiry alerts

## 6.1. Introduction

To benefit from **Adaptive Defense 360**'s advanced security services, you need to purchase licenses of **Adaptive Defense 360** for Windows/Linux/Android, or **Adaptive Defense 360** for OS X if you need protection for OS X systems. Depending on the specific needs of your network, it may be necessary to install/uninstall the protection on some computers, remove computers from the protected computers list, add new computers to the list, etc.

License usage is reflected in the number of available licenses.



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



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

## 6.2. Contracting and renewing licenses

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



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

### 6.2.1 License contracts

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

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

The license contracts will vary depending on the platform:

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

- **License contracts for Mac OS X are specific to OS X:** Specific licenses for OS X

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

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



Figure 12: Details button

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

### License list

**Adaptive Defense 360:** 25 licenses (21 used, 4 unused)

[<<Back](#)

Page 1 of 1

1-2 of 2 items

Items per page

20

[View](#)

Product	Contracted	Type	Expiry date ▲
Adaptive Defense 360 + Advanced Reporting	15	Demo	5/20/2018
Adaptive Defense 360 + Advanced Reporting	10	Demo	5/20/2019

First Previous

1

Next Last

Figure 13: List of license contracts

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

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

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

### 6.3. Protection status

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

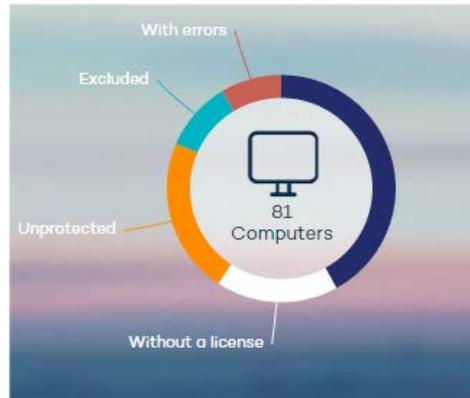


Figure 14: Panel showing the protection status of the network computers

Hover the mouse pointer over each color to display a tooltip with the number of computers corresponding to each category.

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

#### Network computers

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

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

#### OK computers

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

These computers are using a license.

#### Computers without a license

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

Click the white area in the panel. This will take you to the **Without a license** tab of the **Computers** screen, where you will see a complete list of the computers that don't have a license assigned.

These computers do not use up licenses.

### Computers with errors

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

These computers use licenses.

### Excluded computers

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

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

These computers do not use up licenses.

### Unprotected computers

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

These computers do not use up licenses.

## 6.4. Assigning and releasing licenses

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

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

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

### Reassigning licenses

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

To prevent computers without a license from competing for newly contracted licenses, you have to

delete them from the console. To do this, go to the **Without a license** tab in the **Computers** screen, select the computers and click **Delete selected computers**.

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



*You cannot just delete a computer with licenses, as the next time it communicates with the Adaptive Defense 360 server, it will be assigned a license once again.*

## 6.5. License expiry notifications

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

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

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

# 7. Account management

---

Delegating account management

Merging accounts

## 7.1. Introduction

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

*Refer to chapter 8 Users for more information about the different types of permissions*

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

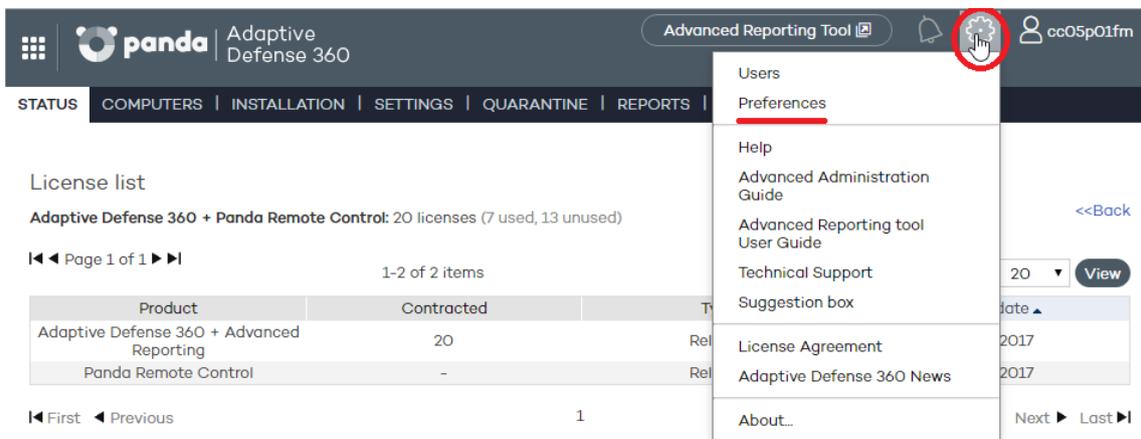


Figure 15: Accessing the Preferences window

### Account management

Click the following link to merge this account with another or delegate the security service.



Figure 16: Account management option

## 7.2. Delegating account management

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

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

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

### Delegate security to your service provider

Enter the identifier of the service provider that will manage the security of this account.

Identifier:

[Instructions](#)

Figure 17: Field to enter the ID of the service provider to delegate security management to

## 7.2.1 Possible errors when delegating account management

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

- **Invalid identifier. Please try again and make sure you enter it correctly.** Try again and make sure you enter the partner ID correctly.
- **You do not have licenses to perform this operation. Contact your usual sales advisor or reseller to renew them.** If your licenses have expired you will not be able to access the account management feature. Please contact your reseller or sales advisor to renew your licenses.
- **Could not perform the operation. Please contact your reseller or sales advisor.** It is possible that the characteristics of the services/licenses that you contracted do not allow you to use the management delegation feature. Please contact your reseller or sales advisor.
- **An error occurred: Could not register the request. Please try again.** This error occurs when the process fails for an unknown reason. Please try again and if you cannot activate the service, contact Panda Security technical support.

## 7.3. Merging accounts

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



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

### 7.3.1 Consequences of merging accounts

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

- The services associated with the source account will be moved to the target account. Those services will cease to be active in the source account, which will be deleted. Also, access to the source account Web console will be denied.
- The target account Web console will display data and information from the computers that were managed from the source account. To check this, just access the target account Web console.

- The protection installed on the computers managed from the source account will be reassigned automatically, and will be managed from the target account. It will not be necessary to reinstall the protection.

### 7.3.2 Requirements for merging accounts

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

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

### 7.3.3 How to merge accounts

- Access the source account Web console (this is the account that will be canceled).
- Click **Manage accounts** in the **Preferences** window. You will be taken to the **Account management window**.
- Select **Merge**.
- Enter the Login Email of a user with total control permissions on the account to transfer the data to, as well as the client number (identifier) provided in the welcome message.
- If you're sure you want to merge the accounts, click **Merge**.

### 7.3.4 Effects of account merging on service configuration

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

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



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

- **Computer groups:** All computer groups in the source account will be added to the target account. In the case of groups with the same name, the same criteria will be applied as with

profiles in the previous point.

- **Reports:** The settings of the reports generated in the source account will not be added to the target account.
- **Statistics:** All detection statistics will be transferred from the source account to the target account.
- **Quarantine:** All items found in the source account quarantine, including excluded and restored items, will be lost.
- **Users:** All users with access to the source account Web console (and their permissions) will be added to the target account, except the default user.

### 7.3.5 Possible error messages when merging accounts

The following errors can occur when merging accounts:

The merging operation cannot be performed as the accounts to merge belong to different resellers. Please contact your Panda Security reseller or sales advisor.

- The merging operation cannot be performed as the customers don't have the same product version. Please check that there are no version updates waiting to be executed. If the problem persists, please contact your Panda Security reseller or sales advisor.
- The merging operation cannot be performed as the customers don't have licenses of the same product and/or service. Please contact your Panda Security reseller or sales advisor for both accounts to have licenses of the same products and/or services.
- Error: The source customer's licenses have expired. Please contact your Panda Security reseller or sales advisor.
- The merging operation cannot be performed as it involves too many computers. However, the operation can be performed by Panda Security. Please contact your reseller directly or Panda Security for tech support.

If more than one error affects the same customer, only the first one will be displayed. When this is resolved, the second error will be displayed, and so forth until all of them are finally fixed.

# 8. Users

---

Creating users

Changing user details

Deleting users

Assigning permissions to users and groups

Types of permissions

## 8.1. Introduction

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

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

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

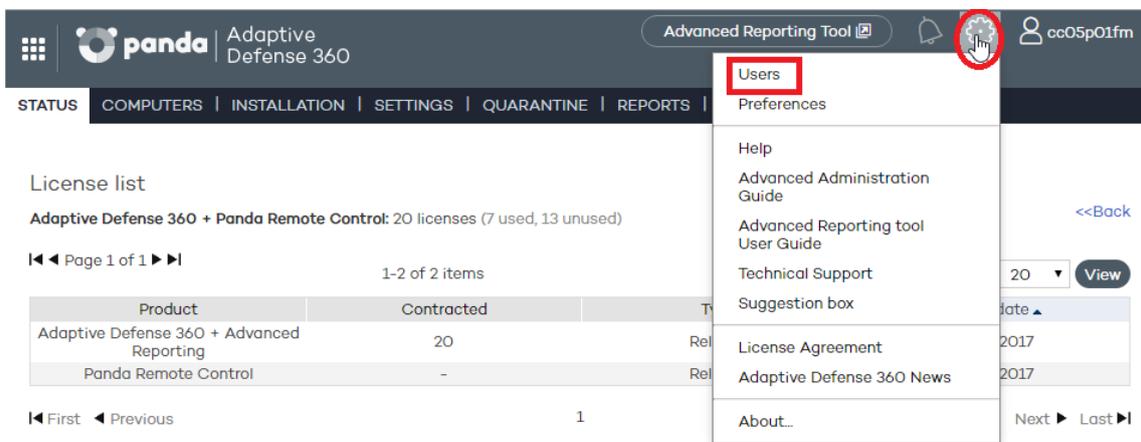


Figure 18: Accessing the Users window

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

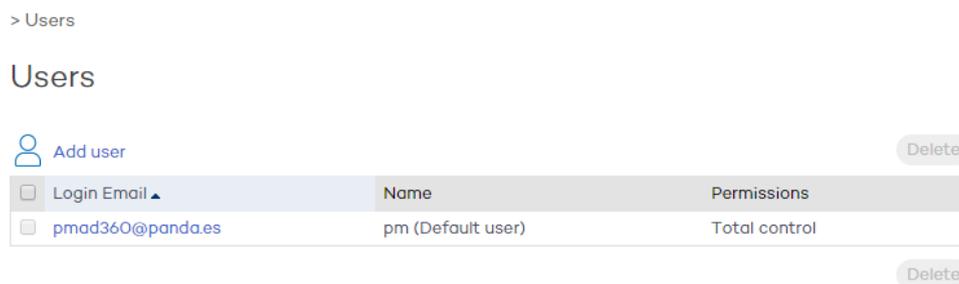


Figure 19: Users window

## 8.2. Creating users

Follow these steps to create a user:

- In the **Users** menu, click **Add user**.
- Enter the **Login Email** and confirm it.

- You can add additional information in the **Comments** section if you want to.
- Select the permission to assign to the user. For more information, refer to the **Types of permissions** section.
- In **Groups**, select the group/subgroup or groups/subgroups that the user will be able to act upon, based on the permissions assigned to them. Users with total control permissions will be able to act on all groups.
- Click **Add**. A message will be displayed informing you that an email message has been sent to the address specified when creating the user.
- After the user has been created, it will appear on the list available in the **Users** section.

### 8.3. Changing user details

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

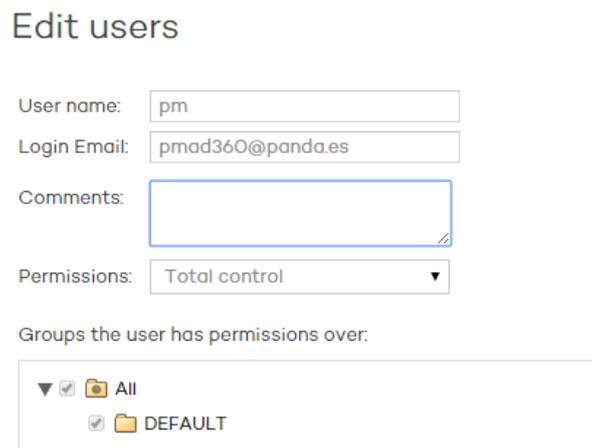


Figure 20: Edit users window

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

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

#### Changing user names

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

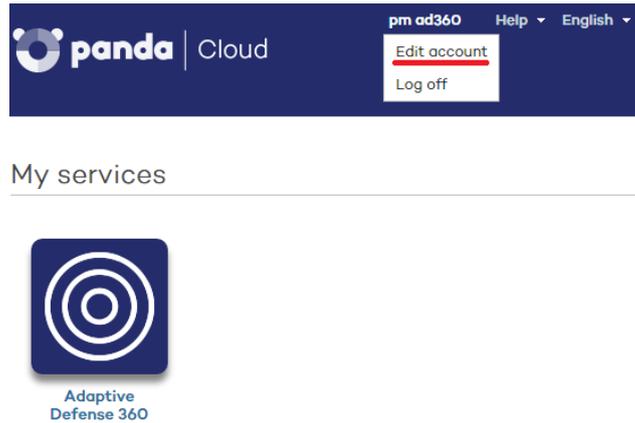


Figure 21: Accessing the Panda Account edit window

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

## Edit your Panda Account

**Account details**

Email address   
[Change password](#)

**Personal details**

First name

Last name

Date of birth

Phone number

Address

State/Region

ZIP code

City

Country

Figure 22: Panda Account edit window

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

### 8.4. Deleting users

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

## 8.5. Assigning permissions to users and groups

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

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

> [Users](#) > Edit users

### Edit users

User name:

Login Email:

Comments:

Permissions:

Groups the user has permissions over:

- ▼   All
  - DEFAULT
  - ▶   CONT\_1
  - ▶   CONT\_2

Figure 23: Editing the groups accesible to a user

### 8.5.1 Permission inheritance

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

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

## 8.6. Types of permissions

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

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

The permissions that exist are:

- Total control permission
- Administrator permission
- Monitoring permission

### 8.6.1 Total control permission

User management

The user can:

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

Group and computer management

The user can:

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

### Profile and report management

The user can:

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

### Search of unprotected computers

The user can:

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

## Protection uninstall

The user can:

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

## License and account management

The user can:

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

### 8.6.2 Administrator permission

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

## User management

The user can:

- Create users
- Delete only the users that they have created
- Edit only the users that they have created
- View only the users that they have created

## Search of unprotected computers

The user can:

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

## Group and computer management

The user can:

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

- Remotely access computers that belong to groups on which they have permissions.

### Protection uninstall

The user can:

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

### Profile and report management

The user can:

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

### 8.6.3 Monitoring permission

The user can:

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

# 9. Installing the protection

---

- Protection deployment overview
- Installing the protection on Windows computers
- Installing the protection on Windows computers with Microsoft Exchange
- Installing the protection on Linux computers
- Installing the protection on Mac OS X computers
- Installing the protection on Android devices
- Introduction to installation using image generation
- Uninstalling the protection

## 9.1. Introduction

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

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

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

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

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

Table 1: Adaptive Defense 360 deployment methods per platform

### 9.1.1 Agent download from the console

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

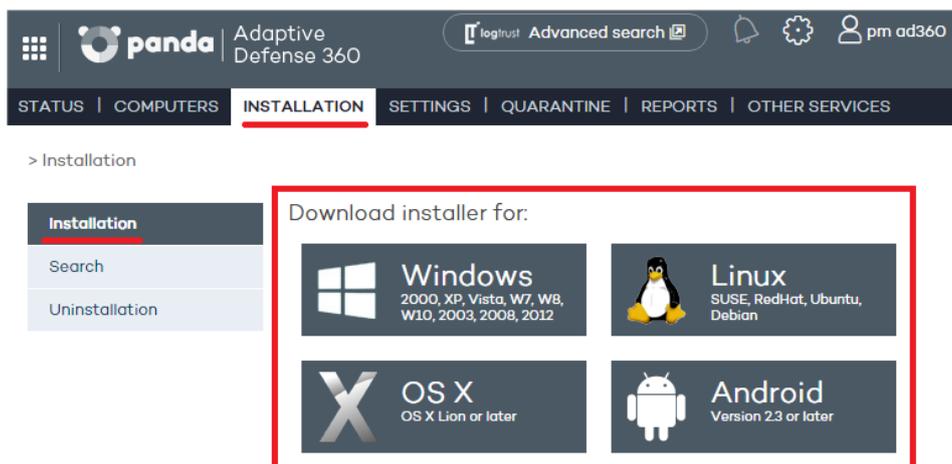


Figure 24: Agent selection window

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



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

### 9.1.2 Generating a download URL

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

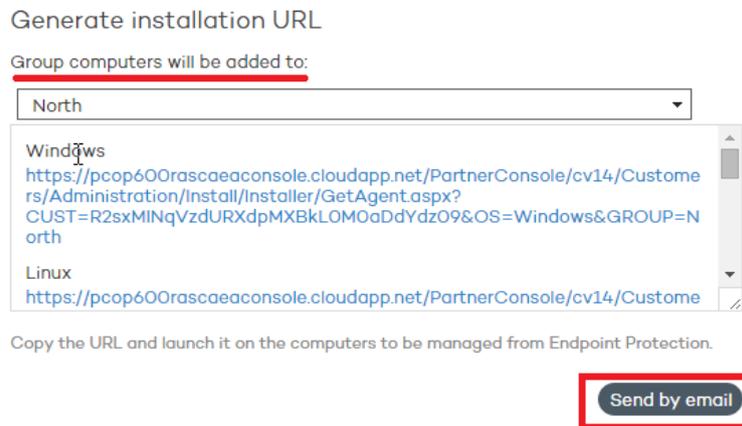


Figure 25: Download URL window

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

You will be prompted to select the group that the computer whose protection you are installing will belong to. Select the relevant group from the drop-down menu displayed. By default, the computer will belong to the DEFAULT group.

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

### 9.1.3 Centralized distribution tool

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

In the Installation window, click Download distribution tool.

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

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



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

#### 9.1.4 Searching for unprotected computers

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

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

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

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

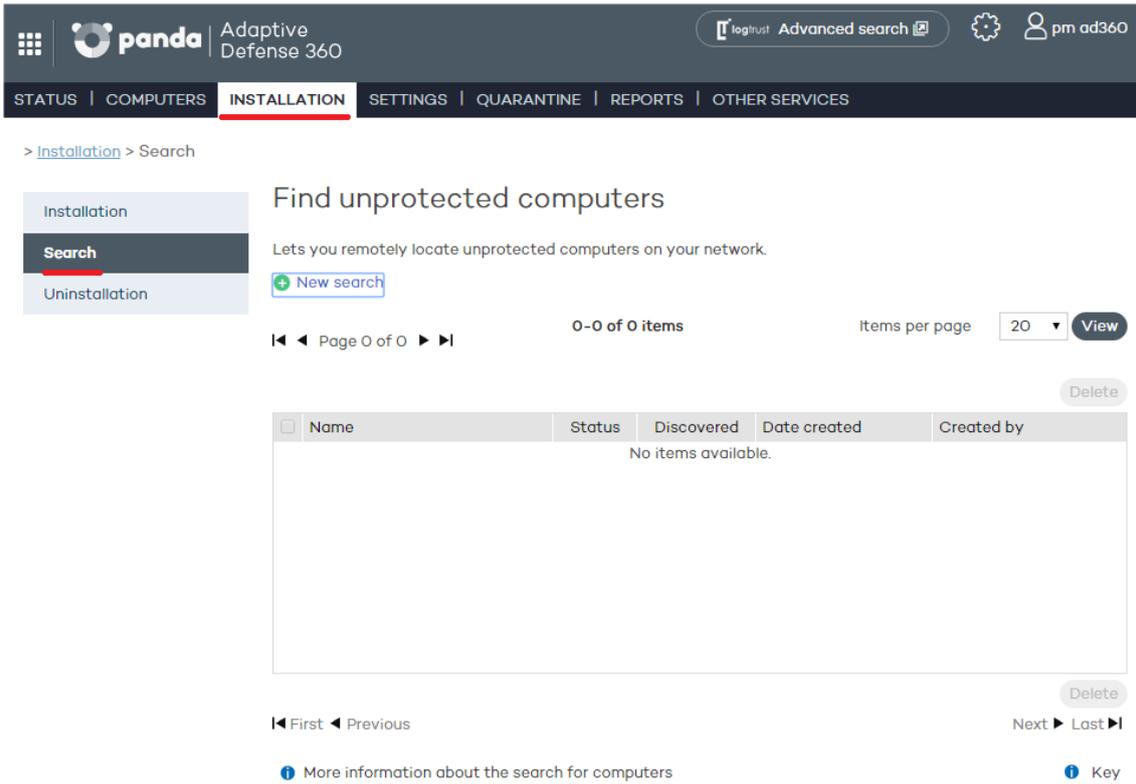


Figure 26: Find unprotected computers window

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

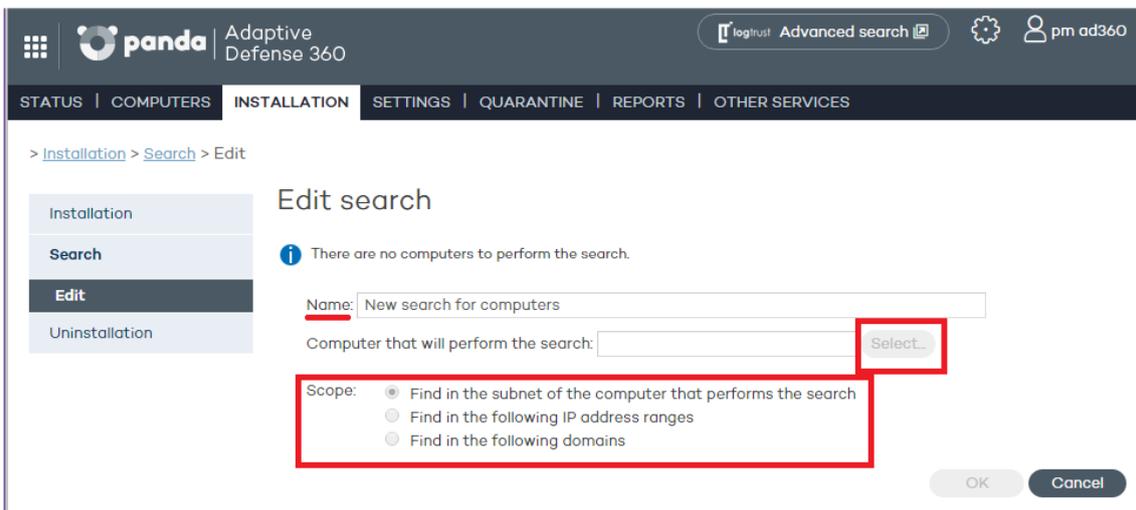


Figure 27: Configuring a computer search task

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

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

## Search types

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

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

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



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

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

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



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

- **One or several domains.**

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

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

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

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

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

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



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

## Search task statuses

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

### Search task action sequence

The action sequence will vary depending on the search type:

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

### Search task results

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

This list contains:

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

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

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

### Details of unprotected computers

The following information is obtained about each unprotected computer found:

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

## 9.2. Protection deployment overview

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

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

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

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

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

### 3. Select the installation procedure

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

### 4. Check whether the computers have another antivirus installed

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

## Trial versions

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

## Full versions

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



Refer to [Appendix 3: List of Uninstallers](#) for a full list of the antivirus solutions that Adaptive Defense 360 uninstalls automatically. If the solution you have to uninstall is not on the list, you'll have to uninstall it manually.

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

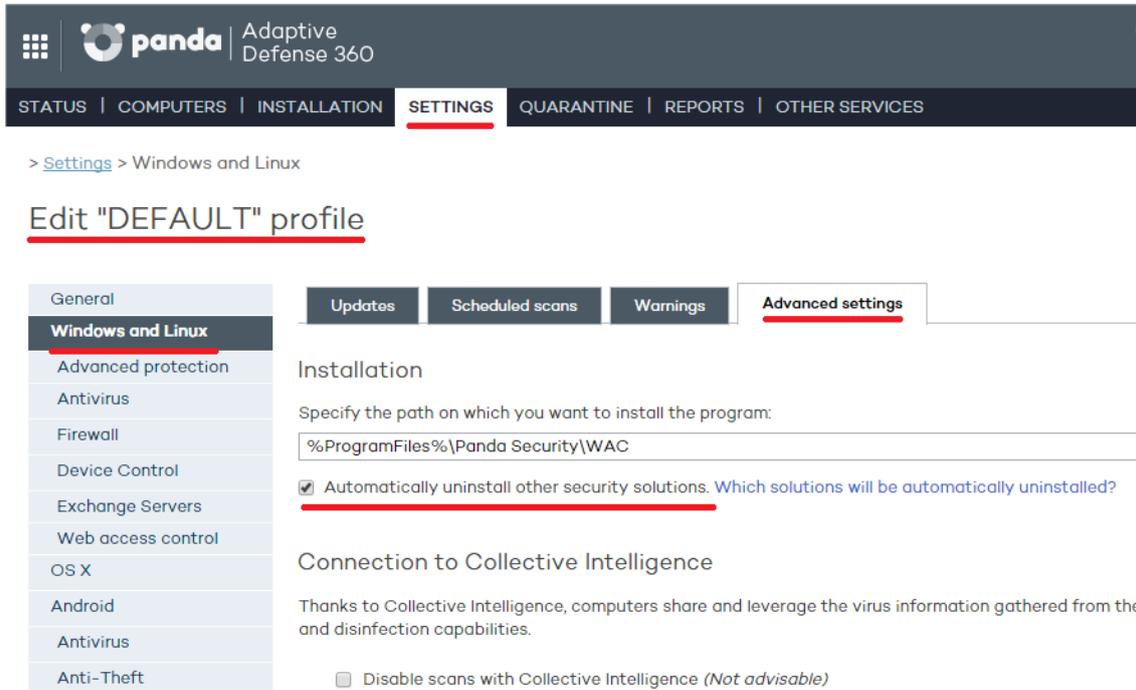


Figure 28: Option to automatically uninstall third-party security products

### Panda Security antivirus solutions

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

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

#### 5. Check if the requirements for the target platform are met

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

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

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



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

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

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

### 9.3. Installing the protection on Windows computers



*To deploy the protection across the entire network, it will be necessary to configure individual searches from the Adaptive Defense 360 console for each network segment.*

You can install **Adaptive Defense 360** on Windows computers manually by downloading the installer from the console or emailing the download URL to end users, or automatically using the centralized distribution tool (as explained in Appendix 1: Centralized installation tools).

#### 9.3.1 Internet access requirements

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

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



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

#### Web management console

- <https://www.pandacloudsecurity.com/>
- <https://managedprotection.pandasecurity.com/>
- <https://pandasecurity.logtrust.com>

#### Updates and upgrades

- <http://acs.pandasoftware.com/member/installers/>

- <http://acs.pandasoftware.com/member/uninstallers/>
- <http://enterprise.updates.pandasoftware.com/pcop/pavsig/>
- <http://enterprise.updates.pandasoftware.com/pcop/files/>
- <http://enterprise.updates.pandasoftware.com/pcop/nano>
- <http://enterprise.updates.pandasoftware.com/pcop/sigfiles/sigs>
- <http://acs.pandasoftware.com/free/>
- <http://acs.pandasoftware.com/sigfiles>
- <http://acs.pandasoftware.com/pcop/uacat>
- <http://enterprise.updates.pandasoftware.com/pcop/uacat/>
- [http://enterprise.updates.pandasoftware.com/updates\\_ent/](http://enterprise.updates.pandasoftware.com/updates_ent/)
- <https://pcopsupport.pandasecurity.com>
- <http://pcopl原因ix.updates.pandasecurity.com/updates/nanoupdate.phtml> (Linux systems)
- [http://pcopl原因ix.downloads.pandasecurity.com/nano/pavsignano/nano\\_1/](http://pcopl原因ix.downloads.pandasecurity.com/nano/pavsignano/nano_1/) (Linux systems)
- <http://www.intego.com> (OS X systems)

### Communication with the server

- <https://mp-agents-inst.pandasecurity.com>
- <http://mp-agents-inst.pandasecurity.com/Agents/Service.svc>
- <https://mp-agents-inst.pandasecurity.com/AgentsSecure/Service.svc>
- <http://mp-agents-sync.pandasecurity.com/Agents/Service.svc>
- <https://mp-agents-sync.pandasecurity.com/AgentsSecure/Service.svc>
- <http://mp-agents-async.pandasecurity.com/Agents/Service.svc>
- <https://agentscomp.pandasecurity.com/AgentsSecure/Service.svc>
- <https://pac100pacprodpcop.table.core.windows.net>
- <https://storage.accesscontrol.pandasecurity.com>
- <https://prws.pandasecurity.com>
- <http://beaglecommunity.appspot.com> (Panda Cloud Cleaner)
- <http://waspproxy.googlemail.com> (Panda Cloud Cleaner)

### Communication with the Collective Intelligence servers

- <http://proinfo.pandasoftware.com>
- <http://proinfo.pandasoftware.com/connectiontest.html>

If the product cannot connect to the aforementioned URLs, it will try to connect to <http://www.iana.org>

- <https://euws.pandasecurity.com>
- <https://rpuws.pandasecurity.com>
- <https://rpkw.s.pandasecurity.com/kdws/sigs>
- <https://rpkw.s.pandasecurity.com/kdws/files>
- <https://cpg-kw.pandasecurity.com>
- <https://cpp-kw.pandasecurity.com>

- <https://cpg-fulg.pandasecurity.com>
- <https://cpp-fulg.pandasecurity.com>
- <https://cpg-fusm.pandasecurity.com>
- <https://cpp-fusm.pandasecurity.com>
- <https://cpg-fuo.pandasecurity.com>
- <https://cpp-fuo.pandasecurity.com>
- <https://ows.pandasecurity.com>

### Communications with Cloud Cleaner

- <https://sm.pandasecurity.com/csm/profile/downloadAgent/>

### Anti-spam and URL Filtering

- [http://\\*.pand.ctmail.com](http://*.pand.ctmail.com)
- <http://download.ctmail.com>

For correct communication among the **Adaptive Defense 360** communications agents, enable ports TCP 18226 and UDP 21226 (company intranet). Also, enable ports 443 and 80 in the proxy.



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

## 9.3.2 Hardware and software requirements

- Processor: Pentium 1 GHz
- RAM: 1 GB
- Space for installation: 650 MB
- **Workstations:**
  - Operating systems: Windows 10, Windows 8.1, Windows 8, Windows 7 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows XP (32-bit and 64-bit) SP2 or later.
- **Servers:**
  - Operating systems: Windows Server 2003 (32-bit and 64-bit) SP1 or later, Windows Server 2008 (32-bit and 64-bit)\*, Windows Server 2008 R2\*, Windows Server 2012 and Windows Server 2012 R2, Windows MultiPoint Server 2012.
  - Windows Core operating systems: Windows Server Core 2008, 2008 R2 and 2012 R2.



*It is not necessary to install a GUI on Windows Server Core operating systems for Adaptive Defense 360 to work properly. Refer to chapter 10 Updating the protection for more information about the update recommendations for this operating system family*

- RAM: 1 GB.
- **Other supported applications:**
  - VMWare ESX 3.x, 4.x, 5.x and 6.x
  - VMWare Workstation 6.0, 6.5, 7.x, 8.x, 9.x, 10.x, 11.x and 12.x
  - Virtual PC 6.x
  - Microsoft Hyper-V Server 2008, 2008R2, 2012, 2012R2 and 2016 3.0
  - Citrix XenDesktop 5.x, XenClient 4.x, XenServer and XenApp 5.x and 6.x



*To deploy the protection with the distribution tool to computers with Windows Server 2008 R2, select the option "Enable remote management of this server from other computers", as specified in the following Microsoft article: <http://support.microsoft.com/kb/976839>.*

## 9.4. Installing the protection on Windows computers with Microsoft Exchange

### 9.4.1 Internet access requirements

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

### 9.4.2 Hardware and software requirements

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

- Exchange 2003:  
[http://technet.microsoft.com/es-es/library/cc164322\(v=exchg.65\).aspx](http://technet.microsoft.com/es-es/library/cc164322(v=exchg.65).aspx)
- Exchange 2007:  
[http://technet.microsoft.com/es-es/library/aa996719\(v=exchg.80\).aspx](http://technet.microsoft.com/es-es/library/aa996719(v=exchg.80).aspx)
- Exchange 2010:  
[http://technet.microsoft.com/es-es/library/aa996719\(v=exchg.141\).aspx](http://technet.microsoft.com/es-es/library/aa996719(v=exchg.141).aspx)
- Exchange 2013  
[http://technet.microsoft.com/es-es/library/aa996719\(v=exchg.150\).aspx](http://technet.microsoft.com/es-es/library/aa996719(v=exchg.150).aspx)
- Exchange 2016  
[https://technet.microsoft.com/es-es/library/aa996719\(v=exchg.160\).aspx](https://technet.microsoft.com/es-es/library/aa996719(v=exchg.160).aspx)

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

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

- Microsoft Exchange Server 2010 included in Windows SBS 2011
- Microsoft Exchange Server 2013 Standard
- Microsoft Exchange Server 2013 Enterprise
- Microsoft Exchange Server 2016 Standard
- Microsoft Exchange Server 2016 Enterprise

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

- Mailbox
- Hub Transport
- Edge Transport

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

- Mailbox

Operating systems supported:

- Exchange 2003: Windows Server 2003 (32-bit) SP1+ and Windows Server 2003 R2 (32-bit)
- Exchange 2007: Windows Server 2003 (64-bit) SP1+, Windows Server 2003 R2 (64-bit), Windows 2008 (64-bit) and Windows 2008 R2
- Exchange 2010: Windows 2008 (64-bit) and Windows 2008 R2
- Exchange 2013: Windows Server 2012 and Windows Server 2012 R2
- Exchange 2016: Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.

## 9.5. Installing the protection on Linux computers

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

### 9.5.1 Internet access requirements

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

- <http://pcoplinox.updates.pandasecurity.com/updates/nanoupdate.phtml>
- [http://pcoplinox.downloads.pandasecurity.com/nano/pavsignano/nano\\_1/](http://pcoplinox.downloads.pandasecurity.com/nano/pavsignano/nano_1/)

### 9.5.2 Hardware and software requirements

#### Supported distributions

- Ubuntu (32-bit and 64-bit), version 12 or later

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

### Prerequisites

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

- The "lsb\_release" utility must be installed (on RedHat and Debian).
  - On Debian, download and install the following package:  
`lsb-release_3.2-23.2squeeze1_all.deb`
  - On RedHat, download and install the following package:  
`redhat-lsb.i686`
- **PavSL protection dependencies (all distributions)**  
The PavSL protection requires the installation of the following libraries to work properly:
  - `libsoup-2.4.so.1` (HTTP client/server library for GNOME)
  - `libgthread-2.0`
  - `libmcrypt.so.4` (MCrypt - encryption functions)
  - `libz.so.1` (zlib compression and decompression library)
- Make sure the `/opt/PCOPAgent/PCOPScheduler/pavsl-bin/` directory contains all the PavSL protection dependencies
- The AT/CRON services must be properly installed and enabled (in all distributions) Make sure the AT and CRON services are properly installed and enabled in the system services.
- The `whiptail` command must be available to run the proxy configuration script.

## 9.6. Installing the protection on Mac OS X computers

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

### 9.6.1 Internet access requirements

In addition to the URLs listed in the Windows section, the following URLs must be accessible to the Linux agent:

- `mp-agents-inst.pandasecurity.com` (OS X systems)
- `mp-agents-sync.pandasecurity.com` (OS X systems)
- `mp-agents-async.pandasecurity.com` (OS X systems)
- `http://www.intego.com` (OS X systems)
- `ttp://www.integodownload.com` (OS X systems)

- <http://www.netupdate2.intego.com> (OS X systems)
- <https://www.netupdate2.intego.com> (OS X systems)

## 9.6.2 Hardware and software requirements

Supported operating systems

**Adaptive Defense 360** supports the following OS X operating systems:

- Mac OS X 10.6 Snow Leopard (Intel Core 2 Duo processor or better)
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite
- Mac OS X 10.11 El Capitan
- MacOS Sierra 10.12

### Hardware

- Processor: Intel® Core 2 Duo
- Hard Disk: 1.5 GB free space

## 9.7. Installing the protection on Android devices

**Adaptive Defense 360** can be installed on Android devices manually by downloading the installer from the Web console, emailing the download URL to end users, or using an Android for Work compatible EMM solution.

Installing the protection manually through a download URL has the peculiarity that, once **Adaptive Defense 360** has been installed on the Android device, it is necessary to take the additional step of adding the Android device to a computer group in the **Adaptive Defense 360** Web console.

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

### Installing the protection by sending the download URL

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

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

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

Once the protection has been installed, it will be necessary to open **Adaptive Defense 360** from the

device and click the second URL included in the email.

### Installing the protection from the Web console

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

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

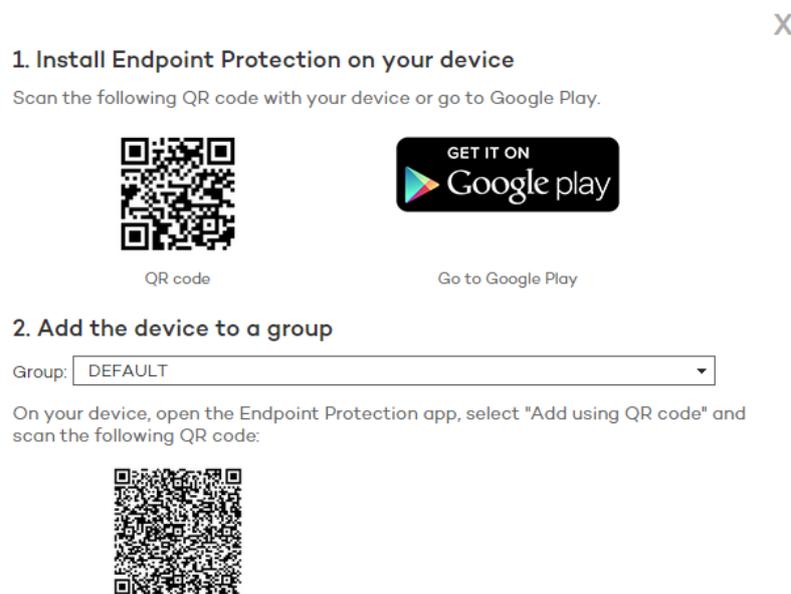


Figure 29: Android agent install window

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

### Installing the protection from an Android for Work compatible EMM tool

EMM (Enterprise Mobility Management) tools are used to, among other things, install apps, track, locate and manage mobile devices, and sync files on a device with those on a server.

All operations are performed remotely regardless of the carrier or service provider.

In the case of Adaptive Defense 360, you can use an Android for Work compatible EMM tool to install the app and integrate it into the Android devices to protect.

To do that, you'll have to configure the following two parameters in your EMM tool:

- Integration URL

Enter the URL displayed in the install window (in **Generate installation URL**), after selecting the group that you want to integrate the device into:

- **Automatic name**

The name assigned to the device will be different depending on the option you select (True or False). The default option is False.

- True

If you select this option, a name will be automatically assigned to the device. This name will be the one displayed in the **Adaptive Defense 360** Web console, and will have the following format:

```
<Device model>_<unique identifier>
```

- False

In this case, you will have to enter the name that you want to assign to the device.

- **Download the Adaptive Defense 360 app**

You can download the app here:

<https://play.google.com/store/apps/details?id=com.pandasecurity.pcop>

### 9.7.1 Internet access requirements

In addition to the URLs listed in the Windows section, the following URLs must be accessible to the Android agent:

- <https://dmp.devicesmc.pandasecurity.com>
- <https://pcopsupport.pandasecurity.com>
- <https://rpuws.pandasecurity.com>
- <https://rpkws.pandasecurity.com/kdws/sigs>
- <http://iext.pandasecurity.com/ProylEXT/ServletExt>

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

### 9.7.2 Hardware and software requirements

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

## 9.8. Introduction to installation using image generation

In networks made up of very homogeneous or virtual 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 users may need, including security tools. Once ready, a copy of the computer's hard disk is extracted which is then copied to the others computers on the network, substantially reducing deployment times.

If the network administrator uses this automated deployment procedure and **Adaptive Defense 360** is part of the base image, it will be necessary to take some additional steps for the procedure to be successful.

Installing the **Adaptive Defense 360** local protection on a computer entails automatically assigning a unique ID to it. This ID will be used by Panda Security to show and refer to the computer in the management console. If, later, a golden image is generated with the **Adaptive Defense 360** local protection already installed on it, and the image is then cloned to other computers, every computer that receives the image will inherit the same **Adaptive Defense 360** ID and, consequently, the console will only display a computer.

To avoid this, delete the generated ID with the program `reintegra.zip`, which can be downloaded from Panda Security's support website:

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

Refer to the above page for specific instructions on how to install the **Adaptive Defense 360** agent on a golden or master image.

### 9.9. Uninstalling the protection

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

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

Table 2: **Adaptive Defense 360** uninstall methods per platform

### 9.9.1 Local uninstall

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



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

#### On Windows 8 and later:

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

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

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

#### On Windows XP:

- Control Panel > Add or remove programs.

#### On OS X:

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

#### On Android devices:

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

### 9.9.2 Uninstalling the protection using the centralized distribution tool



*This option is only available for Windows computers.*

In the Web console main window, click **Installation**. Then, click **Uninstallation** in the menu on the left. Select **Centralized uninstallation**.

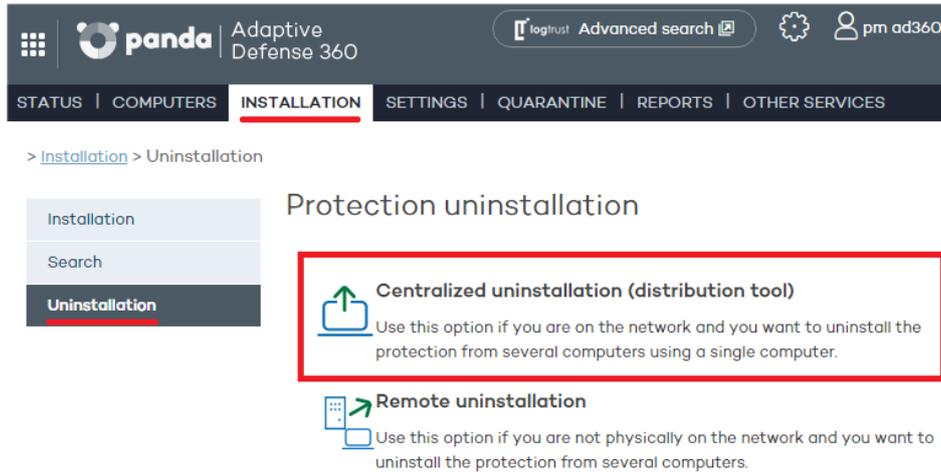


Figure 30: Accessing the centralized uninstall tool

 Refer to Appendix 1: Centralized installation tools for more information

### 9.9.3 Uninstalling the protection from the management console

 This option is only available for Windows computers

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

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

#### Creating a remote uninstall task

- In the Web console main window, click Installation and then Uninstallation in the menu on the left.
- Select Remote uninstallation.

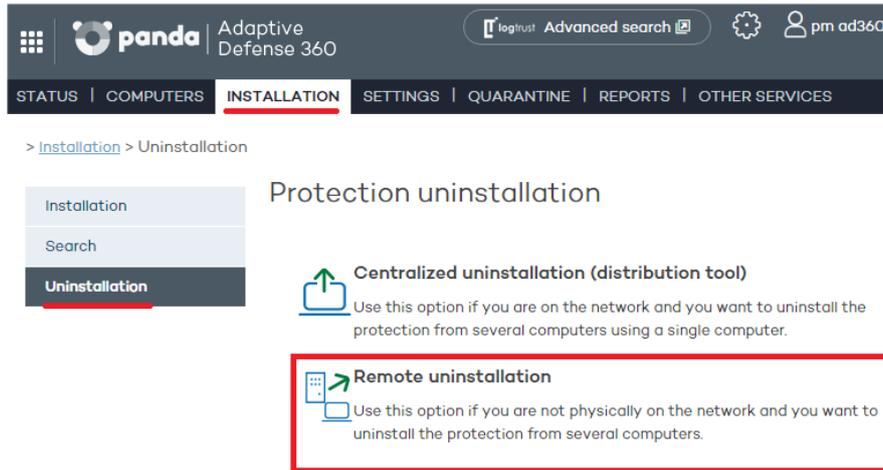


Figure 31: Remote uninstall window

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

- To configure a new uninstall task, click **New uninstallation**. Then, in the **Edit uninstallation** window, name the task and select the group that contains the computers whose protection will be uninstalled. The groups displayed will be those on which you have permissions.
- If the selected group has a configuration profile for which an uninstall password has been set, enter it in the **Password** field.
- Select the computers from the computer list displayed on the **Available computers** tab, and click **Add**. After you select them, they will appear on the **Selected computers** tab.

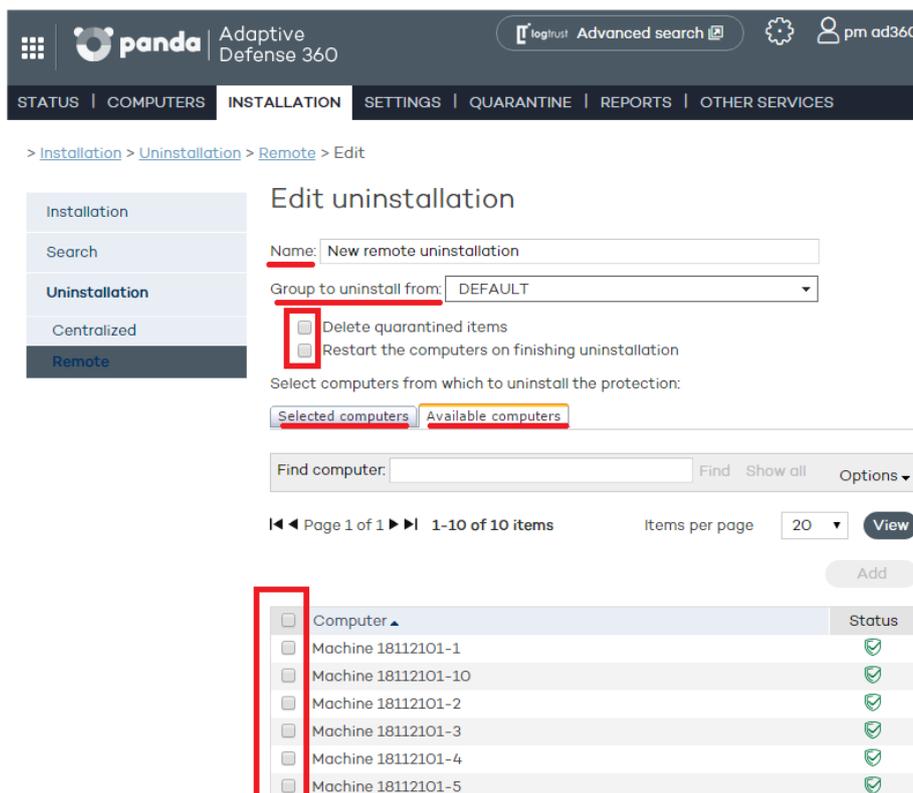


Figure 32: Selecting the computers whose protection will be uninstalled

### Viewing remote uninstall tasks and their results

Uninstall tasks are listed in the **Remote uninstallation** window. To remove them, use the **Delete** button.

The information on this screen is organized into the following columns:

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

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

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

### Remote uninstall results

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

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

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

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

### Incompatibility between searches for unprotected computers and remote uninstall tasks

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

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

# 10. Updating the protection

---

Updating the protection on Windows systems

Updating the protection on Linux systems

Updating the protection on Mac OS X systems

Updating the protection on Android systems

## 10.1. Introduction

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

The components installed on users' computers are the following:

- Communications agent
- Protection engine
- Signature file

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

Module	Platform			
	Windows	Linux	Mac OS X	Android
Communications agent	On demand			
Protection	Automatic and configurable	Local	Automatic	Automatic
Signature file	Automatic and configurable	Automatic	Automatic	Automatic

Table 3: Updates types per platform

- **Automatic and configurable:** Updates can be configured through the console and deployment is remote.
- **Automatic:** Updates cannot be configured but deployment is remote.
- **Local:** Updates are performed manually or using third-party centralized distribution tools.
- **On demand:** The administrator can launch the update whenever appropriate, provided there is an update available. They can also postpone them as long as they want.

## 10.2. Updating the communications agent

The communications agent update process is the same for all platforms. Updates are pushed from the Notifications area in the management console.

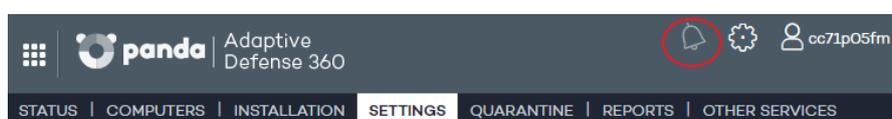


Figure 33: Accessing the **Notifications** area

When a new version is available, a notification is displayed prompting the administrator to update the agent module across all computers with **Adaptive Defense 360** installed.

### 10.3. Updating the protection on Windows systems

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

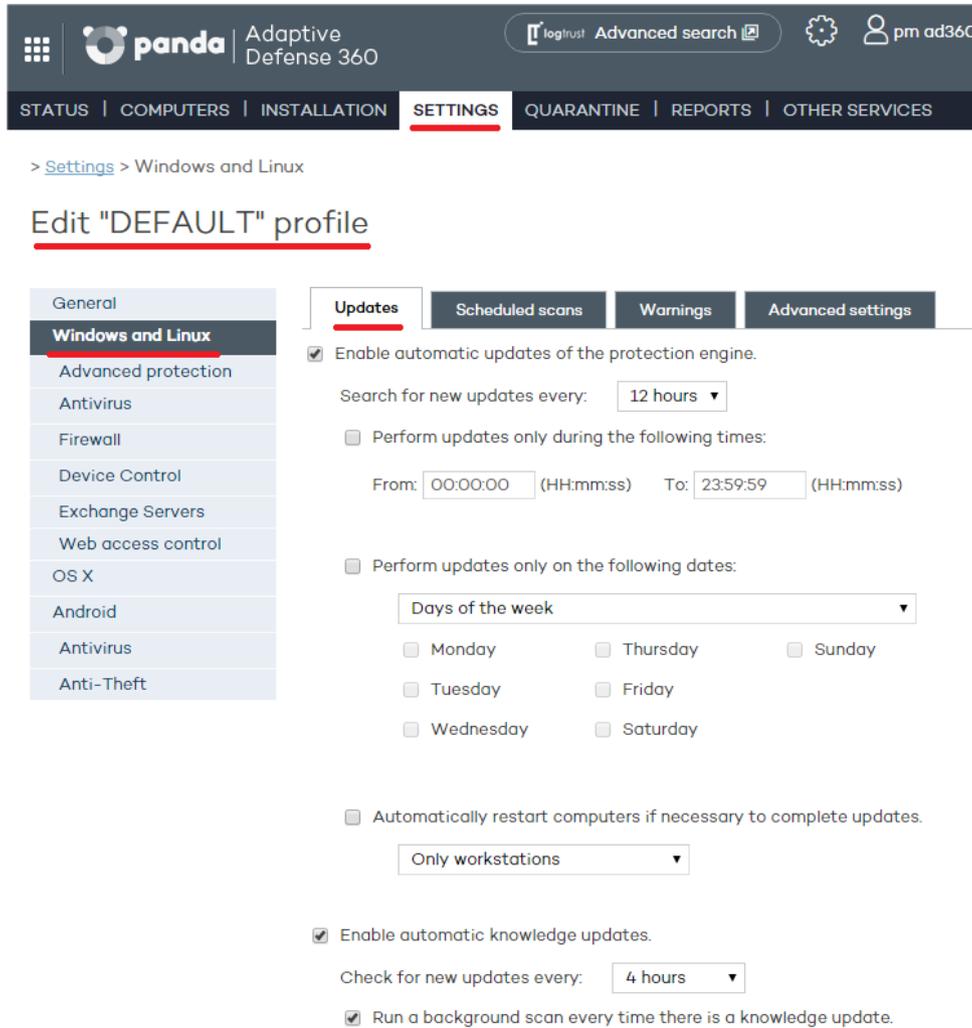


Figure 34: Accessing the Updates window

#### 10.3.1 Updating the protection

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



Figure 35: Configuring the protection update frequency

- You can also select a date and time for the automatic updates to take place. Select the day(s) of the week for updates to occur.

Perform updates only on the following dates:

Days of the week ▼

Monday       Thursday       Sunday  
 Tuesday       Friday  
 Wednesday       Saturday

Figure 36: Configuring the day of the week for updates to occur

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

Perform updates only on the following dates:

Days of the month ▼

First day:  Last day:

Figure 37: Configuring the day of the month for updates to occur

- A date range for updates to take place.

Perform updates only on the following dates:

On the following days ▼

From:  To:

**September, 2015**

Su	Mo	Tu	We	Th	Fr	Sa
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Today: September 2, 2015

Automate updates necessary to complete updates.  
 ▼  
 Enable automatic restarts  
 Check for new updates every  days ▼  
 Run a backup before updates. There is a knowledge update.

Figure 38: Configuring a date range for updates to take place

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

- Indicate which computer families must be automatically restarted after an update.
- Additionally, you can set the time interval at which to perform updates.

Perform updates only during the following times:

From:  (HH:mm:ss) To:  (HH:mm:ss)

Figure 39: Configuring a time interval for updates to take place

### 10.3.2 Updating the signature file

- Select the option to enable the automatic updates feature.
- Use the drop-down menu to select the frequency to search for updates.

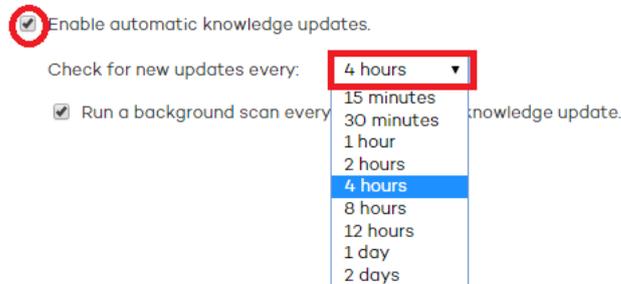


Figure 40: Configuring the frequency for querying the cloud for signature file updates



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

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

### 10.3.3 Peer-to-Peer or rumor functionality

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

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

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

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

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

```

WALUPD.ini
[GENERAL]
UPDATE_FROM_LOCAL_NETWORK=1
WALUPG.ini
    
```

[ GENERAL ]

UPGRADE\_FROM\_LOCAL\_NETWORK=1

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

- **The P2P functionality works as follows:**

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

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

This process is illustrated in the following diagram:

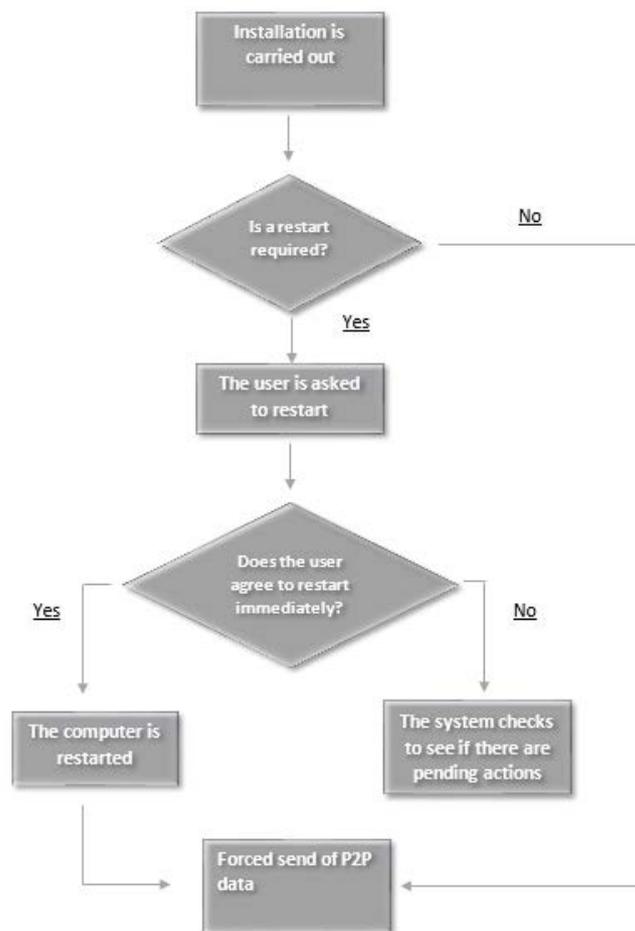


Figure 41: Rumor technology operation diagram

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

If a computer needs a file, it will first check whether another computer on the network has it before downloading it from the Internet. If so, it will request the file from the other computer. The file will be

received asynchronously and there is a maximum time that must elapse before retrying.

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

## 10.4. Updating the protection on Windows Server Core systems

Since Windows Server Core systems don't have a graphical user interface, we advise that you update **Adaptive Defense 360** in a scheduled way. At the end of the update process it is necessary to restart the server to complete the update successfully, however, due to the absence of a graphical interface, the local console won't display any restart notifications and the update might not be completed.

Therefore, we advise that you schedule the update and check the Web management console to make sure the server has been restarted and the update has been correctly installed.

## 10.5. Updating the protection on Linux systems

### 10.5.1 Updating the protection

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

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

### 10.5.2 Updating the signature file

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

## 10.6. Updating the protection on Mac OS X systems

### 10.6.1 Updating the protection

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

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

### 10.6.2 Updating the signature file

In the case of OS X computers, it is not possible to configure the frequency of the automatic updates

of the signature file. It is updated every hour.

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

## 10.7. Updating the protection on Android systems

### 10.7.1 Updating the protection

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

### 10.7.2 Updating the signature file

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

# 11. Groups

---

Computer tree

Group types

Creating a manual group

Creating an automatic group arranged by IP  
address

Creating an automatic group based on Active  
Directory

Adding a computer to a group

Creating and deleting a group

Group restrictions

## 11.1. Introduction

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

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

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

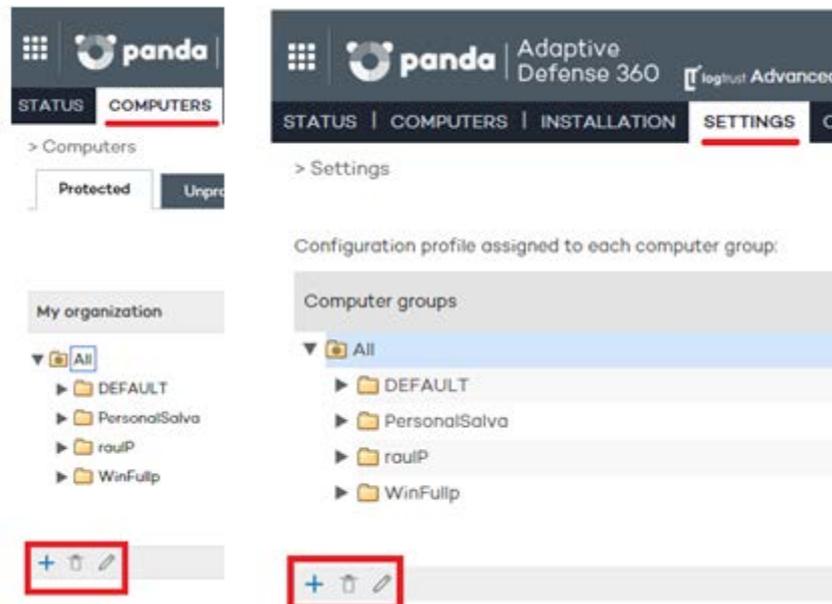


Figure 42: Group creation from the Computers and Settings windows

### 11.1.1 Assigning computers to groups

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

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

## 11.2. Computer tree

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



Figure 43: Computer tree

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

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



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

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

### 11.3. Group types

#### Manual groups

They are identified in the console with the  icon.

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

#### Automatic groups arranged by IP address

They are identified in the console with the  icon.

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

#### Automatic groups based on Active Directory

They are identified in the console with the  icon.

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

### 11.4. Creating a manual group

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

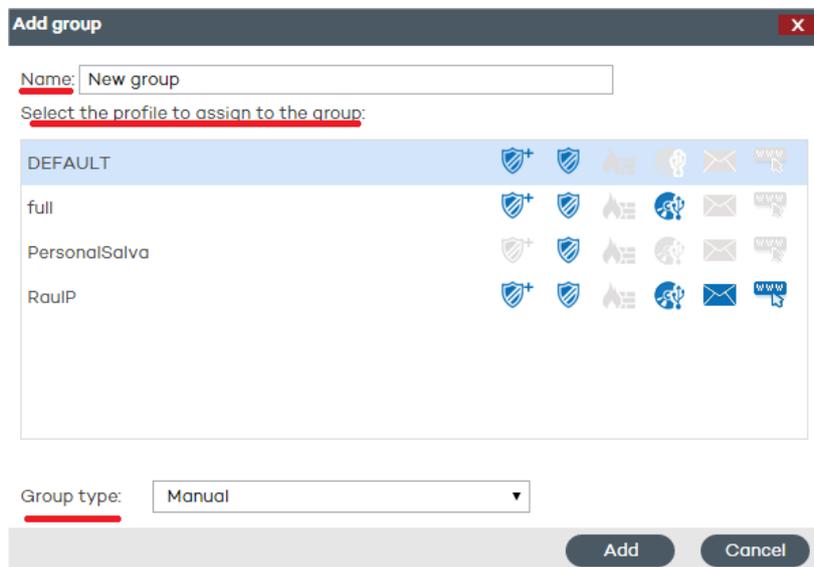


Figure 44: Group creation window

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



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

- Select the Group type: Manual.

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

### 11.5. Creating an automatic group arranged by IP address

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

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

the automatic rules to apply to the group.



Figura 45: Controls for editing an automatic group arranged by IP address

Click the  icon to display the rule creation window.

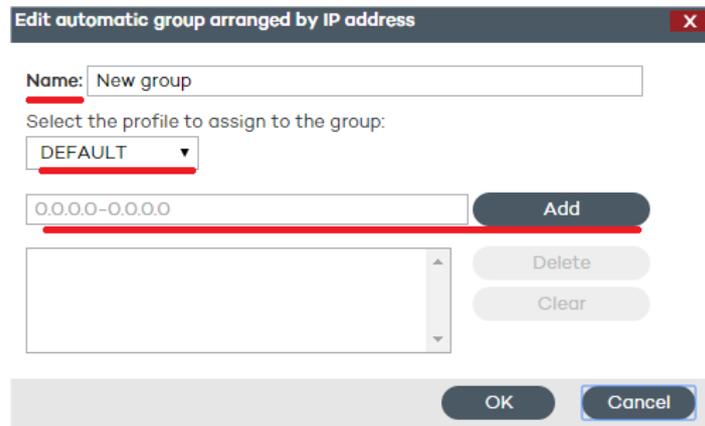


Figure 46: Group edit window

There, you will have to specify:

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

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

### 11.5.1 Importing rules from a .CSV file

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

#### Format of the .CSV file to import

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

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

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

```
\Hall of Justice           HoJustice
```

#### Other examples:

```
\Hospital\EmergencyRoom\Ambulance1      10.10.10.10-10.10.10.19
\Hospital\EmergencyRoom
\Hospital\EmergencyRoom\Ambulance2      10.10.10.20-
10.10.10.29      AmbulanceP
\Hospital\Areilza Clinic      10.10.20.10/22      ClinicProfile
\Hall of Justice\Court of Appeals      10.10.50.10/12      Justice2
```

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



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

### 11.5.2 How automatic groups arranged by IP address work

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

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

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

## 11.6. Creating an automatic group based on Active Directory

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

### 11.6.1 Automatic replication of the Active Directory structure

The process of generating and updating subgroups in an automatic group based on Active

Directory takes place automatically for every computer that is assigned to that type of group. The action sequence is the following:

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

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

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



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

### 11.6.2 Manual replication of the Active Directory structure

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

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

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



Figure 47: Editing a group based on Active Directory

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

The file to import must have the following format:

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

Example of a .CSV file:

```

activedirectory.org      ProfileName
activedirectory.org\Domain Controllers      ProfileName
activedirectory.org\Computers ProfileName
activedirectory.org\OrganizationalUnit1     ProfileName
activedirectory.org\OrganizationalUnit1\Department1 ProfileName
activedirectory.org\OrganizationalUnit1\Department2 ProfileName
    
```

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

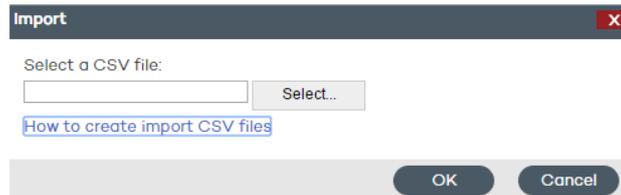


Figure 48: CSV file selection window

### 11.6.3 Viewing a computer's Active Directory path information

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

#### Computer details

- Name:
- IP address:
- Domain:
- Active Directory path:
- Group:
- Installation date:
- Protection version:
- Agent version:
- Knowledge update:
- Last connection:
- Operating system:
- Mail server:
- Comment:

Figure 49: Computer details window

## 11.7. Adding a computer to a group

### 11.7.1 Manual integration

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

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

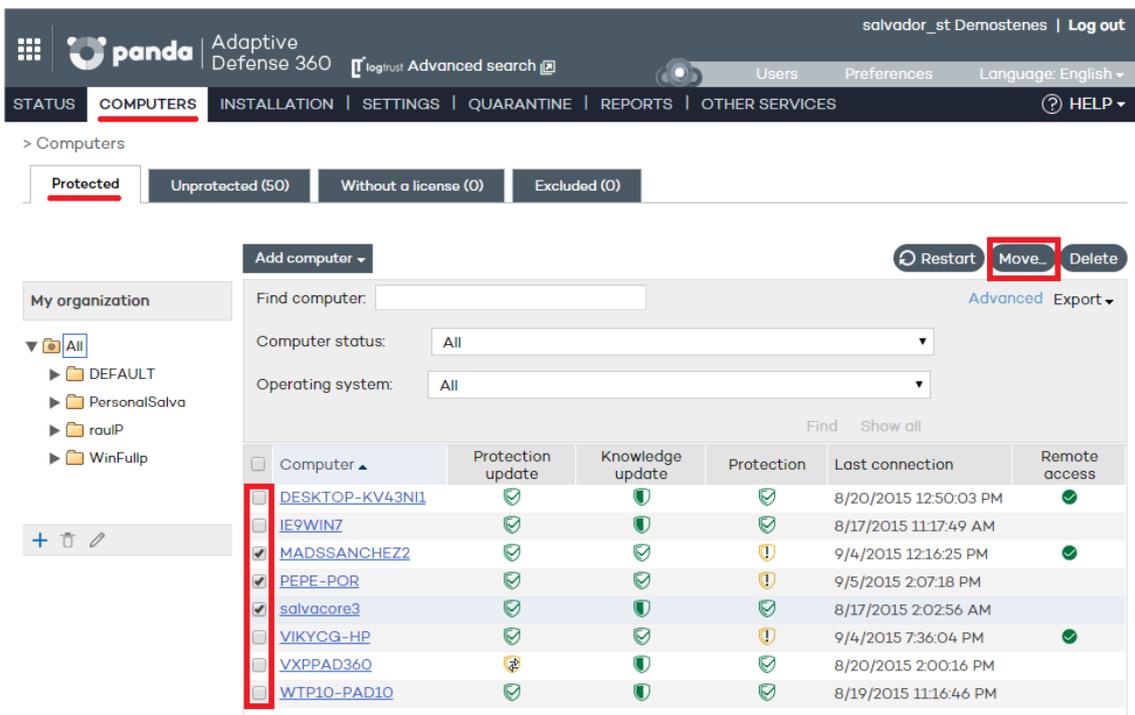


Figure 50: Selecting computers to move

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

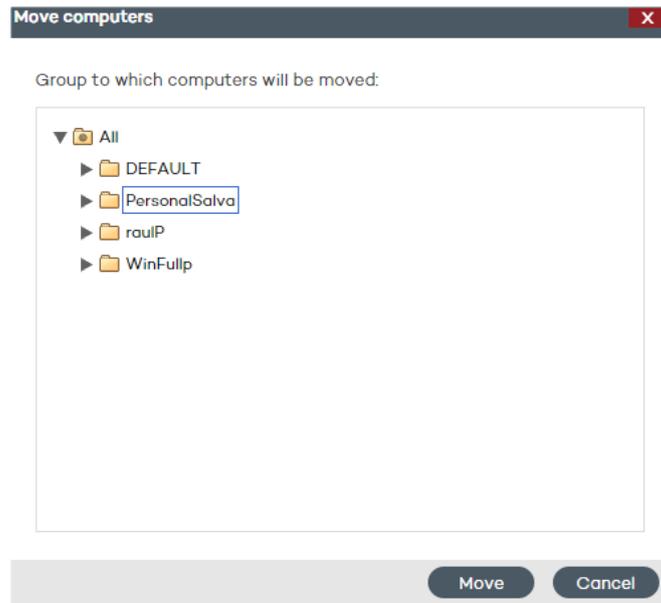


Figure 51: Target group selection window

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

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

### 11.7.2 Adding a computer to a group during installation

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

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

## 11.8. Creating and deleting a group

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

### Editing a manual group

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

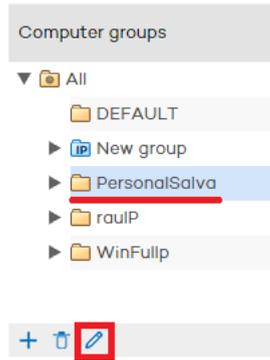


Figure 52: Editing a group

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

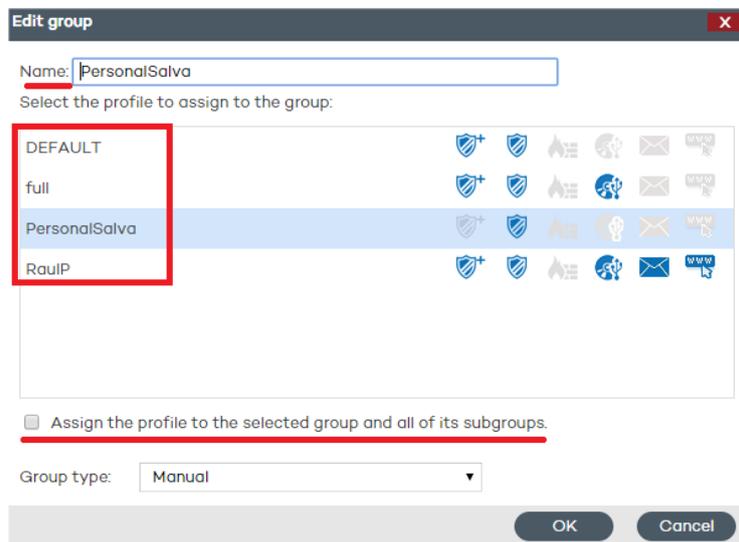


Figure 53: Group edit window

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

### Editing an automatic group arranged by IP address

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

The first case is identical to editing a manual group. To edit subgroups, click the **Edit group** button in the group edition window. The window that opens will display the IP address rules and the subgroups associated with the automatic group.

### Editing an automatic group based on Active Directory

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

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



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

### Deleting a group

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

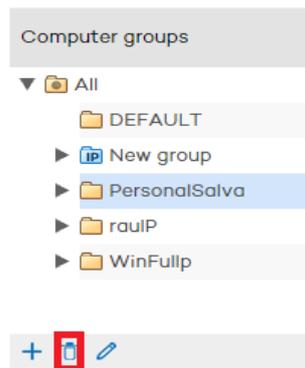


Figure 54: Deleting a group

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

## 11.9. Group restrictions

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



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

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

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

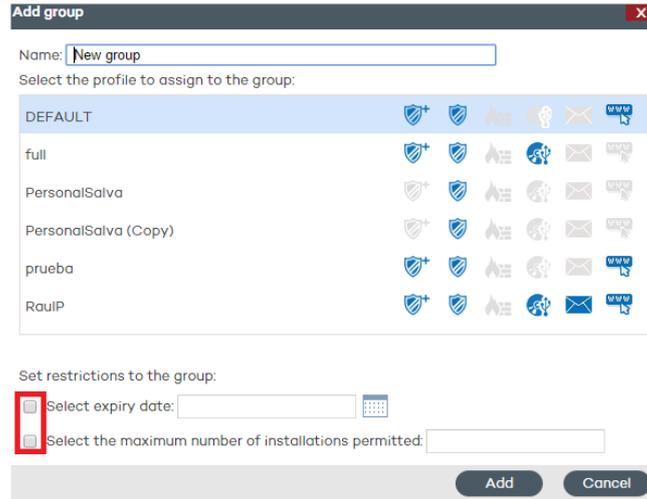


Figure 55: Settings displayed upon selecting **Group restrictions**

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

# 12. Protection profiles

---

Network protection overview and planning  
Creating and managing protection profiles  
Protection profile general settings

## 12.1. Introduction

This chapter provides an introduction to the configuration of security profiles, also called protection profiles, or simply profiles.

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

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

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

## 12.2. Network protection overview and planning

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

### 1. Define the company's security policy

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

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

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

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

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

Table 4: Protection features per supported platform

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

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

Table 5: Protection features per supported server platform

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

## 2. Create a list of all the corporate devices to protect

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

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

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

## 4. Group computers based on their common security requirements

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

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

### 5. Create security profiles

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

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

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

### 6. Assign security profiles to groups

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

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

## 12.3. Creating and managing protection profiles

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

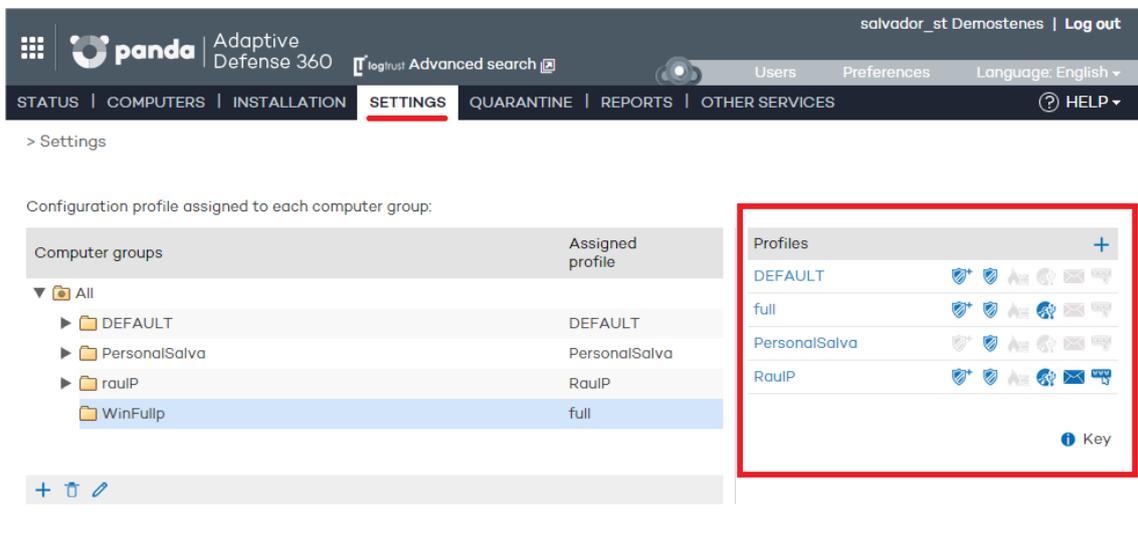


Figure 56: Accessing protection profiles

### 12.3.1 Creating a protection profile

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

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

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



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

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

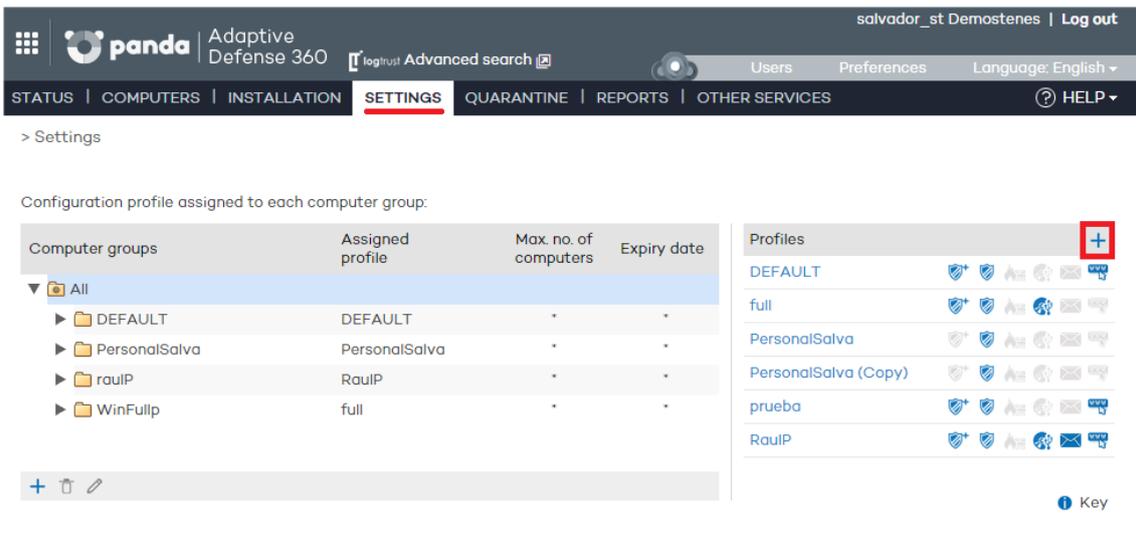


Figure 57: Accessing the security profile creation window

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

### 12.3.2 Copying protection profiles

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

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

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

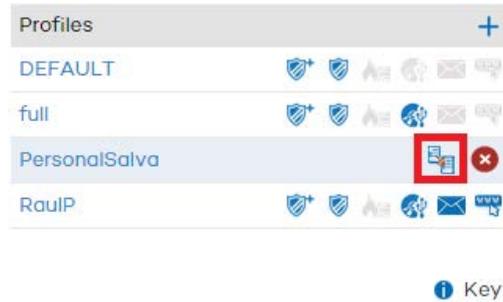


Figure 58: Copying a security profile

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

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

Profile copying is subject to the permissions that you have.

### 12.3.3 Deleting a protection profile

Click the  icon to delete the selected profile.

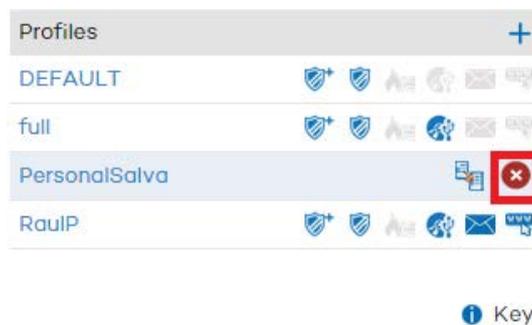


Figure 59: Deleting a security profile

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

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

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

## 12.4. Protection profile general settings

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

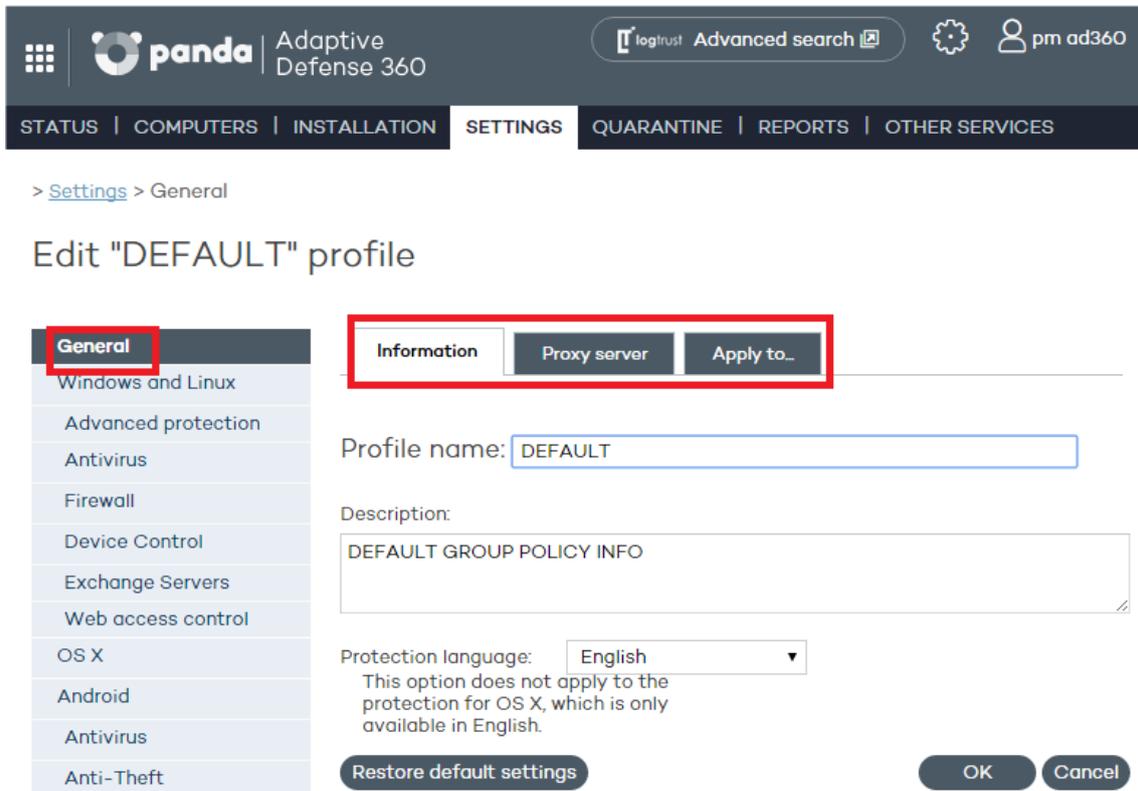


Figure 60: Accessing a protection profile's general settings

The general settings are divided into three tabs:

### Information tab

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

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

### Proxy server tab

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

 In the case of roaming computers with a proxy server configured in their protection profile, or in the event that the proxy server becomes temporarily unavailable, the agent will try to connect to the Internet through other available means.

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

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

### **Apply to... tab**

This tab displays a list of the groups that the profile is applied to.

# 13. Windows protection profiles

---

General settings

Configuring the advanced protection

Configuring the antivirus protection

Configuring the firewall and intrusion detection  
features

Configuring the device control feature

Configuring the protection for Exchange servers

Configuring the Web access control

### 13.1. Introduction

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

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

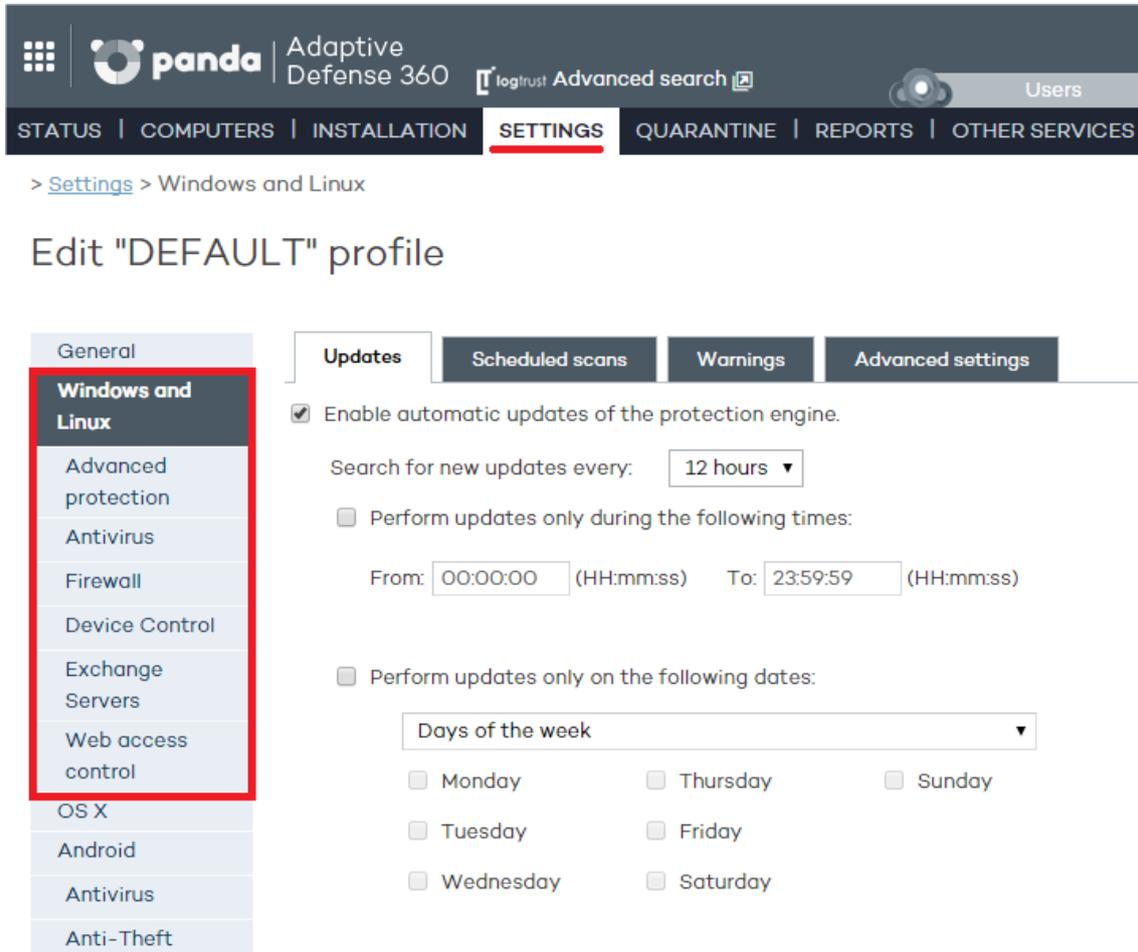


Figure 61: Accessing a protection profile's settings sections

### 13.2. General settings

Click **Windows and Linux** in the side menu. A window will be displayed with four tabs to configure the protection's behavior with respect to updates, scheduled scans and alerts, as well as advanced installation and connectivity settings.

#### Updates

Refer to Chapter 10 Updating the protection for more information about updates.

#### Scheduled scans

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

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

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

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

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

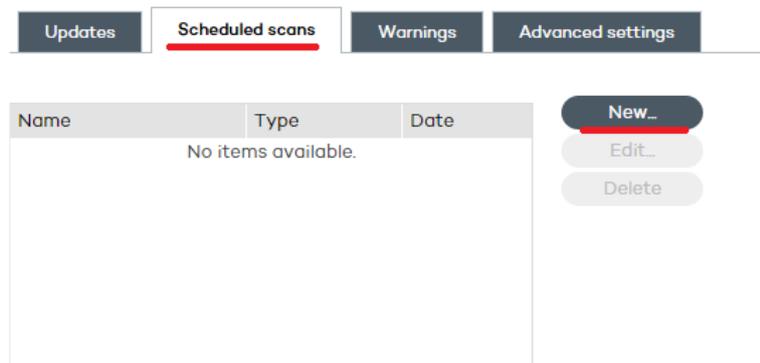


Figure 62: Creating a new scheduled scan

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

#### Examples

`\\computer\folder`

`*c:\folder1\folder2`

The permission that you have will dictate whether or not you can define specific paths to scan. The maximum number of paths to scan for each profile is 10.

- Click the **Advanced settings** option to access a window where you will be able to configure additional aspects of scheduled scans:
  - Select the relevant checkbox to scan compressed files.
  - Select the malicious software you want to scan for. The option to scan viruses will always be enabled.
  - You can scan the entire computer or exclude certain folders or files with specific extensions from the scans. In the latter case, use the **Add**, **Delete** and **Clear** buttons to define the list of exclusions.

## Alerts

This section lets you configure the two types of alerts by the **Adaptive Defense 360** software:

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



Figure 63: Local alerts settings

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

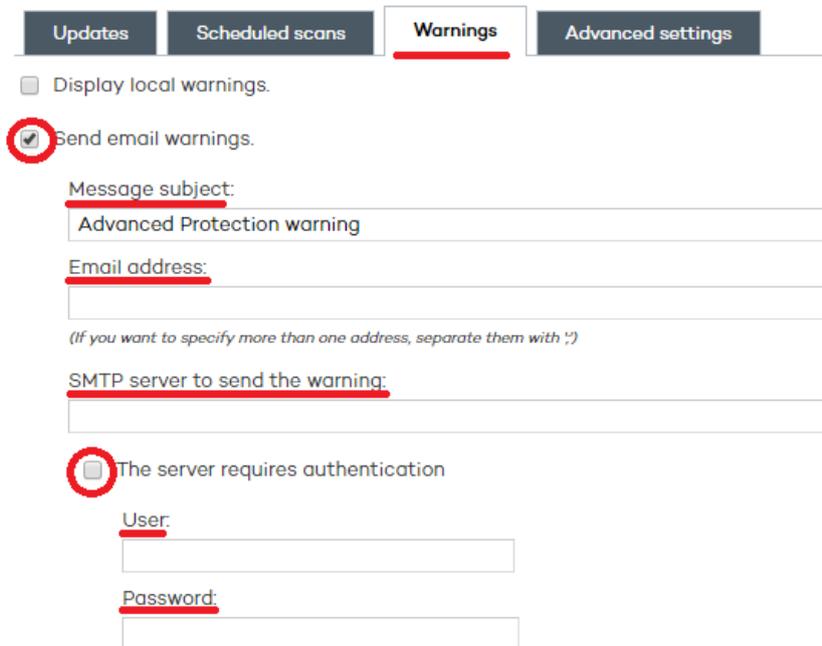


Figure 64: Email alerts settings

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

- **From:** Allows you to indicate the source email address of the alert. This address must belong to a mailbox managed by the mail server specified below or, at least, be accepted by the configured mail server in order to be forwarded by it. If the 'From' email address is left blank,

the alert will be sent from the following address: `computer_name@panda.local`

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

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

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

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

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

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

## Advanced settings

Here you can configure aspects related to the installation of the protection on computers, as well as the connection of these computers to the Internet and to the **Adaptive Defense 360** servers.

You can also configure options related to the suspicious file quarantine.

- **Installation:** Specify in which directory you want to install the protection.
- **Automatically uninstalling other security products:** You can specify if you want **Adaptive Defense 360** to uninstall any existing third-party security product from your computers, or if you prefer both products to coexist. Refer to Chapter 9 Installing the protection for more information.
- **Connection to Collective Intelligence:** This option allows you to disable scans with Collective

Intelligence. It is advisable to keep this option enabled if you want to benefit from the detection power provided by Collective Intelligence.

- **Server connection settings:** Establish how often you want computers to send information to the **Adaptive Defense 360** servers about the status of the protection installed. This must be a value between 12 and 24 hours.
  - Centralize server communication through the following computer: Specify the computer through which connections with the **Adaptive Defense 360** server will be centralized. To do that, select the relevant checkbox and click Select. In the Select computer window, choose a computer or search for it using the Find button. Then click OK.
- **Quarantine settings:** Lets you indicate the path on the user's computer where items restored from Quarantine will be sent to.
- **Administrator password:** The administrator password allows you to uninstall and configure the local protection in administrator mode. That is, it allows you to uninstall **Adaptive Defense 360** from the network computers, or allow end users themselves to enable or disable their protection from the **Adaptive Defense 360** local console. These options are not mutually exclusive, so you can select both at the same time.

### 13.3. Configuring the advanced protection

The advanced protection lets you establish different operating modes to block unknown malware, and protect computers against APTs, advanced threats, and malicious programs designed to take advantage of software vulnerabilities (exploits) in order to infect systems.

#### 13.3.1 Behavior

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

#### 13.3.2 Anti-exploit

The anti-exploit protection blocks, automatically and without user intervention in most cases, all attempts to exploit the vulnerabilities found in the processes with programming bugs installed on

users' computers.

### How does the anti-exploit protection work?

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

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

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

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

- **Automatic exploit blocking**

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

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

- **Exploit detection**

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

Regardless of the time elapsed between when the exploit was detected and when the compromised process is ended, **Adaptive Defense 360** will indicate that the computer was at risk, although, obviously, the risk will actually depend on the time that passed until the process was stopped. **Adaptive Defense 360** can end compromised processes automatically to minimize the negative effects of an attack, or ask the user for permission to do so.

This will allow the user to, for example, save their work or critical information before the compromised process is terminated or their computer is restarted.



*It is advisable to select the option to end compromised processes automatically in order to minimize the impact of exploit attacks*

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

### Anti-exploit protection settings

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



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

### 13.3.3 Exclusions



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

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

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

### 13.3.4 Network usage

Every executable file found on users' computers that is not recognized by **Adaptive Defense 360** will be sent by the agent to our server for analysis. This is configured to have no impact on the

performance of the customer's network (the maximum number of MB that can be transferred in an hour per agent is set by default to 50). Unknown files are sent only once for all the customers using **Adaptive Defense 360**. Additionally, bandwidth management mechanisms have been implemented in order to minimize the impact on the customer's network.

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

### 13.3.5 Privacy

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

## 13.4. Configuring the antivirus protection

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

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

- **Files identified as malware when disinfection is possible**

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

- **Files identified as malware when disinfection is not possible**

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

### Files

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

- Select **Enable permanent file protection**.
- If you want the protection to scan compressed files, select the relevant checkbox.
- Select the malicious software to detect.
  - **Viruses**: Programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly destructive and irreparable.
  - **Hacking tools and PUPs**: Programs that can be used by a hacker to carry out actions that cause problems for the user of the affected computer.



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

Next, select the behavioral detection technologies:

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

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

## Mail

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

- Enable the permanent mail protection, and select the option to scan compressed files.
- Select the malicious software to detect by ticking the relevant checkboxes.
  - **Viruses**
  - **Hacking tools and PUPs**
  - **Suspicious items**
  - **Phishing:** A technique for obtaining confidential information fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

If you want to exclude files with certain extensions from the scans, click **Advanced settings**. This will take you to the **Exclusions** window.



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

## Web

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

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

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



*The virus detection option will always be enabled.*

## 13.5. Configuring the firewall and intrusion detection features

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

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

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

- **Firewall in user mode**

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

This will allow end users to access the firewall settings from the agent installed on their computer.

- **Firewall in administrator mode**

Keep the default option selected (**Apply the following settings to the firewall**), if you want to centrally configure the firewall protection from the Web console. Indicate whether the configuration will be applied to Windows workstations and/or Windows servers.

## General

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

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

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

## Programs

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

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

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

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

2. **Click the Add button to define the way a specific application should behave:**

- **Allow inbound and outbound connections:** The program can connect to the Internet/local network and allows other programs or users to connect to it. There are certain types of programs that need these permissions to work correctly: file swapping programs, chat applications, Internet browsers, etc.
- **Allow outbound connections:** The program can connect to the Internet/local network, but does not accept external connections from other users or applications.
- **Allow inbound connections:** The program accepts connections from programs or users from the Internet/local network, but it will not have outbound permissions to connect.
- **No connection:** The program cannot connect to the Internet or the local network.

## Intrusion prevention

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

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

- **IP explicit path:** Rejects IP packets with an explicit source route field. These are IP packets that are not routed based on their target IP address, but the routing information is defined beforehand.
- **Land Attack:** Stops denial-of-service attacks by TCP/IP stack loops by detecting packets with identical source and destination addresses.
- **SYN flood:** This attack launches TCP connection attempts massively to force the targeted computers to commit resources for each connection. The protection establishes a maximum number of open TCP connections to prevent the computer under attack from becoming saturated.
- **TCP Port Scan:** Detects if a host tries to connect to several ports in a specific time period. It blocks the attack preventing replies to the suspicious host. In addition, it filters the replies so the sender doesn't even get closed port replies.
- **TCP Flags Check:** Detects TCP packets with invalid flag combinations. It acts as a complement to the protection against port scanning by blocking attacks of that type such as "SYN&FIN" and "NULL FLAGS". It also complements the protection against OS fingerprinting attacks as many of these are based on replies to invalid TCP packets.
- **Header Lengths**

- **IP:** Rejects inbound packets with an IP header length that exceeds a specific limit.
- **TCP:** Rejects inbound packets with a TCP header length that exceeds a specific limit.
- **Fragmentation control:** Checks the status of the packet fragments to be reassembled at the destination, protecting the system against memory overflow attacks due to missing fragments, ICMP redirects masked as UDP and computer scanning.
- **UDP Flood:** Rejects UDP streams to a specific port if the number of UDP packets exceeds a preconfigured threshold in a particular period.
- **UDP Port Scan:** Protects the system against UDP port scanning attacks.
- **Smart WINS:** Rejects WINS replies that do not correspond to requests sent by the computer.
- **Smart DNS:** Rejects DNS replies that do not correspond to requests sent by the computer.
- **Smart DHCP:** Rejects DHCP replies that do not correspond to requests sent by the computer.
- **ICMP Attack:** This filter performs various checks.
  - **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:** Rejects Echo requests.
- **Smart ARP:** Rejects ARP replies that do not correspond to requests sent by the protected computer to avoid ARP cache poisoning scenarios.
- **OS Detection:** Falsifies data in replies to the sender to trick operating system detectors. It prevents attacks aimed at taking advantage of vulnerabilities associated with the operating system detected. This protection complements the TCP Flag Checker.

## System

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

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

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

1. **Set the firewall's default action (Programs tab, Default action section):**
  - **Allow access:** Allows communications for all programs with no specific rules assigned. This is the default, basic mode: all programs with no specific rules assigned can communicate with the Internet/local network.
  - **Deny access:** Denies connections for all programs with no specific rules assigned. This is an advanced mode, as it requires adding rules for every frequently used program. Otherwise,

those programs will not be allowed to communicate, affecting their performance.

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

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

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

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

### 13.6. Configuring the device control feature

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

The device control settings allow you to restrict the usage of the peripheral devices connected to your network computers.

Follow the steps below to enable the device control feature:

- Select the **Enable device control** checkbox.

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

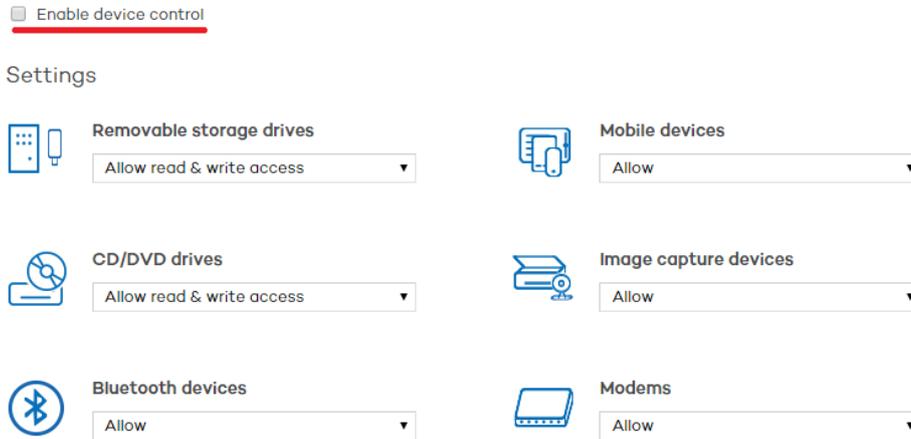


Figure 65: *Device control* feature and supported device categories

### 13.6.1 Device exclusions

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

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

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

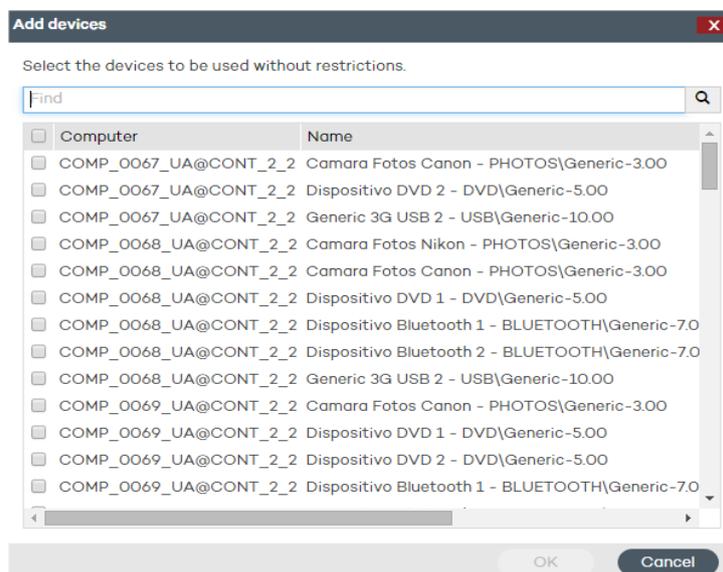


Figure 66: *List of all devices found on the network*

### 13.6.2 Exporting/importing a list of allowed devices

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

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

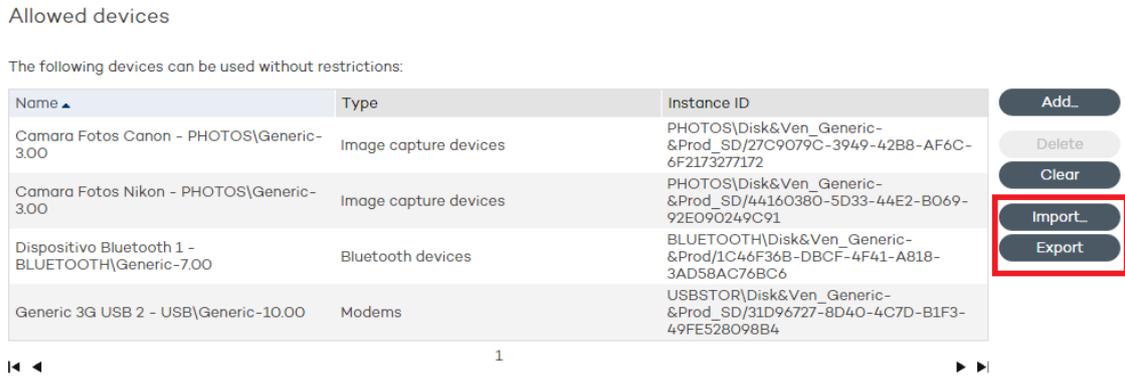


Figure 67: Buttons to **Import** and **Export** exclusion lists

### 13.6.3 Allowing blocked devices

Every time a user tries to connect an unauthorized device to their computer, **Adaptive Defense 360** will block it and log the incident in the **Detection details** section.

To view that section, go to Status > Detection origin > Devices blocked.

There, select the device that you want to allow access to, and click **Allow this device**. Next, select the protection profiles to authorize the device for. The device will be included in the list of allowed devices for all the selected profiles.

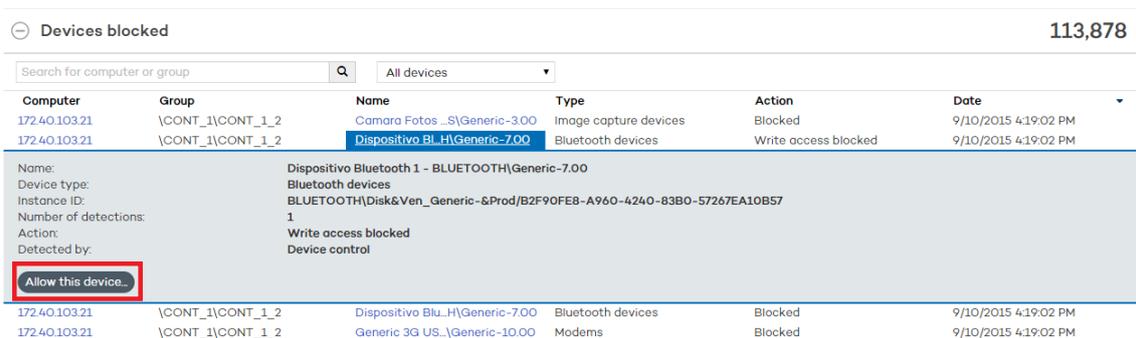


Figure 68: **Allow this device** button in the **Detection details** window

### 13.6.4 Finding a device's unique ID

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

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

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

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

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

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

### 13.6.5 Alerts

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

- Unallowed devices

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

- Read-only devices

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

## 13.7. Configuring the protection for Exchange servers

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



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

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

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

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

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

Table 5: Operating mode supported based on the Exchange version installed

- **Mailbox protection**

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



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

- **Transport protection**

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

### 13.7.1 Antivirus

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

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

- **Mailbox protection**

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

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

### 13.7.2 Anti-spam

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

### Actions to perform on spam messages

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

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

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

### Allowed/denied addresses and domains

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

Keep in mind the following aspects when configuring these lists:

- If a domain is 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.

### Content filtering

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

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



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

- **Consider files with the following extensions dangerous:** Select this checkbox to classify certain extensions as dangerous. Then, use the **Add**, **Delete**, **Clear** and **Restore** buttons to set

the list of extensions to block.

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

### Detection log

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

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

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

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

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

## 13.8. Configuring the Web access control protection

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

### Denying access to specific Web pages

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

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

**Web access restrictions**

Deny access to pages belonging to the following categories:

<input type="checkbox"/> Advertisements & Pop-Ups	<input type="checkbox"/> Alcohol & Tobacco	<input type="checkbox"/> Anonymizers
<input type="checkbox"/> Arts	<input type="checkbox"/> Business	<input type="checkbox"/> Chat
<input type="checkbox"/> Child Abuse Images	<input type="checkbox"/> Computers & Technology	<input type="checkbox"/> Criminal Activity
<input type="checkbox"/> Cults	<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites
<input type="checkbox"/> Education	<input type="checkbox"/> Entertainment	<input type="checkbox"/> Fashion & Beauty
<input type="checkbox"/> Finance	<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Gambling
<input type="checkbox"/> Games	<input type="checkbox"/> General	<input type="checkbox"/> Government
<input type="checkbox"/> Greeting cards	<input type="checkbox"/> Hacking	<input type="checkbox"/> Hate & Intolerance
<input type="checkbox"/> Health & Medicine	<input type="checkbox"/> Illegal Drug	<input type="checkbox"/> Illegal Software
<input type="checkbox"/> Image Sharing	<input type="checkbox"/> Information Security	<input type="checkbox"/> Instant Messaging
<input type="checkbox"/> Job Search	<input type="checkbox"/> Malware & Rootkits	<input type="checkbox"/> Network Errors

Deny access to pages categorized as unknown.

Figure 69: URL category list

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



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

**Denying access to pages categorized as unknown**

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



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

**List of allowed/denied addresses and domains**

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

You can edit these lists at any time.

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

**Database of URLs accessed from computers**

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

The data collected in this database is:

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

### 13.9. Configuring time periods for the Web access control feature

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

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

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

- To select whole days, click the relevant day of the week.
- To select the same time period for every day of the week, click the relevant hours.



*Bear in mind that the system will use the local time on each computer, not the server time.*

# 14. Linux protection profiles

---

General settings  
Configuring the antivirus protection

## 14.1. Introduction

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

This chapter only covers those settings supported for Linux systems.

## 14.2. General settings

### Updates

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

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

Also, in the case of Linux computers, it is not possible to configure the frequency of the automatic updates of the signature file.

### Scheduled scans

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

- Click **New** to go to the **Edit profile – New scan job window**.
- In the window that opens, enter the following data:
  - **Name**: Choose a name for the scan task.
  - **Scan type**: Select the type of scan that you want to create:
    - **Immediate scan**: Once configured, the immediate scan will take place as soon as the computer connects to the **Adaptive Defense 360** server, and the solution checks that the protection configuration has changed.
    - **Scheduled scan**: The scan will take place at the time and date you set in Start date and Start time. Use the drop-down menu to select if the scan start time refers to the **Adaptive Defense 360** server or the user's computer.
    - **Periodic scan**: Set the start date and start time, and select the scan frequency in the Repetition menu.
  - **Scan**: Select the scan scope:
    - **The whole computer**: Scans all hard disks and USB drives
    - **Hard disks**
    - **Other items**: Use this option to scan specific items (files, folders, etc.). You'll have to enter the path of the item to scan. The path must start with /  
*Example: /root/documents*
- **Click the** Advanced settings link to access a new window where you'll be able to configure additional aspects of the scheduled scan:
  - Select the relevant checkbox to scan compressed files.

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

## Alerts

This option is not supported for Linux computers.

## Advanced settings

- **Installation:** On Linux computers, the protection is installed in a default folder that cannot be changed.
- **Connection to Collective Intelligence:** On Linux computers it is not possible to disable the connection to Collective Intelligence. Therefore, as long as a computer is connected to the Internet, the installed protection will query Collective Intelligence.
- **Server connection settings:** This option is not available for Linux computers.
- **Quarantine settings:** The quarantine is not supported for Linux computers
- **Administrator password:** This option is not available for Linux computers.

## 14.3. Configuring the antivirus protection

The permanent file protection is not supported for Linux computers. Therefore, to protect your Linux computers you must run on-demand scans or schedule periodic scans.

# 15. Mac OS X protection profiles

---

Specific characteristics of the protection for Mac  
OS X

General protection settings  
Configuring the antivirus protection

## 15.1. Introduction

To configure a security profile for a Mac OS X computer, go to the **Settings** window. Select the profile to configure from the **Profiles** panel, and select **OS X** from the side menu.

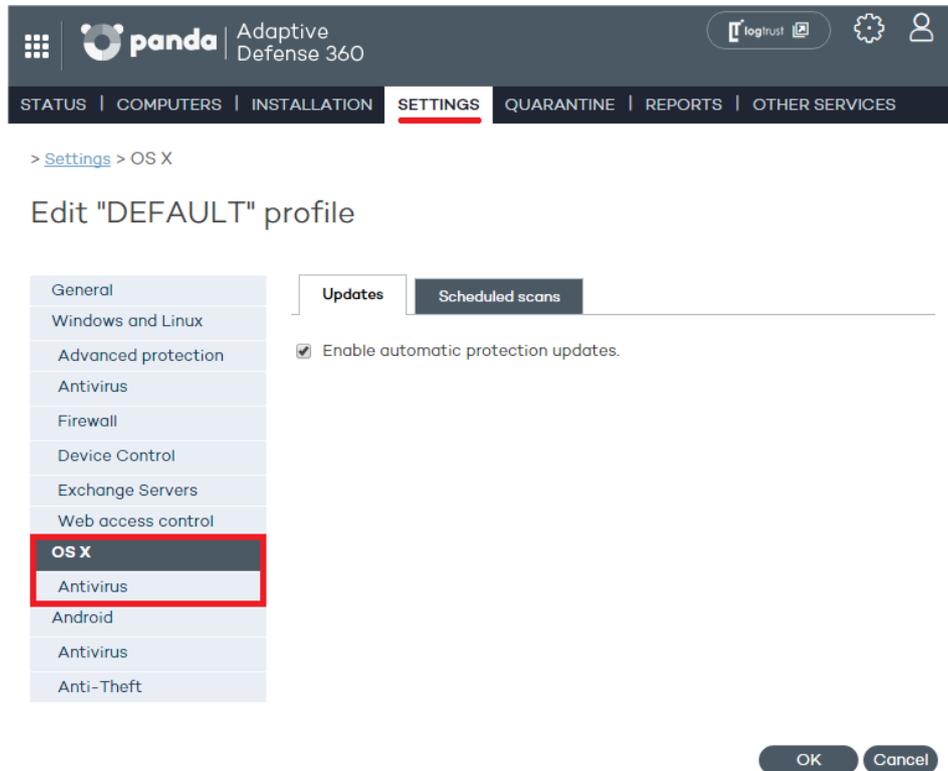


Figure 70: Accessing the profile settings for Mac OS X computers

## 15.2. Specific characteristics of the protection for Mac OS X

The protection for OS X has a series of unique characteristics that set it apart from the protection for Windows/Linux systems. These are as follows:

### Configuring updates on OS X computers

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

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

### Frequency of protection updates on OS X computers

The protection for OS X computers is updated with the following frequency:

- Signature file: Updated every hour
- Protection settings: The agent checks for changes every 4 hours
- Detection information: Updated every 6 hours

- Computer status information: Updated every 12 hours

### Automatic updates of the protection engine (upgrades)

The protection of OS X computers is updated automatically, even though you can disable this feature from the management console. 72 hours after the release of a version more recent than the protection installed on a Mac OS X computer, this will appear as "out-of-date" in the Status window. During the installation process, you will have to uninstall the previous version and install the new one.

## 15.3. General protection settings

Click **OS X** in the menu on the left to access the general protection settings.

### Scheduled scans

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

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

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

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

- Click **New** to go to the **Edit profile – New scan** job window.
- In the window that opens, enter the following data:
  - **Name**: Choose a name for the scan task.
  - **Scan type**: Select the type of scan that you want to create:
    - **Immediate scan**: Once configured, the immediate scan will take place as soon as the computer connects to the **Adaptive Defense 360** server, and the solution checks that the protection configuration has changed.
    - **Scheduled scan**: The scan will take place at the time and date you set in Start date and Start time. Use the drop-down menu to select if the scan start time refers to the **Adaptive Defense 360** server or the user's computer.
    - **Periodic scan**: Set the start date and start time, and select the scan frequency in the Repetition menu.
  - **Scan**: Select the scan scope:
    - **Hard disks**
    - **Other items**: Use this option to scan specific items (files, folders, etc.). You'll have to enter the path of the item to scan.

The path must start with /:

Example:

```
/root/documents
```

The permission that you have will dictate whether or not you'll be able to define

specific paths to scan. The maximum number of paths to scan for each profile is 10.

- Click the **Advanced settings** link to access a window where you will be able to configure additional aspects of scheduled scans:
  - Scan compressed files.
  - Malicious software to detect. The option to scan viruses will always be enabled.
  - Scan the entire computer or exclude certain folders or files with specific extensions from the scans. Use the **Add**, **Delete** and **Clear** buttons to define the list of exclusions.

## 15.4. Configuring the antivirus protection

Select the **Enable permanent file protection** checkbox to protect the file system on your Mac OS X computers.

### Exclusions

This section allows you to configure items, folders, etc. that will not be scanned by **Adaptive Defense**

**360**

# 16. Android protection profiles

---

Configuring the antivirus protection  
Configuring the anti-theft protection

## 16.1. Introduction

The Android protection module is divided into two sections: Antivirus and Anti-Theft.

To configure the protection for your Android tablets or smartphones, go to the **Settings** window. Select the profile to configure from the **Profiles** panel, and click **Android** from the side menu.

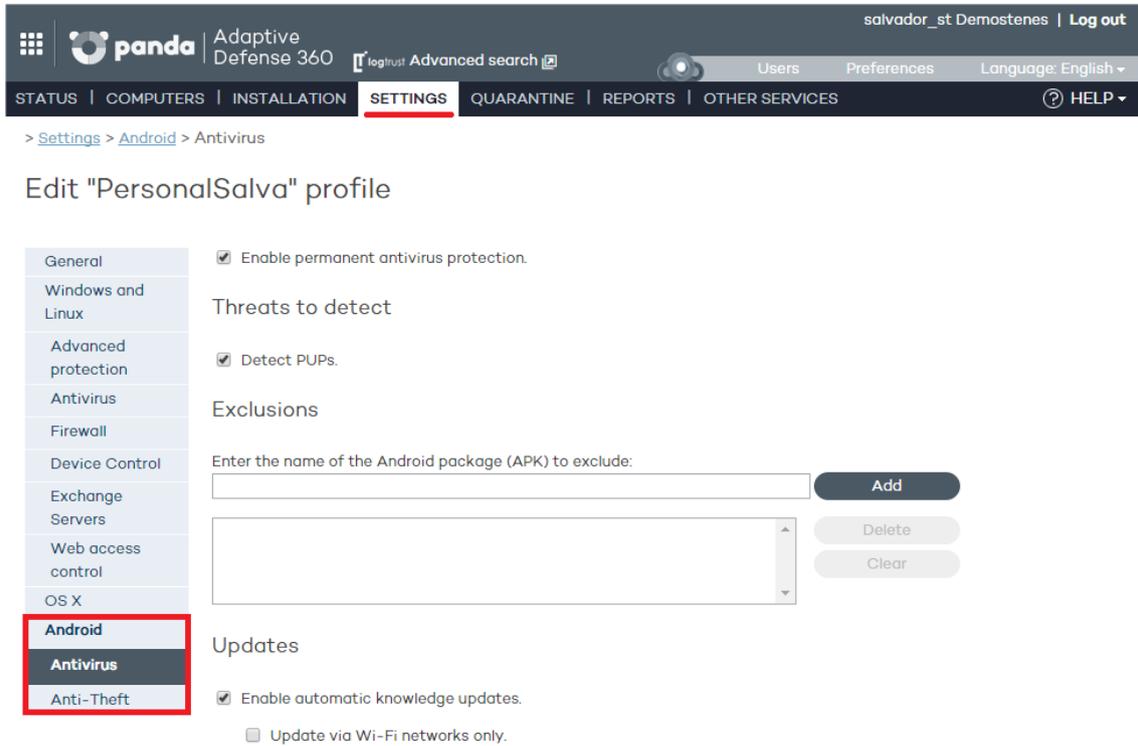


Figure 71: Accessing the protection settings for your Android devices

## 16.2. Configuring the antivirus protection

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

Select the **Enable permanent antivirus protection** checkbox to enable malware detection. Additionally, select the **Detect PUPs** checkbox to also detect potentially unwanted programs.

### Exclusions

The Android protection allows you to exclude installed apps from the scans. To do this, follow the steps below:

- Enter the name of the Android package (.apk) that you want to exclude, and click **Add**.
- Use the **Delete** and **Clear** buttons to clear or edit the contents of the list of exclusions.

### Updates

To update the signature file automatically, select the option **Enable automatic knowledge updates**. Additionally, you can choose to update the protection exclusively through Wi-Fi networks to avoid extra data charges.

### Scheduled scans

To schedule a scan, click the **New** button.

Use the options in the **New scan job** window to configure the scan type: immediate, scheduled or periodic.

As you create scan tasks, these will appear on the list of scheduled scans for the profile whose antivirus protection you are configuring. You can edit or delete them from there.

- **Immediate scan:** Once you have configured the scan, it will take place as soon as the device connects to the **Adaptive Defense 360** server.
- **Scheduled scan:** The scan will take place at the configured date and time. For that to happen, you need to configure the scan sufficiently in advance. If there is no connection to the **Adaptive Defense 360** server at the scheduled date and time, the scan will take place as soon as the connection is re-established.
- **Periodic scan:** The scan will take place at the date and time that you set in the relevant fields. Select the scan frequency. As with scheduled scans, it is advisable to configure periodic scans sufficiently in advance to ensure there is connectivity with the **Adaptive Defense 360** server. Otherwise, the scan will take place as soon as the connection is re-established.

## 16.3. Configuring the anti-theft protection

The anti-theft protection included in **Adaptive Defense 360** will give you total control over the company's Android devices, and will allow you to take a series of actions in case of loss or theft.

Namely, you will be able to locate, lock and wipe the devices, take a picture of the thief, and send it by email to an address of your choice.

To enable this feature, select the **Enable anti-theft protection** checkbox.

- **Report the device's location:** Select this checkbox if you want the protection to automatically report the device's location.
- **Take a picture after three failed unlock attempts and email it to the following addresses:** Select this checkbox if you want to receive an email when there is activity on a stolen device. Then, enter the email address(es) that the picture of the potential thief will be sent to. Use a semicolon (;) to separate them. If, together with the option to snap a picture of the thief, you select the option to report the device's location, the email received will include a photo plus a map showing its location.

Once you have finished configuring the protection, go to the **Computer details** window to track the location of the device, lock it, and change the email address for the **Snap the thief** feature.

## Privacy mode

Administrators can allow end users to use their devices in privacy mode. This allows the end user to disable the options to automatically report the device's location and take a picture of the thief, which will be password-protected.

When enabling the privacy mode, the **Adaptive Defense 360** agent will prompt the end user to set a personal 4-digit access code. Then, the administrator will have to enter this code in the management console if they want to make use of the device location and snap the thief features.

# 17. Malware visibility and monitoring

---

Dashboard

Detections

Lists of incidents and malware detected

## 17.1. Introduction

**Adaptive Defense 360** provides network administrators with four major groups of tools to view the security status of the company's IT resources:

- The dashboard with real-time information.
- Lists of incidents and malware detected.
- Lists of computers and network devices.
- Consolidated reports with data compiled over time.



*Refer to chapters 18 and 19 for more information about the list of network computers and devices as well as consolidated reports*

These four tools enable administrators to accurately appraise the risk of infection to the managed computers.

The end goal of the viewing and monitoring tools is to be able to determine the impact of any security breaches and to take any necessary action, either to mitigate the effects or to prevent similar situations in the future.

## 17.2. Dashboard

The **Adaptive Defense 360** dashboard is available in the **Status** window and is divided into two main areas: **Activity** and **Detections**. Each section contains a series of panels with information that enables administrators to get an immediate picture of the security status of their network.

The panels displayed in the dashboard are generated in real time and are interactive: hover the mouse pointer over the items to display tooltips with further information and click the items to open windows with detailed information.

The dashboard displays information for the time period established by the administrator using the tool at the right of the **Status** window. The options are:

- Last 24 h
- Last 7 days
- Last month
- Last year

Below we describe the various panels and their purpose.

## 17.3. Activity section

The **Activity** section shows a classification of all programs run and scanned on the network's Windows computers, as well as the security incidents detected, and the number of currently blocked items being classified by the system.

**Adaptive Defense 360** reports an incident in the **Activity** section for each computer-threat-threat type (malware or PUP) triplet encountered on the network. If the cause of a specific incident does not disappear, a maximum of two detections will be reported every 24 hours for each computer-threat-threat type triplet that requires the administrator's attention.

In the case of exploit attacks, an alert will be generated every time **Adaptive Defense 360** detects a vulnerability exploit attempt on a user's computer, regardless of the exploit type and the compromised process.

The **Activity** section is divided into the following areas:

- Classification of all programs run and scanned
- Malicious programs and exploits
- Potentially unwanted programs
- Under investigation at our lab

### Classification of all programs run and scanned

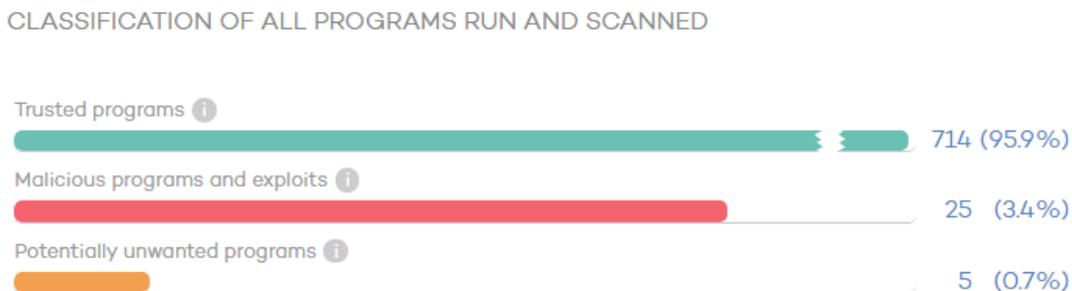


Figure 72: Classification of all programs run and scanned panel

The purpose of this panel is to quickly display the percentage of goodware and malware items seen and classified on the client's network during the time period selected by the administrator. The panel displays three horizontal bars, along with the number of events associated to each item category and a percentage over the total number of events.

 The data in this panel corresponds to the entire IT network, not only to those computers that the administrator has permissions on based on the credentials used to log in to the console. Unclassified items are not shown in the panel.

- **Trusted programs:** Applications seen on the customer's network which have been scanned and classified as goodware.
- **Malicious programs and exploits:** Programs that attempted to run or were scanned in the selected period, and were classified by **Adaptive Defense 360** as malware, exploits, zero-day

threats or targeted attacks.

- **Potentially unwanted programs:** Applications seen on the customer's network which have been scanned and classified as PUP.

Click any of the bars (with the exception of the **Trusted programs** bar) to access a detailed list of the Malware or PUP detections made on the system.

### Malicious programs, exploits and potentially unwanted programs



Figure 73: Detected threats panel

The information displayed in these panels refers to those computers that the administrator has permissions on based on the credentials used to log in to the console. If the administrator does not have permissions on all computers on the network, a warning will be displayed at the top of the panel.

- **Number of incidents/alerts detected**
- **Number of computers with incidents detected**
- **Accessed data:** Number of alerts that include one or more attempts to access information on users' hard disks.
- **Outbound connections:** Number of incidents that involve connections to external computers.
- **Run:** Number of malware samples that have been run.



*Malicious programs and potentially unwanted programs show data with a maximum interval of 1 month. In the event that the administrator set a longer period explanatory text at the top of the panel is displayed.*

Click any of the items in those panels to access the **Malicious programs and exploits** or **PUP** window.

### Currently blocked items being classified

CURRENTLY BLOCKED ITEMS BEING CLASSIFIED



Figure 74: Currently blocked programs being classified panel

This panel shows every unknown process detected on the network that requires further analysis by Panda Security Labs in order to be classified as goodware or malware. Depending on the way the protection has been configured (Lock, Hardening or Audit), these items may be blocked during the time it takes to classify them.

The information displayed in this section is a history of all the items that have been blocked and are pending classification since the service was implemented on the customer's network until the current time, and is not affected by the time period selected by the administrator.

The total number of temporarily blocked items indicates the different applications (different MD5) that are being blocked. This number is independent of the number of run attempts performed by each blocked application. Some bubbles may have the same malware name. This is typical of malware that uses polymorphic techniques to avoid being detected by signature-based traditional antivirus solutions. Every variant of the same malware that has a different MD5 is shown independently.

Each application is counted once only. That is, even if an application tries to run several times on the same computer, it will only be counted once. The size of each bubble is an indicator of the number of computers where the malware was found and blocked.

**Example:**

Suppose the dashboard displays a total of eight currently blocked items pending classification. Each item will be represented with a circle.

Suppose one of the applications tried to run thirty times on the same computer on the same day. As all those attempts took place on the same computer and on the same day, they will count as only one of the eight detections shown in the panel.

Blocked applications are indicated with a color code:

- **Orange:** For applications with a medium probability of being malware.
- **Dark orange:** For applications with a high probability of being malware.
- **Red:** For applications with a very high probability of being malware.

Hover the mouse pointer over a circle to display the application's full name and a series of icons representing key actions:

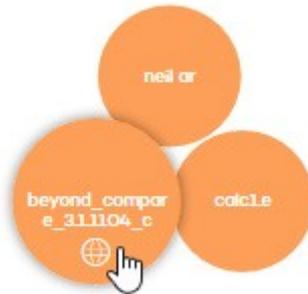


Figure 75: Information about the actions taken by blocked programs

- **Folder:** The program has read data from the user's hard disk.
- **Globe:** The program has connected to another computer.

Click the number of blocked items or any of the circles in the panel to access detailed information about the blocked items in the process of classification.

## 17.4. Detections section

The Detections section displays all of the intrusion attempts managed by **Adaptive Defense 360** in the selected period.

The data shown corresponds to all infection vectors and all supported platforms so that the administrator can have specific information (volume, type, attack method) on the malware found on their computes over a specific period of time.

The Detections section is divided into the following panels:

### Detected threats

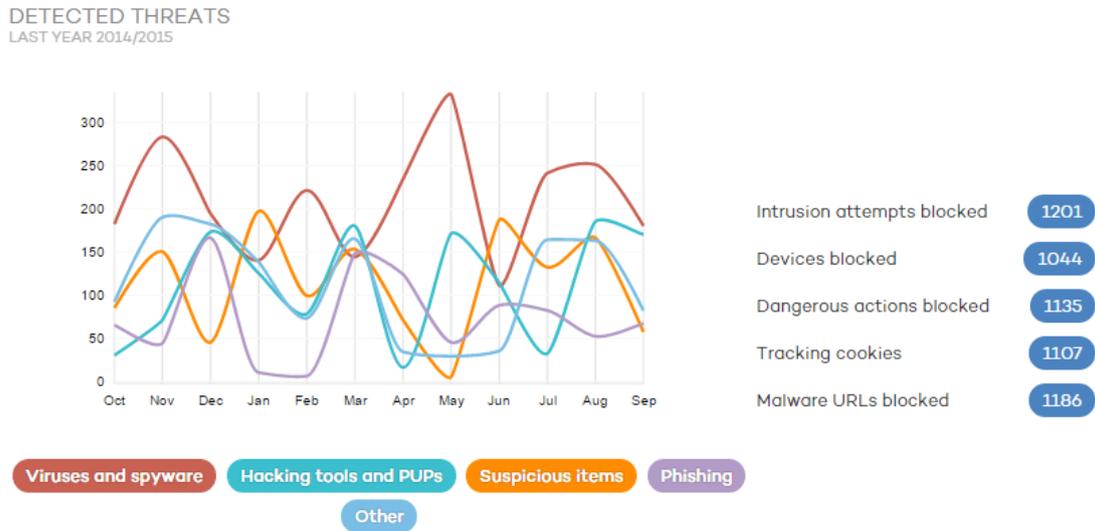


Figure 76: Consolidated activity panel

This panel includes two sections: a line graph and a list.

The line graph displays the evolution of threats detected on the network divided into malware types.

- Viruses and spyware
- Hacking tools and PUPs
- Suspicious items
- Phishing
- Other

The Y axis shows the number of incidents and the X axis the date.

To simplify the content of the panel, move the mouse pointer over each category at the bottom of the graph and the others will disappear.

The list on the right shows the actions which, although not directly related with the malware detected, are nevertheless important in drawing administrators' attention to potentially dangerous situations.

- **Intrusion attempts blocked:** These are attacks blocked by the firewall and the intrusion prevention system.
- **Devices blocked:** Devices blocked by the device control module.
- **Dangerous actions blocked:** Detections made by the local behavior analysis.
- **Tracking cookies:** Cookies detected that monitor users' Internet movements.
- **Malware URLs blocked:** Web addresses that point to pages containing malware.

### Detection origin

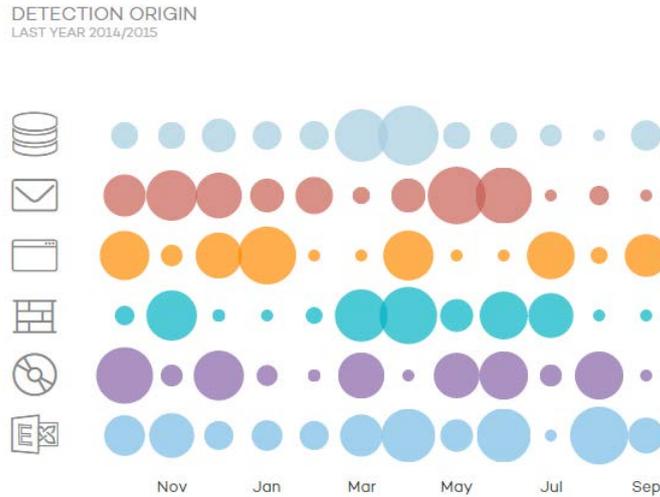


Figure 77: Activity by infection vector

This panel displays the infection vectors used by the malware discovered on the network.

The Y axis contains a series of icons displaying the infection vector:

- File system
- Local email
- Internet
- Firewall / Intrusion detection system
- Device control
- Exchange server

The X axis shows the date of the selected period.

This graph contains a series of different sized circles of different colors. The size of the circle reflects the number of detections. Move the mouse pointer over the circle to see a tooltip to see the number of detections for a certain date and infection vector.

**Detected spam**

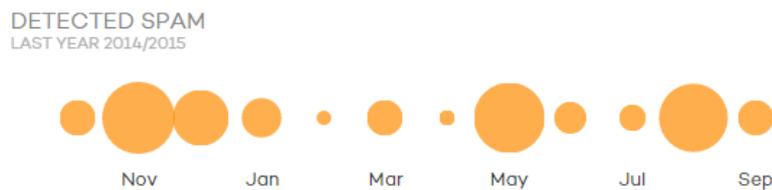


Figure 78: Consolidated spam detections by month

This panel shows the amount of spam detected in the Exchange server.

The X axis shows the dates of the selected period.

This graph contains a series of different sized circles. The size of the circle reflects the number of detections. Move the mouse pointer over the circle to see a tooltip to see the number of detections for a certain date.

**Filtered messages**

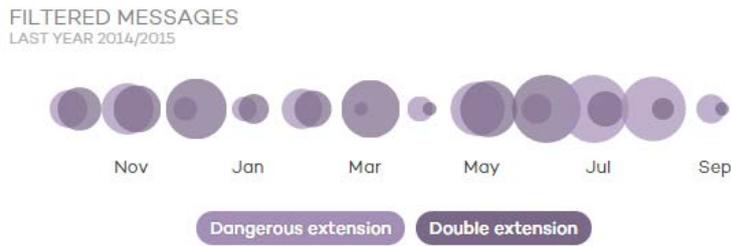


Figure 79: Messages with a dangerous or double extension filtered by month

This panel shows the number of messages that were filtered by the Exchange server content filter.

The X axis shows the dates of the selected period.

This graph contains a series of different sized circles. The size of the circle reflects the number of detections. Move the mouse pointer over the circle to see a tooltip to see the number of events for a certain date.

**Web access**

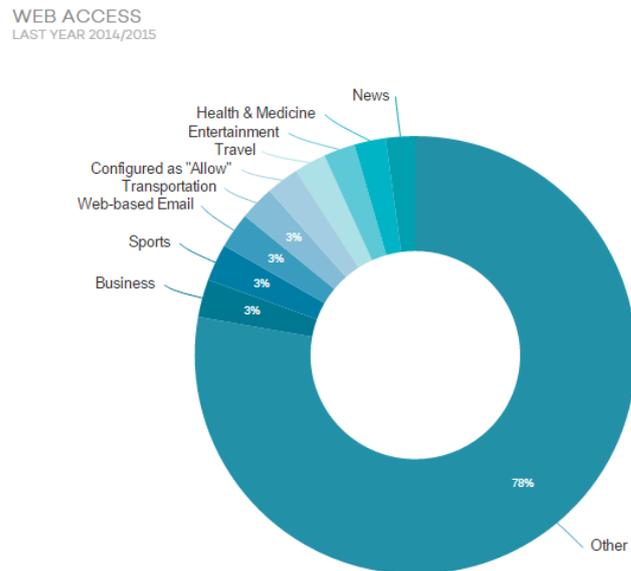


Figure 80: Web accesses by category

This panel shows a pie graph representing the Web page categories requested by network users. Pass the mouse pointer over each segment to see the number of requests for each category.

### 17.5. Activity section lists

The purpose of these lists is to provide administrators with the necessary information to find the source of a problem, assess the severity of an incident and, if required, take the necessary remediation measures to update the company's security policies.

Click the different panels in the **Activity** section to display reports and detailed lists of malware, as well as the software under analysis found on the customer's network.



These lists also allow administrators to add exclusions and unblock blocked items under analysis. See later in this document for more information about the exclusion and unblock operations supported by the solution.

All of these lists have the same structure:

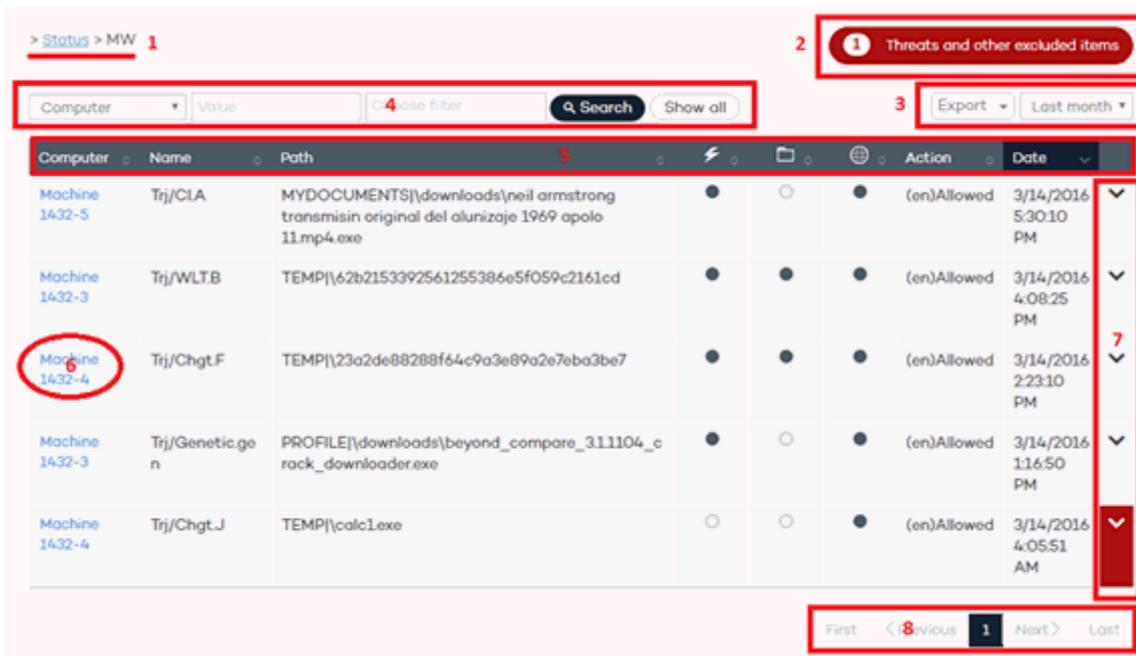


Figure 81: Structure of an Activity list

- List name. (1)
- Notification regarding the existence of files classified as malware by **Adaptive Defense 360** and which have been allowed to run by the administrator. (2)
- **Time interval combo box and list export tool.** The time period combo box allows the administrator to apply the following time filters to the list:
  - Last 24 hours
  - Last day

- Last month.

The export tool allows administrators to save the list to an Excel or CSV file. **(3)**

- **Filter tool.** Each list incorporates its own filters based on the data it contains. These are explained in the relevant sections. **(4)**
- You can sort the data in the tables by clicking the column headers. **(5)**
- Click a computer's name for extended information. **(6)**
  - **IP address:** The computer's IP address
  - **Installation date:** Date when the agent was installed on the computer
  - **Last connection:** Last time the agent connected to the **Adaptive Defense 360** server
  - **Operating system**
  - **Alerts triggered:** Number of alerts triggered in the selected period
  - **Group:** The group the computer belongs to
  - **Protection mode:** Advanced protection mode currently configured for the computer (Audit, Hardening, Lock).
- Drop-down arrow with information about the malware actions. Refer to chapter 22 Forensic analysis for more information about the actions performed by the detected malware. Refer to chapter 20 Remediation tools for more information about the remediation tools provided by **Adaptive Defense 360**
- Pagination controls for easier browsing.

### 17.5.1 Malicious programs and exploits list

Click any of the items in the **Malicious programs and exploits** panel, or the **Malicious programs and exploits** bar in the **Classification of all programs run and scanned** panel, to view a list of all threats found on the computers protected with **Adaptive Defense 360**.

The window displays two types of information, based on the option selected at the top of the list: malicious programs, or exploits.



Figure 82: Malware type selector

#### Malicious programs

Programs whose behavior poses a threat to the user's computer.

At the top of the list there is a search tool:



Figure 83: Filter tool

Filter **(1)** restricts the search indicated in text box **(2)**:

- **Computer:** The search string will be applied to the computer name.
- **Name:** The search string will be applied to the malware name.
- **Date:** The search string will be applied to the date of detection.
- **MD5:** File identification digest value.
- **Infection source:** The search string will be applied to the IP address of the customer's computer that the infection originated from.

Filter (3) shows those threats that match the selected criteria:

- **Not run:** Malware detected by the vulnerability protection.
- **Run:** The malware was run and the computer is infected.
- **Access to data files:** The malware accessed the disk to collect information from the computer, or to create the files and resources necessary for its execution.
- **Communications:** The malware created sockets for communicating with other computers, including localhost.
- **Blocked:** Malware identified by **Adaptive Defense 360** and prevented from running.
- **Quarantined:** The file cannot be disinfected and was sent to quarantine.
- **Deleted**
- **Allowed by the end user:** Malware identified by **Adaptive Defense 360** and allowed to run by the user.
- **Disinfected:** The file was disinfected by the antivirus.

The table fields are as follows:

- **Computer:** Computer where the detection took place.
- **Name:** Malware name.
- **Path:** Full path to the infected file.
- **Already run:** The malware has been run
- **Accessed data:** The threat has accessed files located on the user's computer.
- **Made external connections:** The threat has communicated with remote computers to send or receive data.
- **Last action:** Action taken on the malware (block, allow, quarantine, delete, disinfect, allow by the user, etc.).
- **Date:** Date when the malware was detected on the computer.

## Exploits

This list shows those computers where an exploit attempt has taken place.

The top of the window displays a search tool:



Computer 1 ▾ Value 2 Choose filter 3 🔍 Search Show all

*Figure 84: Exploits list filter tool*

Filter (1) restricts the search indicated in text box (2):

- **Computer:** The search string will be applied to the computer name.
- **Compromised program:** The search string will be applied to the name and path of the file compromised by the exploit.
- **Date:** The search string will be applied to the date of detection.
- **MD5:** The search string will be applied to the MD5 hash value of the compromised file.

Filter (3) shows those threats that match the selected criteria:

- **Risk (YES):** Shows those computers that are or have been at risk
- **Risk (NO):** Shows those computers that have not been at risk
- **Allowed by the user:** Shows those computers where the exploit has not been blocked because the user declined the administrator's request to restart the system or end the compromised process.
- **Allowed by the administrator:** Shows those computers where the exploit has not been blocked because the administrator configured the protection in Audit mode.
- **Blocked (immediately):** Shows those computers where the exploit was immediately blocked before being run. There was no need to end the compromised program.
- **Blocked after the process was ended:** Shows those computers where the exploit was blocked after the compromised process was ended.
- **Detected. Pending restart:** Shows those computers with compromised programs that require a restart which hasn't happened yet.

The table fields are as follows:

- **Computer:** Device where the exploit attempt was detected.
- **Compromised program:** Path and name of the file that was hit by the exploit attack.
- **Action:** Action taken by **Adaptive Defense 360** based on the security policy set by the administrator.
  - **Allowed by the user:** The user declined the administrator's request to restart the system or end the compromised process to block the exploit (the security policy was **Block. Ask the user for permission to end the process**).
  - **Allowed by the administrator:** Exploit detected on a computer whose protection was configured in **Audit** mode.
  - **Blocked (immediately):** The exploit was immediately blocked before being run (the security policy was **Block**). There was no need to end the compromised program.
  - **Blocked after the process was ended:** The exploit was detected and blocked after the compromised program was ended (the security policy was **Block**).
  - **Detected. Pending restart:** The exploit has been detected and requires a computer restart to be blocked (the security policy is **Block**). The computer hasn't been restarted yet.
- **Risk:** Indicates whether or not the computer was at risk after suffering the exploit attack.

- **YES:** Computers that suffered an exploit attack under the following circumstances:
  - The security policy was **Audit**.
  - Or
  - The exploit required the computer to be restarted or the compromised process to be ended. The computer has been at risk regardless of whether these actions have finally been performed or not.
- **NO:** Computers that suffered an exploit attack but the exploit was immediately blocked. There was no need to restart the computer or end the compromised process.
- **Date:** Date when the malware was detected on the computer.

### 17.5.2 Currently blocked items being classified

This panel shows a list of those files in which **Adaptive Defense 360** has detected risks despite their classification is not fully complete. These files are blocked during the time it takes to fully classify them.



Figure 85: Select between viewing only those items that are currently blocked, or a history of all items blocked by **Adaptive Defense 360** since installation

#### Currently blocked



Figure 86: Currently blocked items filter tool

Filter (1) restricts the search indicated in text box (2):

- **Computer:** The search string will be applied to the computer name.
- **Name:** The search string will be applied to the name of the blocked file.
- **Date:** The search string will be applied to the date when the item was blocked.
- **MD5:** The search string will be applied to the digest value of the blocked file.

Filter (3) filters the items on the list by the protection mode in which **Adaptive Defense 360** was configured when blocking the item (Lock or Hardening), as well as by the actions taken by the process: Access to data files and Communications (only if the process was allowed to run before being blocked and its actions were logged by the system).

The **Currently blocked** table fields are as follows:

- **Computer:** Name of the computer where the unknown item was found.
- **Name:** Name of the unknown file.
- **Path:** Path in which the unknown file was detected.

- **Accessed data:** The unknown file has accessed files located on the user's computer.
- **Made external connections:** The unknown file has communicated with remote computers to send or receive data.
- **Protection mode:** Specifies the mode that the protection was configured in at the time of detecting the unknown file.
- **Likelihood of being malicious:** Medium, High, Very High
- **Date:** Date when the unknown file was first seen on the computer.

## History



Figure 87: History list filter tool

Filter (1) restricts the search indicated in text box (2):

- **Computer:** The search string will be applied to the computer name.
- **Name:** The search string will be applied to the name of the blocked file.
- **Date:** The search string will be applied to the date when the item was blocked.
- **MD5:** The search string will be applied to the digest value of the blocked file.

Filter (3) allows you to filter the items on the list by the following criteria:

- **Lock:** The advanced protection mode enabled when the item was blocked.
- **Hardening:** The advanced protection mode enabled when the item was blocked.
- **Access to data files:** The unknown file has accessed files located on the user's computer.
- **Communications:** The unknown file has communicated with remote computers to send or receive data.
- **Blocked:** The unknown file has been blocked.
- **Reclassified as GW:** The unknown file has been classified as goodware.
- **Reclassified as MW:** The unknown file has been classified as malware.
- **Reclassified as PUP:** The unknown file has been classified as a PUP.
- **Excluded:** The unknown file has been unblocked/excluded by the administrator, allowing it to run.
- **Not excluded:** The unknown file has not been unblocked/excluded by the administrator.

The **History** table fields are as follows:

- **Computer:** Name of the computer where the unknown item was found.
- **Name:** Name of the unknown file.
- **Path:** Path in which the unknown file was detected.
- **Action:** Action taken:

- **Blocked:** The unknown file has been blocked.
- **Reclassified as GW:** The unknown file has been classified as goodware.
- **Reclassified as MW:** The unknown file has been classified as malware.
- **Reclassified as PUP:** The unknown file has been classified as a PUP.
- **Accessed data:** The threat has accessed files located on the user's computer.
- **Made external connections:** The threat has communicated with remote computers to send or receive data.
- **Protection mode:** Specifies the mode that the protection was configured in at the time of blocking the item.
- **Excluded:** Indicates whether or not the item was excluded from monitoring.
- **Likelihood of being malicious:** Medium, High, Very High
- **Date.**

### 17.5.3 PUP list

Click any of the items in the **Potentially Unwanted Programs (PUP)** panel to view a list of the threats found on the computers protected with Adaptive Defense 360.

The screen provides different filters to filter the information displayed.

At the top, there is a search tool:



Figure 88: PUP list filter tool

Filter (1) restricts the search indicated in the text box to its right (2):

- **Computer:** The search string will be applied to the computer name.
- **Name:** The search string will be applied to the PUP name.
- **Date:** The search string will be applied to the date of detection.
- **MD5:** File identification digest value

Filter (3) shows the potentially unwanted programs that match the selected criteria:

- **Not run:** PUP detected by the protection against vulnerabilities
- **Run:** The PUP was run and the computer is infected.
- **Access to data files:** The PUP accessed the disk to collect information from the computer, or to create the files and resources necessary for its execution.
- **Communications:** The PUP created sockets for communicating with other computers, including localhost.
- **Blocked:** PUP identified by **Adaptive Defense 360** and prevented from running.
- **Quarantined:** The PUP cannot be disinfected and was sent to quarantine.

- **Deleted**
- **Disinfected:** The PUP was disinfected by the antivirus.
- **Allowed by the end user:** PUP identified by **Adaptive Defense 360** and allowed to run by the user.

The table fields are as follows:

- **Computer:** Computer where the detection took place.
- **Name:** PUP name.
- **Path:** Full path to the PUP file.
- **Already run:** The PUP has been run
- **Accessed data:** The PUP has accessed files located on the user's computer.
- **Made external connections:** The PUP has communicated with remote computers to send or receive data
- **Last action:** Action taken on the PUP (block, allow, quarantine, delete, disinfect, allow by the user, etc.).
- **Date:** Date when the PUP was detected on the computer.

#### 17.5.4 Detection details list

This list offers consolidated and complete information about all detections on all platforms and from all supported infection vectors used by hackers.

To display this list, click the Detected threats or Detection origin panels, in the Detections area of the dashboard.

The information is presented in three lists:

- **Detected threats**
- **Computers with most threats**
- **Most detected malware**

The top toolbar lets you choose the list to display, set the time period and export the data to a file. Click Export to display a window from which you can choose:

- The type of event to export
- File format (Excel, CSV)
- Time period (last 24 hours, last month, last year)

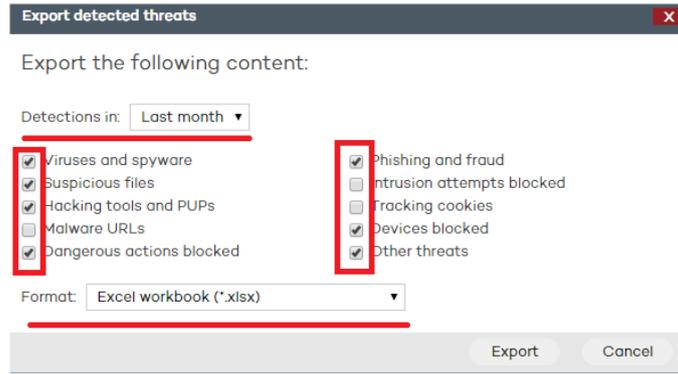


Figure 89: Detection list export settings

### List of detected threats

This displays a list of threats and dangerous events seen on the network and grouped by type:

Category	Count
Viruses and spyware	662,007
Suspicious files	165,705
Hacking tools and PUPs	47,805
Malware URLs	7,587
Dangerous actions blocked	28,959
Phishing and fraud	43,017

Figure 90: Types of detected threats and events

The groups are as follows:

- **Viruses and spyware**
- **Suspicious files:** This displays the files classified as suspicious by the **Adaptive Defense 360** heuristic analysis.
- **Hacking tools and PUPs**
- **Malware URLs:** URL pointing to a page containing malware.
- **Dangerous actions blocked:** This displays the files classified as suspicious by the behavior analysis techniques.
- **Phishing and fraud**
- **Intrusion attempts blocked:** Detections of malformed traffic.
- **Tracking cookies:** Displays the cookies used to spy on users browsing habits.
- **Devices blocked:** Peripheral devices connected to a user's computer that have been

blocked by the administrator.

- **Other threats:** Detection of malware not classified within the above categories (Jokes, etc.)

There is a counter for each group with the number of events during the chosen time period and the type of malware.

Click the  icon of a specific group to display the content as illustrated below.

Viruses and spyware 662,007

Computer	Group	Name	Path	Action	Date
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus6	C:\Win\PorAlli\vir6.exe	Deleted	9/10/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	Super7Virus	C:\Win\PorAlli\vir7.exe	Disinfected	9/10/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus	C:\Win\PorAlli\vir1.exe	Deleted	9/9/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus2	C:\Win\PorAlli\vir2.exe	Disinfected	9/9/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus6	C:\Win\PorAlli\vir6.exe	Deleted	9/9/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus14	C:\Win\PorAlli\vir14.exe	Quarantined	9/9/2015 4:19:02 PM
172.40.103.21	\CONT_1	VirusDeRed_Spyware	C:\Win\PorAlli\vir2.exe	Disinfected	9/9/2015 4:18:55 PM
172.40.103.21	\CONT_1	SuperVirus	C:\Win\PorAlli\vir1.exe	Deleted	9/9/2015 4:18:55 PM
172.40.103.21	\CONT_1	SuperVirus2	C:\Win\PorAlli\vir2.exe	Disinfected	9/9/2015 4:18:55 PM
172.40.103.21	\CONT_1	SuperVirus8	C:\Win\8PorAlli\vir8.exe	Deleted	9/9/2015 4:18:55 PM
ABCDEF982394DCBA	\CONT_2\CONT_2_1	SuperVirus2	C:\Win\PorAlli\vir2.exe	Disinfected	9/8/2015 4:19:10 PM
ABCDEF982394DCBA	\CONT_2\CONT_2_1	Super7Virus	C:\Win\PorAlli\vir7.exe	Disinfected	9/8/2015 4:19:10 PM
ABCDEF982394DCBA	\CONT_2\CONT_2_1	SuperVirus8	C:\Win\8PorAlli\vir8.exe	Deleted	9/8/2015 4:19:10 PM
ABCDEF982394DCBA	\CONT_2\CONT_2_1	SuperVirus14	C:\Win\PorAlli\vir14.exe	Quarantined	9/8/2015 4:19:10 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus6	C:\Win\PorAlli\vir6.exe	Deleted	9/8/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus8	C:\Win\8PorAlli\vir8.exe	Blocked	9/8/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus11	C:\Win\PorAlli\vir11.exe	Quarantined	9/8/2015 4:19:02 PM
172.40.103.21	\CONT_1	VirusDeRed_Spyware	C:\Win\PorAlli\vir2.exe	Disinfected	9/8/2015 4:18:55 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus6	C:\Win\PorAlli\vir6.exe	Deleted	9/7/2015 4:19:02 PM
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus8	C:\Win\8PorAlli\vir8.exe	Blocked	9/7/2015 4:19:02 PM

Figure 91: Detected threat list structure

- **Tools for filtering the information in a group (1):**

The controls displayed will depend on the type of group:

- **Group or computer search**
- Place where the item was detected:
  - Anywhere
  - In the file system
  - In Exchange server
  - In email
- **Type of device:**
  - All devices
  - Removable storage drives
  - Imaging devices
  - CD/DVD drives
  - Bluetooth devices
  - Modems
  - Mobile devices

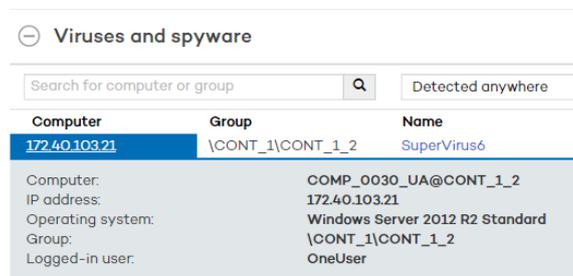
- **Number of rows to display**
- **Pagination tool**
  
- **Information about detected items (2).**

The columns displayed will depend on the type of group

- **Computer:** Name of the computer where the detection took place.
- **Group:** Group to which the computer belongs.
- **Name:** Name of the threat.
- **Path:** Path of the file system where the threat was detected.
- **Action:** Action taken by **Adaptive Defense 360**.
  - **Deleted:** The malware could not be disinfected and has been deleted.
  - **Disinfected**
  - **Quarantined**
  - **Blocked:** The malware has been blocked
  - **Process ended:** The malware was running and **Adaptive Defense 360** killed the process.

- **Information about specific items (3)**

Clicking any item displays further information.



Computer	Group	Name
172.40.103.21	\CONT_1\CONT_1_2	SuperVirus6

Computer:	COMP_0030_UA@CONT_1_2
IP address:	172.40.103.21
Operating system:	Windows Server 2012 R2 Standard
Group:	\CONT_1\CONT_1_2
Logged-in user:	OneUser

Figure 92: Extended information about a particular item

- **Pagination tool (4)**

This lets you establish the number of lines to display in the group and lets you move between pages.

### Computers with most threats

This list adds a grouping level with respect to the **Detected threats** list, as it first displays the computers with most detections. Click each computer to display a breakdown of the types of detections, as in the **Detected threats** list.

- **Information for the detected items.**
- **Computer**

- Group
- Detections
- **First detected:** Date of the first detection during the period
- **Last detected:** Date of the last detection during the period

### Most detected malware

This displays a list of the malware most frequently encountered on the customer’s network.

The screenshot shows the Panda Adaptive Defense 360 interface. At the top, there is a navigation bar with the Panda logo and 'Adaptive Defense 360'. Below this is a menu with options: STATUS, COMPUTERS, INSTALLATION, SETTINGS, QUARANTINE, REPORTS, and OTHER SERVICES. The main content area is titled '> Status > Detection details'. There is a dropdown menu for 'Most detected malware' and an 'Export...' button. A search bar is present with the text 'Search by malware name or type' and a search icon. To the right of the search bar is a dropdown menu for 'All threats' with a '1' next to it. Below the search bar is a table with the following columns: Malware name, Type, Detections, First detected, and Last detected. The table contains 17 rows of data. The 'Detections' column is highlighted with a red box, and the 'All threats' dropdown is also highlighted with a red box. The table data is as follows:

Malware name	Type	Detections	First detected	Last detected
SuperVirus10	Snap Shotter	32	8/18/2015 4:18:59 PM	9/10/2015 4:19:02 PM
SuperVirus3	Joke	32	8/18/2015 4:18:59 PM	9/10/2015 4:19:02 PM
SuperVirus4	Dialer	32	8/18/2015 4:18:59 PM	9/9/2015 4:19:02 PM
SuperVirus8	Trojan	32	8/19/2015 4:18:59 PM	9/9/2015 4:18:55 PM
SuperVirus13	PUP	30	8/21/2015 4:19:07 PM	9/10/2015 4:19:02 PM
SuperVirus2	Spyware	30	8/18/2015 4:18:59 PM	9/9/2015 4:19:02 PM
SuperVirus5	Hacking tool	29	8/19/2015 4:18:59 PM	9/9/2015 4:19:02 PM
SuperVirus	Virus	29	8/18/2015 4:18:59 PM	9/9/2015 4:19:02 PM
SuperVirus12	Tracking cookie	28	8/18/2015 4:18:59 PM	9/9/2015 4:18:55 PM
SuperVirus14	Security risk	27	8/19/2015 4:19:09 PM	9/9/2015 4:19:02 PM
SuperVirus15	Hoax	27	8/19/2015 4:19:09 PM	9/9/2015 4:19:02 PM
SuperVirus9	Key Logger	27	8/18/2015 4:18:59 PM	9/9/2015 4:19:02 PM
SuperVirus6	Adware	26	8/18/2015 4:18:59 PM	9/10/2015 4:19:02 PM
SuperVirus11	Password Stealer	26	8/18/2015 4:18:59 PM	9/8/2015 4:19:02 PM
Super7Virus	Worm	17	8/22/2015 4:18:59 PM	9/10/2015 4:19:02 PM
VirusDeRed_Spyware	Network virus	10	8/19/2015 4:19:09 PM	9/9/2015 4:18:55 PM
Generic Malware	Invalid	2	8/23/2015 4:18:59 PM	8/27/2015 4:19:07 PM

At the bottom of the table, there is a 'Rows' dropdown set to '20' and a pagination indicator '1 - 17 of 17'.

Figure 93: Most detected threats on your network

- Tools for filtering the information on the list (1)
  - Name or type of threat: Enter the name or type of threat.
  - Type of threat: Select the type of threat from the list.
    - Viruses and Spyware
    - Hacking tools and PUPs
    - Tracking cookies
    - Other threats
- Information about detected items (2)
  - Malware name
  - Type
  - Detections

- **First detected**
- **Last detected**
  
- **Information about specific items (3)**

Click the number of detections of a specific threat to display the list of **Detected threats**.

### Web access list

Click the **Web access** panel to display a list with consolidated and complete information on users' access to Web page categories.

This list is divided into four panels:

- Top 10 most accessed categories
- Top 10 computers with most access attempts
- Top 10 most blocked categories
- Top 10 computers with most access attempts blocked

Each panel has a **See full list** link which displays the full list for each category.

## 17.6. Managing exclusions and blocked items

**Adaptive Defense 360** blocks by default every program classified as malware. Additionally, and depending on the advanced protection settings, it will also block never-seen-before programs until they have been scanned and a verdict has been returned about their security.

If a user cannot wait for an unknown item to be classified, or the administrator wants to allow an item classified as malware to run, **Adaptive Defense 360** implements resources to prevent items from being blocked.



*IMPORTANT: We generally advise that you don't unblock items. Items blocked for being considered dangerous pose a real threat to the integrity of IT systems and the data stored across your network. Adaptive Defense 360 classifies items with 99.9999% accuracy, and the unknown items blocked are very likely to end up being classified as dangerous. That's why we recommend that you do not unblock unknown items or items classified as malware/PUP.*

It is important to differentiate between these two concepts: if **Adaptive Defense 360** blocks a user process for being unknown, and the network administrator removes the block imposed, they will be unblocking the item. However, if **Adaptive Defense 360** blocks an item after classifying it as dangerous to the customer (malware or PUP), and the administrator removes the block, they will be excluding the item (or adding an exclusion on the item).

- **General scheme**

This section displays a couple of diagrams illustrating the different situations that a process scanned by **Adaptive Defense 360** can go through, depending on the advanced protection settings, the exclusion list created by the administrator, and the changes that may affect the internal state of the process over time. We are using two diagrams for the sake of clarity: one for known files and the other for unknown files.

### 17.6.1 Known files

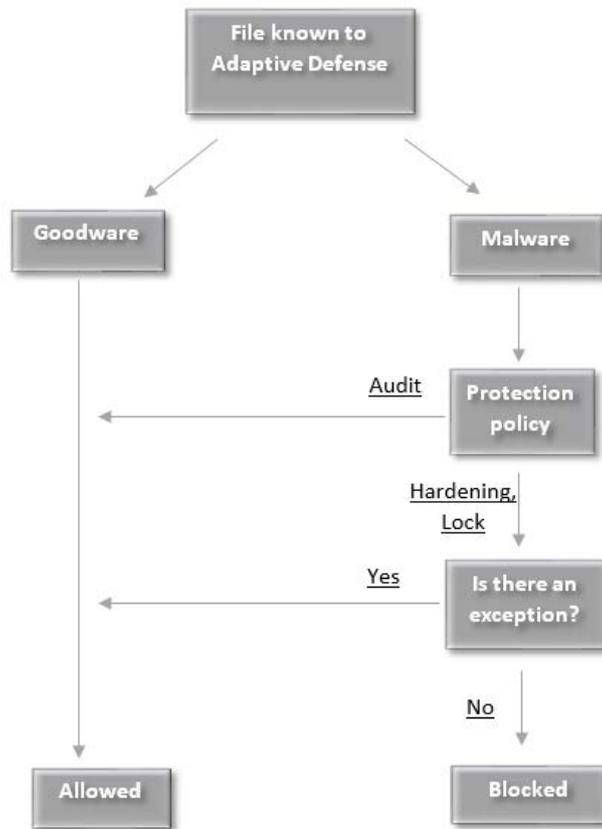


Figure 94: Actions taken on files known to **Adaptive Defense 360**

Processes classified by **Adaptive Defense 360** as malware with the advanced protection set to a mode other than **Audit** will be blocked unless the administrator creates an exclusion that allows them to run.

### 17.6.2 Unknown files

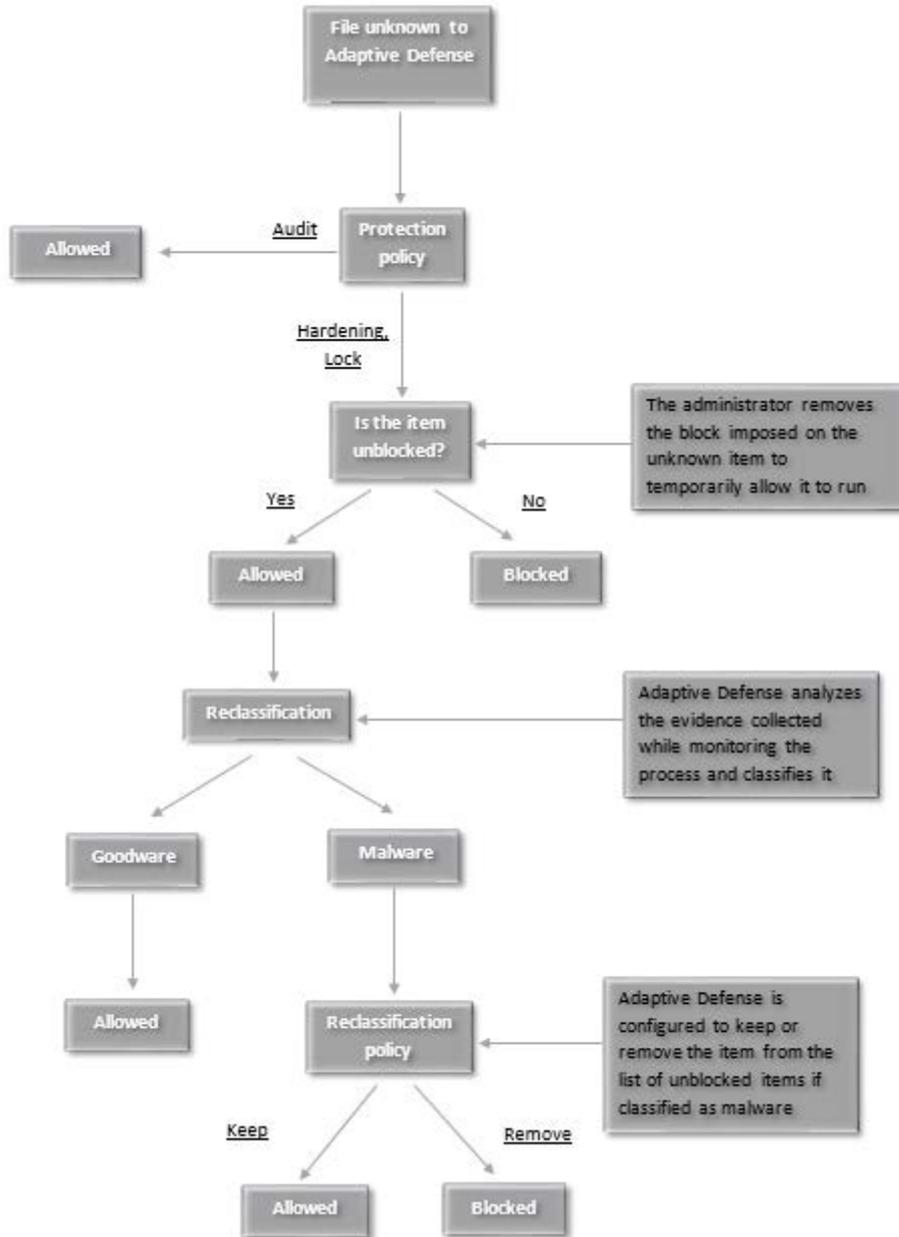


Figure 95: Actions taken on files unknown to **Adaptive Defense 360**

Unknown (not yet classified) processes that are detected with the advanced protection set to a mode other than **Audit** will be blocked unless the network administrator creates an exclusion. Regardless of the exclusion, **Adaptive Defense 360** will classify the file and, depending on the verdict and the reclassification policy selected, the file will be blocked or allowed to continue running.

### 17.6.3 Unblocking unknown items pending classification

If a user cannot wait for the system to automatically unblock a file once it has been finally classified, the administrator can use the button **Do not block again** in the **Currently blocked items** being classified window to remove the block.

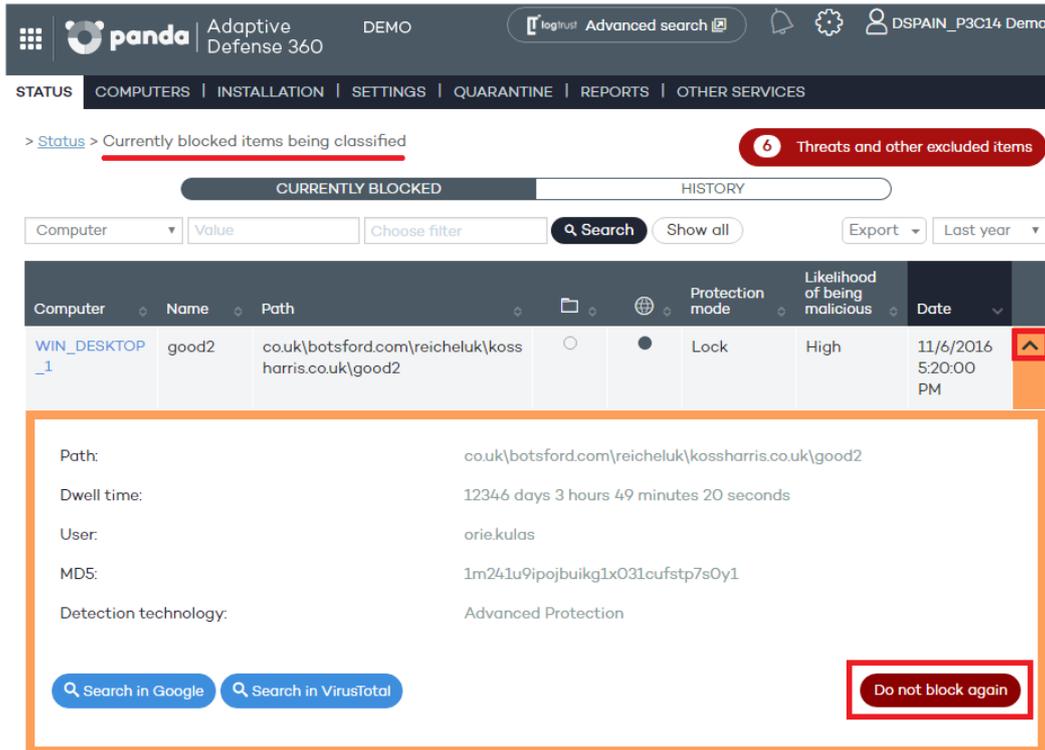


Figure 96: Button to unblock currently blocked items pending classification

Once unblocked, the item will disappear from the **Currently blocked items being classified** window. By doing that, the administrator will allow the item to run under their own responsibility. Nevertheless, **Adaptive Defense 360** will continue scanning the process until it is identified and classified. The unblocked item will appear in the **Threats and other excluded items list**, described later in this chapter.

#### 17.6.4 Excluding items classified as malware or PUP

Excluding an item classified as malware from the scans is equivalent to unblocking a blocked item that is pending classification, although in the former case you are allowing the execution of a program that **Adaptive Defense 360** has already classified as harmful or dangerous.

To exclude an item classified as malware or PUP, the administrator can use the **Do not detect again** button displayed in the **Malware** and **Potentially unwanted programs** lists accessible from the **Activity** dashboard.

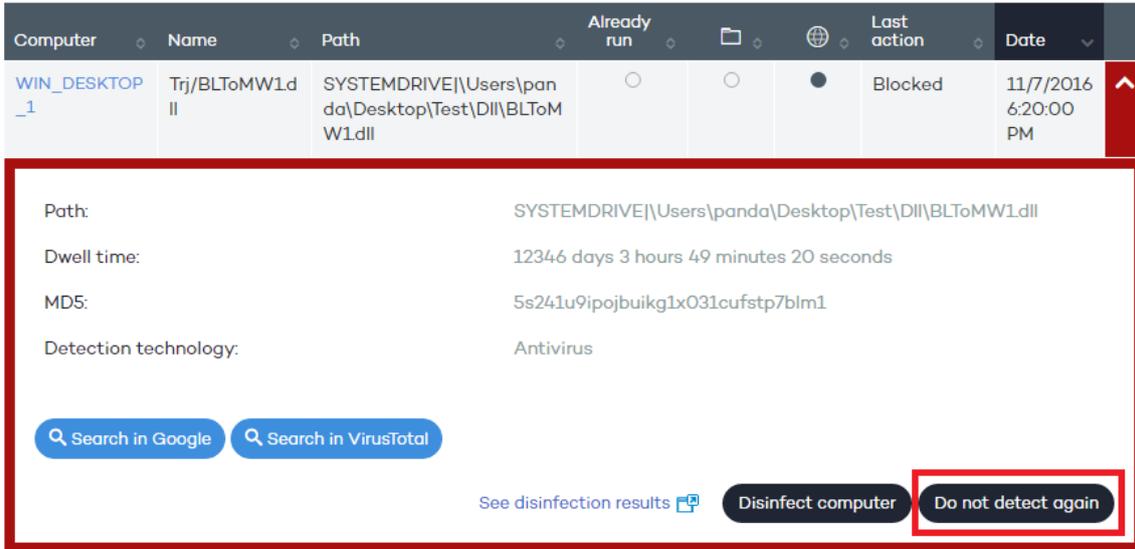


Figure 97: Button to stop detecting a specific threat

Once excluded from the scans, the item in question will stop generating any incidents in the Activity dashboard panels (Malware or PUP, depending on the nature of the item), and will be added to the Threats and other excluded items list, as explained in the next section.

### 17.6.5 Excluded items management window

To manage exclusions and configure the way the solution must behave when a known or unknown item is reclassified, go to the **Threats and other excluded items** window. You can access this window from the button displayed in the **Status** window or at the top of the Malware/PUP/Blocked items lists, which you can access after clicking the relevant panel in the **Activity** dashboard.

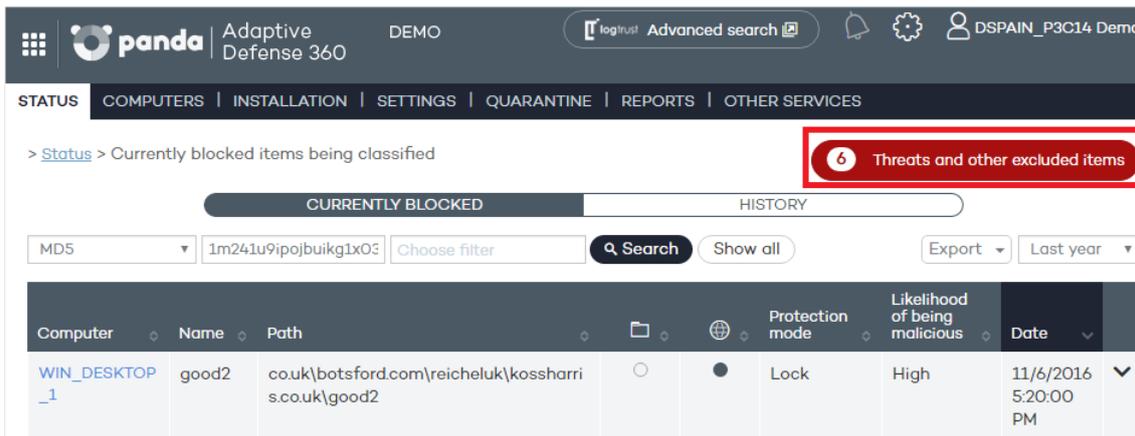


Figure 98: Accessing the excluded item lists from the *Currently blocked threats* list



Figure 99: Accessing the excluded item lists from the **Status** window

The **Threats and other excluded items** window lets you choose between managing the items that are currently allowed or accessing a history of every item that has been allowed so far. The window's contents will change depending on the option you select.

### 17.6.6 Currently allowed items

Shows those items currently excluded from scanning. Every item on the list is allowed to run.

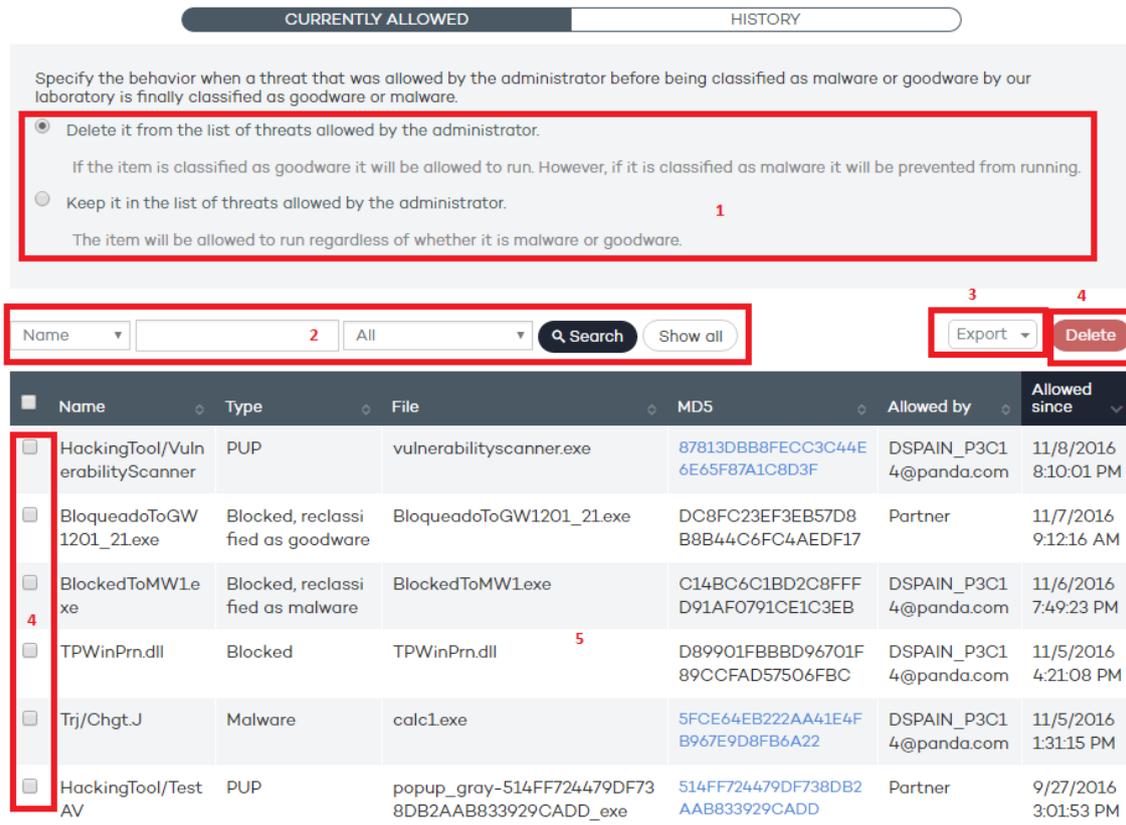


Figure 100: General structure of the **Currently allowed items** list

The **Currently allowed items** window provides the following tools:

- Reclassification policy (1)
- List filter (2)
- List export (3)
- Exclusion removal (4)
- List of currently excluded items (5)

### Reclassification policy (1)

Here you can define the way the system will automatically behave when an item that was unblocked by the administrator changes its internal state and it is necessary to make a new decision about whether to block/unblock it.

There are two possibilities when the administrator chooses to unblock a previously blocked (unknown) item: if the unknown item is finally classified as goodware, no further action will need to be taken, as the system will continue to allow the item to run. However, if the unknown item is finally classified as malware, the administrator will have to choose the action that **Adaptive Defense 360** must take:

- **Delete it from the list of threats allowed by the administrator:** The exclusion will be removed and the item will be blocked, unless the administrator manually generates a new exclusion for the file.
- **Keep it in the list of threats allowed by the administrator:** The exclusion is kept. That is, the item will be allowed to run.

Selecting **Keep it in the list of threats allowed by the administrator** displays a window for the administrator to confirm their selection, as this decision can lead to potentially dangerous situations. Example: An unknown item that is pending classification is unblocked by the administrator in order to be able to run it while the classification process is taking place. Once fully identified, the item turns out to be dangerous. In this case, should the option **Keep it in the list of threats allowed by the administrator** be selected, the malicious item would continue to be allowed to run.

### List filter (2)

The filter on the left restricts the search indicated in the text box to its right:

- **Name:** Malware or PUP name.
- **File:** Name of the unknown file or the file that contains the threat.
- **MD5:** Digest value that uniquely identifies the file.
- **Allowed by:** The console user that created the exclusion.
- **Malware:** Item classified as malware.
- **PUP:** Item classified as a PUP.
- **Unknown (Blocked):** Item that is still pending classification.
- **Reclassified as malware/PUP:** An item that was initially blocked for being unknown and which is later classified as dangerous.

- **Reclassified as goodware:** An item that was initially blocked for being unknown and which is later classified as safe.

Once you set a filter, click **Search** to apply it, or **Show all** to clear the filter and display all items.

### List export (3)

To export the list, click **Export** and select the format that you want to export the file to (xls or csv).

### Exclusion removal (4)

For **Adaptive Defense 360** to ignore the exclusion imposed on a previously excluded or unblocked item, select it from the list and click **Delete**. Once removed from the list, the item will be blocked or not depending on its classification and the advanced protection settings.

### List (5)

- **Name:** Name of the malware or PUP that is allowed to run. If it has not been identified, the column will display the file's name instead.
- **Type:** The file type:
  - **Malware:** Item classified as malware.
  - **PUP:** Item classified as PUP.
  - **Blocked:** The item is unknown and was blocked.
  - **Blocked reclassified as malware/PUP:** An item that was initially blocked for being unknown and which is later classified as dangerous.
  - **Blocked reclassified as goodware:** An item that was initially blocked for being unknown and which is later classified as safe.
- **File:** Name of the unknown file or the file that contains the threat.
- **MD5:** Digest value that uniquely identifies the file.
- **Allowed by:** The console user that created the exclusion.
- **Allowed since:** Date in which the item was allowed to run for the first time.

### 17.6.7 History

This window displays a history of all files excluded by Adaptive Defense 360. The list allows you to view all the states that a file has gone through, from the time it entered the list of excluded or unblocked items until it exited the list, including every intermediate state that the system or the administrator may have applied to it.

> [Status](#) > Threats and other excluded items

CURRENTLY ALLOWED HISTORY

File 1 All Search Show all 2 Export

File	Type	MD5	Action	User	Date
vulnerabilityscanner.exe	PUP	87813DBB8FECC3C44E6E65F87A1C8D3F	Exclusion added. Subsequent runs allowed	DSPAIN_P3C14@panda.com	11/8/2016 8:10:01 PM
BloqueadoToGW1201_21.exe	Blocked	DC8FC23EF3EB57D8B8B44C6FC4AEDF17	Exclusion added. Subsequent runs allowed	Partner	11/7/2016 9:12:16 AM
BlockedToMW1.exe	Blocked	C14BC6C1BD2C8FFF D91AF0791CE1C3EB	Exclusion added. Subsequent runs allowed	DSPAIN_P3C14@panda.com	11/6/2016 7:49:23 PM
TPWinPrn.dll	Blocked	D89901FBBBD96701F89CCFAD57506FBC	Exclusion added. Subsequent runs allowed	DSPAIN_P3C14@panda.com	11/5/2016 4:21:08 PM

Figure101: General structure of the *History* list

### List filter (1)

The filter on the left restricts the search indicated in the text box to its right:

- **File:** Name of the unknown file or the file that contains the threat.
- **MD5:** Digest value that uniquely identifies the file.
- **User:** Login of the user that changed the item's state.

### List export (2)

To export the list, click **Export** and select the format that you want to export the file to (**xls** or **csv**).

### List (3)

- **File:** Name of the unknown file or the file that contains the threat.
- **Type:** The file type:
  - **Malware:** Item classified as malware
  - **PUP:** Item classified as a PUP
  - **Blocked:** The item is unknown and was blocked
- **MD5:** Digest value that uniquely identifies the file.
- **Action:** Indicates how the file's state changed.
  - **Exclusion added. Subsequent runs allowed:** The administrator allowed the process to run and the file entered the list of excluded items.
  - **Removed from the list of excluded items:** The administrator removed the exclusion and the file exited the list of excluded items. The system goes back to its normal behavior regarding the file.
  - **Reclassified as PUP/malware. Exclusion removed:** The file was unknown when it was excluded, and later the system classified it as dangerous. The system removed the exclusion automatically because the exclusion policy was Delete it from the list of threats allowed by the administrator. The item has been blocked from then on.
  - **Reclassified as goodware. Exclusion removed:** The file was unknown when it was excluded, and later the system classified it as safe. The system removed the exclusion automatically because the exclusion policy was Delete it from the list of threats allowed by the administrator. The file is allowed to run.

- **Excluded item reclassified as goodware. The exclusion is kept:** The file was unknown when it was excluded, and later the system classified it as safe. The system keeps the exclusion automatically because the exclusion policy is **Keep it in the list of threats allowed by the administrator**. The file is allowed to run.
  - **Excluded item reclassified as PUP/malware. The exclusion is kept.** The file was unknown when it was excluded, and later the system classified it as dangerous. The system keeps the exclusion automatically because the exclusion policy is **Keep it in the list of threats allowed by the administrator**. The file is allowed to run.
  - **Settings changed to "Remove reclassified programs from the list of allowed threats":** The administrator changed the exclusion policy.
  - **Settings changed to "Keep reclassified programs in the list of allowed threats":** The administrator changed the exclusion policy.
- **User:** Login of the user that changed the item's state, or Automatic if the change was due to an internal reclassification.
  - **Date:** Date when the change took place.

# 18. Computer visibility and monitoring

---

Network computer status  
Computer visibility

## 18.1. Introduction

This chapter describes the resources implemented in **Adaptive Defense 360** to monitor the status of your network computers.

## 18.2. Network computer status

The dashboard provides a brief summary of the protection status of the entire network, in the **Status** menu.



Figure 102: Computer status panel

This section displays the computers that require the administrator's attention:

- Computers that have not connected to the server in the last 72 hours, 7 days and 30 days.
- Computers with outdated protection: the engine, the signature file and those that need a restart to apply an update to the engine of the downloaded protection.

Click the various items in the panel to display the **Protected** tab in the **Computers** window, which contains more detailed information.

## 18.3. Computer visibility

The Computers window contains everything necessary to monitor your IT network and search for computers:

- The group tree
- Status tabs
- Search tools
- A window with details of the computer or device

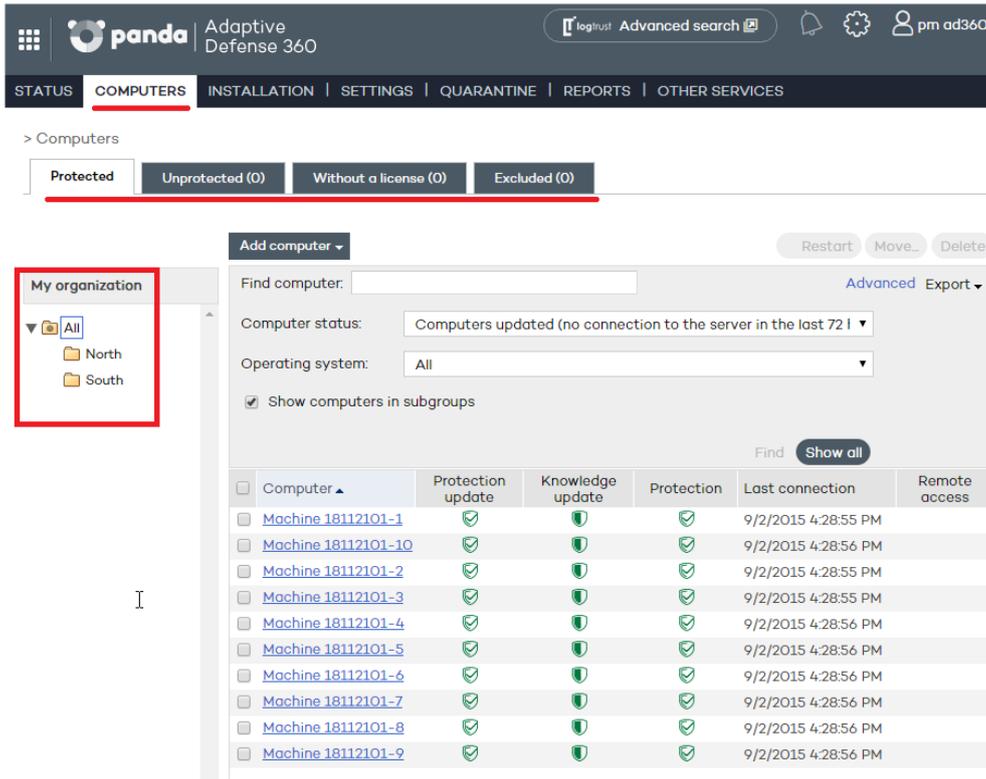


Figure103: Computers window

### Group tree

The group tree on the left-hand side of the window lets you move through the different group levels and view the computers included in each group. Click **All** to display the list of all network computers.

### Tabs

There are four groups each reflecting the protection status of the computers:

- Protected
- Unprotected
- Without a license
- Excluded

### Protected

Computers with the **Adaptive Defense 360** agent correctly installed and with a valid license assigned, although they could have outdated protection or an error in the protection.

### Unprotected

This includes cases where the agent is in the process of installation or removal, the protection has been uninstalled, as well as computers that have been discovered with the discovery tool.

### Without a license

These are computers that had a valid license assigned in the past but the corresponding license

contract has expired and consequently they are unprotected. This also includes computers that belong to a group with restrictions on the maximum number of licenses or on the expiry date and the computer has not met these conditions.

### Excluded

These are computers with an **Adaptive Defense 360** agent installed but that don't compete for a valid license. Administrators can manually exclude computers when the number of valid licenses contracted is lower than the number of computers on the network to protect.

### 18.3.1 Search tools

The list of computers can be filtered using various criteria depending on the selected tab.

In some tabs, moreover, there is an **Advanced** button. Click this to show or hide other search criteria.

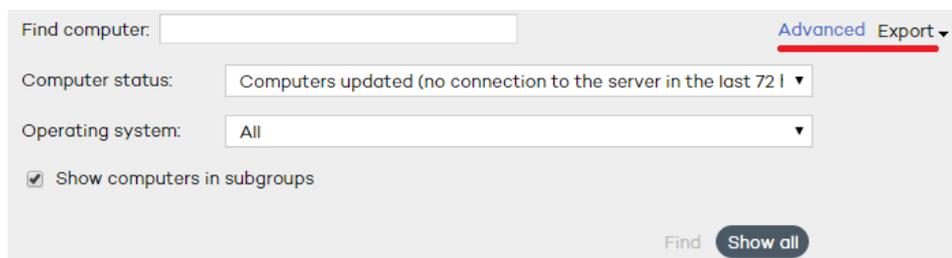


Figure104: Computer search tools

There is also a **Show all** button, which overrides any filters and displays all computers in the selected tab.

Below you can see the search options and criteria for each of the tabs.

### Protected tab

- **Find computer:** Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'
- **Computer status:**
  - All
  - Computers with all protections enabled
  - Computers with all protections disabled
  - Computers with up-to-date protection
  - Computers with out-of-date protection
  - Computers with partially enabled protection: Computers with any of the protection modules disabled.
  - Computers with protection errors
  - Computers pending restart
  - Computers with up-to-date knowledge
  - Computers with out-of-date knowledge
  - Updated computers (no connection to the server in the last 72 hours)

- Updated computers (no connection to the server in the last 7 days)
- Updated computers (no connection to the server in the last 30 days)
- Operating system:
  - All
  - Windows
  - Linux
  - Mac OS X
  - Android
- **Show computers in subgroups:** search in the group selected from the group tree and all its subgroups.

### Unprotected tab

- **Find computer:** Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'
- **Computer status:**
  - All
  - Unprotected computers
  - **Unmanaged computers:** Computers on the network without an agent installed and discovered by the discovery tool.
  - Computers installing the protection
  - Computers uninstalling the protection
  - Computers with errors during installation
  - Computers with errors during uninstallation
  - Computers with unknown name
- **Operating system:**
  - All
  - Windows
  - Linux
  - Mac OS X
  - Android
- **Show computers in subgroups:** Search in the group selected from the group tree and all its subgroups.

### Without a license tab

- **Find computer:** Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'

### Excluded tab

- **Find computer:** Here you can run searches for computers using text strings to coincide with entries in the fields 'name' and 'comments'

## 18.3.2 Lists of computers

Once the search criteria is established, a list is displayed with the computers that meet the criteria.

This list is displayed as a table with a series of columns, which will vary depending on the tab describing the status of the computer.

 *If different computers have the same name and IP address, they will only be displayed as different computers in the Web console if their MAC address and management agent identifier are different. To change the way your computers are presented, click the  icon located at the top of the Web console. For more information, refer to chapter 5 The Web management console.*

### Protected tab

- **Computer:** This shows the list of protected computers, presented either by their name or by their IP address.
- **Protection update:** This indicates the protection status. Move the mouse pointer over the icon to display the meaning of the icon and the protection version.
  -  Updated
  -  Not updated
  -  Awaiting restart
- **Knowledge update:** This indicates the status of the signature file. Move the mouse pointer over the icon to display the meaning of the icon and the update date.
  -  Updated
  -  Hasn't connected in the last 72 hours
  -  Not updated
- **Protection:** Indicates the protection level of the computer. Move the mouse pointer over the icon to display the protections enabled.
  -  All available protections are enabled
  -  Some of the available protections are disabled
  -  Systems with on-demand or scheduled protections
  -  One or more of the protections has an error
- **Last connection:** Date on which the computer last connected to the **Adaptive Defense 360** server.
- **Remote access:** Indicates if the computer can be accessed by means of a remote control tool.
  -  The computer can be accessed using Panda Security's Remote Control tool. Refer to the Remote Control Administrator's Guide for more information about this tool.
  -  The computer has one or multiple third-party remote access tools installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer. If the computer has multiple tools installed, placing the mouse pointer over the icon will display all of them. Select one to access the

computer remotely. Refer to chapter 20 Remediation tools for more information.

### Unprotected tab

- **Computer:** This shows the list of unprotected computers, presented either by their name or by their IP address.
- **Status:** This shows the status of the protection through a series of icons.
  -  Installed
  -  Uninstalled
  -  Uninstallation error
  -  Installation error
  -  Protection successfully uninstalled
- **Details:** Specifies the reason for the computer status. For example, if the status is Installation error, in **Details** you will see the error code. If the **Status** column shows **Unprotected**, the **Details** column will display Protection uninstalled.
- **Last connection:** This shows the date and time of the last connection with the computer.
- **Remote access:** If an icon is displayed in this column, it means that the computer has at least one remote access tool installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer.

### Without a license tab

- **Computer:** This shows the list of computers without a license, presented either by their name or by their IP address.
- **O.S.:** This shows the operating system and service pack version (in the case of Windows).
- **Reason:** This gives the reason why the computer doesn't have a license: insufficient valid licenses or the computer doesn't meet the restrictions of the group it belongs to.

### Excluded tab

- **Computer:** This column shows the list of all excluded computers, presented either by their name or by their IP address. If different computers have the same name and IP address, they will only be displayed as different computers in the Web console if their MAC address and management agent identifier are different. To change the way your computers are presented, click the  icon located at the top of the Web console. For more information, refer to chapter 5 The Web management console.
- **Group:** Group that the excluded computer belongs to.

### 18.3.3 Actions on selected computers

All the lists have an initial selection column. Click the box at the top to select (or unselect) all items in the list. At the foot of the table there is a pagination tool to ease navigation through the pages.

Select one or more computers in the table to take the actions available on the relevant tab.

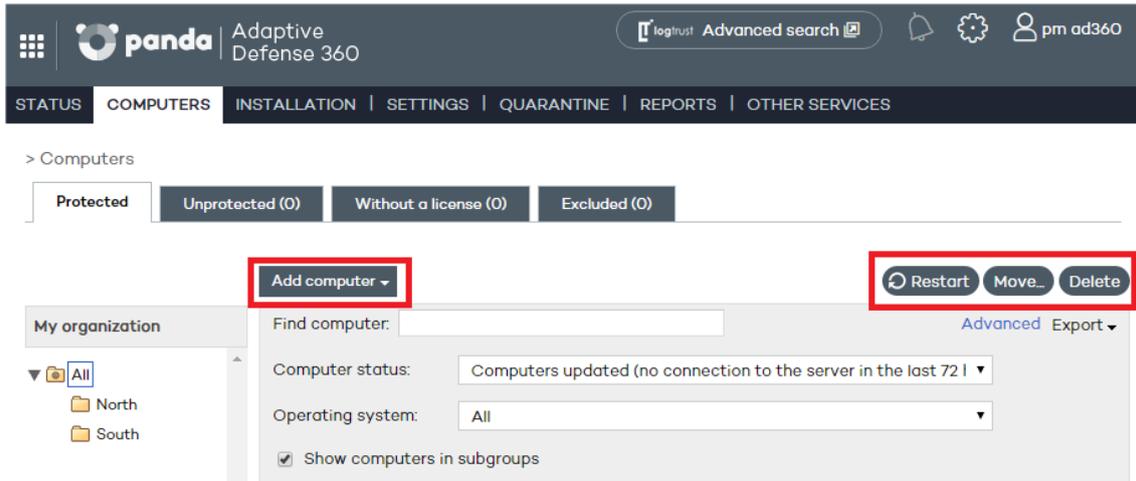


Figure 105: Buttons for managing computers

### Protected tab

- **Add computer:** This shows the **Adaptive Defense 360** agent installation wizard for adding new computers to the management console.
- **Restart:** This restarts the selected computers.
- **Move:** This lets you move the selected computers to another group.
- **Delete:** This option removes the computer from the **Adaptive Defense 360** database, although if the agent is not deleted, it will reappear after the next connection.
- **Remote access:** Indicates if the computer can be accessed by means of a remote control tool. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer. If the computer has multiple tools installed, placing the mouse pointer over the icon will display all of them. Select one to access the computer remotely.

### Unprotected tab

- **Delete selected computers:** The selected computers will be removed from the **Adaptive Defense 360** database.
- **Delete all computers**
- **Exclude selected computers**

### Without a license tab

- **Delete selected computers**
- **Delete all computers**
- **Exclude selected computers**

### Excluded tab

- **Delete selected computers**
- **Delete all computers**

## 18.3.4 Details of Windows, Linux and Mac OS X computers

If you want to access detailed information about a computer, click on it. You will be taken to the **Computer details** window, where you will find information about the computer's status regardless of

whether it is protected or not.

### Computer details

- **Name**
- **IP address**
- **Domain**: Only in Windows computers.
- **Active Directory path**: Only if the computer belongs to an Active Directory.
- **Group**
- **Installation date**
- **Protection version**
- **Agent version**
- **Knowledge date**: Signature file date.
- **Last connection**
- **Operating system**
- **Mail server**
- **Comments**: Use the **Comments** field if you want to add additional information to identify the computer. If you are a user with monitoring permissions, you will not be able to use this field.

### Protection

This displays the status of the protection modules (**Enabled, Disabled, Not applicable**).

- **Advanced protection**. This indicates the protection mode: Monitor, Hardening, Lock. It applies to Windows XP SP2 and later and Windows 2003 Server SP1 and later.
- **File protection**.
- **Mail protection**.
- **Internet browsing protection**.
- **Firewall protection**.
- **Device control**.
- **Antivirus protection for Exchange Server**.
- **Anti-spam protection for Exchange Server**.
- **Content filtering for Exchange Server**.
- **Web Access control**.

### Available tools



*See chapter 20 Remediation tools for more information.*

- **Disinfect computer**: **Adaptive Defense 360** automatically disinfects the malware it detects. If you need to remove advanced malware, use **Panda Cloud Cleaner**. Click the **Disinfect computer** button to use it.
- **Report problem with this computer**: Use this option if you want to report a computer problem

to Panda Security's qualified technicians.

- **Restart computers:** Use this option if you want to restart a computer, including those computers which appear on the list of protected computers as requiring a restart.
- **Delete from database:** Use this option if you want to delete a computer from the database, including those computers that have not connected to the server for a long time. You won't be able to access them or view any information about them.
- **Exclude:** Excluded computers will be shown in the list of excluded computers in the **Computers** window. No information or alerts will be displayed about them anywhere else in the console. You can undo these exclusions at any time.

### 18.3.5 Details of Android devices

In the case of Android devices, the **Computer details** window will display information about the device, and the status of its antivirus and Anti-Theft protection.

If the Anti-Theft feature is enabled for a device, a map will be displayed showing its location and the options provided by the protection: wipe, lock, snap the thief and locate.

If any of the protections displays an error, click the **How to fix errors** link to view a series of troubleshooting instructions to help you resolve the issue.

#### Computer details

The details here are the same as for Windows computers, except:

- **IP address:** Not displayed
- **Domain:** Not displayed
- **Active Directory Path:** Not displayed
- **Device ID:** Character string identifying the device in Adaptive Defense 360

#### Protections

This displays the protection modules enabled:

- Antivirus protection
- Anti-theft protection

#### Available tools

- **Wipe device:** Use the Wipe button to erase all the data on the device and restore its original factory settings.
- **Lock device:** Click the Lock device button to prevent access to it. Enter a four-digit unlock code.
- **Snap the thief:** This feature automatically takes a picture of anyone interacting with a stolen device. Enter the email address to send the picture to.
- **Privacy mode:** Administrators can allow end users to use their devices in privacy mode. This allows the user to disable the options to automatically report the device's location and take a picture of the thief, which will be password-protected.
- **Task list:** Shows a list of the tasks run on the device from the Web console. For more information, refer to the Task list section.

## Task list

The **Computer details** window shows a list of every task (theft alerts, wipe and locate) sent from the Web console to be run on the Android device.

The list shows a status for each task. For example: If there are three theft alert tasks, one of them will appear as **Run**, another one will appear as **Received** and the third one will be **Pending**. As the first task finishes and is removed from the list, the **Received** task will change its status to **Run** and the **Pending** task will change to **Received**.

- **Pending:** Tasks will appear as Pending during the time that elapses between the moment that the task is configured in the Web console and the moment that it is received at the device. Bear in mind that if the device is turned off or offline, the task will also appear as Pending.
- **Received:** In this case, the device has received the task but has not run it yet or the task is in progress and has not finished. For example, in the case of a locate task, the task will appear as Received until the device is effectively located. In the case of a snap the thief task, it will appear as Received as long as no picture is actually taken. That is because the task is not considered to be run until the thief triggers it, that is, touches the device screen.
- **Run:** A task will appear as Run once the device reports that it has been completed (successfully or not).

# 19. Reports

---

Report types

Generating and sending reports

## 19.1. Introduction

**Adaptive Defense 360** lets you generate reports about the security status of your network and any detections made over a given period of time. You can also select the content that will appear in the report, whether you want more detailed information, and if you want graphs.



*Each user will only be able to view those computers that they have permissions on.*

## 19.2. Report types

**Adaptive Defense 360** provides six types of reports:

- Executive report
- Status report
- Detection report
- Threats report
- Console access audit
- Computer status report

### 19.2.1 Executive report

#### Description

This report provides a summary of the three main aspects of network security:

- Status of the protection installed on the network
- Detections and infection attempts on the network
- Service status

#### Content

- Status of the protection installed, and items detected over the last 24 hours, the last 7 days and the last month.
- Top 10 computers with most malware detected and attacks blocked, respectively.
- Top 10 computers with most devices blocked.
- Information about the status of the licenses contracted.
- Number of computers on which the protection is being installed at the time of generating the report (including computers with installation errors).
- Number of spam messages detected.
- Top 10 accessed websites sorted by category.
- Top 10 computers with most Internet access attempts.
- Top 10 computers with most Internet access attempts blocked.

### Supported formats

- XML
- CSV
- TIFF
- PDF
- Web
- Excel

## 19.2.2 Status report

### Description

This report gives an overview of the protection and update status of all computers at the time of report generation. It also reports the number of computers on which the protection is being installed at the time of generating the report (including computers with installation errors).

### Supported formats

- XML
- CSV
- TIFF
- PDF
- Web
- Excel

## 19.2.3 Detection report

### Description

This report shows the detections made during the last 24 hours, the last 7 days, and the last month. It indicates the computer, the group, the type of detection, the number of detections made, the action taken, and the date when the detection took place.

### Supported formats

- XML
- CSV
- TIFF
- PDF
- Web
- Excel

## 19.2.4 Threats report

### Description

This report shows the threats detected by the advanced protection in the selected date range.

### Content

- Computers that represent the greatest risk, that is, those computers where most infections have been detected.
- Detailed information about each detected threat:
  - Malicious programs
  - Potentially unwanted programs (PUPs)
  - Programs under investigation in our lab

For each of these you can see the total number of infections, the number of devices on which they have been detected, whether they have been run, if they have made an external connection and if they have accessed data.

### Supported formats

- XML
- CSV
- TIFF
- PDF
- Web
- Excel

## 19.2.5 Console access audit report

### Description

This report shows the accesses to the console by the service administrators.

### Content

The report includes a line for each access to the Web console, and displays the following information:

- **User:** Login used to access the console.
- **Permissions:** Permissions of the administrator account used to access the console.
- **Login date:** Date and time when the user logged in to the console.
- **Logout date:** Date and time when the user logged out of the console.

### Supported formats

- XML
- CSV
- TIFF
- PDF
- Web
- Excel

## 19.2.6 Computer status report

### Description

Provides detailed information about the status of the computers on your network

### Content

- For each computer:
  - ID
  - IP address
  - Group it belongs to
  - Operating system
- Installed protection
  - Install date
  - Agent version
  - Protection version
- Updates
  - Status of the protection engine last update
  - Status of the knowledge last update
- Activation status for all protection modules (advanced protection, firewall, antivirus, device control, etc.)

### Supported formats

- CSV
- Excel

## 19.3. Generating and sending reports

In the Web console main window, click **Reports**. A new window will open, divided into the following sections:

- Report name and content
- Report scope
- Schedule sending by email

### 19.3.1 Report name and content

Select the name, type and period covered by the report (last 24 hours, last week or last month). The latter option only applies to the Executive, Detection and Threat reports.

Report name:

Report content:

- Executive (Summary of the network status and items detected)
  - Include information from:
  - License status
  - Protection status
  - Detections
- Status (A general view of the current status of the network)
- Detection (Evolution of detections)
- Threats (Active viruses and top risk users)

Figure 106: Configuring the report name and type

### 19.3.2 Report scope

Select the computers covered in the report. Computers are selected by groups.

Report scope:

My organization

- All
- DEFAULT
- CONT\_1
- CONT\_2

Figure 107: Selecting the groups included in the report

### 19.3.3 Scheduled reports

If you don't need to schedule and send the report, but want to view it immediately, click **Show report**. Set the **Frequency** field to **Do not send**. The report will be immediately generated, and will appear on the report list in the left-hand side of the window.

You can save a limitless number of reports. To access an existing report, simply click its name on the list that appears on the left side of the **Reports** window.

You can schedule tasks to send reports by email to selected recipients in different formats. To do that, enter the following data:

- **Frequency:** The frequency of sending the report. Depending on the option you choose you will be able to select a day of the week, the time of the day or the day of the month on which the report will be sent:
  - Monthly
  - Weekly
  - Daily
  - The 1st of the month
- **Format:** The report format

- XML
  - CSV
  - IFF
  - PDF
  - Web
  - Excel
- **To:** The recipient's email address
  - **CC:** Use this field if you want to 'carbon copy' another recipient
  - **Subject:** The subject line of the message

Schedule sending by email:

Frequency:	Weekly	Day:	Sunday	Hour:	08:00
Format:	XML				
To:	<input type="text"/>				
	<small>(Enter the values separated by a semi-colon ;)</small>				
CC:	<input type="text"/>				
Subject:	Adaptive Defense 360 report				

Figure 108: Configuring a scheduled report

You can schedule up to 27 report send tasks. If you reach that limit, you will need to delete a previous task to create a new one.

# 20. Remediation tools

---

- Automatic file disinfection
- On-demand file scanning and disinfection
- Advanced computer disinfection
- Computer restart
- Remote desktop access
- Anti-theft protection

## 20.1. Introduction

**Adaptive Defense 360** provides several remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle presented in chapter 3.

Some of these tools are automatic and don't require administrator intervention, whereas other require the execution of certain actions through the Web console.

All of the remediation tools included in **Adaptive Defense 360** can be used from the Web console without having to physically go to the affected user's computer, thus saving time and travel costs.

The table below illustrates the tools available for each platform and their type (manual or automatic).

Remediation tool	Platform	Type	Purpose
Automatic file disinfection	Windows, Mac OS X, Android	Automatic	To disinfect or quarantine malware at the time of infection.
Exploit blocking	Windows	Automatic/Manual	To block vulnerability exploit attempts and execution of malicious code in compromised processes.
On-demand file scanning and disinfection	Windows, Mac OS X, Linux, Android	Automatic (scheduled) / Manual	To scan, disinfect and quarantine malware at the time chosen by the administrator or at scheduled times.
Computer disinfection	Windows	Manual	To disinfect computers affected by both conventional and advanced malware particularly resilient to removal.
On-demand restart	Windows	Manual	Restarts computers to apply updates, finish manual disinfection tasks and fix protection errors.
Remote desktop access	Windows	Manual	Remote control tools to access infected computers.
Anti-Theft protection	Android	Manual	Tools that help you locate stolen devices and identify the potential thief.

Table 6: List of available remediation tools based on platform



Additionally, Adaptive Defense 360 offers a Remote Control module that allows administrators to remotely access users' devices via advanced troubleshooting tools without the need to install third-party products

## 20.2. Automatic file disinfection

Automatic disinfection is performed by the real-time advanced protection and the antivirus

protection.

Upon detecting malware, **Adaptive Defense 360** automatically cleans the affected item provided there is a disinfection method available. Otherwise, the item is moved to quarantine, as explained in chapter 18.

Automatic disinfection does not require administrator intervention, however, the **Enable permanent file protection** checkbox must be selected in the Antivirus section.



Refer to the relevant chapter for more information about the blocking modes available in Adaptive Defense 360 and the antivirus settings.

Advanced protection mode	Antivirus protection	Behavior
Audit	Enabled	Detection, disinfection, quarantine
Hardening, Lock	Enabled	Detection, blocking of unknown items, disinfection, quarantine
Audit	Disabled	Detection
Hardening, Lock	Disabled	Detection, blocking of unknown items

Table 7: **Adaptive Defense 360's** behavior based on the advanced protection and antivirus protection settings

### 20.3. Exploit blocking

Exploits are blocked by the advanced protection.

Exploit attempts can be blocked manually or automatically depending on the settings applied to the relevant computer, and the type of detected exploit.

Advanced protection mode	Restart required	Behavior	Risk
Detect, Block	NO	Automatic	NO
Detect, Block, Ask for permission	YES	Manual	YES
Detect, Block, Do not ask for permission	YES	Automatic	YES

Table 8: **Adaptive Defense 360's** behavior based on the advanced protection settings and the type of detected exploit

In those cases in which it is not possible to block the exploit before it gets run (Risk YES), it will be

necessary to check the actions taken by the compromised program. Refer to chapter 22 Forensic analysis for more information about the life cycle of the threats detected by **Adaptive Defense 360**.

## 20.4. On-demand file scanning and disinfection

To disinfect files on demand you must create scheduled scan tasks or run individual on-demand scans.

## 20.5. Advanced computer disinfection

Automatic disinfection may fail on computers infected with advanced malware or PUPs, as these threats are much harder to neutralize. These computers can be easily identified by administrators as they will cause new incidents to be constantly reported in the dashboard's **Activity** panel. Only in those cases will it be necessary to use the advanced disinfection tool.

Once you have identified the infected computers, launch our **Cloud Cleaner** disinfection tool remotely and directly from the reported incident itself. To do that, click the **Malicious programs and exploits** or **Potentially unwanted programs** panel (depending on the nature of the incident) in the **Activity** section. Click the specific incident and then click **Disinfect computer**. You can also disinfect a computer from the **Computer details** window (go to the **Computers** tab, click **Protected**, click the relevant computer and finally click **Disinfect computer**).

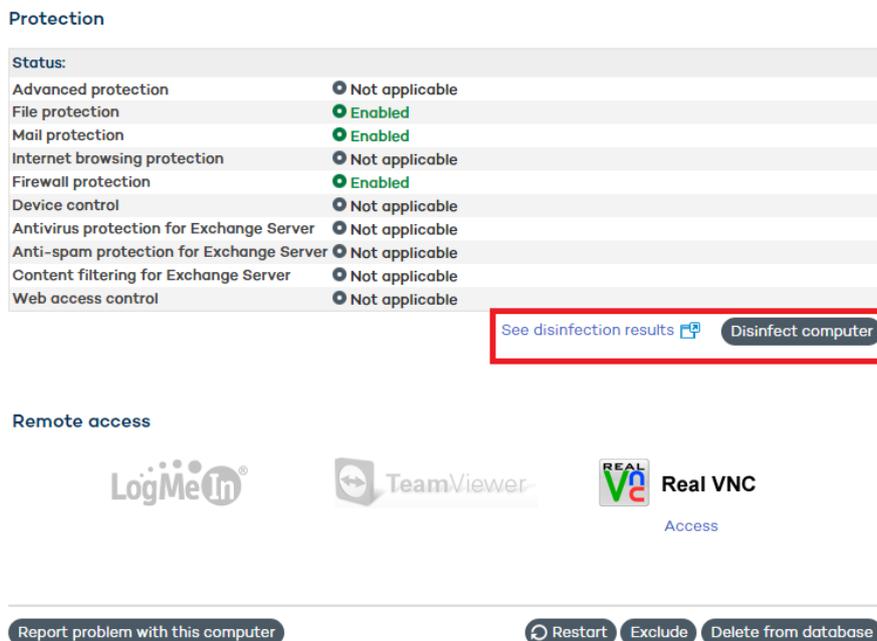


Table 9: Accessing the advanced disinfection tool *Cloud Cleaner*

You will then be shown a quick setup window.

The disinfection menu options are as follows:

- **Remove viruses:** This checkbox is always enabled and cleans the viruses found on the computer.
- **Delete PUPs:** Deletes potentially unwanted programs.
- **Clear browser cache:** Cleans the cache of the Web browser installed on the computer (Internet Explorer, Firefox or Chrome).
- **Delete browsing history:** Cleans the Web browsing history.
- **Delete browser cookies:** Deletes browser cookies.
- **Restore the system policies typically modified by malware:** Restores access to the task manager, shows file extensions, and generally restores all the system policies that the malware may have changed preventing their restoration to the original configuration chosen by the customer.
- **Do you want to display the disinfection console on the computer?** If the answer is yes, it shows the Cloud Cleaner console along with the disinfection results.

Once configured, a disinfection task will be created. Run the task, you'll be able to see the results by clicking the **See disinfection results** link.



*For more information about Cleaner Monitor, see the product's Web help or the link <http://pcopdocuments.azurewebsites.net/Help/pccm/es-ES/index.htm>*

*If you have problems disinfecting a PC, we advise you to manually download and run the most up-to-date version of Panda Cloud Cleaner from <http://pandacloudcleaner.pandasecurity.com>*

## 20.6. Computer restart

The Web console lets administrators restart computers remotely. This is very helpful if you have computers whose protection you need to update or protection problems to fix. Only those computers listed on the list of protected computers can be restarted remotely.

To do that, go to the **Computers** window / **Protected** tab, select the checkbox next to the computer or computers that you want to reboot, and click **Restart**.

## 20.7. Remote desktop access

**Adaptive Defense 360** lets administrators access computers remotely in two ways:

- Through Panda Security's Remote Control module.
- Through third-party remote access tools installed on the target computer.

This section deals only with third-party remote access tools. For more information about Panda Security's Remote Control module, refer to the Remote Control Administrator's Guide.

### 20.7.1 Viewing computers with remote access tools installed

The remote access feature lets you access your network computers from the management console without physically having to be in front of them.

**Adaptive Defense 360** lets you access your network computers using any of the following remote access tools:

- TeamViewer: from 3.x to 8.x
- RealVNC: 4.6.0, 4.5.4, 4.4.4, 4.3.2, 4.2.9 y VNC free 4.1.3
- UltraVNC: 1.0.9.5, 1.0.8.2, 1.0.6.5, 1.0.5.6 y 1.0.1.2
- TightVNC: 2.0.2, 2.0.1 y 2.0.0
- LogMeIn

A small icon will be displayed in the **Computers** window for any computer with any of these tools installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer.

You can enter the credentials from the **Computers** window or in the **Preferences** window accessible through the  icon located at the top of the console.

#### Remote Access

Let my service provider access my computers remotely.

Configure the credentials to access your computers remotely.

	User	Password
 LogMeIn	<input type="text"/>	<input type="text"/>
 TeamViewer	<input type="text"/>	<input type="text"/>
 VNC	<input type="text"/>	<input type="text"/>

Figure 109: Configuring the access credentials for the different remote access tools supported

If the computer has multiple tools installed, placing the mouse pointer over the icon will display all of them. Select one to access the computer remotely.

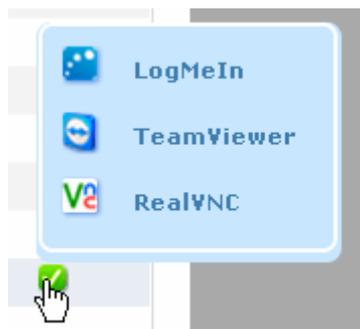


Figure 110: Remote access tool selection window

If a computer has different VNC tools installed, you will only be able to access it through one of them, in the following order of priority: 1-RealVNC, 2-UltraVNC, 3-TightVNC.

You will be able to access more or fewer computers depending on whether you have total control or administrator permissions.

 *If you only have monitoring permissions, you will not be able to access any computers, and the icon in the Remote access column will be grayed out.*

## 20.7.2 How to get remote access to another computer

### Remote access from the Computers window

The first time that you access the Computers window, a warning will be displayed indicating that the network computers don't have any remote access tools installed. If you want to install a remote access tool on them, click the link in the warning.

### Remote access from the Computer details window

You can also access computers remotely from the **Computer details** window, provided the selected computer has a remote access tool installed. If so, click the icon belonging to the remote access tool that you want to use.

Remote access



**Tight VNC**

Access

*Figure 111: Icon in the Computer details window indicating that the remote control tool TightVNC is installed on the user's computer*

To access other computers remotely, install one of the supported remote access tools on them: TightVNC, UltraVNC, RealVNC, TeamViewer or LogMeIn.

If a computer has multiple VNC tools installed, remember that you will only be able to access it using one of the tools in the specified order of priority.

## 20.7.3 How to use the remote access tools

### VNC tools

These tools can only be used to access computers on the same local network as the customer.

Depending on the authentication settings established, you might be able to access them without having to enter any credentials in the console, or otherwise you may have to enter a password, or a

user name and a password to establish a remote connection.

For an administrator to be able to access computers using VNC they must allow execution of a Java applet on their computer, otherwise, they will not be able to access them.

### TeamViewer

This tool can be used to access computers outside the customer's local network.

To access computers through TeamViewer you will only need to enter the computer password. The "user" field can be left blank.

The password you must enter to access a computer through TeamViewer is the computer's TeamViewer password or the password for unattended access to computers. It is not the customer's TeamViewer account password.

It is advisable to have the same TeamViewer password on all computers. The administrator's computer (the computer from which the **Adaptive Defense 360** Web console is accessed) must have TeamViewer installed (it is not enough to have it in "run without installation" mode).

### LogMeIn

This tool can be used to access computers outside the customer's local network.

To access computers via LogMeIn, you need to enter the LogMeIn account user name and password.

## 20.8. Anti-theft protection

The Anti-Theft protection included in **Adaptive Defense 360** will give you total control over your company's Android devices, and will allow you to take a series of actions in case of loss or theft.

Namely, you will be able to locate, lock and wipe your company's devices, take a picture of the thief, and send it by email to an address of your choice.

### 20.8.1 Enabling the anti-theft protection

In the Web console main window, click **Settings**. Then, click the name of the profile you want to configure the Anti-Theft protection for.

In the menu on the left, click the **Anti-Theft** option under Android. If you want **Adaptive Defense 360** to automatically report the device location, select the relevant checkbox.

Additionally, if you want to receive an email when there is activity on a stolen device, select the relevant checkbox. Then, enter the email address(es) that the picture of the potential thief will be sent to. Use a semicolon (;) to separate them.

If, together with the option to snap a picture of the thief, you select the option to report the device's

location, the email received will include a photo plus a map showing its location.

Once you have finished configuring the protection, go to the **Computer details** window to track the location of the device, lock it, and change the email address for the **Snap the thief** feature.

### **Privacy mode**

Administrators can allow end users to use their devices in privacy mode. This allows the user to disable the options to automatically report the device's location and take a picture of the thief, which will be password-protected.

However, it will still be possible to use those options on demand, but only if you have the password entered by the user.

To re-enable the options to automatically report the device's location and snap the thief, it will be necessary to disable the privacy mode.

# 21. Quarantine

---

Quarantine and Malware Freezer behavior  
Quarantine management

## 21.1. Introduction

**Adaptive Defense 360** stores in a designated area of the local computer's hard disk all items that appear to be suspicious or non-disinfectable, as well as the spyware and hacking tools detected.

The quarantine is centrally managed from the Web management console for all Windows computers, allowing administrators to restore, find and delete items without having to physically access users' computers.

## 21.2. Quarantine on Linux and Android devices

On Linux and Android devices, neither suspicious items nor detected malware are sent to quarantine. Detected malware is either disinfected or removed, and suspicious items are reported to the administrator, but no action is taken on them.

OS X computers only have a local quarantine. After a file has been sent to quarantine, you can choose to perform any of the available actions on it (mark as suspicious, repair or delete).

## 21.3. Quarantine and Malware Freezer behavior

### 21.3.1 Storing suspicious files

Quarantined items are stored on the user's computer, in the `%ProgramData%\Panda Security\Panda Security Protection\Quarantine` folder located in the **Adaptive Defense 360** software installation directory. This folder is encrypted and cannot be accessed by any other processes. Thus, it is not possible to directly access or run any quarantined items unless you do so using the corresponding restore tool from the Web console.

### 21.3.2 Sending suspicious items to quarantine

Files are automatically sent to quarantine once they have been scanned and provided they meet the conditions established by Panda Security's PandaLabs department.

Once an item is quarantined for analysis, there are four possible scenarios:

- The item is classified as malicious: It is disinfected and restored to its original location, provided there is a disinfection routine for it.
- The item is classified as malicious, but 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.
- The item is classified as suspicious: It is quarantined for a maximum of 30 days. If it finally turns out to be goodware, it will be automatically restored to its original location.

Restoring an item from quarantine not only restores the file itself but also its Windows permissions, owner, associated registry entries, etc.

## 21.4. Quarantine management

In the Web console main window, click **Quarantine**. A new window will open, divided into two sections: a search area and a section displaying the list of results.

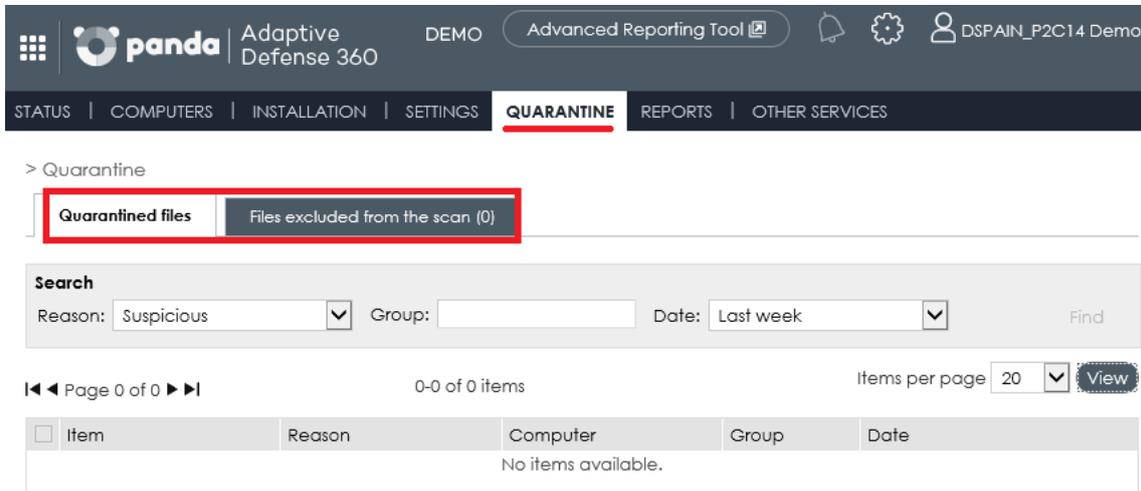


Figure 112: Quarantine window

### 21.4.1 Searching for quarantined items

The search area allows you to filter the items you want to view. There are three filtering parameters:

- **Reason:** Filters files according to the reason they were placed in quarantine. By default, the window displays the items that were sent to quarantine for being suspicious.
  - All
  - Suspicious
  - Infected
  - PUP: Potentially unwanted programs
- **Group:** Once you have selected the type of file you want to find, select the computer group or subgroup you want to search in.
- **Date:** Select the period you want.
  - All
  - Last 24 hours
  - Last week
  - Last month

### 21.4.2 Restoring quarantined items

To restore an item, select the relevant checkbox, click **Restore** and respond affirmatively to the confirmation message. The item will disappear from the search list, and will be moved to the **Files excluded from the scan** window.

If you want to delete any of the items found, select the relevant checkbox, click **Delete** and respond affirmatively to the confirmation message.

### 21.4.3 List of quarantined items

If there are several items that contain the same type of malware, restoring or deleting one of them will also restore or delete the others.

Place the mouse pointer over any of the items in the search list to display a yellow tag with specific information:

- **Computer:** Displays the computer's name or IP address.
- **Group:** Indicates the group to which the computer belongs. The full path of the group is only displayed in the tooltip.

### 21.4.4 Files excluded from scans

If you select an item in the Quarantine window and restore it, the item in question will disappear from the **Quarantined files** section and will be moved to the **Files excluded from the scan** tab.

Just as it is possible to exclude items from quarantine, so it is possible to return them to quarantine. To do that, select the checkbox next to the item that you want to return, and click **Undo exclusion**. Then, respond affirmatively to the confirmation message.

The item will disappear from the list of exclusions, and will be quarantined again as soon as it is detected.

# 22. Forensic analysis

---

Forensic analysis using the action tables

Forensic analysis using the activity graphs

Interpreting the action tables and activity graphs

## 22.1. Introduction

When the **Adaptive Defense 360** dashboard displays an infection, it needs to be determined to what extent the network has been compromised and what the source of the infection was.

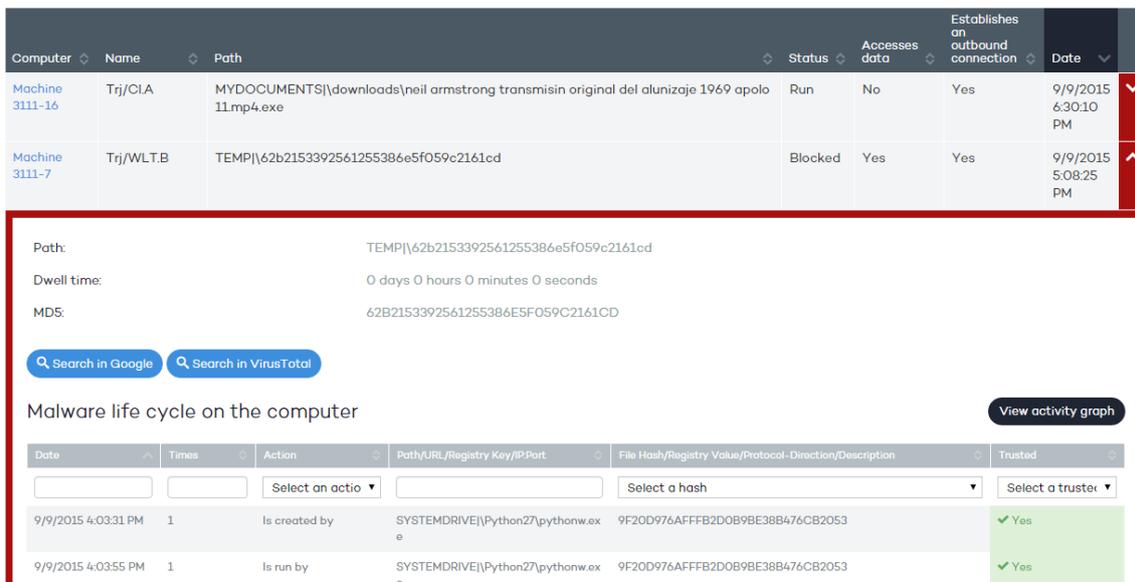
Next-generation malware is characterized by going undetected for long periods of time, taking advantage of this to access sensitive data or company intellectual property. Its objective is economic gain, either through blackmail by encrypting company documents or selling the information obtained to the competition, among other strategies common to these types of attacks.

Whatever the case, it is vital to determine the actions that the malware performed on the network in order to take appropriate measures. **Adaptive Defense 360** is able to continuously monitor all actions triggered by threats and store them to show their path, from their initial appearance on the network until their neutralization.

**Adaptive Defense 360** visually displays this type of information in two ways: through action tables and graphs.

## 22.2. Forensic analysis using the action tables

The **Status** window lets you access lists of the threats detected on the network by clicking the panels available in the **Activity** section. Click any of the threats to obtain a table with detailed information about their activity.



The screenshot shows a table of detected threats and a detailed view of a specific threat's activity.

Computer	Name	Path	Status	Accesses data	Establishes an outbound connection	Date
Machine 3111-16	Trj/CLA	MYDOCUMENTS\downloads\neil armstrong transmisin original del alunizaje 1969 apolo 11.mp4.exe	Run	No	Yes	9/9/2015 6:30:10 PM
Machine 3111-7	Trj/WLT.B	TEMP\62b2153392561255386e5f059c2161cd	Blocked	Yes	Yes	9/9/2015 5:08:25 PM

**Malware life cycle on the computer**

Path: TEMP\62b2153392561255386e5f059c2161cd  
 Dwell time: 0 days 0 hours 0 minutes 0 seconds  
 MD5: 62B2153392561255386E5F059C2161CD

Search in Google Search in VirusTotal

Date	Times	Action	Path/URL/Registry Key/IP/Port	File Hash/Registry Value/Protocol-Direction/Description	Trusted
9/9/2015 4:03:31 PM	1	Is created by	SYSTEMDRIVE\Python27\pythonw.exe	9F20D976AFFFB2D0B98E38B476CB2053	Yes
9/9/2015 4:03:55 PM	1	Is run by	SYSTEMDRIVE\Python27\pythonw.exe	9F20D976AFFFB2D0B98E38B476CB2053	Yes

Figure 113: Accessing a threat's actions/life cycle

### 22.2.1 Malware details

The fields in this table are as follows:

- **Path:** Path of the executable file that contains the malware.

- **Dwell time:** Time during which the threat has been on the system without being classified.
- **User:** User that was logged in on the system at the time of the attack.
- **MD5:** MD5 hash value of the threat. This can be used to look for information on Google or VirusTotal.
- **Detection technology:** Indicates the scan engine that detected the threat (**Advanced protection** for events detected when monitoring the actions taken by processes, or **Antivirus** for signature-based detections).
- **Infection source computer:** Displays the name of the computer the infection originated from, if applicable.
- **Infection source IP address:** Displays the IP address of the computer the infection originated from, if applicable.
- **Infection source user:** The user that was logged in on the computer the infection originated from.
- **Malware life cycle on the computer:** This is a table that details every action taken by the threat.
- **Occurrences on the network:** List of computers on the network where the malware has been found, along with the date when it was first seen.

Additionally, there are two buttons to search for further information on the Internet using Google and the VirusTotal website.

### 22.2.2 Exploit details

The fields in this table are as follows:

- **Compromised program:** Path of the program that was hit by the exploit attempt.
- **Action:** Action taken by **Adaptive Defense 360** based on the security policy set by the administrator.
  - Allowed by the user:** The user declined the administrator's request to restart the system or end the compromised process to block the exploit (the security policy was **Block. Ask the user for permission to end the process**).
  - Allowed by the administrator:** Exploit detected on a computer whose protection was configured in **Audit** mode.
  - Blocked (immediately):** The exploit was immediately blocked before being run (the security policy was **Block**). There was no need to end the compromised program or restart the affected computer.
  - Blocked after the process was ended:** The exploit was detected and blocked after the compromised program was ended or the affected computer was restarted (the security policy was **Block**).
  - Detected. Pending restart:** The exploit has been detected and requires a computer restart to be blocked (the security policy is **Block**). The computer hasn't been restarted yet.
- **Risk:**
  - YES:** The target computer has been at risk. Blocking the exploit required ending the compromised process or restarting the affected computer regardless of the security settings established by the administrator.
  - NO:** The exploit was blocked automatically. It wasn't necessary to end the compromised

process.

- **User:** The user that was logged in on the system when the exploit attempt took place.
- **MD5:** MD5 hash of the compromised process.
- **Detection technology:** Anti-exploit.
- **Possible source of the exploit:** If the exploit was launched from a compromised website, the table will display the URLs accessed by the Internet browser at the time of the attack. Other types of exploits will display the files accessed by the compromised process.
- **Compromised program version:** Internal version of the compromised program. This appears in the executable file's header.
- **Vulnerable program:** The compromised program is not updated to the latest version and has known vulnerabilities that can be leveraged by attackers.
- **Exploit life cycle on the computer:** This is a table that details every action taken by the compromised program.
- **Occurrences on the network:** List of computers on the network where the threat has been found, along with the date when it was first seen on each computer.

### 22.2.3 Action table

The action table for the threat includes only relevant events, because the amount of actions triggered by a process is so high that it would prevent the extraction of useful information for a forensic analysis.

The table content is initially presented in date order, making it easier to follow the development of the threat.

The fields included in the action table are detailed below:

- **Date:** Date of the action.
- **Times:** Number of times the action was executed. A single action executed several times consecutively only appears once in the list of actions.
- **Action:** Action implemented. Below is a list of the actions that can appear in this field:
  - File download
  - Communicates with
  - Accesses data
  - Is run by
  - Runs
  - Is created by
  - Creates
  - Is modified by
  - Modifies
  - Is loaded by
  - Loads
  - Delete
  - Is deleted by
  - Is renamed by

- Renames
- Is killed by
- Kills process
- Creates remote thread
- Has a thread injected by
- Opens
- Is opened by
- Is created by
- Creates
- Creates Reg Key pointing to an exe file
- Modifies Reg Key pointing to an exe file
- **Path/URL/Registry key/IP:Port:** Action entity. Depending on the action type it can contain:
  - **Registry key:** For all actions that involve modifying the Windows registry
  - **IP:port:** For all actions that involve communicating with a local or remote computer
  - **Path:** For all actions that involve access to the computer hard disk
  - **URL:** For all actions that involve access to a URL
- **File Hash/Registry Value/Protocol-Direction/Description:** This field complements the entity. Depending on the action type it can contain:
  - **File Hash:** For all actions that involve access to a file
  - **Registry Value:** For all actions that involve access to the registry
  - **Protocol-Direction:** For all actions that involve communicating with a local or remote computer. The possible values are:
    - TCP
    - UDP
    - Bidirectional
    - UnKnown
    - Description
- **Trusted:** The file is digitally signed

To locate actions of most interest in the list, there is a series of filters in the table header.



Figure 114: Action table filter tool

Some of the fields are text type fields and others are drop-down menus with all the various occurrences given in the selected column. Text searches are flexible and do not require the use of wildcards to search within the text string.

### 22.2.4 Subject and predicate in actions

To correctly understand the format used to present the information in the action list, a parallel needs to be drawn with the natural language:

- All actions have as the subject the file classified as malware. This subject is not indicated in each line of the action table because it is common throughout the table.
- All actions have a verb which relates the subject (the classified threat) with an object, called the entity. The entity is indicated in the **Path/URL/Registry Key/IP:Port** field of the table.
- The entity is complemented with a second field which adds information to the action, which is the **File Hash/Registry Value/Protocol-Direction/Description** field.

The example below illustrates two actions carried out by the same hypothetical malware:

Date	Times	Action	Path/URL/Registry Key/IP:Port	Hash/Registry Value/Protocol-Direction/Description	Trusted
3/30/2015 4:38:40 PM	1	Communicates with	54.69.32.99:80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Loads	PROGRAM_FILES \MOVIES TOOLBAR\SAFETYNT\SAFETYCRT.DLL	9994BF035813FE8EB6BC98E CCBD5B0E1	NO

*Table 10: Example of active actions taken by a threat*

The first action indicates that the malware (subject) **connects to (action)** the IP address 54.69.32.99:80 (entity) through the TCP-bidirectional protocol.

The second action indicates that the malware (subject) **loads (action)** the library PROGRAM\_FILES|\MOVIES TOOLBAR\SAFETYNT\SAFETYCRT.DLL with hash 9994BF035813FE8EB6BC98ECCBD5B0E1

As with natural language, two types of sentences are implemented in **Adaptive Defense 360**:

- **Active:** These are predicative actions (with a subject and predicate) related by an active verb. In these actions, the verb of the action relates the subject, which is always the process classified as a threat, and a direct object, the entity, which can be multiple according to the type of action.
- **Passive:** These are actions where the subject (the process classified as malware) becomes the passive subject (which receives rather than executes the action), and the verb is passive (to be + participle). In this case, the passive verb relates the passive subject which receives the action with the entity, which performs the action.

Examples of active actions are:

- Connects to
- Loads
- Creates

Examples of passive actions are:

- Is created by
- Is downloaded from

An example of a passive action is:

Date	Times	Action	Path/URL/Registry key/IP:Port	Hash/Registry Value/Protocol-Direction/Description	Trusted
3/30/2015 4:51:46 PM	1	Is run by	WINDOWS   \explorer.exe	7522F548A84ABAD8FA516DE5AB3931EF	NO

Table 11: Example of a passive action inflicted on a file

In this action, the malware (passive subject) is run by (passive action) the WINDOWS | \explorer.exe program (entity) with hash 7522F548A84ABAD8FA516DE5AB3931EF



*Active actions let you inspect in detail the steps taken by the malware. By contrast, passive actions usually reflect the infection vector used by the malware (which process run it, which process copied it to the user's computer, etc.).*

### 22.3. Forensic analysis using the activity graphs

Execution graphs visually display the information shown in the action tables, emphasizing the temporal aspect.

The graphs are initially used to provide, at a glance, a general idea of the actions triggered by the threat.

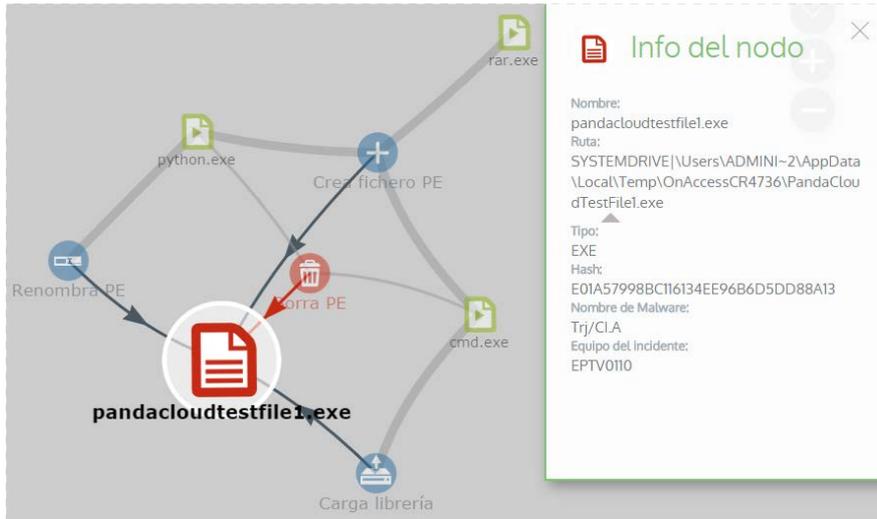


Figure 115: Information displayed by a node in the activity graph

### 22.3.1 Diagrams

The string of actions in the execution graph view is represented by two items:

- **Nodes:** They mostly represent actions or information items
- **Lines and arrows:** They unite the action and information nodes to establish a temporal order and assign each node the role of "subject" or "predicate".

### 22.3.2 Nodes

The nodes show the information through their associated icon, color and descriptive panel on the right of the screen when selected with the mouse.

The color code used is as follows.

- **Red:** Untrusted item, malware, threat.
- **Orange:** Unknown item, unclassified.
- **Green:** Trusted item, goodware.

Listed below are action-type nodes with a brief description:

Symbol	Description
	File downloaded Compressed file created
	Socket / communication used
	Monitoring initiated
	Process created
	Executable file created Library created Key created in the registry
	Executable file modified Registry key modified
	Executable file mapped for write access
	Executable file deleted
	Library loaded
	Service installed
	Executable file renamed
	Process stopped or closed
	Thread created remotely

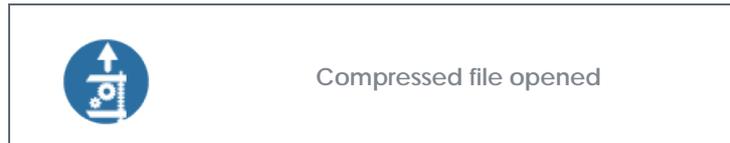


Table 12: Action-type nodes and associated information

Listed below are descriptive-type nodes with a brief description:

Symbol	Description
	File name and extension <b>Green:</b> Goodware <b>Orange:</b> Unclassified <b>Red:</b> Malware/PUP
	Internal computer (it is on the corporate network) <b>Green:</b> Trusted <b>Orange:</b> Unknown <b>Red:</b> Untrusted
	External computers <b>Green:</b> Trusted <b>Orange:</b> Unknown <b>Red:</b> Untrusted
	Country associated with the IP address of an external computer
	File and extension
	Registry key

Table 14: Descriptive-type nodes and associated information

### 22.3.3 Lines and arrows

The lines of the graphs relate the different nodes and help to establish the order in which the actions performed by the threat were executed.

The two attributes of a line are:

- **Line thickness:** The thickness of a line which joins two nodes indicates the number of occurrences that this relationship has had in the graph. The greater number of occurrences, the greater the size of the line
- **Arrow:** Marks the direction of the relationship between the two nodes

### 22.3.4 The timeline

The timeline helps control the display of the string of actions carried out by the threat over time. Use the buttons at the bottom of the screen to position yourself at the precise moment when the threat

carried out a certain action, and retrieve extended information that can help you in the forensic analysis processes.

The timeline of the execution graphs looks like this:

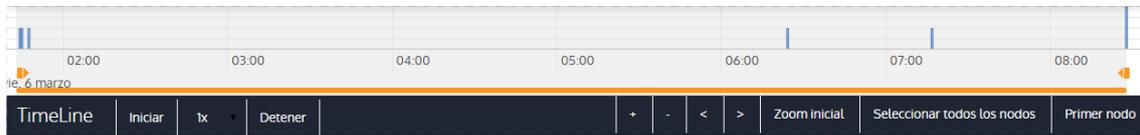


Figure 116: Threat life cycle timeline

Select a specific interval on the timeline by dragging the interval selectors to the left or right to cover the timeframe of most interest to you.



Figure 117: Selecting a time interval in the timeline

After selecting the timeframe, the graph will only show the actions and nodes that fall within that interval. The rest of the actions and nodes will be blurred on the graph.

The actions carried out by the threat are represented on the timeline as vertical bars accompanied by the timestamp, which marks the hour and minute when they occurred.



Figure 117: Date/time information of the actions taken by a threat

### 22.3.5 Zoom in and Zoom out

The + and - buttons of the time bar allow you to zoom in or zoom out for higher resolution if there are many actions in a short time interval.

### 22.3.6 Timeline

To view the string of actions run by the threat, the following controls are used:

- **Start:** Starts the execution of the timeline at a constant speed of 1x. The graphs and lines of actions will appear while passing along the timeline.
- **1x:** Establishes the speed of traveling along the timeline
- **Stop:** Stops the execution of the timeline

- **+ and -**: Zoom in and zoom out of the timeline
- **< and >**: Moves the node selection to the immediately previous or subsequent node
- **Initial zoom**: Restores the initial zoom level if modified with the + and – buttons
- **Select all nodes**: Moves the time selectors to cover the whole timeline
- **First node**: Establishes the time interval at the start, a necessary step for initiating the display of the complete timeline

 *To display the full path of the timeline, first select "First node" and then "Start". To set the travel speed, select the button 1x.*

### 22.3.7 Filters

The controls for filtering the information shown are at the top of the graph.

The filtering criteria available are:

- **Action**: Drop-down menu which lets you select an action type from all those executed by the threat. This way, the graph only shows the nodes that match the action type selected and the adjacent nodes associated with this action
- **Entity**: Drop-down menu which lets you choose an entity (the content of the field Path/URL/Registry key/IP:port)

### 22.3.8 Node movement and general zoom

To move the graph in four directions and zoom in or zoom out, you can use the controls in the top right of the graph.

 *To zoom in and zoom out more easily, you can use the mouse scroll wheel.*

The X symbol allows you to leave the graph view.



Figure 118: Graph controls

If you would rather hide the timeline button zone to use more space on the screen for the graph,

you can select the  symbol located in the bottom right of the graph.

Finally, the behavior of the graph when it is displayed on screen or dragged by one of its nodes can

be configured using the panel shown below, accessible by selecting the  button in the top left of the graph.

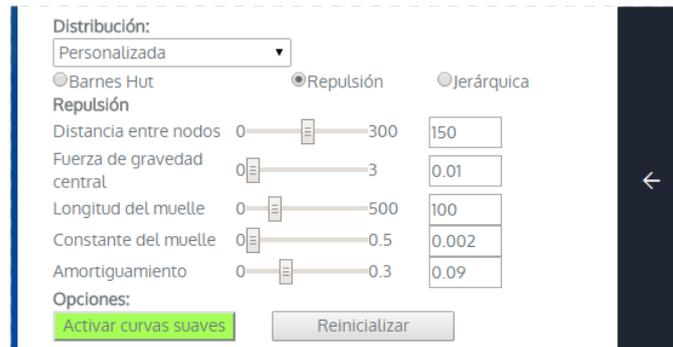


Figure 119: Graph settings panel

## 22.4. Interpreting the action tables and activity graphs

Certain technical knowledge is required to correctly interpret the action tables and activity graphs, as both resources are representations of the dumping of the evidence collected, which must be interpreted by the company's network administrator.

In this chapter, some basic interpretation guidelines are offered through several real malware examples.

 *The name of the threats indicated here can vary among different security vendors. You should use the hash ID to identify specific malware.*

### 22.4.1 Example 1: Viewing the actions executed by the malware Trj/OCJ.A

The top of the alerts table shows critical information about the malware found. In this case the important data is as follows:

- **Date:** 06/04/2015 3:21:36
- **Computer:** XP-BARCELONA1
- **Name:** Trj/OCJ.A
- **Type:** MW
- **Status:** Run
- **Malware path:** TEMP | \Rar\$EXa0.946\appnee.com.patch.exe

Status

The malware status is Run due to the fact that the **Adaptive Defense 360** mode configured was Hardening: The malware already resided on the computer when **Adaptive Defense 360** was installed and was unknown at the time of running.

### Hash

The hash string can be used to obtain more information on sites such as VirusTotal to gain a general idea of the threat and how it works.

### Malware path

The path where the malware was detected for the first time on the computer belongs to a temporary directory and contains the RAR string. Therefore, it comes from a RAR file temporarily uncompressed in the directory, and which gave the appnee.com.patch.exe executable as the result.

### Action table

Step	Date	Action	Path
1	3:17:00	Created by	PROGRAM_FILES   \WinRAR\WinRAR.exe
2	3:17:01	Is run by	PROGRAM_FILES   \WinRAR\WinRAR.exe
3	3:17:13	Creates	TEMP   \bassmod.dll
4	3:17:34	Creates	PROGRAM_FILES   \Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifies	PROGRAM_FILES   \Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Deletes	PROGRAM_FILES   \ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK
7	3:17:41	Creates	PROGRAM_FILES   \Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifies	PROGRAM_FILES   \Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll
9	3:17:59	Runs	PROGRAM_FILES   \Google\Chrome\Application\chrome.exe

Table 13: Action table (Example 1)

Steps 1 and 2 indicate that the malware was uncompressed by WinRAR.Exe and run from that program. The user opened the compressed file and clicked its binary.

Once run, in step 3 the malware created a DLL file (bassmod.dll) in a temporary folder, and another one (step 4) in the installation directory of the Adobe Acrobat 11 program. In step 5, it also modified an Adobe DLL file, to take advantage perhaps of some type of program vulnerability.

After modifying other DLL files, it launched an instance of Chrome which is when the timeline finishes. **Adaptive Defense 360** classified the program as a threat after that string of suspicious actions and stopped its execution.

The timeline shows no actions on the registry, so it is very likely that the malware is not persistent or has not been executed up to the point of surviving a restart of the computer.

The Adobe Acrobat 11 software has been compromised so a reinstall is recommended; however, thanks to the fact that **Adaptive Defense 360** monitors both goodware and malware executables, the execution of a compromised program will be detected when it triggers dangerous actions, and ultimately be blocked.

### 22.4.2 Example 2: Communication with external computers by BetterSurf

BetterSurf is a potentially unwanted program that modifies the Web browser installed on the user's computer and injects ads in the Web pages that they visit.

The top of the alerts table shows critical information about the malware found. The following data is provided in this case:

- **Date:** 3/30/2015
- **Computer:** MARTA-CAL
- **Name:** PUP/BetterSurf
- **Type:** MW
- **Malware path:** PROGRAM\_FILES | \VER0BLOCKANDSURF\N4CD190.EXE
- **Dwell time:** 11 days 22 hours 9 minutes 46 seconds

#### Dwell time

In this case, the dwell time was very long: the malware was dormant on the customer's network for almost 12 days. This is increasingly normal behavior and may be for various reasons: perhaps because the malware has not carried out any suspicious action until very late, or simply because the user downloaded the file but did not run it at the time.

#### Action table

Step	Date	Action	Path / IP
1	08/03/2015 11:16	Created by	TEMP   \08c3b650-e9e14f.exe
2	03/18/2015 11:16	Is run by	SYSTEM   \services.exe
3	03/18/2015 11:16	Loads	PROGRAM_FILES   \VER0BLOF\N4Cd190.dll
4	03/18/2015 11:16	Loads	SYSTEM   \BDL.dll
5	03/18/2015 11:16	Communicates with	127.0.0.1:13879
6	03/18/2015 11:16	Communicates with	37.58.101.205:80
7	03/18/2015 11:17 AM	Communicates with	5.153.39.133:80
8	03/18/2015 11:17 AM	Communicates with	50.97.62.154:80
9	03/18/2015 11:17 AM	Communicates with	50.19.102.217:80

Table 16: Action table (Example 2)

Here it can be seen how the malware established communication with several different IP addresses.

The first of them (step 5) is the computer itself, and the rest are external IP addresses to which it connects via port 80 and from which the advertising content is probably downloaded.

The main prevention measure in this case will be to block those IP addresses in the corporate firewall.



*Before adding rules to block IP addresses in the corporate firewall, you should consult the IP addresses to be blocked in the associated RIR (RIPE, ARIN, APNIC, etc.) to see the network to which they belong. In many cases, the remote infrastructure used by the malware is shared with legitimate services housed in providers such as Amazon and similar, so blocking IP addresses would be the same as blocking access to normal Web pages.*

### 22.4.3 Example 3: Access to the registry by PasswordStealer.BT

PasswordStealer.BT is a Trojan that records the user's activity on the computer and sends the information obtained to the exterior. Among other things, it is able to capture the user's screen, record the keystrokes and send files to a C&C (Command & Control) server.

The top of the alerts table shows critical information about the malware found. The following data is provided in this case:

- **Malware path:** APPDATA | \microsoftupdates\micupdate.exe

The name and location of the executable indicate that the malware poses as a Microsoft update. This particular malware is not able to infect computers by itself; it requires the user to run the virus manually.

#### Status

The malware status is Run due to the fact that the **Adaptive Defense 360** mode configured was Hardening: The malware already resided on the computer when **Adaptive Defense 360** was installed and was unknown at the time of running.

#### Action table

Step	Date	Action	Path
1	03/31/2015 23:29	Is run by	PROGRAM_FILESX86   \internet explorer\iexplore.exe
2	03/31/2015 23:29	Created by	INTERNET_CACHE   \Content.IE5\QGV8PV80\index[1].php
3	03/31/2015 23:30	Creates Reg Key to exe file	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\CurrentVersion \Run?MicUpdate
4	03/31/2015 23:30	Runs	SYSTEMX86   \notepad.exe
5	03/31/2015 23:30	Remote thread created by	SYSTEMX86   \notepad.exe

Table 17: Action table (Example 3)

In this case the malware is created in step 2 by a Web page and run by Internet Explorer.



*The order of actions has a granularity of 1 microsecond. For this reason, several actions executed within the same microsecond may not appear in order in the timeline, as in step 1 and step 2.*

Once run, the malware becomes persistent in step 3 adding a branch in the registry which will launch the program when the computer starts up. It then starts to execute malware actions such as opening the notepad and injecting code in one of its threads.

As a remedial action in this case and in the absence of a known disinfection method, you can minimize the impact of this malware by deleting the registry entry. It is quite possible that on an infected computer the malware prevents you from editing that entry; depending on the case, you would have to either start the computer in safe mode or with a bootable CD to delete that entry.

#### 22.4.4 Example 4: Access to confidential data by Trj/Chgt.F

Trj/Chgt.F was published by Wikileaks at the end of 2014 as a tool used by government agencies in some countries for selective espionage.

In this example, we'll go directly to the action table to show you the behavior of this advanced threat.

##### Action table

Step	Date	Action	Path
1	4/21/2015 2:17:47 PM	Is run by	SYSTEMDRIVE   \Python27\pythonw.exe
2	4/21/2015 2:18:01 PM	Accesses data	#.XLS
3	4/21/2015 2:18:01 PM	Accesses data	#.DOC
4	4/21/2015 2:18:03 PM	Creates	TEMP   \doc.scr
5	4/21/2015 2:18:06 PM	Runs	TEMP   \doc.scr
6	4/21/2015 2:18:37 PM	Runs	PROGRAM_FILES   \Microsoft Office\Office12\WINWORD.EXE
7	4/21/2015 8:58:02 PM	Communicate s with	192.168.0.1:2042

Table 18: Action table (Example 4)

The malware is initially run by the Python interpreter (step 1) to later access an Excel and Word document (steps 2 and 3). In step 4, a file with a .SCR extension is run, probably a screensaver with some type of flaw or error that causes an anomalous situation in the computer and which might be exploited by the malware.

A TCP type connection occurs in step 7. The IP address is private, so the malware would be connecting to the customer's network.

In this case, the content of the files accessed must be checked to assess the loss of information, although looking at the timeline the information accessed seems to not have been extracted from

the customer's network.

**Adaptive Defense 360** will disinfect the threat, and automatically block subsequent executions of the malware for that customer and other customers.

# 23. Appendix 1: Centralized installation tools

---

Installation using Active Directory  
Installation using the distribution tool

### 23.1. Introduction

**Adaptive Defense 360** allows administrators to centrally install the Windows agent on small and medium-sized networks by using the centralized distribution tool (included free of charge) or third-party tools.

This chapter explains how to install the **Adaptive Defense 360** agent on a Windows network with Active Directory and with the distribution tool included in the solution.

### 23.2. Installation using Active Directory

Below we detail the steps for installation using GPO (Group Policy Object).

- Download and share the **Adaptive Defense 360** installer: Move the **Adaptive Defense 360** installer to a shared folder which is accessible to all the computers that are to receive the agent.
- Open the "Active Directory Users and Computers" applet and create a new OU (Organizational Unit) called "Adaptive Defense".

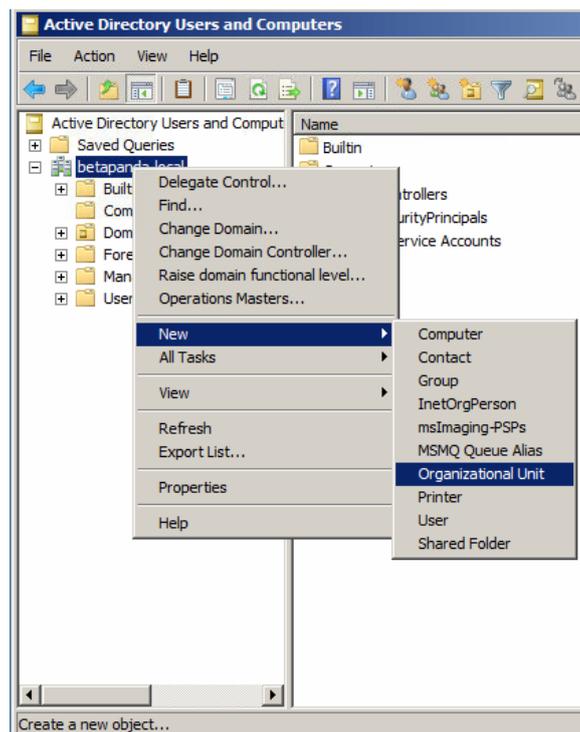


Figure 120: Creating a new Organizational Unit

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

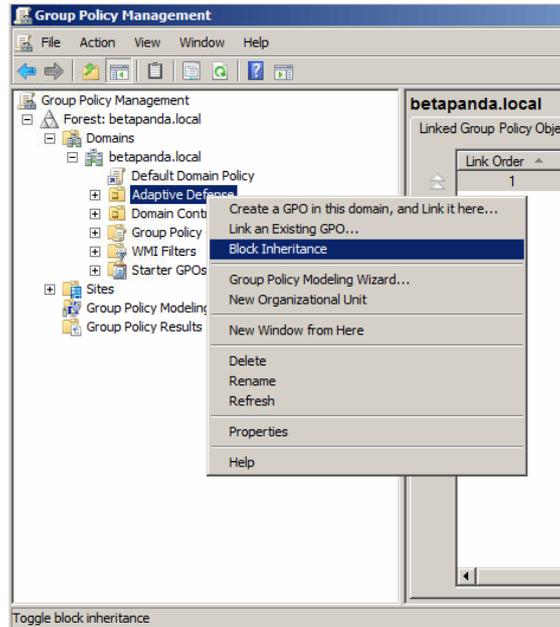


Figure 121: Blocking Inheritance

- Create a new GPO in the “Adaptive Defense” OU.

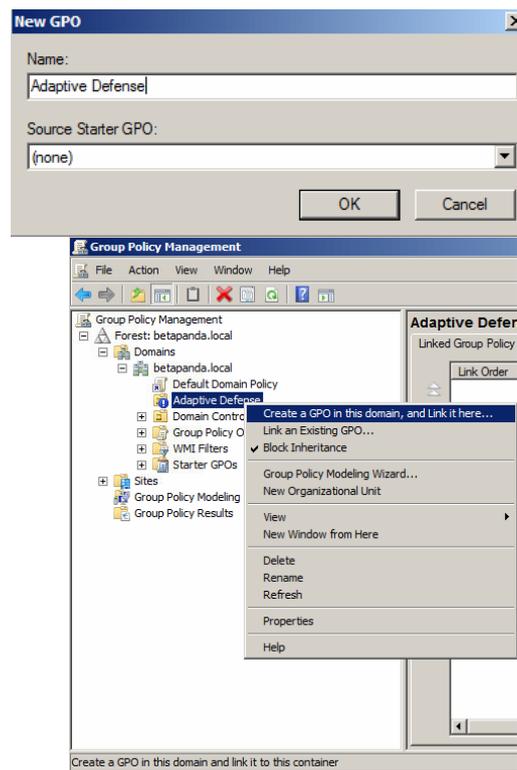


Figure 122: Creating a new GPO

- Edit the GPO and add a new installation Domain package which contains the **Adaptive Defense 360** agent. To do this, you will be asked to add the installer to the GPO

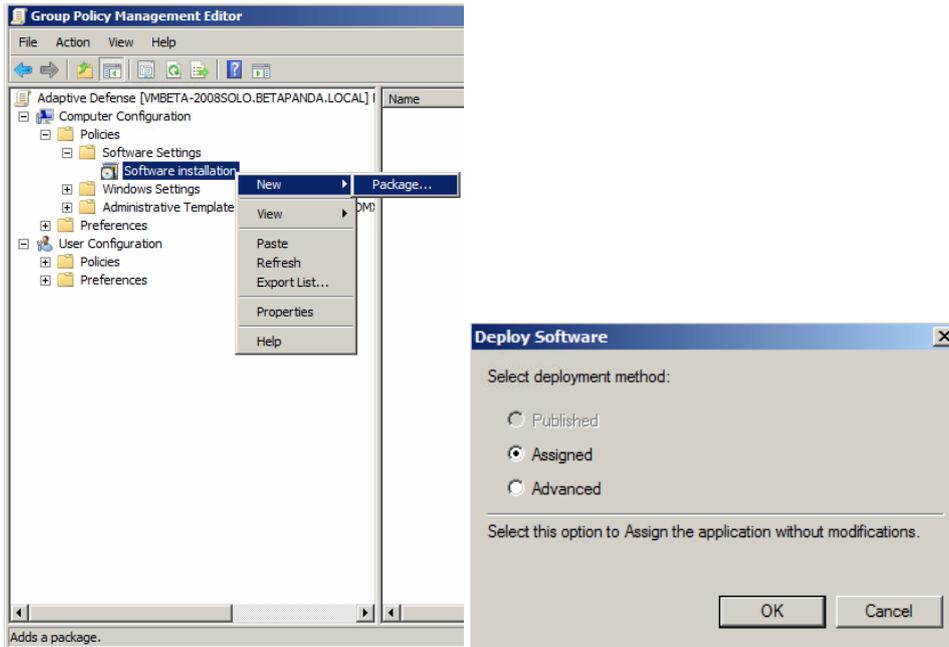


Figure 123: Creating a new installation package

- Once it has been added, go to Properties, Deployment, Advanced, and select the checkbox that bypasses checking the target operating system against the one defined in the installer.

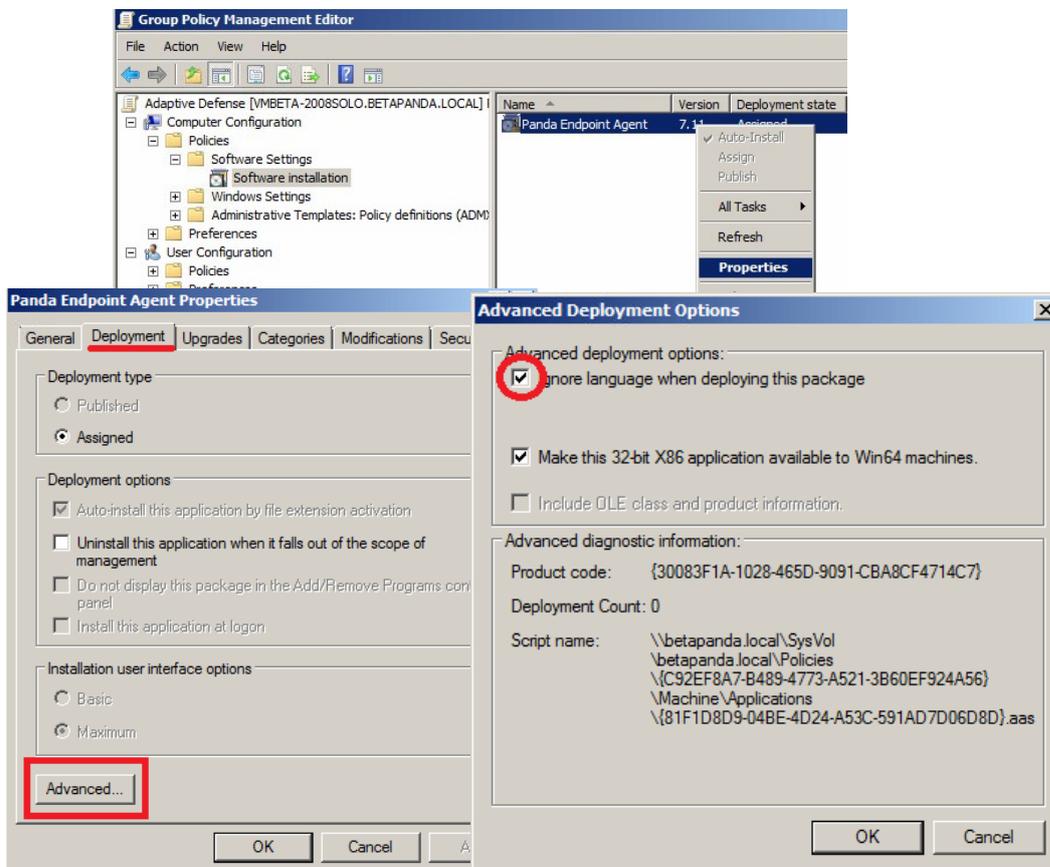


Figura 123: Selecting the option to ignore the language defined in the installer

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

### 23.3. Installation using the distribution tool

#### 23.3.1 Minimum requirements

Installing the agent with the distribution tool requires a Windows computer that meets the following minimum requirements:

- Operating system: Windows, 10, Windows 8.1, Windows 8, Windows 7 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows XP Professional (32-bit and 64-bit), Windows 2000 Professional, Windows Server 2000, Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2, Windows Home Server, Windows Server 2012 and Windows Server 2012 R2.
- Memory: 64 MB
- Hard disk: 20 MB
- Processor: Pentium II 300 MHz or equivalent
- Windows Installer 2.0 (Windows Installer 3.0 is recommended for remote uninstallation)
- Browser: Internet Explorer 6.0 or later
- Other:
  - Access to the Admin\$ resource on the computers to which the protection will be distributed.
  - A user with administrator rights on the computers to which the protection will be distributed.

For the tool to work properly in Internet Explorer, you will need to disable the use of SSL in the Advanced Security Settings and enable the use of TSL:

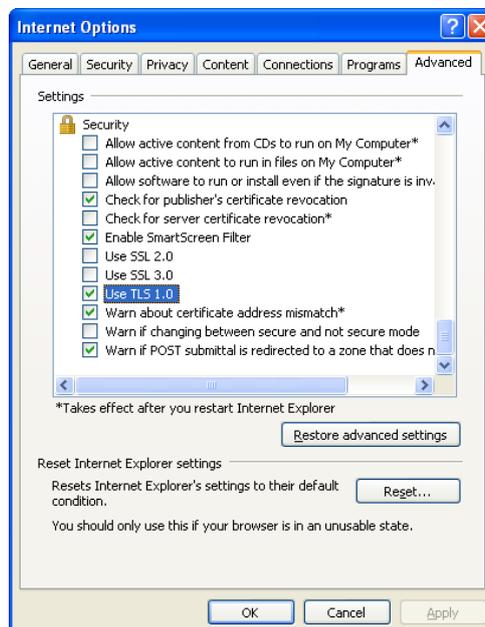


Figure 124: Enabling TLS in Internet Explorer

### 23.3.2 How to deploy the agent

Follow the steps below to install the protection using Panda Security's distribution tool.

To download the distribution tool, go to the **Installation** window and click the **Download distribution tool** link.

- Run the `DistributionTool.msi` file on the computer from which you will distribute the **Adaptive Defense 360** agent to all computers on the network.
- Once installed, run the tool from the Windows Start menu. The Protection installation screen will open, which will allow you to distribute the protection in two ways:

#### Distribution by domain

- Enter the group the computers whose protection you are going to install will be added to. This will determine the protection profile to be applied to those computers.
- In the network tree, select the domains or computers on which you want to install the protection.
- Use a user name and password with administrator permissions to carry out the installation. The user name must be entered in the domain\user name format.
- Once you have entered the credentials, click **Install** to generate the installation tasks.

#### Distribution by IP address or computer name

- Enter the group the computers whose protection you are going to install will be added to. This will determine the protection profile to be applied to those computers.
- Add the names or IP addresses of the computers whose protection you are going to install, separated by commas. You can also select IP address ranges (use the "-" symbol for ranges, e.g. `172.18.15.10 - 172.18.15.50`).
- Use a user name and password with administrator permissions to carry out the installation. The user name must be entered in the domain\user name format.
- Click **Install** to generate the installation tasks.
  - Check the console to see whether the installation task has been created successfully.
  - After that, the protection installation will begin, completely transparently to end users.
  - Restart the computer if prompted.

### 23.3.3 How to uninstall Adaptive Defense 360 centrally

The **Adaptive Defense 360** distribution tool lets you uninstall the protection centrally, avoiding manual intervention from end users throughout the process. To do this, follow the steps below:

- In the tool's console, select **Uninstall protection**. You will be taken to the **Protection uninstallation** window, which allows you to uninstall the protection in two ways:

#### Uninstall by domain

- In the network tree, select the computers or domains from which you want to uninstall the protection.
- Enter the uninstall password created during the installation process. If no password was

created, leave this field blank.

- Use a user name and password with administrator permissions to perform the uninstall. The user name must be entered in the domain\user name format.
- If you want items removed from quarantine during the uninstall process, and computers to be automatically restarted after uninstall, select the relevant checkboxes.
- Once the data is entered, click **Uninstall** to generate the uninstall tasks.

### Uninstall by IP address or computer name

- Enter the names or IP addresses of the computers whose protection you want to uninstall, separated by commas. You can also select IP address ranges (use the "-" symbol for ranges, e.g. 172.18.15.10 - 172.18.15.50).
- Enter the uninstall password created during the installation process. If no password was created, leave this field blank.
- Use a user name and password with administrator permissions to perform the uninstall. The user name must be entered in the domain\user name format.
- If you want items removed from quarantine during the uninstall process, and computers to be automatically restarted after uninstall, select the relevant checkboxes.
- Click Uninstall to generate the uninstall tasks.
  - Check the console to see whether the uninstall task has been created successfully.
  - After that, the uninstall process will begin, completely transparently to end users.
  - Restart the computers when prompted.

# 24. Appendix 2: Communication with endpoints

---

Endpoint communication with the Internet

Bandwidth consumption

Security of communications and stored data

## 24.1. Introduction

This appendix describes the communication between the agents and the **Adaptive Defense 360** server.

## 24.2. Endpoint communication with the Internet

### 24.2.1 Communication periods

The **Adaptive Defense 360** agents installed on network computers communicate with the server at regular intervals. These intervals will depend on the type of communication being transmitted. The figures below indicate the **maximum** time that can elapse before an event that must be transmitted to the server is actually sent.

- **Check for settings changes in the console:** Every 15 minutes.
- **Changes to the computer settings (name, IP address, MAC address, OS version, Service pack, etc.):** Every 12 hours.
- **Computer settings (no changes):** Every 24 hours
- **Check for new signature file:** 4 hours by default.
- **Check for updates to the protection engine:** 12 hours by default.

### 24.2.2 Internet access

The following table shows a summary of how endpoints protected with **Adaptive Defense 360** access the Internet for tasks that require communication over the Internet.

Step	Connected to the Internet	Not connected to the Internet (but at least one networked endpoint has an Internet connection)
Communication with the server	From the endpoint or another endpoint configured for such purpose.	From the endpoint with the Internet connection or the endpoint configured to channel all communications with the server.
Signature file updates	It shares signature files downloaded by other networked endpoints thanks to Adaptive Defense 360's P2P technologies. It only downloads signature files provided no other endpoint has done it previously. It is possible to specify an endpoint to download signature files from the server. This endpoint will also act as a signature repository, so that signature files will not be downloaded again when requested by another computer.	Updates take place from the endpoint with the Internet connection, or the endpoint configured to channel all communications with the server.
Product installation and upgrades	It shares upgrade packages downloaded by other networked endpoints thanks to Adaptive Defense 360's P2P technologies. It	Upgrades take place from the endpoint with the Internet connection, or the endpoint configured to channel all

	only downloads upgrade packages provided no other endpoint has done it previously. It is possible to specify an endpoint to download upgrade packages from the server.	communications with the server.
<b>Access to Collective Intelligence (CI)</b>	Connections to Collective Intelligence are established from each endpoint. *	It is not possible to access Collective Intelligence from endpoints without an Internet connection*.

Table 14: Endpoint tasks and Internet connection

\* If endpoints access the Internet using a corporate proxy server, **Adaptive Defense 360** will use it as well. The proxy server to use can be configured in the **Adaptive Defense 360** settings.

### 24.3. Bandwidth consumption summary table

The following table shows a summary of the bandwidth used by **Adaptive Defense 360** for each type of communication.

Communication	Approximate bandwidth usage
<b>Product installation</b>	8.18 MB: Installer and communications agent 60.5 * MB: Endpoint protection package
<b>Communication with the server</b>	240 KB every 12 hours (190 KB in messages sent every 15 minutes to check for configuration changes, and 50 KB in status, settings and reports messages)
<b>Signature file updates**</b>	25 MB the first time only, after installing the protection. 200-300 KB every 24 hours for signature file patches.
<b>Sending of the actions triggered by each running process</b>	1 MB per day and per endpoint
<b>Product upgrades**</b>	8.18 MB: Communications agent 60.5 MB: Endpoint protection package A product upgrade takes place every 6 months approximately.
<b>Queries to Collective Intelligence</b>	Real-time, on-access protection 500 KB: Bandwidth used on the first day, when the cache is empty. 35-100 KB: Bandwidth used after the first day, once the information is cached. Full scan of the computer 200-500 KB: First full scan of the computer. 50-200 KB: Subsequent full scans of the computer.

Table 15: Bandwidth consumption per computer based on the operation type

\* 46.2 MB for the 64-bit installer

\*\* Signature file and product updates are downloaded by a single endpoint on the network, and shared by the other networked endpoints thanks to **Adaptive Defense 360's** P2P technologies.

The signature file patches will be different depending on how outdated the signature files are. For example, if an endpoint has a two-day old signature file and another one has a one-day old

signature file, the patches to download will be different.

If you select a computer to act as a proxy/repository server, all communications except queries to Collective Intelligence will take place through that computer. Additionally, signature files will be stored in the computer selected as the repository (it will not be necessary to download them again if requested by another computer on the network).

### Estimated bandwidth consumption

Suppose you have a local network consisting of N interconnected computers, and you install **Adaptive Defense 360** on them.

The bandwidth usage will be approximately as follows.

Communication type	Internet bandwidth consumption by N PCs	Local network bandwidth consumption by N PCs
<b>Product installation (1 time only)</b>	8.18 MB for the communications agent & the installer x N computers + 60.5 MB for the endpoint protection package	8.18 MB del instalador y agente de comunicaciones x N computers  60.5 MB for the endpoint protection package
<b>Communication with the server</b>	240 KB every 12 hours x N computers	240 KB every 12 hours x N computers
<b>Sending of the actions triggered by each running process</b>	1 MB per day x N computers	1 MB per day x N computers
<b>Signature file updates</b>	25 MB the first time only, after installing the protection x N computers +  160 KB every 24 hours for signature file patches x N computers	25 MB the first time only, after installing the protection +  160 KB every 24 hours for signature file patches
<b>Product upgrades (approx. every 6 months)</b>	8.18 MB for the communications agent & the installer x N computers + 60.5 * MB for the endpoint protection package	8.18 MB for the communications agent & the installer x N computers + 60.5 * MB for the endpoint protection package
<b>Queries to Collective Intelligence</b>	500 KB the first time x N computers + 35-100 KB every day x N computers	500 KB the first time x N computers + 35-100 KB every day x N computers

Table 16: Bandwidth consumed by N computers (depending on the operation type)

\* 46.2 MB for the 64-bit installer

The new **Adaptive Defense 360** protection model requires information about the actions taken by applications installed on customers' computers.

The collection of data by **Adaptive Defense 360** is strictly in accordance with the guidelines set out below:

- The only information collected is that regarding Windows executable files, (.exe, .dll, etc.) that are run or loaded on the user's computer. No information is gathered about data files.
- The file attributes are normalized, deleting any information referring to the logged in user. So, for example, the file paths are normalized as LOCALAPPDATA\name.exe instead of c:\Users\USER\_NAME\AppData\Local\name.exe)
- The only URLs collected are those from which executable files are downloaded. The URLs visited by users are not collected.
- There is no relation between the data and the user in the data collected.
- Under no circumstances will **Adaptive Defense 360** send personal information to the cloud.

As essential information to support the new protection model, **Adaptive Defense 360** sends information about the actions **taken on each computer**.

Attribute	Data	Description	Example
File	Hash	Hash of the file to which the event refers.	N/A
URL	URL	Address from where an executable file was downloaded.	http://www.malware.com/executable.exe
Path	Path	Normalized path of the file to which the event refers	APPDATA\
Registry	Key / Value	Windows registry key and its corresponding content.	HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\Panda Research\Minerva\Version = 3.2.21
Operation	Operation ID	Identifier of the operation (creation/modification/loading/etc. of an executable, downloading of an executable, communication, etc.)	'0' type events indicate the execution of an executable
Communication	Protocol /Port/ Address	The communication event of a process (not its content) along with the protocol and address	Malware.exe sends data by UDP on port 4865
Software	Software installed	The list of software installed on the endpoint according to the Windows API.	Office 2007, Firefox 25, IBM Client Access 1.0

Table 17: Information sent to the cloud

# 25. Appendix 3: List of Uninstallers

---

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

The behavior will be different depending on the **Adaptive Defense 360** version to install.

### Trial versions

By default, trial versions of **Adaptive Defense 360** can be installed on computers with a solution other than Panda Security installed.

### Commercial versions

By default, it is not possible to install **Adaptive Defense 360** on a computer with a solution other than Panda Security installed. If **Adaptive Defense 360** includes the uninstaller to uninstall the other vendor's product, it will uninstall it and then install Adaptive Defense 360. Otherwise, the installation process will stop.

This behavior can be changed both for trial and commercial versions. Go to **Settings / (Click the profile to edit) / Windows and Linux / Advanced settings**. In addition, both the **Computers** and **Installation** windows will show at all times the installation option you have configured.

The following products will be automatically uninstalled before installing **Adaptive Defense 360**:

Vendor	Product name
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32-bit Edition) AVG Internet Security 2013 (64-bit Edition) AVG AntiVirus Business Edition 2013 (32-bit Edition) AVG AntiVirus Business Edition 2013 (64-bit Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32-bit* AVG Internet Security Business Edition 2011 64-bit (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVG Free v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir Personal Edition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira Antivir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir Personal Edition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x
CA	CA Total Defense for Business Client V14 (32-bit Edition) CA Total Defense for Business Client V14 (64-bit Edition) CA Total Defense R12 Client (32-bit Edition) CA Total Defense R12 Client (64-bit Edition)
Bitdefender	BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32-bit) Check Point Endpoint Security 8.x (64-bit)
ESET	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32-bit) ESET NOD32 Antivirus 4.X (32-bit) ESET NOD32 Antivirus 4.X (64-bit) ESET NOD32 Antivirus 5 (32-bit) ESET NOD32 Antivirus 5 (64-bit) ESET NOD32 Antivirus 6 (32-bit) ESET NOD32 Antivirus 6 (64-bit) ESET NOD32 Antivirus 7 (32-bit) ESET NOD32 Antivirus 7 (64-bit)
Frisk	F-Prot Antivirus 6.0.9.1

F- Secure	<p>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</p>
Kaspersky	<p>Kaspersky Endpoint Security 10 for Windows (32-bit Edition)          Kaspersky Endpoint Security 10 for Windows (64-bit Edition)          Kaspersky Endpoint Security 8 for Windows (32-bit Edition)          Kaspersky Endpoint Security 8 for Windows (64-bit Edition)          Kaspersky Anti-Virus 2010 9.0.0.459*          Kaspersky® Business Space Security          Kaspersky® Work Space Security          Kaspersky Internet Security 8.0, 7.0, 6.0 (with Windows Vista + UAC, you must disable UAC)          Kaspersky Anti-Virus 8*          Kaspersky® Anti-virus 7.0 (with Windows Vista + UAC, you must disable UAC)          Kaspersky Anti-Virus 6.0 for Windows Workstations*</p>
McAfee	<p>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</p>
Norman	<p>Norman Security Suite 10.x (32-bit Edition)          Norman Security Suite 10.x (64-bit Edition)          Norman Security Suite 9.x (32-bit Edition)          Norman Security Suite 9.x (64-bit Edition)          Norman Endpoint Protection 8.x/9.x          Norman Virus Control v5.99</p>
Norton	<p>Norton Antivirus Internet Security 2008*          Norton Antivirus Internet Security 2007          Norton Antivirus Internet Security 2006</p>
Microsoft	<p>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*</p>
MicroWorld Technologies	<p>eScan Corporate for Windows 9.0.824.205</p>
PC Tools	<p>Spyware Doctor with AntiVirus 9.x</p>
Sophos	<p>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</p>

Symantec	<p>Symantec.cloud - Endpoint Protection.cloud 21.x (32-bit)          Symantec.cloud - Endpoint Protection.cloud 21.x (64-bit)          Symantec EndPoint Protection 12.x (32-bit)          Symantec EndPoint Protection 12.x (64-bit)          Symantec EndPoint Protection 11.x (32-bit)          Symantec EndPoint Protection 11.x (64-bit)          Symantec Antivirus 10.1          Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x</p>
Trend Micro	<p>Trend Micro Worry-Free Business Security 8.x (32-bit Edition)          Trend Micro Worry-Free Business Security 8.x (64-bit Edition)          Trend Micro Worry-Free Business Security 7.x (32-bit Edition)          Trend Micro Worry-Free Business Security 7.x (64-bit Edition)          Trend Micro Worry-Free Business Security 6.x (32-bit Edition)          Trend Micro Worry-Free Business Security 6.x (64-bit Edition)          Trend Micro Worry-Free Business Security 5.x          PC-Cillin Internet Security 2006          PC-Cillin Internet Security 2007*          PC-Cillin Internet Security 2008*          Trend Micro OfficeScan Antivirus 8.0          Trend Micro OfficeScan 7.x          Trend Micro OfficeScan 8.x          Trend Micro OfficeScan 10.x</p>
Comodo AntiVirus	Comodo Antivirus V 4.1 32-bit

Panda Security	Panda Cloud Antivirus 3.x
	Panda Cloud Antivirus 2.X
	Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX
	Panda for Desktops 4.07.XX
	Panda for Desktops 4.05.XX
	Panda for Desktops 4.04.10
	Panda for Desktops 4.03.XX and later
	Panda for File Servers 8.50.XX
	Panda for File Servers 8.05.XX
	Panda for File Servers 8.04.10
	Panda for File Servers 8.03.XX and later
	Panda Global Protection 2015*
	Panda Internet Security 2015*
	Panda Antivirus Pro 2015*
	Panda Gold Protection*
	Panda Free Antivirus
	Panda Global Protection 2014*
	Panda Internet Security 2014*
	Panda Antivirus Pro 2014*
	Panda Gold Protection*
	Panda Global Protection 2013*
	Panda Internet Security 2013*
	Panda Antivirus Pro 2013*
	Panda Global Protection 2012*
	Panda Internet Security 2012*
	Panda Antivirus Pro 2012*
	Panda Global Protection 2011*
	Panda Internet Security 2011*
	Panda Antivirus Pro 2011*
	Panda Antivirus for Netbooks (2011)*
	Panda Global Protection 2010
Panda Internet Security 2010	
Panda Antivirus Pro 2010	
Panda Antivirus for Netbooks	
Panda Global Protection 2009	
Panda Internet Security 2009	
Panda Antivirus Pro 2009	
Panda Internet Security 2008	
Panda Antivirus + Firewall 2008	
Panda Antivirus 2008	
Panda Internet Security 2007	
Panda Antivirus + Firewall 2007	
Panda Antivirus 2007	

\* \* Panda 2017, 2016, 2015, 2014, 2013, 2012 products need a reboot to get uninstalled.

\* Comodo Antivirus V4.1 (32-bit): While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\*F-Secure PSB for Workstations 9.00\*: During the installation process of the **Adaptive Defense 360** agent in Windows 7 and Windows Vista, the user will be prompted to select the Allow option.

\*AVG Internet Security Business Edition 2011 32-bit \*: During the **Adaptive Defense 360** agent installation process, the user will be prompted to select the Allow option in several windows.

\*AVG Internet Security Business Edition 2011 64-bit (10.0.1375)\* - During the **Adaptive Defense 360** agent installation process, the user will be prompted to select the Allow option in several windows.

\* Kaspersky Anti-Virus 6.0 for Windows Workstations:

During the **Adaptive Defense 360** agent installation process in 64-bit platforms, the user will be prompted to select the Allow option in several windows.

In order to uninstall the protection, the Kaspersky protection should not be password protected.

While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\* F-Secure PSB for Workstations 9.00: During the **Adaptive Defense 360** agent installation process, the user will be prompted to select the Allow option in two windows.

\* AVG Anti-Virus Network Edition 8.5: During the **Adaptive Defense 360** agent installation process, the user will be prompted to select the Allow option in two windows.

\* Panda Antivirus 2011 products do not uninstall correctly on Windows Vista 64-bit. While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\* Panda Cloud Antivirus 1.4 Pro and Panda Cloud Antivirus 1.4 Free: While the program is being uninstalled, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically with Windows Vista x64.

\* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically with Windows Vista x86 with UAC enabled\*

\*ESET NOD32 Antivirus 3.0.XX (2008) does not uninstall automatically on 64-bit platforms.

\*ESET Smart Security 3.0 does not uninstall automatically on 64-bit platforms.

\* ESET NOD32 Antivirus 2.7: After installation of the **Adaptive Defense 360** agent on the computer, it will restart automatically without displaying any notification or asking for user confirmation.

\*ESET NOD32 Antivirus 2.70.39\*: After installation of the **Adaptive Defense 360** agent on the computer, it will restart automatically without displaying any notification or asking for user confirmation.

\* Sophos Anti-virus SBE 2.5 does not uninstall correctly on Windows 2008.

\* eTrust Antivirus 7.1 does not uninstall correctly on 64-bit platforms (Windows 2003 64-bit and Windows XP 64-bit).

\* Norton Antivirus Internet Security 2008 does not uninstall correctly if the Windows Vista UAC is enabled.

\* BitDefender Free Edition 2009 12.0.12.0. On Windows Vista and UAC enabled, while the program is being uninstalled, the user will be prompted to select the option Allow in the UAC window.

\* Kaspersky Anti-Virus 2010 9.0.0.459. On systems with UAC enabled, while the program is being uninstalled, the user will be prompted to select the option Allow in the UAC window.

\* Kaspersky Anti-Virus 8. On Windows Vista and UAC enabled, while the program is being uninstalled, the user will be prompted to select the option Allow in the UAC window.

\* McAfee Total Protection Services 4.7. The uninstaller does not run correctly if UAC is enabled. Furthermore, on 32-bit platforms user intervention is necessary.

\* Microsoft Live OneCare 2.5 does not uninstall on Windows Small Business Server 2008.

If you have a program not included on this list, contact the corresponding vendor to find out how to uninstall it before installing Adaptive Defense 360.

# 26. Appendix 4: Key concepts

---

**Accumulated knowledge server**

A service that stores and relates the knowledge collected by **Adaptive Defense 360** from the customer's network in real time. It enables searches to be run and advanced graphs to be generated to interpret the information.

**Active Directory**

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed service for finding a range of information on network environments.

**Adaptive protection cycle**

A new security focus based on the integration of a group of services providing protection, detection, monitoring, forensic analysis and problem resolution. All these are centralized in a single management console accessible from anywhere at any time.

**Adware**

Program that automatically runs, displays or downloads advertising to the computer.

**Agent**

The agent is responsible for communication between the managed computers and the **Adaptive Defense 360** servers, as well as managing local processes.

**Alert**

A message concerning the protection activity of **Adaptive Defense 360** when it may require action on the part of the user or administrator. Administrators receive alerts via email, and users receive alerts generated by the agent which appear on the device desktop.

**Antivirus**

Program designed to detect and eliminate viruses and other threats.

**APT (Advanced Persistent Threat)**

A set of processes controlled by hackers and aimed at infecting customers' networks through diverse infection vectors simultaneously and designed to go undetected by traditional antivirus programs for long periods of time. The main aim of these threats is financial (theft of confidential information, intellectual property, etc.).

**ARP (Address Resolution Protocol)**

Protocol used for the resolution of network layer addresses into link layer addresses. On IP networks it translates IP addresses to physical MAC addresses.

**ASLR (Address Space Layout Randomization)**

Address Space Layout Randomization (ASLR) is a security technique used in operating systems to prevent buffer overflow-driven exploits. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. This prevents attackers from illegitimately using calls to certain system functions as they will not know where in memory those functions reside.

### **Audit**

An **Adaptive Defense 360** mode that lets you see the processes run on the protected network computers without taking any remedial action (disinfection or blocking).

### **Block**

This prevents the running of programs cataloged as malware or unclassified, according to the configuration of **Adaptive Defense 360** set by the administrator.

### **Broadcast**

Broadcasting of packets across data networks. One data packet can reach all computers on the same subnet. Broadcast packets don't go through routers and use different addressing methodology to differentiate them from unicast packets.

### **Buffer overflow**

Anomaly affecting the management of a process' input buffers. In a buffer overflow, if the size of the data received is greater than the allocated buffer, the redundant data is not discarded, but is written to adjacent memory locations. This may allow attackers to insert arbitrary executable code into the memory of a program on systems prior to Microsoft's implementation of the DEP (Data Execution Prevention) technology.

### **Cloud**

Cloud computing is a technology that allows services to be offered across the Internet. In IT circles, the word 'cloud' (or 'the cloud') is used as a metaphor for 'the Internet'.

### **Compromised process**

A vulnerable process hit by an exploit attack in order to compromise the security of a user's computer.

### **Computers without a license**

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers will be automatically removed from the list of computers without a license as soon as new licenses are purchased.

### **CVE (Common Vulnerabilities and Exposures)**

List of publicly known cyber-security vulnerabilities defined and maintained by The MITRE

Corporation. Each entry on the list has a unique identifier, allowing CVE to offer a common naming scheme that security tools and human operators can use to exchange information about vulnerabilities with each other.

### **DEP (Data Execution Prevention)**

A feature implemented in operating systems to prevent the execution of code in memory pages marked as non-executable. This feature was developed to prevent buffer-overflow exploits.

### **DHCP**

Service that assigns IP addresses to new computers on the network.

### **Dialer**

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

### **Disinfectable**

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

### **Distribution tool**

Once downloaded from the Internet and installed on the administrator's PC, the distribution tool lets the administrator remotely install and uninstall the protection on selected network computers. In Adaptive Defense 360, the distribution tool can only be used to deploy the protection to Windows computers.

### **DNS (Domain Name System)**

Service that translates domain names to different types of information, generally IP addresses.

### **Domain**

Windows network architecture where the management of shared resources, permissions and users is centralized in a server called a Primary Domain Controller or Active Directory.

### **Environment variable**

This is a string of environment information such as a drive, path or file name that is associated with a symbolic name that Windows can use. You can use the System applet in the Control Panel or the 'set' command at the command prompt to set environment variables.

### **Exchange server**

Mail server developed by Microsoft. Exchange Servers store inbound and/or outbound emails and distribute them to users' email inboxes. To connect to the server and download their email, users must have an email client installed on their computers.

## Excluded computers

Computers selected by the user which are not protected by the solution. Excluded computers are only displayed in the Excluded section, they are not shown anywhere else in the console. No warnings about them are displayed either. Bear in mind that you can undo these exclusions at any time.

## 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, triggering actions that may compromise the security of the target computer.

## Firewall

This is a barrier that can protect information on a system or network when there is a connection to another network, for example, the Internet.

## Forensic analysis

A series of actions and processes carried out by network administrators with special tools in order to track a malicious program and evaluate the consequences when malware has managed to infect a network computer.

## Fragmentation

On data transmission networks, when the MTU of the underlying protocol is less than the size of the transmitted packet, routers divide the packet into smaller segments (fragments) which are routed independently and assembled at the destination.

## Geolocation

Geographical positioning of a device on a map from its coordinates.

## Goodware

A file which after analysis has been classified as legitimate and safe.

## Group

In Adaptive Defense 360, a group is a set of computers to which the same protection configuration profile is applied. **Adaptive Defense 360** includes an initial group *-Default group-* to which the administrator can add all the computers to protect. New groups can also be created.

## Hacking tool

Programs that can be used by a hacker to carry out actions that cause problems for the user of the affected computer (allowing the hacker to control the computer, steal confidential information, scan communication ports, etc.).

## Hardening

An **Adaptive Defense 360** mode that blocks unknown programs downloaded from the Internet as well as all files classified as malware.

## Heap Spraying

Heap Spraying is a technique used to facilitate the exploitation of software vulnerabilities by malicious processes.

As operating systems improve, the success of vulnerability exploit attacks has become increasingly random. In this context, heap sprays take advantage of the fact that on most architectures and operating systems, the start location of large heap allocations is predictable and consecutive allocations are roughly sequential. This allows attackers to insert and later run arbitrary code in the target system's heap memory space.

This technique is widely used to exploit vulnerabilities in Web browsers and Web browser plug-ins.

## Heuristic analysis

Heuristic analysis analyzes hundreds of characteristics of a software file.

This determines the potential of the software to carry out malicious or damaging actions when run on a computer, and whether it is a virus, spyware, a Trojan, a worm, etc.

## Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

## ICMP (Internet Control Message Protocol)

Error notification and monitoring protocol used by the IP protocol on the Internet.

## IDP (Identity Provider)

Centralized service for managing user identity verification.

## IP (Internet Protocol)

Principal Internet protocol for sending and receiving datagrams generated on the underlying link level.

## IP address

Number that identifies a device interface (usually a computer) on a network that uses the IP protocol.

## 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.

### **Local process**

Local processes are responsible for performing the tasks necessary to implement and manage the protection on computers.

### **Lock**

An **Adaptive Defense 360** mode that blocks unknown programs and those classified as malware.

### **MAC address**

Hexadecimal, 48-bit unique identifier of a network card or interface. It is individual: each device has its own MAC address.

### **Machine learning**

This is a branch of artificial intelligence whose aim is to develop technologies that can create programs from unstructured information delivered in the form of examples.

### **Malware**

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 function of the quarantine whose goal is to prevent the loss of data due to false positives. All files classified as malware or suspicious are sent to quarantine, thereby avoiding deleting and losing data if the classification is wrong.

### **Malware life cycle**

Breakdown of all the actions unleashed by a malicious program from the time it is first seen on a customer's computer until it is classified as malware and disinfected.

### **Master Browser**

The role of a computer on a Windows network that keeps a list of all devices that connect to that network segment.

### **MD5 (Message-Digest Algorithm 5)**

This is a cryptographic hash function producing a 128-bit value that represents data input. The MD5 hash calculated on a file can unequivocally identify it or check that it has not been tampered with.

### **MTU (Maximum transmission unit)**

Maximum packet size that a given protocol can transmit.

**Network adapter**

The network adapter allows communication between devices connected to each other, and also allows resources to be shared between two or more computers. It has a unique identifier.

**Network topology**

Physical or logical map of network nodes.

**Notices**

Also called Incidents, these show on the Web console the activity of malicious programs detected by the **Adaptive Defense 360** advanced protection.

**Notifications**

Alerts for administrators about important issues concerning the **Adaptive Defense 360** platform such as new versions of the endpoint protection, licenses about to expire, etc.

**OU (Organizational Unit)**

Hierarchical method for classifying and grouping objects stored in directories.

**Partner**

A company that offers Panda Security products and services.

**Payload**

In the IT and telecommunications sectors, a message payload is the set of useful transmitted data (as opposed to other data that is also sent to facilitate message delivery: header, metadata, control information, etc.).

In IT security circles, however, an exploit's payload is the part of the malware code that controls the malicious actions taken on the system, such as deleting files, stealing data, etc. (as opposed to the part responsible for leveraging the software vulnerability (the exploit) in order to run the payload).

**PDC (Primary Domain Controller)**

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

**Peer To Peer (P2P) functionality**

A Peer-to-Peer network is a network without fixed client or servers, but a series of nodes that work simultaneously as clients and servers for the other nodes on the network. This is a legal way of sharing files, similar to sending them via email or instant messaging, but more efficient.

In the case of Adaptive Defense 360, the P2P feature reduces Internet bandwidth consumption, as computers that have already updated a file from the Internet then share the update with other

connected computers. This prevents saturating Internet connections.

### **Phishing**

A technique for obtaining confidential information fraudulently. The information targeted includes passwords, credit card numbers and bank account details.

### **Port**

A numeric ID assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

### **Potentially Unwanted Programs (PUP)**

A program that may be unwanted, despite the possibility that users consented to download it.

They are usually installed legitimately as part of another program.

### **Profile**

A profile is a specific protection configuration. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

### **Protocol**

System of regulations and specifications used for exchanging data. One of the most commonly used is TCP-IP.

### **Proxy**

A proxy server acts as an intermediary between an internal network (an intranet, for example) and an external connection to the Internet. This allows a connection for receiving files from Web servers to be shared.

### **Proxy functionality**

This feature allows **Adaptive Defense 360** to operate in computers without Internet access, accessing the Web through an agent installed on a computer on the same subnet.

### **Public network**

This is the type of network you find in Internet cafes, airports, etc. Visibility of computers is restricted on such networks, and there are restrictions on sharing files, resources and directories.

### **QR (Quick Response) code**

A matrix of dots that efficiently stores data.

### **Quarantine**

Repository of files that are suspected of being malicious or that cannot be disinfected, as well as the spyware and hacking tools detected.

**Remote access**

Technology that enables someone to connect and interact remotely with a user's computer.

**Responsive / Adaptable Web design (RWD: Responsive Web Design)**

A set of techniques that enable the development of Web pages that automatically adapt to the size and resolution of the device being used to view them.

**RIR (Regional Internet Registry)**

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

**Rootkits**

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is not malicious in itself, but is used by hackers to cover their tracks in previously compromised systems. There are types of malware that use rootkits to hide their presence on the system.

**SCL (Spam Confidence Level)**

The spam confidence level (SCL) is the normalized value assigned to a message that indicates the likelihood that the message is spam, based on the characteristics of a message (such as the content, message header, etc.).

**SIEM (Security Information and Event Management)**

Software that provides storage and real-time analysis of the alerts generated by network devices and the applications on the network.

**Signature file**

The file that allows the antivirus to detect threats.

**SMTP server**

Server that uses SMTP -simple mail transfer protocol- to exchange email messages between computers.

**Spam**

This refers to unsolicited email messages that normally contain advertising and are generally sent out massively and can have a range of negative effects on the recipient.

**Spyware**

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and which collects personal data.

**SSL (Secure Sockets Layer)**

Cryptographic protocol for the secure transmission of data on a network.

**Suspicious file**

A file with a high probability of being malware after having been analyzed by the **Adaptive Defense 360** protection on the user's computer.

**SYN**

Flag in the TOS field of TCP packets that identifies them as the start of the connection.

**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 programs that install themselves on computers and carry out actions that compromise user confidentiality.

**Trusted network**

In this case, we are generally talking about office or home networks. Your computer will be perfectly visible to the other computers on the network. There are no limitations on sharing files, resources or directories.

**UDP (User Datagram Protocol)**

A transport-layer protocol which is not trustworthy and not aimed at connections for exchanging IP packets.

**URL filter by category**

Control over the URLs requested by Internet users, denying or granting permission to access pages based on a URL database divided into subjects or categories.

**Virus**

Viruses are programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly destructive and irreparable.

**VPN (Virtual Private Network)**

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

### **Vulnerable process**

A program which, due to a programming bug, cannot interpret certain input data correctly. Hackers take advantage of specially crafted data packets (exploit) to cause vulnerable processes to malfunction, and run malicious code designed to compromise the security of the target computer.

### **Web console**

Tool for configuring the protection, as well as distributing and managing the agent across all the computers on your network. You can also see the security status of your network and generate and print the reports you want.

### **Window of opportunity**

Time it takes between the first computer (in the world) being infected with new malware and its analysis and inclusion by antivirus companies in signature files to protect computers from infection. This is the period when malware can infect computers without the antivirus being aware of its existence.

### **Workgroup**

Architecture in Windows networks where shared resources, permissions and users can be independently managed from each computer.

 Adaptive Defense 360

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, C/ 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.