



Adaptive Defense

# Guide for Network Administrators

**Version:** 3.20.00-00

**Author:** Panda Security

**Date:** 11/27/2017

## Table of contents

<b>1. PREFACE .....</b>	<b>9</b>
<b>1.1. INTRODUCTION .....</b>	<b>10</b>
<b>1.2. WHO IS THIS GUIDE AIMED AT? .....</b>	<b>10</b>
<b>1.3. WHAT IS ADAPTIVE DEFENSE ON AETHER? .....</b>	<b>10</b>
<b>1.4. ICONS .....</b>	<b>11</b>
<b>2. INTRODUCTION .....</b>	<b>12</b>
<b>2.1. INTRODUCTION .....</b>	<b>13</b>
<b>2.2. ADAPTIVE DEFENSE ON AETHER: KEY FEATURES .....</b>	<b>13</b>
<b>2.3. AETHER PLATFORM: KEY FEATURES .....</b>	<b>14</b>
2.3.1 KEY BENEFITS OF AETHER .....	14
2.3.2 AETHER ARCHITECTURE .....	16
2.3.3 AETHER ON USERS' COMPUTERS .....	16
<b>2.4. ADAPTIVE DEFENSE ARCHITECTURE: KEY COMPONENTS .....</b>	<b>18</b>
2.4.1 ADAPTIVE DEFENSE CLOUD SERVER FARM .....	19
2.4.2 MANAGEMENT CONSOLE WEB SERVER.....	20
2.4.3 COMPUTERS PROTECTED WITH ADAPTIVE DEFENSE .....	20
<b>2.5. ADAPTIVE DEFENSE SERVICES .....</b>	<b>21</b>
2.5.1 ADVANCED REPORTING TOOL SERVICE .....	21
2.5.2 SIEMFEEDER SERVICE: INTEGRATION WITH THE CUSTOMER'S SIEM SERVICE.....	21
2.5.3 SAMPLES FEED .....	22
2.5.4 IP FEEDS.....	22
<b>2.6. ADAPTIVE DEFENSE ON AETHER: USER PROFILE.....</b>	<b>22</b>
<b>2.7. ADAPTIVE DEFENSE ON AETHER: SUPPORTED DEVICES AND LANGUAGES .....</b>	<b>22</b>
<b>2.8. AVAILABLE RESOURCES AND DOCUMENTATION.....</b>	<b>23</b>
<b>3. THE ADAPTIVE PROTECTION FULL CYCLE .....</b>	<b>25</b>
<b>3.1. INTRODUCTION .....</b>	<b>26</b>
<b>3.2. THE ADAPTIVE PROTECTION CYCLE .....</b>	<b>26</b>
<b>3.3. PHASE 1: COMPLETE PROTECTION OF THE IT NETWORK .....</b>	<b>27</b>
3.3.1 ANTI-EXPLOIT PROTECTION .....	27
3.3.2 PROTECTION AGAINST ADVANCED STEALTH TECHNIQUES AND MACRO VIRUSES.....	28
<b>3.4. PHASE 2: DETECTION AND MONITORING.....</b>	<b>28</b>
3.4.1 ADVANCED PERMANENT PROTECTION .....	28
3.4.2 MONITORING DATA FILES .....	30
3.4.3 NETWORK STATUS VISIBILITY.....	30
<b>3.5. PHASE 3: REMEDIATION AND RESPONSE .....</b>	<b>31</b>
<b>3.6. PHASE 4: ADAPTATION .....</b>	<b>32</b>
<b>4. THE MANAGEMENT CONSOLE.....</b>	<b>33</b>
<b>4.1. INTRODUCTION .....</b>	<b>34</b>
4.1.1 WEB CONSOLE REQUIREMENTS.....	34

4.1.2	IDP FEDERATION .....	35
<b>4.2.</b>	<b>GENERAL CHARACTERISTICS OF THE CONSOLE.....</b>	<b>35</b>
<b>4.3.</b>	<b>GENERAL STRUCTURE OF THE WEB MANAGEMENT CONSOLE .....</b>	<b>35</b>
4.3.1	TOP MENU (1) .....	36
4.3.2	SIDE MENU (2).....	38
4.3.3	WIDGETS (3) .....	38
4.3.4	TAB MENU .....	39
4.3.5	FILTERING AND SEARCH TOOLS .....	39
4.3.6	BACK BUTTON .....	40
4.3.7	SETTINGS ELEMENTS (8).....	40
4.3.8	CONTEXT MENUS .....	40
4.3.9	LISTS .....	41
<b>5.</b>	<b><u>LICENSES.....</u></b>	<b>43</b>
<b>5.1.</b>	<b>INTRODUCTION .....</b>	<b>44</b>
<b>5.2.</b>	<b>DEFINITIONS AND KEY CONCEPTS FOR MANAGING LICENSES .....</b>	<b>44</b>
5.2.1	LICENSE CONTRACTS .....	44
5.2.2	COMPUTER STATUS .....	44
5.2.3	LICENSE STATUS AND GROUPS .....	45
5.2.4	TYPES OF LICENSES.....	45
5.2.5	LICENSE MANAGEMENT.....	45
5.2.6	LICENSE RELEASE .....	46
5.2.7	PROCESSES FOR ASSIGNING AND RELEASING LICENSES.....	46
<b>5.3.</b>	<b>CONTRACTED LICENSES.....</b>	<b>47</b>
5.3.1	WIDGET .....	47
5.3.2	LICENSE LIST .....	49
<b>5.4.</b>	<b>EXPIRED LICENSES.....</b>	<b>51</b>
5.4.1	EXPIRY NOTIFICATIONS .....	51
5.4.2	WITHDRAWAL OF EXPIRED LICENSES .....	52
<b>5.5.</b>	<b>ADDING TRIAL LICENSES TO COMMERCIAL LICENSES .....</b>	<b>52</b>
<b>5.6.</b>	<b>SEARCHING FOR COMPUTERS BASED ON THE STATUS OF THEIR LICENSES .....</b>	<b>53</b>
<b>6.</b>	<b><u>INSTALLING THE ADAPTIVE DEFENSE SOFTWARE .....</u></b>	<b>54</b>
<b>6.1.</b>	<b>INTRODUCTION .....</b>	<b>55</b>
<b>6.2.</b>	<b>PROTECTION DEPLOYMENT OVERVIEW .....</b>	<b>55</b>
<b>6.3.</b>	<b>INSTALLATION REQUIREMENTS .....</b>	<b>57</b>
6.3.1	REQUIREMENTS FOR EACH SUPPORTED PLATFORM.....	57
6.3.2	NETWORK REQUIREMENTS.....	58
<b>6.4.</b>	<b>MANUALLY DOWNLOADING AND INSTALLING THE ADAPTIVE DEFENSE SOFTWARE .....</b>	<b>58</b>
6.4.1	DOWNLOADING THE INSTALLATION PACKAGE FROM THE WEB CONSOLE .....	58
6.4.2	GENERATING A DOWNLOAD URL .....	59
6.4.3	MANUALLY INSTALLING THE ADAPTIVE DEFENSE SOFTWARE .....	59
<b>6.5.</b>	<b>AUTOMATIC COMPUTER DISCOVERY AND REMOTE INSTALLATION.....</b>	<b>60</b>
6.5.1	REQUIREMENTS FOR INSTALLING ADAPTIVE DEFENSE .....	60
6.5.2	COMPUTER DISCOVERY.....	60
6.5.3	DISCOVERY SCOPE.....	61
6.5.4	SCHEDULING COMPUTER DISCOVERY TASKS.....	61
6.5.5	LIST OF DISCOVERED COMPUTERS.....	62

6.5.6	DETAILS OF A DISCOVERED COMPUTER .....	66
6.5.7	INSTALLING THE PROTECTION ON COMPUTERS.....	67
<b>6.6.</b>	<b>INSTALLATION WITH CENTRALIZED TOOLS .....</b>	<b>68</b>
<b>6.7.</b>	<b>INSTALLATION USING IMAGE GENERATION .....</b>	<b>72</b>
<b>6.8.</b>	<b>UNINSTALLING THE SOFTWARE .....</b>	<b>72</b>
<b>7.</b>	<b><u>MANAGING COMPUTERS AND DEVICES .....</u></b>	<b><u>74</u></b>
<b>7.1.</b>	<b>INTRODUCTION .....</b>	<b>75</b>
7.1.1	REQUIREMENTS FOR MANAGING COMPUTERS FROM THE MANAGEMENT CONSOLE .....	75
<b>7.2.</b>	<b>THE COMPUTERS AREA .....</b>	<b>75</b>
7.2.1	THE COMPUTERS TREE PANEL .....	77
7.2.2	THE COMPUTERS LIST PANEL.....	78
7.2.3	COMPUTERS LIST.....	79
<b>7.3.</b>	<b>FILTERS TREE.....</b>	<b>81</b>
7.3.1	WHAT IS A FILTER? .....	81
7.3.2	GROUPS OF FILTERS .....	81
7.3.3	PREDEFINED FILTERS.....	82
7.3.4	CREATING AND ORGANIZING FILTERS .....	82
7.3.5	FILTER SETTINGS.....	84
7.3.6	FILTER RULES.....	84
7.3.7	LOGICAL OPERATORS .....	85
7.3.8	GROUPS OF FILTER RULES .....	85
<b>7.4.</b>	<b>GROUPS TREE .....</b>	<b>86</b>
7.4.1	WHAT IS A GROUP?.....	87
7.4.2	GROUP TYPES .....	87
7.4.3	GROUPS STRUCTURE.....	87
7.4.4	ACTIVE DIRECTORY GROUPS .....	87
7.4.5	CREATING AND ORGANIZING GROUPS .....	88
7.4.6	MOVING COMPUTERS FROM ONE GROUP TO ANOTHER .....	89
<b>7.5.</b>	<b>COMPUTER DETAILS .....</b>	<b>90</b>
7.5.1	GENERAL SECTION (1) .....	90
7.5.2	COMPUTER NOTIFICATIONS SECTION (2) .....	91
7.5.3	DETAILS SECTION (3) .....	92
7.5.4	HARDWARE SECTION (4) .....	93
7.5.5	SOFTWARE SECTION (5) .....	93
7.5.6	SETTINGS SECTION (6).....	94
7.5.7	FORCE SYNCHRONIZATION (7).....	94
7.5.8	CONTEXT MENU .....	94
<b>8.</b>	<b><u>MANAGING SETTINGS.....</u></b>	<b><u>95</u></b>
<b>8.1.</b>	<b>INTRODUCTION .....</b>	<b>96</b>
<b>8.2.</b>	<b>WHAT ARE SETTINGS? .....</b>	<b>96</b>
<b>8.3.</b>	<b>OVERVIEW OF ASSIGNING SETTINGS TO COMPUTERS .....</b>	<b>96</b>
8.3.1	IMMEDIATE DEPLOYMENT OF SETTINGS.....	97
8.3.2	MULTI-LEVEL TREES.....	97
8.3.3	INHERITANCE.....	97
8.3.4	MANUAL SETTINGS .....	97
8.3.5	DEFAULT SETTINGS .....	97

<b>8.4. MODULAR VS MONOLITHIC SETTINGS PROFILES.....</b>	<b>98</b>
<b>8.5. OVERVIEW OF THE FOUR TYPES OF SETTINGS.....</b>	<b>100</b>
<b>8.6. CREATING AND MANAGING SETTINGS.....</b>	<b>101</b>
<b>8.7. MANUAL AND AUTOMATIC ASSIGNING OF SETTINGS TO GROUPS OF COMPUTERS .....</b>	<b>102</b>
8.7.1 ASSIGNING SETTINGS DIRECTLY/MANUALLY.....	102
8.7.2 INDIRECT ASSIGNING OF SETTINGS: THE TWO RULES OF INHERITANCE.....	104
8.7.3 INHERITANCE LIMITS.....	105
8.7.4 OVERWRITING SETTINGS .....	106
8.7.5 DELETING MANUALLY ASSIGNED SETTINGS AND RESTORING INHERITANCE .....	110
8.7.6 MOVING GROUPS AND COMPUTERS.....	111
<b>8.8. VIEWING THE ASSIGNED SETTINGS .....</b>	<b>111</b>
<b><u>9. AGENT AND LOCAL PROTECTION SETTINGS.....</u></b>	<b><u>114</u></b>
<b>9.1. INTRODUCTION .....</b>	<b>115</b>
<b>9.2. CONFIGURING THE PANDA AGENT ROLE.....</b>	<b>115</b>
9.2.1 PROXY ROLE .....	115
9.2.2 CACHE/REPOSITORY ROLE .....	116
9.2.3 DISCOVERY COMPUTER ROLE .....	117
<b>9.3. CONFIGURING INTERNET ACCESS VIA A PROXY SERVER.....</b>	<b>117</b>
<b>9.4. CONFIGURING REAL-TIME COMMUNICATION .....</b>	<b>119</b>
<b>9.5. CONFIGURING THE AGENT LANGUAGE .....</b>	<b>119</b>
<b>9.6. CONFIGURING THE ANTI-TAMPER PROTECTION AND PASSWORD .....</b>	<b>120</b>
9.6.1 ANTI-TAMPER PROTECTION.....	120
9.6.2 PASSWORD-PROTECTION OF THE AGENT.....	120
<b><u>10. SECURITY SETTINGS FOR WORKSTATIONS AND SERVERS .....</u></b>	<b><u>121</u></b>
<b>10.1. INTRODUCTION.....</b>	<b>122</b>
<b>10.2. INTRODUCTION TO THE SECURITY SETTINGS FOR WORKSTATIONS AND SERVERS.....</b>	<b>122</b>
<b>10.3. GENERAL SETTINGS.....</b>	<b>122</b>
10.3.1 UPDATES.....	122
10.3.2 UNINSTALL OTHER SECURITY PRODUCTS .....	122
10.3.3 EXCLUSIONS .....	123
<b>10.4. ADVANCED PROTECTION .....</b>	<b>123</b>
10.4.1 BEHAVIOR.....	123
10.4.2 ANTI-EXPLOIT .....	124
10.4.3 PRIVACY.....	125
10.4.4 NETWORK USAGE.....	125
<b><u>11. SOFTWARE UPDATES .....</u></b>	<b><u>127</u></b>
<b>11.1. INTRODUCTION.....</b>	<b>128</b>
<b>11.2. CONFIGURING PROTECTION ENGINE UPDATES .....</b>	<b>128</b>
<b>11.3. CONFIGURING COMMUNICATIONS AGENT UPDATES .....</b>	<b>129</b>
<b>11.4. CONFIGURING KNOWLEDGE UPDATES.....</b>	<b>129</b>
<b><u>12. MALWARE AND NETWORK VISIBILITY .....</u></b>	<b><u>130</u></b>

<b>12.1. INTRODUCTION.....</b>	<b>131</b>
<b>12.2. OVERVIEW OF THE STATUS MENU .....</b>	<b>131</b>
<b>12.3. AVAILABLE PANELS/WIDGETS.....</b>	<b>133</b>
12.3.1 PROTECTION STATUS .....	133
12.3.2 OFFLINE COMPUTERS.....	135
12.3.3 OUTDATED PROTECTION .....	136
12.3.4 CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED.....	137
12.3.5 THREATS ALLOWED BY THE ADMINISTRATOR .....	139
12.3.6 MALWARE/PUP ACTIVITY.....	140
12.3.7 EXPLOIT ACTIVITY .....	142
12.3.8 CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED .....	142
<b>12.4. INTRODUCTION TO THE LISTS .....</b>	<b>143</b>
12.4.1 TEMPLATES, SETTINGS AND VIEWS .....	144
12.4.2 MY LISTS PANEL.....	145
12.4.3 CREATING CUSTOM LISTS .....	146
12.4.4 DELETING A LIST .....	147
12.4.5 CONFIGURING A CUSTOM LIST .....	148
<b>12.5. AVAILABLE LISTS .....</b>	<b>148</b>
12.5.1 COMPUTER PROTECTION STATUS LIST .....	148
12.5.2 LIST OF CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED.....	151
12.5.3 HISTORY OF BLOCKED PROGRAMS LIST .....	153
12.5.4 LIST OF THREATS ALLOWED BY THE ADMINISTRATOR .....	156
12.5.5 HISTORY OF THREATS ALLOWED BY THE ADMINISTRATOR LIST .....	158
12.5.6 MALWARE/PUP ACTIVITY LIST .....	160
12.5.7 EXPLOIT ACTIVITY LIST.....	162
12.5.8 LICENSES LIST .....	164
12.5.9 'UNMANAGED COMPUTERS DISCOVERED' LIST .....	164
<b>12.6. DEFAULT LISTS .....</b>	<b>164</b>
<b><u>13. MANAGING THREATS, QUARANTINED ITEMS AND ITEMS BEING CLASSIFIED .....</u></b>	<b><u>166</u></b>
<b>13.1. INTRODUCTION.....</b>	<b>167</b>
<b>13.2. TOOLS FOR MANAGING BLOCKED ITEMS AND EXCLUSIONS.....</b>	<b>168</b>
<b>13.3. ACTION DIAGRAMS FOR KNOWN AND UNKNOWN PROCESSES .....</b>	<b>169</b>
13.3.1 ACTION DIAGRAM FOR KNOWN FILES.....	170
13.3.2 UNKNOWN FILES.....	170
<b>13.4. RECLASSIFICATION POLICY .....</b>	<b>171</b>
13.4.1 CHANGING THE RECLASSIFICATION POLICY.....	172
13.4.2 RECLASSIFICATION TRACEABILITY .....	173
<b>13.5. UNBLOCKING/EXCLUDING ITEMS.....</b>	<b>174</b>
13.5.1 EXCLUDING UNKNOWN ITEMS PENDING CLASSIFICATION .....	174
13.5.2 EXCLUDING ITEMS CLASSIFIED AS MALWARE OR PUP .....	174
<b>13.6. MANAGING EXCLUDED ITEMS.....</b>	<b>174</b>
<b>13.7. STRATEGIES TO SUPERVISE INSTALLATION OF NEW SOFTWARE .....</b>	<b>175</b>
<b>13.8. MANAGING THE BACKUP/QUARANTINE AREA .....</b>	<b>176</b>
13.8.1 VIEWING QUARANTINED ITEMS .....	176
13.8.2 RESTORING QUARANTINED ITEMS .....	177
<b><u>14. FORENSIC ANALYSIS.....</u></b>	<b><u>178</u></b>

<b>14.1. INTRODUCTION.....</b>	<b>179</b>
<b>14.2. DETAILS OF THREATS AND CURRENTLY BLOCKED PROGRAMS IN THE PROCESS OF CLASSIFICATION.....</b>	<b>179</b>
14.2.1 MALWARE DETECTION, PUP DETECTION AND CURRENTLY BLOCKED PROGRAMS IN THE PROCESS OF CLASSIFICATION.....	179
14.2.2 EXPLOIT DETECTION.....	181
<b>14.3. ACTION TABLES.....</b>	<b>182</b>
14.2.3 SUBJECT AND PREDICATE IN ACTIONS.....	184
<b>14.4. EXECUTION GRAPHS .....</b>	<b>185</b>
14.3.1 DIAGRAMS.....	186
14.3.2 NODES .....	186
14.3.3 LINES AND ARROWS.....	188
14.3.4 THE TIMELINE.....	189
14.3.5 ZOOM IN AND ZOOM OUT.....	190
14.3.6 TIMELINE .....	190
14.3.7 FILTERS .....	190
14.3.8 NODE MOVEMENT AND GENERAL ZOOM .....	190
<b>14.5. EXCEL TABLES.....</b>	<b>192</b>
<b>14.6. INTERPRETING THE ACTION TABLES AND EXECUTION GRAPHS .....</b>	<b>193</b>
14.4.1 EXAMPLE 1: VIEWING THE ACTIONS EXECUTED BY THE MALWARE TRJ/OCJ.A .....	194
14.4.2 EXAMPLE 2: COMMUNICATION WITH EXTERNAL COMPUTERS BY BETTERSURF.....	195
14.4.3 EXAMPLE 3: ACCESS TO THE REGISTRY BY PASSWORDSTEALER.BT .....	196
<b><u>15. REMEDIATION TOOLS .....</u></b>	<b><u>199</u></b>
<b>15.1. INTRODUCTION.....</b>	<b>200</b>
<b>15.2. ON-DEMAND COMPUTER DISINFECTION .....</b>	<b>200</b>
15.2.1 HOW ON-DEMAND DISINFECTION WORKS.....	200
15.2.2 CHARACTERISTICS OF ON-DEMAND DISINFECTION TASKS.....	200
15.2.3 CREATING ON-DEMAND DISINFECTION TASKS.....	200
<b>15.3. MANAGING DISINFECTION TASKS .....</b>	<b>202</b>
<b>15.4. COMPUTER RESTART .....</b>	<b>203</b>
<b>15.5. REPORTING A PROBLEM .....</b>	<b>204</b>
<b>15.6. ALLOWING EXTERNAL ACCESS TO THE WEB CONSOLE .....</b>	<b>204</b>
<b><u>16. ALERTS.....</u></b>	<b><u>205</u></b>
<b>16.1. INTRODUCTION.....</b>	<b>206</b>
<b>16.2. EMAIL ALERTS .....</b>	<b>206</b>
16.2.1 CONFIGURING EMAIL ALERTS .....	206
16.2.1 ACCESS PERMISSIONS AND ALERTS .....	207
16.2.2 ALERT TYPES.....	207
<b><u>17. REPORTS.....</u></b>	<b><u>211</u></b>
<b>17.1. INTRODUCTION.....</b>	<b>212</b>
<b>17.2. ON-DEMAND GENERATION OF EXECUTIVE REPORTS .....</b>	<b>212</b>
17.2.1 INFORMATION REQUIRED TO GENERATE AN ON-DEMAND REPORT .....	212
<b>17.3. SCHEDULED SENDING OF EXECUTIVE REPORTS .....</b>	<b>213</b>
17.3.1 INFORMATION REQUIRED TO GENERATE A SCHEDULED REPORT.....	213

<b><u>18. CONTROLLING AND MONITORING THE MANAGEMENT CONSOLE</u></b> .....	<b>215</b>
<b>18.1. INTRODUCTION</b> .....	<b>216</b>
<b>18.2. WHAT IS A USER ACCOUNT?</b> .....	<b>216</b>
18.2.1 USER ACCOUNT STRUCTURE .....	216
18.2.2 WHAT IS THE MAIN USER? .....	216
<b>18.3. WHAT IS A ROLE?</b> .....	<b>217</b>
18.3.1 ROLE STRUCTURE .....	217
18.3.2 WHY ARE ROLES NECESSARY? .....	217
18.3.3 FULL CONTROL ROLE .....	218
18.3.4 MONITORING ROLE .....	218
<b>18.4. WHAT IS A PERMISSION?</b> .....	<b>218</b>
18.4.1 UNDERSTANDING PERMISSIONS.....	219
<b>18.5. ACCESSING THE USER ACCOUNT AND ROLE SETTINGS</b> .....	<b>222</b>
<b>18.6. CREATING AND CONFIGURING USER ACCOUNTS</b> .....	<b>222</b>
<b>18.7. CREATING AND CONFIGURING ROLES</b> .....	<b>223</b>
<b>18.8. USER ACCOUNT ACTIVITY LOG</b> .....	<b>223</b>
18.8.1 ACTION LOG .....	223
18.8.2 SESSION LOG .....	226
<b><u>19. APPENDIX 1: ADAPTIVE DEFENSE REQUIREMENTS</u></b> .....	<b>228</b>
<b>19.1. REQUIREMENTS FOR WINDOWS PLATFORMS</b> .....	<b>229</b>
19.1.1 SUPPORTED OPERATING SYSTEMS .....	229
19.1.2 HARDWARE REQUIREMENTS .....	229
<b>19.2. WEB CONSOLE ACCESS</b> .....	<b>229</b>
<b>19.3. ACCESS TO SERVICE URLS</b> .....	<b>230</b>
<b><u>20. APPENDIX 2: CREATING AND MANAGING A PANDA ACCOUNT</u></b> .....	<b>231</b>
<b>20.1. INTRODUCTION</b> .....	<b>232</b>
<b>20.2. CREATING A PANDA ACCOUNT</b> .....	<b>232</b>
<b>20.3. ACTIVATING YOUR PANDA ACCOUNT</b> .....	<b>232</b>
<b><u>21. APPENDIX 3: LIST OF UNINSTALLERS</u></b> .....	<b>234</b>
<b><u>22. APPENDIX 4: KEY CONCEPTS</u></b> .....	<b>241</b>



# 1. Preface

---

Who is this guide aimed at?  
What is Adaptive Defense on Aether?  
Icons

## 1.1. Introduction

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

## 1.2. Who is this guide aimed at?

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

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

## 1.3. What is Adaptive Defense on Aether?

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

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

### **Adaptive Defense**

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

### **Aether Platform**

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

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

## 1.4. Icons

The following icons are used in this guide:



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



Suggestions and recommendations



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



Additional information available in other chapters or sections of the guide

# 2. Introduction

---

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

## 2.1. Introduction

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

### **It allows the execution of legitimate software only**

**Adaptive Defense on Aether** protects workstations and servers by allowing only legitimate software to run, while monitoring and classifying all processes run on the customer's IT network based on their nature and behavior.

### **It adapts to the organization's environment**

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

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

### **Assessment and remediation of security problems**

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

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

Adaptive Defense doesn't require the installation of a new management or maintenance infrastructure in the organization, thereby reducing the total cost of ownership (TCO)

## 2.2. Adaptive Defense on Aether: key features

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

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



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

### 2.3. Aether Platform: key features

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

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

**Adaptive Defense** operates completely transparently on **Aether** for administrators and users alike, as it has been designed from the bottom up.

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

#### 2.3.1 Key benefits of Aether

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

- **Cloud management platform**

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

- It does not require management servers to host the management console on the customer's premises: as it operates from the cloud, it can be accessed directly by all

devices subscribed to the service, from anywhere and at any time, regardless of whether they are office-based or on-the-road.

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

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

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

- **Multi-product**

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

- **Minimize the learning curve:** all products share the same platform, thereby reducing the time that administrators require to learn how to use the new tool, which in turn reduces the TCO.
- **Single deployment for multiple products:** only one software program is required on each device to deliver the functionality of all products compatible with **Aether Platform**. This minimizes the resource consumption on users' devices in comparison with separate products.
- **Greater synergy between products:** all products report through the same console and on a single platform: administrators have a single dashboard from which they can see all the generated data, reducing the time and effort invested in maintaining several independent information repositories and in consolidating the information into a single format.

- **Flexible and granular settings**

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

- **Complete and customized information**

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

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

### 2.3.2 Aether architecture

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

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

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

### 2.3.3 Aether on users' computers

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

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

- **Aether real-time communications agent**

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





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

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

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

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

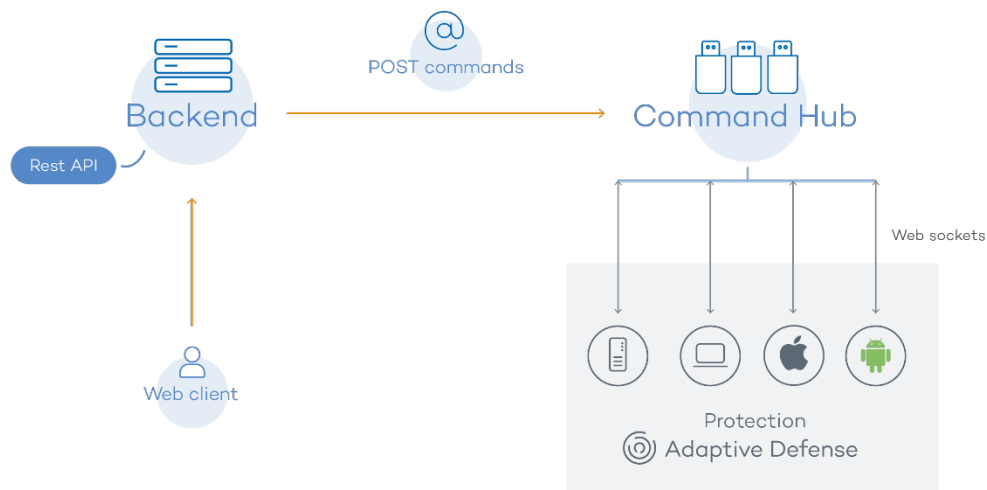


Figure 3: flowchart of the commands entered via the management console

## 2.4. Adaptive Defense architecture: key components

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

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

**Adaptive Defense** is made up of the following components:

- Cloud server farm
- Management console Web server
- Computers protected with **Adaptive Defense** through the installed agent
- 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 each of these components.

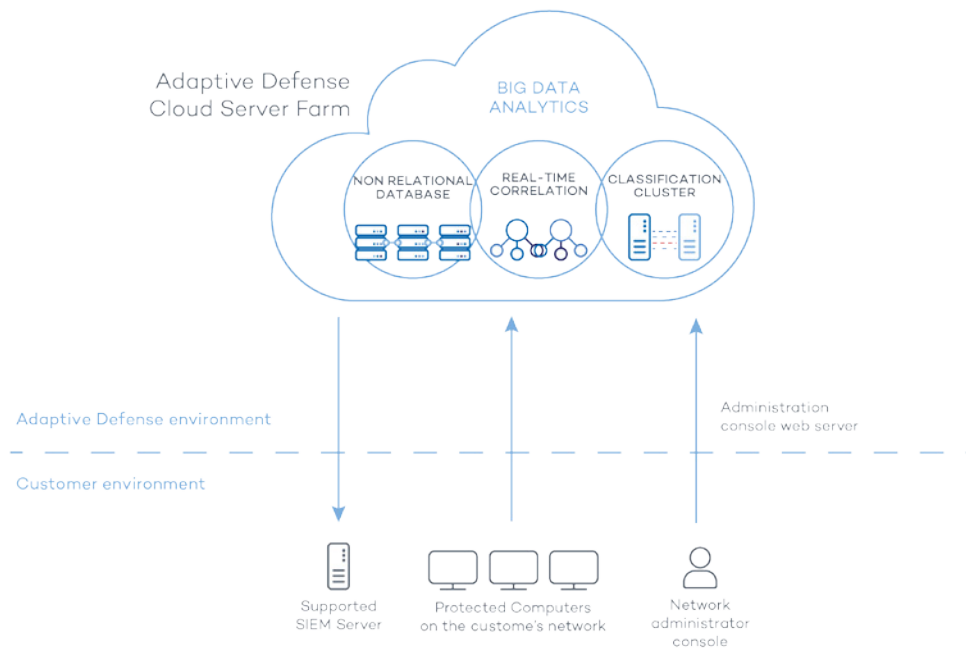


Figure 4: *Adaptive Defense* general structure

### 2.4.1 Adaptive Defense cloud server farm

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

The **Adaptive Defense** server cluster is made up of a server farm hosted in the cloud which forms a Big Data exploitation environment. It is in this environment where we continually apply the Machine Learning rules that classify each of the processes run on users' computers.

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

- 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** is monitored and analyzed. This eliminates the uncertainty that characterizes traditional antivirus solutions, which can recognize malware items but cannot identify any other application.
- The delay in classifying processes seen for the first time (the malware window of opportunity) is minimal, as **Adaptive Defense** sends the actions triggered by each process in real time to our servers. Our cloud servers are constantly working on the actions collected by our sensors, significantly reducing any delay in issuing a classification and the time that computers are exposed to threats. In addition, every executable file found on users'

computers that is unknown to the **Adaptive Defense** platform is sent by the agent to our servers for analysis.



*The impact of sending unknown files to our servers for analysis is minimal on the customer's network. Unknown files are sent only once for all customers using Adaptive Defense. Additionally, bandwidth management mechanisms have also been implemented, as well as per-agent and per-hour limits in order to minimize the impact on the customer's network.*

- The continuous monitoring of every process allows **Adaptive Defense** to classify as malware items which initially behaved as goodware. This is typical of targeted attacks and other advanced threats designed to operate under the radar.
- There is minimal consumption of CPU resources on the user's computer (2% compared to 5%-15% usage by traditional security solutions), as the entire scanning and classification process is carried out in the cloud. The agent installed simply collects the classification sent by the **Adaptive Defense** server and takes a corrective action.
- Cloud-based scanning frees customers from having to install and maintain a dedicated hardware and software infrastructure, or stay up to date with license payments and manage warranties, notably reducing the TCO.

## 2.4.2 Management console Web server

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

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



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

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

## 2.4.3 Computers protected with Adaptive Defense

**Adaptive Defense** requires the installation of a small software component called **agent** on all computers on the network susceptible of having security problems.

This component is made up of two modules: the Panda communications agent and the **Adaptive Defense** protection module.

The **Adaptive Defense** protection module contains the technologies designed to protect customers' computers. **Adaptive Defense** provides, in a single product, everything necessary to detect

targeted and next-generation malware (APTs), as well as remediation tools to disinfect compromised computers and assess the impact of intrusion attempts.



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

## 2.5. Adaptive Defense services

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

### 2.5.1 Advanced Reporting Tool service

**Adaptive Defense** 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.

The actions triggered by the processes run across the IT network are sent to **Advanced Reporting Tool**, where they are flexibly and visually correlated in order to extract security intelligence and obtain additional information on threats and the way users are using corporate computers.

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



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

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

**Adaptive Defense** integrates with the most popular third-party SIEM solutions used by customers, transmitting data about the applications run on their computers. This information is sent to the SIEM server along with all the knowledge generated by **Adaptive Defense**, allowing administrators to leverage it with their own systems.

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

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora



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

### 2.5.3 Samples Feed

This service is a perfect complement for those companies that have their own malware analysis laboratory.

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

Panda Security also delivers malware automations, that is, comprehensive execution reports detailing the actions taken by the malware in Panda Security's real-machine sandbox infrastructures.

### 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 to increase the protection level of their network.

## 2.6. Adaptive Defense on Aether: user profile

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

## 2.7. Adaptive Defense on Aether: supported devices and languages



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

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

- Windows Workstation
- Windows Server

Additionally, the management console supports the following Web browsers:

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

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

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

## 2.8. Available resources and documentation

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

### Guide for Network Administrators

<http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/ADAPTIVEDEFENSEoAP-guide-3.20.0-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/uk/support/adaptive-defense-aether.htm>

**Product Page**

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



# 3. The adaptive protection full cycle

---

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

### 3.1. Introduction

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

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

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

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

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

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

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

### 3.2. The adaptive protection cycle

The aim of **Adaptive Defense** 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**, a company's technical department will receive unambiguous classification of absolutely all programs run on its IT resources.

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

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

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

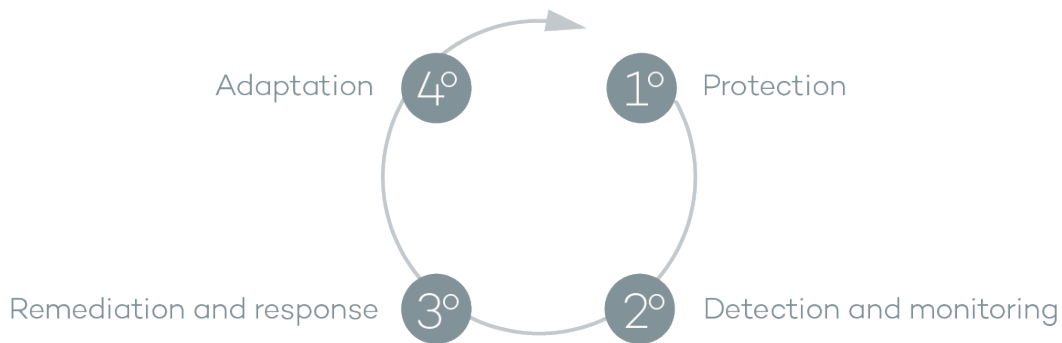


Figure 5: adaptive protection cycle

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

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

#### 3.3.1 Anti-exploit protection

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

Exploit threats leverage both known and unknown (zero-day) vulnerabilities, triggering a chain of events (CKC, Cyber Kill Chain) that they must follow to compromise systems. **Adaptive Defense** 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** 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** to detect the exploit techniques used by hackers, going beyond the traditional approach used by other security products and consisting of searching for patterns and statically detecting CVE-payload pairs through signature files.

In short, **Adaptive Defense** 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 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 solution's signature files, **Adaptive Defense** uses several detection engines that scan the behavior of processes locally.

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

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

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

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

### 3.4.1 Advanced permanent protection

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

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

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

- **Audit**

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

- **Hardening**

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

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

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



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

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

- **Lock**

In environments where security is the top priority, and in order to offer maximum security guarantees, **Adaptive Defense** should be configured in Lock mode. In this mode, the software that is in the

process of classification is prevented from running. This means that only legitimate software is allowed to run.

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



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

### 3.4.2 Monitoring data files

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

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

### 3.4.3 Network status visibility

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

The important thing in this phase is not only to be able to determine whether the customer's network has been attacked and the extent of the attack, but to have the necessary information to determine the likelihood of an infection.

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

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

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

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



*Refer to 12 Malware and network visibility for more information about how to view and monitor computers and processes*

### 3.5. Phase 3: remediation and response

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

- **Response**

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

Additionally, the **Advanced Reporting Tool** service stores every action taken by the processes run by users (goodware, malware or unknown processes). **Advanced Reporting Tool** extends the functionality of the forensic analysis module, enabling administrators to perform advanced searches and generate activity graphs to facilitate data analysis and interpretation.

- **Remediation**

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



*Refer to chapter 15 Remediation tools for more information*

### 3.6. Phase 4: adaptation

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

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

**Adaptive Defense** can be used to strengthen the organization's security status simply by changing the operating mode of the advanced protection: if the company's users tend to always use the same software, but there are users who install programs from dubious sources, a possible solution to reduce the risk posed by those users is to enable the Lock mode provided by the advanced protection. This will minimize malware exposure on top risk computers, preventing the unwanted use of illegitimate programs.



# 4. The management console

---

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

## 4.1. Introduction

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

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

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

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

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

- **Service management from anywhere at anytime**

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

### 4.1.1 Web console requirements

The Web console can be accessed from the following link:

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

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

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



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

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

### 4.1.2 IDP federation

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

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

## 4.2. General characteristics of the console

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

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

## 4.3. General structure of the Web management console

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

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

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




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

### 4.3.1 Top menu (1)

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

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

#### Panda Cloud button

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

#### Status menu

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



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

## Computers menu

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

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



Refer to chapter 8 Managing settings for more information.

## Settings menu

Lets you define different types of settings:

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



Refer to chapter 18 Controlling and monitoring the management console for more information.

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



Refer to chapter 9 for more information.

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



Refer to chapter 16 Alerts for more information.

## Tasks menu

Provides the ability to view all the disinfection tasks that are in progress as well as those previously launched.



Refer to chapter 15 Remediation tools for more information.

### General Settings menu

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

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

### User Account menu

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

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

### 4.3.2 Side menu (2)

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

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

### 4.3.3 Widgets (3)

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

 Refer to chapter 12 Malware and network visibility for more information.

### 4.3.4 Tab menu

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

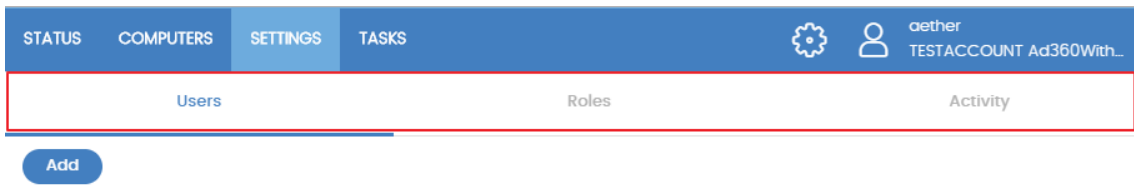


Figure 7: tab menu

### 4.3.5 Filtering and search tools

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

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

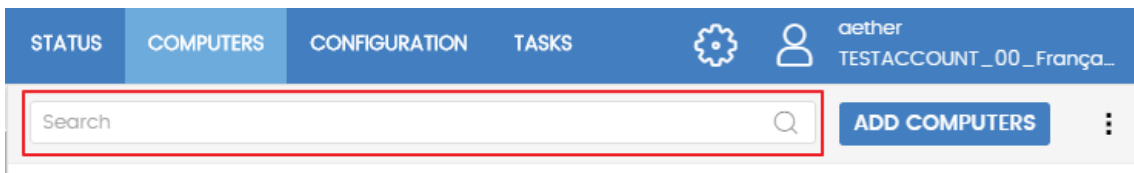


Figure 8: search tool

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

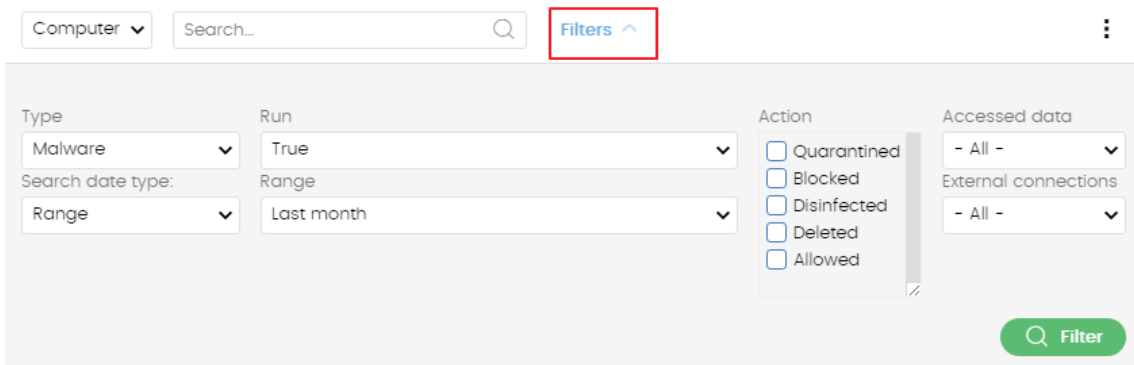


Figure 9: filtering tool for data lists

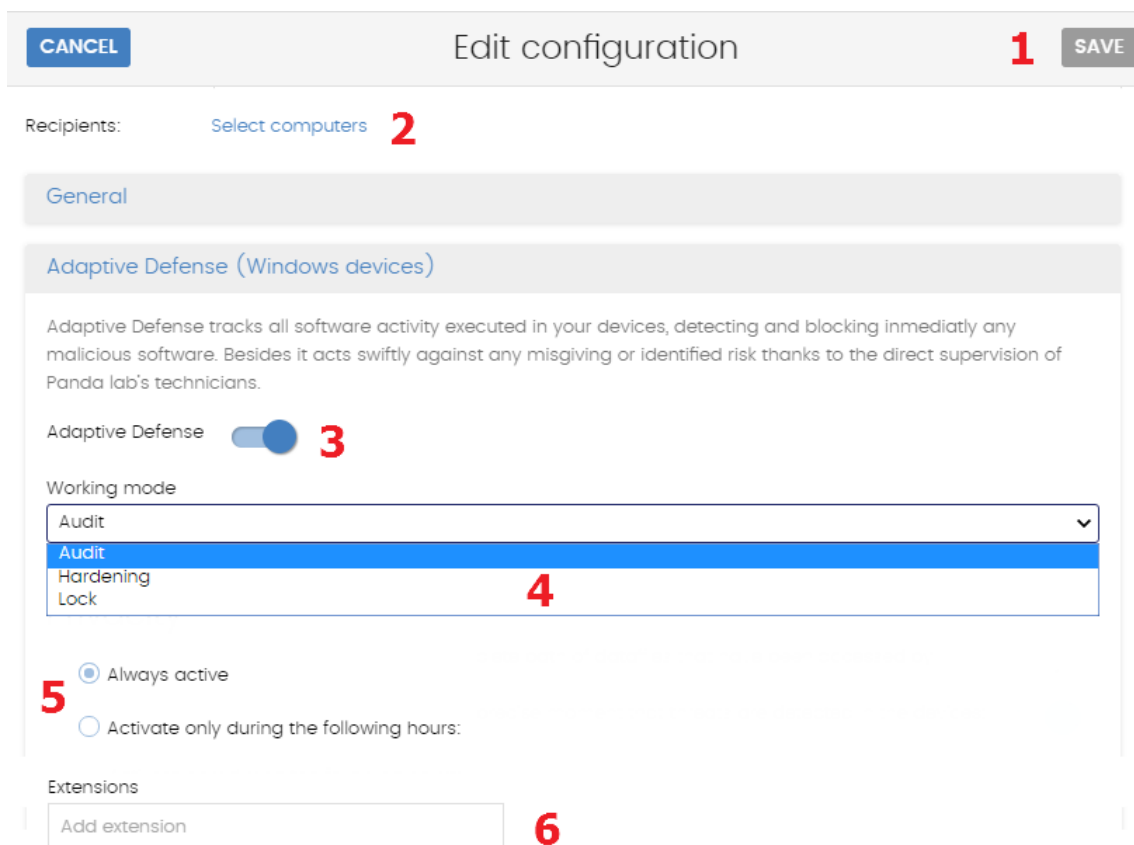
### 4.3.6 Back button

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

### 4.3.7 Settings elements (8)

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


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



The screenshot shows the 'Edit configuration' interface for Adaptive Defense. At the top, there is a header bar with a 'CANCEL' button (1), the title 'Edit configuration', and a 'SAVE' button (1). Below the header, there is a 'Recipients:' section with a 'Select computers' link (2). The main content area is titled 'General' and 'Adaptive Defense (Windows devices)'. It contains a descriptive paragraph, a toggle switch for 'Adaptive Defense' (3), a 'Working mode' dropdown menu (4) with options 'Audit', 'Hardening', and 'Lock', and radio buttons for 'Always active' (5) and 'Activate only during the following hours:'. At the bottom, there is an 'Extensions' section with an 'Add extension' text field (6).

Figure 10: controls for using the management console

### 4.3.8 Context menus

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



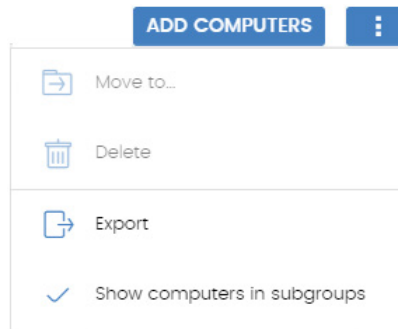


Figure 11: context menu

### 4.3.9 Lists

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

Executed malware **1**

**3**

---

**2** Filters ^

Type: Malware

Date search type: Range Range: Last month

Search: Host Name Run: True

Action:

- Moved quarantine
- Blocked
- Cleaned
- Deleted
- Allowed

Accessed data: - All -

External connections: - All -

**4**

**5** FILTER

Host Name	Threat	File path	⚡	📄	🌐	Action	Date
Machine_Cus tomer_1_id38	Malware Nam e 2	Malware Path Sample 2	●	●	○	Deleted	3/10/2017 1:00: 00 AM
Machine_Cus tomer_1_id38	Malware Nam e 14	Malware Path Sample 14	●	●	○	Allowed	3/15/2017 12:1 8:00 AM
Machine_Cus tomer_1_id38	Malware Nam e 8	Malware Path Sample 8	●	●	○	Cleaned	3/14/2017 9:2 4:00 PM
Machine_Cus tomer_1_id38	Malware Nam e 10	Malware Path Sample 10	●	●	○	Blocked	3/14/2017 10:2 2:00 PM
Machine_Cus tomer_1_id38	Malware Nam e 4	Malware Path Sample 4	●	●	○	Blocked	3/14/2017 7:28: 00 PM

**6**

**7** 10 entries v 1 to 10 of 2140 **8** **9** **10** **11** **12** **13**

Figure 12: items in lists

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

the top of the list view. Click the same header a second time to switch between ascending and descending order. This is indicated with arrows (↑ for ascending and ↓ for descending).

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

# 5. Licenses

---

Definitions and key concepts

Contracted licenses

Expired licenses

Trial licenses

Computer search based on license status

## 5.1. Introduction

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

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

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



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

## 5.2. Definitions and key concepts for managing licenses

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

### 5.2.1 License contracts

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

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

### 5.2.2 Computer status

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

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



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

### 5.2.3 License status and groups

There are two possible status types for contracted licenses:

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

Licenses are separated into two groups according to their status:

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

### 5.2.4 Types of licenses

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

### 5.2.5 License management

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

#### Automatic assignment of licenses

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

#### Manual assignment of licenses

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

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



icon to assign a free license to the computer automatically.

### 5.2.6 License release

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

#### Automatic release

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


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

#### Manual release

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

Follow the steps below to manually release an **Adaptive Defense** license:

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

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

### 5.2.7 Processes for assigning and releasing licenses

#### Case 1: excluded computers and those with assigned licenses

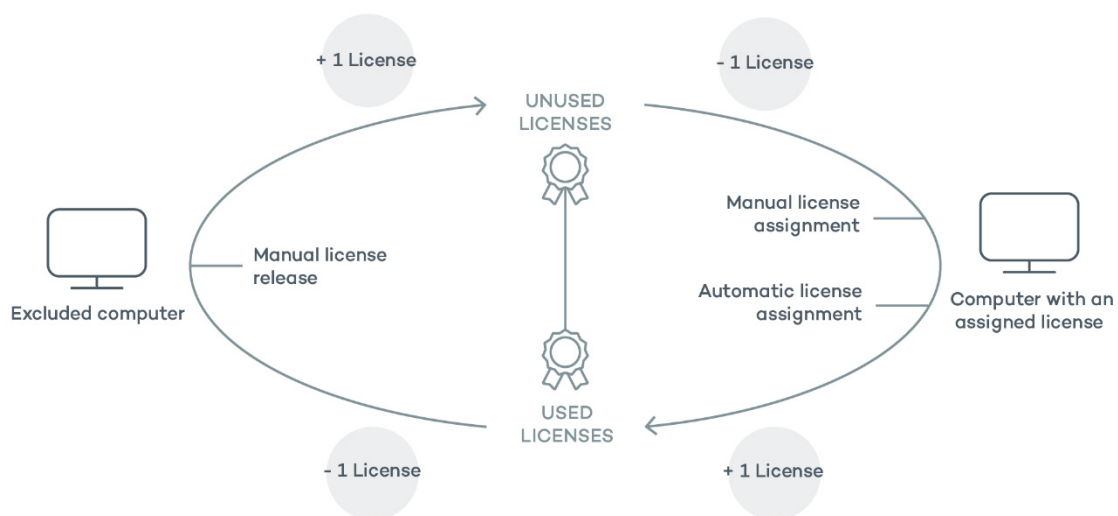


Figure 13: modification of license group with excluded computers and those with licenses assigned

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

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

### Case 2: computers without an assigned license

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

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

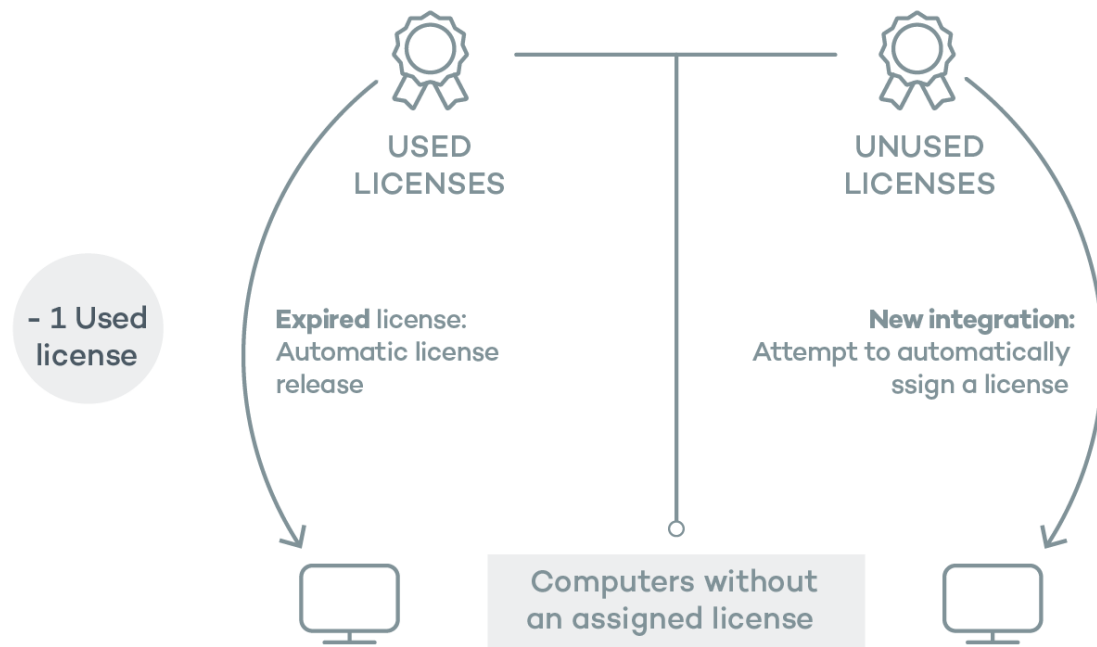


Figure 14: computers without an assigned license due to expiry of the license contract and because the group of unused licenses is empty.

## 5.3. Contracted licenses

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

### 5.3.1 Widget

The panel shows how the contracted product licenses are distributed.

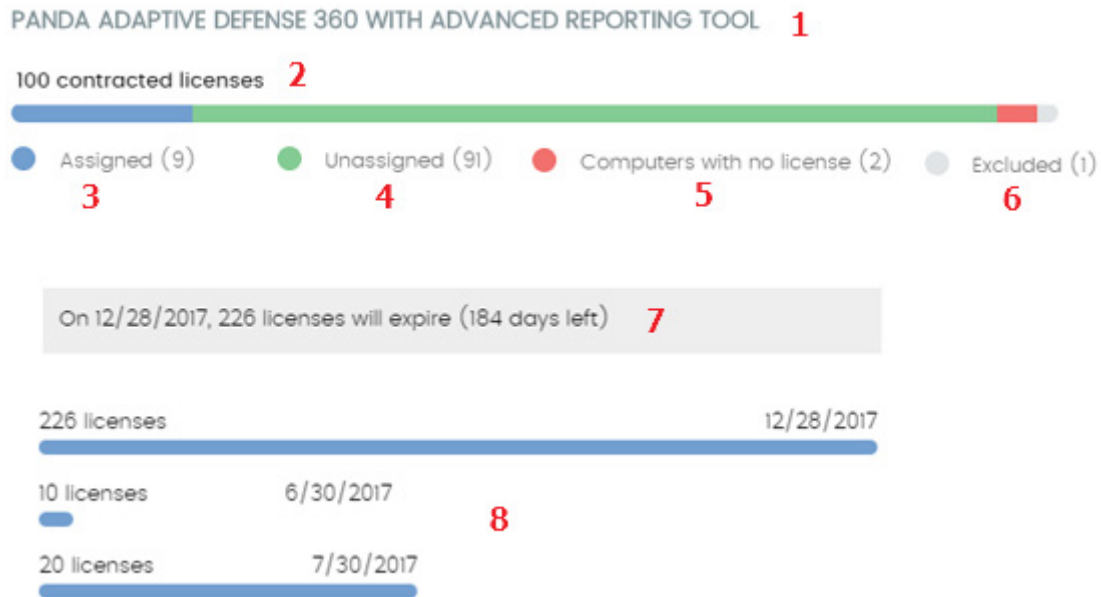


Figure 15: license panel with three license contracts

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

### Name of the contracted product (1)

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

### Total number of contracted licenses (2)

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

### Assigned (3)

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



### Unassigned (4)

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

### Computers without a license (5)

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

### Excluded computers (6)

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

### License expiry (7)

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

### License contract expiry (8)

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

## 5.3.2 License list

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



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

Table 1: protected computer list fields

### Fields displayed in the exported file

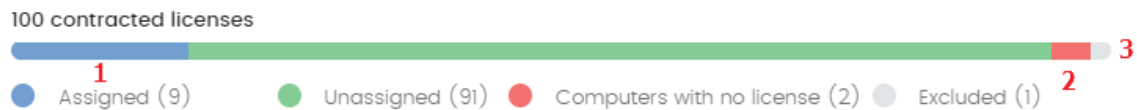
Filed	Comment	Values
Client	Customer account that the product belongs to.	Character string

Filed	Comment	Values
Computer type		Workstation Laptop Mobile device Server
Computer	Computer name	Character string
Operating system	Operating system installed, internal version and patch status.	Character string
Active Directory	Path in the company's Active Directory tree where the computer is found	Character string
Virtual machine	Indicates whether the computer is physical or virtual	Boolean
Agent version		Character string
Protection version		Character string
Installation date	Date that the Adaptive Defense software was successfully installed.	Date
Last connection date	Date that the computer status was last sent to the Panda Security cloud	Date
License status		Assigned Unassigned Excluded
Group	Folder within the Adaptive Defense group tree to which the computer belongs	Character string
IP address	Primary IP address of the computer.	Character string
Domain	Windows domain that the computer belongs to	Character string
Description		Character string

Table 2: fields in the Licenses exported file

**Filter tool**

Field	Comment	Values
Find computer	Computer name	Character string
Computer type		Workstation laptop Mobile device Server
Platform	Operating system installed.	All Windows Linux MacOS Android
Last connection	Date that the computer status was last sent to the Panda Security cloud	All More than 72 hours More than 7 days More than 30 days
License status		Assigned Unassigned Excluded

*Table 3: filter fields for the Licenses list*
**Lists accessible from the panel**

*Figure 16: hotspots in the Contracted licenses panel*

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

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

## 5.4. Expired licenses

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

### 5.4.1 Expiry notifications

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

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



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

### 5.4.2 Withdrawal of expired licenses

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

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

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



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

### 5.5. Adding Trial licenses to Commercial licenses

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

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

Once the trial period has ended, the license contract created for the trial will be deleted, the commercial license contract will be reactivated, and the network computers will be

downgraded automatically, returning to the previous settings.

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

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



*Refer to chapter 7 Managing computers and devices for more information about how to create an Adaptive Defense filter*

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

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

# 6. Installing the Adaptive Defense software

---

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

## 6.1. Introduction

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

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

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

## 6.2. Protection deployment overview

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

### Identify the unprotected devices on the network

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

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



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

### Check if the minimum requirements for the target platform are met

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

### Select the installation procedure

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

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

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

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

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



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

You can install **Adaptive Defense** on a computer that already has an antivirus solution from another vendor, since, by default, both security solutions will coexist on the same system without any problems.

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



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

- **Panda Security antivirus products**

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

Table 4 summarizes the necessary conditions for a computer restart.

Previous product	Adaptive Defense on Aether	Restart
None	Trial or commercial version	NO
Endpoint Protection Legacy, Endpoint Protection Plus Legacy, Adaptive Defense Legacy, Adaptive Defense Legacy, Panda Fusion Legacy	Commercial version	LIKELY (Only if a protection upgrade is required)
Third-party antivirus	Trial version	NO (By default, both products will coexist)



Third-party antivirus	Commercial version	LIKELY (A restart may be necessary to finish uninstalling the third-party product)
Citrix systems	Trial or commercial version	LIKELY (with older versions)

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

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

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

### Determine the computers' default settings

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

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

## 6.3. Installation requirements



*For a full description of the necessary requirements for each platform, refer to Appendix 1: adaptive Defense requirements*

### 6.3.1 Requirements for each supported platform


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

### 6.3.2 Network requirements

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

## 6.4. Manually downloading and installing the Adaptive Defense software

### 6.4.1 Downloading the installation package from the Web console



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

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

- Go to the **Computers** menu, click **Add computers**, and select the platform to protect: windows, Linux, Android or MacOS (Figure 17).
- Select the group that the computer will integrate into (Figure 18):
  - To integrate the computer into a native group, click **Add computers to this group (1)** and select a destination in the folder tree displayed.
  - To integrate the computer into an Active Directory group, click **Add computers to their Active Directory path (2)**.
- Next, you must select the proxy and language settings **(3)** to apply to the computer. If the computer is to be integrated into a native group, it will automatically inherit the settings of the folder where it will reside. However, if you choose to integrate it into an Active Directory group, you'll have to manually select the proxy and language settings from those displayed in the drop-down menu. If the automatic selection does not meet your needs, click the drop-down menu and select one of the available options.

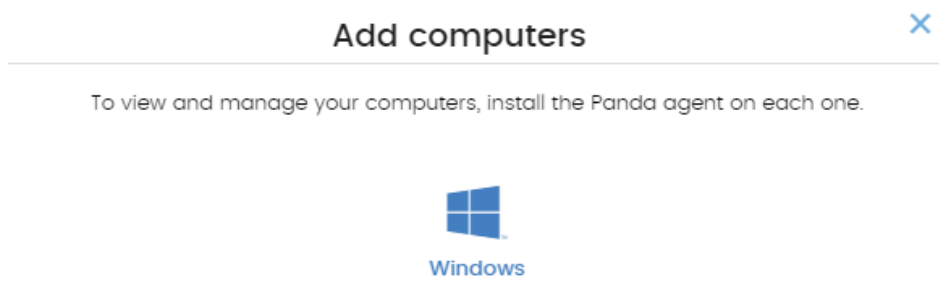


Figure 17: platform selection window

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

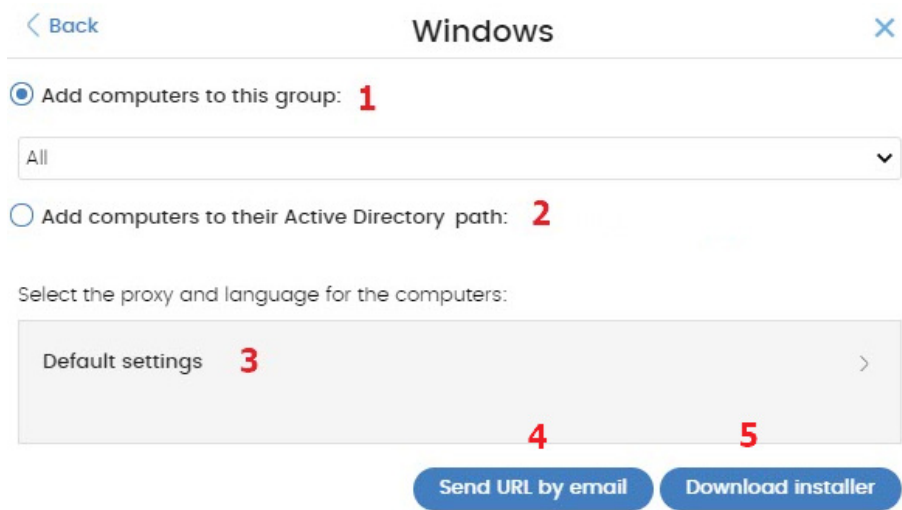


Figure 18: configuración del paquete de descarga

### 6.4.2 Generating a download URL

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

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

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

End users will automatically receive an email with the download link. Clicking the link will download the installer.

### 6.4.3 Manually installing the Adaptive Defense software



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

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

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

## 6.5. Automatic computer discovery and remote installation

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

### 6.5.1 Requirements for installing Adaptive Defense

For you to be able to install **Adaptive Defense** remotely, the following requirements must be met:

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



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

### 6.5.2 Computer discovery

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

#### Requirements for finding unprotected computers on your network

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

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



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

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

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

## Characteristics of a discovery computer

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

The following information is displayed for each discovery computer:

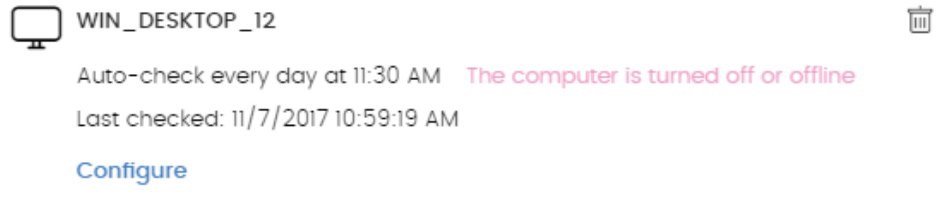


Figure 19: information displayed for each discovery computer

### Computer name

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

### 6.5.3 Discovery scope

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

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

### 6.5.4 Scheduling computer discovery tasks

#### Scheduling a task

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

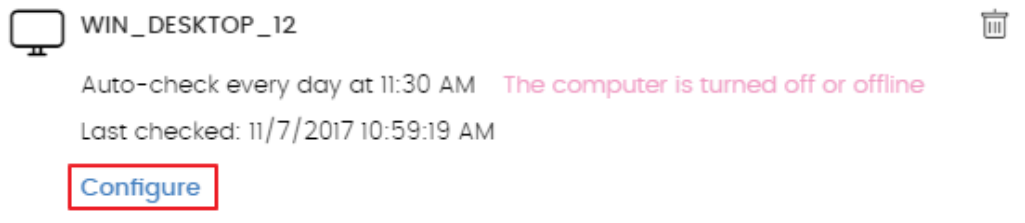


Figure 20: access to the discovery task settings window

- **Automatic execution of discovery tasks**
  - Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Discovery** tab. Select a discovery computer and click **Configure**.
  - From the **Run automatically** drop-down menu, select **Every day**.
  - Select the start time of the scheduled task.
  - Select whether to take the discovery computer's local time or the **Adaptive Defense** server time as reference.
  - Click **OK**. The discovery computer will show a summary of the scheduled task in its description.
  
- **Manual execution of discovery tasks**
  - Click the **Settings** menu at the top of the console. Then, click **Network settings** from the side menu and click the **Discovery** tab. Select a discovery computer and click **Configure**.
  - From the **Run automatically** drop-down menu, select **No**.
  - Click **OK**. The computer will display a **Check now** link which you can use to run a discovery task on demand.

### 6.5.5 List of discovered computers

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

There are two ways to access this list:

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

- **Protection status widget**

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

## PROTECTION STATUS


 Figure 21: access to the list of discovered computers from the **Protection status** widget

- **My lists**

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

**Description of the list of discovered computers**

Campo	Comentario	Valores
Computer	Name of the discovered computer	Character string
Status	Indicates the computer status with regard to the installation process	<ul style="list-style-type: none"> <li>— <b>Discovered:</b> the computer is eligible for installation, but the installation process has not started yet</li> <li>☁ <b>Installing:</b> the installation process is in progress</li> <li>⚠ <b>Installation error:</b> displays a message specifying the type of error. See later for a description of all possible errors</li> </ul>
IP address	The computer's primary IP address	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card	Character string
Discovered by	Name of the discovery computer	Character string

Campo	Comentario	Valores
Status	Date when the computer was last discovered	Date

Table 5: fields in the list of discovered computers

Next is a description of the possible error messages:

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

#### Fields displayed in the exported file

Campo	Comentario	Valores
Customer	Customer account that the service belongs to	Character string
Computer	Name of the discovered computer	Character string
IP	The computer's primary IP address	Character string
MAC address	The computer's physical address.	Character string
NIC manufacturer	Manufacturer of the discovery computer's network interface card	Character string



Campo	Comentario	Valores
Domain	Windows domain the computer belongs to	Character string
First seen	Date when the computer was first discovered	Character string
First seen by	Name of the discovery computer that first saw the workstation/server	Character string
Last seen	Date when the computer was last discovered	Date
Last seen by	Name of the discovery computer that last saw the workstation/server	Character string

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

### Filter tool

Campo	Comentario	Valores
Search	Search by computer name, IP address, NIC manufacturer or discovery computer	Character string
Status	Adaptive Defense installation status	<b>Discovered:</b> the computer is eligible for installation, but the installation process has not started yet <b>Installing:</b> the installation process is in progress <b>Installation error</b>
Last seen	Date when the computer was last discovered	Last 24 hours Last 7 days Last month

Table 7: filters available in the list of discovered computers

### Hidden computers

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

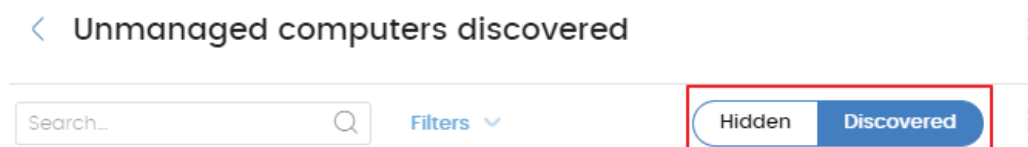


Figure 22: discovered/Hidden computer list selector

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


- To hide a single computer, click the computer's context menu and select **Hide and do not discover again (4)**

### Deleted computers

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

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

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



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

### 6.5.6 Details of a discovered computer

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

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

**1**

#### Computer details

Computer name:	Discovered_00_01
Description:	<a href="#">Change</a>
First seen:	11/6/2017 10:59:18 AM
Last seen:	11/6/2017 10:59:20 AM
IP address:	192.168.1.1 <b>2</b>
Physical addresses (MAC addresses):	64:51:06:00:00:01
Domain:	Domain_00
NIC manufacturer:	Hewlett Packard

#### Discovered by

Computer	Last seen
<a href="#">WIN_DESKTOP_4</a> <b>3</b>	11/6/2017 10:59:18 AM
<a href="#">WIN_DESKTOP_12</a>	11/6/2017 10:59:19 AM

Figure 23: details of a discovered computer

## Computer alerts

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

## Computer details

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

## Last discovery computer

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

## 6.5.7 Installing the protection on computers

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

### From the list of discovered computers

- Go to the list of discovered computers. There are three ways to do this:

- Go to **My lists** on the left-hand side menu and click the **Add** link. From the drop-down menu, select the **Unmanaged computers discovered** list.
- Go to the **Status** menu at the top of the console. In the **Protection status** widget, click the link **XX computers have been discovered that are not being managed by Panda Adaptive Defense**.
- Go to the **Computers** menu at the top of the console. Click **Add computers** and select **Discovery and remote installation**. A wizard will be displayed. Click the link **View unmanaged computers discovered**
- From the list of discovered computers, select **Discovered** or **Hidden** depending on the status of the relevant computers **(1)**
- Select the checkboxes that correspond to the computers that you want to install the software on
- To install it on multiple computers simultaneously, click the general context menu and select **Install Panda agent**
- To install it on a single computer, click the computer's context menu and then click **Install Panda agent**
- Configure the installation by following the steps described in section 6.4.3 Manually installing the Adaptive Defense software.
- You can enter one or multiple installation credentials. Use the local administrator account of the target computer or the domain that it belongs to in order to install the software successfully

### From the computer details window

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

## 6.6. Installation with centralized tools

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

### 1 Download and share the Adaptive Defense installer

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

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

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

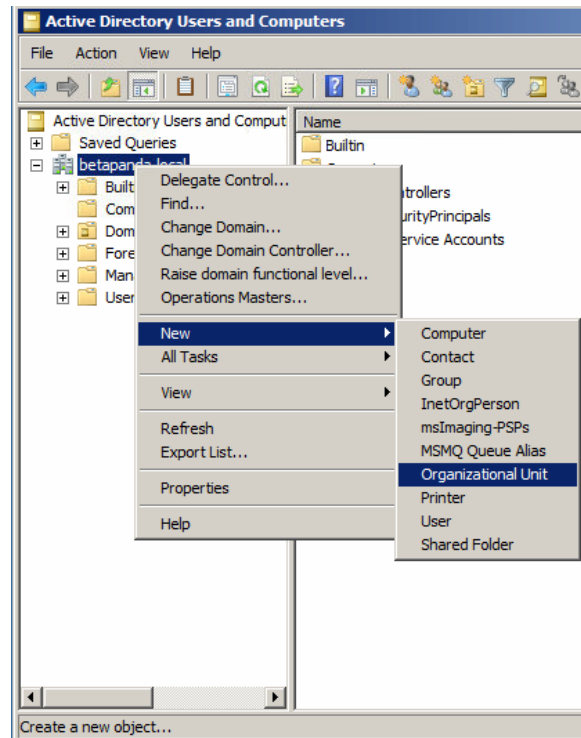


Figure 24: create an Organizational Unit

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

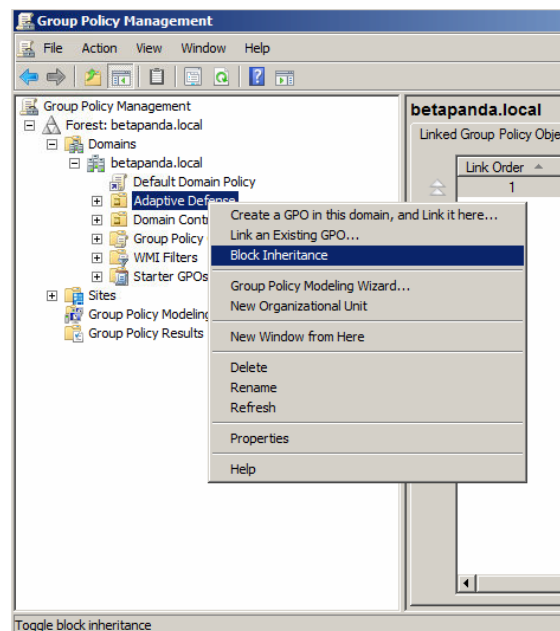


Figure 25: block inheritance

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

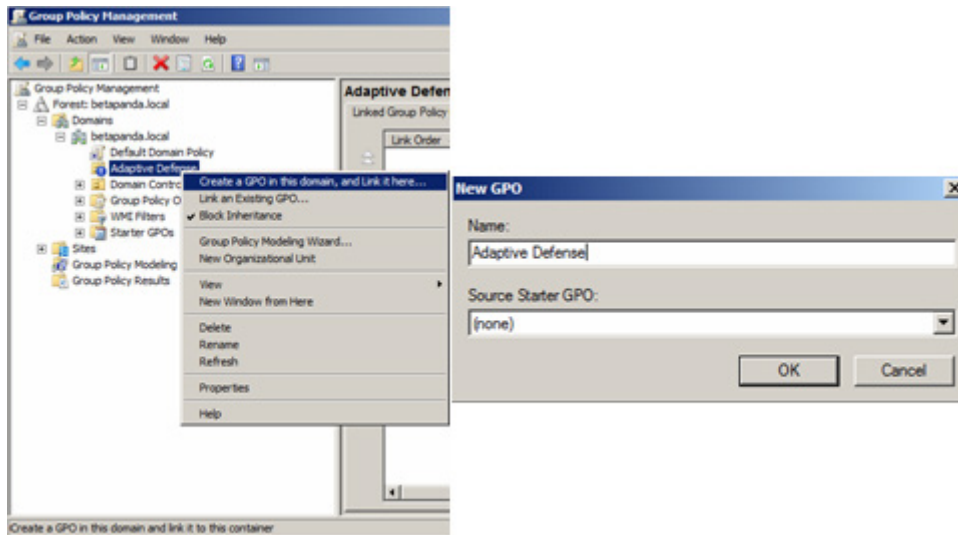


Figure 26: create a GPO

### 3 Add a new installation package to the newly created GPO

- Edit the GPO.

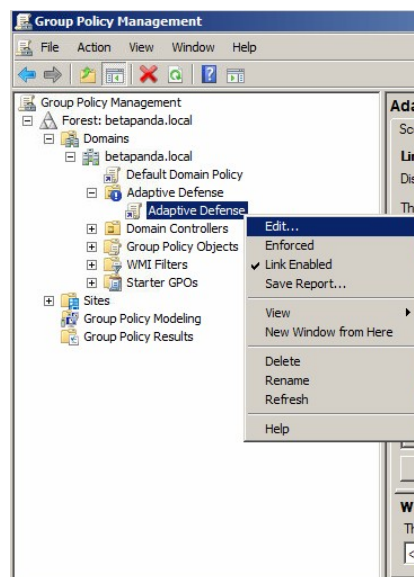


Figure 27: edit the newly created GPO

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

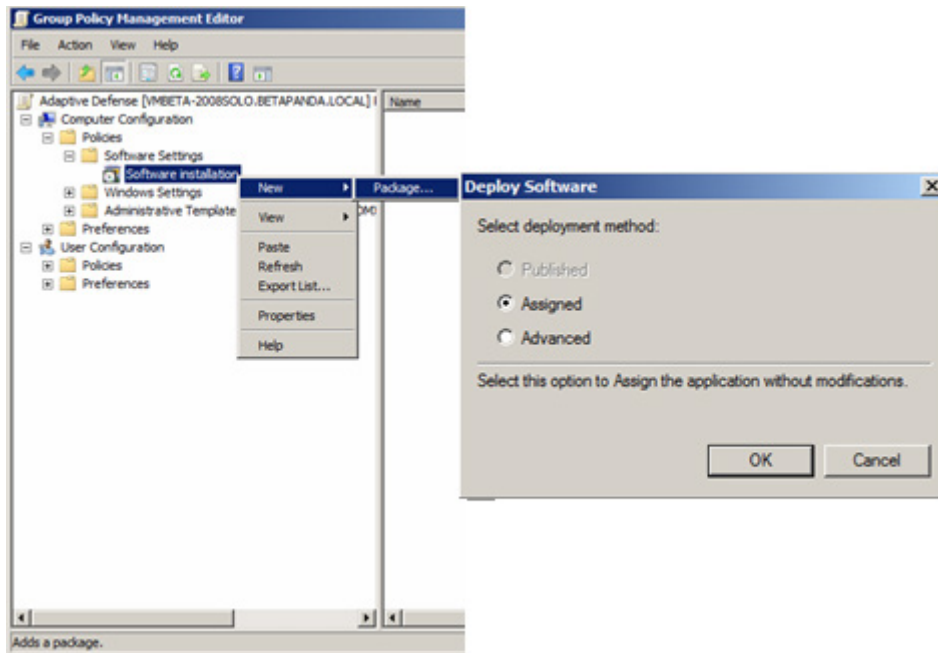


Figure 28: assign a new deployment package

#### 4 Edit the deployment properties

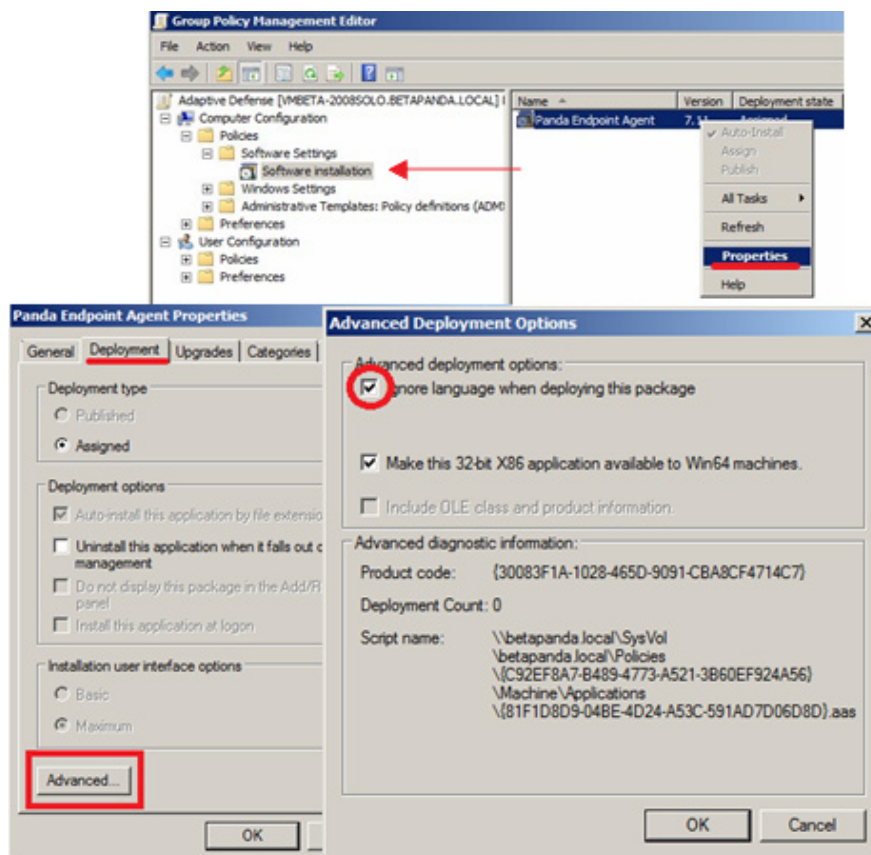


Figure 29: configure the deployment package

- Go to Properties, Deployment, Advanced, and select the checkbox to avoid checking the target operating system against the one defined in the installer.
- Finally, in the Adaptive Defense OU you created in "Active Directory Users and Computers", add all the network computers to which the software will be sent.

## 6.7. Installation using image generation

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

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

If the network administrator uses this automated deployment procedure and **Adaptive Defense** 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** software on a computer entails automatically assigning a unique ID to it. This ID is used by Panda Security to show and identify the computer in the management console. If, later, a golden image is generated with the **Adaptive Defense** software installed on it, and the image is then cloned to other computers, every computer that receives the image will inherit the same **Adaptive Defense** ID and, consequently, the console will only display a computer.

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

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

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

## 6.8. Uninstalling the software

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



**On Windows 8 and later:**

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

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

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

**On Windows XP:**

- Control Panel > Add or remove programs.

# 7. Managing computers and devices

---

The Computers area  
The Filters tree  
The Groups tree  
Computer details

## 7.1. Introduction

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

### 7.1.1 Requirements for managing computers from the management console

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

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

Devices without an **Adaptive Defense** license but with **Aether** installed will appear in the management console, although the protection will be uninstalled and scan tasks or other **Adaptive Defense** resources won't be run.



*Computers with expired licenses will not benefit from the advanced protection. In this condition, Adaptive Defense won't be able to protect them against advanced threats. Panda Security strongly recommends that organizations renew the contracted services in order to keep their IT networks properly protected.*

## 7.2. The Computers area

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

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

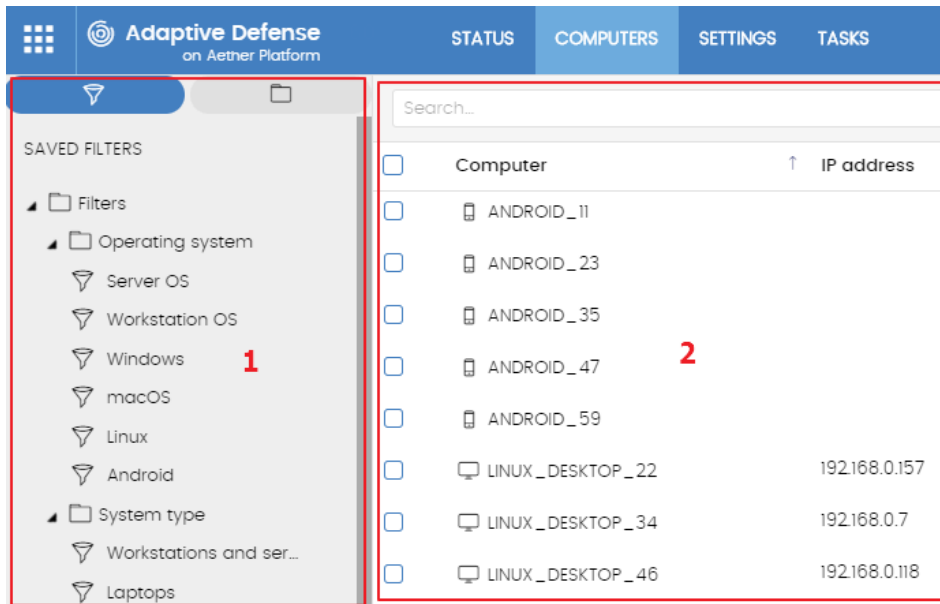


Figure 30: general view of the panels in the Computers area

### Display computers in subgroups

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

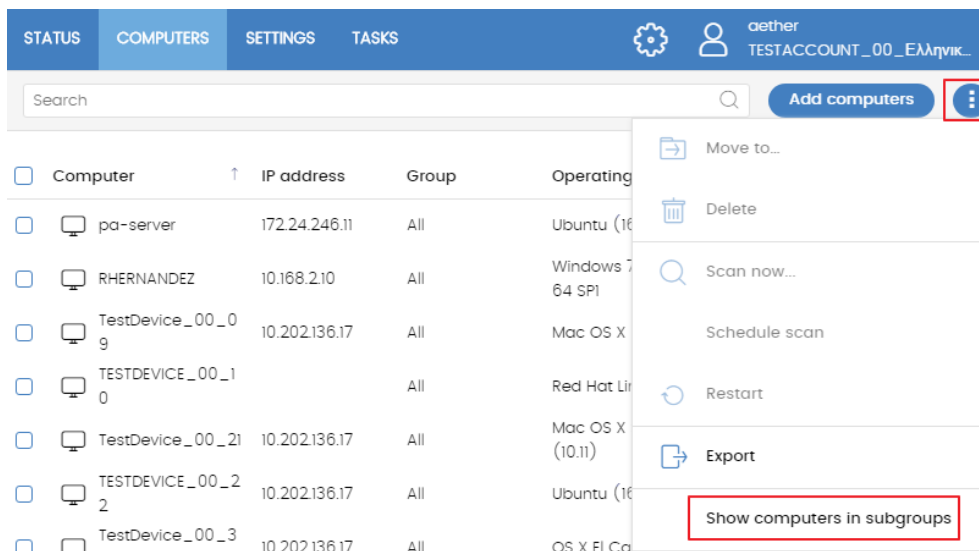


Figure 31: show computers in subgroups

## 7.2.1 The Computers tree panel

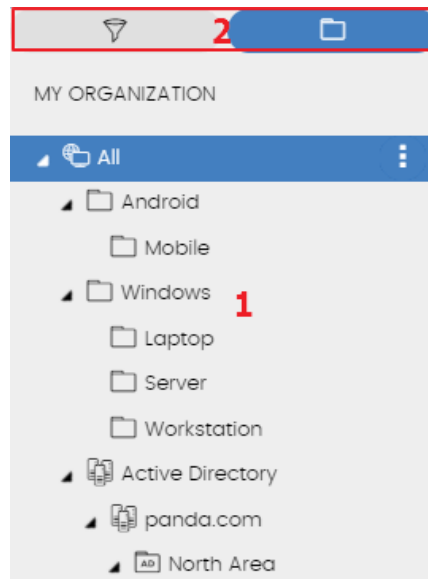




Figure 32: the Computers tree panel

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

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

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

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



*To locate unprotected computers or those with certain security criteria or protection status, see Chapter 12 Malware and network visibility. To assign security settings profiles, see Chapter 8 Managing settings. To run troubleshooting tasks, see chapter 15 Remediation tools*

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

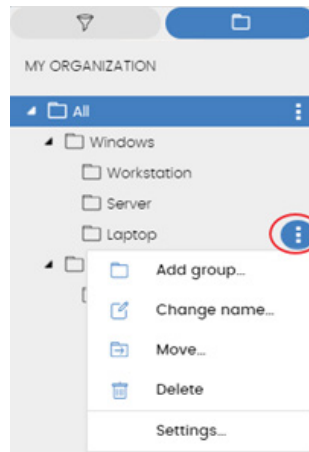
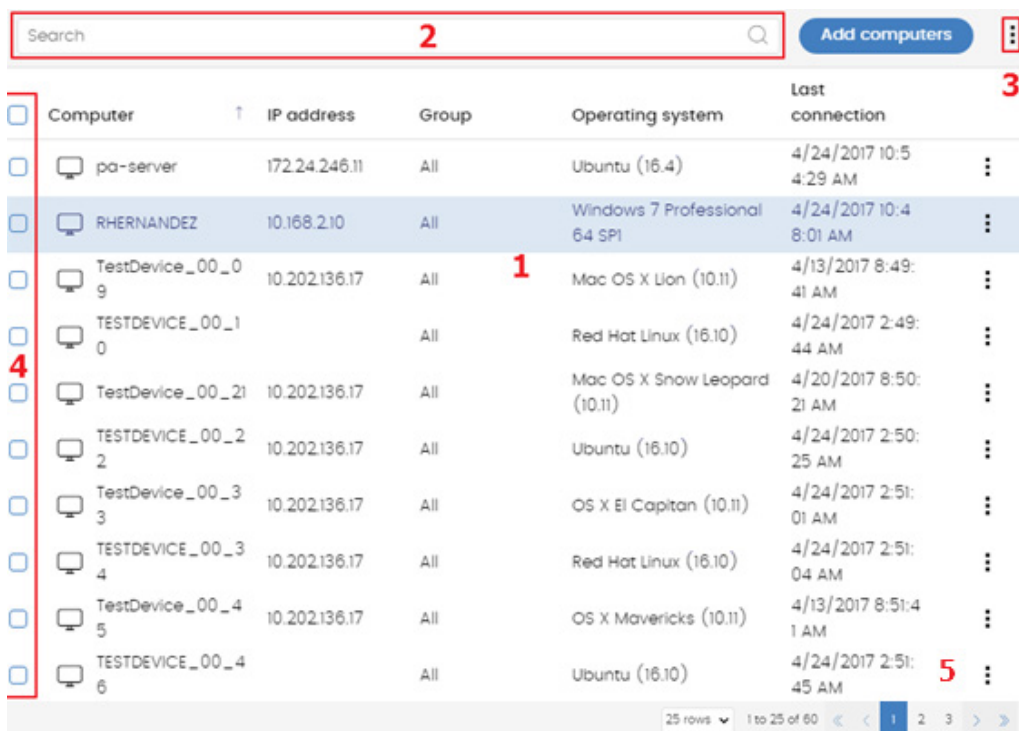


Figure 33: pop-up menu with all available operations for the selected branch

## 7.2.2 The Computers list panel

This screen displays the following information:

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



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

Figure 34: the Computers list screen

The search tool lets you locate computers by name. Partial matches can be included and uppercase/lowercase letters are not differentiated.

### 7.2.3 Computers list

You will see the following details for each computer:








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

Table 8: fields in the Computers list

#### Fields displayed in the exported file

Campo	Comentario	Valores
Customer	Customer account that the service belongs to	Character string
Computer type	Type of device	Workstation Laptop Server
Computer	Computer name	Character string
IP addresses	List of the IP addresses of the cards installed on the computer	Character string
Physical addresses (MAC)	List of the physical addresses of the cards installed on the computer	Character string
Domain	Windows domain to which the computer belongs	Character string

Campo	Comentario	Valores
Active Directory	Path in the company's Active Directory tree where the computer is found	Character string
Group	Folder in the Adaptive Defense Groups tree to which the computer belongs	Character string
Agent version		Character string
System boot date		Date
Installation date	Date when the Adaptive Defense software was successfully installed on the computer	Date
Last connection date	Last time the computer connected to the cloud	Date
Platform	Type of operating system installed	Windows Linux MacOS Android
Operating system	Operating system installed on the computer, internal version and patches applied	Character string
Virtual machine	Indicates whether the computer is physical or virtual	Boolean
Protection version		Character string
Last update on	Date the protection was last updated	Date
Licenses	Licensed product	Adaptive Defense
Proxy and language settings	Name of the proxy and language settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer has inherited the proxy and language settings	Character string
Security settings for workstations and servers	Name of the security settings applied to the workstation or server	Character string
Settings inherited from	Name of the folder from which the computer has inherited its settings	Character string
Security settings for Android devices	Name of the security settings applied to the mobile device	Character string
Settings inherited from	Name of the folder from which the device has inherited its settings	Character string
Per-computer settings	Name of the settings applied to the computer	Character string
Settings inherited from	Name of the folder from which the computer has inherited its settings	
Description		Character string

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



### 7.3. Filters tree

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

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

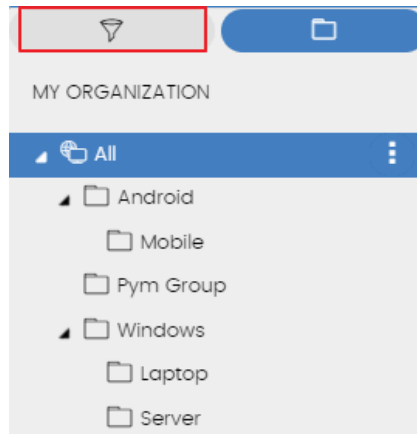


Figure 35: how to access the Filters tree

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

#### 7.3.1 What is a filter?

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



*A computer can belong to more than one filter.*

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

#### 7.3.2 Groups of filters

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

### 7.3.3 Predefined filters

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



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

Name	Group	Description
Workstations and servers	Type of device	List of physical workstations and servers
Virtual machines	Type of device	List of virtual machines
Server operating systems	Operating system	List of computers with a server operating system installed
Workstation operating systems	Operating system	List of computers with a workstation operating system installed
Java	Software	List of all computers with the Java JRE SDK installed
Adobe Acrobat Reader	Software	List of all computers with Acrobat Reader installed
Adobe Flash Player	Software	List of all computers with Flash player installed
Google Chrome	Software	List of all computers with Chrome browser installed
Mozilla Firefox	Software	List of all computers with Firefox browser installed

*Table 10: list of predefined filters*

### 7.3.4 Creating and organizing filters

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

#### Creating filters

To create a filter, follow the steps below:

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



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

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

### Creating folders

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



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

### Deleting filters and folders

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



*You cannot delete the 'Filters' root node.*

### Moving and copying filters and folders

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

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




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

### Renaming filters and folders

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

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

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

### 7.3.5 Filter settings

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

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

A filter has four sections:

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

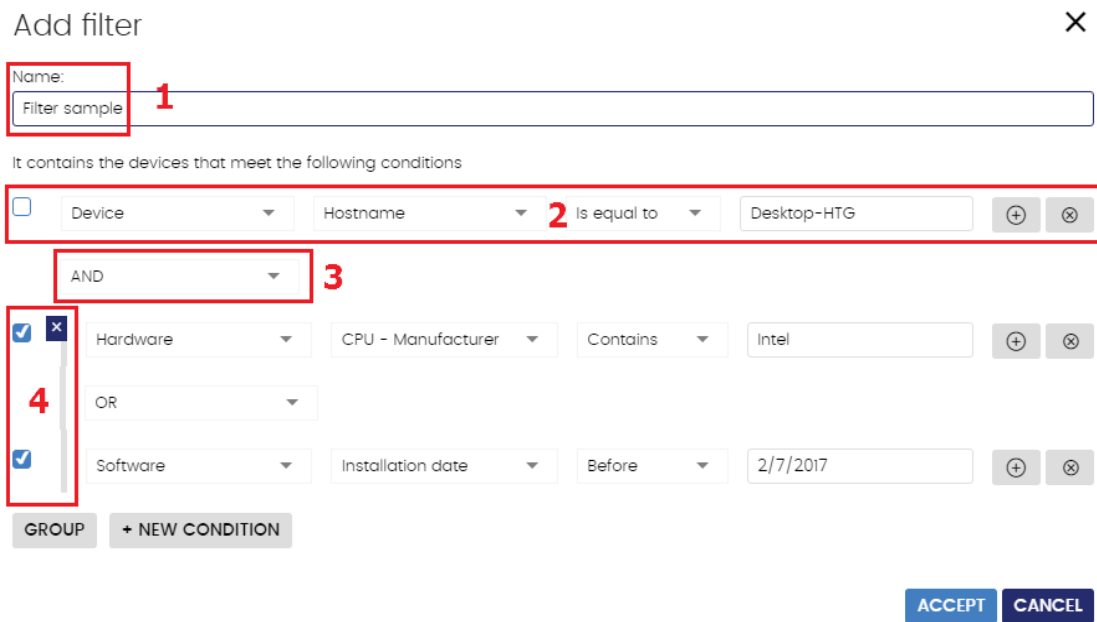


Figure 36: general view of the filter settings

### 7.3.6 Filter rules

A filter rule comprises the items described below:

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

will change to reflect entries such as 'date', etc.



Figure 37: components of a filter rule

To add rules to a filter, click the



icon. To delete them, click



### 7.3.7 Logical operators

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

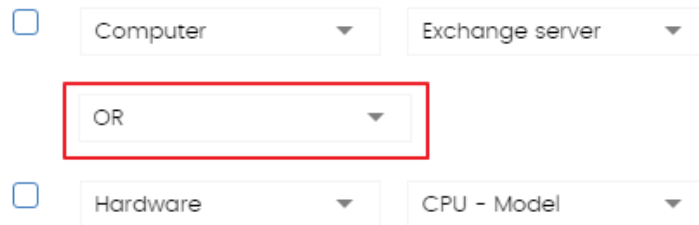


Figure 38: logical operator OR

### 7.3.8 Groups of filter rules

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

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

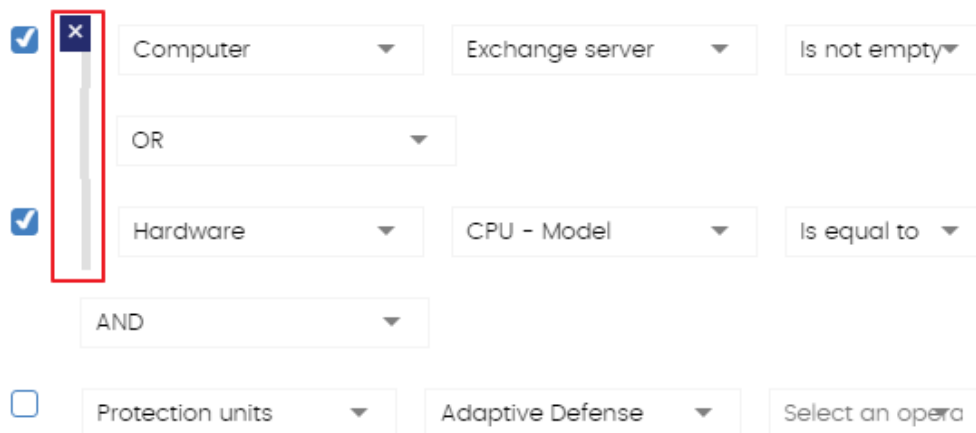


Figure 39: group of filter rules equivalent to (Rule 1 OR Rule 2) AND Rule 3

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

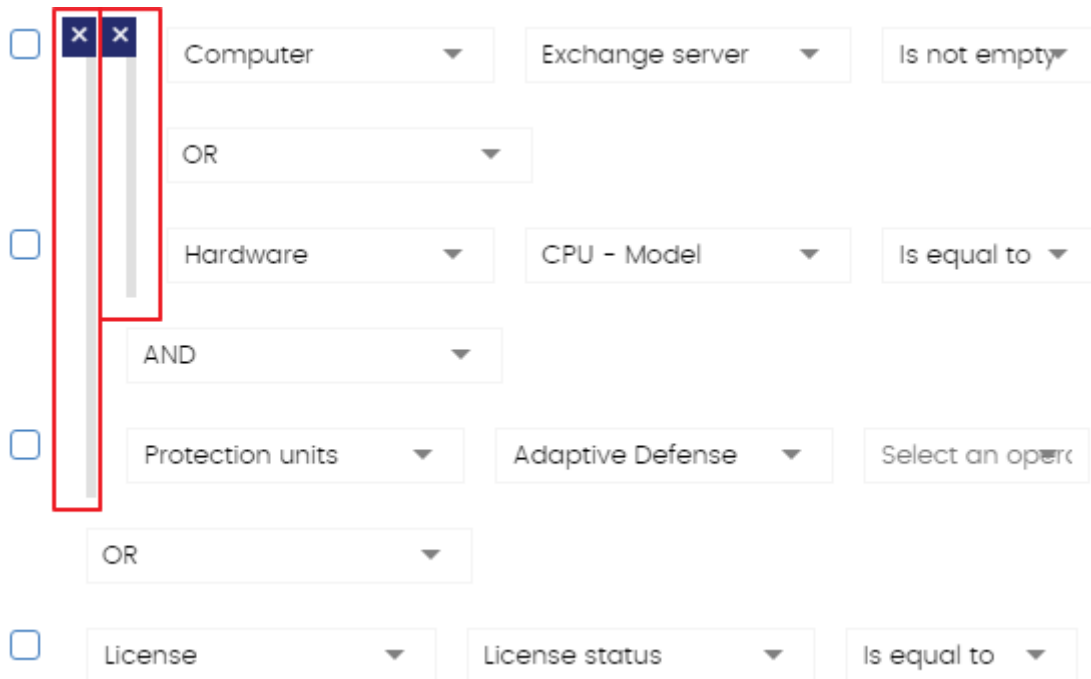


Figure 40: nested group equivalent to ((Rule 1 AND Rule 2) AND Rule 3) OR Rule 4

## 7.4. Groups tree

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

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

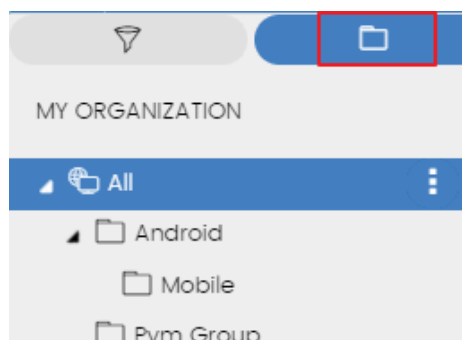


Figure 41: accessing the Groups tree

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






### 7.4.1 What is a group?

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



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

### 7.4.2 Group types

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


### 7.4.3 Groups structure

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



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

### 7.4.4 Active Directory groups

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

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

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

## 7.4.5 Creating and organizing groups

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

### Creating groups

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



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

### Deleting groups

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



*The All root node cannot be deleted*

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

### Moving groups

To move a group, follow the steps below:

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



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

### Renaming groups

To rename a group, follow the steps below:

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



- Enter the new name.




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

### 7.4.6 Moving computers from one group to another

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


#### Moving groups of computers to groups

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

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

#### Moving a single computer to a group

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

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

#### Moving computers from an Active Directory group

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

#### Moving computers to an Active Directory group

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

#### Returning multiple computers to their Active Directory group

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

## 7.5. Computer details

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

The Details window is divided into six sections:

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



Figure 42: general view of the computer details

### 7.5.1 General section (1)

This contains the following information:

- **Name of the computer and icon** indicating the type of computer.
- **IP address**: IP address of the computer.
- **Active Directory path**: full path to the computer in the company's Active Directory.
- **Group**: the folder in the Groups tree to which the computer belongs.

- **Operating system:** full version of the operating system installed on the computer.
- **Computer role:** indicates if the computer has any of the following roles assigned to it: discovery computer, cache or proxy.

## 7.5.2 Computer notifications section (2)

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

### Unprotected computer:

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

### Out-of-date computer:

- **Computer pending restart:** the update for the security engine has been downloaded but the computer needs to be restarted for it to be applied. See Chapter 17 to restart the computer remotely.
- **Protection updates disabled:** the software won't receive any improvements. This will jeopardize the security of the computer in the future. See Chapter 8 to create and assign 'Per-computer settings' that allow the software to be updated.
- **Knowledge updates disabled:** the software won't receive any updates to the signature file. This will jeopardize the security of the computer in the short-term. See Chapters 9 and 10 to create security settings that allow the signature file to be updated.
- **Knowledge update error:** the download of the signature file failed. There is an explanation in this chapter of how to check the free space on your hard disk. See Chapter 17 to restart the computer. See Chapter 6 to reinstall software on the computer.

### Blocked files

The computer contains unknown files that are in the process of classification and cannot be run. See the **Currently blocked programs being classified** panel in the dashboard to check the file and add an exclusion if necessary. See Chapter 15 to manage items that are in the process of classification.

### Offline since...

The computer has not connected to the Panda Security cloud in several days. Check the connectivity of the computer and the firewall settings. See chapter 13 Managing threats,

quarantined items and items being classified to check whether the connectivity requirements are fulfilled. See Chapter 6 to reinstall the software.

### Pending restart

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

### 7.5.3 Details section (3)

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

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



*For more information about the security details of the protected computers, see chapter 12 Malware and network visibility.*

### 7.5.4 Hardware section (4)

This contains the following information:

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

### 7.5.5 Software section (5)

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

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



#### Search tool

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

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

#### Change log

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

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

### 7.5.6 Settings section (6)

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

### 7.5.7 Force synchronization (7)

Sends all pending changes from the computer to the cloud.

### 7.5.8 Context menu

Shows the different actions you can take on the computer:

- **Move to:** moves the computer to a standard group.
- **Move to Active Directory group:** moves the computer to its original Active Directory group.
- **Delete:** frees up the **Adaptive Defense** license and deletes the computer from the Web console.
- **Disinfect:** lets you run a disinfection task immediately. Refer to chapter 15 Remediation tools for more information.
- **Scan now:** lets you run a scan task immediately. Refer to chapter 15 Remediation tools for more information.
- **Schedule scan.** Lets you schedule a scan task. Refer to chapter 15 Remediation tools for more information.
- **Restart:** restarts the computer immediately. Refer to chapter 15 Remediation tools for more information.
- **Report a problem:** opens a support ticket for Panda Security's support department. Refer to chapter 15 Remediation tools for more information.

## 8. Managing settings

---

What are settings?

Overview of assigning settings

Modular vs monolithic settings profiles

Overview of the four types of settings

Per-computer settings

Manual and automatic assigning of settings

Viewing assigned settings

## 8.1. Introduction

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

## 8.2. What are settings?

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

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

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

## 8.3. Overview of assigning settings to computers

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

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

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



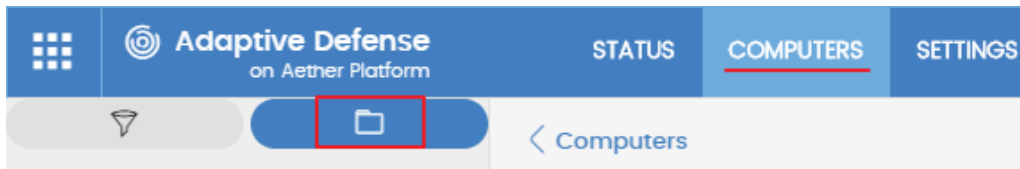


Figure 43: accessing the Groups tree

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



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

### 8.3.1 Immediate deployment of settings

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



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

### 8.3.2 Multi-level trees

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

### 8.3.3 Inheritance

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

### 8.3.4 Manual settings

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

### 8.3.5 Default settings

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

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

- Default settings (Proxy and language)
- Default settings (Per-computer settings)
- Default settings (Security settings for workstations and servers)

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

#### 8.4. Modular vs monolithic settings profiles

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

The three types of profiles are as follows:

- Proxy and language settings
- Per-computer settings
- Security settings for workstations and servers

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

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

##### **Case study: creating settings for several offices**

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

Network of a company formed by several offices:



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

**Monolithic profile**



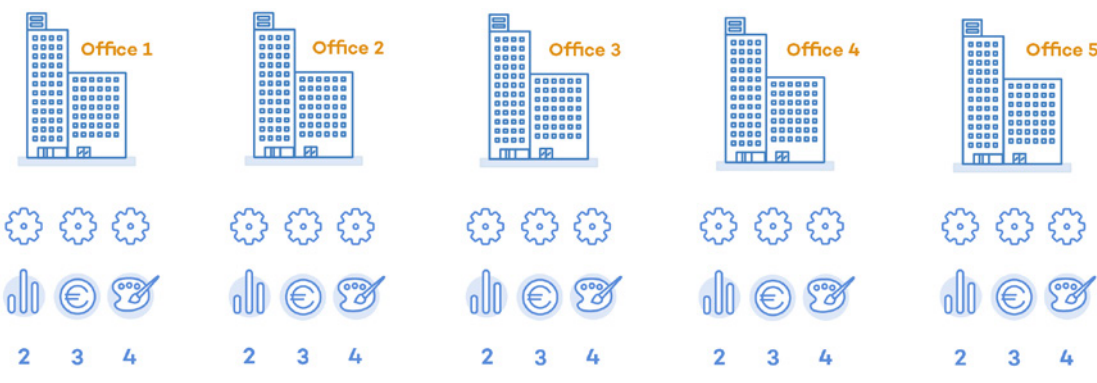
However, as **Adaptive Defense** separates the proxy settings from the security settings, the number of profiles needed is reduced ( $5 \text{ proxy profiles} + 3 \text{ department profiles} = 8$ ) as the security profiles for

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


**Proxy and Language modular profile**



**Security modular profile**



8.5. Overview of the four types of settings

 Refer to chapters 8, 9 and 10 for more information about the Panda agent settings and the protections compatible with each supported platform.

**Proxy and language settings**

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

**Per-computer settings**

Let you define several settings pertaining to the Panda agent:

- Update frequency of the **Adaptive Defense** software installed on computers. Refer to chapter 11 Software updates for more information.

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

## Workstation and server settings

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

### 8.6. Creating and managing settings

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

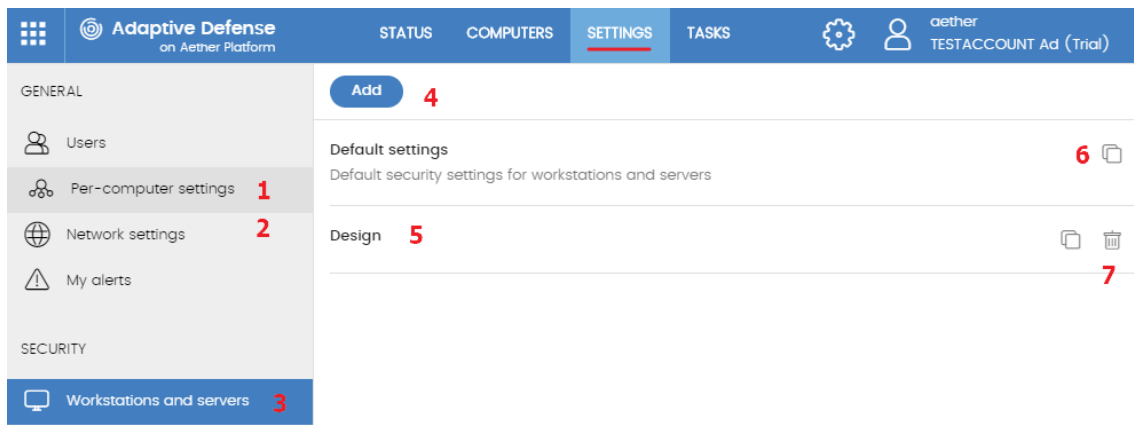


Figure 44: screen for creating and managing settings profiles

#### Creating settings

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

#### Copying and deleting settings

Use the icons **(6)** and **(7)** to copy and delete a settings profile, although if it has been assigned to one or more computers, you won't be able to delete it until it has been freed up. Click the settings profile in order to edit it.



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

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

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

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

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

### 8.7.1 Assigning settings directly/manually

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

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

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



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

#### From the Groups tree

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

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

#### From the computer list panel

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

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

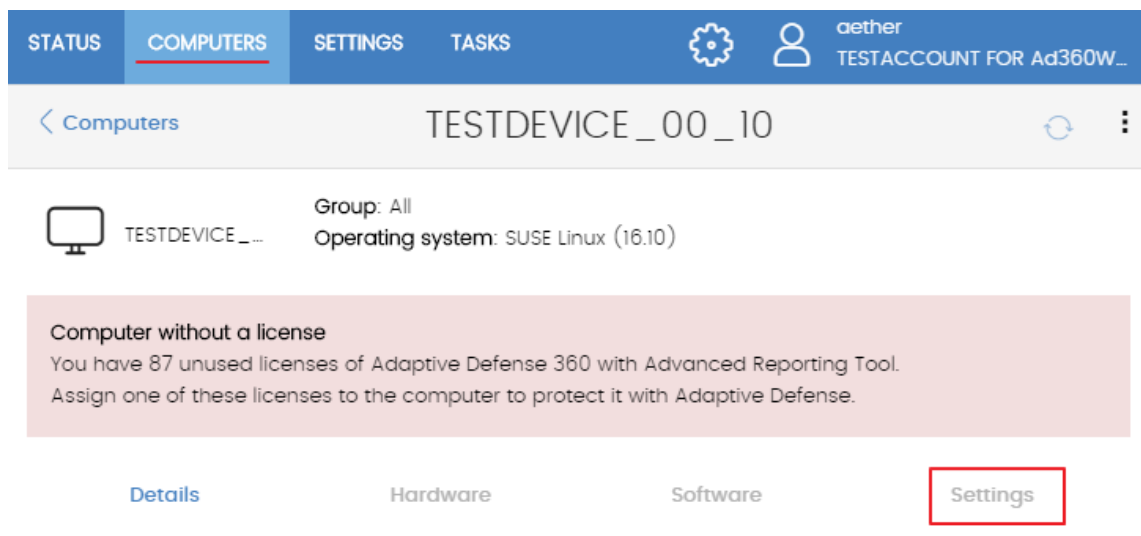



Figure 45: access to settings from the computer details tab.

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

### From the settings profile itself

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

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



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

### 8.7.2 Indirect assigning of settings: the two rules of inheritance

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

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

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

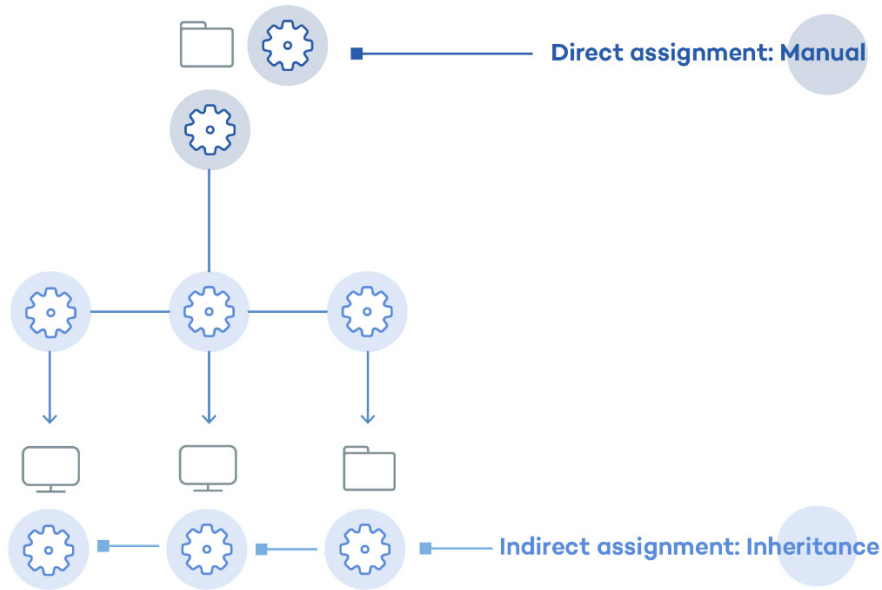


Figure 46: example of inheritance/indirect assigning. The parent group receives the settings that are then pushed out to the child nodes



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

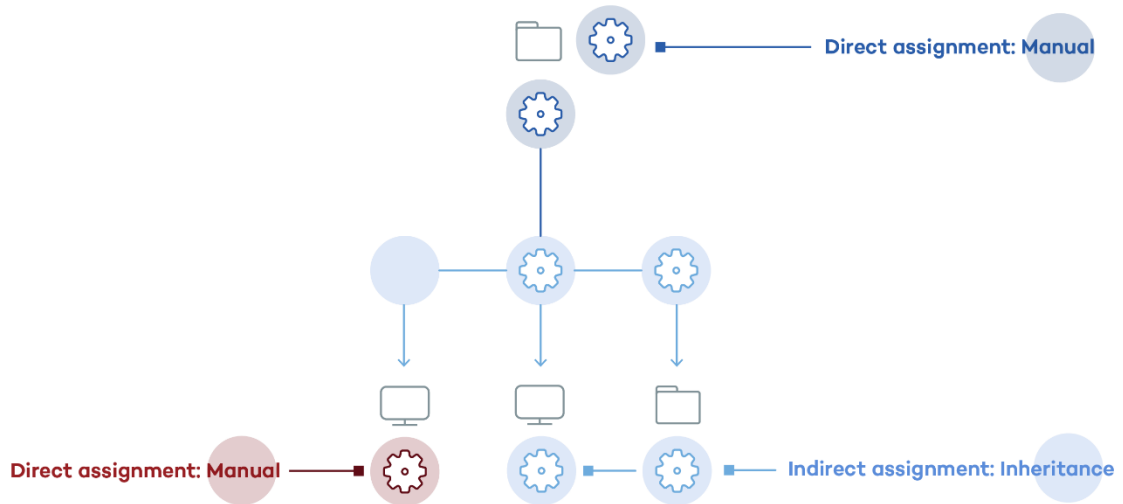


Figure 47: example of the priority of direct assigning over indirect. The inherited settings are overwritten with the manually assigned ones

### 8.7.3 Inheritance limits

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

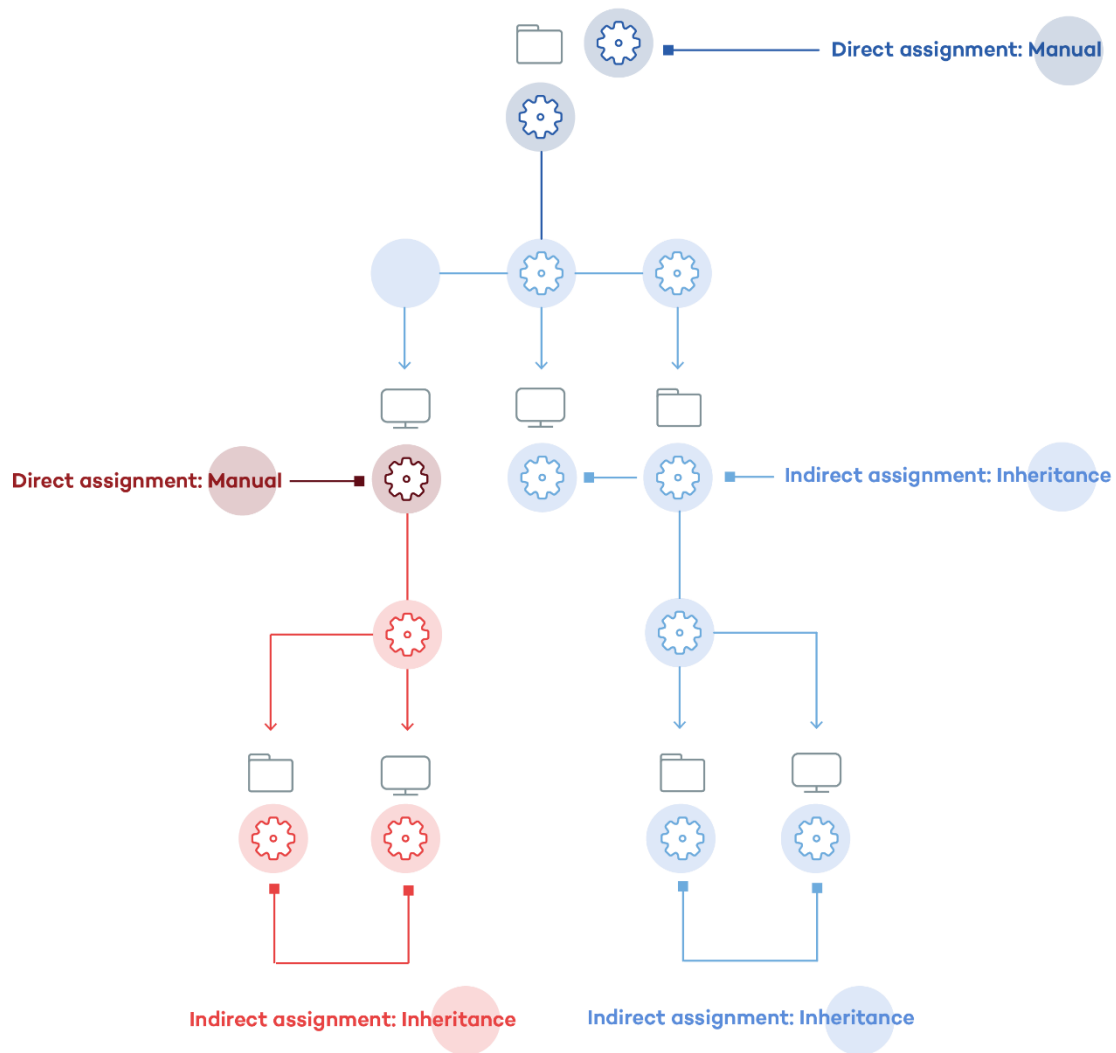


Figure 48: example of inheritance restricted by manual/direct assignment of settings. The parent node settings are passed on to the dependent branches of the tree but stop once manually assigned settings are found

#### 8.7.4 Overwriting settings

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

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

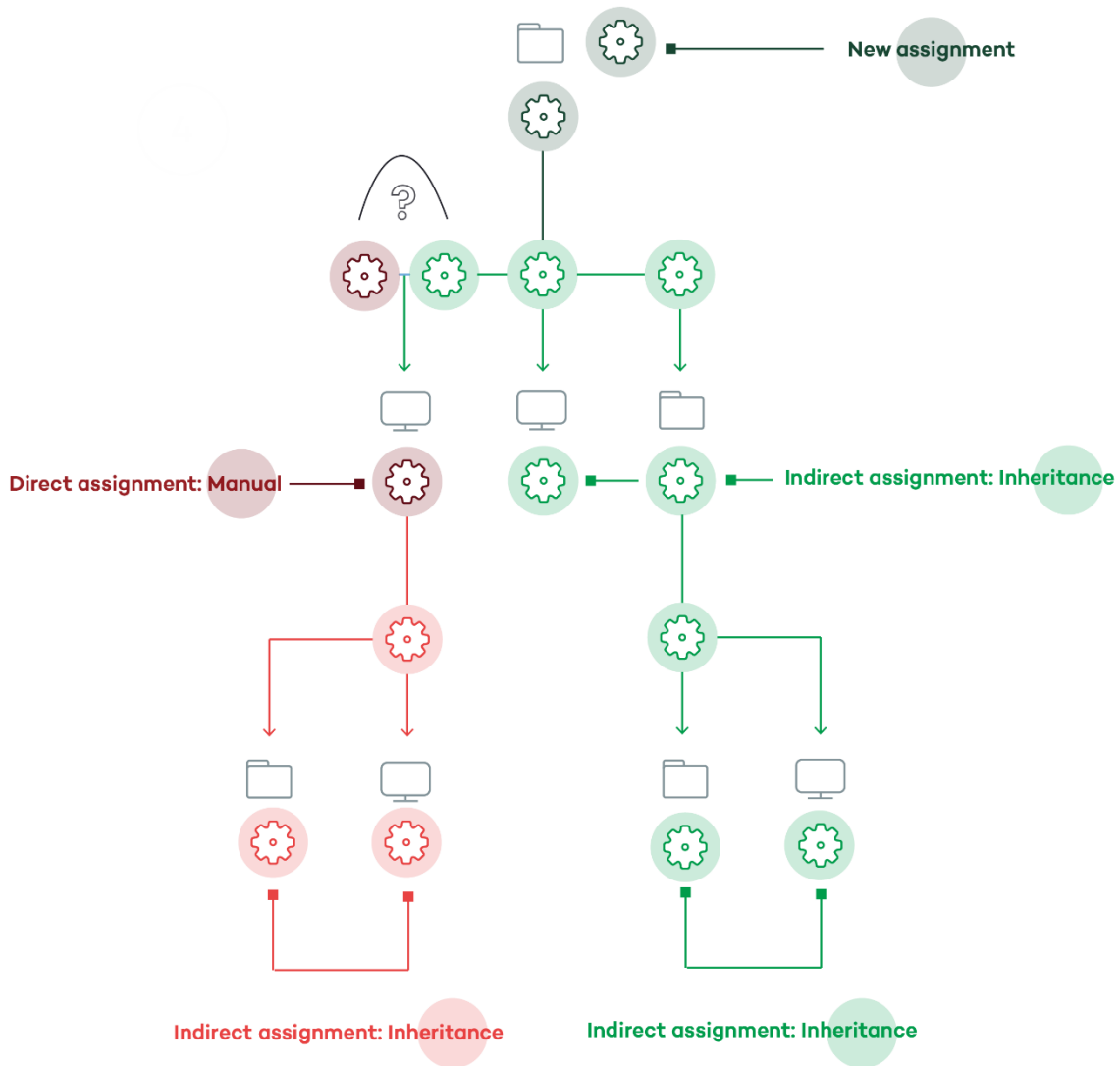


Figure 49: change to the inherited settings in a node that affects the manually applied settings of items lower down

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

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

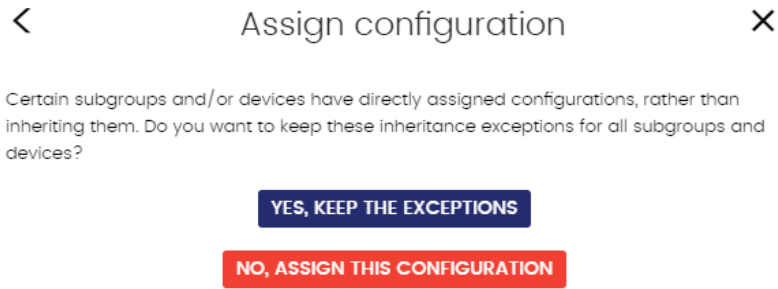


Figure 50: window for selecting the way that settings changes are applied to a branch containing groups configured manually

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

#### Make all inherit these settings



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

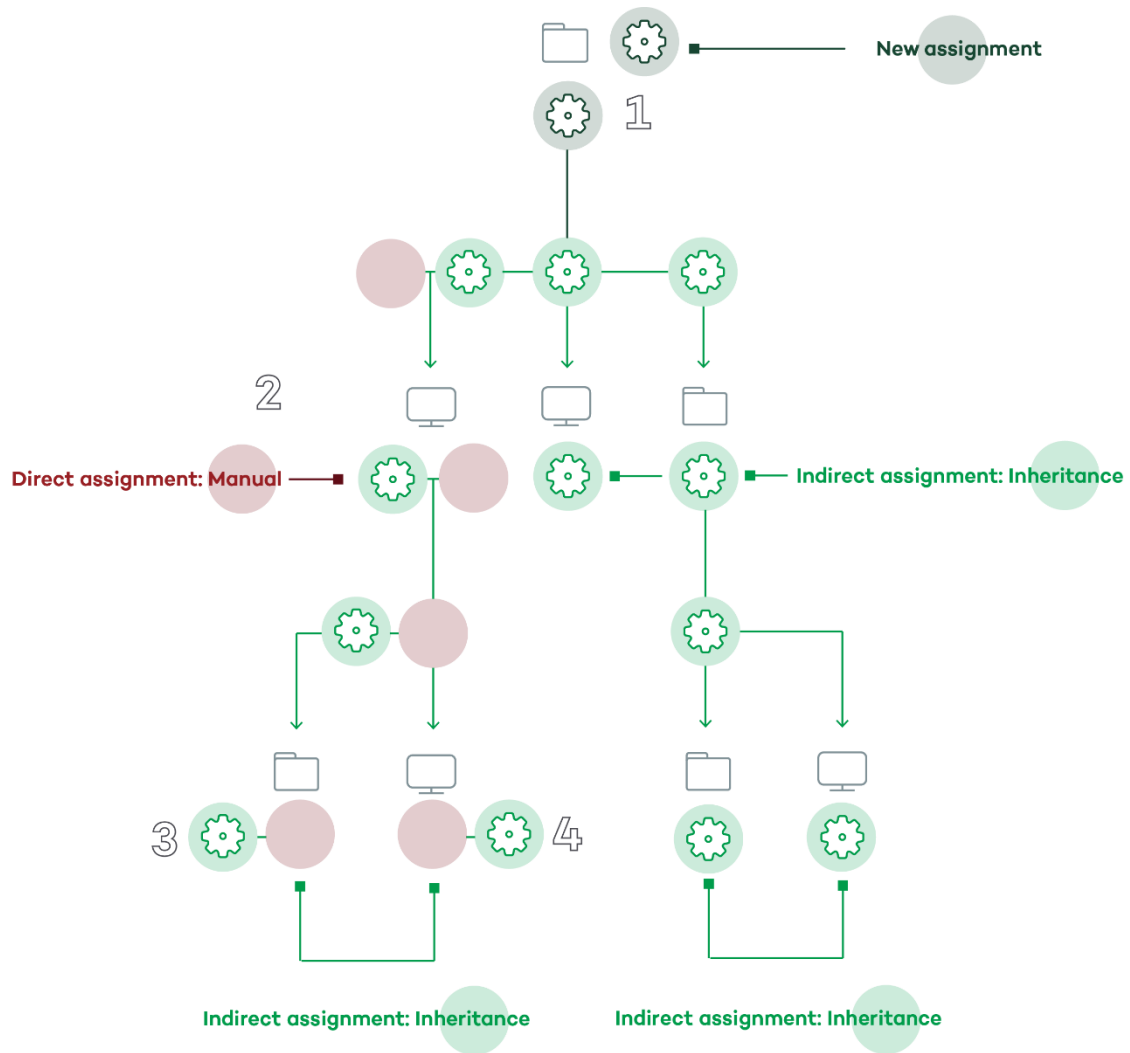



Figure 51: the manual settings are deleted and the settings inherited from the parent node are applied

 *The choice to overwrite the manual settings is only offered once. If there are several manually assigned settings at different levels, all of them will be deleted.*

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

**Keep all settings**

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

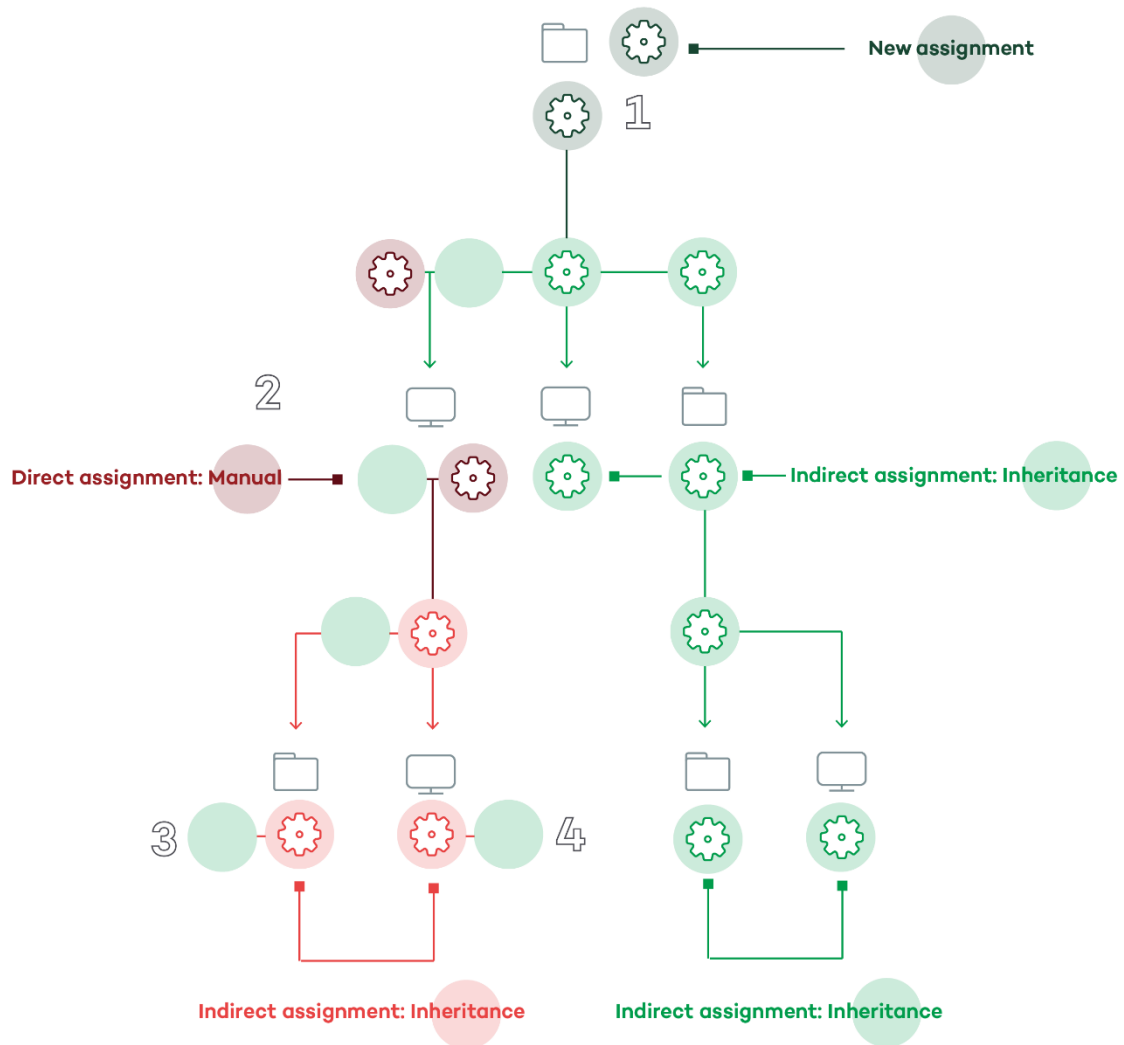


Figure 52: manually applied settings are maintained

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

### 8.7.5 Deleting manually assigned settings and restoring inheritance

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

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

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

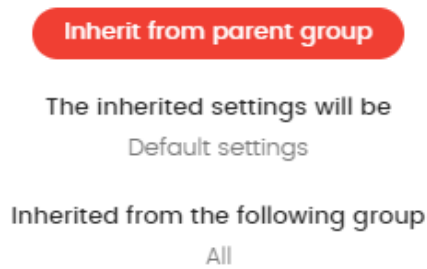


Figure 53: button for deleting manual settings and re-establishing inheritance

### 8.7.6 Moving groups and computers

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

#### Moving individual computers

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

#### Moving groups

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

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

### 8.8. Viewing the assigned settings

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

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

## Groups tree

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

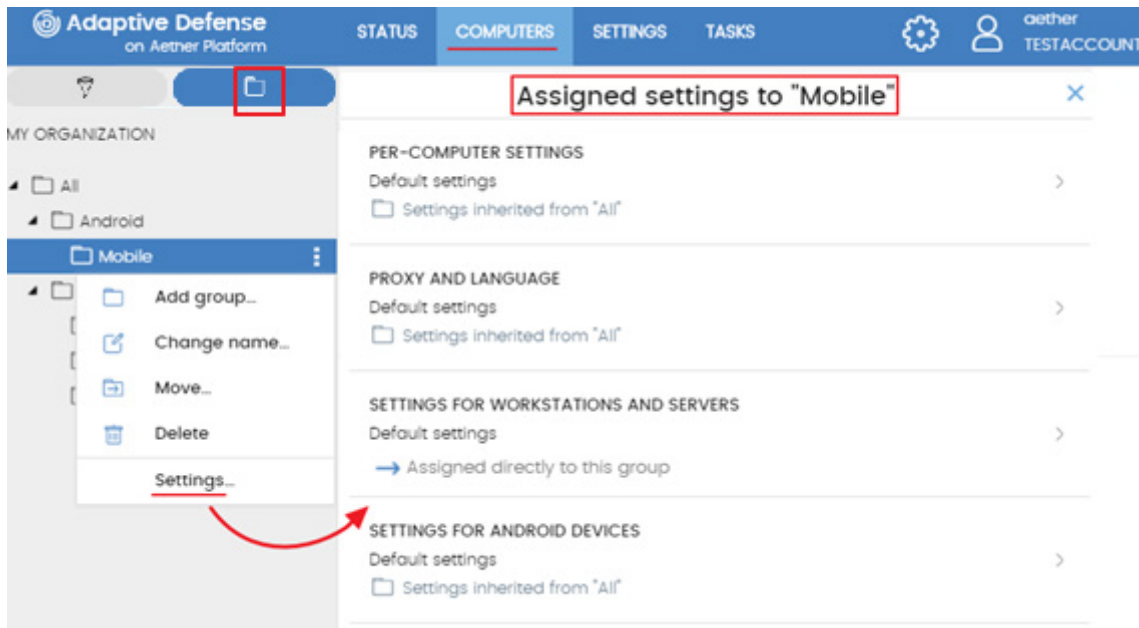


Figure 54: settings assigned from the Groups tree

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

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

## Computer settings tab

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



### Exporting the list of computers

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

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

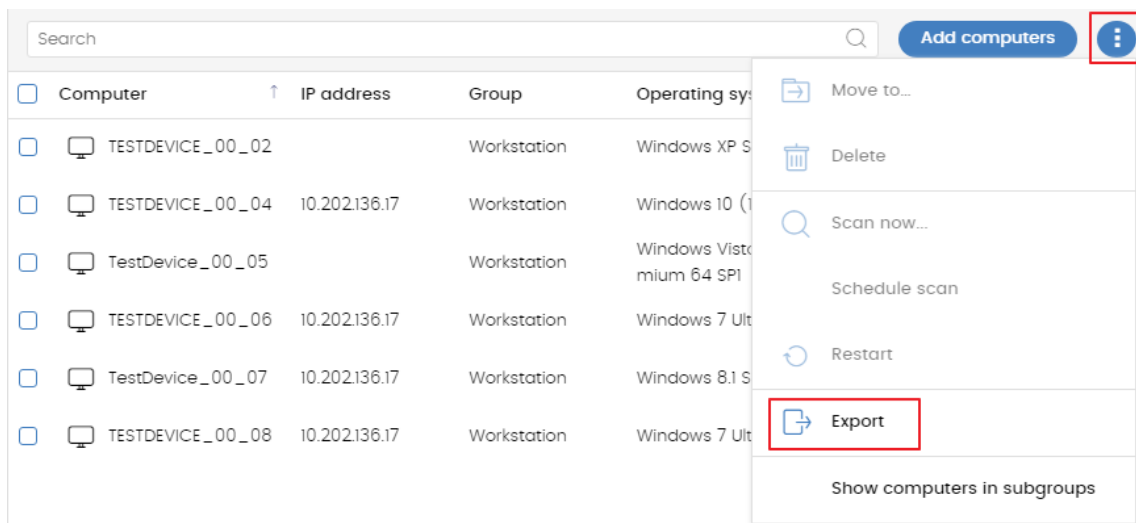


Figure 55: exporting the list of computers in CSV format

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

## 9. Agent and local protection settings

---

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

## 9.1. Introduction

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

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

## 9.2. Configuring the Panda agent role

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

- Proxy
- Discovery computer
- Cache

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

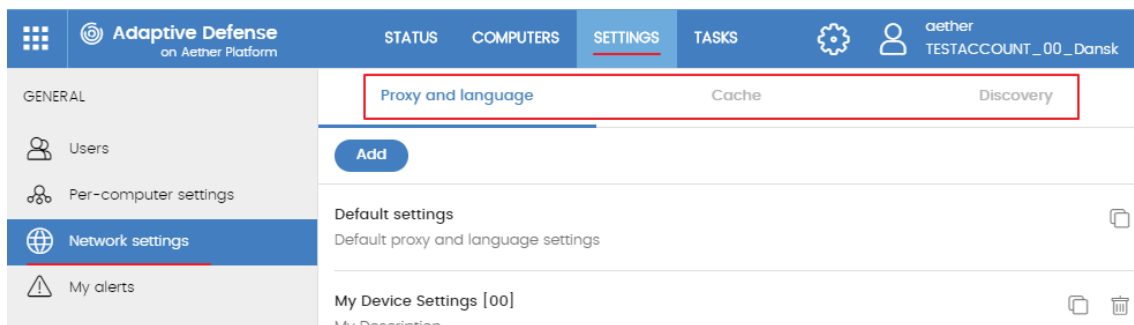


Figure 56: access to the role settings window

### 9.2.1 Proxy role


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

#### Configuring a computer as a proxy server

- Click the **Proxy and language** tab. Select an existing **Proxy and language** settings profile or create a new one.
- Expand the **Proxy** section and select **Adaptive Defense proxy**

- Click **Select computer...**
- In the computer selection window, click **Add proxy server**. A list will be displayed with all managed computers that haven't been designated as proxy server yet.
- Select the computers that will act as a proxy server for all other workstations and servers protected by **Adaptive Defense**

### Revoking the proxy role

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

## 9.2.2 Cache/repository role


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

### Configuring a computer as a cache

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

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

### Revoking the cache role

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

## Requirements and limitations of computers with the cache role

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



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

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

## Discovery of cache nodes

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

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

### 9.2.3 Discovery computer role

The **Discovery** tab is directly related to the installation and deployment of **Adaptive Defense** across the customer's network. Refer to chapter 6 Installing the Adaptive Defense software for more information about the **Adaptive Defense** discovery and installation processes.

## 9.3. Configuring Internet access via a proxy server

### Configuring proxy usage

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

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

- **Panda Adaptive Defense proxy:** access via the **Adaptive Defense** agent installed on a computer on the network.
  
- **Do not use proxy**

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

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

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

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



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

### Fallback mechanism

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

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

- WPAD (Web Proxy Auto-discovery Protocol): a request is sent to the network via DNS or DHCP to get the URL that points to the PAC settings file.

## 9.4. Configuring real-time communication

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

### Disabling real-time communication

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

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

## 9.5. Configuring the agent language

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

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

- Russian
- Japanese
- Finnish



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

## 9.6. Configuring the Anti-Tamper protection and password

### 9.6.1 Anti-Tamper protection

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

#### Enabling the Anti-Tamper protection

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

### 9.6.2 Password-protection of the agent

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

#### Setting up the password

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



# 10. Security settings for workstations and servers

---

Introduction to the security settings for workstations and servers

General settings

Advanced Protection

## 10.1. Introduction

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

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

## 10.2. Introduction to the security settings for workstations and servers

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

- **General:** lets you configure the updates, the removal of competitor products, and file exclusions from scans.
- **Advanced protection (Windows devices):** lets you configure the behavior of the advanced protection and the anti-exploit protection against APTs, targeted attacks, and advanced malware capable of leveraging known and zero-day exploits.

## 10.3. General settings

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

### 10.3.1 Updates

Refer to chapter 11 Software updates for more information about how to update the agent, the protection, and the software signature file installed on users' computers.

### 10.3.2 Uninstall other security products

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

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

### 10.3.3 Exclusions



*These settings affect both the disinfection tasks and the advanced protection.*

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

#### Disk files

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

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

#### Exclude the following email attachments:

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

## 10.4. Advanced protection

### 10.4.1 Behavior

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

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

## 10.4.2 Anti-exploit

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

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

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

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

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

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

- **Automatic exploit blocking**

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

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

- **Exploit detection**

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

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

**Adaptive Defense** can end a compromised process automatically to minimize the negative effects of an attack, or ask the user for permission to do so in order to remove it from memory. This will allow

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

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

### Anti-exploit protection settings

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



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

### 10.4.3 Privacy

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

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

### 10.4.4 Network usage

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

# 11. Software updates

---

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

## 11.1. Introduction

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

The components installed on users' computers are the following:

- Panda Platform communications agent
- **Adaptive Defense** protection engine
- Signature file

## 11.2. Configuring protection engine updates

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

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



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

### Running updates at specific time intervals

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

- Start time
- End time

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

### Running updates on specific days

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

- **Any day**: the updates will run when they are available.
- **Days of the week**: use the checkboxes to select the days of the week when the **Adaptive Defense** updates will run. If an update is available, it will run on the first day of the week that coincides with the administrator's selection.



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

## Computer restart

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

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

### 11.3. Configuring communications agent updates

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

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

### 11.4. Configuring knowledge updates

To configure **Adaptive Defense's** signature file updates, access the security settings for workstations and servers. This can be accessed by clicking the **Settings** menu at the top of the console, and choosing **Workstations and servers** from the left-hand side menu.

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

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



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

# 12. Malware and network visibility

---

Overview of the Status menu  
Available panels/widgets  
Introduction to the lists  
Available lists  
Default lists

## 12.1. Introduction

**Adaptive Defense** offers administrators three large groups of tools for viewing the security status and the networks they manage:

- The dashboard, with real-time, up-to-date information
- Custom lists showing incidents, detected malware and managed devices along with their status
- Networks status reports with information collected and consolidated over time

Visualization and monitoring tools determine in real time the network security status as well as the impact of any possible security breaches in order to facilitate the implementation of appropriate security measures.

## 12.2. Overview of the Status menu

The **Status** menu includes the main visualization tools and has several sections, which you can see below:

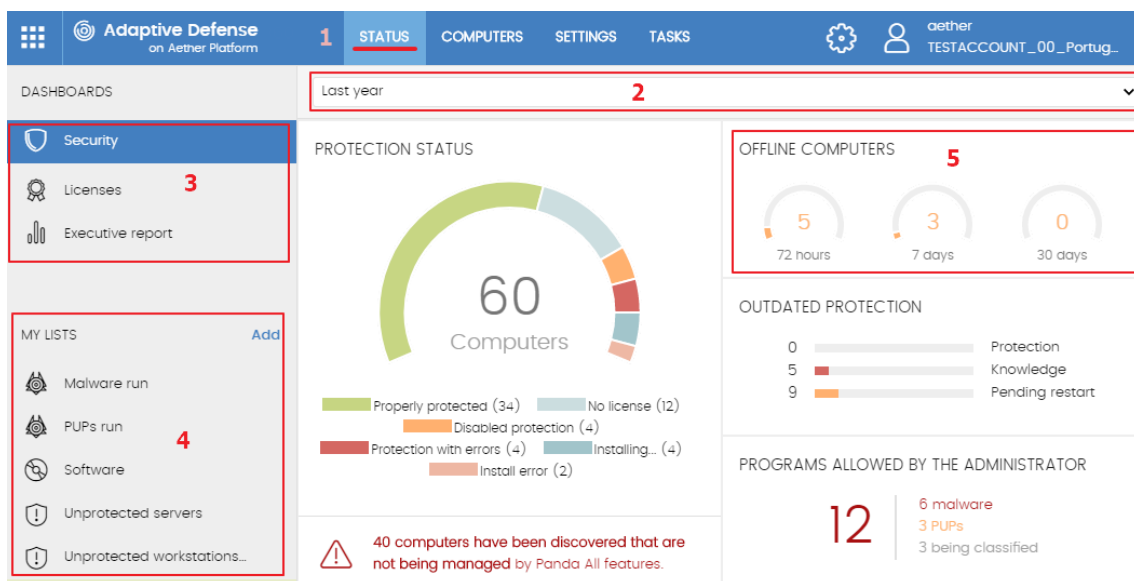


Figure 57: the Status window with the dashboard and access to the lists

### Accessing the dashboard (1)

You can access the dashboard through the **Status** menu at the top of the screen. From the dashboard you can access different widgets, as well as the lists.

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

### Time period selector (2)

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

- Last 24 h
- Last 7 days
- Last month
- Last year



*Not all information panels offer information for the last year. Those that don't support this option have a notice at the top of the screen to this effect.*

### Dashboard selector (3)

- **Security**: security status of the IT network.
- **Web access and spam**: blocking and filtering of Internet contents and unsolicited email on Microsoft Exchange servers.
- **Licenses**: refer to chapter 5 for more information about license management.
- **Executive report**: refer to chapter 17 for more information about how to configure and generate reports.

This chapter deals with the resources provided in sections **Security** and **Web and spam access**.

### My lists (4)

The lists are data tables with the information presented in the panels. This includes highly detailed information and has search tools to locate the information you need.

### Information panels/widgets (5)

The dashboard has a series of widgets related to a specific aspect of network security.

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

All the graphs have a key explaining the meaning of the data, and have hotspots that can be selected to display lists with predefined filters.

## PROTECTION STATUS

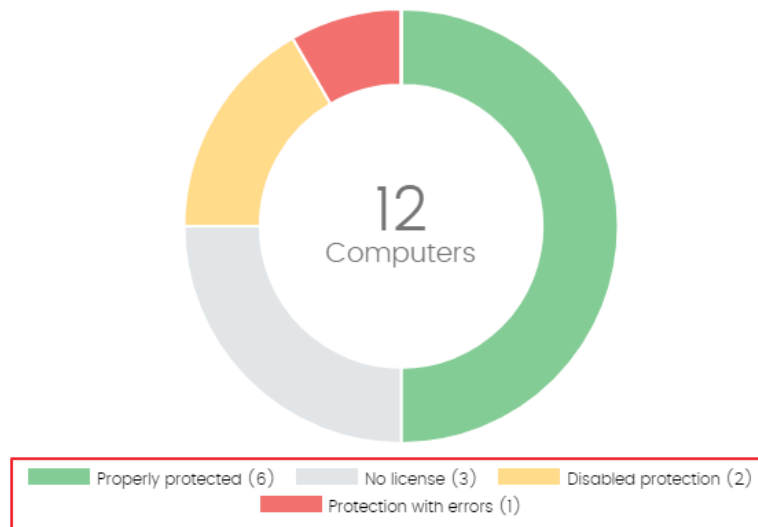


Figure 58: tooltips with detailed information and keys about the data shown

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

- Pie charts
- Histograms

Click the items in the graphs to display more detailed lists.

### 12.3. Available panels/widgets

Below is a description of the different widgets displayed in the **Adaptive Defense** dashboard, their areas and hotspots, as well as their tooltips and their meaning.

#### 12.3.1 Protection status

**Protection status** shows those computers where **Adaptive Defense** is working properly and those where there have been errors or problems installing or running the protection module. The status of the network computers is represented with a circle with different colors and associated counters.

The panel offers a graphical representation and percentage of those computers with the same status.

## PROTECTION STATUS



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

Figure 59: 'Protection status' panel



The sum of all computers can be more than 100% as the status types are not mutually exclusive.

- **Meaning of the different status types**

- **Properly protected:** indicates the percentage of computers where **Adaptive Defense** installed without errors and is working properly.
- **Installing:** this indicates the percentage of computers on which **Adaptive Defense** is currently being installed.
- **No license:** computers without a license are those that are not protected because there are insufficient licenses or because an available license has not been assigned to the computer.
- **Disabled protection:** these are computers that don't have the antivirus or the advanced protection enabled, if the latter is available for the operating system on that particular computer.
- **Protection with errors:** this includes computers with **Adaptive Defense** installed, but for one reason or another the protection module is not responding to the requests from the Panda Security server.
- **Install error:** this indicates the computers on which the installation of the protection has not been properly completed.
- **Center:** the center of the pie chart indicates the total percentage of unprotected computers out of all of those visible to **Adaptive Defense**. For a computer to be visible it must have the **Panda agent** installed.

- Lists accessible from the panel

PROTECTION STATUS



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

Figure 60: hotspots in the 'Protection status' panel

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

- (1) Computer protection status list filtered by Protection status = Properly protected
- (2) Computer protection status list filtered by Protection status = Protection with errors
- (3) Computer protection status list filtered by Protection status = Installing
- (4) Computer protection status list filtered by Protection status = Disabled protection
- (5) Computer protection status list filtered by Protection status = No license
- (6) Computer protection status list filtered by Protection status = Install error
- (7) Computer protection status list without any filters

### 12.3.2 Offline computers

OFFLINE COMPUTERS



Figure 61: offline computers panel

**Offline computers** displays the computers that have not connected to the Panda Security cloud for a certain amount of time. Such computers are susceptible to security problems and require special attention from the administrator.

- **Meaning of the pie charts displayed**
  - **72 hours:** number of computers that have not reported their status in the last 72 hours.
  - **7 days:** number of computers that have not reported their status in the last 7 days.
  - **30 days:** number of computers that have not reported their status in the last 30 days.
  
- **Lists accessible from the panel**

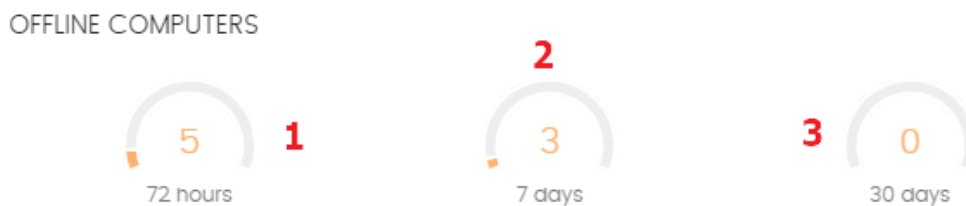


Figure 62: hotspots in the Offline computers panel

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

- (1) **Offline computers** list filtered by **Last connection** = More than 72 hours ago
- (2) **Offline computers** list filtered by **Last connection** = More than 7 days ago
- (3) **Offline computers** list filtered by **Last connection** = More than 30 days ago

### 12.3.3 Outdated protection

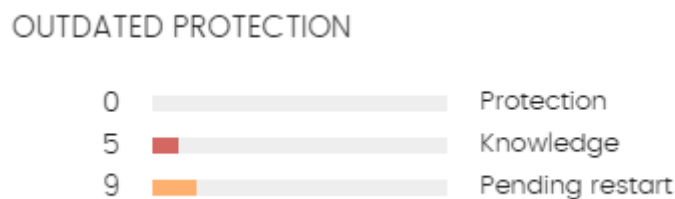


Figure 63: outdated protection panel

**Outdated protection** displays the computers on which the latest version of the signature file is more than three days older than the latest one released by Panda Security. It also displays the computers on which the latest version of the antivirus engine is more than seven days older than the latest one released by Panda Security. Such computers are therefore vulnerable to attacks from threats.



- **Meaning of the bars**

The panel shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts:

- **Protection:** for at least seven days the computer has had a version of the antivirus engine older than the latest one released by Panda Security.
- **Knowledge:** it has been at least three days since the computer has updated the signature file.
- **Pending restart:** the computer requires a restart to complete the update.

- **Lists accessible from the panel**

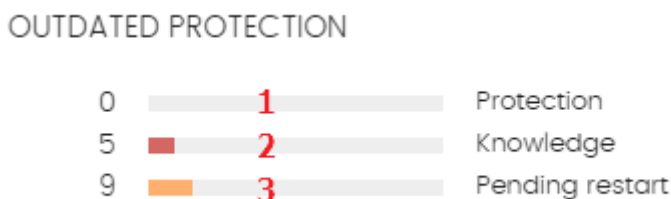


Figure 64: hotspots in the Outdated protection panel

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

- (1) **Computer protection status** list filtered by **Updated protection** = No
- (2) **Computer protection status** list filtered by **Knowledge** = No
- (3) **Computer protection status** list filtered by **Updated protection** = Pending restart

### 12.3.4 Currently blocked programs being classified

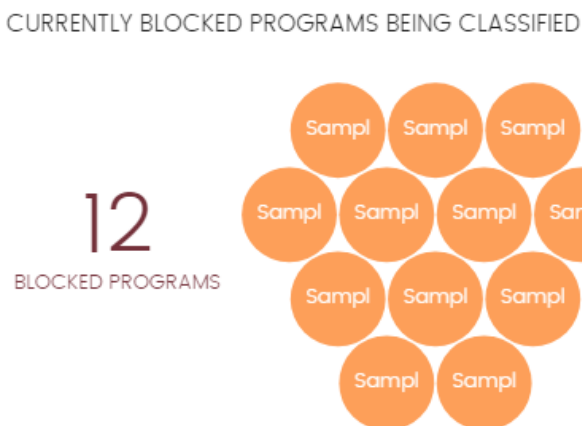


Figure 65: currently blocked programs being classified panel

The information displayed in **Currently blocked programs being classified** is a history of blocked items that have not yet been classified. It covers from the start-up of the service to the current moment, and is not affected by the administrator selecting the time period.

In the example panel, there are 12 blocked items in classification. These are 12 applications that have been blocked and are being investigated. Each one is represented by a circle.

The total number of blocked items in classification represents the different applications (different MD5s) that are being blocked. This number is regardless of the number of attempts to run the blocked application on each computer in the network.

Each version of the program (different MD5) is shown independently.

The size of the circles reflects the number of computers where the blocked unknown program was detected. In this way, a process that is run on many computers will have a single large circle allocated, compared to a process that has only been run on a single computer, which will be represented with a smaller circle.

- **Meaning of the colors used in the panel**

In the panel, blocked applications are displayed with the color code indicated below:

- **Orange:** programs with average chances of being malware.
- **Dark orange:** programs with high chances of being malware.
- **Red:** programs with very high chances of being malware.

When you hover the mouse pointer over the circle, each circle expands to show the complete name and a series of icons representing key actions:



*Figure 66: graphical representation of a program in the process of classification*

- **Folder:** the program has read data from the user's hard disk.
- **Globe:** the program has connected to another computer.

- Lists accessible from the panel

CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED

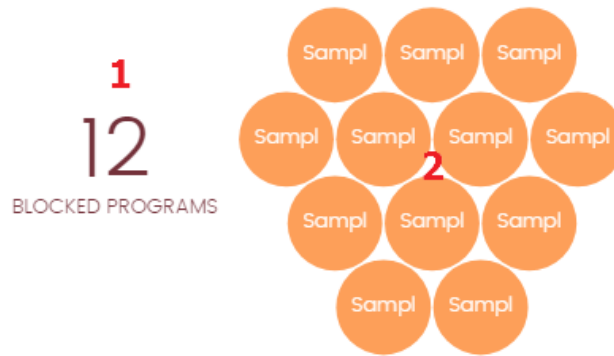


Figure 67: hotspots in the 'Currently blocked programs being classified' panel

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

- (1) Currently blocked programs being classified list with no filters
- (2) Currently blocked programs being classified list filtered by Search = File hash

### 12.3.5 Threats allowed by the administrator

THREATS ALLOWED BY THE ADMINISTRATOR

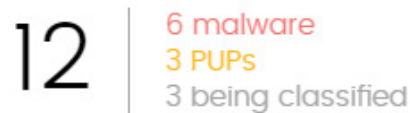


Figure 68: threats allowed by the administrator panel

**Adaptive Defense** blocks all programs classified as malware and, in addition, depending on the advanced protection settings, it can also block unknown programs until they are analyzed and given a security rating.

If a user cannot wait for this classification to be issued, or the administrator wants to allow the running of an item already classified as a threat, **Adaptive Defense** has tools to avoid such items from being blocked.



*Adaptive Defense allows the execution of all libraries and binaries used by the programs allowed by the administrator, except for those that are known threats.*

- **Meaning of the information displayed in the panel**

The panel represents the total number of items excluded from blocking, broken down into three types:

- Malware
- PUP
- Being classified

- **Lists accessible from the panel**

### THREATS ALLOWED BY THE ADMINISTRATOR



Figure 69: hotspots in the 'Threats allowed by the administrator' panel

- (1) Threats allowed by the administrator list with no filters
- (2) Threats allowed by the administrator list filtered by **Current classification** = Malware
- (3) Threats allowed by the administrator list filtered by **Current classification** = PUP
- (4) Threats allowed by the administrator list filtered by **Current classification** = Being classified (blocked and suspicious items)

### 12.3.6 Malware/PUP activity

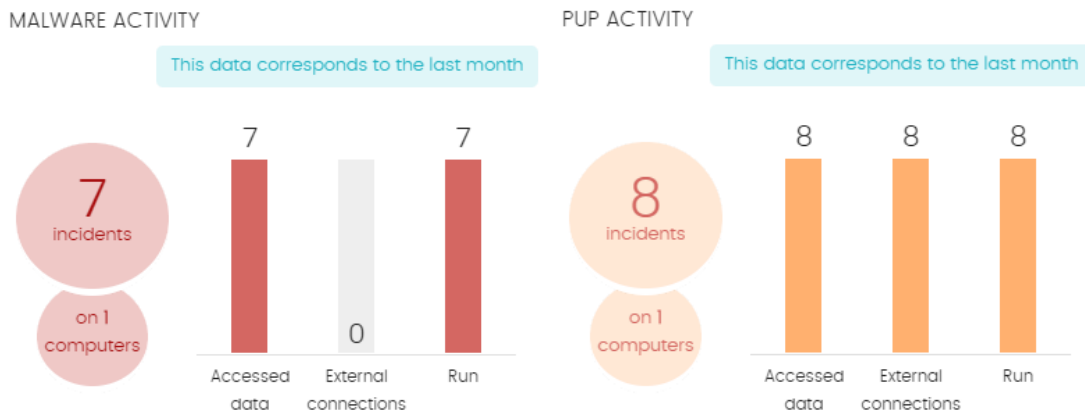



Figure 70: malware/PUP activity panel

Malware/PUP activity shows the incidents detected in the file system of the Windows computers on the network. **Adaptive Defense** generates an incident in the PUP/Malware Activity panel for each computer-threat-different type of threat triplet encountered on the network. If the original cause of the warning is not resolved, a maximum of two incidents will be generated every 24 hours for each computer-threat detected that requires attention.

- **Meaning of the information displayed in the panel**
- **Number of incidents/alerts & number of computers where they are detected**
- **Accessed data:** number of alerts that include one or more attempts to access user information on the computer's hard disk.
- **External connections:** number of alerts regarding connections to other computers.
- **Run:** number of malware samples run.



The Malware activity, PUP activity, and Exploit activity panels show data over a maximum period of one month. Should the administrator set a greater time period, an explanatory text will be displayed above the list.

- **Lists accessible from the panel**

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

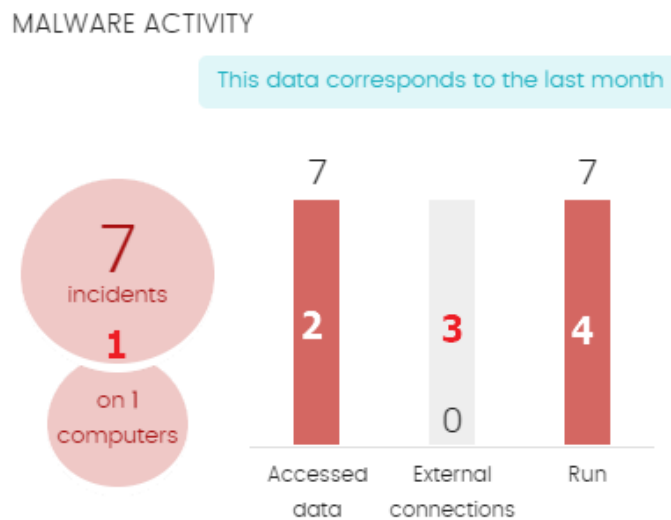


Figure 71: hotspots in the 'Malware/PUP activity' panel

- (1) **Malware activity** list filtered by **Threat type** = (Malware OR PUP)
- (2) **Malware activity** list filtered by **Accessed data** = True
- (3) **Malware activity** list filtered by **External connections** = True
- (4) **Malware activity** list filtered by **Run** = True

### 12.3.7 Exploit activity

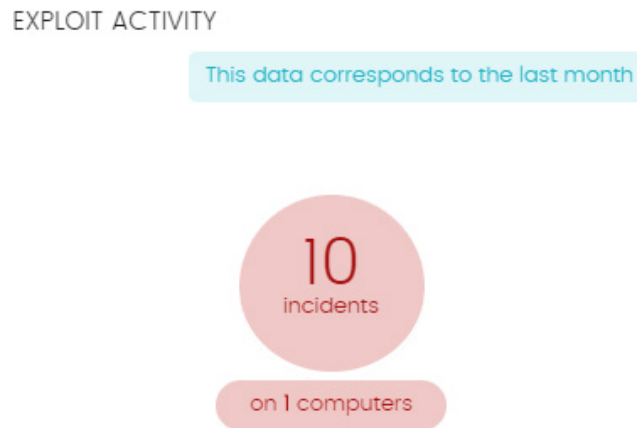


Figure 72: exploit activity panel

The Exploit activity panel shows the number of vulnerability exploit attacks suffered by the Windows computers on the network. **Adaptive Defense** reports an incident in the Exploit activity panel for each computer/different exploit attack pair found on the network. If an attack is repeated, a maximum of 10 incidents will be reported every 24 hours for each computer-exploit pair found.

- **Meaning of the information displayed in the panel**
- **Number of incidents/attacks & number of computers where they are detected**
  
- **Lists accessible from the panel**

Regardless of where you click in the panel, the list displayed will show a list of all the exploits detected across the network with no filters.

### 12.3.8 Classification of all programs run and scanned

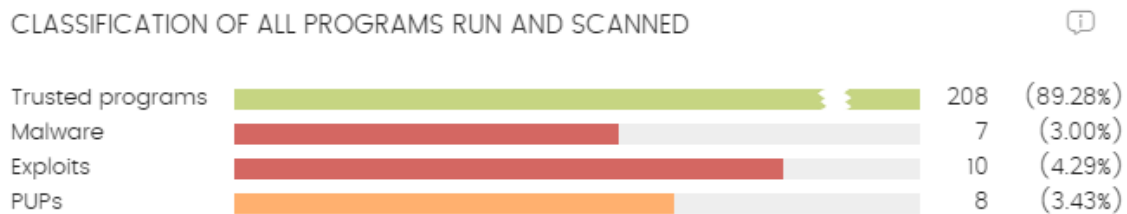


Figure 73: 'Classification of all programs run and scanned' panel

The purpose of this panel is to quickly display the percentage of goodware and malware items seen and classified on the customer's network during the time period selected by the administrator.

- **Meaning of the bars used in the panel**

The panel displays four horizontal bars, along with the number of events associated with each category and a percentage over the total number of events.



*The data in this panel corresponds to the entire IT network, not only to those computers that the administrator has permissions on based on the credentials used to log in to the console. Unclassified items are not shown in the panel.*

- **Trusted programs:** applications seen on the customer's network which have been scanned and classified as goodware.
- **Malicious programs:** programs that attempted to run or were scanned in the selected period, and were classified by **Adaptive Defense** as malware or a targeted attack.
- **Exploits:** number of attempts to exploit the applications installed across the network.
- **PUPs:** programs that attempted to run or were scanned in the selected period, and were classified by **Adaptive Defense** as a PUP (Potentially Unwanted Program).

- **Lists accessible from the panel**

#### CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED



Figure 74: hotspots in the 'Classification of all programs run and scanned' panel

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

Click the **Malicious programs**, **Exploits** and **PUPs** bars to display the following information:

- (1) **malware activity** list with no preconfigured filters
- (2) **exploit activity** list with no preconfigured filters
- (3) **PUP activity** list with no preconfigured filters

## 12.4. Introduction to the lists

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

### 12.4.1 Templates, settings and views

The **Adaptive Defense** lists are, in effect, *templates*, that allow one or more *settings*. A list can be thought of as the source of data about a specific area.

*Settings* are values specifically assigned to the search tools and filters associated to each template.

The *settings* of a *template* result in a list which the administrator can edit and consult later. This way, administrators can save time defining searches and filters about *Lists* which they can use again later.

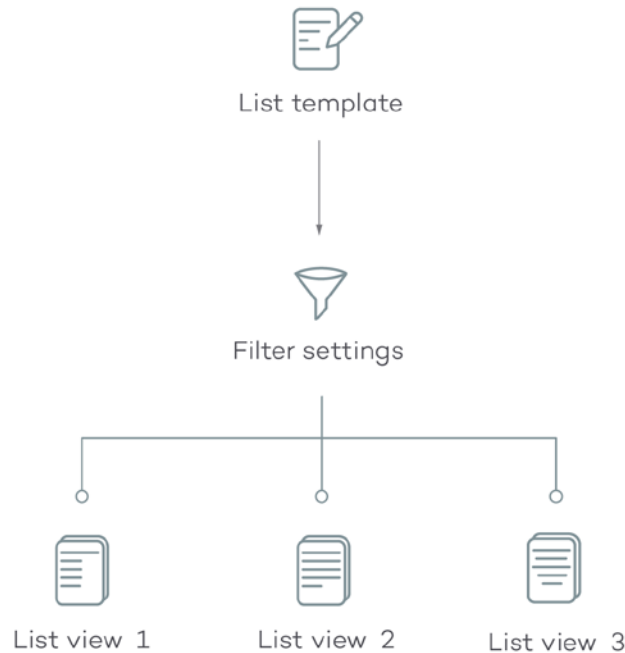


Figure 75: generating three lists from the same template/data source

#### List templates

There are six templates that correspond to the types of information displayed below:

- Malware and PUP activity
- Exploit activity
- Currently blocked programs in the process of classification
- Computer protection status
- Licenses
- Unmanaged computers discovered

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



### Settings

In the context of lists, the settings represent a data filter specified by the administrator and associated to a template. Each template has different filters according to the type of data displayed.

Administrators can establish as many filter settings for a template as they wish, in order to enable different views of the same source of data.

### Views of lists

The combination of a *template* and *settings* results in a specific view of the list. A template can have several associated views if the administrator has created various settings for the same template.

The screenshot shows the 'Copy of Malware run' settings panel. At the top, there is a title 'Copy of Malware run' (1) and a 'Save' button (5). Below the title is a text input field 'Enter a description...' (2). A 'Computer' dropdown menu and a search bar are visible (3). A 'Filters' button (3) and a menu icon (6) are also present. The settings section (4) includes dropdowns for 'Type' (Malware), 'Run' (True), 'Search date type' (Range), and 'Range' (Last month). An 'Action' list with checkboxes for 'Quarantined', 'Blocked', 'Disinfected', 'Deleted', and 'Allowed' is shown. 'Accessed data' and 'External connections' dropdowns are set to '- All -'. A 'Filter' button (7) is at the bottom right. Below the settings is a table (8) with columns: Computer, Threat, Path, Status icons, Action, and Date.

Computer	Threat	Path				Action	Date
Machine_Cu stomer_1_01 4a	Malware Nam e 14	Malware Path Sample 14	●	●	○	Blocked	4/24/2017 2:1 8:00 AM
Machine_Cu stomer_1_01 4a	Malware Nam e 12	Malware Path Sample 12	●	●	○	Blocked	4/24/2017 1:2 0:00 AM
Machine_Cu stomer_1_01 4a	Malware Nam e 10	Malware Path Sample 10	●	●	○	Deleted	4/24/2017 12: 22:00 AM

Figure 76: overview of a list

### 12.4.2 My lists panel

All created lists are displayed on the left-hand side panel **My lists**, on the **Status** main screen.

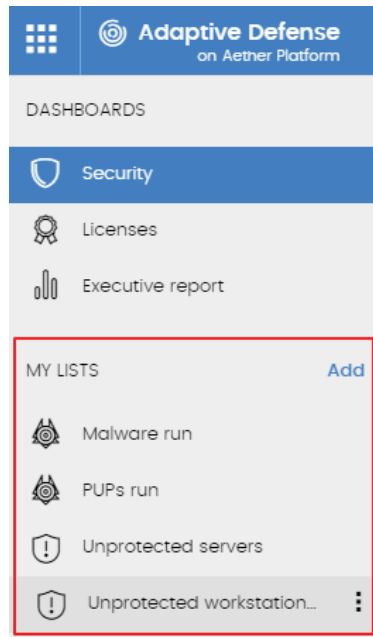


Figure 77: 'My lists' side panel

### 12.4.3 Creating custom lists

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

- From the My lists side menu

Click **Add** in the panel on the left to display a window with a drop-down menu with the eleven available templates (Figure 78).

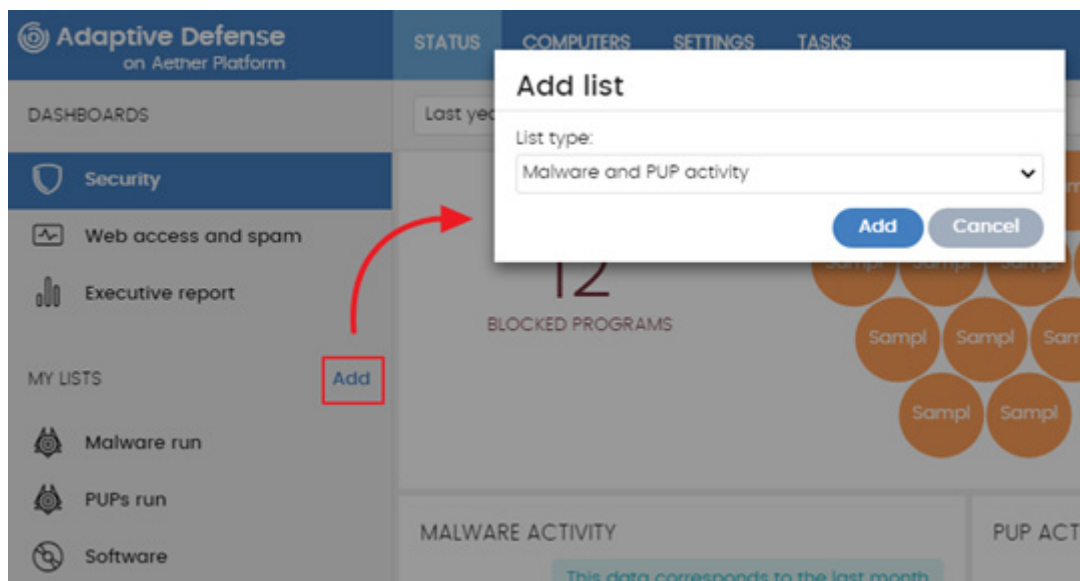


Figure 78: available lists

- **From a dashboard panel**
  - Click a widget on the dashboard to open its associated template.
  - Click its context menu **(6)** and select **Copy**. A new list will be created.
  - Edit the list filters, name and description and click **Save (5)**.
  
- **From an existing list**
  - You can copy an existing list by clicking its context menu **(6)** and clicking **Copy**.
  
- **From the context menu of the My lists panel**
  - Click the context menu of the list you want to copy.
  - Click **Make a copy**.
  - A new view will be created which you can edit according to your preferences.

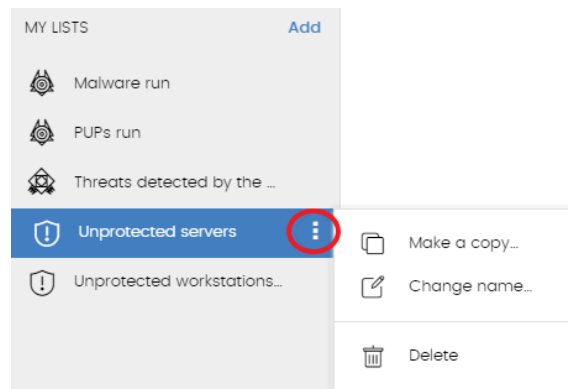




Figure 79: context menu of the lists available in the 'My lists' panel

#### 12.4.4 Deleting a list

There are two different ways to delete a list:

- **From the My lists panel**
  - From the **My lists** panel, click the context menu of the list you want to delete.
  - Click the  icon.
  
- **From the list itself**
  - Click the list's context menu **(6)**
  - Click the  icon from the drop-down menu displayed.

## 12.4.5 Configuring a custom list

To define a new list, follow the steps below:

- Assign a new name to the list **(1)**. By default, the console creates a new name for the list by adding the string "New" to the type of list, or "Copy" if the list is a copy of a previous one.
- Assign a description **(2)**: this step is optional.
- Click the link **Filters (3)** to display the settings and search section.
- Set the data filter **(4)** to display the relevant details.
- Click **Filter (7)** to apply the configured filter in order to check if it meets your needs. The search result will be displayed in the list **(8)**.
- Click **Save (5)**. The list will be added to the panel on the left under **My lists**, and can be accessed by clicking on the name.

Also, in the menu button **(6)** there is an option to export the list to CSV format and to make a copy of it.










*The file generated when exporting a list to CSV format adds additional fields with respect to the list displayed in the Web console. These fields are documented later for each list.*

## 12.5. Available lists

### 12.5.1 Computer protection status list

This list displays all the network computers in detail, with filters that let you locate those workstations or mobile devices that are not protected due to one of the reasons displayed in the panel.

Field	Comments	Values
<b>Computer</b>	Name of the unprotected computer	Character string
<b>Advanced protection</b>	Status of the advanced protection	 Not installed  Error  Enabled  Disabled  No license
<b>Updated protection</b>	This indicates whether the installed protection module has the latest version released.  Hover the mouse pointer over the	 Updated  Not updated (7 days without updating since last




Field	Comments	Values
	field to see the version of the protection installed.	release)  Pending restart
Knowledge	<p>This indicates whether the signature file installed on the computer is the latest version.</p> <p>Hover the mouse pointer over the field to see the date of the latest version installed.</p>	 Updated  Not updated (3 days without updating since last release)
Last connection	Date of the last time that the Adaptive Defense status was sent to the Panda Security cloud.	Date

Table 11: fields in the Computer protection status list

### Fields displayed in the exported file

Field	Comments	Values
Customer	Customer account of the service	Character string
Computer type	Type of device	Workstation Laptop Server
Computer	Computer name	Character string
IP address	Primary IP address of the computer	Character string
Domain	Windows domain to which the computer belongs	Character string
Description		Text
Group	Folder in the Adaptive Defense folder tree to which the computer belongs	Character string
Agent version		Character string

Field	Comments	Values
Installation date	Date on which the Adaptive Defense software was successfully installed on the computer	Date
Last update on	Date of the last update of the signature file	Date
Operating system	Operating system on the computer, internal version and patches applied	Character string
Protection updated	Indicates whether the installed protection has the latest version released	Binary value
Protection version		Character string
Updated knowledge	Last version of the signature file downloaded on the device	Binary
Last connection date	Date when the Adaptive Defense status was last sent to Panda Security's cloud	Date
Advanced protection	Protection status	Not installed Error Enabled Disabled No license

Table 12: fields of the 'Computer protection status' exported file

### Filter tool



Field	Comments	Values
Computer type	Type of device	Workstation Laptop Server
Find computer	Computer name	Character string
Last connection	The last time that the Adaptive	All

Field	Comments	Values
	Defense status was sent to the Panda Security cloud	More than 72 hours More than 7 days More than 30 days
Updated protection	This indicates whether the installed protection module has the latest version released.	All Yes No Pending restart
Knowledge	Update status of the signature file of the antivirus protection	Binary
Reason		Not installed Protection with errors Enabled Protection disabled No license No protection

Table 13: filter fields for the Computer protection status list

### 12.5.2 List of Currently blocked programs being classified

This list shows those files in which **Adaptive Defense** has preliminarily detected some risk despite their classification is not fully complete. These files are blocked during the time it takes to fully classify them.

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Path	Name of the unknown file and its path on the user's computer	Character string
Accessed data 	The unknown file has accessed data on the user's computer	Binary
Made external connections 	The unknown file has communicated with other computers to send or receive data	Binary
Protection mode	The mode of the advanced protection when the unknown file was detected	Audit Hardening Lock
Likelihood of being malicious	Probability that the file turns out to be malicious	Medium, High, Very high

Field	Comments	Values
Date	Date the unknown file was first detected	Date

Table 14: fields in the list of currently blocked programs

### Fields displayed in the exported file



Refer to chapter 14 Forensic analysis for more information about this file

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Threat	Name of the unknown file	Character string
Path	Name of the unknown file and its path on the user's computer	Character string
Protection mode	The mode of the protection when the unknown file was detected	Audit Hardening Lock
Accessed data	The unknown file has accessed data on the user's computer	Binary
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary
Likelihood of being malicious	Probability that the file turns out to be malicious	Medium, High, Very high
Date	Date the unknown file was first detected	Date
Dwell time	Time that the file has been on the customer's network without classification	Date
User	User account under which the file was run	Character string
Hash	String identifying the file	Character string
Source computer	Displays the name of the computer the blocked program came from, if applicable	Character string
Source IP address	Displays the IP address of the computer the blocked program came from, if applicable	Character string



Field	Comments	Values
Source user	The user that was logged in on the computer that the blocked program came from	Character string

Table 15: fields of the 'Currently blocked files' exported file

### Filter tool

Field	Comments	Values
Search date type	<b>Range:</b> this lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month
Search	<b>Computer:</b> device on which the unknown item was detected  <b>File name</b>  <b>Hash:</b> string that identifies the file  <b>Source of the blocked program:</b> allows you to search by the user, IP address or name of the computer that the blocked item came from	Character string
Protection modes	The mode of the advanced protection when the unknown file was detected	<b>Hardening</b> <b>Lock</b>
Accessed data	The unknown file has accessed data on the user's computer	Binary
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary

Table 16: filter fields for the 'Currently blocked programs' list

### 12.5.3 History of blocked programs list

This list shows a history of all threats and unknown files in the process of classification that have been allowed to run by the administrator.

This list is not accessible through any panels in the dashboard. To access it, click the History link on the Currently blocked programs being classified screen.

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string



Field	Comments	Values
Path	Name of the unknown file and its path on the user's computer	Character string
Action	Action taken by Adaptive Defense	Blocked Reclassified as GW Reclassified as MW Reclassified as PUP
Accessed data 	The unknown file has accessed data on the user's computer	Binary
Made external connections 	The unknown file has communicated with other computers to send or receive data	Binary
Protection mode	The mode of the advanced protection when the unknown file was detected	Audit Hardening Lock
Excluded	The unknown file has been unblocked/excluded by the administrator so it can be run	Binary
Likelihood of being malicious	Chances of the unknown file actually being malware	Medium, High, Very high
Date	Date the unknown file was first detected	Date

Table 17: fields in the Blocked programs history

### Fields displayed in the exported file


Refer to chapter 14 Forensic analysis for more information about this file

Field	Comments	Values
Computer	Name of the computer on which the unknown file was detected	Character string
Threat	Name of the unknown file	Character string
Path	Path of the unknown file on the user's computer	Character string
Protection mode	The mode of the advanced protection when the unknown file was detected	Audit Hardening Lock

Field	Comments	Values
Action	Action taken by Adaptive Defense	Blocked Reclassified as GW Reclassified as MW Reclassified as a PUP
Accessed data	The unknown file has accessed data on the user's computer	Binary
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary
Excluded	The unknown file has been unblocked/excluded by the administrator to allow it to run	Binary
Likelihood of being malicious	Probability that the file turns out to be malicious	Medium, High, Very high
Date	Date the unknown file was first detected	Date
Dwell time	Time that the file has been on the customer's network without classification	Date
User	User account under which the file was run	Character string
Hash	String identifying the file	Character string
Source computer	Name of the computer the blocked program came from, if applicable	Character string
Source IP address	IP address of the computer the blocked program came from, if applicable	Character string
Source user	The user that was logged in on the computer that the blocked program came from	Character string

Table 18: fields of the 'History of blocked programs' exported file

### Filter tool

Field	Comments	Values
Search	<p><b>Computer:</b> device on which the unknown item was detected</p> <p><b>Threat:</b> name of the threat</p> <p><b>Hash:</b> string that identifies the file</p> <p><b>Threat:</b> name of the threat</p> <p><b>Source:</b> allows you to search by the user, IP address or name of the computer that the blocked item came from</p>	Character string

Field	Comments	Values
Range	Lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month
Action	Action taken by Adaptive Defense	Blocked Reclassified as GW Reclassified as MW Reclassified as PUP
Excluded	The unknown file has been unblocked/excluded by the administrator so it can be run	Binary
Protection mode	Operating mode of the advanced protection when the unknown file was detected	Hardening Lock
Accessed data	The unknown file has accessed data on the user's computer	Binary
Made external connections	The unknown file has communicated with other computers to send or receive data	Binary

Table 19: fields of the 'History of blocked programs' exported file

### 12.5.4 List of Threats allowed by the administrator

This list shows in detail all the items being classified or classified as threats which the administrator has allowed to be run.



*This list can only be accessed from the Threats allowed by the administrator widget*

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Type	Type of file	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string


Field	Comments	Values
Allowed by	Console user that created the exclusion	Character string
Allowed since	Date that the administrator created the file exclusion	Date
Delete 	This lets you revoke the file exclusion	

Table 20: fields in the Threats allowed by the administrator list

### Fields in the exported file

Fields	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Current type	Type of file at the time the list is accessed	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
Original type	Type of file at the time it was first allowed to be blocked	Malware PUP Blocked Blocked reclassified as Malware/PUP Blocked reclassified as Goodware
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Allowed by	Console user that created the exclusion	Character string
Allowed since	Date that the administrator created the file exclusion	Date

Table 21: fields in the 'Threats allowed by the administrator' exported file

### Filter tool

Field	Comments	Values
Search	<b>Threat:</b> name of the malware or PUP  <b>Allowed by:</b> console user that created the exclusion  <b>File:</b> name of the file containing the threat  <b>Hash:</b> string that identifies the file	Character string
Current classification	File classification at the time the list is accessed	Malware PUP Goodware

Field	Comments	Values
		Being classified (Blocked and suspicious)
<b>Original classification</b>	File classification at the time it was first blocked	Malware PUP Blocked Suspicious

Table 22: filter available in the Threats allowed by the administrator list

### 12.5.5 History of Threats allowed by the administrator list

This displays a history of all events that have taken place with respect to the threats and unknown files that the administrator has allowed to run.

This list doesn't have a corresponding panel in the dashboard. To access it, click the **History** link in the **Threats allowed by the administrator** window.

Field	Comments	Values
<b>Threat</b>	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
<b>Type</b>	Type of threat allowed to run	Malware PUP Blocked Suspicious
<b>File</b>	Name of the unknown file or file that contains the threat	Character string
<b>Hash</b>	String identifying the file	Character string
<b>Action</b>	Action taken on the allowed item	Exclusion removed by the user Exclusion removed after reclassification Exclusion added by the user Exclusion kept after reclassification
<b>User</b>	User account under which the relevant action was taken	Character string
<b>Date</b>	Date the event took place	Date

Table 23: fields in the History of threats allowed by the administrator list

**Fields included in the exported file**

Field	Comments	Values
Threat	Name of the malware or PUP allowed to run. If it is an unknown item, the name of the file will be specified instead.	Character string
Current type	Type of threat the last time it was allowed to run.	Malware PUP Blocked Suspicious
Original type	File type when the event occurred.	
File	Name of the unknown file or file that contains the threat	Character string
Hash	String identifying the file	Character string
Action	Action taken	Exclusion removed by the user Exclusion removed after reclassification Exclusion kept by the user Exclusion kept after reclassification
User	User account of the user that allowed the threat	Character string
Date	Date the event took place	Date

*Table 24: fields in the History of threats allowed by the administrator*

Field	Comments	Values
Search	<b>User:</b> user account of the user that allowed the threat  <b>File:</b> name of the file containing the threat  <b>Hash:</b> string identifying the file	Character string
Current classification	File classification at the time the list is accessed	Malware PUP Goodware Being classified (Blocked and suspicious)
Original classification	File classification at the time it was first blocked	Malware PUP Blocked Suspicious

Field	Comments	Values
Action	Action taken on the allowed item	Exclusion removed by the user Exclusion removed after reclassification Exclusion kept by the user Exclusion kept after reclassification

Table 25: filters available in the History of threats allowed by the administrator list

### 12.5.6 Malware/PUP activity list

This shows administrators the list of threats found on the computers protected by **Adaptive Defense**. This is necessary in order to locate the source of problems, determine the seriousness of incidents and, where necessary, take any troubleshooting measures and update the organization's security policy.

Field	Comments	Values
Computer	Name of the computer on which the threat was detected	Character string
Threat	Name of the threat detected	Character string
Path	Path of the infected file	Character string
Already run	The threat has already been run and the computer could be compromised	Binary
Accessed data	The threat has accessed data on the user's computer	Binary
Made external connections	The threat has communicated with other computers to send or receive data	Binary
Action	Action taken on the malware	Quarantined Blocked Disinfected Deleted Allowed
Date	Date that the threat was detected on the computer	date

Table 26: fields in the Malware/PUP activity list

#### Fields displayed in the exported file



Refer to chapter 14 Forensic analysis for more information about this file



Field	Comments	Values
Computer	Name of the computer on which the threat was detected	Character string
Threat	Name of the threat detected	Character string
Path	Path of the infected file	Character string
Action	Action taken on the malware	Quarantined Blocked Disinfected Deleted Allowed
Run	The threat has already been run and the computer could be compromised	Binary
Accessed data	The threat has accessed data on the user's computer	Binary
Made external connections	The threat has communicated with other computers to send or receive data	Binary
Excluded	The threat has been excluded by the administrator so it can be run	Binary
Date	Date the threat was detected on the computer	Date
Dwell time	Time that the threat has been on the network without classification	Character string
User	User account under which the threat was run	Character string
Hash	String identifying the file	Character string
Source computer	Name of the computer the infection originated from, if applicable	Character string
Source IP address	IP address of the computer the infection originated from, if applicable	Character string
Source user	The user that was logged in on the computer the infection originated from.	Character string

Table 27: fields in the Malware/PUP activity exported file

### Filter tool

Field	Comments	Values
Search	<p><b>Computer:</b> device on which the threat was detected</p> <p><b>Name:</b> name of the threat</p> <p><b>Hash:</b> string that identifies the file</p> <p><b>Infection source:</b> allows you to search by the user, IP address or name of the computer that the infected file came from.</p>	Character string

Field	Comments	Values
	from	
Type	Type of threat	Malware PUP
Range	Lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month Last year
Run	The threat has already been run and the computer could be compromised	True False
Action	Action taken on the threat	Quarantined Blocked Disinfected Deleted Allowed
Accessed data	The threat has accessed data on the user's computer	Binary
Made external connections	The threat has communicated with other computers to send or receive data	True False

Table 28: filter fields in the Malware/PUP activity list

### 12.5.7 Exploit activity list

Shows a list of all computers with programs compromised by vulnerability exploit attempts. The purpose of this list is to provide administrators with the necessary information to find the source of a problem, assess the severity of an incident and, if required, take the necessary remediation measures and update the company's security policies.

**Adaptive Defense** can take the following actions on detected exploits:

- **Allowed:** the exploit was allowed to run as the anti-exploit protection was configured in 'Audit' mode.
- **Blocked:** the exploit was blocked before it could run.
- **Allowed by the user:** the computer user was asked for permission to end the compromised process, but decided to let the exploit run.
- **Process ended:** the exploit has been deleted, but managed to partially run.
- **Pending restart:** the user has been informed of the need to restart their computer in order to completely remove the exploit. Meanwhile, the exploit has continued to run.

Field	Comment	Values
Computer	Name of the computer where the threat was detected	Character string
Compromised program	Program hit by the exploit attack	Character string

Field	Comment	Values
Action	Action taken on the exploit	Allowed by the user Allowed Blocked Process ended Pending restart
Exploit run	Indicates if the exploit managed to run or was blocked before it could affect the vulnerable program	Binary
Date	Date when the exploit attempt was detected on the computer	Date

Table 29: fields in the Exploit activity list

### Fields displayed in the exported file



Refer to chapter 14 Forensic analysis for more information about this file

Field	Comment	Values
Computer	Name of the computer where the threat was detected	Character string
Compromised program	Program hit by the exploit attack	Character string
Hash	String identifying the compromised program	Character string
Last action	Action taken on the exploit	Allowed by the user Allowed by the administrator Blocked (immediately) Blocked after the process was ended
Risk	Indicates if the computer is or has been at risk, or the exploit was blocked before it could affect the vulnerable program	Binary
Date	Date when the exploit attempt was detected on the computer	Date

Table 30: fields of the 'Exploit activity' exported file

### Filter tool

Field	Comments	Values
Search	<p><b>Computer:</b> device on which the threat was detected</p> <p><b>Hash:</b> string that identifies the compromised program</p>	Character string

Field	Comments	Values
Range	Lets you set the time period, from the current moment back	Last 24 hours Last 7 days Last month
Exploit run	Indicates if the exploit managed to run or was blocked before it could affect the vulnerable program	Binary value
Action	Action taken on the exploit	Allowed by the user Allowed Blocked Process ended Pending restart

Table 31: filter fields for the Exploit activity list

### 12.5.8 Licenses list

The Licenses list is covered in chapter 5 Licenses

### 12.5.9 'Unmanaged computers discovered' list

The **Unmanaged computers discovered** list is covered in chapter .

## 12.6. Default lists

The management console includes four lists generated by default:

- Unprotected workstations and laptops
- Malware run
- PUPs run
- Unprotected servers

### Unprotected workstations and laptops

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

- Computers on which the **Adaptive Defense** software is currently being installed or that have an installation problem.
- Computers with the protection disabled or with errors.
- Computers without a license assigned or with expired licenses.

### Malware run

This locates the network computers on which threats have run in the last month. These devices may be infected for one of these reasons:

- The administrator has unblocked an unknown item before it has been classified and it turned out to be malware
- The administrator excluded a known threat from scans in order to run it.
- The computer was in Audit or Hardening mode and the threat existed prior to the installation of **Adaptive Defense**

### PUPs run

This locates the network computers on which unwanted programs have run in the last month. These devices may be infected for one of these reasons:

- The administrator has unblocked an unwanted program before it has been classified and it turned out to be malware.
- The administrator excluded an unwanted program from scans in order to run it.
- The computer was in Audit or Hardening mode and the unwanted program existed prior to the installation of **Adaptive Defense**

### Unprotected servers

This list lets you locate all servers, regardless of the operating system installed, that may be vulnerable to threats due to a problem with the protection:

- Servers on which the **Adaptive Defense** software is currently being installed or that have an installation problem.
- Servers with the protection disabled or with errors.
- Servers without a license assigned or with expired licenses

# 13. Managing threats, quarantined items and items being classified

---

Tools for managing blocked and excluded  
items

Action diagrams for known and unknown  
processes

Reclassification policies

Unblocking/Excluding items

Managing excluded items

Strategies to supervise installation of new  
software

Quarantine management

## 13.1. Introduction

**Adaptive Defense** provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This balance is achieved through the use of several configurable tools:

- Tools for managing blocked items being classified
- Tools for managing the execution of processes classified as threats
- Tools for managing the backup/quarantine area

### Considerations about managing blocked unknown items

**Adaptive Defense** ensures network protection through two operational modes available in the advanced protection settings for Windows devices: **hardening** and **Lock**. These modes prevent the execution of all unknown processes on users' computers.



*Refer to chapter 10 for more information about Adaptive Defense's advanced protection modes*

Panda Security's Machine Learning technologies in the company's Big Data environments scan all unknown processes, automatically returning a classification within the first 24 hours since they were first seen. Unknown processes are accurately and unambiguously classified as goodware and malware, and this classification is shared with all Panda Security customers, so that they can all benefit from the company's malware knowledge.

**Adaptive Defense** blocks the execution of every process being classified, thus preventing potential risk situations. However, in a minority of cases, these automated scans cannot classify the unknown process with the level of accuracy required (99.999%), and manual intervention is needed by a malware specialist.

In these cases, and should the item being classified be essential for the company's activities, the administrator may consider it necessary to take a certain risk and let the item run.

### Considerations about managing processes classified as malware

In other cases, the administrator may want to allow the execution of certain types of malware which, despite posing a potential threat, provide features valued by users. This is the case of PUPs, for example. These include toolbars that offer search capabilities but also collect users' private data and confidential corporate information for advertising purposes.

### Considerations about quarantine management

Finally, administrators may want to have access to items classified as threats and deleted from users' computers.

## 13.2. Tools for managing blocked items and exclusions

Administrators can manage blocked items and exclusions from different areas within the management console. Below we provide a quick reference guide to find these tools quickly.

All of these tools are accessible from the **Status (1)** menu at the top of the console. Click the relevant widget in the dashboard.

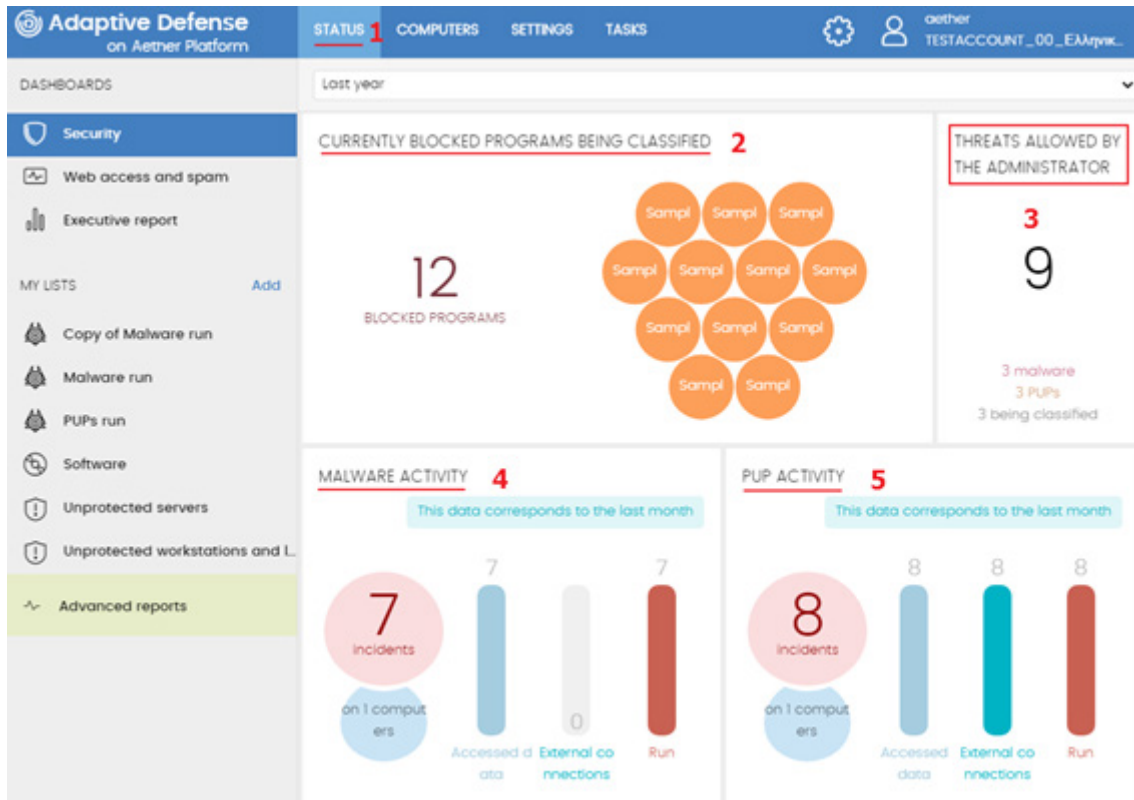



Figure 80: dashboard tools to manage blocked items and exclusions

### Lists

- To get a list of currently blocked items being classified: go to the **Currently blocked programs being classified** panel (2)
- To get a list of currently blocked items classified as malware: go to the **Malware activity** panel (4)
- To get a list of currently blocked items classified as PUPs: go to the **PUP activity** panel (5)
- To get a list of currently excluded items: go to the **Threats allowed by the administrator** panel (3)
- To get a history of currently excluded items: Go to the **Threats allowed by the administrator** panel (3), **History** context menu
- To see the state changes of excluded items: go to the **Threats allowed by the administrator** panel (3), **History** context menu



### Adding and removing exclusions

- **To add a malware exclusion:** go to the **Malware activity** panel (4), select a threat, click **Do not detect again**
- **To add a PUP exclusion:** go to the **PUP activity** panel (5), select a threat, click **Do not detect again**
- **To remove an exclusion:** Go to the **Threats allowed by the administrator** panel (3), select a threat and click the icon 

### Behavior changes

- **To change the solution's behavior when an item is reclassified:** go to the **Threats allowed by the administrator** panel (3), click the **Change behavior** link.

## 13.3. Action diagrams for known and unknown processes

**Adaptive Defense** blocks all programs classified as malware by default. Additionally, and depending on the advanced protection settings, it will also block never-seen-before programs until they have been scanned and a verdict has been returned about their security.

If a user cannot wait for an unknown item to be classified, or the administrator wants to allow an item classified as malware to run, **Adaptive Defense** implements tools to create an exclusion and allow a blocked item to run.



*IMPORTANT: we generally advise that you don't unblock blocked items. Items blocked for being considered dangerous pose a real threat to the integrity of your IT systems and the data stored across your network. Adaptive Defense classifies items with 99.9999% accuracy, and the unknown items blocked are very likely to end up being classified as dangerous. That's why we recommend that you do not unblock as yet unknown items or items classified as malware/PUP.*

### 13.3.1 Action diagram for known files

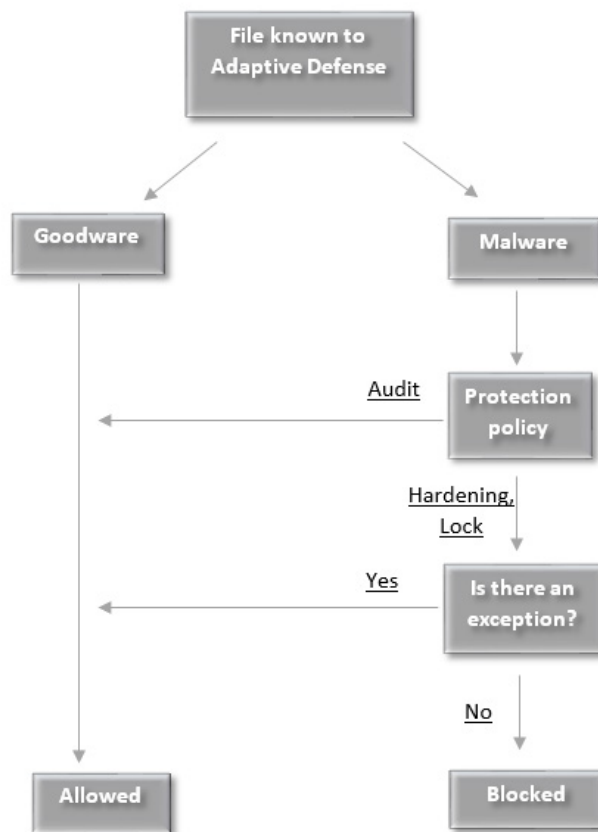


Figure 81: action diagram for known classified processes

Processes classified by **Adaptive Defense** 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.

### 13.3.2 Unknown files

Unknown (not yet classified) processes that are detected with the advanced protection set to a mode other than **Audit** will be blocked unless the network administrator creates an exclusion. Regardless of the exclusion, **Adaptive Defense** will classify the file and, depending on the verdict and the reclassification policy selected, the file will be blocked or allowed to continue running.

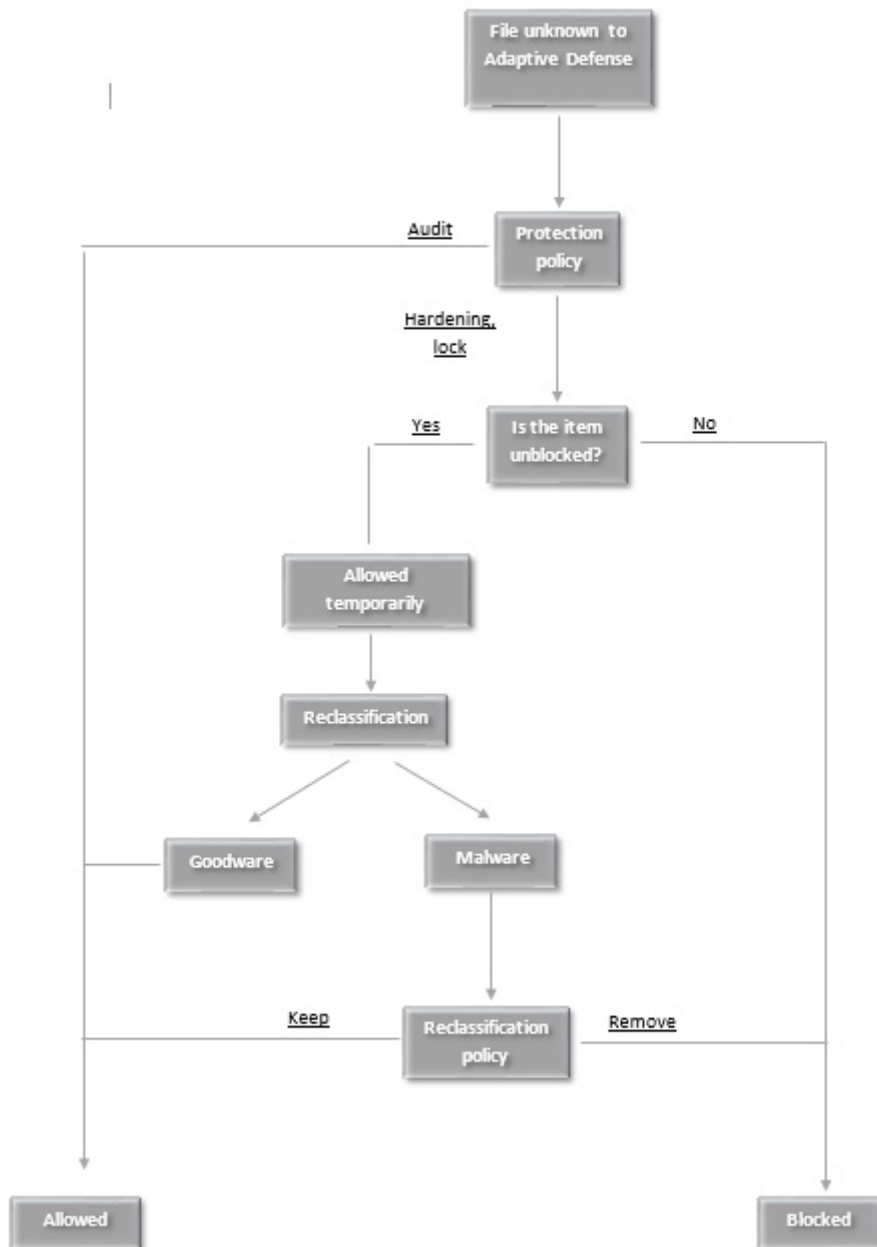


Figure 82: action diagram for unknown processes

### 13.4. Reclassification policy

The reclassification policies let you define the way **Adaptive Defense** will automatically behave when an item that was unblocked by the administrator changes its internal state and it is necessary to make a new decision about whether to block/unblock it.

There are two possibilities when the administrator chooses to unblock a previously blocked (unknown) item: if the unknown item is finally classified as goodware, no further action will need to be taken, as the system will continue to allow it to run. However, if the unknown item is finally

classified as malware, the administrator will have to choose the action that **Adaptive Defense** 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 on the list of threats allowed by the administrator:** the exclusion is kept. That is, the item will be allowed to run.

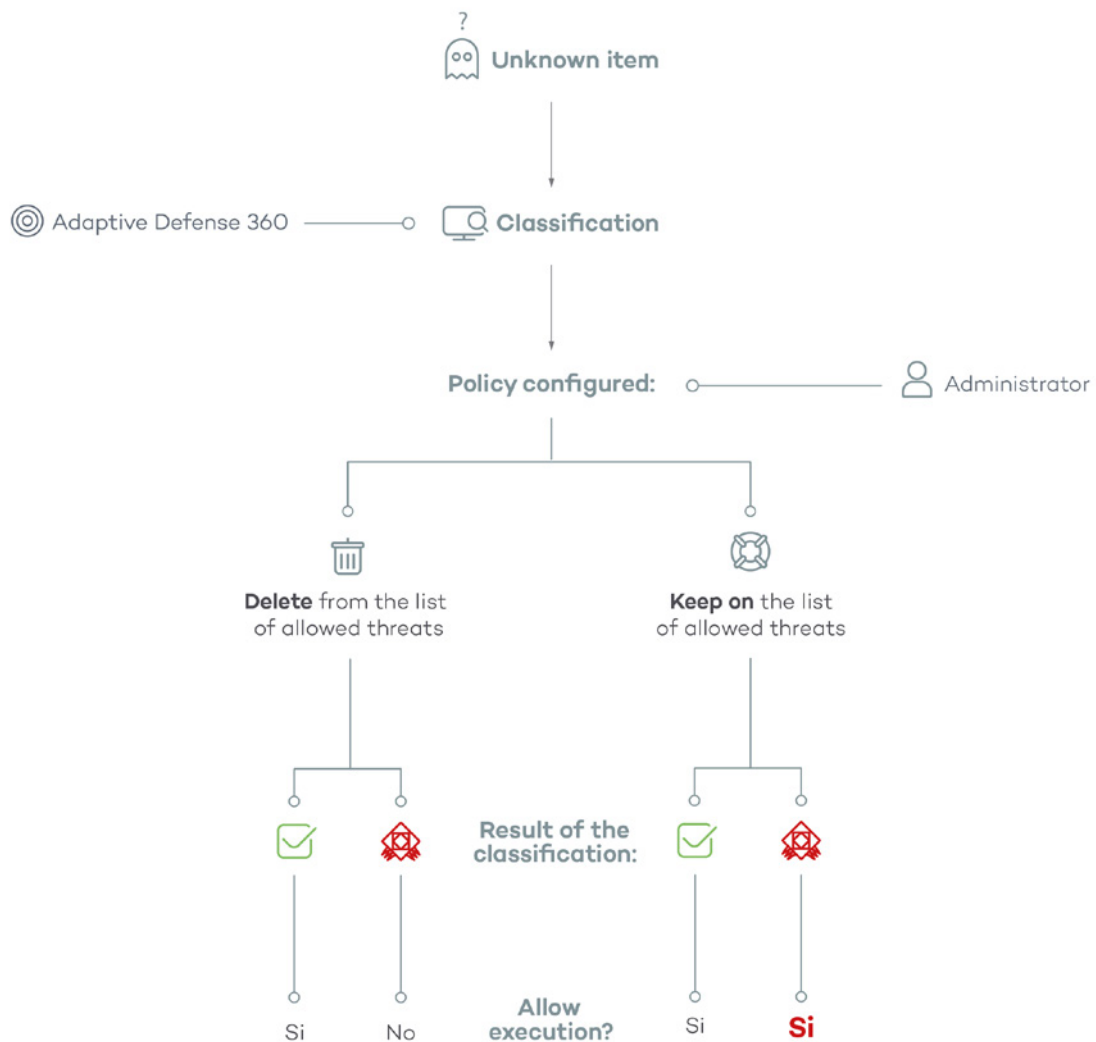


Figure 83: adaptive Defense's behavior based on the reclassification policy selected and the classification result

### 13.4.1 Changing the reclassification policy

Go to the **Status** menu at the top of the console and click the **Threats allowed by the administrator** panel. Click the **Change behavior** link to select the reclassification policy to apply.

 *Reclassification policies are general for all computers on the network irrespective of the assigned settings*

Selecting **Keep it on the list of threats allowed by the administrator** will display a warning on the **Threats allowed by the administrator** screen, indicating that this can lead to potentially dangerous situations. Example: an unknown item that is pending classification is unblocked by the administrator in order to allow its execution while the classification process is taking place. Once fully identified, the items turns out to be dangerous. In this case, should the option **Keep it on the list of threats allowed by the administrator** be selected, the malicious item would continue to be allowed to run.

### 13.4.2 Reclassification traceability

It is very important to know if **Adaptive Defense** has reclassified an unknown item, especially if the administrator selected the **Keep it on the list of threats allowed by the administrator** policy.

#### Traceability using the History of allowed threats

To view the history of reclassifications of an excluded file, go to the **Threats allowed by the administrator** panel and click the context menu to display the history of allowed threats. A list will appear with the name of all allowed threats and the events that have taken place (**Action** column).

#### Traceability using the alerts

**Adaptive Defense** sends administrators an alert every time an unknown item gets blocked. Not only this, they can also receive a notification every time a previously unblocked item is reclassified.

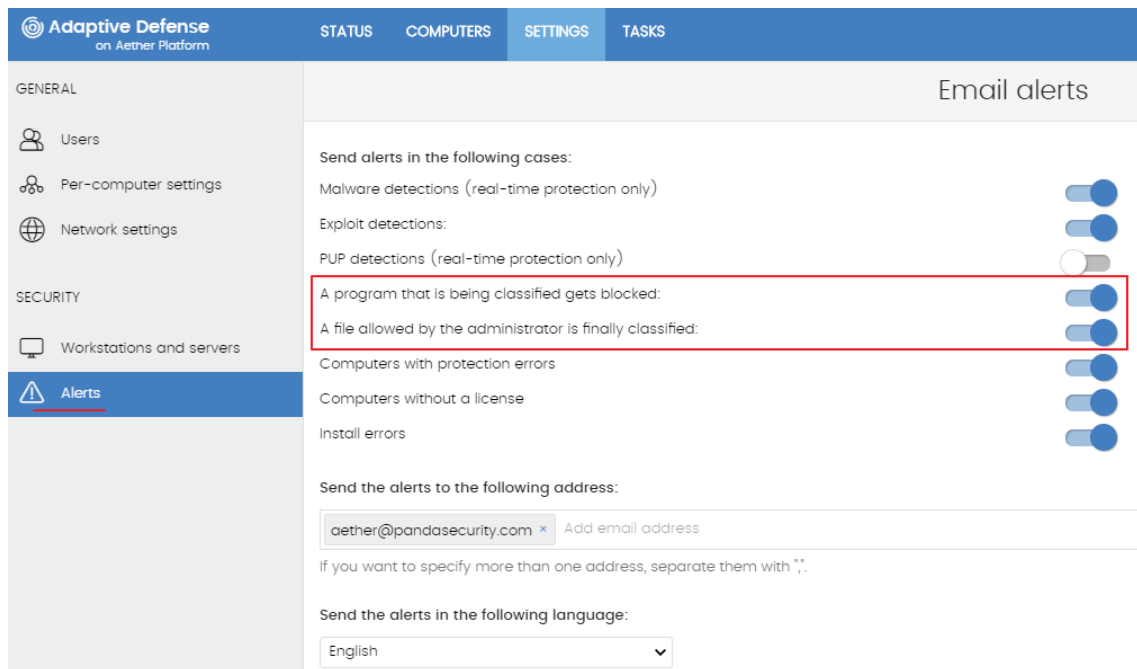


Figure 84: configuring the alerts received after an item is blocked or reclassified

## 13.5. Unblocking/Excluding items



*Excluding or unblocking a program causes Adaptive Defense to allow the execution of both the program and all of its libraries and binary files (unless they are known threats).*

Depending on whether you want to allow the execution of a file being classified, or of a file classified as a threat, go to the **Currently blocked programs being classified** or **Malware/PUP activity** panel.

### 13.5.1 Excluding unknown items pending classification

If users cannot wait for the system to automatically unblock a file once it has been classified, the administrator can use the button **Unblock** in the **Currently blocked items being classified** window to allow its execution.

Once unblocked, the item will disappear from the **Currently blocked items being classified** screen, and will be run under the administrator's responsibility. Nevertheless, **Adaptive Defense** will continue scanning the process until it is identified and classified. The unblocked item will appear in the **Threats allowed by the administrator** list, described later in the chapter.

### 13.5.2 Excluding items classified as malware or PUP

Excluding an item classified as malware from the scans is equivalent to unblocking a blocked item that is pending classification, although in this case you are allowing the execution of a program that **Adaptive Defense** has already classified as harmful or dangerous.

Go to the **Malware/PUP activity** panel, select a threat, and click the **Do not detect again** button to allow it to run.

Once excluded from the scans, the item in question will stop generating incidents in the **Malware/PUP activity** panels, and will be added to the **Threats and other excluded items** list, as explained in the next section.

## 13.6. Managing excluded items

To manage excluded items, as well as to configure the solution's behavior when an unknown item or a known item classified as a threat is reclassified, go to the **Threats allowed by the administrator** panel.

This panel lets you view and manage currently allowed files, as well as access a history of all excluded items.

### List of currently excluded items

**Threats allowed by the administrator** displays items with an active exclusion. Every item on the list is allowed to run.

### History

Click the context menu to display a history of all files excluded in **Adaptive Defense** and the actions taken on them. This list allows you to view all the states that a file has gone through (allowed or blocked), from the time it entered the **Threats allowed by the administrator** list until it exited it.

## 13.7. Strategies to supervise installation of new software

During the normal operation of a computer protected with **Adaptive Defense**, the solution may detect a small percentage of unknown programs that need classification, and depending on the advanced configuration selected, these programs may be blocked until the classification process returns a verdict (goodware or malware). This will prevent end users from temporarily using those programs.

If the IT department controls the installation of programs on the network and wants to minimize the impact of unknown software on users' activities, while ensuring security, it is advisable to prepare the environment for the execution of new software before deploying it massively across the network.

This process can be divided into four phases:

### Configuring a test PC

The aim of this phase is to determine if the software to be installed on the network is known or unknown to Panda Security. To do this, you can use the PC of a network user or use a computer dedicated to this purpose. This computer should be configured in **Hardening** mode.

### Installing the software

This step consists of installing the software and running it normally. If **Adaptive Defense** finds an unknown module or program, it will block it, displaying a pop-up window on the local computer. Also, a new item will be added to be **Currently blocked items being classified** panel. Internally, **Adaptive Defense** will log the events generated by the program, sending the binary files to the cloud for analysis.

If no items are blocked in **Hardening** mode, change the advance protection settings to **Lock** mode, and run the newly installed program again. If new items are blocked, they will be shown in the **Currently blocked items being classified** panel.

### Reclassifying blocked programs

As soon as **Adaptive Defense** returns a verdict about the blocked programs, it will send an email to the administrator informing them of whether it will unblock them or keep them blocked depending

on whether they are goodware or malware. If all processes are classified as goodware, the installed software will be valid for use across the organization's network.

### **Sending the program directly to Panda Security's cloud**

Since **Adaptive Defense** is designed to not interfere with network performance when sending files to Panda Security's cloud, file send can be delayed. To speed up the send process, contact Panda Security's Support Department.

## 13.8. Managing the backup/quarantine area

**Adaptive Defense's** quarantine is a backup area that stores the items deleted after being classified as a threat.

Quarantined items are stored on each user's computer, in the Quarantine folder located in the software installation directory. This folder is encrypted and cannot be accessed by any other process. Thus, it is not possible to directly access or run any quarantined items, unless you do it using the Web console's restore tool.

**Adaptive Defense** also quarantines suspicious files automatically, provided they meet the conditions established by Panda Security's PandaLabs department.

Once a suspicious item has been quarantined for further analysis, there are four possible scenarios:

- The item is classified as malicious but there is a disinfection routine for it: it is disinfected and restored to its original location.
- The item is classified as malicious, and there is no disinfection routine for it: it is quarantined for seven days.
- The item is identified as harmless: it is restored to its original location.
- Suspicious items are quarantined for a maximum of 30 days. If they finally turn out to be goodware, they are automatically restored to their original location.



*Adaptive Defense doesn't delete files from users' computers. All deleted files are actually sent to the backup area*

### 13.8.1 Viewing quarantined items

Administrators can view quarantined items through the lists and the following dashboard widgets:

- Malware activity
- PUP activity

Use the filtering tools to view quarantined items (use the **Action** filter: "Quarantined" or "Deleted").



### 13.8.2 Restoring quarantined items

To restore a quarantined item, select it and click **Restore and do not detect again**. This will copy the item to its original location and restore its original permissions, owner, the registry keys associated with the file and any other information.

# 14. Forensic analysis

---

Details of blocked programs and threats  
The action tables  
The execution graphs  
Interpreting the action tables and execution graphs

## 14.1. Introduction

Next-generation malware is characterized by going undetected for long periods of time, taking advantage of this to access corporate sensitive data and intellectual property. Its objective is economic gain, either through blackmail by encrypting corporate documents for ransom, or selling the information obtained to the competition, among other strategies common to these types of attacks.

When the **Adaptive Defense** dashboard displays an infection risk, it needs to be determined to what extent the network has been compromised and the source of the infection. To do this, it is essential to know the actions taken by the malware in order to implement the necessary preventive and remedial measures. **Adaptive Defense** continuously monitors all actions triggered by threats, and stores them to show their progress, from the time they were first seen on the network until their neutralization.

**Adaptive Defense** presents this information in several ways depending on the level of detail and the information required:

- Through detail pages
- Through action tables
- Through graphs
- Through Excel files.

## 14.2. Details of threats and currently blocked programs in the process of classification

The **Status** menu at the top of the console lets you access lists of detected threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified.**

Click a specific threat to open a window (**Malware detection**, **PUP detection**, **Exploit detection** or **Blocked program details**) where you can find detailed information about the threat on the **Details** tab.


### 14.2.1 Malware detection, PUP detection and currently blocked programs in the process of classification

These windows are divided into five sections:

- Overview
- Affected computer
- Threat impact on the computer
- Infection source
- Occurrences on other computers

### Overview




- **Threat:** name of the threat and unique hash that identifies it.
- **Action:** action taken by **Adaptive Defense** on the item.
  - Quarantined
  - Blocked
  - Disinfected
  - Deleted

 Refer to chapter 13 for more information about the actions administrators can take on the items found

### Affected computer

- **Computer:** name of the computer where the threat was found, IP address and folder in the Groups tree.
- **User:** operating system user under which the threat was loaded and run.
- **Protection mode:** operating mode of the advanced protection when the detection occurred (**Audit, Hardening, Lock**).
- **Detection path:** file system path of the threat.

### Threat impact on the computer

- **Threat:** name of the detected threat and file identification string (hash). Two buttons are available to search for additional information on Google and VirusTotal's website. If the threat is a newly discovered threat, the text **New threat** will be displayed.
- **Activity:** summary of the most important actions taken by the malware:
  - Has run 
  - Has accessed data files 
  - Has exchanged data with other computers 
- **Detection date**
- **Dwell time:** time during which the threat has been on the system without being classified.

## Infection source

- **Source computer:** displays the name of the computer the infection originated from, if applicable.
- **Source IP address:** displays the IP address of the computer the infection originated from, if applicable.
- **Source user:** the user that was logged in on the computer the infection originated from.

## Occurrences on other computers

Displays all computers on the network where the malware has been seen.

- **Computer:** computer name
- **File path:** name and path of the file that contains the malware
- **First seen:** date the threat was first detected on the computer

You can also access a chart detailing the malware activity. This chart is discussed later in this chapter.

## 14.2.2 Exploit detection

This window is divided into five sections:

- **Overview**
- **Affected computer**
- **Exploit impact on the computer**
- **Infection source**
- **Occurrences on other computers**



### Overview

- **Compromised program:** name of the program that was hit by the exploit and hash that identifies it.
- **Action:** shows the action taken by **Adaptive Defense** on the program hit by the exploit.
  - **Allowed:** the exploit was allowed to run as the anti-exploit protection was configured in "Audit" mode.
  - **Blocked:** the exploit was blocked before it could run.
  - **Allowed by the user:** the computer user was asked for permission to end the compromised process, but decided to let the exploit run.
  - **Process ended:** the exploit has been deleted, but managed to partially run.
  - **Pending restart:** the user has been informed of the need to restart their computer in order to completely remove the exploit. Meanwhile, the exploit has continued to run.

### Affected computer

- **Computer:** name of the computer where the threat was found, IP address and folder in the Groups tree.
- **User:** operating system user under which the threat was loaded and run.
- **Protection mode:** operating mode of the advanced protection when the detection occurred (**Audit, Hardening, Lock**).
- **Detection path:** file system path of the threat.

### Exploit impact on the computer

- **Compromised program:** name and path of the program that was hit by the exploit attempt. If **Adaptive Defense** detects that the program is not updated to the latest available version, the  **Vulnerable program** warning message is displayed.
- **Activity**  : indicates if the exploit managed to run before being detected by **Adaptive Defense**.
- **Detection date**
- **Last accessed URLs:** list of the last URLs accessed by the vulnerable process hit by the exploit

You can also access a chart detailing the exploit activity. This chart is discussed later in this chapter.

## 14.3. Action tables

The **Status** menu at the top of the console lets you access lists of detected threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified.**

Click a specific threat to open a window (**Malware detection, PUP detection, Exploit detection** or **Blocked program details**) where you can find detailed information about the actions taken by the threat on the **Activity** tab.

The **Activity** tab displays an action table with the most relevant events triggered by the threat.



*The number of actions and events triggered by a process is very high. Therefore, displaying all of them would hinder the extraction of useful information to perform a forensic analysis.*

The table content is initially sorted by date, making it easier to follow the progress of the threat.

Table 32 shows the fields included in the action table:

Field	Comment	Values
Date	Date of the action	Date
Times	Number of times the action was executed. A single action executed several times consecutively will only appear once on the list	Numeric value
Action	Action logged by the system and command line associated with it	Downloaded from Communicates with Accesses data Is run by Runs Is created by Creates Is modified by Modifies Is loaded by Loads Is deleted by Deletes Is renamed by Renames Is killed by Kills process Creates remote thread Thread injected by Is opened by Opens Creates Is created by Creates key pointing to Exe file Modifies key pointing to Exe file
Path/URL/Registry Key/IP:Port	Action entity. It can have the following values depending on the action type:	<p><b>Registry key:</b> for actions that involve modifying the Windows registry</p> <p><b>IP:Port:</b> for actions that involve communicating with a local or remote computer</p> <p><b>Path:</b> for actions that involve access to the computer hard disk</p> <p><b>URL:</b> for actions that involve access to a URL</p>
File Hash/Registry Value/Protocol-Direction/Description	This field complements the entity field	<p><b>File Hash:</b> for actions that involve access to a file</p> <p><b>Registry Value:</b> for actions that involve access to the registry</p> <p><b>Protocol-Direction:</b> for actions that involve communicating with</p>

Field	Comment	Values
		a local or remote computer. Possible values are: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• Bidirectional</li> <li>• Unknown</li> <li>• Description</li> </ul>
Trusted	The file is digitally signed	Binary value

Table 32: fields displayed in a threat's action table

### 14.2.3 Subject and predicate in actions

To correctly understand the format used to present the information in the action list, a parallel needs to be drawn with the natural language:

- All actions have as the subject the file classified as a threat. This subject is not indicated in each line of the action table because it is common throughout the table.
- All actions have a verb which relates the subject (the classified threat) with an object, called entity. The entity is indicated in the **Path/URL/Registry key/IP:port** field of the table.
- The entity is complemented with a second field which adds information to the action: **file Hash/Registry Value/Protocol-Direction/Description**.

Table 33 shows two actions carried out by the same hypothetical malware:

Date	Times	Action	Path/URL/Registry Key/IP	File Hash/Registry Value/Protocol/Description	Trusted
3/30/2015 4:38:40 PM	1	Communicates with	54.69.32.99/80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Loads	PROGRAM_FILES \MOVIES TOOLBAR\SAFETYNT\SAFETYCRT.DLL	9994BF035813FE8EB6BC98E CCBD5B0E1	NO

Table 33: action list of a sample threat

The first action indicates that the malware (subject) **connected to (action)** the IP address 54.69.32.99:80 (entity) through the TCP-bidirectional protocol.

The second action indicates that the malware (subject) **loaded (action)** the library PROGRAM\_FILES|\MOVIES TOOLBAR\SAFETYNT\SAFETYCRT.DLL with hash 9994BF035813FE8EB6BC98ECCBD5B0E1.

As with natural language, two types of sentences are implemented in **Adaptive Defense**:

- **Active:** these are predicative actions (with a subject and predicate) related by an active verb. In these actions, the verb of the action relates the subject, which is always the process



classified as a threat, and a direct object, the entity, which can be multiple according to the type of action.

- **Passive:** these are actions where the subject (the process classified as a threat) becomes the passive subject (which receives, rather than executes the action), and the verb is passive (to be + participle). In this case, the passive verb relates the passive subject which receives the action with the entity, which performs the action.

Examples of active actions are:

- Communicates with
- Loads
- Creates

Examples of passive actions are:

- Is created by
- Is downloaded from

Table 34 shows an example of a passive action:

Date	Times	Action	File Path/URL/Registry Key/IP	File Hash/Registry Value/Protocol/Description	Trusted
3/30/2015 4:51:46 PM	1	Is run by	WINDOWS   \ explorer.exe	7522F548A84ABAD8FA516D E5AB3931EF	NO

Table 34: example of a passive action

In this action, the malware (passive subject) **is run by** (passive action) the WINDOWS | \explorer.exe program (entity) with hash 7522F548A84ABAD8FA516DE5AB3931EF.



*Active actions let you inspect in detail the steps taken by the threat. By contrast, passive actions usually reflect the infection vector used by the malware (which process ran it, which process copied it to the user's computer, etc.).*

## 14.4. Execution graphs

The **Status** menu at the top of the console lets you access lists of detected threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified.**

Click a specific threat. A different window will open depending on the type of threat: **malware detection**, **PUP detection**, **Exploit detection** or **Blocked program details**. Go to the **Activity** tab and click the **View activity graph** button.

Execution graphs offer a graphical representation of the information shown in the action tables, emphasizing the temporal aspect.

These graphs provide an at-a-glance idea of the actions triggered by the threat.



Figure 85: example of a graph representing a threat's activities

### 14.3.1 Diagrams

Execution graphs represent the actions taken by threats with two elements:

- **Nodes:** they mostly represent actions or information items.
- **Lines and arrows:** they join the action and information nodes to establish a temporal order, and assign each node the role of "subject" or "predicate".











### 14.3.2 Nodes

The nodes show information through their associated icon, color, and descriptive panel on the right of the screen when selected with the mouse.

The color code used is as follows:

- **Red:** untrusted item, malware, threat.
- **Orange:** unknown/unclassified item.
- **Green:** trusted item, goodware.

Table 35 shows action-type nodes with a brief description:

Symbol	Description
	File download Compressed file created
	Socket/communication used
	Monitoring initiated
	Process created
	Executable file created Library created Key created in the registry
	Executable file modified Registry key modified
	Executable file mapped for write access
	Executable file deleted
	Library loaded
	Service installed
	Executable file renamed
	Process stopped or closed



Symbol	Description
	Thread created remotely
	Compressed file opened

Table 35: graphical representation of the malware actions shown in the execution graph

Table 36 shows descriptive-type nodes with a brief description:













Symbol	Description
 filename.exe  filename.exe  filename.exe	File name and extension Green: goodware Orange: unclassified item Red: malware/PUP
 pcname  pcname  pcname	Internal computer (it is on the corporate network) Green: trusted Orange: unknown Red: untrusted
 pcname  pcname  pcname	External computer Green: trusted Orange: unknown Red: untrusted
 Spain	Country associated with the IP address of an external computer
	File and extension
	Registry key

Table 36: graphical representation of descriptive-type nodes in the execution graph

### 14.3.3 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:** 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

### 14.3.4 The timeline

The timeline helps control the display of the string of actions carried out by the threat over time. Using the buttons at the bottom of the screen you can position yourself at the precise moment 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:

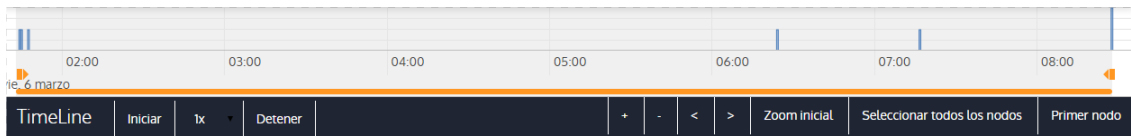


Figure 86: graphical representation of a threat's timeline

You can select a specific interval on the timeline dragging the interval selectors to the left or right to cover the timeframe of most interest to you.



Figure 87: time selectors

After selecting a timeframe, the graph will only show the actions and nodes that fall within that interval. The rest of the actions and nodes will be blurred on the graph.

The actions carried out by the threat are represented on the timeline as vertical bars accompanied by a timestamp, which indicates the hour and minute when they occurred.

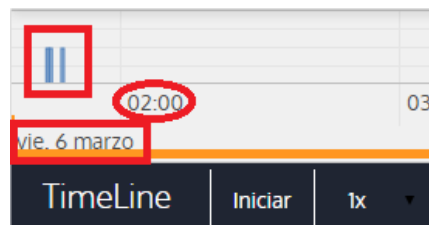


Figure 88: timestamp, date and actions carried out by the threat

### 14.3.5 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.

### 14.3.6 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 representing the actions will appear while passing along the timeline.
- **1x**: establishes the speed of traveling along the timeline.
- **Stop**: stops the execution of the timeline.
- **+ and -**: zoom in and zoom out of the timeline.
- **< and >**: moves the node selection to the immediately previous or subsequent node.
- **Initial zoom**: restores the initial zoom level if modified with the + and – buttons.
- **Select all nodes**: moves the time selectors to cover the whole timeline.
- **First node**: establishes the time interval at the start, a necessary step for initiating the display of the complete timeline.



*To display the full path of the timeline, first select “First node” and then “Start”. To set the travel speed, select the button 1x.*

### 14.3.7 Filters

The controls for filtering the information shown in the execution graph are at the top of the graph.



*Figure 89: filters in the execution graph*

The available filtering criteria are:

- **Action**: drop-down menu which lets you select an action type from all those executed by the threat. This way, the graph will only show the nodes that match the action type selected and the adjacent nodes associated with this action.
- **Entity**: drop-down menu which lets you choose an entity (the content of the field Path/URL/Registry Key/IP:Port).


### 14.3.8 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.



Figure 90: buttons to zoom in and zoom out of the graph

 To zoom in and zoom out more easily, you can use the mouse's scroll wheel.

The X symbol allows you to leave the graph view. If you would rather hide the timeline button zone to use more space on the screen for the graph, you can select the  icon located in the bottom right of the graph.

Finally, you can configure the behavior of the graph through the panel below. To access it, click the  button in the top left corner of the graph.

**Layout:**

Custom ▼

Barnes Hut
  Repulsion
  Hierarchical

**Repulsion**

Node distance 0 300

Central gravity 0 3

Spring length 0 500

Spring constant 0 0.5

Damping 0 0.3

**Options:**

←

Figure 91: execution graph settings panel

## 14.5. Excel tables

The **Status** menu at the top of the console lets you access lists of threats and currently blocked programs through the following widgets:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Currently blocked programs being classified**

Click the context menu and select **Export list and details** from the drop-down menu displayed. An Excel file will be downloaded with the full lifecycle of all threats on the list

Campo	Comentario	Valores
Date	Date when the action took place	Date
Hash	String identifying the threat	Character string
Threat	Threat name	
User	User account under which the threat was run	Character string
Computer	Name of the computer where the threat was detected	Character string
Path	Name and path to the threat on the user's computer	Character string
Accessed data	The threat accessed files located on the user's computer	Binary value
Action	Action logged by the system	Downloaded from Communicates with Accesses data Run by Runs Created by Creates Modified by Modifies Loaded by Loads Deleted by Deletes Renamed by Renames Killed by Kills process Creates remote thread Thread injected by Opened by Opens Creates Created by Creates registry key to run Modifies registry key to run
Command Line	Command line associated with the action	Character string



Campo	Comentario	Valores
Event date		Date
Times	Number of times the action was executed. A single action executed several times consecutively will only appear once on the list	Numeric value
Path/URL/Registry Key/IP:Port	Action entity. It can have the following values depending on the action type:	<p><b>Registry key:</b> for actions that involve modifying the Windows registry</p> <p><b>IP:Port:</b> for actions that involve communicating with a local or remote computer</p> <p><b>Path:</b> for actions that involve access to the computer hard disk</p> <p><b>URL:</b> for actions that involve access to a URL</p>
File Hash/Registry Value/Protocol-Direction/Description	This field complements the entity field	<p><b>File hash:</b> for actions that involve access to a file</p> <p><b>Registry value:</b> for actions that involve access to the registry</p> <p><b>Protocol-Direction:</b> for actions that involve communicating with a local or remote computer. Possible values are:</p> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• Bidirectional</li> <li>• Unknown</li> <li>• Description</li> </ul>
Trusted	The file is digitally signed	Binary value

Table 37: fields in the 'List and details' exported file

## 14.6. Interpreting the action tables and execution graphs

The action tables and execution graphs are graphical representations of the evidence collected on the customer's computers. These must be interpreted by the organization's network administrator. A certain degree of technical knowledge is necessary to be able to extract activity patterns and key information in each situation.

Below we provide some basic guidelines to interpret the action tables with some real-life examples of threats.



The name of the threats indicated here can vary among different security vendors. You should use the hash ID to identify specific malware.

### 14.4.1 Example 1: viewing the actions executed by the malware Trj/OCJ.A

The **Details** tab shows the key information about the malware found. In this case the important data is as follows:

- **Threat:** trj/OCJ.A
- **Computer:** XP-BARCELONA1
- **Detection path:** TEMP|\Rar\$EXa0.946\appnee.com.patch.exe

#### Activity

The **Activity** tab shows some actions. This is because **Adaptive Defense** was configured in **Hardening** mode and the malware already resided on the computer when **Adaptive Defense** was installed. The malware was unknown at the time of running.

#### Hash

Use the hash string to obtain more information on sites such as VirusTotal to get a general idea of the threat and how it works.

#### Detection path

The path where the malware was detected for the first time on the computer belongs to a temporary directory and contains the RAR string. Therefore, the threat comes from a RAR file temporarily uncompressed in the directory, and which gave the appnee.com.patch.exe executable as the result.

#### Activity tab

Step	Date	Action	Path
1	3:17:00	Is created by	PROGRAM_FILES \WinRAR\WinRAR.exe
2	3:17:01	Is run by	PROGRAM_FILES \WinRAR\WinRAR.exe
3	3:17:13	Creates	TEMP \bassmod.dll
4	3:17:34	Creates	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifies	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Deletes	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
7	3:17:41	Creates	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifies	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll

Step	Date	Action	Path
9	3:17:59	Runs	PROGRAM_FILES  \Google\ Chrome\Application\chrome.exe

Table 38: list of actions performed by Trj/OCJ.A

Steps 1 and 2 indicate that the malware was uncompressed by WinRar.Exe and run from that program. The user opened the compressed file and clicked its binary.

Once run, in step 3 the malware created a DLL file (bassmod.dll) in a temporary folder, and another one (step 4) in the installation directory of the Adobe Acrobat 11 program. In step 5, it modified an Adobe DLL file, to take advantage perhaps of a program vulnerability.

After modifying other DLL files, it launched an instance of Google Chrome which is when the timeline finishes. **Adaptive Defense** classified the program as a threat after that string of suspicious actions and stopped its execution.

The timeline shows no actions on the registry, so it is very likely that the malware is not persistent or wasn't able to modify the registry to ensure it could survive a computer restart.

The software Adobe Acrobat 11 was compromised so a reinstall is recommended. Thanks to the fact that **Adaptive Defense** monitors both goodware and malware executables, the execution of a compromised program will be detected as soon as it triggers dangerous actions, and ultimately be blocked.

#### 14.4.2 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, injecting ads in the Web pages they visit.

The **Details** tab shows the key information about the malware found. In this case it shows the following data:

- **Name:** PUP/BetterSurf
- **Computer:** MARTA-CAL
- **Detection path:** PROGRAM\_FILES| \VER0BLOCKANDSURF\N4CD190.EXE
- **Dwell time:** 11 days 22 hours 9 minutes 46 seconds

#### Dwell time

In this case, the dwell time is very long: the malware remained dormant on the customer's network for almost 12 days. This is increasingly normal behavior and may be for various reasons. For example, the malware did not carry out any suspicious actions until very late, or the user downloaded the file but did not run it at the time. In both cases, the threat was unknown to the security service, so there was no malware signature to compare it to.

### Activity tab

Step	Date	Action	Path
1	03/08/2015 11:16	Is created by	SMTP, 08c3b650, e9e14f.exe
2	03/18/2015 11:16	Is run by	SYSTEM   \services.exe
3	03/18/2015 11:16	Loads	PROGRAM_FILES   \VER0BLOF\N4Cd190.dll
4	03/18/2015 11:16	Loads	SYSTEM   \BDL.dll
5	03/18/2015 11:16	Communicates with	127.0.0.1/13879
6	03/18/2015 11:16	Communicates with	37.58.101.205/80
7	03/18/2015 11:17	Communicates with	5.153.39.133/80
8	03/18/2015 11:17	Communicates with	50.97.62.154/80
9	03/18/2015 11:17	Communicates with	50.19.102.217/80

Table 39: list of actions performed by PUP/BetterSurf

In this case you can see how the malware communicated with different IP addresses. The first address (step 5) is the infected computer itself, and the rest are external IP addresses to which it connected via port 80 and from which the advertising content was probably downloaded.

The main preventive measure in this case should be to block those IP addresses in the corporate firewall.



*Before adding rules to block IP addresses in the corporate firewall, you should consult those IP addresses in the associated RIR (RIPE, ARIN, APNIC, etc.) to see the network to which they belong. In many cases, the remote infrastructure used by malware is shared with legitimate services housed in providers such as Amazon and similar, so blocking certain IP addresses would be the same as blocking access to legitimate Web pages.*

#### 14.4.3 Example 3: access to the registry by PasswordStealer.BT

PasswordStealer.BT is a Trojan that logs the user's activity on the infected computer and sends the information obtained to an external server. Among other things, it captures screens, records keystrokes and sends files to a C&C (Command & Control) server.

The **Details** tab shows the key information about the malware found. In this case it shows the following data:

- **Detection path:** APPDATA | \microsoftupdates\micupdate.exe

The name and location of the executable file indicate that the malware poses as a Microsoft update. This particular malware cannot infect computers by itself; it requires the user to run it manually.

### Activity tab


The **Activity** tab shows some actions. This is because **Adaptive Defense** was configured in **Hardening** mode and the malware already resided on the computer when **Adaptive Defense** was installed. The malware was unknown at the time of running.

### Action table

Step	Date	Action	Path
1	03/31/2015 23:29	Is run by	PROGRAM_FILESX86   \internet explorer\iexplore.exe
2	03/31/2015 23:29	Is created by	INTERNET_CACHE   \Content.IE5\ QGV8PV80\ index[1].php
3	03/31/2015 23:30	Creates key pointing to Exe file	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\CurrentVersion\Run?MicUpdate
4	03/31/2015 23:30	Runs	SYSTEMX86   \notepad.exe
5	03/31/2015 23:30	Thread injected by	SYSTEMX86   \notepad.exe

Table 40. List of actions performed by PasswordStealer.BT

In this case, the malware was generated in step 2 by a Web page and run by Internet Explorer.



*The order of the actions has a granularity of 1 microsecond. For this reason, the actions executed within the same microsecond may not appear in order in the timeline, as in step 1 and step 2.*

Once run, the malware became persistent in step 3, adding a branch to the Windows registry in order to run every time the computer started up. It then started to execute typical malware actions such as opening the notepad and injecting code in one of its threads.

As a remedial action in this case and in the absence of a known disinfection method, you could minimize the impact of the malware by deleting the malicious registry entry. However, it is quite possible that the malware might prevent you from modifying that entry on infected computers; In that case, you would have to either start the computer in safe mode or with a bootable CD to delete the entry.

### Example 4: access to confidential data by Trj/Chgt.F

Trj/Chgt.F was uncovered by WikiLeaks at the end of 2014 as a tool used by government agencies in some countries for selective espionage.

In this example, we'll go directly to the **Activity** tab to show you the behavior of this advanced threat.

### Action table

Step	Date	Action	Path
1	4/21/2015 2:17:47 PM	Is run by	SYSTEMDRIVE \Python27\pythonw.exe
2	4/21/2015 2:18:01 PM	Accesses data	#.XLS
3	4/21/2015 2:18:01 PM	Accesses data	#.DOC
4	4/21/2015 2:18:03 PM	Creates	TEMP \doc.scr
5	4/21/2015 2:18:06 PM	Runs	TEMP \doc.scr
6	4/21/2015 2:18:37 PM	Runs	PROGRAM_FILES \Microsoft Office\Office12\WINWORD.EXE
7	4/21/2015 8:58:02 PM	Communicates with	192.168.0.1/2042

Table 41. List of actions performed by Tj/Chgt.F

The malware was initially run by the Python interpreter (step 1), and later accessed an Excel file and a Word document (steps 2 and 3). In step 4, a file with an `scr` extension was run, probably a screensaver with some type of flaw or error that could be exploited by the malware.

In step 7 the malware established a TCP connection. The IP address is private, so the malware connected to the customer's own network.

In a case like this it is important to check the content of the files accessed by the threat in order to assess the loss of information. However, the timeline of this particular attack shows that no information was extracted from the customer's network.

**Adaptive Defense** disinfected the threat, and automatically prevented all subsequent executions of the malware for this and other customers.

# 15. Remediation tools

---

- On-demand file disinfection
- Computer restart
- Disinfection tasks
- Reporting computer problems
- External access to the console

## 15.1. Introduction

**Adaptive Defense** provides remediation tools that allow administrators to resolve the issues found in the Protection, Detection and Monitoring phases of the adaptive protection cycle.

## 15.2. On-demand computer disinfection

### 15.2.1 How on-demand disinfection works

On-demand disinfection looks for malware in the following areas of the scanned computer:

- Memory
- Internal storage devices
- Storage devices physically connected to the computer (USB drives and other data repositories)

Additionally, the predetermined action taken by the scan process is:

- Disinfectable files: infected files are replaced with a clean version.
- Non-disinfectable files: they are deleted and a backup copy is moved to quarantine.

### 15.2.2 Characteristics of on-demand disinfection tasks

- Maximum run time: unlimited
- Task start:
  - If the target computer is turned on, the task will start as soon as it is launched
  - If the target computer is turned off, the task will be postponed until the computer becomes available within the next 7 days

### 15.2.3 Creating on-demand disinfection tasks

To disinfect a computer on demand, you must create an immediate disinfection task.

There are two ways to create a disinfection task from the management console:

- From the **Computers** menu at the top of the console
- From a computer's **Details** tab

#### Disinfecting computers from the Computers menu

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- To disinfect a single computer, click the computer's context menu on the computer list **(1)**.



- To disinfect multiple computers, use the checkboxes to select the computers to scan **(3)**, and click the global context menu **(2)**.
- Select the option **Disinfect** from the drop-down menu.

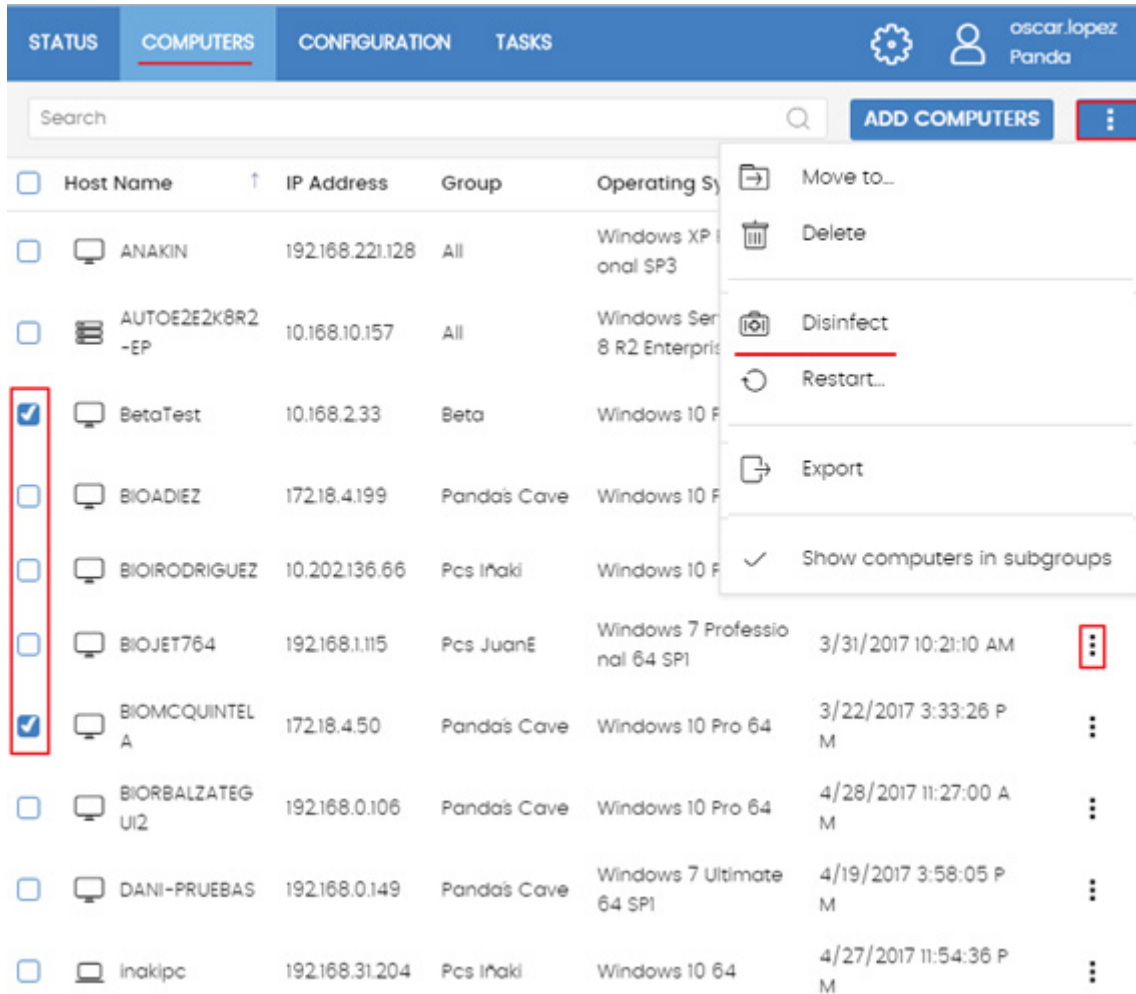


Figure 92: creating a disinfection task from the Computers menu

### Disinfecting computers from the Computer details screen

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- Click the computer to scan to view the **Details** screen.
- From the context menu, select **Disinfect**.



Figure 93: disinfecting a computer from the Computer details screen

### 15.3. Managing disinfection tasks

The **Tasks** menu at the top of the console allows administrators to view the results of the disinfection tasks launched, as well as cancel and delete them.

#### Canceling a disinfection task

To cancel a disinfection task that has already been launched, click the **Cancel** link. The task will be canceled, but it won't disappear from the task window so that you can still view its results.

#### Deleting disinfection tasks

Only canceled tasks can be deleted. Click the  icon to remove a canceled task from the list of tasks.



#### Viewing task results

You can view the current results of any published task by clicking the **View results** link. A window with the results will appear, along with some filters for you to search for specific information.

Table 42 shows the fields in the task table:

Field	Comment	Values
Computer	Name of the computer where the disinfection event took place	Character string
IP address	The computer's primary IP address	Character string
Status	<b>Pending:</b> the task tried to launch the scan, but the target computer was not accessible. There is a wait period of 7 days <b>In progress:</b> the scan is underway <b>Success:</b> the scan finished successfully <b>Failed:</b> the scan failed, returning an error <b>Expired:</b> the task didn't even start as the 7-day wait period expired <b>Canceled:</b> the task was manually canceled	Character string
Start date	Scan start date	Date
End date	Scan end date	Date
Detections	Number of detections made on the computer	Numeric value

Table 42: filtering parameters for task results

Table 43 displays the available search filters:

Field	Comment	Values
Date	Drop-down menu with the date when the task became 'Active'. An active task will launch a scan immediately, or wait until the target machine is available. This date is specified in the Date column.	Date
Detections	Lets you specify whether to display computers with detections or clean computers.	Binary value
Status	<b>Pending:</b> the task has not been run yet as the target computer is unavailable <b>In progress:</b> the scan is underway <b>Success:</b> the scan finished successfully <b>Failed:</b> the scan failed and returned an error <b>Canceled:</b> the task was manually canceled	Enumeration

Table 43: task search filters

## 15.4. Computer restart

The Web console lets administrators restart computers remotely. This is very helpful if you have computers whose protection needs updating or if there are protection problems to fix.

- Go to the **Computers** menu at the top of the console and select a computer using the left-hand panel.
- To restart a single computer, click the computer's context menu on the computer list.

- To restart multiple computers, use the checkboxes to select the computers to restart, and click the global context menu.
- From the drop-down menu, select **Restart**.

### 15.5. Reporting a problem

It is possible that the **Adaptive Defense** software may occasionally function incorrectly. Some symptoms could include:

- Errors reporting the computer status.
- Errors downloading knowledge or engine updates.
- Engine errors.

If **Adaptive Defense** functions incorrectly on some network computers, you can contact Panda Security's support department through the console and automatically send all the information required for diagnosis. To do this, click **Computers**, select the computers with errors, and click the context menu. A menu will appear entitled **Report a problem**.

### 15.6. Allowing external access to the Web console

If the administrator finds problems they can't resolve, they can grant Panda Security's support team access to their console. Follow the steps below:

- Click the **Settings** menu at the top of the console. Then, click **Users** from the side menu.
- On the **Users** tab, click **Allow the Panda Security S.L. team to access my console**

# 16. Alerts

---

Email alerts

## 16.1. Introduction

The alert system is a tool provided by **Adaptive Defense** to quickly notify administrators of important situations to ensure the proper operation of the security service.

Namely, an alert will be sent to the administrator every time one of the following events occur:

- A malware specimen, PUP or exploit is detected
- An unknown item (malware or PUP) is reclassified
- A process unknown to **Adaptive Defense** is blocked while it is being classified
- There is a change in the license status
- There are install errors or a computer is unprotected

## 16.2. Email alerts

Email alerts are messages sent by **Adaptive Defense** to the administrator's email account. As previously explained, the system will send a message to the configured recipients' email accounts when certain events occur.

### 16.2.1 Configuring email alerts

Go to the **Settings** menu at the top of the Web console. Then click **Alerts** from the left-hand menu.

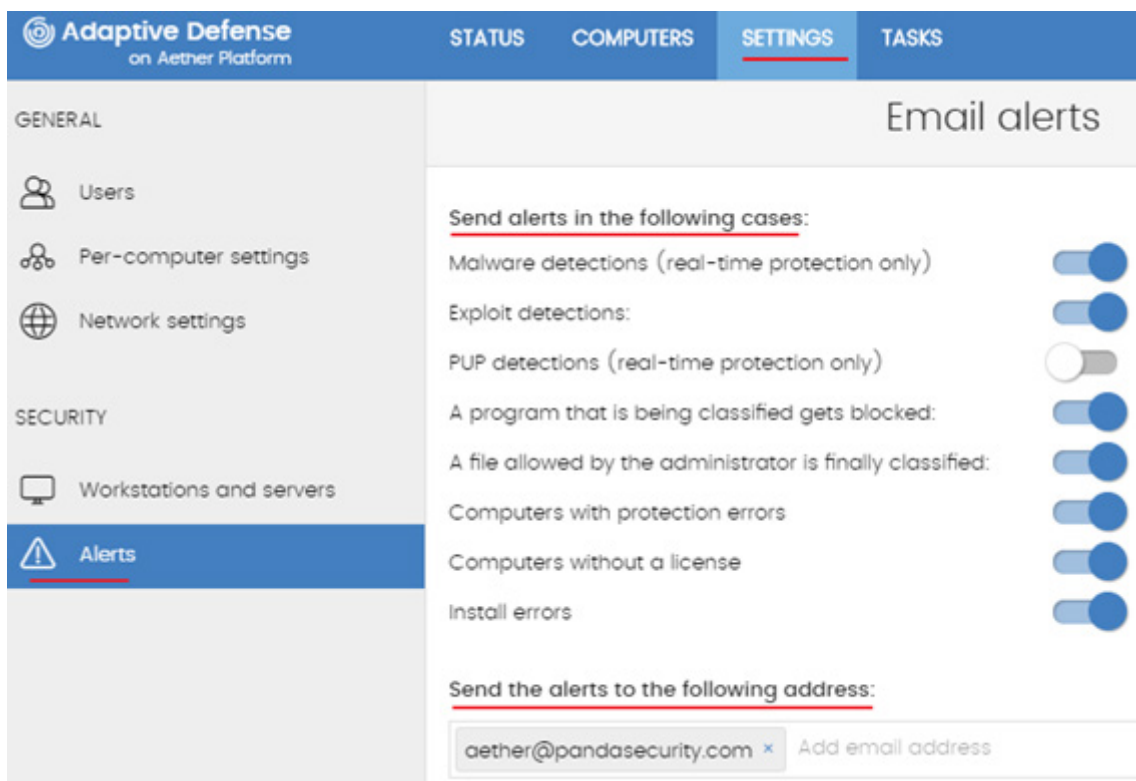


Figure 94: alert settings screen

This screen lets administrators specify the email addresses to send messages to (**Send the alerts to the following address:**). You can also enable and disable each of the alert types to send.

## 16.2.2 Access permissions and alerts

Alerts are defined independently for each user of the Web console. The contents displayed in an alert will vary depending on the managed computers that are visible to the recipient's role.

## 16.2.3 Alert types

### Malware/PUP detections (real-time protection only)

These alerts have the following characteristics:

- An alert is generated in real time for each malware detected on a computer on the network.
- A maximum of two messages will be sent per computer/malware/day.

The alert message will contain the following information:

- Whether it is the first or second message generated for that threat/computer/day.
- Name of the malicious program.
- Name of the computer where the item was detected.
- Group to which the computer belongs.
- Detection date and time (in UTC format).
- Path of the malicious program.
- Hash.
- Actions taken by the program (life cycle), if it managed to run before being blocked.
- Occurrences on the network: list of computers where the malware was found.

### Exploit detections

These alerts have the following characteristics:

- An alert is generated for each exploit attempt detected, without limitations.
- There is a maximum of 10 alerts per day/computer/exploit.

The alert message will contain the following information:

- Name, path and hash of the program that was hit by the exploit attempt
- Name of the computer where the exploit attempt was detected
- Group to which the computer belongs

- Detection date and time (in UTC format)
- Action taken by **Adaptive Defense**
- Computer risk level
- Assessment of the target program's security level
- Actions taken by the exploit (life cycle), if it managed to run before being blocked
- Possible source of the exploit

### Alerts generated when a program that is being classified gets blocked

These alerts have the following characteristics:

- An alert is generated in real time for each unknown program detected in the file system.

The alert message will contain the following information:

- Name of the unknown program.
- Name of the computer where the item was detected.
- Group to which the computer belongs
- Detection date and time (in UTC format).
- Path of the unknown program.
- Hash.
- Actions taken by the program (life cycle), if it managed to run before being blocked.
- Occurrences on the network: list of computers where the unknown program was found.

### Alerts generated when a file allowed by the administrator is finally classified

Administrator-allowed files are those files which the administrator has allowed to run despite being blocked by **Adaptive Defense** for being unknown or having been categorized as a threat. As soon as **Adaptive Defense** finishes classifying a previously unknown item, it will inform the administrator of its verdict, as this will affect the action to be taken on the item (allow or block), depending on the reclassification policy defined by the administrator.



*Refer to chapter 13 Managing threats, quarantined items and items being classified, for more information about reclassification policies*

- **Alert generated when an unknown item is finally classified as goodware**

The system will generate an alert every time an unknown item that was allowed to run by the administrator is finally classified. And, depending on the verdict, the administrator's exclusion will be



kept or removed based on the selected reclassification policy. In the case of goodware items, the exclusion will be automatically removed by the system and the item will be allowed to continue running.

- **Alert generated when an unknown item is reclassified as malware/PUP**

The system will generate an alert every time an unknown item that was allowed to run by the administrator is finally classified. And, depending on the verdict, the administrator's exclusion will be kept or removed based on the selected reclassification policy. If the item is classified as malware/PUP and the exclusion is kept, the item will continue to be allowed to run, posing a threat to the system. If, however, the exclusion is removed, the item will be prevented from running, rendering it harmless to the organization.

### Protection and install errors

These alerts have the following characteristics:

- An alert is generated for each unprotected computer found on the network
- An alert is generated for each computer with a protection or install error

The alert message will contain the following information:

- Name of the unprotected computer
- Group to which the computer belongs
- Computer information (name, description, operating system, IP address, group, Active Directory path, domain)
- Detection date and time (in UTC format)
- Reason: **protection with errors** or **Install error**

### Computers without a license

These alerts have the following characteristics:

- An alert is generated every time the solution fails to assign a license to a computer due to lack of sufficient free licenses

The alert message will contain the following information:

- Name of the unprotected computer
- Group to which the computer belongs
- Computer information (name, description, operating system, IP address, group, Active Directory path, domain)

- Detection date and time (in UTC format)
- Reason: **computer without a license**

Additionally, an alert will also be generated under the following circumstances:

- Every time a license contract expires

The alert message will contain the following information:

- Number of computers that are left without a license
- Number of expired licenses
- Product whose licenses have expired
- License contract expiration date

# 17. Reports

---

On-demand generation of executive reports  
Scheduled sending of executive reports

## 17.1. Introduction

**Adaptive Defense** allows administrators to generate and send, automatically or manually, executive reports that consolidate all the information collected by the solution in the selected period.

## 17.2. On-demand generation of executive reports

Go to the **Status** menu at the top of the console, and click the **Executive report** option from the left-hand menu. This will open the report settings window. This window is divided into two tabs: **view** and **Schedule**. Click the **View** tab to configure the executive report to display.

### 17.2.1 Information required to generate an on-demand report

The following information will be required:

- **Information for the following dates:** specify the time interval to be covered by the report
  - **Last month**
  - **Last 7 days**
  - **Last 24 hours**
- **Information for the following computers:** specify the computers to extract information from
  - **All computers**
  - **Selected computers:** displays the group tree. Use the checkboxes to select the groups you want
- **Include the following content:** lets you select the type of information to be included in the report
  - **License status:** shows the number of contracted and used licenses. For more information, refer to chapter 5 Licenses
  - **Network status:** shows the way the **Adaptive Defense** software is working on those computers where it is installed. It includes information from the following dashboard widgets: **unprotected computers** and **Outdated protection**. For more information, refer to chapter 13 Malware and network visibility.
  - **Detections:** shows the threats detected across the network. It includes information from the following dashboard widgets: **malware activity** and **PUP activity**. For more information, refer to chapter 13 Malware and network visibility.

Once you have finished configuring the settings, click the **View** button to display the report in a new window.




*Check that neither your Internet browser nor any installed extension blocks the display of pop-ups*

### 17.3. Scheduled sending of executive reports

Go to the **Status** menu at the top of the console, and click the **Executive report** option from the left-hand menu. This will open the report settings window. This window is divided into two tabs: **view** and **Schedule**. Click the **Schedule** tab to configure a scheduled executive report.

#### 17.3.1 Information required to generate a scheduled report

The scheduled reports window displays a list of all configured reports. Click **Add** to add a new scheduled report. To delete a configured report, click the  icon. To edit a configured report, click its name.

To configure a scheduled report, enter the following information:

- **Name:** name of the scheduled report that will be displayed on the list of configured reports.
- **Send automatically:** lets you schedule the sending of the executive report, or save the settings without sending the report.
- **Date and frequency:** lets you specify the day when the report will be sent and its frequency. Select **Every day**, **Every week** or **Every month**. The content of the drop-down menus will vary depending on your selection.
- **The following information:** this section displays the following settings: **dates**, **Computers** and **Content**. Click the arrow to the right to configure the following options:
  - **Information for the following dates:** specify the time interval to be covered by the report
    - **Last month**
    - **Last 7 days**
    - **Last 24 hours**
  - **Information for the following computers:** specify the computers to extract information from
    - **All computers**
    - **Selected computers:** displays the group tree. Use the checkboxes to select the groups you want
  - **Include the following content:** lets you select the type of information to be included in the report
    - **License status:** shows the number of contracted and used licenses. For more information, refer to chapter 5 Licenses
    - **Network status:** shows the way the **Adaptive Defense** software is working on those computers where it is installed. It includes information from the following dashboard widgets: **unprotected computers** and **Outdated protection**.
    - **Detections:** shows the threats detected across the network. It includes information from the following dashboard widgets: **malware activity** and **PUP activity**.
- **To:** enter the email address that the report will be sent to. You can enter multiple addresses separated by commas.
- **CC:**

- **BCC:** use this field to send a copy of the report to a recipient without notifying other recipients that this was done.
- **Subject:** specify the email subject line.
- **Format:** select the format of the email attachment (the report): pDF, Excel, or Word.
- **Language:** select the language of the report.

# 18. Controlling and monitoring the management console

---

What is a user account?

What is a role?

What is a permission?

Accessing the user account and role settings

Creating and configuring user accounts

Creating and configuring roles

Activity log

## 18.1. Introduction

This chapter describes the resources implemented in **Adaptive Defense** to control and monitor the actions taken by the network administrators that access the Web management console.

These resources are as follows:

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

## 18.2. What is a user account?

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

User accounts are only used by the administrators that access the **Adaptive Defense** console. In general, each administrator will have a unique personal account, and it is possible to create as many accounts as necessary.



*Unlike the rest of this manual, where the word "user" refers to the person that uses a computer or device, in this chapter "user" refers to the account used by the administrator to access the Web console*

### 18.2.1 User account structure

A user account comprises the following items:

- **Account login name:** this is assigned when the account is created and the aim is to identify the administrator accessing the account.
- **Account password:** this is assigned once the account is created and is designed to control access to the account.
- **Assigned role:** this can be selected once the user account is created. It lets you determine which computers the account user will be able to manage and the action they will be able to take.

### 18.2.2 What is the main user?

The main user is the user account provided by Panda Security to the customer when providing the **Adaptive Defense** service. This account has the **Full control** role, which is explained below.

The settings of the main user cannot be edited or deleted.



### 18.3. What is a role?

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

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

#### 18.3.1 Role structure

A role is made up of the following:

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

#### 18.3.2 Why are roles necessary?

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

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

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

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

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

Depending on its purpose, a computer may be assigned to a technician specialized in the relevant field. For example, file servers may be assigned to a group of specialized technicians.

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

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

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

### 18.3.3 Full Control role

The **Adaptive Defense** license comes with the **Full Control** role predefined. The default administration account belongs to this role, and with this it is possible to take almost all actions that are available in the console.

The **Full Control** role cannot be deleted, edited or viewed, and any user account can belong to this role if it is assigned through the console.

### 18.3.4 Monitoring role

The **Monitoring role** is especially designed for network administrators responsible for monitoring networks, but without sufficient permissions to take actions such as editing settings or launching on-demand scans.

The permissions enabled in the **Monitoring role** are as follows:

- View security settings for workstations and servers.
- View detections and threats.
- Access to advanced reports

## 18.4. What is a permission?

A permission regulates access to a particular aspect of the management console. There are 15 types of permissions that provide access to many aspects of the **Adaptive Defense** console. A specific configuration from all available permissions generates a role, which can be assigned to one or more user accounts.

The **Adaptive Defense** permissions are as follows:

- Manage users and roles
- Assign licenses

- Modify computer tree
- Add, discover and delete computers
- Configure proxies and language
- Modify per-computer settings (updates, passwords, etc.)
- Restart computers
- Configure security settings for workstations and servers
- View security settings for workstations and servers
- View detections and threats
- Access to Advanced Reporting Tool
- Disinfect computers
- Exclude threats temporarily (malware, PUPs and blocked items)

### 18.4.1 Understanding permissions

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

#### Manage users and roles

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

#### Assign licenses

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

#### Modify the computer tree

- **Enabled:** the account user has complete access to the Groups tree, and can create and delete groups, as well as move computers to groups that have been created.
- **Disabled:** the account user can view the Groups tree and the settings assigned to each group, but cannot create new groups or move computers. They can change the group settings, as this action is governed by the permission **Configure security settings for workstations and servers**.

#### Add, discover and delete computers

- **Enabled:** the account user can distribute the installer to their network computers and integrate them into the **Adaptive Defense** console. They can also delete computers from the console and configure all aspects related to the discovery of unmanaged computers: assign and revoke the 'discovery computer' role, edit discovery settings, launch an immediate discovery task, and install the Panda agent remotely from the list of discovery computers.
- **Disabled:** the account user cannot download the installer, nor distribute it to computers. They cannot delete computers from the console or access the computer discovery feature.

### Configure proxies and languages

- **Enabled:** the account user can create new **Proxy and language** settings, edit or delete existing ones and assign them to computers in the console.
- **Disabled:** the account user cannot create new **Proxy and language** settings, nor edit or delete existing ones.



*Given that moving a computer in the Groups tree can change the assigned Proxy and language settings, when you disable Configure Proxies and languages you also have to disable the permission Modify Groups tree.*

### Modify per-computer settings (updates, passwords, etc.)

- **Enabled:** the account user can create new **Per-computer settings**, edit or delete existing ones and assign them to computers in the console.
- **Disabled:** the account user cannot create new **Per-computer settings**, nor edit or delete existing ones.



*Given that moving a computer in the Groups tree can change the assigned Per-computer settings, when you disable Modify per-computer settings you also have to disable the permission Modify Groups tree.*

### Restart computers

- **Enabled:** the account user can restart computers by going to the **Computers** menu and selecting **Restart** from the context menu (workstations and servers).
- **Disabled:** the account user cannot restart computers.

### Configure security settings for workstations and servers

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



*Given that moving a computer in the Groups tree can change the assigned Workstations and servers settings, when you disable Configure security for workstations and servers you also have to disable the permission Modify Groups tree.*

When you disable this permission, you will see the permission **View security settings for workstations and servers**.

## View security settings for workstations and servers



*This permission can only be accessed when you disable **Configure security for Workstations and servers**.*

- **Enabled:** the account user can only see the security settings created as well as the settings of a computer or group.
- **Disabled:** the account user won't be able to see the security settings created nor access the settings assigned to each computer.

## View detections and threats

- **Enabled:** the account user will be able to see the panels and lists in the **Security** section of the **Status** menu, and create new lists with custom filters.
- **Disabled:** the account user won't be able to see the panels and lists in the **Security** section of the **Status** menu, nor create new lists with custom filters.



*Access to features related to excluding and unblocking threats and unknown items is determined through the permission **Exclude threats temporarily (Malware, PUPs and blocked items)**.*

## Access to Advanced Reporting Tool

- **Enabled:** the account user will be able to access the **Advanced Reporting Tool** section from the panel on the left in the **Status** menu.
- **Disabled:** access to the **Advanced Reporting Tool** section is hidden.

## Disinfect computers

- **Enabled:** the account user will be able to launch immediate disinfection tasks.
- **Disabled:** the account user won't be able to launch immediate disinfection tasks, nor interrupt immediate disinfection tasks already in progress. They can only view the immediate disinfection tasks launched.

## Exclude threats temporarily (Malware, PUPs and blocked items)

- **Enabled:** the account user can unblock, prevent detection, block, not allow and change the behavior with respect to reclassified malware, PUPs and unknown items in the process of classification.
- **Disabled:** the account user won't be able to unblock, prevent detection, block, not allow or change the behavior with respect to reclassified malware, PUPs and unknown items in the process of classification



*It is necessary to enable **View detections and threats** in order to fully implement **Exclude threats temporarily (Malware, PUPs, and blocked items)**.*

## 18.5. Accessing the user account and role settings

In the **Settings** menu, when you click the **Users** panel, there are two sections associated with the management of roles and user accounts:

- **Users:** this lets you create new user accounts and define the roles they belong to.
- **Roles:** this lets you create and edit settings for accessing **Adaptive Defense** resources.

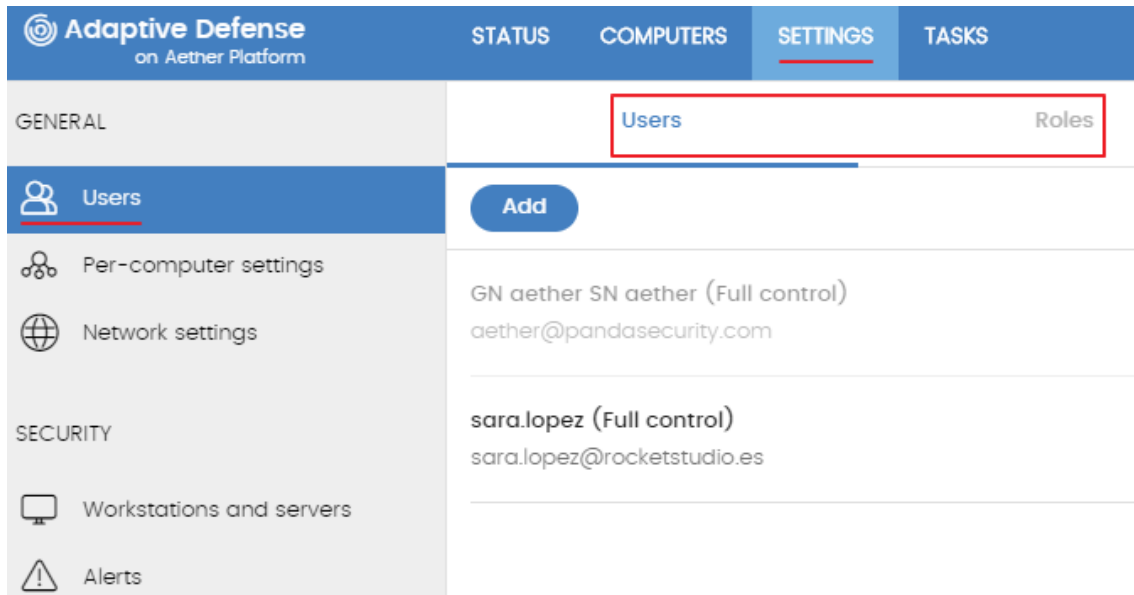



Figure 95: accessing the role and user settings

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



## 18.6. Creating and configuring user accounts

In the **Settings** menu, in the panel on the left, click **Users** and then the tab **Users** and you will be able to take all necessary actions related to the creation and editing of user accounts.

- **Add new user account:** click **Add** to add a new user, set the email account for accessing the account, the role to which it belongs, and a description of the account. The system will send an email to the account to generate the login password.
- **Edit a user account:** click the name of the user to display a window with all the account details that can be edited.
- **Delete or disable user accounts:** click the  icon of a user account to delete it. Click a user account and select the button **Block this user** to temporarily block access to the Web console from this account. If the account is currently logged in it will be blocked immediately.

## 18.7. Creating and configuring roles

In the **Settings** menu, click **Users** in the left-hand panel and then **Roles**, and you will be able to take all necessary actions related to the creation and editing of roles.

- **Add new role:** click **Add**. You will be asked for the name of the role, a description (optional), to select from the available computers, and a specific configuration of permissions.
- **Edit a role:** click the name of the role to display a window with all the settings that can be edited.
- **Copy a role:** click the  icon to display a window with a new role with exactly the same settings as the original one.
- **Delete role:** click the  icon of a role to delete it. If, when you delete a role, it already has user accounts assigned, the process of deleting it will be canceled.

## 18.8. User account activity log

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

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

### 18.8.1 Action log

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

#### Fields displayed in the Actions list

Field	Comment	Values
Date	Date and time that the action was carried out	Date
User	User account that performed the action	Character string
Action	Type of action	Access Add scheduled report Assign license Block Delete Change 'Per-computer settings' Change 'Security settings' Change group Change parent group Change 'Proxy and language' Cancel Configure discovery Create

		Unassign license Stop allowing Unblock Discover now Designate cache computer Designate discovery computer Designate Panda proxy Edit Edit description Edit scheduled report Edit name Delete Delete scheduled report Inherit 'Per-computer settings' Inherit 'Security settings' Inherit 'Proxy and language' Install Locate Move to Active Directory path Move computers to their Active Directory path Hide Allow Publish Restart computers Restore communications Revoke cache computer Revoke discovery computer Revoke Panda proxy Sync group Make visible
<b>Item type</b>	Type of console object the action was performed on	Threat Settings Android device Computer Unmanaged computer Filter Group Device group Executive report Advanced reports List Preference for sending emails Role Task - Security scan User
<b>Item</b>	Console object the action was performed on	Character string

Table 44: fields in the Action log

**Fields displayed in the exported file**

Field	Comment	Values
<b>Date</b>	Date and time that the action was carried out	Date
<b>User</b>	User account that performed the action	Character string



Field	Comment	Values
Action	Type of action	Access Add scheduled report Assign license Block Delete Change 'Per-computer settings' Change 'Security settings' Change group Change parent group Change 'Proxy and language' Cancel Configure discovery Create Unassign license Stop allowing Unblock Discover now Designate cache computer Designate discovery computer Designate Panda proxy Edit Edit description Edit scheduled report Edit name Delete Delete scheduled report Inherit 'Per-computer settings' Inherit 'Security settings' Inherit 'Proxy and language' Install Locate Move to Active Directory path Move computers to their Active Directory path Hide Allow Publish Restart computers Restore communications Revoke cache computer Revoke discovery computer Revoke Panda proxy Sync group Make visible
Item type	Type of console object the action was performed on	Threat Settings Android device Computer Unmanaged computer Filter Group Device group Executive report Advanced reports List Preference for sending emails Role Task - Security scan User

Field	Comment	Values
Item	Console object the action was performed on	Character string

Table 45: fields in the 'Action log' exported file

### Filter tool

Field	Comment	Values
From		Date
To		Date
Users		List of all user accounts that have been created in the management console

Table 46: filters available in the Action log

## 18.8.2 Session log

The **Sessions** section displays a list of all accesses to the management console, and allows you to export the information to an Excel file and filter the information.

### Fields displayed in the Sessions list

Field	Comment	Values
Date	Date and time that the access took place	Date
User	User account that accessed the console	Character string
Activity		Log in Log out
IP address	IP address from which the console was accessed	Character string

Table 47: fields in the Sessions list

### Fields displayed in the exported file

Field	Comment	Values
Date	Date and time that the access took place	Date
User	User account that accessed the console	Character string
Activity		Log in Log out
IP address	IP address from which the console was accessed	Character string

Table 48: fields in the 'Sessions' exported file

**Filter tool**

Field	Comment	Values
From		Date
To		Date
Users		List of all user accounts that have been created in the management console

*Table 49: filter fields in the Sessions list*

# 19. Appendix 1: adaptive Defense requirements

---

Windows platforms  
Web console access  
Access to service URLs

## 19.1. Requirements for Windows platforms

### 19.1.1 Supported operating systems

#### Workstations

- Windows XP SP3 (32 bits)
- Windows Vista (32 and 64-bit)
- Windows 7 (32 and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)

#### Servers

- Windows 2003 (32-bit, 64-bit and R2) SP2 and later
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 and 2016

### 19.1.2 Hardware requirements

- Processor: pentium 1 GHz
- RAM: 1 GB
- Free space disk for the installation: 650 MB

## 19.2. Web console access

The **Adaptive Defense** management console can be accessed with the latest version of the following compatible browsers.

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

### 19.3. Access to service URLs

For **Adaptive Defense** to work correctly, the protected computers must be able to access the following URLs.

- [https://\\*.pandasecurity.com](https://*.pandasecurity.com)
- [http://\\*.pandasecurity.com](http://*.pandasecurity.com)
- [https://\\*.windows.net](https://*.windows.net)
- <https://pandasecurity.logtrust.com>
- [http://\\*.pandasoftware.com](http://*.pandasoftware.com)

#### **Inbound and outbound traffic (anti-spam and URL filtering)**

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

#### **Ports**

- Port 80 (HTTP, WebSocket)
- Port 443 (HTTPS)

# 20. Appendix 2: creating and managing a Panda Account

---

Creating a Panda Account  
Activating your Panda Account

## 20.1. 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** Web console.

## 20.2. 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**, you will receive an email message from Panda Security.
- Click the link in the message to access a site from which you will be able to create your Panda Account.

### Fill out the form

- Fill out the form with the relevant data.
- Use the drop-down menu in the bottom-right corner if you want to change the language of the form.
- You can view the license agreement and privacy policy by clicking the corresponding links.
- Click **Create** to receive a message at the email address entered in the form. Follow the instructions in that message to activate your account.

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

# 21. Appendix 3: list of uninstallers

---

On installing **Adaptive Defense**, other security products might be detected on the computer. In that case,

Table 50 shows the products that will be automatically uninstalled before installing **Adaptive Defense** across the network.

Vendor	Product name
Computer Associates	eTrust AntiVirus 8.1.655, 8.1.660, 7.1* eTrust 8.0
Avast	Avast! Free Antivirus 2014 Avast! 8.x Free Antivirus Avast! 7.x Free Antivirus Avast! 6.x Free Antivirus Avast! 5.x Free Antivirus Avast! 4 Free Antivirus Avast! 4 Small Business Server Edition Avast! 4 Windows Home Server Edition 4.8
AVG	AVG Internet Security 2013 (32bit- Edition) AVG Internet Security 2013 (64bit- Edition) AVG AntiVirus Business Edition 2013 (32bit- Edition) AVG AntiVirus Business Edition 2013 (64bit- Edition) AVG CloudCare 2.x AVG Anti-Virus Business Edition 2012 AVG Internet Security 2011 AVG Internet Security Business Edition 2011 32bits* AVG Internet Security Business Edition 2011 64bits (10.0.1375)* AVG Anti-Virus Network Edition 8.5* AVG Internet Security SBS Edition 8 Anti-Virus SBS Edition 8.0 AVGFree v8.5, v8, v7.5, v7.0
Avira	Avira AntiVir PersonalEdition Classic 7.x, 6.x Avira AntiVir Personal Edition 8.x Avira AntiVir Personal - Free Antivirus 10.x, 9.x Avira Free Antivirus 2012, 2013 Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x Avira Antivirus Premium 2013, 2012, 10.x, 9.x
CA	CA Total Defense for Business Client V14 (32bit- Edition) CA Total Defense for Business Client V14 (64bit- Edition) CA Total Defense R12 Client (32bit- Edition) CA Total Defense R12 Client (64bit- Edition)
Bitdefender	BitDefender Endpoint Protection 6.x BitDefender Business Client 11.0.22 BitDefender Free Edition 2009 12.0.12.0* Bit Defender Standard 9.9.0.082
Check Point	Check Point Endpoint Security 8.x (32 bits) Check Point Endpoint Security 8.x (64 bits)
Eset	ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7* ESET Smart Security 3.0* ESET Smart Security 5 (32 bits) ESET NOD32 Antivirus 4.X (32 bits) ESET NOD32 Antivirus 4.X (64 bits) ESET NOD32 Antivirus 5 (32 bits) ESET NOD32 Antivirus 5 (64 bits) ESET NOD32 Antivirus 6 (32 bits) ESET NOD32 Antivirus 6 (64 bits) ESET NOD32 Antivirus 7 (32 bits)

	ESET NOD32 Antivirus 7 (64 bits)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
Frisk	F-Prot Antivirus 6.0.9.1
F- Secure	F-secure PSB Workstation Security 10.x F-Secure PSB for Workstations 9.00* F-Secure Antivirus for Workstation 9 F-Secure PSB Workstation Security 7.21 F-Secure Protection Service for Business 8.0, 7.1 F-Secure Internet Security 2009 F-Secure Internet Security 2008 F-Secure Internet Security 2007 F-Secure Internet Security 2006 F-Secure Client Security 9.x F-Secure Client Security 8.x Antivirus Client Security 7.1 F-Secure Antivirus for Workstation 8
iSheriff	iSheriff Endpoint Security 5.x
Kaspersky	Kaspersky Endpoint Security 10 for Windows (32bit- Edition) Kaspersky Endpoint Security 10 for Windows (64bit- Edition) Kaspersky Endpoint Security 8 for Windows (32bit- Edition) Kaspersky Endpoint Security 8 for Windows (64bit- Edition) Kaspersky Anti-Virus 2010 9.0.0.459* Kaspersky® Business Space Security Kaspersky® Work Space Security Kaspersky Internet Security 8.0, 7.0, 6.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 8* Kaspersky® Anti-virus 7.0 (con Windows Vista+UAC, es necesario desactivar UAC) Kaspersky Anti-Virus 6.0 for Windows Workstations*
McAfee	McAfee LiveSafe 2016 x86 / x64 McAfee SaaS Endpoint Protection 6.x, 5.X McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0 McAfee Internet Security Suite 2007 McAfee Total Protection Service 4.7* McAfee Total Protection 2008
Norman	Norman Security Suite 10.x (32bit- Edition) Norman Security Suite 10.x (64bit- Edition) Norman Security Suite 9.x (32bit- Edition) Norman Security Suite 9.x (64bit- Edition) Norman Endpoint Protection 8.x/9.x Norman Virus Control v5.99
Norton	Norton Antivirus Internet Security 2008* Norton Antivirus Internet Security 2007 Norton Antivirus Internet Security 2006
Microsoft	Microsoft Security Essentials 1.x Microsoft Forefront EndPoint Protection 2010 Microsoft Security Essentials 4.x Microsoft Security Essentials 2.0 Microsoft Live OneCare Microsoft Live OneCare 2.5*
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205
PC Tools	Spyware Doctor with AntiVirus 9.x

<b>Sophos</b>	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
<b>Symantec</b>	Symantec.cloud - Endpoint Protection.cloud 22.x Symantec.cloud - Endpoint Protection.cloud 21.x (32bits) Symantec.cloud - Endpoint Protection.cloud 21.x (64bits) Symantec EndPoint Protection 14.x (32bits) Symantec EndPoint Protection 14.x (64bits) Symantec EndPoint Protection 12.x (32bits) Symantec EndPoint Protection 12.x (64bits) Symantec EndPoint Protection 11.x (32bits) Symantec EndPoint Protection 11.x (64bits) Symantec Antivirus 10.1 Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x
<b>Trend Micro</b>	Trend Micro Worry-Free Business Security 8.x (32bit- Edition) Trend Micro Worry-Free Business Security 8.x (64bit- Edition) Trend Micro Worry-Free Business Security 7.x (32bit- Edition) Trend Micro Worry-Free Business Security 7.x (64bit- Edition) Trend Micro Worry-Free Business Security 6.x (32bit- Edition) Trend Micro Worry-Free Business Security 6.x (64bit- Edition) Trend Micro Worry-Free Business Security 5.x PC-Cillin Internet Security 2006 PC-Cillin Internet Security 2007* PC-Cillin Internet Security 2008* Trend Micro OfficeScan Antivirus 8.0 Trend Micro OfficeScan 7.x Trend Micro OfficeScan 8.x Trend Micro OfficeScan 10.x Trend Micro OfficeScan 11.x
<b>Comodo AntiVirus</b>	Comodo Antivirus V 4.1 32bits
<b>Panda Security</b>	Panda Cloud Antivirus 3.x Panda Cloud Antivirus 2.X Panda Cloud Antivirus 1.X
	Panda for Desktops 4.50.XX Panda for Desktops 4.07.XX Panda for Desktops 4.05.XX Panda for Desktops 4.04.10 Panda for Desktops 4.03.XX and earlier versions
	Panda for File Servers 8.50.XX Panda for File Servers 8.05.XX Panda for File Servers 8.04.10 Panda for File Servers 8.03.XX and earlier versions
	Panda Global Protection 2017* Panda Internet Security 2017* Panda Antivirus Pro 2017* Panda Gold Protection 2017*
	Panda Global Protection 2016* Panda Internet Security 2016* Panda Antivirus Pro 2016* Panda Gold Protection 2016*
	Panda Global Protection 2015* Panda Internet Security 2015* Panda Antivirus Pro 2015*

Panda Gold Protection* Panda Free Antivirus
Panda Global Protection 2014* Panda Internet Security 2014* Panda Antivirus Pro 2014* Panda Gold Protection*
Panda Global Protection 2013* Panda Internet Security 2013* Panda Antivirus Pro 2013*
Panda Global Protection 2012* Panda Internet Security 2012* Panda Antivirus Pro 2012*
Panda Global Protection 2011* Panda Internet Security 2011* Panda Antivirus Pro 2011* Panda Antivirus for Netbooks (2011)*
Panda Global Protection 2010 Panda Internet Security 2010 Panda Antivirus Pro 2010 Panda Antivirus for Netbooks
Panda Global Protection 2009 Panda Internet Security 2009 Panda Antivirus Pro 2009
Panda Internet Security 2008 Panda Antivirus+Firewall 2008 Panda Antivirus 2008
Panda Internet Security 2007 Panda Antivirus + Firewall 2007 Panda Antivirus 2007

Table 50: list of uninstallers

\* Panda 2017, 2016, 2015, 2014, 2013, 2012 products need a reboot to be uninstalled successfully.

\* Comodo Antivirus V4.1 (32-bit) - Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\*F-Secure PSB for Workstations 9.00 - During the installation process of the Endpoint Protection agent on Windows 7 and Windows Vista systems, the user will be prompted to select the Allow option.

\*AVG Internet Security Business Edition 2011 (32-bit) - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in several windows.

\*AVG Internet Security Business Edition 2011 (64-bit) (10.0.1375) - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in several windows.

\* Kaspersky Anti-Virus 6.0 for Windows workstations:

During the installation process of the Endpoint Protection agent on 64-bit platforms, the user will be prompted to select the Allow option in several windows.

To be able to uninstall the protection, the Kaspersky protection must not be password-protected.

Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\* F-Secure PSB for Workstations 9.00 - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in two windows.

\* AVG Anti-Virus Network Edition 8.5 - During the installation process of the Endpoint Protection agent, the user will be prompted to select the Allow option in two windows.

\* Panda Antivirus 2011 products do not uninstall correctly on 64-bit platforms. Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\* Panda Cloud Antivirus 1.4 Pro and Panda Cloud Antivirus 1.4 Free - Upon uninstalling the program, if UAC is enabled, the user will be prompted to select the option Allow in the UAC window.

\* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically on Windows Vista x64 systems.

\* Trend Micro - PC-Cillin Internet Security 2007 and 2008 cannot be uninstalled automatically on Windows Vista x64 systems with UAC enabled.

\* ESET NOD32 Antivirus 3.0.XX (2008) does not uninstall automatically on Windows Vista x64 systems.

\* ESET NOD32 Antivirus 2.7\*: after installing the Endpoint Protection agent on the computer, the system will restart automatically without displaying any notifications or asking for user confirmation.

\* ESET NOD32 Antivirus 2.70.39\*: after installing the Endpoint Protection agent on the computer, the system will restart automatically without displaying any notifications or asking for user confirmation.

\* ESET Smart Security 3.0 does not uninstall automatically on Windows Vista x64 systems.

\* Sophos Anti-virus SBE 2.5 does not uninstall correctly on Windows 2008 systems.

\* eTrust Antivirus 7.1 does not uninstall correctly on 64-bit platforms.

\* Norton Antivirus Internet Security 2008 does not uninstall correctly if the Windows Vista UAC is enabled.

\* BitDefender Free Edition 2009 12.0.12.0: on Windows Vista systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

\* Kaspersky Anti-Virus 2010 9.0.0.459: on systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

\* Kaspersky Anti-Virus 8: on Windows Vista systems with UAC enabled, if the user tries to uninstall the program, they will be prompted to select the option Allow in the UAC window.

\* McAfee Total Protection Services 4.7. The uninstaller does not run correctly if UAC is enabled. Furthermore, 32-bit platforms require user intervention.

\* Microsoft Live OneCare 2.5 does not uninstall correctly on Windows Small Business Server 2008.

If you have a program not included on this list, contact the relevant vendor to find out how to uninstall it before installing **Adaptive Defense on Aether**.



# 22. Appendix 4: key Concepts

**Active Directory**

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed directory service for finding a range of information on network environments.

**Activity graph/execution graph**

Graphical representation of the actions triggered by threats over time.

**Adaptive Defense software**

Program installed on the computers to protect. It consists of two modules: the Panda agent and the protection.

**Adaptive protection cycle**

A new security approach based on the integration of a group of services providing protection, detection, monitoring, forensic analysis and remediation capabilities into a single management console accessible from anywhere at any time.

**Advanced Protection**

Technology that continuously monitors and collects information from all processes running on the Windows computers on your network, and sends it to Panda Security's cloud for analysis. This information is analyzed using Machine Learning techniques in Big Data environments, returning an accurate classification (goodware or malware).

**Advanced reports**

See Advanced Reporting Tool (ART).

**Advanced Reporting Tool (ART)**

A real-time, advanced service for exploiting the knowledge generated by the products Adaptive Defense and Adaptive Defense. It allows organizations to detect unknown threats, targeted attacks and APTs, with graphical representations of the activities performed by the processes run by users, emphasizing events related to security and data extraction.

**Adware**

Program that automatically runs, displays or downloads advertising to the computer.

**Panda agent**

One of the modules included in the Adaptive Defense software. It manages communications between computers on the network and Panda Security's cloud-based servers, in addition to managing local processes.

**Alert**

See Incident.

### Anti-Tamper protection

A set of technologies aimed at preventing tampering of the **Adaptive Defense** processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

### Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, anti-exploit techniques, etc.), to detect and remove computer viruses and other threats.

### APT (Advanced Persistent Threat)

A set of strategies implemented by hackers and aimed at infecting customers' networks through multiple infection vectors simultaneously. They are designed to go undetected by traditional antivirus programs for long periods of time. Their main aim is financial (through theft of confidential information, intellectual property, etc.).

### ASLR (Address Space Layout Randomization)

Address Space Layout Randomization (ASLR) is a security technique used in operating systems to prevent buffer overflow-driven exploits. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. This prevents attackers from illegitimately using calls to certain system functions as they will not know where in memory those functions reside.

### Automatic assignment of settings

See Inheritance.

### Audit

An **Adaptive Defense** operating mode that lets you view the processes run on the protected network without taking any remedial action (disinfect or block).

### Backup

Storage area for non-disinfectable malicious files, as well as the spyware items and hacking tools detected on your network. All programs classified as threats and removed from the system are temporarily moved to the backup/quarantine area for a period of 7/30 days based on their type.

### Behavior change

**Adaptive Defense** can behave in two ways when an unknown item that was allowed by the administrator is finally classified as goodware or malware:

- Delete it from the list of allowed threats: if the item is classified as goodware it will continue to run. However, if it is classified as malware it will be prevented from running.
- Keep it on the list of allowed threats: the item will be allowed to run regardless of whether it is malware or goodware.

## **Block**

Action taken by the advanced protection that consists of preventing the execution of programs classified as a threat and programs unknown to **Adaptive Defense**.

## **Blocked item**

Depending on the way in which the advanced protection has been configured, **Adaptive Defense** will prevent the execution of all programs classified as malware/PUP as well as unknown programs until they are fully classified.

## **Broadcasting**

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network simultaneously, without the need to send it individually to each device. Broadcast packets don't go through routers and use different addressing methodology to differentiate them from unicast packets.

## **Buffer overflow**

Anomaly affecting the management of a process' input buffers. In a buffer overflow, if the size of the data received is greater than the allocated buffer, the redundant data is not discarded, but is written to adjacent memory locations. This may allow attackers to insert arbitrary executable code into the memory of a program on systems prior to Microsoft's implementation of the DEP (Data Execution Prevention) technology.

## **Cache/Repository (role)**

Computers that automatically download and store all files required so that other computers with **Adaptive Defense** installed can update their signature file, agent and protection engine without having to access the Internet. This saves bandwidth as it won't be necessary for each computer to separately download the updates they need. All updates are downloaded centrally for all computers on the network.

## **Cloud (Cloud computing)**

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

## **Compromised process**

A vulnerable process hit by an exploit attack in order to compromise the security of a user's computer.

## **Computers without a license**

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers are not protected, but are displayed in the Web management console.

## **CVE (Common Vulnerabilities and Exposures)**

List of publicly known cyber-security vulnerabilities defined and maintained by The MITRE Corporation. Each entry on the list has a unique identifier, allowing CVE to offer a common naming scheme that security tools and human operators can use to exchange information about vulnerabilities with each other.

### **DEP (Data Execution Prevention)**

A feature implemented in operating systems to prevent the execution of code in memory pages marked as non-executable. This feature was developed to prevent buffer-overflow exploits.

### **Dialer**

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

### **Discovery computer (role)**

Computers capable of finding unmanaged workstations and servers on the network in order to remotely install the **Adaptive Defense** agent on them.

### **Disinfectable file**

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

### **Domain**

Windows network architecture where the management of shared resources, permissions and users is centralized in a server called a Primary Domain Controller (PDC) or Active Directory (AD).

### **Domain Name System (DNS)**

Service that translates domain names into different types of information, generally IP addresses.

### **Dwell time**

Length of time that a threat has remained undetected on the network.

### **Entity**

Predicate or complement included in the action tables of the forensic analysis module.

### **Environment variable**

A string consisting of environment information such as a drive, path or file name, which is associated with a symbolic name that Windows can use. You can use the System applet in the Control Panel or the 'set' command at the command prompt to set environment variables.

### **Excluded program**

Programs that were initially blocked as they were classified as malware or PUP, but have been selectively and temporarily allowed by the administrator, who excluded them from the scans performed by the solution.

**Exploit**

Generally speaking, an exploit is a sequence of specially crafted data aimed at causing a controlled error in the execution of a vulnerable program. Once the error occurs, the compromised process will mistakenly interpret certain parts of the data sequence as executable code, taking malicious actions that may compromise the security of the target computer.

**Filter**

A dynamic-type computer container that automatically groups together those items that meet the conditions defined by the administrator. Filters simplify the assignment of security settings, and facilitate management of all computers on the network.

**Filter tree**

Collection of filters grouped into folders, used to organize all computers on the network and facilitate the assignment of settings.

**Firewall**

Technology that blocks the network traffic that coincides with certain patterns defined in rules established by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

**Folder tree**

Hierarchical structure consisting of static groups, used to organize all computers on the network and facilitate the assignment of settings.

**Forensic analysis**

A series of actions and processes carried out by network administrators with special tools in order to track malicious programs and assess the consequences of an infection.

**Geolocation**

Geographical positioning of a device on a map from its coordinates.

**Goodware**

A file which, after analysis, has been classified as legitimate and safe.

**Group**

Static container that groups one or more computers on the network. Computers are assigned to groups manually. Groups simplify the assignment of security settings, and facilitate management of all computers on the network.

**Hacking tool**

Programs used by hackers to carry out actions that cause problems for the user of the affected computer (allowing the hacker to control the computer, steal confidential information, scan communication ports, etc.).

### **Hardening**

An **Adaptive Defense** operating mode that blocks unknown programs downloaded from the Internet as well as all files classified as malware.

### **Heap Spraying**

Heap Spraying is a technique used to facilitate the exploitation of software vulnerabilities by malicious processes.

As operating systems improve, the success of vulnerability exploit attacks has become increasingly random. In this context, heap sprays take advantage of the fact that on most architectures and operating systems, the start location of large heap allocations is predictable and consecutive allocations are roughly sequential. This allows attackers to insert and later run arbitrary code in the target system's heap memory space.

This technique is widely used to exploit vulnerabilities in Web browsers and Web browser plug-ins.

### **Heuristic scanning**

Static scanning that employs a set of techniques to inspect suspicious programs based on hundreds of file characteristics. It can determine the likelihood that a program may take malicious actions when run on a user's computer.

### **Hoaxes**

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

### **IDP (Identity Provider)**

Centralized service for managing user identity verification.

### **Incident**

Message relating to **Adaptive Defense's** advanced protection that may require administrator intervention. Incidents are reported to the administrator through the management console or via email (alerts), and to end users through pop-up messages generated by the agent and displayed locally on the protected device.

### **Indirect assignment of settings**

See Inheritance.

### **Infection vector**

The means used by malware to infect users' computers. The most common infection vectors are Web browsing, email and pen drives.

**Inheritance**

A method for automatically assigning settings to all subsets of a larger, parent group, saving management time. Also referred to as 'automatic assignment of settings' or 'indirect assignment of settings'.

**IP address**

Number that identifies a device interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

**IP Feeds**

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

**Item reclassification**

See Behavior change.

**Joke**

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

**Lock**

An **Adaptive Defense** operating mode that blocks unknown programs as well as all files classified as malware.

**Machine learning**

This is a branch of artificial intelligence whose aim is to develop technologies capable of predicting behaviors from unstructured data delivered in the form of examples.

**Malware**

This term is used to refer to all programs that contain malicious code (MALicious softWARE), whether it is a virus, Trojan, worm or any other threat to the security of IT systems. Malware tries to infiltrate or damage computers, often without users knowing, for a variety of reasons.

**Malware Freezer**

A feature of the quarantine/backup module whose goal is to prevent data loss due to false positives. All files classified as malware or suspicious are sent to the quarantine/backup area, thereby avoiding deleting and losing data if the classification is wrong.

**Malware 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.

**Manual assignment of settings**



Direct assignment of a set of settings to a group, as opposed to the automatic or indirect assignment of settings, which uses the inheritance feature to assign settings without administrator intervention.

### **MD5 (Message-Digest Algorithm 5)**

A cryptographic hash function producing a 128-bit value that represents data input. The MD5 hash value calculated for a file is used to identify it unequivocally or check that it has not been tampered with.

### **Network adapter**

Hardware that allows communication among different computers connected through a data network. A computer can have more than one network adapter installed, and is identified in the system through a unique identifier.

### **Network topology**

Physical or logical map of network nodes.

### **OU (Organizational Unit)**

Hierarchical method for classifying and grouping objects stored in directories.

### **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).

### **Partner**

A company that offers Panda Security products and services.

### **PDC (Primary Domain Controller)**

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

### **Peer to Peer (P2P) functionality**

Information transfer mechanism that uses the network bandwidth more efficiently on networks with nodes that work simultaneously as clients and servers, establishing a direct two-way communication.

**Adaptive Defense** implements P2P connections to reduce bandwidth usage, as those computers whose signature file has been already updated will share the update locally with those computers that also need to update it.

### Phishing

A technique for obtaining confidential information from a user fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

### Port

Unique ID number assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

### Potentially Unwanted Program (PUP)

A program that may be unwanted, despite the possibility that users consented to download it. Potentially unwanted programs are often downloaded inadvertently along with other programs.

### Protection (module)

One of the two components of the **Adaptive Defense** software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

### Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

### Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

### Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the **Adaptive Defense** cloud.

### Proxy functionality

This feature allows **Adaptive Defense** to operate on computers without Internet access, accessing the Web through an agent installed on another computer on the same subnet.

### QR (Quick Response) Code

A matrix of dots that efficiently stores data.

### Quarantine

See Backup.

### Role

Specific permission configuration applied to one or more user accounts, and which authorizes users to view and edit certain resources of the console.

**Rootkit**

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is used by attackers to hide evidence and utilities on previously compromised systems.

**ROP**

Return-oriented programming (ROP) is a computer security exploit technique that allows attackers to run arbitrary code in the presence of protection technologies such as DEP and ASLR.

Traditional stack buffer overflow attacks occurred when a program wrote to a memory address on the program's call stack outside of the intended data structure, which is usually a fixed-length buffer. However, those attacks were rendered ineffective when techniques such as DEP were massively incorporated into operation systems. These techniques prevent the execution of code in regions marked as non-executable.

In a ROP attack, the attacker gains control of the call stack to hijack program control flow and then executes carefully chosen machine instruction sequences that are already present in the machine's memory, called "gadgets". Chained together, these gadgets allow the attacker to perform arbitrary operations on the targeted machine.

**RWD (Responsive Web Design)**

A set of techniques that enable the development of Web pages that automatically adapt to the size and resolution of the device being used to view them.

**Samples Feed**

A service for delivering normalized malware and automations through a REST API to companies with their own anti-malware laboratory.

**Settings**

See Settings profile.

**Settings profile**

Specific settings governing the protection or any other aspect of the managed computer. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

**SIEM (Security Information and Event Management)**

Software that provides storage and real-time analysis of the alerts generated by network devices.

**Signature file**

File that contains the patterns used by the antivirus to detect threats.

**SMTP server**

Server that uses SMTP (Simple Mail Transfer Protocol) to exchange email messages between computers.

### **Spam**

This term refers to unsolicited email messages that usually contain advertising and are generally sent out massively. Spam can have a range of negative effects on the recipient.

### **Suspicious item**

A program with a high probability of being malware after having been scanned by the **Adaptive Defense** protection installed on the user's computer.

### **Spyware**

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and collects personal data.

### **SSL (Secure Sockets Layer)**

Cryptographic protocol for the secure transmission of data sent over the Internet.

### **Task**

Set of actions scheduled for execution at a configured frequency during a specific period of time.

### **TCO (Total Cost of Ownership)**

Financial estimate of the total direct and indirect costs of owning a product or system.

### **TCP (Transmission Control Protocol)**

The main transport-layer Internet protocol, aimed at connections for exchanging IP packets.

### **TLS (Transport Layer Security)**

New version of protocol SSL 3.0.

### **Trojans**

Programs that reach computers disguised as harmless software to install themselves on computers and carry out actions that compromise user confidentiality.

### **UDP (User Datagram Protocol)**

A transport-layer protocol which is unreliable and unsuited for connections for exchanging IP packets.

### **Unblocked program**

Program blocked during the classification process but temporarily and selectively allowed by the administrator to avoid disrupting user activity.

### **User (console)**

Information set used by **Adaptive Defense** to regulate administrator access to the Web console and establish the actions that administrators can take on the network's computers.

### **User (network)**

A company's workers using computing devices to do their job.

### **User account**

See User.

### **Virus**

Programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

VPN (Virtual Private Network)

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

### **Vulnerable process**

A program which, due to a programming bug, cannot interpret certain input data correctly. Hackers take advantage of specially crafted data packets (exploits) to cause vulnerable processes to malfunction, and run malicious code designed to compromise the security of the target computer.

### **Web console**

Tool to manage the advanced security service **Adaptive Defense**, accessible anywhere, anytime through a supported Internet browser. The Web console allows administrators to deploy the security software, push security settings, and view the protection status. It also provides access to a set of forensic analysis tools to assess the scope of security problems.

### **Widget (Panel)**

Panel containing a configurable graph representing a particular aspect of network security. **Adaptive Defense's** dashboard is made up of different widgets.

### **Window of opportunity**

The time it takes between when the first computer in the world is infected with a new malware specimen and its analysis and inclusion by antivirus companies in their signature files to protect computers from infections. This is the period when malware can infect computers without antivirus software being aware of its existence.

### **Workgroup**

Architecture in Windows networks where shared resources, permissions and users are managed independently on each computer.



Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, Santiago de Compostela, 12, 48003 Bilbao (Bizkaia) SPAIN.

Registered trademarks. Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names may be registered trademarks of their respective owners.

© Panda Security 2017. All rights reserved.