



# PANDA **CLOUD OFFICE PROTECTION**

Advanced Administration Guide



## Panda Cloud Office Protection

---

### Copyright notice

© Panda Security 2012. All rights reserved.

Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, C/ Gran Via Don Diego Lopez de Haro 4, 48001 Bilbao (Bizkaia) SPAIN.

### Trademarks

Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. All other product names may be registered trademarks of their respective companies.

© Panda Security 2012. All rights reserved.

PCOP-610



Who should read this guide? .....	13
Introduction .....	13
Protection .....	14
Installation .....	15
Security from the cloud and Collective Intelligence .....	15
What is the 'cloud'?.....	15
What is Collective Intelligence? .....	15
Information .....	16
How did detection work before Collective Intelligence? .....	16
How does detection with Collective Intelligence work?.....	16
Information and queries .....	17
Information, queries and services.....	17
Useful links .....	17
Panda Cloud Office Protection Services .....	18
Other products and services.....	18
Other products and services.....	18
Services .....	18
MalwareRadar audits.....	19
Email cleaning.....	19
Web traffic security management.....	19
Requirements and URLs.....	19
Requirements and URLs .....	19



Computer requirements .....	19
URLs .....	20
URLs .....	20
<b>Key concepts .....</b>	<b>21</b>
Key concepts.....	21
<b>Login to the Web console .....</b>	<b>27</b>
The Web console .....	27
Preferences .....	28
General options .....	29
Default view .....	29
Group restrictions.....	29
Remote access .....	29
Automatic management of suspicious files .....	30
Account management .....	30
Computer blacklist .....	30
<b>License management.....</b>	<b>30</b>
Types of clients .....	30
Subscriber .....	30
Non-subscriber .....	30
Warnings related with licenses.....	31
Updating the number of licenses .....	31
License expiry date warning .....	31
Blacklist .....	32
Canceling licenses .....	32



Computers affected .....	32
Managed computers .....	33
Adding licenses using the activation code .....	33
Adding licenses using the activation code .....	33
Possible errors when adding licenses .....	34
<b>Account management .....</b>	<b>35</b>
Introduction to account management .....	35
Delegating the management of an account .....	35
Merging accounts .....	35
Delegating the management of an account.....	35
Delegating the management of an account .....	35
Possible errors on delegating account management.....	36
Merging accounts .....	37
Merging accounts .....	37
Possible errors when merging accounts .....	39
Consequences of merging accounts.....	40
<b>Creating and managing users.....</b>	<b>40</b>
Creating and managing users.....	40
<b>Types of permissions .....</b>	<b>41</b>
Types of permissions .....	41
Total control permission .....	42
User management .....	42
Profile management.....	42
Group and computer management.....	42



Unprotected computer search.....	43
Managing licenses and accounts.....	43
Protection uninstallation .....	43
<b>Administrator permission .....</b>	<b>43</b>
User management .....	43
Unprotected computer search.....	44
Group and computer management.....	44
Protection uninstallation .....	44
Profile management.....	44
Monitoring permission.....	45
<b>Configuring the protection.....</b>	<b>45</b>
Introduction.....	45
Default profile .....	46
<b>Creating/copying profiles.....</b>	<b>46</b>
Creating a profile.....	46
Copying a profile .....	47
<b>General profile settings .....</b>	<b>48</b>
General profile settings.....	48
<i>Main</i> tab .....	48
<i>Scheduled scans</i> tab .....	49
<i>Warnings</i> tab.....	49
<i>Apply to</i> tab .....	49
Scheduled scan settings .....	50
How to configure scans.....	50



Advanced scan settings.....	51
Edit profile - Advanced settings.....	52
Installation.....	52
Internet connection.....	52
Connection to Collective Intelligence.....	52
Server connection options .....	52
Quarantine options.....	53
Uninstallation .....	53
<b>Antivirus protection settings .....</b>	<b>53</b>
Antivirus protection settings .....	53
Files tab.....	54
Mail tab.....	54
Local scans .....	54
Right-click scan of a selected item .....	55
Local scans from Panda Endpoint Protection .....	55
Advanced antivirus settings - File protection .....	56
Exclusions.....	56
Advanced antivirus settings - Email protection.....	56
<b>Firewall protection settings.....</b>	<b>57</b>
Introduction .....	57
Configuration from the Web administration console .....	57
Configuration from the local console (Endpoint) .....	87
Personal firewall .....	88
Configuration from the Web console .....	88
Configuration from the local console (Endpoint).....	89



<b>Device Control settings .....</b>	<b>95</b>
Device control settings.....	95
Notifications.....	95
How to enable device control .....	95
<b>Exchange Server protection settings .....</b>	<b>96</b>
Introduction.....	96
Minimum requirements .....	96
Antivirus .....	97
Anti-spam .....	97
Exchange Server antivirus protection.....	98
Mailbox protection .....	98
Transport protection.....	99
Intelligent mailbox scan .....	100
Exchange Server anti-spam protection .....	101
Actions to perform on spam messages.....	101
Allowed/denied addresses and domains .....	102
<b>Creating groups .....</b>	<b>103</b>
Creating groups .....	103
Assigning computers to groups .....	104
<b>Installing the protection .....</b>	<b>104</b>
Recommendations prior to installation.....	104
Computer requirements .....	104
Closing other applications during installation .....	104
Presence of other protection software on computers .....	105





Configuring exclusions in the file protection for servers with Exchange Server .....	105
Installation modes .....	106
Installation modes .....	106
Quick installation .....	107
Installing the protection with the installation program .....	107
Installing the protection with the distribution tool .....	108
Installation cases.....	110
Installation cases .....	110
<b>Uninstalling other protections.....</b>	<b>111</b>
Uninstalling other protections .....	111
Automatic uninstallation .....	111
Manual uninstallation .....	111
<b>Protection status .....</b>	<b>112</b>
Protection status.....	112
Notifications.....	112
Licenses .....	112
Detections .....	113
Scheduled scans .....	114
Results of the scheduled scan jobs.....	115
List of detections .....	116
Search results .....	116
<b>Monitoring of computers.....</b>	<b>117</b>
Introduction.....	117
Protected computers .....	119



Computer search .....	119
Unprotected computers .....	121
Computer search .....	121
Computer details .....	122
<b>Remote access to computers.....</b>	<b>123</b>
Remote access to computers.....	123
How to gain remote access to a different computer.....	124
How to use the remote access tools .....	124
VNC tools.....	124
TeamViewer .....	125
LogMeln .....	125
<b>Unprotected computer search .....</b>	<b>126</b>
Unprotected computer search .....	126
Configuring searches for unprotected computers.....	126
Viewing searches and results.....	127
Viewing searches .....	127
Search results .....	128
<b>Quarantine .....</b>	<b>128</b>
Quarantine .....	128
Files excluded from the scan .....	130
<b>Reports.....</b>	<b>130</b>
Generating reports .....	130
Types of reports.....	131



Report display.....	132
<b>Uninstallation .....</b>	<b>133</b>
Types of uninstallation .....	133
Local uninstallation.....	134
Centralized uninstallation .....	134
Remote uninstallation.....	136
Creating remote uninstallation tasks .....	136
Viewing remote unistallation tasks and their results .....	137
Compatibility between searches for unprotected computers and remote uninstallation .....	138
<b>Troubleshooting &amp; FAQs.....</b>	<b>139</b>
Troubleshooting .....	139
Frequently Asked Questions.....	139
How is the Panda Cloud Office Protection Web console accessed? .....	139
What are the installation requirements for Panda Cloud Office Protection? .....	140
What checks must be carried out before installing Panda Cloud Office Protection? .....	140
What are the components of Panda Cloud Office Protection? .....	141
What is the Panda Cloud Office Protection administration agent? .....	142
What do the P2P and proxy functions implemented in Panda Cloud Office Protection consist of? .....	143
How is Panda Cloud Office Protection installed through the installation program? .....	145
How is Panda Cloud Office Protection installed through the distribution tool? .....	147
Can Panda Cloud Office Protection be installed on a network with AdminSecure protection? .	148
How can a computer be included in the blacklist? .....	149
How can a computer be restored from the blacklist?.....	150
Why is no information received from a computer that was in the blacklist but has been restored? .....	150



Why are some computers out-of-date after a Panda Cloud Office Protection update? .....	150
What does Panda Cloud Office Protection do when connecting to the cloud? .....	151
How does Panda Cloud Office Protection access the cloud depending on the type of scan? ...	153
Is it possible to disable queries to the cloud? .....	154
How often do computers notify the status of the installed protection to the Panda Cloud Office Protection servers? .....	154
Once you have created an immediate scan job in the Panda Cloud Office Protection Web console, how long does it take for the endpoint to recognize and apply it? .....	155
<b>Appendix 1: Commandline scripts for basic operations .....</b>	<b>155</b>
Installation .....	156
Previous steps. Downloading the installation package.....	156
Installation steps .....	159
Verifying protection installation .....	161
Verification steps .....	161
Uninstalling Panda Cloud Office Protection .....	162
Uninstallation steps.....	162
Updating the signature file.....	163
Steps for updating the signature files .....	164
Updating settings .....	164
Steps for updating the settings.....	164
Getting the date of the signature files .....	164
Obtaining the signature files date .....	165
Getting the status of the antivirus, the firewall and the device control modules.	166
Getting information on the status of the protection.....	167
<b>Appendix 2: Deploying the protection .....</b>	<b>171</b>
The administration agent.....	171



Peer to Peer (P2P) function .....	171
Dinamic proxy .....	174
Static proxy .....	175
Installation times .....	177
Deploying Panda Endpoint Agent .....	181
Deployment of Panda EndPoint Protection .....	196
<b>Appendix 3: Automatic computer search.....</b>	<b>204</b>
Aspects to bear in mind when creating a search job .....	204
Search job action sequence and job status .....	206
Cases in which the server may NOT be aware that a computer search job has finished .....	208



### Who should read this guide?

This Advanced Administration Guide is aimed at network administrators who want to keep their networks free from viruses and other threats.

The guide offers a detailed explanation of the protection installation, configuration and monitoring processes as well as useful information about how to have complete control over computers through remote access tools.

The appendixes include a description of the different operations that can be performed from the command line, the protection deployment process, FAQs and examples of how to install the solution according to specific needs.

This guide complements the basic documentation available in the product documentation area, at:

<http://www.pandasecurity.com/enterprise/downloads/docs/product/managedprotection/>, especially in the Web help and the basic administration guide.



#### IMPORTANT NOTE

*For information about the protection on computers with the following operating systems: Windows 2000, Windows XP 32-bit SP0/SP1, Windows XP 64-bit, Windows Server 2003 32-bit SP0, Windows Server 2003 R2 32-bit SP0, Windows Server 2003 64-bit or Windows Server 2003 R2 64-bit, refer to the [Advanced Administration Guide for versions prior to 6.0](#) in the product documentation area.*

We hope you find this advanced administration guide useful.

### Introduction

Panda Cloud Office Protection is a complete security solution to protect your computer network and manage security online with none of the hassle. The protection neutralizes [spyware](#), [Trojans](#), [viruses](#) and any other threats that target your computers.

Its main features include:



## Panda Cloud Office Protection

---

- ☁ Maximum protection for PCs, laptops and servers.
- ☁ Easy to install, manage and maintain through its Web console.
- ☁ Management and organization based on protection profiles and user groups.

Panda Cloud Office Protection's management center is the Web console, which allows you to:

1. Configure the protection, distribute it and install it on computers.
2. Monitor the status of the protection on computers.
3. Extract reports about the security status and threats detected.
4. Manage items detected to monitor at any time what has been detected, when and on which computers.
5. Configure the quarantine of suspicious items.

If you want to enjoy other services, like email protection (Panda Cloud Email Protection), Web traffic protection (Panda Cloud Internet Protection) or on-demand, online malware audits (MalwareRadar), click **Other products** and select the relevant option.

## Protection

Depending on your computers' protection needs, you will be able to create [profiles](#) and configure the protection's behavior ([Antivirus](#), [Firewall](#), [Device Control](#) and [Exchange Servers](#)) for the profile that you are creating. Then, you can assign that profile to the [computer groups](#) to protect.



*You can only enable the Exchange Server protection if you have bought Panda Cloud Office Protection Advanced licenses.*

You can configure the protection installed on computers before or after the installation. However, we recommend you spend some time carefully analyzing the protection needs of your network. These needs might vary from one computer to another, or be the same for all computers on the network. Depending on these circumstances you might need to create new profiles or use the Panda Cloud Office Protection default settings.



### Installation

Before installing the protection, check the [Recommendations prior to installation](#). You will find **important information** about the installation and uninstallation processes, how to configure the protection language, and how to use the quick installation and default installation options.

The configuration and installation processes are totally under your control: you will decide at all times what computers to protect, with what protection and the installation mode.

Once you have selected the computers to protect and the configuration profiles, you must distribute and install the protection. To help you through the process, we have prepared some information about the available [installation methods](#) and [installation cases](#). We hope you find them useful.

## Security from the cloud and Collective Intelligence

### What is the 'cloud'?

Cloud computing is a technology that allows services to be offered across the Internet. To this effect, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

Panda Cloud Office Protection is served from the cloud, connecting to Collective Intelligence servers to protect your computer at all times, increasing the detection capacity and not interfering with the performance of the computer. Now all knowledge is in the cloud, and thanks to Panda Cloud Office Protection, you can benefit from this.

### What is Collective Intelligence?

Collective Intelligence is a security platform created by Panda Security, offering high-level protection in real time, exponentially increasing the detection capacity of Panda Cloud Office Protection.





### Information

Throughout its history, Panda Security has always been in the technological vanguard of the international market thanks to its innovation in anti-malware security, and as a visionary company, it has consistently offered innovations to the market two years ahead of its rivals.

In 2006, Panda Security began to develop a set of technologies based on artificial intelligence. This set of techniques, dubbed Collective Intelligence, is able to analyze, classify and disinfect 99.5% of the new malware samples received every day at the laboratory, keeping users protected practically in real time.

This leaves laboratory technicians to process the remaining 0.5% of malware received. These cases, which tend to be more technologically complex, require more than Collective Intelligence to determine whether or not they are malware.

These technologies were first released in 2007 and currently all Panda Security solutions benefit from this vast knowledge base, offering protection ratios way above the market average.

### How did detection work before Collective Intelligence?

Previously, laboratories received malware samples (new viruses, worms or Trojans) and technicians manually analyzed them before creating the corresponding vaccine. Once published across the Internet, users could download the vaccine to their signature files in order to ensure protection against the new threat.

This model ceased to become useful once Panda Security laboratories went from receiving 100 samples a day to 50,000. This would require a whole army of technicians working against the clock to analyze all the new examples of malware received.

### How does detection with Collective Intelligence work?

Collective Intelligence has servers that classify and process all the data provided through the user community about detections on their computers. Panda Cloud Office Protection sends requests to Collective Intelligence whenever it requires, ensuring



maximum detection capacity without negatively affecting resource consumption on computers.

When new malware is detected on a computer in the user community, Panda Cloud Office Protection sends the information to the Collective Intelligence servers in the cloud, automatically and anonymously. The information is processed by the servers, delivering the solution to all other users in the community in real time. Hence the name Collective Intelligence.

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

## Information and queries

### Information, queries and services

Along with the products themselves, Panda Security offers you help files and documentation to extend information, resolve queries, access the latest updates and benefit from other services. You can also keep up-to-speed on the latest IT security news. Visit the Panda Security website to access all the information you need.

### Useful links

- [Main page](#): All the Panda Security information at your disposal.
- [Documentation](#): All the latest product documentation and other publications.
- [Tech Support](#): Clear up any questions you have about infections, [viruses](#), products and Panda Security services, with continuous and fully up-to-date information, any time of the day, all year round.
- [Evaluation software](#): Panda Security offers you free trial software of the product you want.
- [Products](#): Check out the features of all Panda Security products. You can also buy them or try them without obligation.



## Panda Cloud Office Protection

---

### Panda Cloud Office Protection Services

Panda Cloud Office Protection is a byword for permanent protection against all IT security threats. With Panda Cloud Office Protection you will be kept fully up-to-date on the security status of all your computers, and you will always be able to decide how and when you want to protect them .

In addition to this Help, which will let you get the most out of your protection, Panda Security offers you other services. These value-added services will ensure that you always have access to expert advice and the latest security technology used by Panda Security.

Services offered by Panda Cloud Office Protection:

- [Daily updates of the Signature File](#).
- [Specialized Tech Support](#) via email and telephone.
- General updates of Panda Cloud Office Protection: New features, improvements to the detection capacity, etc.
- Documentation: Access to the [Advanced Administration Guide](#).

## Other products and services

### Other products and services

From the Panda Cloud Office Protection Web console, you can access other products and services that will let you, among other things, carry out security audits and implement security measures for email.

### Services

Click **Services**, at the bottom of the Web console. From the **Services** window you can send Panda Security suggestions and access the Help area where you will find the answers to any doubts that you might have about Panda Cloud Office Protection, and other information and utilities that Panda Security offers you.



### MalwareRadar audits

In the main screen of the Web console, click the **Other products** tab. If you want to perform a malware audit on your network, you can use MalwareRadar. MalwareRadar is an online, on-demand audit service that detects and disinfects [malware](#), especially latest generation malware that can go undetected by traditional solutions.

To start the audit, click **Go to MalwareRadar**.

### Email cleaning

As an owner of Panda Cloud Email Protection licenses, you can use cloud-based cleaning of your email, with a minimal impact on your computers. Click **Other products** and use the corresponding button to access the Panda Cloud Email Protection Web console, from where you can implement the cleaning.

If you do not have any licenses, you can go to the registration page and try the evaluation version.

### Web traffic security management

Panda Cloud Internet Protection guarantees secure Internet access and Web traffic management for your corporate network.

Use the corresponding button to access the trial version. If you have licenses, use the corresponding button to access the console. Otherwise, you can access the trial version by clicking **Other products** and using the corresponding button.

## Requirements and URLs

### Requirements and URLs

#### Computer requirements

Panda Cloud Office Protection is the ideal solution to protect your computer network. Nevertheless, to make the most out of it, the computers used in the protection access,



## Panda Cloud Office Protection

---

installation, configuration and deployment processes will need to meet a series of hardware and software requirements.

Click [here](#) for detailed information about the minimum system requirements. You will find all the information you need plus shortcuts to everything you need to know about Panda Security and its products.

### URLs

To access the Panda Cloud Office Protection servers and be able to download updates, at least one of the protected computers must have access to a series of Web pages. Click [here](#) to see the list of URLs to access.

### URLs

To access the Panda Cloud Office Protection servers and be able to download updates, at least one of the protected computers must have access to a series of Web pages. These are:

#### **To update the signature file and protection engine**

[http://enterprise.updates.pandasoftware.com/updates\\_ent/](http://enterprise.updates.pandasoftware.com/updates_ent/)

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

<http://acs.pandasoftware.com/member/uninstallers/>

<http://acs.pandasoftware.com/member/pavsig/>

<http://acs.pandasoftware.com/free/>

#### **To send suspicious files**

<http://hercules.pandasoftware.com/getqesi.aspx>

<http://hercules.pandasoftware.com/getqesd.aspx>

#### **For communication with the server**

<http://mp-agents.pandasecurity.com>



## Panda Cloud Office Protection

---

<https://mp-agents.pandasecurity.com>

### For communication with the servers of Collective Intelligence

<http://cache.pandasoftware.com/>

<http://proinfo.pandasoftware.com/connectiontest.htm>



*Ports (client intranet) TCP 18226 and UDP 21226 must be opened to allow correct communication between the Panda Cloud Office Protection agents.*

## Key concepts

### Key concepts

#### **Network adapter**

The network adapter allows communication between devices connected to each other and also allows resources to be shared between two or more computers. It has a unique identifier.

#### **Adware**

Program that automatically runs, displays or downloads advertising to the computer.

#### **Administration agent**

This is the agent responsible for communication between the administered computers and the Panda Cloud Office Protection servers, as well as managing local processes.

#### **Genetic heuristic scan**

The genetic heuristic scan analyzes suspect items on the basis of "digital genes", represented by a few hundred characters in each file scanned. This determines the potential of the software to carry out malicious or damaging action when run on a computer, and whether it is a virus, spyware, a Trojan, a worm, etc.



### ***Antivirus***

Programs designed to detect and eliminate viruses and other threats.

### ***Signature file***

This is the file that allows the antivirus to detect threats.

### ***Broadcast domain***

This is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.

### ***Client Web console***

The Web console lets you configure, distribute and manage the protection across computers on your network. It also lets you see the security status of your network and generate and print the reports you want.

### ***Quarantine***

Quarantine is the place where suspicious or non-disinfectable items are stored, as well as spyware and hacking tools detected.

### ***Dialers***

Program that redirects users that connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

### ***IP address***

Number that identifies an interface in a network device (usually a computer) that uses the IP protocol.

### ***MAC address***



Hexadecimal, 48-bit unique identifier of a network card or interface. It is individual; each device has its own MAC address.

### ***Firewall***

This is a barrier that can protect information in a system or network when there is a connection to another network, for example, the Internet.

### ***Peer to Peer (P2P) function***

Network without fixed client or servers, but a series of nodes that work simultaneously as clients and servers for the other nodes on the network. This is a legal way of sharing files, similar to sending them via email or instant messaging, just more efficient.

In the case of Panda Cloud Office Protection, the P2P feature reduces use of bandwidth for the Internet connection, as computers that have already updated a file from the Internet then share the update with other connected computers. This prevents saturating Internet connections.

### ***Proxy function***

This feature allows Panda Cloud Office Protection to operate in computers without Internet access, accessing through an agent installed on a computer in the same subnet.

### ***Group***

In Panda Cloud Office Protection, this is a set of computers to which the same protection settings profile is applied. There is an initial group or *Default* group in Panda Cloud Office Protection to which the administrator can add all the computers to protect. New groups can also be created.

### ***Distribution tool***

Once downloaded from the Internet and installed on the administrator's PC, the distribution tool lets you remotely install and uninstall the protection on selected network computers.





### ***Hacking tools***

Programs that can be used by a hacker to carry out actions that cause problems for the user of the affected computer (allowing the hacker to control the computer, steal confidential information, scan communication ports, etc.).

### ***Hoaxes***

These are spoof messages, normally emails, warning of viruses/threats which do not really exist.

### ***Administration agent identifier***

A unique number or GUID (*Globally Unique Identifier*) which identifies each administration agent of Panda Cloud Office Protection.

### ***Joke***

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

### ***Blacklist***

This is a list of computers to which the protection will not be distributed. If a computer in the blacklist already has the protection installed, it will not be updated. Groups of expired computers and computers whose maximum number of installations allowed has been exceeded are also blacklisted.

### ***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.



### ***Node***

In computer networks, each computer on the network is a node, and if talking about the Internet, each server also represents a node.

### ***The Cloud***

Cloud computing is a technology that allows services to be offered across the Internet. The cloud is a term used metaphorically around the Internet.

### ***Panda Endpoint Protection***

Name of the protection distributed and installed by Panda Cloud Office Protection on the computers on the network.

### ***Profile***

A profile is a specific protection configuration. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

### ***Phishing***

A technique for obtaining confidential information fraudulently. The information targeted includes passwords, credit cards and bank account details.

### ***Local process***

The local processes are responsible for performing the tasks necessary to implement and manage the protection on computers.

### ***Protocol***

System used for interconnection of computers. One of the most commonly-used is TCP-IP.

### ***Proxy server***



A proxy server acts as an intermediary between an internal network (an intranet, for example) and an external connection to the Internet. This allows a connection for receiving files from Web servers to be shared.

### ***Port***

Point through which a computer is accessed and information is exchanged (inbound/outbound) between the computer and external sources (via TCP/IP).

### ***Rootkits***

A program designed to hide objects such as processes, files or Windows registry entries (often including its own). This type of software is not malicious in itself, but is used by hackers to cover their tracks in previously compromised systems. There are types of malware that use rootkits to hide their presence on the system.

### ***Exchange Server***

Microsoft's email server software. Exchange Server stores inbound and/or outbound emails and distributes them to the appropriate Exchange Server users. To connect to the server and download their email, users must have an email client installed on their computers.

### ***SMTP server***

Server that uses SMTP -simple mail transfer protocol- to exchange email messages between computers.

### ***Spyware***

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and which collects personal data.

### ***Network topology***

The communication structure of nodes on a network.



### ***Trojans***

Programs that reach computers disguised as harmless programs that install themselves on computers and carry out actions that compromise user confidentiality.

### ***Public network***

This is the type of network you will find in cybercafes or airports, etc. Visibility of computers will be restricted on such networks, and there are restrictions on sharing files, resources and directories.

### ***Trusted network***

In this case we are generally talking about office or domestic networks. A computer will be perfectly visible to the other computers on the network. There are no limitations on sharing files, resources or directories.

### ***Environment variable***

This is a string containing information about the environment, such as the drive, path or filename, associated with a symbolic name that Windows can use. The System option in the control panel or the system symbol Set command can define environment variables.

### ***Viruses***

Viruses are programs that can enter computers or IT systems in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

## **Login to the Web console**

### **The Web console**

To log in to the Web console:

Enter your Login Email and Password.



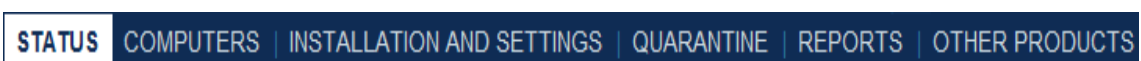
## Panda Cloud Office Protection

---

➡ **Note:** *If your license subscription has expired, you can renew it by contacting your reseller or sales advisor.*

Accept the terms and conditions of the **License agreement** (you will only be asked to do so once).

You will then see the main window of the Web console. From this window you can access the following areas: **Status**, **Computers**, **Installation and settings**, **Quarantine**, **Reports** and **Other products**.



The **Exit** option lets you log out. To select the language for viewing the Web console, use the **Language** list next to the active language.

To create new users and assign them access permissions and management privileges, click [Users](#).

To configure the general console settings, click [Preferences](#).

If you want to access the Help, discover the latest Panda Cloud Office Protection news or check the Advanced Administration Guide, select the relevant option in the **Help** drop-down menu. Use this menu as well to view the License Agreement.

### Preferences

From this window you have control over a number of general settings regarding the Web console:



### General options

If you want the QuickStart guide to be displayed every time you log in to the console, select the **Show QuickStart guide on login** checkbox.

### Default view

Choose the way in which computers are displayed: by name or by IP address. Select the option you want.

### Group restrictions

Select this option to limit the number of installations and the [groups'](#) expiry dates. Select the relevant checkbox.

### Remote access

Go to this section to enter the credentials to access other computers using different remote access tools.

These credentials are unique for each user, that is, every user of the administration console will enter their own credentials to access computers.

If you don't want to allow your service provider to access your computers, clear the option **Let my service provider access my computers remotely**.

### Remote access from the Panda Cloud Partner Center console

If the client console is accessed from the Panda Cloud Partner Center console, the credentials entered by the user that accesses it for the first time will be the same as those used by other users of the Panda Cloud Partner Center console that try to access it later.

Every user that accesses the client console from the Panda Cloud Partner Center console will be able to change the access credentials, although this change will affect other users.



### Automatic management of suspicious files

Use this option if you want to send suspicious files to our laboratory for analysis. In the event of malware infection, we will send you a response and distribute adequate protection as soon as possible.

### Account management

If you are a user with [total control permissions](#), you will have access to the [account management](#) feature. To do this, click **Manage accounts**.

### Computer blacklist

You can draw up a list of computers to which the protection will not be distributed. You can always add or remove computers to/from the list. Groups of expired computers and computers whose maximum number of installations allowed has been exceeded are also blacklisted.

Unprotected computers will also appear in the blacklist. Go to the [unprotected computers](#) section for more details.

## License management

### Types of clients

#### Subscriber

Clients who buy licenses with no expiry date. If you are a subscriber client, you will see the following text in the Licenses section in the Status window: "Valid until: Permanent". You won't have to worry about your license expiry date.

#### Non-subscriber

Clients whose licenses have an expiry date. If you are a non-subscriber client, you will see the following text in the Licenses section in the Status window: "Valid until: 00/00/0000".



### Warnings related with licenses

You have a series of Panda Cloud Office Protection licenses. Depending on your needs, you can [install the protection](#) on computers, [uninstall](#) it, remove computers from the list of protected computers, add computers to that list, etc.

As you use your licenses, the number of available licenses will decrease.

### Updating the number of licenses

If you:

**Install the protection on a computer** ► One license is subtracted from the total number of available licenses.

**Remove a computer from the list of protected computers** ► One license is added to the total number of available licenses.

**Reduce by X the number of contracted licenses** ► A number of computers will be blacklisted. This number will be the amount by which the number of contracted licenses has been exceeded.

### License expiry date warning

In the notification area you will see different warnings in relation to the proximity of the expiry date: whether it has been exceeded, if there are less than 30 days remaining, and if licenses expiring would leave you with fewer licenses available than those actually being used.



*In both cases you can renew the license by contacting your usual reseller or sales advisor. Panda Cloud Office Protection will display a reminder in the [Status](#) window. When the 30-day period is over, you will have an additional 15-day grace period to renew the licenses. After this, you will not be able to renew them.*





### Blacklist

A computer can be blacklisted manually or automatically when you try to install the protection on it once the maximum number of installations allowed has been exceeded, or when the license has expired. Automatic blacklisting also occurs when any restrictions placed on a group are exceeded. These restrictions can be configured in the [Preferences](#) screen.

Blacklisted computers don't update. Also, they are not taken into account in the statistics, [reports](#) and scans carried out by Panda Cloud Office Protection. However, the computer license will not be added to the total number of licenses used, but will be subtracted from it.



*A computer can only be removed from the blacklist when there are licenses available and it has been blacklisted manually.*

### Canceling licenses

Where there are several maintenance contracts, this screen shows the most recent expiry date of licenses, the number of licenses that need to be canceled, and the warning that once the expiry date is exceeded the affected computers will be automatically **blacklisted**.

You can choose between canceling the number of licenses that you need in the first computers that had the protection installed or the last. Use the **Cancel licenses menu** and click **Apply**. You will see a list of the computers and licenses that need to be released.

### Computers affected

This is the default tab. It displays the list of computers whose licenses will be canceled and therefore will cease to be administered. The information is divided into four columns: **Computer**, **Group**, **Installation date**, and **Insertion**.

This last column displays the term **Automatic** if the computer has been selected in the **Cancel licenses** menu, or **Manual** if it comes from the **Managed computers** tab. Select the checkbox corresponding to the computer whose license you want to cancel, and then click **Exclude**.



The **Options** menu lets you filter the search of computers, specifying the time when the protection was installed on computers.

### Managed computers

This tab displays the computers that you administer. If you want to add any of them to the list of affected computers, select the corresponding checkboxes and click **Add**. The computer will be moved to the list of affected computers. The **Insertion** column will display **Manual**.

Finally, after the expiry date, the computers and licenses that have been canceled will be sent from the affected computers list to the blacklist.

### Adding licenses using the activation code

#### Adding licenses using the activation code

This feature lets you decide when to add licenses.

From the Web console you can access the **License activation** form to activate the service quickly and simply, using the activation code provided by Panda Security or your distributor when you bought the solution.

Follow these steps:

Click **Add additional licenses** in the **Status** window. You will see the **License activation** window.

Enter the activation code.

Click **OK**.



**Note:** *The process of adding licenses is not immediate, and you will have to wait a short time before the additional licenses are displayed in the **Licences** section of the **Status window**.*




In the event of an error, refer to the [Possible errors in the process of adding licenses](#) section.

### Possible errors when adding licenses

The following errors can occur when entering the activation code:

 *The activation code entered is invalid/doesn't exist*

Make sure you have entered the code correctly.

 *The activation code entered is already in use*

The activation code is already being used. In this case, contact your reseller or sales advisor to obtain a new code.

 *Could not perform the operation*

It is possible that the characteristics of the services/licenses that you have contracted do not allow you to use the license extension feature.

This error will also appear if a Panda Cloud Office Protection client tries to add licenses by entering a Panda Cloud Office Protection Advanced activation code in the Client console and vice versa.

### Other errors

Once you have successfully entered the activation code, you may see the following error:

 *Could not register the request*

This error occurs when the process has failed for an unknown reason. Please try again and if you cannot activate the service, contact Panda Security technical support.



## Account management

### Introduction to account management

If you are a user with [total control permissions](#), you will have access to the Panda Cloud Office Protection account management options: delegating management of an account and managing accounts. Both options can be accessed from the **Account management** screen (*Preferences / Manage accounts*).

### Delegating the management of an account

This feature lets you allow another client to manage the security of your computers. For more information about this option, refer to the section on [Delegating account management](#).

### Merging accounts

When there are several client accounts, they can be merged to allow central management of the security of all the computers. For more information about this option, refer to the section on [Merging accounts](#).

### Delegating the management of an account

#### Delegating the management of an account

If you want to delegate the management of the security of your computers to a partner, you can do so using the **Delegate service** feature. The partner to whom you delegate the service will have access to your console.



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

Follow these steps:

Click **Manage accounts**, in the **Preferences** window. You will see the **Account management** window.



## Panda Cloud Office Protection

---

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

To confirm that you want to continue with the delegation, click **Delegate**.



**Note:** *The process of delegating management is not immediate, and you will have to wait until your data is accessible to the specified partner.*

In the event of an error, refer to the [Possible errors when delegating the management of an account](#) section.

### Possible errors on delegating account management

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



*Invalid identifier. Please make sure you have entered it correctly and try again.*

Please make sure you have entered these details correctly.



*You do not have licenses to perform this operation. Contact your sales advisor or your usual reseller to renew them.*

If your licenses have expired you will not be able to access the management delegation feature.

Please contact your reseller or sales advisor to renew the licenses.



*Could not perform the operation. Please contact your reseller or sales advisor.*

It is possible that the characteristics of the services/licenses that you have contracted do not allow you to use the management delegation feature.

Please contact your reseller or sales advisor.

### Other errors



*An error occurred: could not register the request. Please try again later.*



This error occurs when the process has failed for an unknown reason. Please try again and if you cannot activate the service, contact Panda Security technical support.

## Merging accounts

### Merging accounts

#### What does merging accounts involve?

If you have several client accounts and you want to merge them in order to manage them centrally, you can do this through the account merging function. This lets you manage all your accounts from a single Web console.



*It is **VERY IMPORTANT** that before you merge accounts you understand the consequences. Please refer to the section on [Consequences of merging accounts](#).*

#### How are accounts merged?

Basically, the process consists of transferring data from the source account (account A) to the target account (account B). This target account must already be active.

To merge accounts:

1. Access the Web console of account A (the source account which will be canceled).
2. Click **Manage accounts**, in the **Preferences** window. You will see the **Account management** window.
3. Select **Merge**.
4. Enter the *Login Email* and password of account B (the target account to which the data from account A will be transferred). This data was provided in the welcome message when you opened the account.
5. Once you're sure you want to merge the accounts, click **Merge**.



*The process of transferring data is not immediate, and so it will take time before you can check this has been successful in the account B Web console.*



In the event of an error, refer to the section on [Possible errors in the merging of accounts](#).

### What information is transferred in the process of merging accounts?

The merging of accounts involves transferring information about the computers managed from account A.

Below you will see all the information that is transferred:

**All active maintenance contracts that have not expired**, i.e, information about active licenses, start and end dates, types of licenses, etc.

**Settings profiles.** All settings profiles from the source account. If there is a profile with the same name in the target account (for example, *Sales Profile*), the profile from the source account will be renamed with a numeric suffix (*Sales Profile-1*).



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

**Groups of computers.** All groups of computers. In the case of groups with the same name, the same criteria will be applied as with profiles in the previous point.



*The default group -Default- will be transferred to the target account, but will be considered as just another group and will lose the status of default profile.*

**Information** about active protection and blacklisted computers.

**Reports** and detection statistics.

**All items in quarantine**, including excluded and restored items.



**Web console users** (with their corresponding permissions) except the *default* user.

### Possible errors when merging accounts

When accessing the form for **merging accounts**, you may encounter the following errors:

*The Login Email and/or password are incorrect*

Please make sure you have entered these details correctly.

*Could not perform the operation*

It is possible that the characteristics of the services/licenses that you have contracted do not allow you to use the merge accounts feature. Please check with your reseller or sales advisor.

*You do not have licenses to perform this operation*

If your licenses have expired you will not be able to access the merge account feature. Please contact your reseller or sales advisor to renew the licenses.

*The specified account is already being merged*

If the account B (target account) that you have specified is already being merged, you will have to wait for that process to finish before starting.

*The account with which you have started the session exceeds the maximum number of computers allowed*

The process of merging accounts is only possible if account A (source account) has less than 10,000 computers.

*The accounts to be merged belong to different versions of Panda Cloud Office Protection*

For the merging of accounts A and B to be carried out correctly, they must both correspond to the same version of Panda Cloud Office Protection. It is unlikely that the accounts belong to different versions, other than in situations where a version has been updated.





### *Could not register the request*

This occurs when the process has failed for an unknown reason. Please try again and if you cannot merge accounts, contact Panda Security tech support.

## Consequences of merging accounts

Before merging accounts, it is **VERY IMPORTANT** that you are aware of the consequences:

The **services associated** to account A **will cease to be active**, and the account will be deleted. Obviously, access to the Web console from account A will be denied.

In the Web console of account B you will see the data and information about computers managed from account A. To check this, just access the Web console from account B.

The protection installed in computers managed from account A **will be reassigned automatically**, and will be manageable from account B. **It will not be necessary to reinstall the protection.**



*The process of transferring data is not immediate, and so it will take time before you can check this has been successful in the account B Web console.*

In the event of an error, refer to the section on [Possible errors in the merging of accounts](#).

## Creating and managing users

### Creating and managing users

If the default option offered by Panda Cloud Office Protection does not adapt to the protection needs of your network, you can create new users and assign different types of permissions, depending on what you want each user to manage.



In the main screen of the Web Console, click **Users**.

The **Users** window distributes information in three columns: **Name**, **Permissions**, and **Status**. As you create users, these appear in the list, along with the type of permissions that you have given them and their status (enabled or disabled).

You may need to create new user groups and assign them different permissions for management and control of groups. Panda Cloud Office Protection makes this very easy for you.



*The default user displayed by Panda Cloud Office Protection cannot be removed, and only the comments can be modified. The application displays it in the list as a name (default user).*

1. Click **Create new user** to access the **Users - Edition** window. Fill out the User name, Email, Password and Repeat password fields.
2. You can add information in the **Comments** section.
3. In **Groups**, select the group or groups on which the administrator and monitoring user can operate, in accordance with the permissions you have assigned them. Users with total control permissions can act on all groups.
4. Click **OK**.
5. In the main **Users - Edition** window, check that the user has been created and that the name, permission and status appear correctly in the list.
6. To remove a user, select the corresponding checkbox and click **Delete**.

## Types of permissions

### Types of permissions

Panda Cloud Office Protection includes three types of permissions. The permission assigned to a user will dictate which actions they can take and on which computers or groups.



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

The permissions that exist are:

 [Total control](#)

 [Administrator](#)

 [Monitoring](#)

Select the type of permission to consult the specifications. This will be useful for assigning different functions to members of your team, and getting maximum performance from all the Panda Cloud Office Protection security features.

## Total control permission

### User management

1. View all users created on the system.
2. Remove users.

### Profile management

1. Copy profiles and view all copies made of all profiles.
2. Configure scheduled scans of specific paths for each profile.

### Group and computer management

1. Create and delete groups.
2. Manage the configuration of the protection profiles of all groups.
3. Assign computers to groups.
4. Move computers from one group to another.



5. Edit the **Comments** field in the [Computer details](#) screen.
6. Access any computer remotely.

### Unprotected computer search

1. Configure searches for unprotected computers.
2. View and/or remove any of the jobs created.

### Managing licenses and accounts

1. Use the option to [extend licenses using the activation code](#).
2. Use the option to [merge accounts](#).
3. [Delegate security management](#) to a partner.

### Protection uninstallation

1. Configure protection uninstallation jobs.
2. View and/or remove any of the jobs created.

### Administrator permission

The user management and protection settings/uninstallation actions that administrator users can perform, are restricted to those users, computers or groups on which the administrator user has permission.

### User management

Administrator users can:

1. Modify their user credentials.
2. Create users.



### Unprotected computer search

Administrator users can:

1. Create search jobs to be launched by computers on which they have permissions.
2. View and/or delete any of the previously created search jobs but only from computers in groups on which they have permissions.

### Group and computer management

Administrator users can:

1. Create groups and manage the profile settings for the groups on which they have permissions.
2. Delete groups on which they have permissions.
3. Edit the **Comments** field of the computers on which they have permissions, in the [Computer details](#) screen.
4. Remotely access computers that belong to groups on which they have permissions.

### Protection uninstallation

Administrator users can:

1. Configure uninstallation tasks on computers and groups on which they have permissions.
2. View and/or delete uninstallation jobs, but only on computers belonging to groups on which they have permissions.

### Profile management

Administrator users can:

1. Create and view new profiles.
2. Create copies of profiles on which they have permission and view them.
3. Configure scheduled scans of specific paths for profiles on which they have permissions or which they have created.



### Monitoring permission

Users can:

1. Modify their credentials.
2. View and monitor the protection of the groups assigned to them.
3. View profiles assigned to groups on which they have permissions.
4. View searches for protected computers made from computers belonging to groups on which they have permissions.
5. View uninstallation jobs in groups on which they have permissions.

## Configuring the protection

### Introduction

The protection provided by Panda Cloud Office Protection is designed to be installed and distributed across your IT network. Therefore, the protection to be installed will vary depending on the computers to protect and your specific security needs.

You can configure the protection before or after installation. To do this, you have to create a [profile](#) and then assign it to a group or groups.

In this Help file the configuration process is explained as a step prior to installing the protection on the computers.

When assigning profiles to the groups created, there are several options: one single profile applied to several groups, each group with a different profile, or just one profile and one group.

When you create a profile you configure the way that the protection will operate for this specific profile, i.e., you determine which types of scans are carried out on which elements, and how often the protection is updated.



## Panda Cloud Office Protection

---

Before starting to **install** the protection, you must create and configure the profiles you need. Then, create groups of computers and assign profiles to the groups, so that each group will have a specific protection profile.



*If you do not need to create any profiles or groups in addition to those Panda Cloud Office Protection includes by default, go to the **Installation and settings** menu and select the **Default** group. Then, select the installation mode you want to use for installing the protection on your computers.*

### Default profile

Select **Profiles** to go to the **Installation program profiles** window. This window displays the existing profiles.

The first time you go to this window you will see the **Default** profile and information about the associated protection (Antivirus, Firewall, Device Control and Exchange Servers).

The Exchange Server protection is disabled by default, and can only be enabled by clients with Panda Cloud Office Protection licenses.



*The Exchange Server protection supports Exchange 2003, 2007 and 2010.*

If at any time you want to change the settings of this profile, click its name. This will take you to the **Edit profile** window. Make any changes you require and save them using the **Save** option. If later you want to restore the original settings of the profile, you can do so using the option **Restore default settings** in the **Edit profile** window.

## Creating/copying profiles

### Creating a profile

If you need to create new profiles, they will be displayed in the **Installation program profiles** window next to the **Default** profile with information about the protection included.



You can always edit the settings of a profile by clicking on its name and going to the **Edit profile** window as explained for the default profile.

If you try to assign a profile name that is already being used, an error message will appear.

### Permissions needed

If you cannot view the profile that already exists, it is probably because you do not have the relevant permission. For more information, refer to the [Types of permission](#) section.

To create a new profile, click **Create new profile**, and go to the **Edit profile** window. From there you will be able to [configure the new profile](#).

### Configuring the profile

Configuration of the profile is structured in the following sections: General, Antivirus, Firewall, Device Control and Exchange Server protection (this option is only available if you have Panda Cloud Office Protection Advanced licenses).

The whole configuration process is described in the following sections:

[General profile settings](#)

[Antivirus protection settings](#)

[Firewall protection settings](#)

[Device Control settings](#)

[Exchange Server protection settings](#)

### Copying a profile

Panda Cloud Office Protection gives you the option to make copies of existing profiles. This is useful when you think that the basic settings of a profile that you have created could be used for other computers.





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

To use this option, copy the profile by clicking **Installation and settings > Profiles** and go to the **Installation program profiles** screen. Select the profile you want to copy -up to 10- and click **Copy**.

Once you have copied the profile, this will be displayed with the name *Copy of <profile\_name>*, and you can rename it by clicking it and entering a name in the **Edit profile** screen.



*In the case of the Default profile, you can make a copy, although the copy will not have the status of default profile and will not be assigned automatically to any computer. The original Default profile will be the only predetermined one.*

Profile copying is subject to the permissions that you have. For more information refer to the section on [Types of permission](#).

## General profile settings

### General profile settings

In this section you can select general configuration options related to the profile, and it is therefore important to have a clear idea of the type of profile you want, largely depending on the computers that you want to protect with this profile.

To access the settings, click Installation and settings / Profiles / Create new profile.

#### *Main tab*

The options in this tab will allow you to name the profile you are creating and enable automatic updates of the protection engine and the [signature file](#). Select the relevant checkboxes.



You can also add an additional description to identify the profile and select the language in which you want the protection installed. By clicking **Advanced settings** you will go to the [Edit profile – Advanced settings](#) window.

### *Scheduled scans tab*

Click the **Scheduled scans** tab to create periodic, individual or immediate scan tasks of the entire PC or certain parts of it.

You can also schedule scans just of email or specify specific paths to scan the folders or files that you want.

### *Warnings tab*

Here you can configure warnings to be displayed when malware, intrusion attempts or unallowed devices are detected on computers. You can also indicate whether these warnings will be local, by email or both.

The difference is that local warnings are displayed on the computer or computers on which the detection occurs, while the email warnings are sent to the selected computers. Follow these steps:

1. First, select the checkbox Send warning via email on detection of malicious software.
2. Complete the **Message subject** field.
3. Enter an email address and specify the SMTP server to be used for sending warnings. If the server requires authentication, enter the corresponding user name and password.
4. Click **OK**.

### *Apply to tab*

When you assign the profile to a group or groups, these will appear in this list.



### Scheduled scan settings

By selecting the **Scheduled scan** tab you can create, periodic on-demand or immediate scan tasks of either the whole computer or just certain components.

You can also schedule scans just of email or specify specific paths to scan the folders or files that you want.

As you create scan jobs, these will be added to the list of **Scheduled scans** in the **Edit profile** window, from which you can edit them or remove them if desired.

### How to configure scans

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

Follow these steps:

1. **Name:** Choose a name for the scan job.
2. **Scan type:** Select the type of scan you want to create (immediate, scheduled or periodic).



**Immediate scan:** Once you have configured the scan, it will take place as soon as the computer connects to the Panda Cloud Office Protection server and the solution recognizes that there has been a change to the protection settings.



**Scheduled scan:** The scan will take place at the date and time that you have set in the **Start date** and **Start time** fields.



**Periodic scan:** Set the **Start date and time** and select the frequency in the **Repetition** drop-down menu.

**Scan:** Select the option you want.

All the computer



Hard disks

Email

Other items

Use this option to scan specific items (files, folders, etc.). Enter the path of the item to scan. The format of the path must start with `\\`, (letter):`\`. Examples:

\* `\\folder1\folder2`

\* `c:\folder1\folder`

No more than 10 paths can be included for each profile. You can establish the paths of specific items to scan depending on the permissions that you have. For more information, refer to the [Types of permission](#) section.

**Start date:** Specify the date of the scan.

**Start time:** Specify the time of the scan bearing in mind whether the time is that of the local computer or the Panda Cloud Office Protection server.

**Repetition:** If the scan is periodic, here you can specify the frequency (daily, weekly or monthly).

## Advanced scan settings

You can access this screen from the **Advanced settings** link in the **Edit profile – new scan job** screen. Here you can configure additional aspects of the [scheduled scans](#).

Follow these steps:

1. Select in the general settings section if you want to enable scanning of compressed files.
2. Select the malicious software you want to scan for.



3. You can scan the entire computer or exclude certain folders or files with specific extensions. Use the **Add**, **Clear** and **Delete** buttons to define the list of excluded items.

### Edit profile - Advanced settings

You can access this window by clicking on the **Advanced settings** link in the **Main** tab of the **Edit profile** window.

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

### Installation

Indicate in which directory you want to install the protection. Panda Cloud Office Protection will show a default path, which you can change if you want.

### Internet connection

Specify the computer's Internet connection, if it uses a proxy, and if proxy authentication is required.

### Connection to Collective Intelligence

Administrators can disable scans with Collective Intelligence. It is advisable to keep this option enabled if you want to benefit from all the protection provided by Collective Intelligence.

### Server connection options

Establish how often you want the computer to send information to the Panda Cloud Office Protection servers about the status of the protection installed. You can change the frequency displayed by default, but it must be a value between 12 and 24 hours.



## Panda Cloud Office Protection

---

You can also specify the computer through which connections with the Panda Cloud Office Protection server are centralized. To do this, select the corresponding checkbox and click **Select**. In the **Computer selection** screen, choose the computer or search for it using the **Find** button. Then click **OK**.

### Requirements for the computer to use for connections to the server:

1. Internet connection.
2. At least 128 MB of RAM.
3. It must be a [protected computer](#) (in the list of protected computers) and have version 5.04 or later of the agent.
4. It must not be in the [blacklist](#).
5. It must not go more than 72 hours without connecting to the server.

### Quarantine options

Files in quarantine are analyzed to determine whether they represent a threat or not. If they do not represent a threat, you can restore the files using the Restore option in the Quarantine window and indicating the path to the directory.

### Uninstallation

Use this section if you want to set an uninstallation password. This will be required when you want to uninstall the protection from those computers to which the profile is applied.

## Antivirus protection settings

### Antivirus protection settings

To access the antivirus protection settings, click Installation and settings / Profiles / Create ☐ new ☐ profile / ☐ Antivirus.

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



### Files tab

Here you can configure the basic operation of the antivirus with respect to file protection. If you want more detailed settings, click **Advanced settings**. This will take you to the [Advanced antivirus settings - File protection](#) window.

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



*Detection of viruses will always be enabled while the file protection is enabled.*

If you want the protection to block malicious actions and suspicious behaviors select the relevant checkbox.

### Mail tab

In this window you can configure how the email antivirus protection will operate in the profile you are creating. If you want more detailed settings, click **Advanced settings**. This will take you to the [Advanced antivirus settings - Mail protection](#) window.

1. Indicate if you want to enable the permanent email protection, as well as scanning compressed files.
2. Select the malicious software to detect. Select the relevant checkboxes.
3. Click **OK**.

### Local scans

Panda Endpoint Protection is the name of the protection that Panda Cloud Office Protection deploys and installs on computers. Once installed, you can access different scan options through the Windows right-click menu or through the right-click menu of the protection itself.



### Right-click scan of a selected item

Select a folder, drive, file or any other scannable item and right-click it. You will then see a Windows menu, giving you the option to **Scan with Panda Endpoint Protection**.

The scan will be launched immediately. You can pause the scan and restart it later. When it is finished you will see the result of the scan and you will also be able to print, export or save the report.

### Local scans from Panda Endpoint Protection

#### Optimized scan

If you select this option, Panda Endpoint Protection will scan the computer folders that usually contain malware in order to detect and remove threats as soon as possible.

#### Other scans

You will have two options once you click this option:

#### ***Scan all My Computer***

This option carries out an in-depth scan of all items on your PC: all disk drives, memory, etc. The duration of the scan will depend on the amount of data stored on your computer, as well as the computer characteristics.

#### ***Scan other items...***

This is the option to use when you only want to scan a specific file, folder, etc. It lets you scan just the selected items rather than your entire computer. Once you select this option, indicate which folders or files you want to scan and click **Start**.



**Important:** Make sure your computer is connected to the Internet before starting the scan to ensure maximum detection capacity.





Apart from these on-demand scans, Panda Endpoint Protection also protects you permanently by scanning all the files that you open or run at any time, and neutralizing any possible threats.

### Advanced antivirus settings - File protection

This screen lets you configure the file protection options for a profile. You can do this based on general criteria for all types of files or scan only those files with a certain extension. Similarly, you can also select certain file extensions to exclude from scanning.

#### Exclusions

1. Use the relevant button (**Add**, **Delete** and **Clear**) to make up the list of items (Extensions, Folders, Files) to exclude from scans.
2. When you have finished, click **OK** to save the changes.

### Advanced antivirus settings - Email protection

To ensure an optimum level of protection on your computers, it is essential to protect them from threats that can reach systems through email.

Panda Cloud Office Protection lets you configure the email antivirus protection for each profile. You can do this generally, for all files received, or according to extensions.

1. Use the **Add**, **Delete** and **Clear** buttons to define the excluded items list.
2. When you have finished, click **OK** to save the changes.



## Firewall protection settings

### Introduction

Firstly, you must decide if the users to which the profile will be applied will be allowed to configure the firewall from their computers. If so, select **Allow configuration of the firewall by the client**.

Otherwise, if you want the configuration to be available only from the [Web console](#), you, as the administrator, will establish the restrictions, blocking, permissions, etc.

If you choose to configure the firewall from the Web console, keep the default option to **Apply the following firewall settings** and continue configuring it through the General, Programs, Intrusion prevention, and System tabs.

Below is a description of the different settings available in each mode.

### Configuration from the Web administration console

Select the option **Apply the following firewall settings** in the **Edit Profile** screen.

Selecting this option enables the following settings:

**General:** Global firewall protection configuration options.

**Programs:** Configuration of Program rules.

**Intrusion prevention:** Configuration of the types of intrusions detected by the Firewall protection.

**System:** Configuration of System rules.

Select to enable the firewall for Windows workstations and/or servers.



## Panda Cloud Office Protection

We now describe the options included in each configuration section (General, Programs, Intrusion prevention and System).

### Edit profile

Profile: New profile (2012-04-17 10:43:24)

- ☐ Allow configuration of the firewall by the client.  
☒ Apply the following firewall settings.

- ☒ Enable firewall for Windows workstations  
☐ Enable firewall for Windows servers

General

Programs

Intrusion prevention

System

The behavior of the firewall will depend on the type of network to which it is connected. The type of network is assigned automatically depending on the location of the computer and this setting can be modified from here.

Select the type of network to which you are connected:

- ☐ Public network  
Public locations, such as airports, cybercafés, universities, etc. Your computer will be visible to other users of the network and use of the network will be limited for some programs
- ☒ Trusted network  
Home or office networks where you know and trust the other users and the devices on these networks. Your computer will be visible to other network users and you can also see computers and devices on the network



### General

This section contains the general firewall settings.

#### Network selection

The firewall behavior depends on the type of network the user is connected to. Select the type of network the computers that belong to the selected profile are connected to. The restrictiveness of the firewall will depend on the type of network:

##### Public network

The network is visible to other users and therefore has a low security level. In this type of network, the firewall is configured more restrictively to increase computer security.

##### Trusted network

Private network, not visible to users from the outside. In these cases, network security is already higher and the firewall behaves more permissively, yet without compromising computer security.

As you will see later, administrators can define new program and system rules that only apply to computers configured with one network type, or which apply to both.

### Program rules

In this section, you can define the connection permissions for applications running on computers. There is a series of predefined Panda rules which establish permissions for common applications.



## Panda Cloud Office Protection

General

Programs

Intrusion prevention

System

You can establish which programs can communicate using the network.

☒ Enable Panda rules.

Show: 

User rules

Programs	Communication
No items available.	

Add

Settings

Delete

Below is a description of the available options:

**Enable Panda rules:** You can enable or disable the set of predefined program rules. This set of rules includes the settings of the communication permissions for common applications, and is updated from Panda Security through the signature file.

**Show:** You can select the set of rules to display.

**Panda rules:** The rules defined by Panda will be displayed. These rules cannot be configured by administrators, they can only be viewed, enabled or disabled.



## Panda Cloud Office Protection

☒ Enable Panda rules.

Show: Panda rules

Programs ▲	Communication
\$CommonProgramFiles\System\Mapi\...	Allow inbound and outbound connecti
\$CommonProgramFilesWoW64\System\...	Allow inbound and outbound connecti
\$ProgFilesDir\Internet Explorer\...	Custom
\$ProgFilesDir\Microsoft ActiveSy...	Custom
\$ProgFilesDir\Microsoft ActiveSy...	Custom
\$ProgFilesDir\Microsoft ActiveSy...	Custom
\$ProgFilesDir\Mozilla Firefox\fi...	Custom
\$ProgFilesDir\Mozilla Firefox\up...	Custom
\$ProgFilesDir\Mozilla Thunderbir...	Custom
\$ProgFilesDir\Mozilla Thunderbir...	Custom
\$ProgFilesDir\Outlook Express\ms...	Custom
\$ProgFilesDir\Windows Mail\WinMa...	Custom
\$ProgFilesDir\Windows Media Play...	Custom
\$ProgFilesDir\Windows Sidebar\si...	Custom
\$ProgFilesWoW64Dir\cmdl32.exe	Custom

1 2 3 4 5 6 7 8 9 10 ...

### User rules

The rules defined by the administrator will be displayed. To create a new rule, click **Add** and access the next screen.

### Edit profile - New program rule

Profile: New profile (2012-04-17 10:55:35)

Enter the information about the program that you want to configure:

Program:

Browse...

Communication: No connection

OK Cancel

Enter the executable file of the application you want to create a rule for. You can do this in two ways:

By clicking **Browse**



When you click the button, Windows Explorer will open. This will allow you to select the application you want to create a rule for. This is only possible if the application is installed on the computer from which you are accessing the Web administration console.

**Program:** Enter the path of the application (on computers belonging to this profile).

**Edit profile - New program rule**

Profile: New profile (2012-04-17 10:55:35)

Enter the information about the program that you want to configure:

Program:

Communication:

OK Cancel

Then, select the Communication permissions that will be granted to the program from the drop-down menu.

The types of connections are:

### No connection

The application will not be able to communicate. Consequently, all inbound and outbound connections will be denied.

### Allow inbound and outbound connections

The program will allow outbound connections and inbound connections (it will allow other programs or users to connect to it). Some programs, such as file exchange programs, require these types of permissions to operate correctly.



### Allow inbound connections

The program will allow inbound connections (from programs or users), but it will deny outbound connections.

### Allow outbound connections

The program will allow outbound connections, but will deny inbound connections (from other users or applications).

In order to deny all communications, select **No connection** and click **OK** to finish creating the rule.

The rule created will be added to the User rules list.

The User rules list lets you modify the type of communication configured in a rule, by selecting any of the previously mentioned communication types:

No connection

Allow inbound and outbound connections

Allow inbound connections

Allow outbound connections

Here there is a new type:

### Custom

In the previous connection types, inbound and outbound communication permissions are assigned to a program regardless of the communication ports, protocols, etc.

If necessary, you can create advanced program connection rules by creating a Custom rule and indicating the ports, protocols, etc. the programs can use.





## Panda Cloud Office Protection

General Programs Intrusion prevention System

You can establish which programs can communicate using the network.

☒ Enable Panda rules.

Show: User rules

Programs	Communication
Depl_0	No connection

Add  
Settings  
Delete

On selecting **Custom** as the communication type, the **Settings** button is enabled.

### Edit profile - Custom permission settings

Profile: New profile (2012-04-17 10:55:35)

Custom permission settings

Program:  
Depl\_0

Action	Direction	Zone	Protocols	Ports	IPs
Deny	Inbound	All	All	All	All
Deny	Outbound	All	All	All	All

Up  
Down  
Add...  
Settings...  
Delete

(the permissions will be defined in descending order and if there is no corresponding rule defined, the connection will be allowed)

Click this button to access the **Custom permission settings** screen, where the rule settings are displayed.



**Edit profile - Edit custom permission rule**

Profile: New profile (2012-04-17 10:55:35)

Action:	Deny	Zone:	All
Direction:	Inbound	Protocol:	All
Ports:	All	Custom:	
IPs:	All	Custom:	

OK Cancel

In this case, we will show you how to customize a **No connection**-type rule, which involves two firewall rules.

In this section you can configure the following rule values:

### Action

This lets you configure the action to be taken by the rule:

- Allow application communication.
- Deny application communication.

### Direction

This lets you configure the communication direction:

### Inbound

The rule will only apply to inbound communications aimed at the application.

### Outbound

The rule will only apply to outbound communications generated by the application.

### Zone

This lets you define the zone in which the rule will be applied:



### Trusted network

The rule will only apply to computers that belong to a profile with a network configured as a Trusted network.

### Public network

The rule will only apply to computers that belong to a profile with a network configured as a Public network.

### All

The rule will apply to all computers that belong to a profile, regardless of the zone configured.

**Edit profile - Edit custom permission rule**

Profile: New profile (2012-04-17 10:55:35)

Action:	Deny	Zone:	All
Direction:	Inbound	Protocol:	All
Ports:	All	Custom:	TCP
IPs:	All	Custom:	UDP

OK Cancel

### Protocol

This lets you define the communication protocol:

#### TCP

The rule will only apply to the communications carried out by the application through the TCP protocol.

#### UDP

The rule will only apply to the communications carried out by the application through the UDP protocol.



### **All**

The rule will apply to all the communications carried out by the application through the TCP and UDP protocols.

### **Ports**

In this section you can select the port(s):

#### **All**

It will apply to all the ports used by the application.

#### **Custom**

This lets you define the ports that the application rule will apply to.

Selecting this option will enable the **Custom** field, where you can enter the port values:

#### **Single port**

Enter the port value (For example: 4662).

#### **List of ports**

Enter a list of ports separated by commas (For example: 4662, 4665).

#### **Range of ports**

Enter a list of ports separated by a dash (For example: 4662-4665).

#### **Lists and ranges**

Use a combination of the previous methods (For example: 4662, 4665-4670, 4675).

#### **Predefined ports**

A list of common ports.



### Edit profile - Edit custom permission rule

Profile: New profile (2012-04-17 10:55:35)

Action:	Deny	Zone:	All
Direction:	Inbound	Protocol:	All
Ports:	All	Custom:	
IPs:	Custom	Custom:	

- 7 (echo)
- 9 (discard)
- 11 (sysstat)
- 13 (daytime)
- 17 (qotd)
- 19 (chargen)
- 20 (ftp data)
- 21 (ftp)
- 23 (telnet)
- 25 (smtp)
- 37 (time)
- 39 (rip)
- 42 (nameserver)
- 43 (nicname)
- 53 (domain)
- 67 (bootps)
- 68 (bootpc)
- 69 (tftp)
- 70 (gopher)
- 79 (finger)
- 80 (http)
- 88 (kerberos sec)
- 101 (hostname)
- 102 (iso tsap)
- 107 (rtelnet)
- 109 (pop2)
- 110 (pop3)
- 111 (sunrpc)

OK Cancel

Panda Security 2012

Console optimized for IE7, Firefox 3, Chrome 4.0

### IPs

In this section you can select the IP address(es):

### All

It will apply to all the IP addresses the application accesses.

### Custom

This lets you define the IP address(es) the rule will apply to if they are accessed by the application.



Selecting this option enables the **Custom** field, where you can enter the following IP values:

### Single IP address

Enter the IP address value (For example: 192.168.1.10).

### List of IP addresses

Enter a list of IP addresses separated by commas (For example: 192.168.1.10, 192.168.1.15).

### Range of IP addresses

Enter a list of IP addresses separated by a dash (For example: 192.168.1.10-192.168.1.15).

### Lists and ranges

Use a combination of the previous methods (For example: 192.168.1.10, 192.168.1.15-192.168.1.20, 192.168.1.25).

**Edit profile - Edit custom permission rule**

Profile: New profile (2012-04-17 10:55:35)

Action:	Deny	Zone:	All
Direction:	Inbound	Protocol:	All
Ports:	All	Custom:	
IPs:	All	Custom:	

IPs dropdown menu options: All, Custom

OK Cancel

In this case, define a rule to deny inbound connections to port 57884 of the TCP protocol for all the IP addresses, which only applies to computers on Trusted networks.



### Edit profile - Edit custom permission rule

Profile: New profile (2012-04-17 10:55:35)

Action:	Deny	Zone:	All
Direction:	Inbound	Protocol:	TCP
Ports:	Custom	Custom:	57884
IPs:	All	Custom:	

OK Cancel

Click **OK** to return to the **Custom permission settings** section, where a summary of the changes made to the rule is displayed:

### Edit profile - Custom permission settings

Profile: New profile (2012-04-17 10:55:35)

Custom permission settings

Program:  
Depl\_0

Action	Direction	Zone	Protocols	Ports	IPs
Deny	Inbound	All	TCP	57884	All
Deny	Outbound	All	All	All	All

Up  
Down  
Add...  
Settings...  
Delete

(the permissions will be defined in descending order and if there is no corresponding rule defined, the connection will be allowed)

OK Cancel

Repeat the same process to configure the rule for outbound connections:

In this case, define a rule to deny outbound connections to port 57884 of the TCP protocol for all the IPs, which only applies to computers on Trusted networks.



### Edit profile - Edit custom permission rule

Profile: New profile (2012-04-17 10:55:35)

Action:	Deny	Zone:	Trusted network
Direction:	Outbound	Protocol:	TCP
Ports:	Custom	Custom:	57884
IPs:	All	Custom:	

OK

Cancel

Click **OK** to return to the **Custom permission settings** section, where a summary of the changes made to both rules is displayed:

### Edit profile - Custom permission settings

Profile: New profile (2012-04-17 10:55:35)

#### Custom permission settings

Program:  
Depl\_0

Action	Direction	Zone	Protocols	Ports	IPs
Deny	Inbound	All	TCP	57884	All
Deny	Outbound	All	All	All	All
Deny	Outbound	Trusted ne...	TCP	57884	All

Up

Down

Add...

Settings...

Delete

(the permissions will be defined in descending order and if there is no corresponding rule defined, the connection will be allowed)

OK

Cancel

Click **OK** to finish customizing the rule and return to the **Edit profile** section, where a list of the defined user rules (including the customized rule) will be displayed:





### Edit profile

Profile: New profile (2012-04-17 10:55:35)

☐ Allow configuration of the firewall by the client.  
☒ Apply the following firewall settings.

☒ Enable firewall for Windows workstations  
☐ Enable firewall for Windows servers

**General** **Programs** Intrusion prevention System

You can establish which programs can communicate using the network.

☒ Enable Panda rules.

Show: User rules ▾

Programs ▴	Communication
Depl_0	Custom ▾

Add  
Settings  
Delete



To eliminate the rule created, select it from the user rules list, and click **Delete**.

A message will be displayed requesting confirmation to delete the rule.

If you click **Yes**, the rule will be deleted. If you click **No**, you will return to the **Edit Profile** screen and the rule will remain.

Once you have defined the rules to apply to the profile's computers, you can specify how the firewall behaves for applications without a defined rule:

In cases where there is no rule defined, the following action will be applied:	
Default action:	<div><div>Allow access</div><div>▼</div><div>Allow access</div><div>Deny access</div></div>

You can:

- **Allow access:** The communications of all the applications without a defined rule will be allowed.
- **Deny access:** The communications of all the applications without a defined rule will be denied.



### Intrusion prevention

In this section you can configure the types of intrusions that will be detected by the firewall. You can enable or disable the detection of different intrusion types through the relevant checkbox:

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> IP explicit path | <input type="checkbox"/> Smart WINS               |
| <input checked="" type="checkbox"/> Land Attack      | <input type="checkbox"/> Smart DNS                |
| <input checked="" type="checkbox"/> SYN flood        | <input type="checkbox"/> Smart DHCP               |
| <input checked="" type="checkbox"/> TCP Port Scan    | <input checked="" type="checkbox"/> ICMP Attack   |
| <input checked="" type="checkbox"/> TCP Flags Check  | <input type="checkbox"/> ICMP Filter echo request |
| <input checked="" type="checkbox"/> Header lengths   | <input checked="" type="checkbox"/> Smart ARP     |
| <input checked="" type="checkbox"/> UDP Flood        | <input checked="" type="checkbox"/> OS Detection  |
| <input checked="" type="checkbox"/> UDP Port Scan    |   |



### System rules

System rules (unlike application rules) affect all network communications. They work at protocol, port and service level, and have priority over application rules.

In this section, you can create new rules, view existing rules, modify them or delete them. To make the configuration process easier, a series of rules predefined by Panda is provided.

The screenshot shows the 'System' tab in the configuration interface. At the top, there are four tabs: 'General', 'Programs', 'Intrusion prevention', and 'System'. Below the tabs, a message states: 'Add the connection rules you want. These rules are general and have priority over rules selected individually for each program.' There is a checkbox labeled 'Enable Panda rules.' which is checked. Below this is a 'Show:' dropdown menu currently set to 'User rules'. A table with columns 'Rule name', 'Action to take', 'Protocol', and 'Direction' is shown, containing the text 'No items available.' To the right of the table are buttons for 'Up', 'Down', 'Add', 'Settings', and 'Delete'. At the bottom left of the table area are navigation arrows.

Below is a description of the available options:

#### Enable Panda rules

You can enable or disable the system rules predefined by Panda. This set of rules includes the settings of the communication permissions for the most popular network services, and can be updated from Panda through the signature file.

This close-up shows the 'Show:' dropdown menu. It has a checked checkbox for 'Enable Panda rules.' and a dropdown arrow. The dropdown list is open, showing three options: 'User rules' (selected), 'User rules', and 'Panda rules'. A 'Rule' label is visible to the left of the dropdown list.



### Show

Select the set of rules to be displayed:

### Panda rules

The rules defined by Panda will be displayed. These rules cannot be configured by administrators, they can only be viewed, enabled or disabled.

☒ Enable Panda rules.

Show: Panda rules

Rule name	Action to take	Protocol	Direction
Deny NetBIOS (TCP) in in...	<span>Deny communication</span>	TCP	Inbound
Allow Windows Messenger ...	<span>Allow communication</span>	UDP	Inbound
Deny Windows Messenger S...	<span>Deny communication</span>	UDP	Inbound
Allow Distributed Transa...	<span>Allow communication</span>	TCP	Inbound
Block Distributed Transa...	<span>Deny communication</span>	TCP	Inbound

1

### User rules

The rules defined by the administrator are displayed.

Show: User rules

Rule name	Action to take	Protocol	Direction
No items available.			

Up  
Down  
  
Add  
Settings  
Delete



In this case, no user rule has been defined for this profile. To create a new rule, click **Add** and go to the next screen.

### Edit profile - New system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:	<input type="text" value="Allow"/>	Protocol:	<input type="text" value="TCP"/>
Direction:	<input type="text" value="Outbound"/>	Local ports:	<input type="text" value="All"/>
Zone:	<input type="text" value="All"/>	Custom:	<input type="text"/>
		Remote ports:	<input type="text" value="All"/>
		Custom:	<input type="text"/>

PC it applies to:

IP:	<input type="text"/>	<i>Example: 192.168.1.1-192.168.1.254,172.1.1.1</i> <i>Write the addresses and ranges separated by commas.</i>
MAC:	<input type="text"/>	<i>Example: 00:12:49:7D:22:F7</i> <i>Write the addresses and ranges separated by a colon.</i>

In this section you can configure the following rule values:

### Rule name

Identifier or description of the rule being created.

### Action

This lets you configure the action to be taken by the rule:

Allow communication.

Deny communication.

### Direction

This lets you configure the communication direction:



### **Inbound**

The rule will only apply to inbound communications (generated externally and aimed at the computer).

### **Outbound**

The rule will only apply to outbound communications (outbound communication generated in the computer).

### **Zone**

This lets you define the zone in which the rule will be applied:

#### **Trusted network**

The rule will only apply to computers that belong to a profile with a network configured as Trusted network.

#### **Public network**

The rule will only apply to computers that belong to a profile with a network configured as Public network.

### **All**

The rule will apply to all computers that belong to a profile, regardless of the zone configured.

### **Protocol**

This lets you define the communication protocol:

#### **TCP**

The rule will only apply to communications carried out on the computer through the TCP protocol.

#### **UDP**

The rule will only apply to communications carried out on the computer through the UDP protocol.



### ICMP services

The rule will only apply to communications carried out on the computer through different services that use the ICMP protocol.

### IP types

The rule will only apply to communications carried out on the computer through different services that use the IP protocol.

### Edit profile - New system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:	<input type="text" value="Allow"/>	Protocol:	<input type="text" value="TCP"/>
Direction:	<input type="text" value="Outbound"/>	Local ports:	<div><div>TCP</div><div>UDP</div><div>ICMP services</div><div>IP types</div></div>
Zone:	<input type="text" value="All"/>	Custom:	<input type="text"/>
		Remote ports:	<input type="text" value="All"/>
		Custom:	<input type="text"/>

PC it applies to:

IP:	<input type="text"/>	Example: 192.168.1.1-192.168.1.254,172.1.1.1 Write the addresses and ranges separated by commas.
MAC:	<input type="text"/>	Example: 00:12:49:7D:22:F7 Write the addresses and ranges separated by a colon.

If you select the TCP or UDP protocol, you can configure the following values:

### Local ports

Ports used by the local computer to communicate.

### Remote ports

Ports used by the target computer to communicate.





## Edit profile - New system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:  Protocol:

Direction:  Local ports:

Zone:  Custom:

Remote ports:

Custom:

PC it applies to:

IP:  Example: 192.168.1.1-192.168.1.25  
Write the addresses and ranges separated by commas

MAC:  Example: 00:12:49:7D:22:F7  
Write the addresses and ranges separated by commas

© Panda Security 2012

7 (echo)  
9 (discard)  
11 (systat)  
13 (daytime)  
17 (qotd)  
19 (chargen)  
20 (ftp data)  
21 (ftp)  
23 (telnet)  
25 (smtp)  
37 (time)  
42 (nameserver)  
43 (nioname)  
53 (domain)  
70 (gopher)  
79 (finger)  
80 (http)  
88 (kerberos sec)  
101 (hostname)  
102 (iso tsap)  
107 (rtelnet)  
109 (pop2)  
110 (pop3)  
111 (sunrpc)  
113 (auth)  
117 (uucp path)  
119 (nnntp)  
135 (epmap)



To configure the ports you can select one of the following values:

### **All**

This will apply to all the ports used by the application.

### **Custom**

This lets you define the ports that the application rule will apply to.

Selecting this option enables the **Custom** field, where you can enter the following port values:

### **Single port**

Enter the port value (For example: 4662).

### **List of ports**

Enter a list of ports separated by commas (For example: 4662, 4665).

### **Range of ports**

Enter a list of ports separated by a dash (For example: 4662-4665).

### **Lists and ranges**

Use a combination of the previous methods (For example: 4662, 4665-4670, 4675).

### **Predefined ports**

A list of common ports is provided.

TCP

UDP

ICMP

IP types



## Panda Cloud Office Protection

If you select the ICMP services protocol, you must select one or several options displayed in the **Services** section, or select the value **All** for the rule to apply to all the ICMP Services.

### Edit profile - New system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:  Protocol:

Direction:  Services:   
Echo Reply  
Destination Unreachable  
Source Quench

Zone:

PC it applies to:

IP:  Example: 192.168.1.1-192.168.1.254,172.1.1.1  
Write the addresses and ranges separated by commas.

MAC:  Example: 00:12:49:7D:22:F7  
Write the addresses and ranges separated by a colon.

If you select the IP types protocol, you must select one or several options displayed in the **Protocols** to which it applies section, or select the value **All** for the rule to apply to all the IP Protocols.

### Edit profile - New system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:  Protocol:

Direction:  Protocols to which it applies:   
HOPOPT (IPv6 Hop-by-Hop Option)  
ICMP (Internet Control Message)  
IGMP (Internet Group Management)

Zone:

PC it applies to:

IP:  Example: 192.168.1.1-192.168.1.254,172.1.1.1  
Write the addresses and ranges separated by commas.

MAC:  Example: 00:12:49:7D:22:F7  
Write the addresses and ranges separated by a colon.



Finally, you can indicate the computers the rule will apply to, specifying the following fields:

### **IP**

In this section you can configure the IP address(es) of the computers the rule will apply to:

#### **Single IP**

Enter the IP value (For example: 192.168.1.10).

#### **List of IP addresses**

Enter a list of IP addresses separated by commas (For example: 192.168.1.10, 192.168.1.15).

#### **Range of IP addresses**

Enter a list of IP addresses separated by a dash (For example: 192.168.1.10-192.168.1.15).

#### **Lists and ranges**

Use a combination of the previous methods (For example: 192.168.1.10, 192.168.1.15-192.168.1.20, 192.168.1.25).

### **MAC**

In this section you can configure the MAC addresses of the computers the rule will apply to:

#### **Single MAC**

Enter the MAC address (For example: 00:AF:C8:05:E0:FF).

#### **List of MAC addresses**

Enter a list of MAC addresses separated by commas (For example: 00:AF:C8:05:E0:FF, 08:06:AC:15:E2:FF).



In this example we will show you how to define a rule to deny HTTP communications. This way, you will deny outbound connections to the remote port 80 of the TCP protocol for all the zones. This rule will apply to all the profile computers (without configuring the IP or MAC fields).

### Edit profile - New system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:	<input type="text" value="Deny"/>	Protocol:	<input type="text" value="TCP"/>
Direction:	<input type="text" value="Outbound"/>	Local ports:	<input type="text" value="All"/>
Zone:	<input type="text" value="All"/>	Custom:	<input type="text"/>
		Remote ports:	<input type="text" value="80 (http)"/>
		Custom:	<input type="text"/>

PC it applies to:

IP:	<input type="text"/>	Example: 192.168.1.1-192.168.1.254,172.1.1.1 Write the addresses and ranges separated by commas.
MAC:	<input type="text"/>	Example: 00:12:49:7D:22:F7 Write the addresses and ranges separated by a colon.

Click **OK** to finish creating the rule and return to the **Edit profile** section, where a list of the defined user rules (including the custom rule) will be displayed:



### Edit profile

Profile: New profile (2012-04-17 10:55:35)

☐ Allow configuration of the firewall by the client.

☒ Apply the following firewall settings.

☒ Enable firewall for Windows workstations

☐ Enable firewall for Windows servers

General

Programs

Intrusion prevention

System

Add the connection rules you want. These rules are general and have priority over rules selected individually for each program.

☒ Enable Panda rules.

Show: User rules

Rule name	Action to take	Protocol	Direction	
Deny HTTP	<span>Allow communication</span>	TCP	Outbound	<div><div>Up</div><div>Down</div></div>
				<div><div>Add</div><div>Settings</div><div>Delete</div></div>

1

To modify a parameter in a rule created, select the rule from the user rules list and click **Settings**. When you click the button, you will see the **Edit system rule** screen, where you can modify any parameter.



### Edit profile - Edit system rule

Profile: New profile (2012-04-17 10:55:35)

Rule name:

Action:	<input type="text" value="Allow"/>	Protocol:	<input type="text" value="TCP"/>
Direction:	<input type="text" value="Outbound"/>	Local ports:	<input type="text" value="All"/>
Zone:	<input type="text" value="All"/>	Custom:	<input type="text"/>
		Remote ports:	<input type="text" value="80 (http)"/>
		Custom:	<input type="text"/>

PC it applies to:

IP:	<input type="text"/>	<i>Example: 192.168.1.1-192.168.1.254,172.1.1.1</i> <i>Write the addresses and ranges separated by commas.</i>
MAC:	<input type="text"/>	<i>Example: 00:12:49:7D:22:F7</i> <i>Write the addresses and ranges separated by a colon.</i>

If you have a set of rules, the rules will be applied in descending order (from the first to the last).

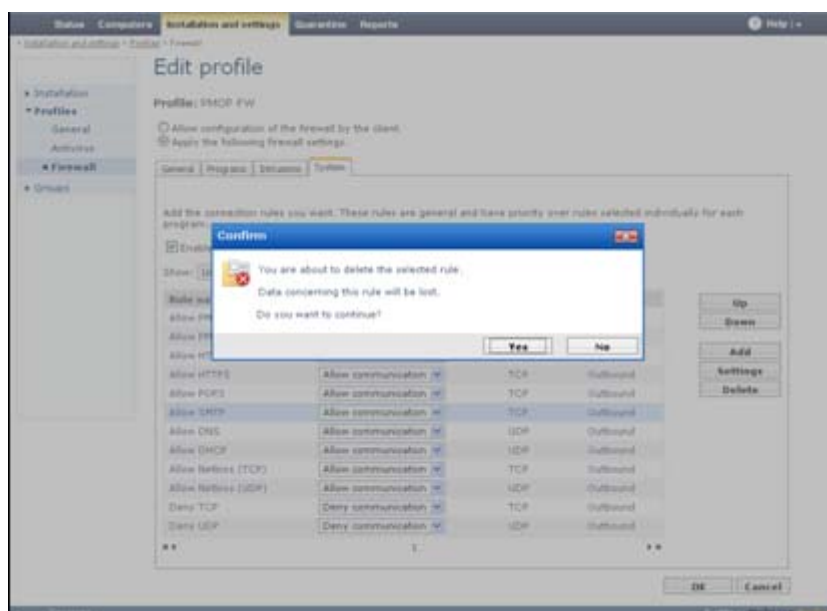
You can change the order by using the **Up** and **Down** buttons. To do so, select the rule you want to move and click the relevant buttons to rearrange the list.

To eliminate a rule, select it from the user rules list, and click **Delete**.

A message will be displayed requesting confirmation to delete the rule.



## Panda Cloud Office Protection




If you click **Yes**, the rule will be deleted. If you click **No**, you will return to the **Edit Profile** screen and the rule will remain.

### Configuration from the local console (Endpoint)

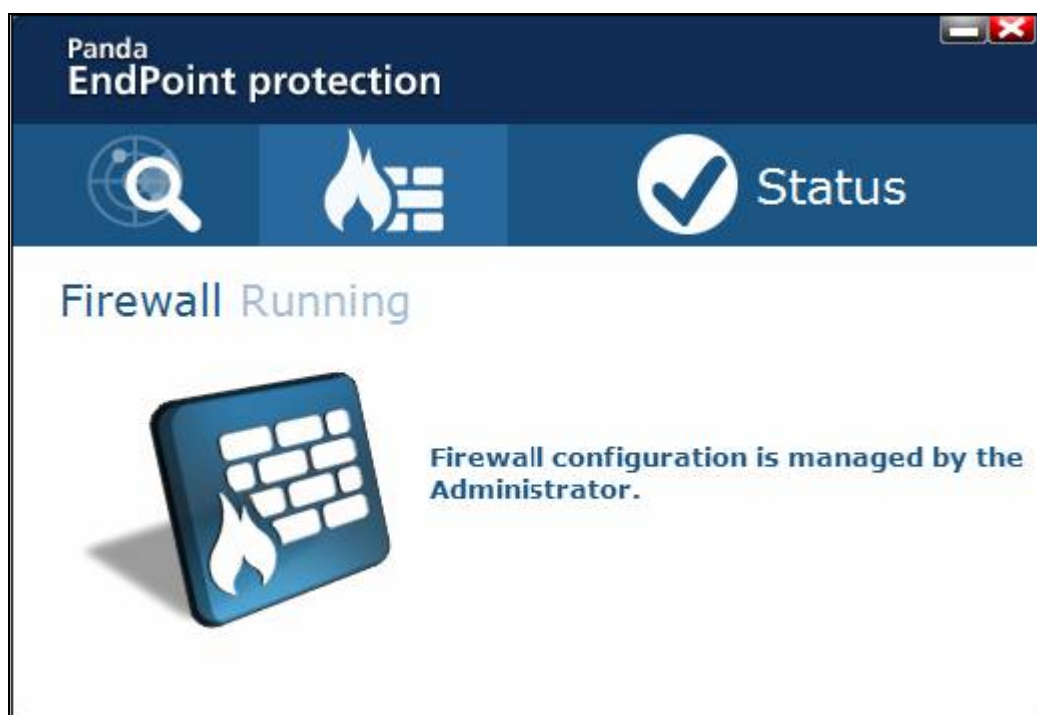
In Managed mode, the firewall can only be configured by the administrator from the Web administration console.

In this case, the firewall cannot be configured from the local console on the workstations or servers with the protection installed.

Right-click the protection icon to display a pop-up menu. Click **Panda Endpoint**

**Protection** to display the protection main screen. When you click the  icon, the following message is displayed:





### Personal firewall

The following section describes the settings options available for firewalls configured in Personal mode, both from the Web administration console or the local console on the workstation or the server.

#### Configuration from the Web console

To configure the firewall in Personal mode, select the option **Allow configuration of the firewall by the client** in the **Edit Profile** screen.



### Edit profile

Profile: New profile (2012-04-17 11:37:32)

☒ Allow configuration of the firewall by the client.  
☐ Apply the following firewall settings.

☒ Enable firewall for Windows workstations  
☐ Enable firewall for Windows servers

General

Programs

Intrusion prevention

System

The behavior of the firewall will depend on the type of network to which it is connected. The type of network is assigned automatically depending on the location of the computer and this setting can be modified from here.

Select the type of network to which you are connected:

☐ Public network  
Public locations, such as airports, cybercafés, universities, etc. Your computer will be visible to other users of the network and use of the network will be limited for some programs

☒ Trusted network  
Home or office networks where you know and trust the other users and the devices on these networks. Your computer will be visible to other network users and you can also see computers and devices on the network

In Personal mode, the firewall is configured through the computer's local console, not through the Web console. Selecting this option disables all other firewall settings options in the Web administration console.

### Configuration from the local console (Endpoint)

In Personal mode, the firewall can only be configured by the user of the workstation or server with the protection installed. The protection is configured from the local console.

To access the local console, select **Panda Endpoint Protection** from the menu displayed on right-clicking the icon in the traybar.

Panda Endpoint Protection
Update
Panda Endpoint Protection help

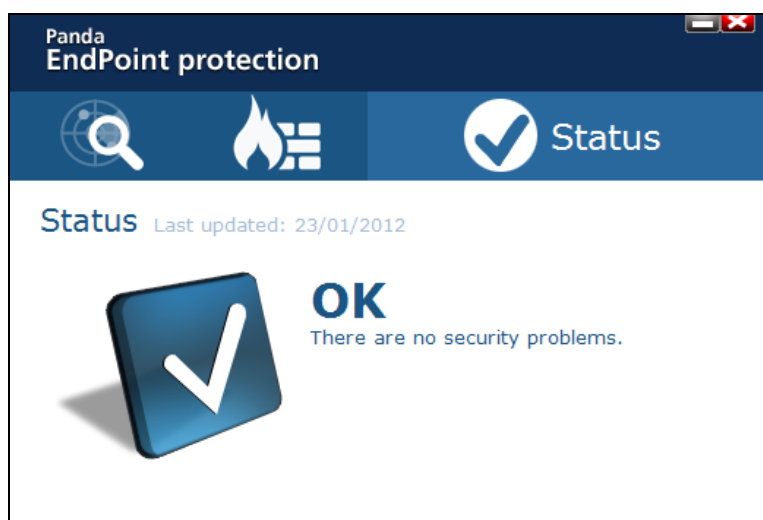



## Panda Cloud Office Protection

---

You will then access the local console.

First, the screen displays the status of the protection installed on the computer.



To access the firewall settings, click .

The firewall is a filter that protects your PC, preventing unauthorized intruders from entering. It is also an effective tool for allowing you to use the Internet securely.

The Panda Endpoint Protection firewall doesn't just filter inbound and outbound connections when the computer connects to the Internet, it also monitors connections between your computer and other network computers with which you can share files, folders, printers and other resources.

Every time a program tries to connect to the Internet from your computer, or when an external program or user tries to connect to your PC, Panda Endpoint Protection will ask you if you want to allow the connection. It does this through pop-up messages that let you authorize or deny connections and configure other related aspects.


By doing this, as you assign permissions and configure the settings, you will gain total control of the connections established to and from your computer.



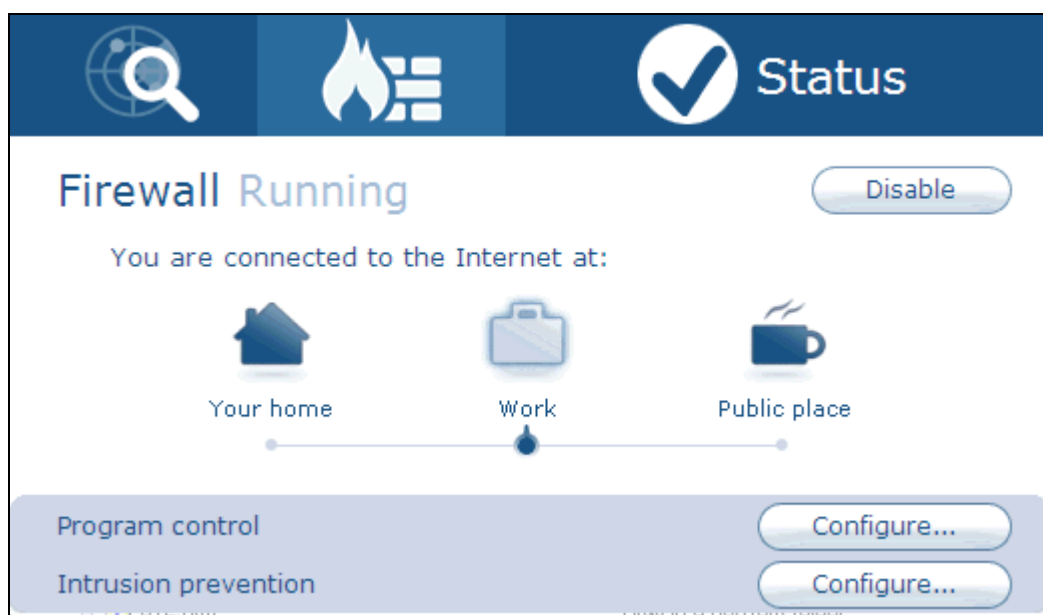
## Panda Cloud Office Protection

### Program control



Click the  icon to display the main screen of the protection. This screen lets you configure the firewall, provided the firewall is in Personal mode and the Administrator has authorized you to do so.

Remember that you can only enable, disable and configure the firewall provided you have the appropriate permissions to do so. If the firewall is being managed by an Administrator, it will be the Administrator who enables, disables and configures the firewall protection for your computer.



Click **Configure**. This will take you to the **Program control** screen. From here you can set the user and factory rules you want to apply for the various programs and set their priority.

You can also configure the firewall through the pop-up messages displayed by Panda Endpoint Protection when there is an attempt to connect to or from the Internet.



When these messages appear, read them carefully so you know which program is trying to make a connection. If it is a trusted program, the connection should be allowed.

If you have any doubts about the program, it is advisable not to allow the connection. In any case, remember that you can change the permissions assigned to a program through the pop-up warnings at any time by changing them in the firewall settings.

### Configuring user rules

Follow these steps to configure the user rules:

1. In the Program control screen, click Add to access the Edit rule screen.
2. Enter a name for the rule.
3. Select if the rule will apply to a specific program or to all of them. If it only applies to a specific program, click Select to select it.
4. In Action, select the communication direction:

#### **Allow outbound connections**

The program can connect to the Internet, but does not accept external connections from other users or applications.

#### **Allow inbound connections**

The program accepts connections from programs or users from the Internet, but it will not have outbound permissions to connect.

#### **Deny outbound connections**

The program cannot connect to the Internet.



### Deny inbound connections

The program does not accept connections from programs or users from the Internet.

Select if the firewall configuration for this rule will apply when you are connected to the Internet at home, work or a public place.

Finally, select a protocol, port or range of ports, and an IP address or range of IP addresses.

To edit or delete a rule, select it and click the relevant button. To increase or decrease



the priority of a rule, click the relevant arrow . The rule will move up or down.

### Configuring factory rules

The factory rules are control rules recommended by our experts, which affect communication of certain applications.

The factory rules let you set connection rules for the entire system. These rules will not have priority over user rules.

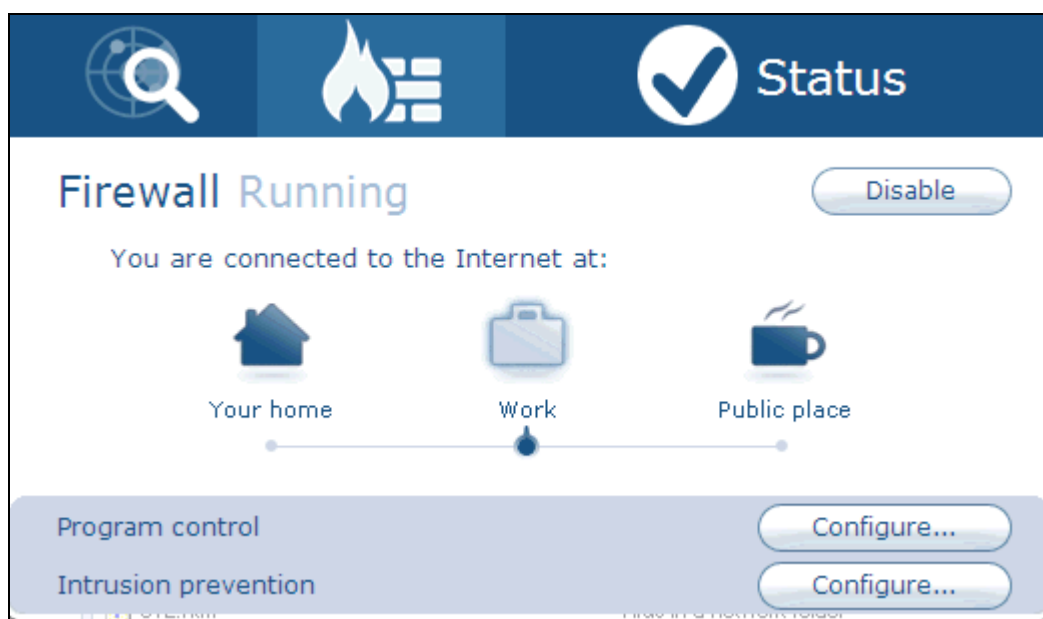
Follow these steps to configure the factory rules:

1. Click the **Factory rules** tab in the **Program control** screen.
2. Select the relevant checkbox to enable the rules.
3. To change the settings of any of the factory rules, select it and click **Edit**. This will take you to the **Edit rule** screen.



### Intrusion prevention

Intrusion prevention lets you select the types of intrusions that you want the firewall to block. In the main screen of the protection, click **Intrusion prevention**.



The **Intrusion prevention** screen displays a list of the IDS attacks the firewall protects against.

### IDS attacks

The *Intrusion Detection System (IDS)* is a program used to detect unauthorized access to a PC or a network.

It is based on detailed analysis of network traffic, comparing it against identifiers of known attacks or suspicious behavior, such as port scanning, malformed packets, etc. The IDS doesn't just analyze the type of traffic, it also checks content and behavior.



## Device Control settings

### Device control settings

Popular devices like USB flash drives, CD/DVD readers, image devices and Bluetooth devices can become an entry point for malware infections.

The device control settings allow you to configure the device control protection for the profile you are creating. Select the device or devices you want to authorize and assign a usage level to them.

### Notifications

Different notifications will be displayed depending on the detected device.

### Unallowed devices

If the protection detects that you have connected a device not allowed for the computer's security profile, a warning is displayed informing you that you do not have permission to access it.

### Read-only devices

The connected device appears in the My Computer directory, but a warning message is displayed if you double-click it. The warning message will indicate that you do not have permission to access it.

### How to enable device control

1. In the Edit profile screen, select Profiles / Device control.
2. Select the **Enable device control** checkbox.
3. In the relevant menu, select the authorization level for the corresponding device.
4. In the case of USB flash drives and CD/DVD drives you can choose between *Allow* or *Allow read access*. In the case of Bluetooth, image devices and USB modems, the available options are *Allow* and *Do not allow*.
5. Click **OK** to save your device control settings.





# Exchange Server protection settings

## Introduction

Provided you have the relevant licenses, you can use the Web console to enable the Panda Cloud Office Protection Advanced protection for Exchange Server and apply it to any Exchange Server that you are managing.

## Minimum requirements

Exchange 2003:

<http://www.microsoft.com/middleeast/windowsserversystem/exchange/evaluation/sysreqs/2003.aspx>

Exchange 2007:

[http://technet.microsoft.com/en-us/library/aa996719\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us/library/aa996719(v=exchg.80).aspx)

Exchange 2010:

<http://www.microsoft.com/exchange/en-us/system-requirements.aspx>

## Exclusions for the permanent file protection

On computers with Exchange Server installed, Microsoft recommends excluding certain files from the permanent file protection.

You will find more information about these exclusions from the following links:

Exchange 2003:

<http://support.microsoft.com/kb/934864/en-us>

Exchange Server 2007:

[http://technet.microsoft.com/en-us/library/aa996719\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us/library/aa996719(v=exchg.80).aspx)

Exchange Server 2010:



## Panda Cloud Office Protection

---

<http://technet.microsoft.com/en-us/library/bb123737.aspx>

The Panda Cloud Office Protection Advanced Exchange Server protection is made up of the following units:

### Antivirus

This unit scans for viruses, hacking tools and suspicious/potentially unwanted programs sent to the Exchange Server mailboxes, and monitors access to the Exchange Server mailboxes and public folders.

For more information about the antivirus protection, refer to the [Exchange Server antivirus protection](#) section.

### Anti-spam

This unit detects and neutralizes spam.

For more information about the anti-spam protection, refer to the [Exchange Server anti-spam protection](#) section.

### Monitoring the Exchange Server protection

As with the other protection modules offered by Panda Cloud Office Protection (antivirus, firewall, device control), you can monitor the status of the Exchange Server protection in the [Computers](#) window, as well as in the [reports](#) generated by Panda Cloud Office Protection.

The detections made by the Exchange Server protection will be visible in:

1. The [Detections by source](#) section in the **Status** window, together with the other detections reported by the different Panda Cloud Office Protection modules.
2. The [list of detections](#).
3. The detection, executive and extended executive [reports](#)



### Exchange Server antivirus protection

#### Mailbox protection

To access the settings of the antivirus protection for Exchange Server, click **Installation and Settings / Profiles / Create new profile/ Exchange Servers / Antivirus**.

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

#### Mailbox protection

Select the Enable mailbox protection checkbox.

By enabling the mailbox protection you will keep email messages stored in your Exchange Server mailboxes malware-free. This will improve your security and prevent data theft and data loss.

In **Malicious software to detect** select the items to detect.

#### *How mailbox protection works*

The mailbox protection acts on the specific malicious or suspicious item rather than on the entire message. That is, if malware is detected in an attached file, the protection will act on that file.

The protection works as follows:

1. The protection takes on the specific file the action defined by our laboratory experts: Disinfect, Delete or Move to quarantine.
2. A security\_alert.txt notification is sent to the user.
3. If restored from quarantine, the email is restored to the recipient's mailbox. If a problem occurs during the restore process, the message is directly moved to the Lost&Found folder, where a file will appear with the name of the suspicious item.



### Transport protection

To access the settings of the antivirus protection for Exchange Server, click **Installation and Settings / Profiles / Create new profile/ Exchange Servers / Antivirus**.

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

### Transport protection

1. Select the Enable transport protection checkbox.
2. By enabling this feature you will make sure that the email that circulates through your Exchange Servers is free from viruses and malware.
3. In **Malicious software to detect** select the items to detect.

### *How transport protection works*

The transport protection acts on the whole message, as follows:

1. If the protection detects malware or a suspicious file, it moves the whole message to quarantine, regardless of the action to take. These messages will be quarantined for the period of time set by Panda Security: 7 days for malware and 14 days for suspicious items. After this period, the malware is deleted and suspicious files are restored once it is confirmed that they are harmless.
2. If a message is moved to quarantine, a notification is sent to the message recipients with the subject of the original message and a warning indicating that the message has been moved to quarantine and they must contact their administrator if they want to retrieve it.
3. If restored from quarantine, the email is restored to the recipient's mailbox. If a problem occurs during the restore process, the message is directly moved to



the Lost&Found folder, where a file will appear with the name of the message subject. This file contains the whole message.

### Intelligent mailbox scan

The intelligent mailbox scan runs during periods of low server activity, scanning the email messages stored in the organization's Exchange Server.

In addition, it only scans messages that have not been previously scanned and contain attached files.

Disabling the mailbox protection also disables the intelligent mailbox scan.

### ***How background scans work***

Background scans work in the same way as mailbox scans. They work as follows:

1. This feature is disabled by default.
2. It only scans files that have not been previously scanned.
3. The background scan only scans messages that have attached files.
4. Disabling the mailbox protection also disables the intelligent mailbox scan.
5. This scan type is not controlled by the user, that is, the scan is enabled but is not constantly scanning mailboxes like on-demand scans. It is the Exchange Server that passes items to the protection for scanning purposes when the computer is idle.
6. This scan type quarantines only the specific item detected as malware. When an item is restored, the process is as follows:
7. The item will be restored to its original destination.
8. The subject text of the restored message will be that of the original message.
9. The restored message won't show the original message body but an informative text.
10. An exclusion will be created for the restored item.



### Exchange Server anti-spam protection

Eliminating junk mail -spam- from Exchange Servers is a time-consuming task. Spam not only is a frequent source of scams, but also a huge time-waster.

To tackle these problems, Panda Cloud Office Protection Advanced now includes anti-spam protection for Exchange Server. This feature will help you make the most out of your time and increase the security of your Exchange Servers.

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

### Actions to perform on spam messages

The available actions are:

#### Let the message through

The tag *Spam* will be added to the subject line of messages let through. This is the default option.

#### Move the message to...

You must specify the email address that the message will be moved to. In addition, the tag *Spam* will be added to the *subject line* of moved messages.

#### Delete the message

#### Flag with SCL (Spam Confidence Level)

What is SCL?

The *Spam Confidence Level (SCL)* is a value (from 0 to 9) assigned to a message that indicates, based on the characteristics of the message (such as the content, message header, and so forth), the likelihood that the message is spam.



A value of 9 indicates a extremely high likelihood that the message is spam. 0 is assigned to messages that are not spam.

The SCL value can be used to configure a threshold in Active Directory above which you consider a message to be spam. Panda Cloud Office Protection Advanced flags messages with the relevant SCL value and lets them through. Then, it is the administrator who establishes, based on the threshold set in Active Directory, the action to be taken on the message.

### Allowed/denied addresses and domains

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

**Add:** Use this button to select, one by one, the email addresses and/or domains to add to the list.

**Delete:** Use this button to delete addresses/domains.

**Clear:** Use this button to clear the whole list.

Keep in mind the following aspects when configuring these lists:

1. If a domain is on the blacklist but an address in the domain is on the whitelist, the address will be allowed. However, all other addresses in the domain will be blocked.
2. If a domain is on the whitelist but an address in the domain is on the blacklist, that address will be blocked. However, all other addresses in the domain will be allowed.
3. If a domain (e.g.: domain.com) is on the blacklist and one of its subdomains (e.g.: mail1.domain.com) is on the whitelist, the addresses from the



subdomain will be allowed. However, all other addresses in the domain or in any other of its subdomains will be blocked.

4. If a domain is on the whitelist, all subdomains in the domain will also be whitelisted.

## Creating groups

### Creating groups

Panda Cloud Office Protection lets you group a series of computers and apply the same protection profile to the whole group.

1. Click **Installation and settings > Groups**, to open the main **Groups** window. As you create groups and associate them to profiles, the groups will appear here, with their name and profile.

The information is divided into four columns: **Name**, **Profile**, **Max. number of installations**, and **Expiry date**. The last two will only be available if you have selected the **Assign restrictions to groups** option in the [Preferences](#) window.

By default the application shows the **Default** group and profile. None of these can be deleted.

2. Click **Create new group** to access the **Edit group** window. Enter the name of the group in the relevant text box.
3. In the **Profile** menu, select the profile to assign to the group.



*If you selected the **Assign restrictions to groups** option in the [Preferences](#) window, you will be able to select the expiry date and the maximum number of installations for the group, by using the relevant checkboxes.*





### Assigning computers to groups

Once you have assigned the name and the profile, you can select the computers to belong to the group from **Available computers**.

Follow these steps:

1. Select the computers and click **Assign**.
2. Click the **Computers in group** tab, and check that the computers have been correctly assigned to the group.
3. If you want to move any computer from one group to another, select it and choose the group in the **Move selected computers to the group** drop-down menu. Then click **Move**.
4. Click **OK** and the application will display the main **Groups** window. The group you have just created will appear with its name and profile on the list.
5. If you want to remove any group, select the checkbox of the group you want to remove and click **Delete**.



**Note:** Remember that if you eliminate any group all relevant data will be lost.

## Installing the protection

### Recommendations prior to installation

#### Computer requirements

Regardless of the installation method to use, it is advisable to check the [requirements](#) to be met by the computers the protection is to be installed on.

#### Closing other applications during installation

It is advisable to close all other applications during installation. This is particularly important with email applications, as if they are not closed during installation this may lead to an error in the email protection. This error would appear when placing the mouse pointer on the **Protections** column in the **Detection details** window. To fix



## Panda Cloud Office Protection

---

this, it would be necessary to restart the computer. The console would then update the protection status, fixing the error.


### Presence of other protection software on computers

It is very important that before installing Panda Cloud Office Protection on computers, you make sure that no other antivirus or security solution is installed.

Some of these will be detected and uninstalled automatically by the Panda Cloud Office Protection installer. You can consult a list of the antiviruses that Panda Cloud Office Protection uninstalls automatically by clicking [here](#).

If yours is not in the list, uninstall it manually.

 In Windows XP: Control Panel > Add or remove programs

 In Windows Vista or Windows 7: Control Panel > Programs and features > Uninstall

### Configuring exclusions in the file protection for servers with Exchange Server

To prevent interference between Panda Cloud Office Protection servers and Exchange servers, any servers with Panda Cloud Office Protection should have a series of folders excluded from the file protection.

For more information, go to the [Technical Support Center](#).



*If you have Panda Cloud Office Protection licenses, the exclusions will have taken place by default.*



## Installation modes

### Installation modes

Panda Cloud Office Protection offers two ways to install the protection: In both cases, the process includes the download and installation of the [administration agent](#)(.msi), which in turn starts the process of installing the protection on the computers.

*If any error occurs when installing the agent, a message is displayed with the error code, a brief description, and a link to the corresponding Help pages.*

#### [Installing the protection with the installation program](#)

You can install the protection on computers either manually or using your own network tools.

#### [Installing the protection with the distribution tool](#)

After downloading and installing the distribution tool on a computer, you can use it to distribute and install the protection on the other selected computers.

This method is advisable when you don't want the user to intervene in the installation process. It is also time efficient as it is not necessary to launch the installation individually on each computer.

If, due to your security needs or the configuration of your computer network, you don't need to create new profiles, you can perform a [quick installation](#).

In this case you must also choose between the installation methods above, but the installation process will be shorter as you will not be creating additional profiles or groups.



*It is very important in all cases that, before installing Panda Cloud Office Protection the protection on computers, you make sure that no other antivirus or security solution is installed. To do this, check the [Recommendations prior to installation](#).*



## Panda Cloud Office Protection

---

### Quick installation

If you do not need to create profiles or groups other than those created by default by Panda Cloud Office Protection –both called **Default**– , you can carry out a quick installation of the protection.

In this case you must also choose between the aforementioned installation methods, but the installation process will be shorter as you will not be creating additional profiles or groups.

If you want to modify the **Default** profile settings, click on the name of the profile in the **Installation program profiles** screen.

You will see the **Edit profile** screen.

Configure the profile as detailed in the sections on [General settings](#), [Antivirus protection settings](#), [Firewall protection settings](#) and [Device control settings](#).



*If later you want to restore the default profile, you can do so using the **Restore default settings** option in the **Edit profile** screen.*

1. In the Installation and settings area, click Installation and select the Default group
2. Select the language and profile you want to assign.
3. Install the protection on the computers you want to protect. Use the **installation mode** that best adapts to your needs and the characteristics of your IT network.

### Installing the protection with the installation program

#### Downloading the installation program



## Panda Cloud Office Protection

---



*Before installing the protection, don't forget to check the [requirements](#) that the computers must meet.*

1. Select the group of computers on which you want to install the protection from the **Group** drop-down menu.
2. In the Installation and Settings area, click Use installation program and then Download installation program.
3. In the download dialog box, select **Save**, then, once it has downloaded, run the file from the directory you have saved it to. A wizard will guide you through the installation process.
4. Distribute the protection to the rest of the computers in the network. To do this you can use your own tools or install it manually.

### ***Sending the link via email***

Click **Send via email**. Automatically, users will receive an email with the download link. Click the link to start downloading the installer.

## Installing the protection with the distribution tool

### **Downloading the distribution tool**



*Before downloading the distribution tool, check the [requirements](#) that the computers must meet.*

#### **Tool for distributing the installation program**

You can use the distribution tool for centralized installation of the protection on computers connected to the network.



[Download distribution tool](#)

The [distribution tool](#) lets you install the protection centrally, avoiding manual intervention from users throughout the process.



## Panda Cloud Office Protection

---



*Remember that, if you want to uninstall the protection, you will be asked to enter the password that you set for the corresponding settings profile.*

1. In Installation and settings, click Download distribution tool.
2. In the download dialog box, select **Save**, then, once it has downloaded, run the file from the directory you have saved it to. A wizard will guide you through the installation process.

Once you have installed the Panda Cloud Office Protection distribution tool, you have to open it in order to deploy the protection on to the computers. You will then see the main window from which you can install and uninstall the protection.

### Installing the protection

When selecting the computers to which to install the protection, the distribution tool lets you do this on the basis of two criteria: by domains or by IP address/computer name.

#### ***By domain***

1. Click Install protection.
2. Click By domains.
3. Indicate the group of computers (optional).
4. In the tree, find the computers to which you want to distribute the protection, and enable the corresponding checkboxes.

You can also enter a user name and password with administrator privileges on the selected computers. It is advisable to use a domain administrator password. In this way you won't have to specify the user name and password of every computer.

#### ***By IP or computer name***

1. Click By IP or computer name.
2. Indicate the group of computers (optional).



## Panda Cloud Office Protection

---

3. Select the computers to which you want to distribute the protection. You can indicate the computers' names, IP addresses or IP address range, separating this data with commas. Click **Add** to add them to the list, or **Delete** to remove them.

 Example of individual IP: 127.0.0.1

 Example of group name: COMPUTER03

 Example of a range of IP's: 192.0.17.5-192.0.17.145

You can also enter a user name and password with administrator privileges on the selected computers. It is advisable to use a domain administrator password. In this way you won't have to specify the user name and password of every computer.

For more information about the task, enable the **Events log** (**View** menu)

### Installing the protection using other tools

If you often use other network distribution tools you can use them to distribute the protection.

## Installation cases

### Installation cases

#### Installing the solution on computers without any protection installed

1. Access the Web Console and enter your Login Email and password.
2. Create a [new profile](#) (or use the [default profile](#), depending on your needs).
3. Configure the [antivirus protection](#), [firewall protection](#) and [device control](#) for the new profile. If you have Panda Cloud Office Protection Advanced licenses you can also configure the Exchange server protection.
4. [Create a new group](#) (optional).



5. Install the protection. Use the [installation method](#) that best adapts to your needs and the characteristics of your computer network.

### Installing the solution on computers with protection installed

The installation process is similar to the previous one. However, it is very important that before installing Panda Cloud Office Protection on computers, you make sure that no other [antivirus](#) or security solution is installed. To do this, check the [Recommendations prior to installation](#).



*In most cases, when installing the new protection and uninstalling the previous one, you will need to restart the computer once (twice at most).*

## Uninstalling other protections

### Uninstalling other protections

#### Automatic uninstallation

When starting the installation process, Panda Cloud Office Protection detects many other security solutions and uninstalls them automatically

You can consult a list of the antiviruses that Panda Cloud Office Protection uninstalls automatically by clicking [here](#). If yours is not in the list, uninstall it manually.



*Before you install Panda Cloud Office Protection you need to close any other applications that might be in use.*

#### Manual uninstallation

 In Windows XP

Control Panel > Add or remove programs

 In Windows Vista or Windows 7

Control Panel > Programs and features > Uninstall





Then you can start to install Panda Cloud Office Protection.

## Protection status

### Protection status

The **Status** area is divided into three sections: **Notifications**, **Licenses** and **Detections**.

#### Notifications

This area is only displayed when there are issues that may be of interest to you, such as the availability of new product versions or warnings about technical incidents, messages about your license status, or any critical issue that requires your attention.

When licenses expire your computers will cease to be protected, and so it is advisable to buy more licenses by contacting your reseller or sales advisor.

#### Licenses

Here you can see the number of Panda Cloud Office Protection or Panda Cloud Office Protection Advanced licenses that you have contracted and their expiry date. For more information about license management, go to the [License management](#) section.



*Clients can only have one license type: either Panda Cloud Office Protection or Panda Cloud Office Protection Advanced.*

In this section there will also be information about your Panda Cloud Email Protection and/or Panda Cloud Internet Protection licenses, i.e. the [clean mail and Web traffic protection](#).

If you have more than two Panda Cloud Office Protection license contracts, or one for Panda Cloud Email Protection or Panda Cloud Internet Protection, you can see the details by clicking the **View details** link.



## Panda Cloud Office Protection

---

If a license contract expires within 30 days and, once expired, the number of licenses used exceeds the number of licenses contracted, you can use the option to cancel licenses. To do this, click **Select licenses to release** and you will go to the **License cancellation** window.

If you are a user with total control permissions, you can cancel licenses on the computers that you select. If you choose this option, the affected computers will cease to be protected, and once the expiry date has been exceeded they will automatically be **blacklisted**.

### List of licenses

This window shows the information in two tabs. One of them lists the information about the Panda Cloud Office Protection or Panda Cloud Office Protection Advanced licenses, and the other includes information about the other protections.

In the case of Panda Cloud Office Protection / Panda Cloud Office Protection Advanced, the data is displayed in four columns: **Expiry date**, **Contracted** (total number of licenses contracted), **Type** (type of licenses), and **Units** (details of the protection contracted: antivirus, firewall, or device control).

In the case of other products, you will see the name of the product, the number of licenses and their expiry dates.

As licenses expire they will disappear from the list.

### Detections

In this section there are two panels displaying the type and source of the detections occurred.

To see detections over a given period of time, select an option in the **Period** menu and click **Apply**.



### Detections by type

It displays detections of each type of threat. It also displays information about the total number of intrusion attempts, devices, dangerous operations and *tracking cookies* blocked.

### Detections by source

It tells you the origin of the detection. You will find definitions of the different types of threats in the [Key concepts](#) section.

It includes the detections reported by the following protection modules:

File system

Mail

Firewall

Device control

Exchange Server

1. Click on the images to expand them. You can also print them.
2. If you want to see a list of [scheduled scans](#), click the **Scheduled scans** link.
3. Click **List of detections** for more information about detections.




*The list of detections shows the items detected over the last seven days.*

### Scheduled scans


From this screen you can see at all times which scheduled scan jobs have been created for the different settings profiles, and access the results of these jobs. To access this window, click the **Scheduled scans** link in the **Status** window.


The information is structured in four columns:



 **Name.** Displays the name of the scheduled scan job. If you click the job name, you will see the window with the results of the scheduled scan.

 **Profile.** This specifies the settings profile to which the scheduled scan belongs.

 **Frequency.** This details the type of scan (periodic, immediate, scheduled)

 **Task status.** This column uses a series of icons to indicate the status of the scan task (*Waiting, In progress, Finished, Finished with errors, Timeout exceeded*). You can access the list of icons by placing the cursor on the option **Key**.

### Results of the scheduled scan jobs

In this window you will see a list of computers subject to the scan jobs, unless the scan status is *Waiting*.

If it is a periodic scan, you can choose between the options **See result of last scan** or **See results of previous scans**.

The data is displayed in six columns:

1. **Computer** This indicates which computer was subject to the scan. The computer will be listed by name or IP address, in accordance with your selection in the [Preferences](#) window.
2. **Group** The group to which the computer belongs.
3. **Status.** In this column there is a series of icons to indicate the status of the computer (*Error, Scanning, Finishing, Timeout exceeded*). You can access the list of icons by placing the cursor on the option **Key**.
4. **Detections** Here you can see the number of detections during the scan. Click the number to access a [list of detections](#).
5. **Start date** Indicates the task start date and time.
6. **End date.** Indicates the task end date and time.

If you want to consult the [configuration of the scheduled scans](#) for this profile, click **See settings**.



### List of detections

The detection monitoring feature allows you to carry out searches of your network to know when your computers have been in danger, what types of threats have been detected, and which action was taken against them.

Use the **Options** menu to activate the filter which lets you look for computers depending on the group to which they belong and the type of detection.

Select the type of threat detected or the source of the detection. You can also select **All detections**.

Click **Find**.

### Search results

The **Computer** column shows the list of scanned computers, presented either by name or by their IP address. If you want to change the way they are presented, you can do this from **Preferences > Default view**.

In the **Group** column you will see the group to which the computer belongs.

The **Name** column indicates the name of the threat, and the **Type** column provides information about the type of blocked threat and/or device (USB flash drives, CD/DVD drives, Bluetooth, image devices, etc.). **Instances** indicates the number of times the detection was made.

Finally, **Action** indicates the action taken by Panda Cloud Office Protection to neutralize the attack, and in **Date** you can see the date and exact time that the threat was detected.



*The list of detections shows the items detected over the last seven days.*



*As a general rule, in the **Detection monitoring** window, when you place the cursor on any of the items in the search list, a yellow tag will appear with information about the item.*

Finally, you can get more details about the detection. Click the [+] symbol next to the name or the IP address of any of the computers, and you will go to the **Detection details** window.

Detections made by the Exchange (Exchange 2007/Exchange 2010) Server Protection background scans will appear as "Notified by: Intelligent mailbox scan".

On Exchange 2003 servers it is not possible to differentiate between items detected by the background scan or by other types of scans. They will appear as "Notified by: Exchange Server Protection".

In some cases, you will be able to access information that Panda Security offers on its Web page about certain threats. To do this, click **View description**.

### Exporting the list

The list of detections made can be exported, either to Excel or to CSV.

To do this, click on the relevant icon next to **Export to**.

Both formats include a header which specifies the date and time when the file was created, a summary of the search criteria, and the details of the list, including the source IP address of the infection(s).

## Monitoring of computers

### Introduction

You can see the status of computers from the Web console. For those computers to which you have distributed the protection, you can monitor the status at all times. To do this, Panda Cloud Office Protection uses two lists of computers:



 List of [protected computers](#)

 List of [unprotected computers](#)

Each list offers an overview of the protection status of the computers, and also details of whether the protection has been installed correctly, if an error occurred during installation, if it is pending restart and if the protection is up-to-date.

To access the lists of protected and unprotected computers, use the **Computers** tab. You will see the **Computers** screen, which has two tabs: **Protected** and **Unprotected**.

Click the corresponding tab. You can search for computers, and export the list to excel or csv format. In both cases, when you click on the name of a computer you will see the computer details screen.

### Remote access to computers

Both the **Protected computers** and **Unprotected computers** tabs show the computers with remote control tools installed, so that you, depending on the permissions you have, can access them through the administration console.



*You will not be able to remotely access unprotected computers that show any of the following status information:*

- Discovered computer
- Uninstalled computer

If the computer has different remote access tools installed and you place the cursor over the icon in the **Remote access** column, you will be able to see all the tools installed on the computer. Click the icon to access the computer.



If the computer has different VCN tools installed (RealVNC, UltraVNC, TightVNC), you will only be able to access other computers remotely through one of them, in the following order of priority:

- RealVNC
- UltraVNC
- TightVNC

For more information on how to install the remote access tools on computers, click the link on the blue information panel. Refer to the [Remote access to computers](#) section for more information.

### Protected computers

The list of protected computers lets you know the status of the protection installed on the computers on your network.

### Computer search

You can choose for all protected computers to be displayed, using the **Show all** button, or use the **Options** drop-down menu and enable the filter that lets you search for computers depending on the status of the protection installed on them: enabled, disabled, with errors, pending restart, etc.

This search tool is also useful for finding out which computers do not have an up-to-date version of the signature file or getting a list of those which for whatever reason have not connected to the Panda Cloud Office Protection server in the last 48 hours.

Select the status from the **Computer status** drop-down menu and click **Find**.

The search results are presented in five columns:





The **Computer** column shows the list of scanned computers, presented either by name or by their IP address. If different computers have the same name and IP address, they will be displayed as different computers in the Web console provided that their [MAC address](#) and [administration agent identifier](#) are different.

If you want to change the way they are presented, you can do this from **Preferences > Default view**.

The **Protection update**, **Signature update**, and **Protection** columns use a series of icons to indicate the update status of the protection and their general situation.

Updates:	Protection:
Updated.	Correct.
Pending restart.	Disabled.
Outdated.	With errors.
Not installed.	
Updated (no connection to the server in the last 72 hours).	

In **Last connection** you can see the exact date and time at which the computer last connected to the update server.

**Remote access.** When an icon is displayed in this column it means that the computer has some remote access tools installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer.

If the computer has multiple tools installed, place your mouse pointer over the icon to see all of them. Select one to access the computer remotely.



*If you place the mouse pointer over a computer's name, a yellow tag will be displayed with information about the computer's IP address, the group the computer belongs to and the operating system installed.*



### Unprotected computers

In this window you can see which of the computers are not protected.

A computer may appear as unprotected when the installation or uninstallation process is in progress or when there has been an error during installation or uninstallation.

### Computer search

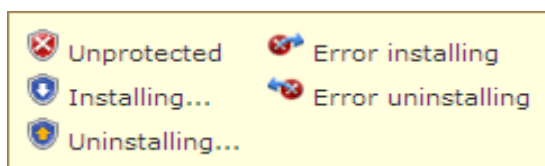
You can choose to display all unprotected computers, using the **Show all** button, or you can use the **Options** menu to enable the filter that will allow you to look for unprotected computers.

Select the status from the **Computer status** drop-down menu and click **Find**.

The search results are presented in five columns:


☁ The **Computer** column shows the list of scanned computers, presented either by their name or by their IP address. If the name of the computer is not known, you will see the word *Unknown*.


☁ The **Status** column describes the situation of the protection. For this there are a series of icons:



☁ The **Details** column describes the reason for the status of the computer. For example, if the status is *Error installing*, in **Details** you will see the error code. If, on the other hand, the **Status** column shows *Without protection*, **Details** will show *Protection uninstalled*.



 **Last connection.** This shows the date and time of the last connection with the computer.

 **Remote access.** When an icon is displayed in this column it means that the computer has remote access software installed. If the computer has only one tool installed, click the icon to access it. Enter the relevant credentials and access the computer.

If the computer has multiple tools installed, place your mouse pointer over the icon to see all of them. Select one to access the computer remotely.

### Computer details

If you want to access protection details about a specific computer, click on the computer. You will then see the **Details of protected computer** window, with information about the status of the protection installed on the computer.

Use the **Comment** field if you want to add additional information to identify the computer. If you are a user with monitoring permissions, you will not be able to access this field. For more information, refer to the [Types of permissions](#) section.

To add the computer to the blacklist, click **Add to blacklist**. To remove it from the database, click **Delete from database**.

### Exporting the list

The list of computers generated in the search can be exported, either to Excel or to CSV.

To do this, click on the relevant icon next to **Export to**.

Both formats include a header specifying the date and time the file was created, a summary of the search criteria, and data about the computer, the group to which it belongs, the signature file and protection versions, operating system, and IP address.



## Remote access to computers

### Remote access to computers

The remote access feature lets you access your network computers from your administration console without having to physically go there.

Panda Cloud Office Protection lets you access computers using any of the following remote access tools:

 TeamViewer

 RealVNC

 UltraVNC

 TightVNC

 LogmeIn

A small icon will be displayed in the **Computers** window by any computer with these tools installed. If the computer has only one tool installed, click the icon to access it. Enter your credentials and access the computer.

You can enter your credentials in the Computers or [Preferences](#) window.

If the computer has several tools installed, place your mouse cursor over the icon to display all of them. Select one to access the computer remotely.

Refer to the [How to use the remote access tools](#) section for more information about these tools.



*If the computer has different VCN tools installed, you will only be able to access it remotely through one of them, in the following order of priority:*



- 1-RealVNC
- 2-UltraVNC
- 3-TightVNC.

You will be able to access more or less computers depending on whether you have [total control](#) or [administrator](#) permissions. If you only have [monitoring](#) permissions you will not be able to access any computer and the **Remote access** icon will be disabled.

### How to gain remote access to a different computer

#### Remote access from the Computers window

The first time that you access the **Computers** window a warning will be displayed indicating that your computers don't have any remote access tools installed. If you want to install a tool, click the link in the warning.

#### Remote access from the Computer details window

You can also use the remote access feature from the **Computer details** window, provided the selected computer has a remote access tool installed. If so, click the icon of the tool that you want to use.

To access other computers remotely, install one of the supported remote access tools on them: TightVNC, UltraVNC, RealVNC, TeamViewer, LogMeIn.

If the computer has various VCN tools, remember that you will only be able to access it remotely in the above priority order.

### How to use the remote access tools

#### VNC tools

These tools can only be used to access computers on the same local network as the client.



## Panda Cloud Office Protection

---

Depending on the tools authentication configuration, you might be able to access them without having to enter any credentials in the console, or you may have to configure a user name and a password to establish a remote connection.

For the administrator to be able to access computers through these tools they must allow the execution of a Java applet on their computer, otherwise, they will not be able to access them.

### TeamViewer

This tool can be used to access computers outside the client's local network.

To access computers through TeamViewer you will only need to enter the computer password. The "user" field can be left blank.



*The password you must enter to access a computer through TeamViewer is the computer's TeamViewer password or the password for unattended access to computers. It is not the TeamViewer customer account password.*

Every user of the Panda Cloud Office Protection console that wants to access other computers remotely with TeamViewer must enter the same password.

The administrator's computer (the computer through which the console is accessed) must have TeamViewer installed (it is not enough to have it in "run without installation" mode).

### LogMeIn

This tool can be used to access computers outside the client's local network.

To access computers with LogMeIn, you need to enter the user name and password for your LogMeIn account.



## Unprotected computer search

### Unprotected computer search

In order to improve monitoring of the protection installed on computers, Panda Cloud Office Protection lets you search for unprotected computers.

Administrators can even do this remotely, seeing at any time which computers are protected or unprotected, from a location outside the network.



*If you need to simultaneously search for unprotected computers and uninstall the protection remotely, refer to the [Compatibility of remote management tasks](#) section.*

### Configuring searches for unprotected computers

In the main window of the Web console, click **Installation and settings**. Then, select **Search** in the menu on the left. This will take you to the **Search for unprotected computers** window.

To configure a new search task, click **New search**. Then, in the **Edit search** window, use the **Select** button to choose the computer that will perform the search.

The scope of the search will be defined depending on whether you choose the subnet of the computer performing the search, certain IP address ranges or certain domains.

### Requirements for the computer performing the search

In order to perform the search, the computer must meet a series of minimum requirements, which are as follows:

1. It must have a connection to the Internet and have connected to the Panda Cloud Office Protection server in the last 72 hours.
2. It must be protected with version 5.05 or later of Panda Cloud Office Protection



3. It must be operating and not be on a blacklist or performing remote uninstallation tasks.



*It is important that there are no remote uninstallation tasks configured on the computer. For more information, refer to the [Compatibility of remote management tasks](#) section.*

To find out more about how the results of the searches are displayed, refer to the [Viewing search results](#) section.

## Viewing searches and results

### Viewing searches

Searches created are listed in the **Find unprotected computers** screen, from where you can also remove search jobs, using the **Delete button**.



*The jobs with the status **Starting** or **In progress** cannot be deleted.*

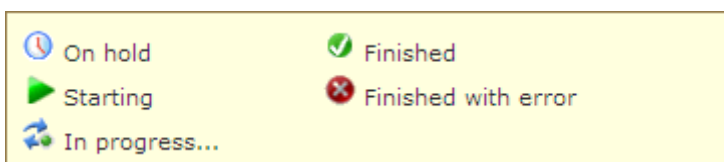
Information is organized into the following columns:



**Name:** This shows the name given to the search when created.



**Status:** The status icons indicate the status of the search job.



**Discovered:** This details the number of unprotected computers discovered.



**Date of creation:** Date the search job was created.



**Created by:** User that created the job.





Depending on your permissions, you can create, view, or remove search jobs. For more information refer to the section on [Types of permission](#).

### Search results

Click on the name of the search and you will see a screen with details about the result of the selected search.

When you click on the name of a search in the **Find unprotected computers** screen, you will see the **result of the search**. This displays all the unprotected computers that have been discovered after running the corresponding search.

In addition to the name of the search, the start and end date and the status, this screen also offers information about any errors that occur during the search.



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


If you want to consult the search settings, use the **View settings** link.

## Quarantine


### Quarantine

Panda Cloud Office Protection stores in quarantine suspicious or non-disinfectable items, as well as spyware and hacking tools detected.

Once suspicious items have been quarantined and sent for analysis, there are three possible scenarios:

 Items are determined **as malicious**: They are disinfected and then restored to their original location, provided that a disinfection routine exists for them.



 Items are determined as malicious, but there is no disinfection routine: They are eliminated.

 It is established that **the items in question are not malicious**: They are directly restored to their original location.

In the Web console main screen, click **Quarantine** to open it. The screen is divided into two sections: a search engine and another section displaying the list of results.

In the search area you can filter the items you want to view. There are four filter parameters:

### Reason

Select the type of files to find in the **Reason** menu. Files are classified according to the reason they were put in quarantine.

### Group

Once you have selected the type of file you want to find, select the group of computers you want to search.

### Date

Select the period you want.

Click **Find**.

If you want to restore any item, select the relevant checkbox, click **Restore** and respond affirmatively to the confirmation message. The item will disappear from the search list and you will be able to find it in the **Files excluded from the scan** window.

If you want to delete any of the items found, select the relevant checkbox, click **Delete** and respond affirmatively to the confirmation message.



➡ *If there are several items with the same type of malware, when restoring or deleting one of them, all the rest will also be restored or deleted.*

➡ *When you place the cursor on any of the items in the search list, a yellow tag will appear with information about the item.*

➡ *The **Computer** column displays the name of the computer or its IP address, depending on what you selected in the **Default view** section, in **Preferences**.*

## Files excluded from the scan

If you select an item in the [Quarantine](#) screen and restore it, the item disappears from **Quarantined files** and becomes a file excluded from the scan (**Quarantine / Files excluded from the scan**).

Just as you can exclude items from quarantine, you can also return them to quarantine. To do this, select the checkbox corresponding to the item you want to return, and click **Undo exclusion**. Then accept the confirmation message.

The item will disappear from the list of exclusions, and will reappear in the quarantine list when it is detected again.

## Reports

### Generating reports

Panda Cloud Office Protection lets you generate reports about the security status of your network and any detections made over a given period of time. You can also select the content that appears in the report, whether you want more detailed information and if you want graphs. All of these options are quick and simple to manage.


1. In the main window of the Web console, click **Reports**. You will then see the Reports window. This window is divided into two sections, one with a report filter and another for viewing results.



2. In the **Period** menu, select the period you want to be reflected in the report (last 24 hours, last 7 days, or last month).
3. In the case of executive or detection reports covering the last 7 days or the last month, the data shown will correspond to the activities that took place between 0:00 (UTC time) seven days or one month ago, and the time when the report has been generated.
4. In the tree below **Report scope**, select the group or groups to be included in the report.
5. Select a type of report and click **Generate report**.

When the report has been generated, it will be displayed on the right-hand side of the window. Consult the [Viewing reports](#) section.








*If you place the cursor on the  icon, you will get information about the reports and their content.*

### Types of reports

#### Executive


Information:


-  Status of the protection installed and items detected over the last 24 hours, last seven days or last month.
-  Top 10 *lists* of computers with malware detected and attacks blocked, respectively.
-  Top 10 *lists* of computers with devices blocked.
-  Information about the status of the licenses contracted.
-  Number of computers in which the protection is being installed at the time of generating the report (including computers with installation errors).
-  If you have Panda Cloud Office Protection Advanced licenses, the report will display the number of spam messages detected.



### Status


Information:


 It gives an overview of the protection and update status at the time of report generation.

 Number of computers in which the protection is being installed at the time of generating the report (including computers with installation errors).

### Detection

Information:

 Describes detections made during the last 24 hours, last 7 days, or last month.

 Lists the computer, the group, the type of detection, the number of detections made, the action taken and the date of the detection.

## Report display


When the report has been generated, it will be displayed on the right-hand side of the window. You have a series of controls to move around the pages, as well as carrying out searches and modifying the width of the page.

To export the report, select the format from the list and click **Export**.



*To export the reports in Internet Explorer, the option **Do not save encrypted pages to disk** must be disabled in the **Security** section of the **Advanced** tab in **Tools > Internet options**.*

Click  to refresh the report view.

Click  to print the report.



*The first time you want to print a report (only available in Internet Explorer) you will be asked to install an ActiveX control from the SQLServer.*

## Uninstallation

### Types of uninstallation

You can uninstall the protection in different ways:



#### Local uninstallation

If you want to uninstall locally, you will have to do it physically from each of the computers, using the corresponding option in the operating system's control panel.



#### Centralized uninstallation

Centralized uninstallation of the protection on several computers can be performed from the [distribution tool](#). This tool is downloaded and run on a computer from which the process for uninstalling the protection from selected computers is launched.



#### Remote uninstallation

There is also a remote uninstallation method, used to uninstall the protection from a Web console in a different location from the computers. You can configure uninstallation jobs and specify which computers will be affected.



*If necessary, the local and centralized uninstallation methods can be password protected using the password that you can set when you create the settings profile.*

Select the uninstallation method about which you would like more information:



[Local uninstallation](#)



[Centralized uninstallation](#)



[Remote uninstallation](#)



### Local uninstallation

Local uninstallation of the protection is performed from each computer on which it is installed.

 In Windows XP

Control Panel > Add or remove programs

 In Windows Vista or Windows 7

Control Panel > Programs and features > Uninstall

### Centralized uninstallation

In the main console window, click **Installation and settings** and then **Uninstallation** from the menu on the left. Select **Centralized uninstallation**. You will see the **Centralized uninstallation** screen.

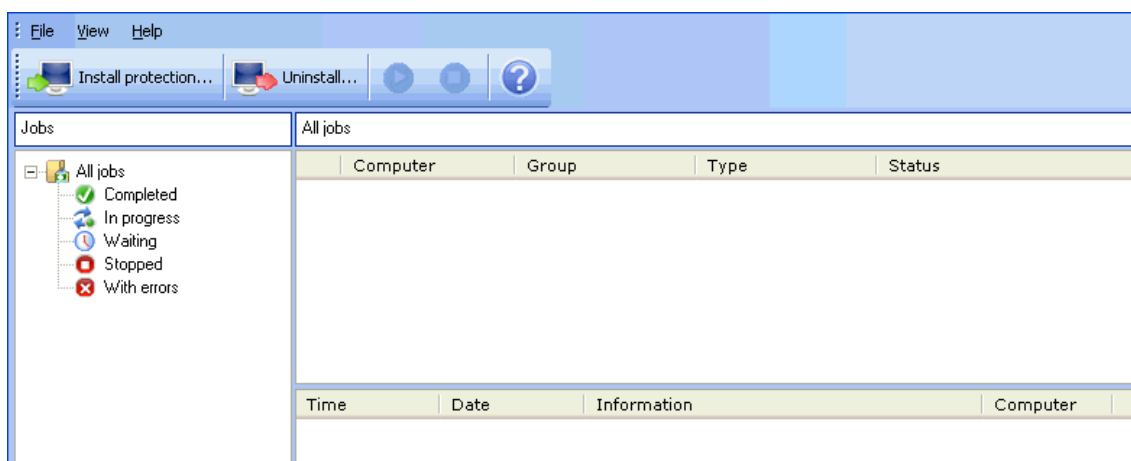


***IMPORTANT:** Before downloading and installing the distribution tool, check the [requirements for the computer](#) from which the tool is deployed.*

### Downloading and installing the distribution tool

1. In the main console window, click Installation and settings and then Uninstallation from the menu on the left. Select Centralized uninstallation (distribution tool).
2. In the download dialog box, select **Save**, then, once it has downloaded, run the file from the directory you have saved it to. A wizard will guide you through the installation process.

Once you have installed the distribution tool, you have to open it in order to uninstall the protection from the computers. You will see the main window from which you can uninstall the protection:



### Uninstallation by domains

1. Open the distribution tool.
2. In the main window, click **Uninstall**.
3. In the tree, find the computers from which you want to uninstall the protection, and enable the corresponding checkboxes.
4. If necessary, you will be asked to enter [the password you created for the corresponding profile](#).
5. Enter the user name and password with administrator privileges that you used for the selected computers.
6. If you want items removed from quarantine during the uninstallation process, and for the computers to be restarted after uninstallation, enable the corresponding checkboxes.

### Uninstallation by IP or computer name

1. Open the distribution tool.
2. In the main window of the distribution tool, click **Uninstall**.
3. Select the computers from which you want to uninstall the protection. You can indicate the computers' names, IP addresses or IP address range, separating this data with commas.
4. If necessary, you will be asked to enter [the password you created for the corresponding profile](#).





5. Enter the user name and password with administrator privileges that you used for the selected computers.
6. If you want items removed from [quarantine](#) during the uninstallation process, and for the computers to be restarted after uninstallation, enable the corresponding checkboxes.

## Remote uninstallation

### Creating remote uninstallation tasks

Remote uninstallation lets you uninstall the protection from the Web console simply and effectively without needing to physically access each computer. This type of uninstallation therefore saves on costs and legwork.

The process first involves creating uninstallation tasks, and then configuring these tasks. To do this, the administrator must select the group and computers in the group from which the protection will be uninstalled. It is then possible to check the results and details of the uninstallation on each computer

### How to uninstall the protection remotely

1. In the main window of the Web console, click **Installation and settings** and then **Uninstallation** from the menu on the left.
2. Select Remote uninstallation. You will see the Remote uninstallation window.



*To configure uninstallation tasks the user must have total control or administrator permissions. For more information, refer to the [Types of permissions](#) section.*

3. To configure a new uninstallation task, click **New uninstallation**.

Then, in the **Edit uninstallation** window you can name the task and select the **group** from the drop-down menu that contains the computers from which you want to uninstall the protection. The groups displayed will be those on which you have permissions.



*If you select the option **Restart the computers on finishing uninstallation**, remember to save all the information that is being used on the computers.*


4. If the selected group has a settings profile that includes password-protected uninstallation, you will have to enter the password in the corresponding box.
5. Select the computers from the **Available computers** list and click Add. When you select them, they will appear in the **Selected computers** tab.
6. To see [the results of any of the remote uninstallation task](#), go to the **Remote uninstallation** window.

### Viewing remote uninstallation tasks and their results

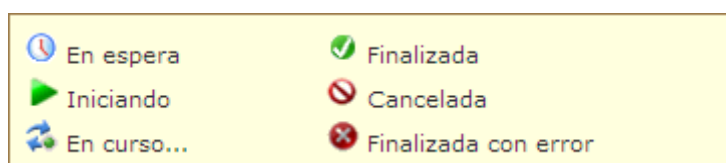
#### Viewing uninstallations


Uninstallation tasks are listed in the **Remote uninstallation** window, where you can also eliminate them if you want by using the **Delete** button.

Information is organized into the following columns:


 **Name:** This shows the name given to the uninstallation task when created.

 **Status:** The status icons indicate the status of the uninstallation task.



 - **Uninstalled protection:** Shows the uninstalled protections.

 **Date created:** Date the uninstallation task was created.

 **Created by:** User that created the task.



Depending on your permissions, you can create, view, or remove uninstallation tasks. For more information, refer to the [Types of permissions](#) section.

To see the results of any of the uninstallations, click on the name and you will go to the [Results](#) screen.

### Remote uninstallation result

When you click on the name of an uninstallation in the **Remote uninstallation** window, you will see the **results**.

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



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


If you want to consult the uninstallation settings, use the **View settings** link.

### Compatibility between searches for unprotected computers and remote uninstallation

 If a computer is involved in an uninstallation job (*waiting, starting up, or in progress*), **it is not possible**:

To create another uninstallation job for it.

To select it as the computer from which to launch [searches for unprotected computers](#).

 If a computer is running a job for discovering unprotected computers, **it is not possible**:

[To create an uninstallation job for it.](#)



## Troubleshooting & FAQs

### Troubleshooting

Should you have any queries, go to the tech support page where you will find a list of the most common Panda Cloud Office Protection error codes, and up-to-date information about all of them. Click [here](#) or enter the following URL in your Internet browser:

<http://www.pandasecurity.com/enterprise/support/card?id=50032&idIdioma=1&idSolucion=147&idProducto=124>

### Frequently Asked Questions

#### How is the Panda Cloud Office Protection Web console accessed?

Panda Cloud Office Protection is managed online through its Web console. Follow the steps below to access it:

Go to the following URL:

<https://managedprotection.pandasecurity.com>

Enter the Login Email and Password.

Accept the terms and conditions of the **License agreement** (you will only be asked to do so once).

Once you have logged in to Web console, the **Status** tab will be shown.

The **Exit** option lets you log out. You can also select the language for viewing the Web console, using the list next to the active language.



### What is a profile?

The Panda Cloud Office Protection settings are based on the creation of profiles and groups of computers to which specific policies are assigned. A policy is a set of settings applicable to one or more groups of computers. All computers belonging to the same group will be assigned the same policy.

### Configuring a profile

Access the Web console.

In the **Installation and Settings** menu, select **Profiles** on the left of the Web console.

You will see all of the profiles created, as well as the **Default** profile. On selecting a profile, the sections that correspond to each profile will be displayed in the left panel: General, Antivirus, Firewall and Device Control.

### What are the installation requirements for Panda Cloud Office Protection?

To install Panda Cloud Office Protection, the computers involved in the installation process have to meet a series of requirements.

This affects the computers on which the protection will be installed and the computer from which the protection will be deployed. Several conditions must also be met to access the Web console. These requirements are specified in the [System requirements](#) section.

### What checks must be carried out before installing Panda Cloud Office Protection?

Before installing Panda Cloud Office Protection you are advised to carry out several checks regarding other protection installed on the computer, Panda Cloud Office Protection-AdminSecure compatibility and keep other applications closed while Panda Cloud Office Protection is installed.



All these tips are available in the [Recommendations prior to installation](#) section.

### What are the components of Panda Cloud Office Protection?

Panda Cloud Office Protection comprises four main components:

- The Web console.
- The antivirus unit
- The firewall unit.
- The Device Control unit.

### The Web console

The Web console allows you to manage the network computer protection.

### The antivirus unit

The [antivirus unit](#) is installed from the Web console and includes the following protection:

- Files: Permanent protection monitoring access to disks.
- Mail (only workstations): Email protection

### The firewall unit

The firewall unit monitors all Internet connections, blocking or allowing access depending on the rules configured. It implements detection and blocking of **IDS intrusions** and **network virus attacks** that Trojans use to spread. Administrators can configure the operational mode of the firewall protection.



### **Centralized administration (from the Web console)**

Administrators define the configuration they want to apply to the computers. It is configured from the Web console.

### **Administration from the client (from the Panda Endpoint Protection icon):**

The end-user of the protection in each computer is responsible for configuring the firewall. There are a series of rules predefined by Panda which establish permissions for common applications. Rules can be created or modified from the options available in the firewall settings.

### **Device Control**

Popular devices like USB flash drives, CD/DVD readers, image devices, Bluetooth devices and modems can become an entry point for infections.

The device control settings allow you to configure the device control protection for the profile you are creating. Select the device or devices you want to authorize and assign a usage level to them.

### **What is the Panda Cloud Office Protection administration agent?**

The administration agent is an item distributed to all computers that use Panda Cloud Office Protection services. Once installed, it triggers the installation of the protection on the computers. It has three main functions:

- Establish a communication between the local processes on computers and Panda Cloud Office Protection servers.
  
- Establish a communication between local processes on computers and other agents.
  
- Establish a communication between other agents and Panda Cloud Office Protection servers (proxy function).



Further information about the agent and its main functions is available in the [Protection deployment](#) section.

What do the P2P and proxy functions implemented in Panda Cloud Office Protection consist of?

### P2P system

The local installation and update processes in Panda Cloud Office Protection (walupg and walupd\*) use a certain logic to detect whether the necessary installation or update files are available on another agent on the network.

This way, it will get the installation or update files from another computer on the network instead of downloading them from the Internet. This logic is known as a [P2P system](#) and its main objective is to reduce bandwidth consumption.

The local installation and update processes are:

walupg: Local process for installing and updating the protection.  
walupd: Local process for updating the signature files.

### Functioning

When a computer downloads a file from the Internet, it can serve it to other computers so that they don't need to connect to the Internet to get it.

When the computer finishes updating the virus signature file or the protection, it broadcasts information about the available files to the other computers on the network.

When a computer needs a file, it will first try to obtain it through the P2P system. If this fails, it will try to download it from the Internet.



*For a computer to serve files to other computers through P2P, it must have at least 128 MB of RAM.*





### Proxy

The Panda Cloud Office Protection agent has proxy features. This means that the solution can access the Internet through an agent installed on a computer with an Internet connection.



*To act as a proxy for other agents, the computer must meet the following requirements: to have a direct connection to the Internet and to have at least 128 MB of RAM. Besides, the computer must not be blacklisted and the installation sequence must have finished.*

This system will only be used when it is not possible to access the Internet directly.

### Functioning

The agent detects it cannot access the Internet and broadcasts a request to find the computers that can act as a proxy.

The computers are listed in a file called Proxy.dat (a maximum of 10).

The next time the agent cannot access the Internet directly, it will try the first computer on the list.

Every request sent to the Proxy.dat file will be addressed at a different computer, to avoid using the same computer all the time.

Also, proxies have an availability indicator. When an agent on the proxy list cannot be accessed, its level of availability will decrease. The initial availability value is 3. Once it reaches 0 the computer is removed from the Proxy.dat list.

### Static proxy

If you want all access to the Internet to be made through a specific computer chosen by the administrator, instead of dynamically through certain computers, the



communications agent offers the possibility to specify which computer you want to act as a proxy.

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

1. It must have an agent installed (version 6.0 or later).
2. It must have direct Internet access.
3. It must have at least 128MB of RAM.
4. It must have established a connection to the server in the last 72 hours
5. The computer must not be blacklisted and the protection installation sequence must have finished.

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

You can select another computer to work as a static proxy. If a computer stops acting as a static proxy due to having been blacklisted, but is then white listed it can be reconfigured to work as a static proxy so that all communications with the server pass through it.

To configure a static proxy, go to the Proxy/Repository server section in the Advanced settings screen (available from the Main tab in the general profile settings).

### How is Panda Cloud Office Protection installed through the installation program?

First, you must install the administration agent (.msi), which downloads the protection to install it on your computers.

Panda Cloud Office Protection offers two options for distributing the protection to your computers using the installation program:



Downloading the installation file onto the administrator's computer and then carry out the installation on the rest of the network.

Sending the link to the installation file to each computer by email so that each user can download it and run it manually.

### Downloading the installation program

1. Access the Web console.
2. Click **Installation and settings**.
3. Click **Installation** in the menu on the left.
4. In **Protection settings**, open the menu to select the group of computers to which to apply the configuration for the chosen group.
5. In the **Installation mode, Installation program** section, click the arrow in the **Use the installation program** section. Click **Download installation program**.
6. Click **Save** in the WAgent.msi file download screen.

Once the download is complete, run the file from the director in which you have saved it. A wizard will guide you through the installation process.

Distribute the protection to the rest of the computers on the network. You can use your own tools (Logon Script, Active Directory, Tivoli, etc), or install it manually.

### Sending the link via email

Click **Send via email**. Automatically, users will receive an email with the download link. If you prefer, you can copy the direct link on the computers in which you want to install the protection.

Panda Cloud Office Protection can also be installed through the [distribution tool](#).



Further information about the Panda Cloud Office Protection installation is available in the [Installation modes](#) section.

### How is Panda Cloud Office Protection installed through the distribution tool?

The Panda Cloud Office Protection distribution tool lets you install the protection centrally, avoiding manual intervention from users throughout the process.

### Downloading the distribution tool

1. Access the Web console.
2. Click **Installation and Settings**.
3. Click **Installation** in the menu on the left.
4. In **Type of installation**, select the **Group** to add computers to when installing the protection.
5. Click **Download distribution tool**
6. Click **Save** in the Wadistributiontool.msi download screen.
7. Run the Wadistributiontool.msi file from the directory in which you have saved it. A wizard will guide you through the installation process.

### Installing the protection

1. Go to **Start > Programs > Panda Distribution tool**, or to the shortcut on the Windows Desktop.
2. In the tool console, select **Install protection**. The **Protection installation** screen will open, which allows you distribute the protection in two ways:

### Distribution by Domain

1. Enter the group to add computers to when installing the protection. This selection will define the settings policies that will be applied to those computers.



## Panda Cloud Office Protection

---

2. In the network tree, select the domains or computers on which you want to carry out the installation.
3. Use a user name and password with administrator permissions to carry out the installation. The user name must be entered in domain\user name format.
4. Once the data is entered, click **Install** to generate the installation jobs.

### Distribution by IP address or computer name

1. Enter the group to add computers to when installing the protection. This selection will define the settings policies that will be applied to those computers.
2. Add the names of the computers or their IP addresses, separated by commas. You can also select IP address ranges (use the "-" symbol for ranges, e.g. 172.18.15.10 – 172.18.15.50).
3. Use a user name and password with administrator permissions to carry out the installation. The user name must be entered in domain\user name format.
4. Click **Install** to generate the installation jobs.
5. Check the console to see whether the installation job has been carried out successfully. From then on the protection installation will begin, completely transparently.
6. Restart the computer if prompted.

Further information about the Panda Cloud Office Protection installation is available in the [Installing the protection](#) section.

### Can Panda Cloud Office Protection be installed on a network with AdminSecure protection?

Before installing Panda Cloud Office Protection on computers with the distributed AdminSecure protection, you must disable AdminSecure's **Automatic installation** option.

If not, when the AdminSecure agent detects that Panda Cloud Office Protection is installed, it will uninstall it and will install the AdminSecure protection again.



## Panda Cloud Office Protection

---

Two things can occur depending on the AdminSecure version:

If the AdminSecure version is later than AdminSecure 4.02 SP2, Panda Cloud Office Protection will be automatically uninstalled through the uninstaller included in AdminSecure.

If the AdminSecure version is previous to AdminSecure 4.02 SP2, Panda Cloud Office Protection cannot be automatically uninstalled. Consequently, the AdminSecure protection will be installed (even if Panda Cloud Office Protection is installed), causing undesired effects.

On disabling the **Automatic installation** option in AdminSecure, you can either disable it on all computers or just on those in which Panda Cloud Office Protection will be installed. In short, you will configure the computers in which AdminSecure will not be automatically installed, or, in other words, the computers that will be an exception to AdminSecure's automatic installation rule.

To disable the **Automatic installation** option in AdminSecure:

1. In the AdminSecure console, select **Settings > Automatic installation**
2. Click **Configure exceptions**, and use the **Add** button to select the computers to be excluded from the installation process.

### How can a computer be included in the blacklist?

It can be done manually or automatically.

#### Manually

Use the options in the **Preferences** screen.

#### Automatically



A computer is automatically included in the blacklist when you try to install on it protection whose license has expired, or when the maximum installations have been exceeded.

The computer will not be updated and the information from that computer will not be taken into account in the reports and statistics obtained by Panda Cloud Office Protection.

### How can a computer be restored from the blacklist?

To restore the computer and take it out of the blacklist, there must be available licenses.

If the computer has been manually included in the blacklist, select it and use the **Restore** option in the **Preferences** screen.

### Why is no information received from a computer that was in the blacklist but has been restored?

If a computer is restored and some days pass without it sending information to the server, it could be because the user has not yet been validated. After a maximum of five days, the computer will once again start to send information.

### Why are some computers out-of-date after a Panda Cloud Office Protection update?

Sometimes, after upgrading the version of Panda Cloud Office Protection, the **Protection update** column of the **Computers** tab shows computers with out-of-date protection.

One possible reason for this situation is that the **Automatic updates** option for the computers' profile is not enabled.



### Solution

Enable the automatic updates for the profile corresponding to the computers with this error.

To do this, follow the steps below:

1. Go to the **Installation and settings** tab.
2. Select **Profiles** in the panel on the left.
3. Click one of the out-of-date computers in the list.
4. Edit the profile of the out-of-date computers and select the **General** settings.
5. Make sure the **Enable automatic updates** checkbox is selected in the **Automatic updates** section.
6. Then click **Advanced update options**.
7. Check that the option **Enable automatic updates of the protection engine** is enabled in the **Protection engine update** section.
8. Click **OK**.

Once the automatic updates are enabled, check that after the update period configured in the settings, the protection engine is updated correctly.

### What does Panda Cloud Office Protection do when connecting to the cloud?

Computers require an Internet connection for the protection to access the cloud. Therefore, if necessary, it is advisable for the administrator to configure the proxy in the Panda Cloud Office Protection Web console.

If the proxy is not configured, the protection will try to access the Internet in the following way:

It will try to use the update **settings in the Web console**.





If these settings do not exist or it is impossible to access the Internet with them, the protection will use the **settings established by the user in the local warning** displayed (if they have been configured).

If these settings do not exist or it is impossible to access the Internet, a **direct connection will be attempted**.

If the Internet cannot be directly accessed, the **Internet Explorer settings will be used** (proxy server and port values configured in the browser).

If the Internet cannot be accessed with these settings and a proxy is configured in Internet Explorer, the following warning will be displayed to users:



This **local warning is only shown once a day** in order not to annoy end-users. When the warning is displayed, users will have three attempts (maximum) to enter the correct values.



## Panda Cloud Office Protection

---

For the warning to be displayed every 24h, the date and time in which it was last displayed is saved in the **titw.cfg** configuration file of the protection.

To try the Internet connection, the protection will carry out an HTTP query to the following URL:

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

To query the cloud, the protection will access the following URL:

<http://cache2.pandasecurity.com>

### How does Panda Cloud Office Protection access the cloud depending on the type of scan?

If you want to disable cloud-based scans, you can do so from the administration console. Go to **Installation and settings > Profiles**, and select the profile to edit. Then, go to the **General** section > **Main** tab > **Advanced settings**, and select **Disable scans with Collective Intelligence**.

However, it is advisable to keep this option enabled if you want to benefit from all the protection provided by Collective Intelligence.

### Panda Cloud Office Protection accesses the cloud in the following scan types:

#### User scans

Any type of scan launched from the bear icon in the notifications area, or by right-clicking an item and selecting the Scan option.

#### Scheduled scans

Any type of scan launched from the Panda Cloud Office Protection Web console

#### Background scans



Scans scheduled by Panda whose aim is to scan areas of the computer where malware is usually stored.

### Memory scans

This scan takes place when the signature files have been updated.

Everything that exists in memory will be scanned using the cache knowledge so as not to launch queries to the cloud for files that have already been analyzed.

A scan monitoring mechanism has been implemented to prevent scans from overlapping:

If a memory scan is running, a new one will not be launched.

### Is it possible to disable queries to the cloud?

If you want to disable cloud-based scans, you can do so from the administration console. Go to **Installation and settings > Profiles**, and select the profile to edit. Then, go to the **General** section > **Main** tab > **Advanced settings**, and select **Disable scans with Collective Intelligence**.

However, it is advisable to keep this option enabled if you want to benefit from all the protection provided by Collective Intelligence.

If you want to disable queries to the cloud, you must delete the registry key GlkProductID in HKLM\SOFTWARE\Panda Software\Setup



*You must restart the **Panda Software Controller** service for the change to the registry values to take effect.*

How often do computers notify the status of the installed protection to the Panda Cloud Office Protection servers?



The status message is programmed to be sent every X hours (this value can be set in the Edit profile – Advanced settings screen). However, it will only be sent provided there has been a change in the protection status compared to a previous situation. If no change has occurred, the message is sent once a day.

You can change the frequency displayed by default, but it must be a value between 12 and 24 hours. If, for example, you set the value to 14, the protection status message will be sent to the Panda Cloud Office Protection servers every 14 hours.

The status message is sent regardless of whether you have selected or not a computer to centralize all communications with the server from.

Once you have created an immediate scan job in the Panda Cloud Office Protection Web console, how long does it take for the endpoint to recognize and apply it?

Scan jobs are created through the Scheduled scans tab in the Edit profile screen. Follow these steps:

1. **Click New to go to the** Edit profile – New scan job window.
2. **Name:** Choose a name for the scan job.
3. **Scan type:** Select a scan type (in this case, immediate scan).
4. Once configured, the immediate scan will take place when the computer connects to the Panda Cloud Office Protection server (every 4 hours, at most) and the solution checks that the protection settings have changed.

The detection report is sent once the immediate scan is complete.

## Appendix 1: Commandline scripts for basic operations

The basic operations that can be performed are:



- Remote installation
- Remote verification of installation
- Uninstallation
- Update of the virus signature file
- Update of policies or settings
- Running on-demand scans: full scans, mail scans, etc.
- Getting the date of the last signature file
- Getting the status of the antivirus and firewall

## Installation

### Previous steps. Downloading the installation package

Before starting to install the protection, you must get the Panda Cloud Office Protection installation package: WaAgent.msi. This installation package could be located in the Remote Desktop Management SaaS repository for the client in question.

### Options for downloading the installation package

The installation package could either be generic or specific for the client and the security profile. Depending on the option selected, the commandline command used may have to comply with certain specific parameters. The download options are:

Download the package from any client account and with the DEFAULT profile. Then, during installation, use the client ID parameter and the group ID parameter with the security profile for this client. This indicates to which client the protection belongs and the corresponding security profile and group.

Download the corresponding installation package for each client. In this case, there is no need to indicate the client ID.

Download the corresponding installation packet for each client and for each group with the client's security profile. In this case there is no need to indicate the client ID nor the group to which the computer belongs.



## Panda Cloud Office Protection

---

### Downloading the installation package (WaAgent.msi)

Go to the specific client account through the Panda Cloud Office Protection client console.



Go to the **Installation and settings** tab. Download the installation package for this client for the Default group, corresponding to the default security profile, i.e. antimalware and centralized firewall.



Installation

Profiles

Groups

Search

Uninstallation

### Installing the protection

To install the protection modules on your computers, choose a group for the computers and the installation mode.

#### Group

Select the group to add computers to when installing the protection.

Group:

Language: English    Profile: DEFAULT

[What is a group?](#)

#### Installation mode

You can install the protection on computers using the distribution tool or through the installation program.


#### Installation program

Use the installation program to install the protection on network computers either manually or using your own tools.

☒ [Use the installation program](#)

#### Tool for distributing the installation program

You can use the distribution tool for centralized installation of the protection on computers connected to the network.

 [Download distribution tool](#)

[More information about the installation tool.](#)

Download the installation package and save it locally.



Installation

Profiles

Groups

Search

Uninstallation

## Installing the protection

To install the protection modules on your computers, choose a group for the computers and the installation mode.

### Group

Select the group to add computers to when installing the protection.

Group:

Language: English    Profile: DEFAULT [What is a group?](#)

### Installation mode

You can install the protection on computers using the distribution tool or through the installation program.

### Installation program

Use the installation program to install the protection on network computers either manually or using your own tools.

[Use the installation program](#)

You can download the installation program and run it on each of the PCs you want to protect.

[Download installation program](#)

If you want, you can send the link for accessing the installation program to your network users by email so that they can execute it from their workstation.

Direct link:  
[http://poop800rascaeconsole.cloudapp.net/Console/v8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST=\[95C2837E-018B-4E9C-808D-A9C1DE8EA7D4\]&GROUP=DEFAULT](http://poop800rascaeconsole.cloudapp.net/Console/v8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST=[95C2837E-018B-4E9C-808D-A9C1DE8EA7D4]&GROUP=DEFAULT)  
Send via email: [Send via email](#)

## Installation steps

### Step 1.

Download the installation package to the desktops.

### Step 2.

Run the installation command in the directory where you have downloaded the installation package.

```
msiexec /i "WaAgent.msi" /qn <GROUP> <GUID> <ALLOWREBOOT>
```





## Panda Cloud Office Protection

---

The optional parameters are:

<GROUP> The group and therefore the security profile of the computer.


The msi file will already have a value assigned in the download. This value can be overwritten, specifying the GROUP parameter.


<GUID> Client ID for the computer on which the protection is being installed.

The msi file will already have a value assigned in the download. This value can be overwritten, specifying the GUID parameter.

The GUID is available in the Installation and settings section of the Web console, as the CUST parameter in the shortcut to the installation package.

**Installation program**  
Use the installation program to install the protection on network computers either manually or using your own tools.  
[Use the installation program](#)

 You can download the installation program and run it on each of the PCs you want to protect.  
[Download installation program](#)

 If you want, you can send the link for accessing the installation program to your network users by email so that they can execute it from their workstation.  
Direct link:  
<http://pcop800rascaeaconsole.cloudapp.net/Console/v8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST={95C2837E-018B-4E9C-808D-A9C1DE8EA7D4}&GROUP=DEFAULT>  
Send via email: [Send via email](#)

<ALLOWREBOOT>. Lets you specify if the protection installer can restart the computer once installation is complete.

ALLOWREBOOT=TRUE ➔ Allow restart.

ALLOWREBOOT=FALSE ➔ Don't allow restart.



### Examples

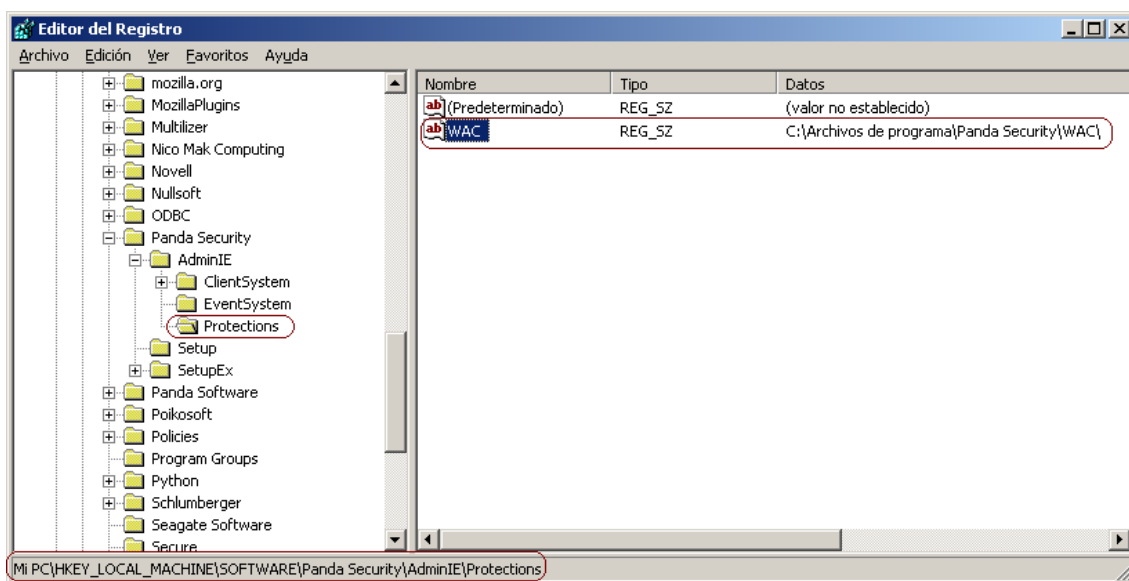
```
msiexec /i " WaAgent.msi" GROUP=GROUP_ONLYAV GUID=81729831 /qn
```

```
msiexec /i " WaAgent.msi" GROUP=DEFAULT ALLOWREBOOT=TRUE /qn
```

### Verifying protection installation

You can check if Panda Cloud Office Protection is installed by checking the registry key.

HKLM\Software\Panda Security\AdminIE\Protections



### Verification steps

Step 1. Check whether the following key exists:

HKLM\Software\Panda Security\AdminIE\Protections

If it does, go to step two. If it doesn't, then the protection is not installed.



Step 2.

Get the WAC value. The data associated with this value indicate the location of the protection installation.

If it exists and it is not empty, then the protection is installed.

If it does not exist or it is empty, then the protection is not installed.

## Uninstalling Panda Cloud Office Protection

To uninstall Panda Cloud Office Protection from a computer you must first uninstall the agent and then the protection.

### Uninstallation steps

Step 1. The command for uninstalling the agent is available by consulting the UnPath value in the HKLM\SOFTWARE\Panda Security\SetupEx\AdminIE registry key.

Step 2. The agent uninstallation is run silently:

```
<HKLM\SOFTWARE\Panda Security\SetupEx\AdminIE Unpath value> /qn  
PASS=<Password>
```

You will only need to use the PASS parameter if you have configured an uninstallation password in the profile.

Step 3. The command for uninstalling the protection is available by consulting the UnPath value in the HKLM\SOFTWARE\Panda Security\Setup registry key.

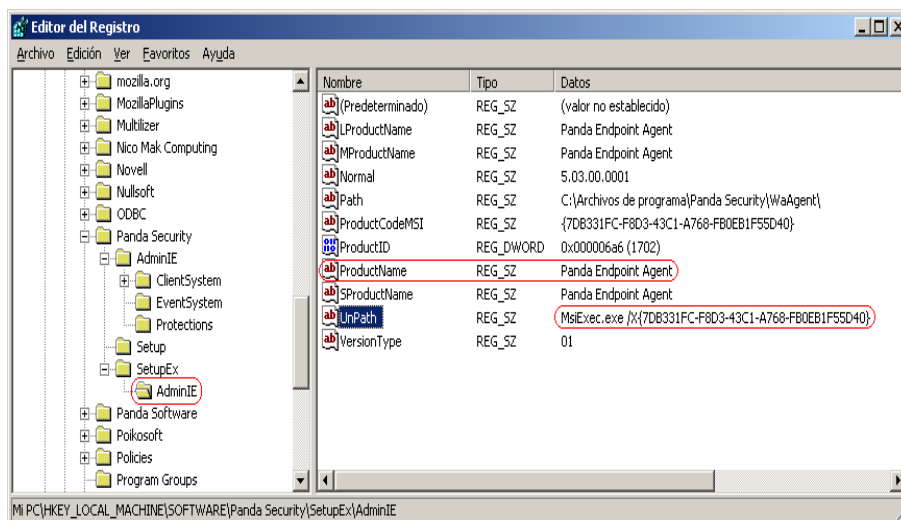
Step 4. The protection uninstallation is run silently:

```
<HKLM\SOFTWARE\Panda Security\Setup Unpath value> /qn  
PASS=<Password>
```

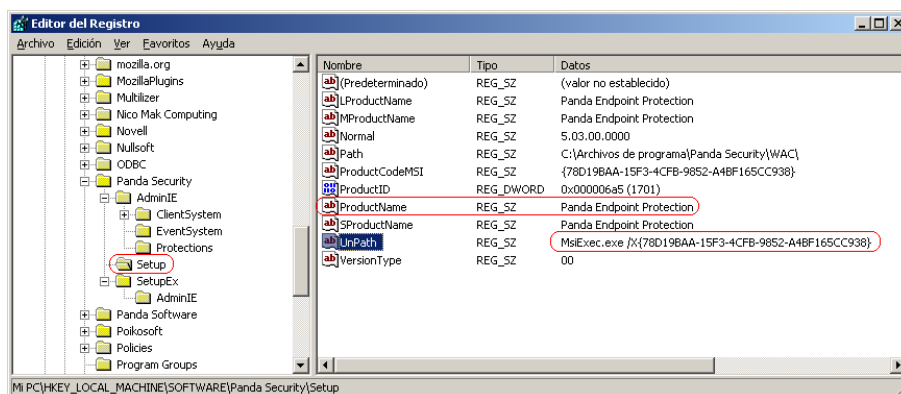
You will only need to use the PASS parameter if you have configured an uninstallation password in the profile.



Example:



**MsiExec.exe /X{7DB331FC-F8D3-43C1-A768-FB0EB1F55D40} /qn**



**MsiExec.exe /X{78D19BAA-15F3-4CFB-9852-A4BF165CC938} /qn**

## Updating the signature file

The signature file is updated through the WalUpd local process.



### Steps for updating the signature files

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG.exe WALUPD -force
```

### Updating settings

If any changes are made to the security profile of the group to which the computer belongs, this will be deployed to the workstation the next time it consults the server. However, it is possible to force the update of the settings through the WalConf local process.

### Steps for updating the settings

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG.exe WALCONF -force
```

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG walscan -T: <FILENAME> -P: WAC -A: START
```

### Getting the date of the signature files

The process to determine if the protection is updated with the latest signature files is carried out in the backend of Panda Cloud Office Protection.

The agent sends the server the date of the last update and this is checked against the date of the last signature files published.



In this section we explain the mechanism for getting the date of the last signature file update on the computer.

Remember that this information, along with other information about the protection status, is updated continually on the computer in a file called WALTEST.DAT.

This is an XML file, and can be treated as such in order to parse its content for such information (see Appendix 1).

In the <PavsigDate> section there is information relating to the date of the last signature file update.

You therefore need to get this file and process its content, searching for the <PavsigDate> tag

### Obtaining the signature files date

Step 0. Prior to getting the information, it is advisable to launch an update of the signature files as detailed in Section 4. Then refresh the information in waltest.dat by launching the waltest local process.

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng
```

```
WAPLPMNG.exe WALUPD -force
```

```
WAPLPMNG waltest -force
```

```
(Update the file WALTEST.DAT)
```



### Step 1.

Go to the Waltest local process directory and get the waltest.dat file.

```
CD %ProgramFiles%\Panda Security\WaAgent\WalTest  
(find the file: WALTEST.DAT)
```

### Step 2.

Look for the tag "<PavSigDate>". To do this, you can use a program for parsing XML files, so you'll have to rename the waltest.dat file to XML, or use the FindString DOS command for finding strings in files.

Here we explain how to get this information using the FindString command.

```
FindStr "<PavSigDate>" waltest.dat  
(find tag <PavSigDate>)
```

The information will be similar to the following:

```
<PavSigDate>2012-03-23 12:25:43</PavSigDate>
```

In this example, the date of the last signature file is "2012-03-23 12:25:43".

## Getting the status of the antivirus, the firewall and the device control modules

This information, along with other information on the real status of the protection, is continually refreshed in the WALTEST.DAT file.



As mentioned above, this is an XML file, and can be treated as such in order to parse its content for such information (see Appendix 1).

In the <AVSTATUSINFO> section there is information about the status of each of the antivirus protections. Each <JOBID> section refers to each protection. The information available is as follows:

<IsInstalled> Protection installed

<IsStarted> It is running.

<IsActivated> It has been enabled in the configuration

The values and meanings of the JobIDs are:

JobID	Meaning
2	File protection (permanent file protection)
4	Email protection (permanent email protection)
64	Firewall protection
256	Device Control

### Getting information on the status of the protection

#### Step 0.

Previously, although it is not necessary, it is advisable to launch an update of the waltest.dat file by running the WalTest local process.





```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng
WAPLPMNG waltest -force
(Update the file WALTEST.DAT)
CD %ProgramFiles%\Panda Security\WaAgent\WalTest
(find the file: WALTEST.DAT)
```

### Step 1.

Go to the Waltest local process directory and get the waltest.dat file.

```
CD %ProgramFiles%\Panda Security\WaAgent\WalTest
(find the file: WALTEST.DAT)
```

### Step 2.

Get the information you require.

```
FindStr "<JobID> <IsInstalled> <IsStarted> <IsActivated>" waltest.dat
(find info in the file WALTEST.DAT)
```

The information will be similar to the following:

```
<AVStatusInfo><JobStatusInfo><JobInfo><JobID>2</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
```



```
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>4</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>8</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>16</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>64</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
```

In this example, you will see the following:

Permanent file protection (JobID = 2): Installed, running and active.

Permanent email protection (JobID = 4): Installed, running and active.

Firewall (JobID = 64): Installed, running and active.

Device control (JobID = 256): Installed, running and active

### **WALTEST.DAT format. <AVSTATUSINFO>**

```
<AVProducts><AVProduct><AVID><AVName>WAC</AVName>
<AVVersion>6.00.12.0000</AVVersion>
```



```
</AVID><PendingUpgrade>>false</PendingUpgrade>
<PavSigDate>2012-03-23 12:25:43</PavSigDate>
<MUID>69c87ea1-90d4-463d-999a-89302d311e26</MUID>
<AVStatusInfo><JobStatusInfo><JobInfo><JobID>2</JobID>
<UnitID>1</UnitID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>4</JobID>
<UnitID>1</UnitID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>64</JobID>
<UnitID>2</UnitID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>256</JobID>
<UnitID>8</UnitID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
```



```
<IsStarted>true</IsStarted>  
<IsActivated>true</IsActivated>  
<IsStatusCoherence>true</IsStatusCoherence>  
<ReqConform>0</ReqConform>  
</JobStatus></JobStatusInfo></AVStatusInfo></AVProduct></AVProducts></TestReport>
```

## Appendix 2: Deploying the protection

Before going into detail on the files, registry keys and folders created on deploying the protection on computers, we offer information about the administration agent, the P2P function, the proxy function and protection installation times.

All these factors are important to have more in-depth knowledge of the deployment process.

### The administration agent

The agent is responsible for communication between the administered computers and the Panda Cloud Office Protection servers. Effectively, it 'talks' with the agents on the computers in the same group and is responsible for downloading installation programs from the Internet.

When the agent installer is run, the Panda Cloud Office Protection installation process is launched, which involves a series of different tasks: downloading settings, installing the protection, updating the signature files, etc.

As a fundamental component in the dialogue between different computers, the agent is a key part of the P2P process described below.

### Peer to Peer (P2P) function

In the case of Panda, the P2P feature reduces bandwidth usage, as computers that have already updated a file from the Internet then share the update with other connected computers. This prevents saturating Internet connections.



The P2P feature is very useful in the deployment of Panda Cloud Office Protection when it comes to downloading the installation program.

When one of the computers has downloaded the installation program from the Internet, the others are informed by the communication agents, which have then started the Panda Cloud Office Protection installation process.

Instead of accessing the Internet, they get the installation program directly from other computers. Then the protection is installed.

This function is also very useful when updating the protection engine and the signature files, and is implemented in the two local processes that need to download files from the Internet: WalUpd and WalUpg. Activation is carried out in the configuration files of these processes.

WALUPD.ini

[GENERAL]

UPDATE\_FROM\_LOCAL\_NETWORK=1

WALUPG.ini

[GENERAL]

UPGRADE\_FROM\_LOCAL\_NETWORK=1

The P2P feature is independent in each of these local processes.

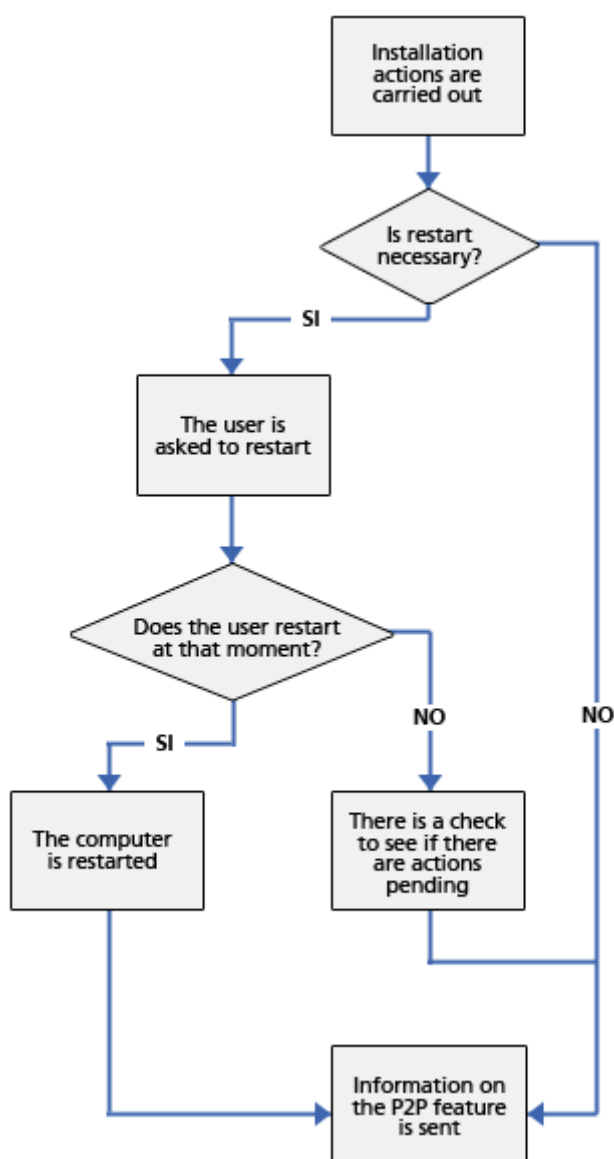
### The P2P feature works as follows

When a computer has updated signature files or any protection (or the agent itself), it sends a broadcast with the information about the files that it has to the rest of the computers on the network.



With respect to the sending of information in WALUpg, if a restart is necessary after installing/updating the protection, if the user chooses to restart later, the information on the P2P feature will be sent immediately instead of waiting for the restart.

This function is detailed in the following diagram:





The computers save the information and use it when they need it.

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

The computer with the file receives a request for the file and sends the message containing the file in response.

The computer that requested the file receives it and can continue with the update or upgrade.



*For computers to send files to others through the P2P feature they must have at least 128 MB of RAM.*

### Dinamic proxy

The agents contain a list with information about computers on the network with agents and which can send messages to the Internet. These agents are called proxies.



*To act as a proxy for other agents, the computer must meet the following requirements: to have a direct connection to the Internet and to have at least 128 MB of RAM. Besides, the computer must not be blacklisted and the installation sequence must have finished.*

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

When it is waiting for data from the list of valid proxies, the proxy module will not attend other requests.



The list of proxies has a value associated to each proxy with a maximum number of attempts to connect with another agent before it will be considered invalid. By default the number is three, and when this value reaches zero the agent will be considered invalid as a proxy.

If at any time all the proxies in the list are invalid, the list itself will be considered invalid and the search for proxies is launched through the message "Who is proxy?"

It is possible that the message is sent correctly to the proxy in the list, but the proxy discovers it does not have an Internet connection. In this case, the remote agent will repeat the sequence described here, resending the message to a proxy in the list, but it will also send via TCP a message to the agent that sent the message saying "I am not Proxy", to indicate that it should be removed from the list as it does not have a connection to the Internet.

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

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

The message contains a list of the proxies through which it has passed, to avoid being sent twice to the same proxy without Internet connection.

### Static proxy

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

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

It must have an agent installed (version 6.0 or later)





It must have direct Internet access

It must have at least 128MB of RAM

It must have established a connection to the server in the last 72 hours

The computer must not be blacklisted and the installation sequence must have finished.

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

You can select another computer to work as a static proxy. If a computer stops acting as a static proxy because it has been blacklisted, but is then whitelisted it must be reconfigured to work as a static proxy so that all communications with the server pass through it.

When the agent has to access the Internet it will first try to communicate using the static proxy. If communication with the static proxy is not possible, it will try to establish connection using the usual sequence of communications.

If a valid configuration is stored, it will try to communicate using this configuration.

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

If it cannot connect directly, it will try through another dynamic proxy, as described in the section above.

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



To configure a static proxy, go to the Proxy/Repository server section in the Advanced settings screen (available from the Main tab in the general profile settings).

### Installation times

Below we list the different times required for installing the various components of Panda Cloud Office Protection on a computer to manage, taking into account bandwidth available for the Internet (direct installation) and local network (installation using the local network).

#### Direct installation

#### Test environment

The performance tests were carried out in the following test environment.

PC	Features
A	P4 1,6 GH, 512 MB, XP SP2
B	P3 1,2 GH, 256 MB, XP SP2

The tests emulated the following bandwidth conditions using software allowing a reduction in available bandwidth:

Bandwidth (Kbps)
3048
1024
512
256
128
56



### Size of all downloaded items

The following items were downloaded from the Internet:

Protection installer: 37 MB

Signature files: 12.5 MB.

### Test plan

The study emulated the different bandwidth availability scenarios using specific software, and for each computer and bandwidth parameter, the agent was installed with direct connection to the Internet.

The installation tests included the installation of antivirus (AV) and firewall (FW) protection.

### Results

The results obtained are displayed in the following table:

Legend:

AV installation:

Installation time of the antivirus and firewall protection.

AV+SIG installation:

Installation time of the antivirus and firewall protection and first complete update of the signature file

HTTP AV download:

Time for downloading the protection installer using the browser (Internet Explorer 6.0)



HTTP SIG download:

Time for downloading the signature files using the browser (Internet Explorer 6.0)

Bandwidth (Kbps)	AV Installation		AV + SIGs Installation		HTTP Download AV		HTTP Download SIGs	
	A	B	A	B	A	B	A	B
3072	00:06:05	00:07:05	00:08:50	00:10:50	00:02:07	00:02:07	00:00:35	00:00:35
1024	00:11:19	00:11:19	00:16:25	00:17:25	00:06:28	00:06:28	00:02:04	00:02:04
512	00:16:43	00:16:43	00:21:53	00:22:53	00:13:05	00:13:05	00:04:10	00:04:10
256	00:31:43		00:40:03		00:26:43		00:08:20	
128	00:52:20		01:13:00		00:49:20		00:16:40	
56	01:37:20		02:09:30		01:26:20		00:29:10	



Some tests were not carried out on computer B as they would not have provided any additional information to the results on computer A.

## Installation via local network

### Test environment

The performance tests were carried out in the following test environment:



PC	Features
A	Intel Core 2 1.86 GB, 256 MB, XP SP2
B	Intel Core 2 1.86 GB, 256 MB, XP SP2

The tests emulated the following bandwidth conditions using software allowing a reduction in available bandwidth:

Bandwidth (Mbps)
100
10
3
2
1

### Size of the items transmitted across the network

The following items were transmitted across the network:

Protection installer: 50 MB

Signature files: 12.5 MB.

### Test plan

The study emulated the different bandwidth availability scenarios using specific software, and for each computer and bandwidth parameter, the agent was installed with a direct connection to the Internet. The installation tests included the installation of the antivirus and firewall protection.



### Results

The results obtained are displayed in the following table:

Bandwidth (Mbps)	AV Installation		AV + SIGs Installation	
	A-B	B-A	A-B	B-A
100	00:04:55		00:05:05	
10	00:05:30		00:05:50	
3	00:07:00		00:07:42	
2	00:08:05		00:09:07	
1	00:11:19		00:13:24	



Given that A and B have the same characteristics, only distribution from A to B has been tested.

Below you will find detailed information about the files, registry keys, [local processes](#) and services created on installing Panda Endpoint Agent on the administered computers.

## Deploying Panda Endpoint Agent

### Main architecture modules

Panda Endpoint Agent comprises the following four main components:

Administration agent

Local processes

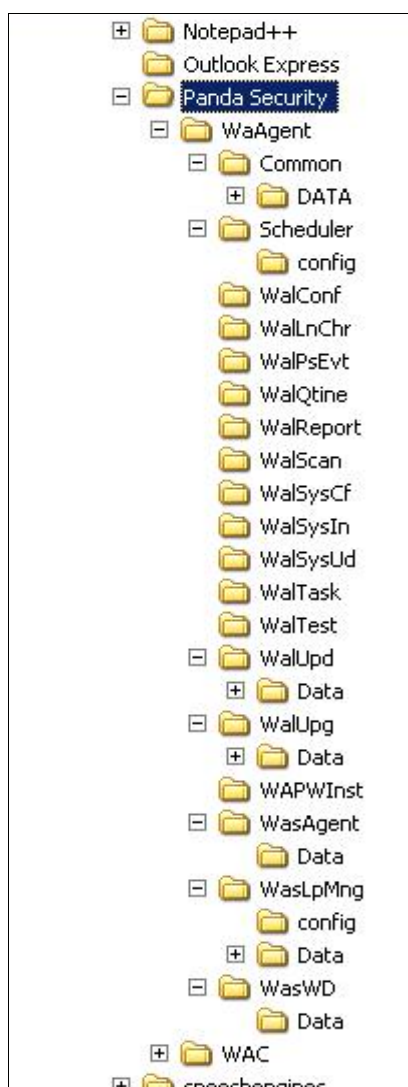
Watchdog



Task scheduler

### Panda Endpoint Agent folder tree and registry entries

In the following diagram, AdminIEClientPath is the root path where the modules are installed.





WaAgent – Root installation folder of Panda Endpoint Agent.

Common – Folder with the common files, such as WalAgApi.dll, kernel libraries, etc. A sub-folder called **Data** is created in this folder during execution of local processes.

Scheduler – Folder where the task scheduler files will be saved.

`scheduler\Config` - Folder where the task scheduler tokens will be saved.

WalHost – Folder where the administration agent service files will be saved. A sub-folder called Data will be created in this folder during execution of local processes.

WalConf – Folder where the WalConf local process files will be saved.

WalTest – Folder where the WalTest local process files will be saved.

WalLnChr – Folder where the WalLnCh local process files will be saved.

WalPsevt - Folder where the WalLPsEvt local process files will be saved.

WalQtine – Folder where the WalQtine local process files will be saved.

WalReport – Folder where the WalReport local process files will be saved.

WalScan – Folder where the WalScan local process files will be saved.

WalSNet – Folder where the WalSNet local process files will be saved.

WalSysCf – Folder where the WalSysCf plugin files will be saved.

WalSysIn – Folder where the WalSysIn plugin files will be saved.

WalSysUd – Folder where the WalSysUd plugin files will be saved.

WalTask – Folder where the WalTask plugin files will be saved.

WalUpd – Folder where the WalUpd local process files will be saved. A sub-folder called **Data** will be created in this folder during execution of local processes

WalUpg – Folder where the WalUpg local process files will be saved. A sub-folder called **Data** will be created in this folder during execution of local processes

WAPWInst – Folder where the files of the installation supervision process will be saved.

WasAgent – Installation root directory of the administration agent. When run, the agent creates a subfolder called **Data**.

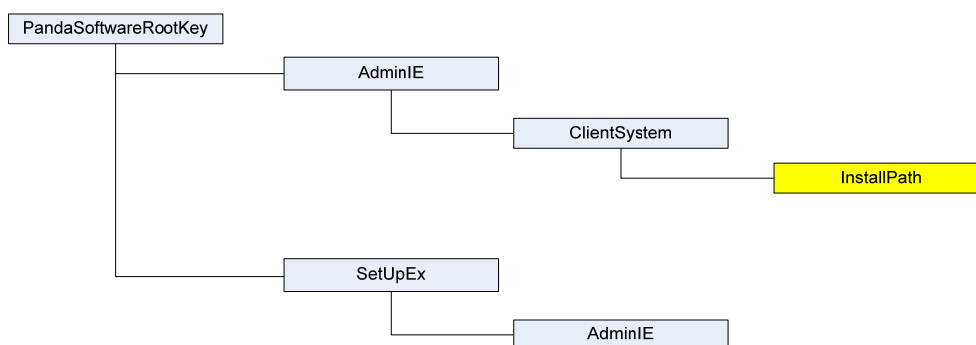




WasLpMng – Folder where the local process manager files will be saved.

WasLpMng\Config – Folder where the local process manager tokens will be saved.

### Windows registry entries tree



**Panda Security** refers to the Windows registry key **HKEY\_LOCAL\_MACHINE\SOFTWARE\Panda Security**.

### AdminIE

- Folder where all Panda Cloud Office Protection registry entries are created.

ClientSystem

- Registry key containing the Panda Endpoint Agent entries. These entries are:

- **InstallPath** – This contains the root directly in which Panda Endpoint Agent has been installed ("AdminIEClientPath")

EventSystem

Contains the event system settings

Protections



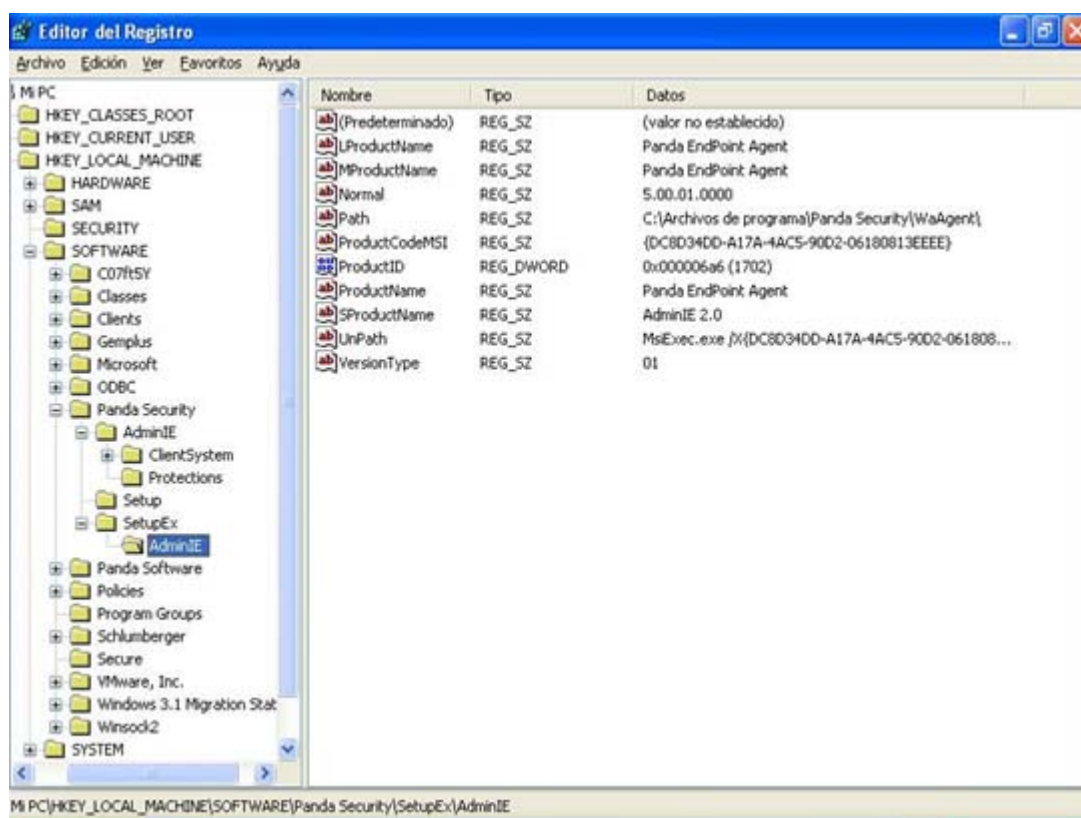
Contains information about the protection.

WAHost

Contains the administration agent service settings.

**SetupEx** - Folder in which the registry entries are created which will be used by the agent installers.

**AdminIE** - Registry key containing the Panda Endpoint Agent entries used by the installers. These entries are illustrated in the following diagram:



When run, the agent creates the "AgentSystem" key under "ClientSystem". Within this key several entries are created. All the installer has to do is to delete the "AgentSystem" key and its entries in the uninstallation process.



### Distribution of files

All administered computers have the administration agent installed. Along with the agent, local processes are also installed. Below we list all the paths and files of the administration agent and their local processes:

#### Administration agent

The agent is installed in `<Admin\EClientPath>\WasAgent`

- WasAgent.conf
- WasAgent.dll
- WaPIRes.exe
- WAInterface.dll
- Wa\_AGPRX.dat
- LPTokens.dat
- INTEGRA.dat
- INTEGRA.bak (generated during installation but not distributed)
- AgentSystem.DAT
- proxy.dat (generated during installation but not distributed)

During execution of the agent the "Data" subfolder is created with the following files:

- WasAgent.log
- WasLpMng.log
- WapWinst.log
- Counters.ini

The "AgentSystem" registry key is also created under "ClientSystem". Within this key several entries are created:



- Value1
- Value2
- Value3

If the Internet connection is via proxy, the connection details requested from the user are stored in AgentSystem.dat in the folder **<AdminIEClientPath>\WasAgent**.

All must be deleted during uninstallation.

### WalConf local process

Installed in **< AdminIEClientPath >\WalConf**

- WalConf.ini
- WalConf.dll

The following file is created during execution of this local process:

- Walconf.log

### WalLnChr local process

Installed in **< AdminIEClientPath >\WalLnChr**

- WalLnChr.dll

The following file is created during execution of this local process:

- WalLnchr.log



### WalQtine local process

Installed in < AdminIEClientPath > \WalQtine

- WalQtine.ini
- WalQtine.dll

The following file is created during execution of this local process:

WalQtine.log

### WalReport local process

Installed in < AdminIEClientPath > \WalReport

- WalReport.dll
- WalReport.ini

The following file is created during execution of this local process:

- WalReport.log

### WalScan local process

Installed in < AdminIEClientPath > \WalScan

- WalScan.dll
- WalScan.ini

The following file is created during execution of this local process:

WalScan.log



### WalTest local process

Installed in < AdminIEClientPath > \WalTest

- WalTest.dll
- WalTest.ini

The following files are created during execution of this local process:

- WalTest.dat
- WalTest.log
- Waltestlt.dat
- Waltestdf.dat

### WalUpd local process

Installed in < AdminIEClientPath > \WalUPd

- WalUpd.dll
- WalUpd.ini

The following files are created during execution of this local process:

- Counters.ini
- WalUpd.log

The subfolder Data is created and contains the Catalog subdirectory which can have the following files:



- WEB\_GUID
- WEB\_CATALOG
- LAST\_GUID
- LAST\_CATALOG
- LOCAL\_CATALOG
- RUMOR\_TABLE
- LOCAL\_CATALOG.TMP

Additionally, the Files subdirectory is created which temporarily holds the files needed for updates.

### WalUpg local process

Installed in < AdminIEClientPath > \WalUPg

- WalUpg.dll
- WalUpg.ini
- PavGenUn.exe
- Settings.ini

The following files are created during execution of this local process:

- Counters.ini
- WalUpg.dat
- WalUpg.log
- WAUPGTD.dat
- WAC\_Installer.log
- Agent\_Installer.log



The subfolder Data is created and contains the Catalog subdirectory which can have the following files:

- WEB\_GUID
- WEB\_CATALOG
- LAST\_GUID
- LAST\_CATALOG
- LOCAL\_CATALOG
- RUMOR\_TABLE
- LOCAL\_CATALOG.TMP

Additionally, the Files subdirectory is created which temporarily holds the installers needed for product installations/updates.

### WalSNet local process

Installed in < AdminIEClientPath >\WalSNet

- WalSNet.dll
- WalSNet.ini

The following files are created during the execution of this local process:

- WALNet.log
- WALNET.dat

### WalTask plugin

Installed in < AdminIEClientPath >\WalTask

- WalTask.dll





- WalTask.ini

The following files are created during execution of this local process:

- WalTask.log

SCAN\_TASKS.DAT

### WalSysCf plugin

Installed in < AdminIEClientPath > \WalSysCf

- WalSysCf.dll
- WalSysCf.dat

The following file is created during execution of this local process:

- WalSysCf.log

### WalSysUd plugin

Installed in < AdminIEClientPath > \WalSysUd

- WalSysUd\WalSysUd.dll

### Local process manager

Installed in < AdminIEClientPath > \WasLpMng

- WapLpMng.exe
- WasLpMng.exe
- Config\Plugins.tok (in the config subdirectory)
- WapLpmng.ini
- WasLpmng.ini



The following files are created during the installation process:

- WapLpmng.log
- WasLpmng.log

### Task scheduler

Installed in < AdminIEClientPath >\Scheduler

- PavAt.exe
- PavSched.exe
- PavAt3Api.dll
- Config\tokens.tok (in the config subdirectory)

The following files are created during execution of this local process:

- **Pavsched.cfg** (generated during the installation process)
- **Tasklist.lst** (generated during installation but not distributed)

### Main service

Installed in < AdminIEClientPath >\WAHost

- WAHost.exe
- WAHostClit.dll



### Common libraries

Installed in < AdminIEClientPath > \Common

APIcr.dll

AVDETECT.INI

DATA

libxml2.dll

MiniCrypto.dll

PavInfo.ini

pavsddl.dll

Platforms.ini

pskalloc.dll

PSLogSys.dll

pssdet.dll

psspa.dll

putczip.dll

puturar.dll

putuzip.dll

WalAgApi.dll

WalCount.dll

WALLMIInf.dll

WALMNAPI.dll

WALOSInf.dll

WALRVNCInf.dll

WALTVNCInf.dll

WALTVWRInf.dll

WALUtils.dll



WalUtils.ini

WALUVNCInf.dll

WaPrxRepos.dll

WaPrxRepos.Ini

WCheckReq.dll

The “Data” subfolder is created during execution, which contains the protection policies so that they are available when the protection is installed.

The following files are created:

- PavInfo
- WalUtils.log
- WALMNAPI.log
- WALLMIInf.log
- WALRVNCInf.log
- WALTVNCInf.log
- WALUtils.log
- WALTVWRInf.log
- WALUVNCInf.log

### Services

Panda Endpoint Agent creates the following service:

- WAHost.exe

Services are installed by calling the executable file through the option “-RegServer”, and are uninstalled through the option “-UnregServer”



### Deployment of Panda EndPoint Protection

#### Panda EndPoint Protection directory structure

Users can choose the path where they want to install the product, however, the default installation path is:

'%PROGRAMFILES%\Panda Security\WAC\' .....

InstallPath

Panda EndPoint Protection installation path. This contains the files needed for Panda EndPoint Protection to operate.

**Cache:** Contains the local signature files.

**Data:** Contains the behavior analysis technology data files.

**Drivers:** Contains the binaries used to install/uninstall the units.

**NNSNahs:** Binaries used to install the firewall intermediate driver.

**PSINDvct:** Binaries used to install the Device Control technology driver.

**Lang:** Contains the dictionaries with the strings in the various languages.

**LostandFound:** Contains the items restored from quarantine when they've been moved by the email protection or when they couldn't be restored to the original path.

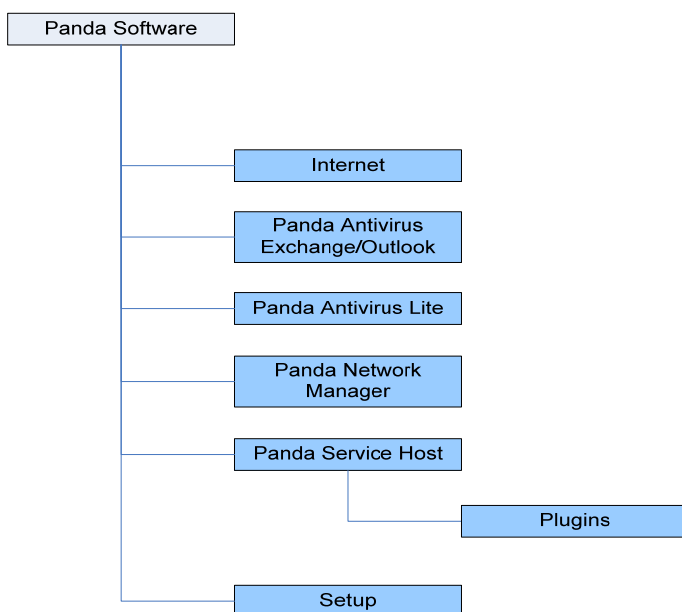
**Quarantine:** Contains quarantined items.



**PskTmp:** Temporary configuration files created during the scan.

### Registry entries

#### Registry entries in Panda Software



**Panda Security:** Key in HKEY\_LOCAL\_MACHINE\Software\Panda Security that contains the protection keys and values.

**AdminIE\Protections:** Key that contains the WAC value indicating where the client is installed.

**Nano Av\Boot:** Kept to maintain compatibility with previous versions. Not currently used.



**Nano AV\ModAV:** Kept to maintain compatibility with previous versions. Not currently used.

**Nano Av\Live:** Contains the DownloadFolder value indicating the client's downloads folder

**Nano Av\Panda Main Service:** Contains the plug-in loading values for the antivirus main module.

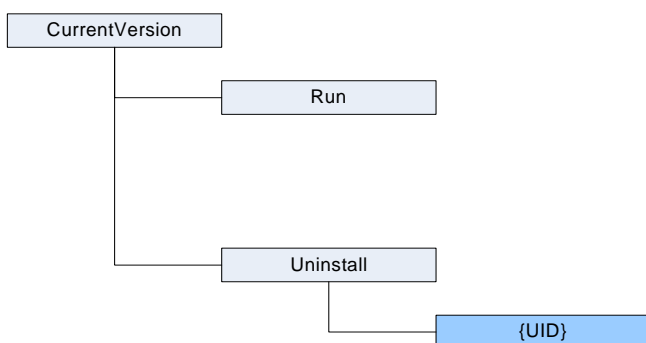
**Nano Av\Setup:** Contains the protection installation path.

**Panda Service Host:** Contains the plugins loaded in the service: update system, antivirus main system, engine, file and process interception system, device control configuration system, firewall.

**Panda Software\Setup:** Product information (name, version, ID, installation path, etc.)

### Registry entries in Windows\CurrentVersion

This section deals with the registry entries Panda EndPoint Protection creates in the "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion" key.



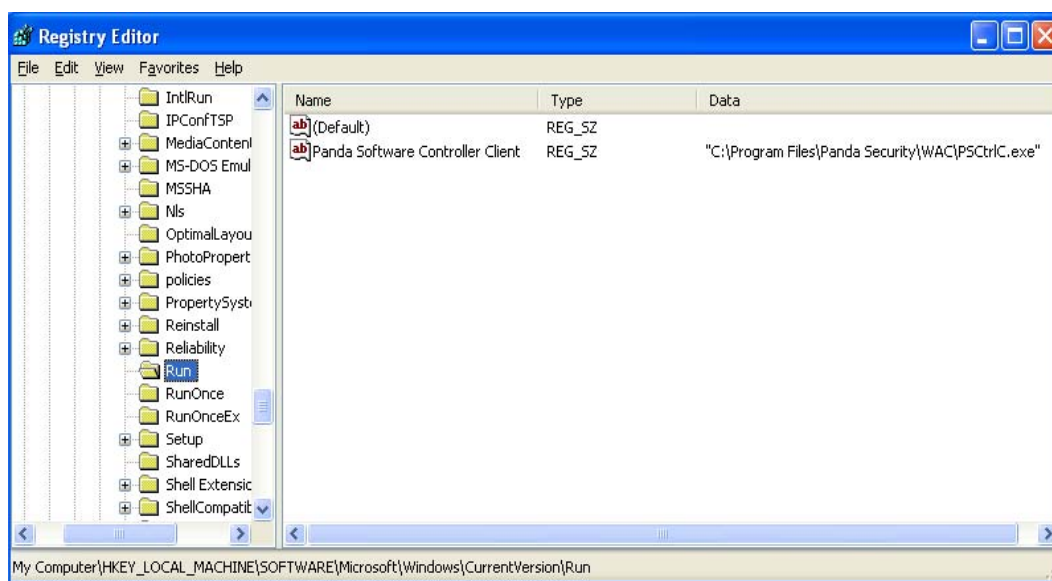


CurrentVersion

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Run

System key that indicates the path of the applications launched at the beginning.

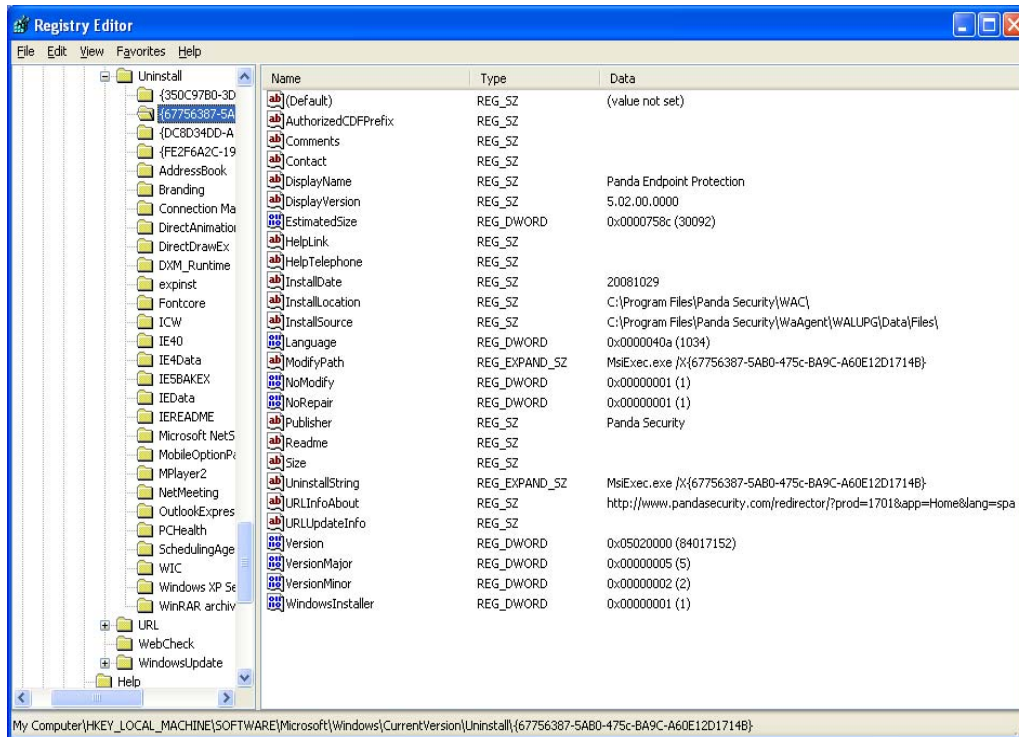


Uninstall

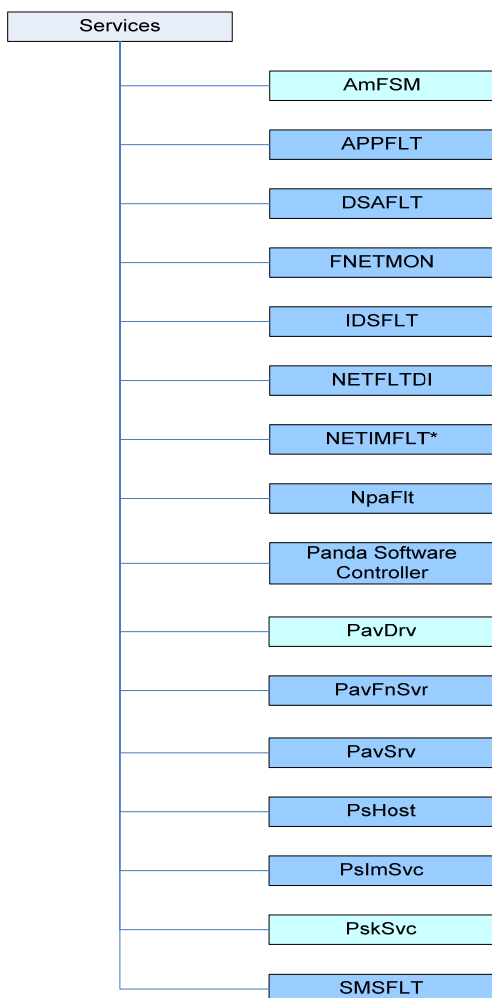
System key with information about uninstallers of products installed on the system.

**Panda Universal Agent Endpoint:** Key with the information needed to uninstall the product.





## Registry entries in Services



Services HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services

**NNSALPC:** Firewall driver

**NNSHTTP:** Firewall driver

**NNSIDS:** Firewall driver

**NNSNAHS:** Firewall driver



**NNSPICC:** Firewall driver

**NNSPIHS:** Firewall driver

**NNSPOP3:** Firewall driver

**NNSPROT:** Firewall driver

**NNSPRV:** Firewall driver

**NNSSMTP:** Firewall driver

**NNSSTRM:** Firewall driver

**NNSTLSC:** Firewall driver

**PRKPAVPROC:** Driver used in rookit scanning.

**PSBOOT.SYS:** Driver for operations at boot.

**PSINAflt:** Intercepting filter.

**PSINDvct:** Device Control driver.

**DVCTPROV.sys:** Device Control driver.

**PSINFile:** File intercepting driver.

**PSINKNC:** Kernel intercepting driver.

**PSINProc:** Process intercepting driver.

**PSINProt:** Protection driver (shield, KRE).

**PSKMAD:** Memory scanner driver.

### Services

**PSUAService:** Task control and management service in sessions.

**NanoServiceMain:** Client's main service for all protection modules.

**CLOUDUPDATEREX:** Upgrade tasks service.

### Processes



Apart from the services mentioned above, the following processes can be run on the system:

bspatch.exe

Process used to patch signature files.

PAV2WSC.exe

Process used to update the antivirus status in Windows Security Center.

PSANCU.exe

Process used to perform configuration tasks during client installation and upgrades.

PSINanoRun.exe

Process used to install and upgrade the client.

PSNCSysAction.exe

Process used to enable/disable the firewall's NNSNaHS intermediate driver.

PSUAMain.exe

Traybar process.

PSUNMain.exe

Client interface process.

Setup.exe

Installation and upgrade tasks process.

WAScanner.exe



Process that manages the background scanning tasks configured from the Web console.

### Appendix 3: Automatic computer search

Panda Cloud Office Protection includes a computer search system that gives administrators a global vision of the unprotected computers on the network.

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

#### Aspects to bear in mind when creating a search job

Searches run once per job.

The search job starts once the computer that must perform the search downloads the search command from the Panda Cloud Office Protection server. There is then a time period between the creation and running of a job.

You can start search jobs immediately through the **Update** option in the right-click menu of the protection installed on the computer that performs the search. Otherwise, a maximum of 4 hours may pass before the job is run.

You can define several search jobs for the computer that must perform them. In this case, the jobs will take place sequentially, in the established order.

If the computer is restarted during a computer search job, the job will start again 5 minutes after restart. Before this, the computer will query the server to find out if the job is still valid.



### Information to provide on configuring a search job

Job name (a maximum of 50 characters).

You cannot give two jobs the same name for the same client.

You cannot use the following characters: <, >, ", ',

Computer from which to launch the search job. This computer must be selected from the list of protected computers.

Finally, the administrator must select the scope of the search, among the following options:

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

One or several ranges of **IP addresses (IPv4)**. If ranges are entered that contain some common IP addresses, the relevant computers will be found only once.

One of several **domains** entered by the user.

### Requirements for the computer that performs the search

To have the agent and the protection installed, and be correctly integrated into the Panda Cloud Office Protection server.

The agent must be version 5.05 or later.

It cannot be blacklisted.

It must have established a connection to the Panda Cloud Office Protection server in the last 72 hours.

It cannot be carrying out an uninstallation job, that is, it cannot show any of the following statuses regarding an uninstallation job:

"On hold"

"Starting"

"Uninstalling"



It must have an Internet connection, either directly or through other computers ('proxy' feature)

As the search job progresses, Panda Cloud Office Protection will show the relevant status.

### Search job action sequence and job status

The user launches the search job through the Client Console (from a computer with the protection installed).

Job status: On hold

The computer that performs the search downloads the search command from the server. The server becomes aware of the action and changes the job status.

Job status: Starting

The computer that performs the search calculates the priority of the new job in relation to other jobs that might also be waiting to be run. The new job waits its turn according to the priority queue.

Job status: Starting

The computer that performs the search checks to see if it fulfills the requirements to run the job.

Job status: Starting

A message is sent to the server indicating that the job has started running.

Job status: In progress

The computer that performs the search starts scanning the network for the relevant computers.



Job status: In progress

### Search job action sequence

Getting a list of computers

By IP address (Ranges of IP addresses and subnet)

The system pings each IP address using the ICMP protocol

It waits for a response to the pings

It tries to resolve the names of the IP addresses that respond

By domain

A list is made of all the computers that belong to the domain

Checking to see if the computers on the list have the agent installed

A message is sent to the agent

The system waits for the response

### Generating a computer list and sending the results to the server

Search job results

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

This list contains:

1. Computers without an agent installed.
2. Computers integrated into another client.

It is not possible to communicate with agents from other clients, therefore no response is received and the system understands the computer is unprotected.





Computers with an agent version prior to 5.05.

The agent on these computers cannot respond to search messages, and so they are considered unprotected.

Computers with an agent version 5.05 or later, which haven't responded to the search message in due time. The wait time for a response is = 3 sec (wait factor)\* Number of computers that responded to the ICMP ping+30 sec (security margin).

**NOTE:** Blacklisted computers (provided they have an agent version 5.05 or later and are integrated into the client's console) are not considered as unprotected computers and will **NOT** appear as the result of the search job.

Details of unprotected computers

The following information is obtained about each unprotected computer found:

IP address.

Computer name, if the computer that performed the search could resolve it.

## Cases in which the server may NOT be aware that a computer search job has finished

### Case 1

The job status is "On hold", "Starting" or "In progress", and the protection of the computer that performs the search is uninstalled, the computer disappears from the database or is blacklisted while the job is running.

### Consequences

The computer that performs the search will not be able to inform the server of the job result.

As soon as the server is aware that the computer that performs the search has been eliminated, blacklisted or its protection has been uninstalled\*, the status of the search job will change to "Finished with error".



NOTE: It is considered that the protection has been uninstalled from the computer that performs the search as soon as it sends an 'uninstallation complete' message.

Also, if the computer that performs the search is eliminated...:

Its name is removed from the search job settings screen, and an error message is displayed indicating that the computer has been eliminated.

Once the computer is eliminated, the information about the group that the computer belonged to is also deleted. Therefore, monitoring users and administrators with permissions over that job (that is, with permissions over the group that the computer that performed the search belonged to), will not be able to view it.

### Case 2

The job status is "On hold", "Starting" or "In progress", and the computer that performs the search is blacklisted and restored later on.

### Consequences

The computer will continue with the job it was running, and therefore the job status may change from 'Finished with error' to 'Finished'. This is the only possible change of status.

If the computer that performs the search has communication problems while running it, it will not be able to inform the server of the job status and results.

The job status will remain unchanged ("On hold" "Starting" or "In progress") until it is eliminated.

If an error occurs while the job is being run (status "On hold", "Starting" or "In progress"):

The job status will remain unchanged ("On hold" "Starting" or "In progress") until it is eliminated.

If the **job is interrupted**, the following happens:



## Panda Cloud Office Protection

---

If the computer that performs the search is turned off before the search is complete (either on purpose or for any other reason), the agent will behave as follows on restarting the computer:

It queries the server to check if the job is still valid:

If it is valid, it will perform the search from the start again.

If it is not valid as the job has timed out, the search is canceled.

It waits 5 minutes after the computer has restarted to launch the search job again.