

## CORPORATE SOLUTIONS 4.07.

# RELEASE NOTES

### CONTENTS

<b>1. Centralized Administration: AdminSecure</b> .....	<b>2</b>
<b>1.1. Compatibility with previous versions of AdminSecure</b> .....	<b>2</b>
<b>2. Panda for Desktops (2000/XP/Vista/Win7) and Panda for File Servers (2000/2003/2008): Changes common to both products</b> .....	<b>2</b>
<b>2.1. Protection improvements</b> .....	<b>2</b>
2.1.1. Cloud-based scanning.....	2
2.1.1.1. Disabling cloud-based scans .....	3
2.1.2. Checking trusted digital signatures in suspicious items detected .....	4
<b>2.2. Compatible with Microsoft Office 2010</b> .....	<b>4</b>
<b>2.3. Detection of malware run from a pen drive (ExFAT file system)</b> .....	<b>5</b>
<b>2.4. Bugs corrected</b> .....	<b>5</b>
<b>3. Panda for Desktops (2000/XP/Vista/Win7): New Features</b> .....	<b>6</b>
<b>3.1. Microsoft Outlook 2010</b> .....	<b>6</b>
<b>3.2. On-demand scans of email include Windows Live Mail messages</b> .....	<b>7</b>
<b>4. ANNEX I: Versions table</b> .....	<b>9</b>

## **1. CENTRALIZED ADMINISTRATION: ADMINSECURE**

### **1.1. Compatibility with previous versions of AdminSecure**

The functional changes described here have been incorporated into the products Panda Security for Desktops and Panda Security for File Servers. These new product versions will be compatible with AdminSecure 4.04.XX and 4.05.XX.

## **2. PANDA FOR DESKTOPS (2000/XP/VISTA/WIN7) AND PANDA FOR FILE SERVERS (2000/2003/2008): CHANGES COMMON TO BOTH PRODUCTS**

### **2.1. Protection improvements**

#### **2.1.1. Cloud-based scanning**

Panda Security for Desktops and Panda Security for File Servers incorporate cloud-based scanning. These are the characteristics of this type of scanning:

- There will be a malware cache that will expire after 24 hours.
- Cloud queries won't have a digital goodware signature cache.
- The cloud scans will be able to classify items as suspicious.
- All configuration parameters must be obtained from one or more configuration files.
- Scheduled scans will also make use of local signatures.
- All executable files will be scanned from the cloud; there will be no limit on the types of files.
- Exclusions on the basis of reclassification of suspicious items will last for one month.
- It will be possible to scan folders recursively (as at present), and non-recursively (new feature).

#### **Memory scan**

- The memory scan will scan the same items as at present.
- The scan will be launched every 2 hours. However, if the computer cannot send queries to the cloud (either because it is disabled or there is no Internet connection), it won't be launched every 2 hours. It will be launched with the frequency established prior to the inclusion of cloud scans.
- Everything that exists in memory will be scanned using the cache knowledge so as not to launch cloud scans on items that are already identified.

#### **'High-risk' folder scan**

- By high-risk folders we mean those folders that Panda Security has identified as typical malware containers.
- Panda Security considers the following high-risk folders should be scanned:
  - The root directory of all local drives
  - The profile of all logged-in users
  - The system temporary folder
  - The Windows folder (non-recursively)
  - The System32 folder
- The scan will take place every 24 hours.
- If the computer cannot send queries to the cloud (either because it is disabled or there is no Internet connection), the scans will be performed every 48 hours using the signature file.
- Exclusions. The following won't be scanned:
  - Active users' recycle bins
- On servers, these scans will work as follows:
  - They will be performed once a week.
  - If the computer cannot send queries to the cloud, they will be performed once every two weeks.
  - Shared drives won't be scanned.

#### 2.1.1.1. Disabling cloud-based scans

You can disable the cloud-based scans using the registry keys. It is not possible, however, to do so from the AdminSecure Console.

You can disable:

- Memory scans.
- Background scans.
- Cloud queries as a whole.

## 2.1.2. Checking trusted digital signatures in suspicious items detected

We have improved the sensitivity of the heuristic engine used by the file permanent protection and on-demand scans of Panda Security for Desktops and Panda Security for File Servers.

### **On-demand scanning**

When, in an on-demand scan, a suspicious item is detected in a signed file, the signature will be contrasted with the Panda Security trusted digital signature file. This checking is synchronous (it takes place at the time of detection):

- If the detected file has a trusted digital signature, it won't be reported as suspicious or sent to quarantine.
- If the detected file DOESN'T have a trusted digital signature, it is reported as suspicious and sent to quarantine.

### **File permanent protection**

The programs also check the digital signature of suspicious items detected by the file permanent protection. The goodwill cache will be continuously used and fed with new data, if there is any, after each update of the signature file.

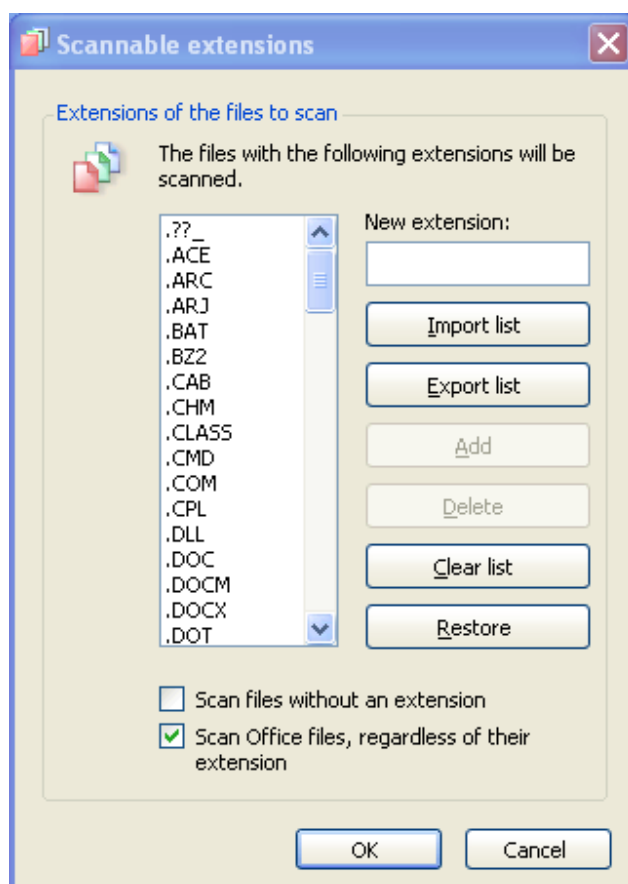
### **1:N signatures**

Both protections include detection of suspicious items using 1:N signatures.

## 2.2. Compatible with Microsoft Office 2010

Panda for Desktops and Panda for File Servers are compatible with all Microsoft Office 2010 extensions.

The option to scan all Office documents, available in the antivirus settings for Windows desktops and servers in the AdminSecure console, lets you scan Office 2010 documents:



## 2.3. Detection of malware run from a pen drive (ExFAT file system)

Panda for Desktops and Panda for File Servers detect malware in any ExFAT formatted drive, for example, a pen drive.

- The file permanent protection detects malware accessed from this type of drive.
- On-demand scans of ExFAT folders or drives detect all types of malware except rootkits.

## 2.4. Bugs corrected

- Incompatibility problems with the SecMaker NetID software
- Incompatibility problems installing the products' shield on HP Proliant G6 servers.
- A blue screen was displayed after upgrading Panda for Desktops to version 4.05.10
- Permanent protection counters were not restarted on clicking the Reset counters button.
- Items were not manually deleted from the quarantine or when they exceeded the day limit to be automatically deleted.

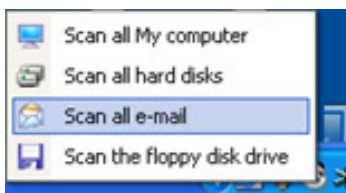
- Memory blockage on launching an on-demand scan of "All My Computer".
- Occasionally, on disabling the TruPrevent and NetworkSecure protection, they kept on running.
- When Panda for Desktops was updated to version 4.05.10/15 the shared files could not be accessed.
- When a scan was scheduled the status was not updated.
- File loading to an NLB server was very slow.
- Error code 2101 occurred on updating the signature file on workstations.
- Problems occurred on receiving a warning email with Courier Mail Server 2.08.
- TruPrevent and Network Secure execution errors.

### 3. PANDA FOR DESKTOPS (2000/XP/VISTA/WIN7): NEW FEATURES

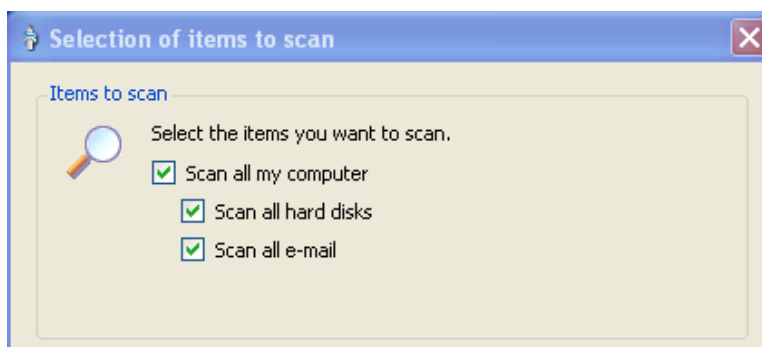
#### 3.1. Microsoft Outlook 2010

Even though Panda Security for Desktops doesn't include a specific mail interception technology version for Outlook 2010, it does have a number of features compatible with Outlook 2010:

- Mail received in Outlook 2010 under POP3 and SMTP will be scanned. Interception of these messages will take place at protocol level.
- You can run **on-demand scans** from the protection's pop-up menu:



- You can run on-demand scans from the AdminSecure console:

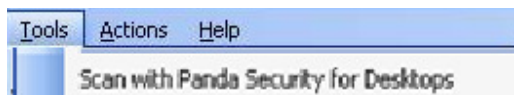


There are, however, the following limitations:

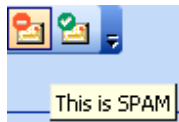
- There will be no option to scan messages from the Outlook 2010 toolbar.



- The option 'Scan with Panda Security for Desktops' will not be available in the 'Tools' menu of Outlook 2010.



- There will be no option to classify messages as spam or not spam from the Outlook 2010 toolbar.



- There will be no MAPI permanent mail protection; i.e. messages exchanged between Outlook 2010 and the Exchange server using MAPI will not be scanned during the interception, but locally.

### 3.2. On-demand scans of email include Windows Live Mail messages

Panda Security for Desktops will also scan messages stored locally in Windows Live Mail.

- On-demand scans launched from the protection's pop-up menu will scan Windows Live Mail messages.
- On-demand scans configured from the AdminSecure console will scan **Windows Live Mail** messages.

**Panda Security for Desktops**

### Scanning e-mail

**Scan in progress**

Outlook Express ▾

Windows Mail ▾

...

	Memory	Boot	Files	Messages
Scanned:	-	0	0	0
Infected:	0	0	0	0
Disinfected:	0	0	0	0
Moved to quarantine:	-	-	0	0
Deleted:	-	-	0	0

## 4. ANNEX I: Versions table

### 4.1 Panda for Business 4.07.00

<b>MODULE</b>	<b>VERSION</b>
<b>AdminSecure</b>	4.05.xx
<b>Panda for Desktops (2000/XP/Vista/Win7)</b>	4.07.10
<b>Panda for File Servers (2000/2003/2008)</b>	8.07.10