

## CORPORATE SOLUTIONS 4.04

# DOCUMENT OF CHANGES

### CONTENTS

<b>1. Centralized Administration: AdminSecure</b> .....	<b>1</b>
<b>1.1. New features of the version</b> .....	<b>1</b>
1.1.1. Improved processing of numerous configuration jobs.....	1
1.1.2. Optimized search of network computers.....	1
1.1.3. Improved management of installation and update incidents .....	2
1.1.4. More efficient AdminSecure upgrades .....	2
1.1.5. Usability of lists displayed in the console .....	4
1.1.6. Distribution servers: Improved proxy servers with integrated authentication.....	4
1.1.7. More automatic uninstallers in AdminSecure .....	4
1.1.8. Technological adaptation.....	5
<b>1.2. Bugs corrected</b> .....	<b>5</b>
<b>2. Panda for Desktops (2000/XP/Vista)</b> .....	<b>7</b>
<b>2.1. New features of the version</b> .....	<b>7</b>
2.1.1. Technological adaptation.....	7
<b>2.2. Bugs corrected</b> .....	<b>7</b>
<b>3. Panda for File Servers (2000/2003/2008)</b> .....	<b>8</b>
<b>3.1. New features of the version</b> .....	<b>8</b>
3.1.1. Technological adaptation.....	8
<b>3.2. Bugs corrected</b> .....	<b>8</b>
<b>4. Panda for Exchange (2007 and 2000/2003)</b> .....	<b>9</b>
<b>4.1. New features of the version</b> .....	<b>9</b>
4.1.1. New Content Filter feature.....	9
4.1.2. Improved treatment of messaged received at the "Badmail" folder in Exchange 2007 .....	10
4.1.3. Technological adaptation.....	10
<b>4.2. Bugs corrected</b> .....	<b>11</b>
<b>5. Panda for ISA</b> .....	<b>11</b>
<b>5.1. New features of the version</b> .....	<b>11</b>
<b>5.2. Bugs corrected</b> .....	<b>11</b>

- 6. Panda for Domino ..... 11**
  - 6.1. New features of the version..... 11**
  - 6.2. Bugs corrected ..... 11**
- 7. Panda for Linux and Panda for Linux Servers..... 12**
- 8. Panda Commandline (Windows)..... 12**
  - 8.1. New features of the version..... 12**
  - 8.2. Bugs corrected ..... 12**
  
- ANNEX I: Versions table..... 13**

# 1. CENTRALIZED ADMINISTRATION: ADMINSECURE

## 1.1. New features of the version

### 1.1.1. Improved processing of numerous configuration jobs

When general changes were made to the configuration and there was a large number of computers to be configured, the distribution server could crash.

This version fixes that problem, which mainly affected networks with more than 200 computers.

This has been achieved by **optimizing the process for sending configuration modification jobs** in the server, and including the possibility of limiting the maximum number of jobs in progress (the default value is 10).

You can increase or reduce that number depending on the network needs, through the following registry entry:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Panda Software\Panda Administrator 3.0\AdminServer\  
**MaxRunningConfigTask**

### 1.1.2. Optimized search of network computers

In previous versions, the **process to identify the network computers to protect** wasn't very effective.

The process made a call and waited to receive replies from computers. In some cases, these replies took too long to arrive or were incorrectly processed (they were lost or other types of errors were reported).

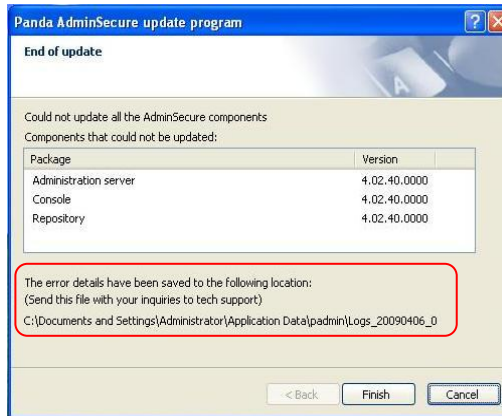
To resolve this, the following improvements have been made:

- The default wait time –1 second– can be increased through a Windows registry key (WaitTimeOut). This way, administrators can increase the time to receive replies.
- All replies received are filtered by the ICMP (Internet Control Message Protocol) so that only valid replies are processed (those of the Echo reply type).

### 1.1.3. Improved management of installation and update incidents

When installation/update errors occurred, it was difficult to obtain information to diagnose the cause of the error.

From this version onwards, when an error occurs, a **message is shown indicating the path to the log files** with information about the cause of the error.



### 1.1.4. More efficient AdminSecure upgrades

The **AdminSecure upgrades could fail**, leaving the original installation inoperative.

To avoid this, many administrators chose to uninstall AdminSecure and reinstall it again, which was very time consuming as they had to reconfigure the entire console again.

This version incorporates checkpoints at specially conflictive points for the upgrade so that it is possible to apply a solution before errors occur.

✓ **Recently restarted computer:**

It is advisable that the computer where AdminSecure is installed has been restarted recently. The upgrade will check to see if the computer has been on for more than 48 hours. If it has, the user will be warned that before carrying out the upgrade it is recommended to have restarted the computer recently.



✓ **Change of database name:**

Quite frequently, administrators decided to change the database name after installation. In cases like that, upgrades carried out at a later time couldn't find the database and an error occurred. Now, this type of situation is detected and the database is updated keeping the name chosen by the administrator.

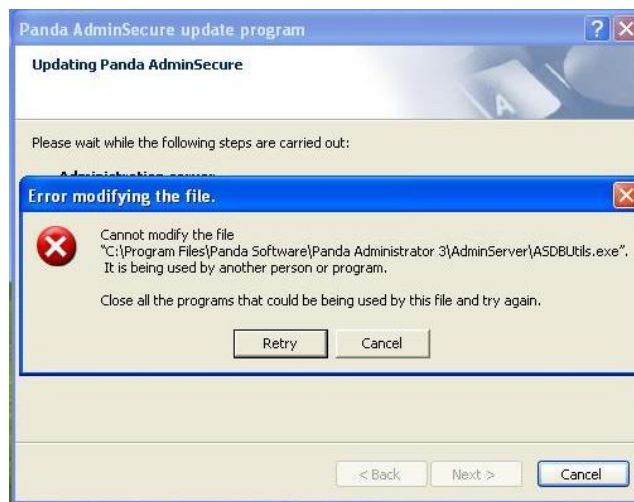
✓ **Permissions to update the database:**

If the user doesn't have the necessary permissions to update the database, a screen asking for them is displayed to continue with the update.



✓ **Files in use:**

The process will check if there are files that cannot be updated as they are in use at the time of the upgrade. If some is detected, the administrator will receive a notification and will be requested to stop them manually.



### 1.1.5. Usability of lists displayed in the console

At present, the **information displayed in the console is refreshed** every 20 seconds.

This can be rather annoying. Therefore, **this feature will be disabled by default from version 4.04 onwards**. In any event, it will be possible to refresh the information through the relevant command, or using the F5 key.

### 1.1.6. Distribution servers: Improved proxy servers with integrated authentication

In some scenarios, when the distribution server had to get updates through a proxy server that only had integrated authentication enabled, it was not possible to download the updates.

This version modifies the distribution server and its associated components, so that just by configuring Internet access in the usual way, authentication can take place in proxy servers that only support integrated authentication.

### 1.1.7. More automatic uninstallers in AdminSecure

This version automatically uninstalls a larger number of antivirus programs. This has resulted in easier protection uninstallation-installation processes.

Thanks to the automatic uninstallers, the administrator does not need to manually uninstall the antivirus programs installed on the network. They are automatically uninstalled when Panda for Desktops or Panda for File Servers are installed.

These are the new products that are automatically uninstalled:

ANTIVIRUS PROGRAMS
Trend Micro OfficeScan 7.5
Trend Micro OfficeScan 8.0
F-Secure Anti-Virus Client Security 6.03
Panda Antivirus Pro 2009
Panda Global Protection 2009
Panda Internet Security 2009
Panda Endpoint Protection (PMOP) 5.02.03
Panda Endpoint Protection (PMOP) 5.03.00
Panda Endpoint Protection (PMOP) 5.03.01

### 1.1.8. Technological adaptation

- ✓ From this version onwards it is possible to install AdminSecure on Windows Vista SP2.
- ✓ AdminSecure will be able to identify computers with the new Microsoft platform **Windows 7**.

### 1.2. Bugs corrected

- Fixed problems detecting computers.
- Some special versions of Symantec 10.1 were not uninstalled correctly.
- Under certain conditions, error 1545 occurred on applying the protection settings.
- Fixed problems installing the agent on computers with Windows 9x.
- Fixed update problems on computers with Windows 9x.
- The infected file was not displayed in reports generated by the user.
- Fixed an installation problem on some Windows 2003 Small Business SP2 servers.
- Some errors occurred in some languages on deploying the protection from the Installation wizard.

- On certain occasions, the corporate resources use level was never green.
- In some Windows 2008 versions, it was impossible to install AdminSecure due to a permission error.
- The server changed the listening port on incorrect restarts or during installations on virtual machines, and the computer was not displayed in the console.
- The distribution server authentication process launched updates when it shouldn't.
- Some special versions of Symantec 11.0.3 were not uninstalled correctly.
- On some occasions, the Internet Explorer 7 browser stopped working after installing the protection.
- Detection events were not displayed correctly in Greek.
- On some occasions, the settings to update the protection automatically were not applied.
- Scan jobs whose status was "Scheduled" could not be removed.
- The event log was deleted unexpectedly.
- The result shown by the Top Ten list of Viruses and other known threats was not always correct. Depending on the time interval chosen, there was a lack of coherence between the graph and the virus list.
- Login script modification from the console for Novell networks failed and returned an error message.
- If sending of quarantined items failed due to an error on Panda's servers, a warning was displayed informing that the proxy credentials were incorrect.

## 2. PANDA FOR DESKTOPS (2000/XP/VISTA)

### 2.1. New features of the version

#### 2.1.1. Technological adaptation

- ✓ From this version onwards, **Panda for Desktops** will be identified by the Windows Security Center on Windows Vista SP1. This way, computers with this protection installed will be displayed as secure.
- ✓ **Panda for Desktops** can be deployed from this version onwards to computers with:
  - Windows Vista SP2
  - Windows Embedded POSReady 2009

### 2.2. Bugs corrected

- When a message was detected as Phishing and it was over 4Kb in size, the message body was eliminated.
- When permanent protection was monitored, and email protection was disabled, errors 1915 occurred in the AdminSecure events.
- The message "Error Creating COM Object" was displayed on starting up a computer. The reason was that system registration was not completely correct. This is now detected and fixed on restart.
- Computers that used the [www.securstar.com](http://www.securstar.com) DriverCrypt software could not be started.
- You couldn't disable the protection by malware type.
- On surfing the Internet with Internet Explorer 7, if you opened several tabs, sometimes the browser stopped working.
- Computers with the Vista operating system, a signature file dated between 02/16/2009 and 02/19/2009 and TruPrevent enabled, froze at startup.

## 3. PANDA FOR FILE SERVERS (2000/2003/2008)

### 3.1. New features of the version

#### 3.1.1. Technological adaptation

- ✓ **Panda for File Servers** is compatible, from this version onwards, with:
  - Windows Server 2008 SP2
  - Microsoft Small Business 2008
  - Citrix XenApp 5
- ✓ **Panda for File Servers** stops being compatible, from this version onwards, with:
  - Novell Servers

### 3.2. Bugs corrected

- Scanning certain files created with Office 2007 returned an error and the protection stopped scanning.
- On computers with TruPrevent installed but disabled, an error message was incorrectly displayed in the agent log files. If events were enabled, this error appeared in the Windows system events too.
- When Panda for File Servers was upgraded but the servers were not restarted after installation, the administrator session was blocked for several days, and the servers eventually restarted themselves without administrator authorization.
- Running VMWare Server on 64-bit systems, if a memory scan was performed or the signature files were updated, the virtual machines that were running stopped.

## 4. PANDA FOR EXCHANGE (2007 AND 2000/2003)

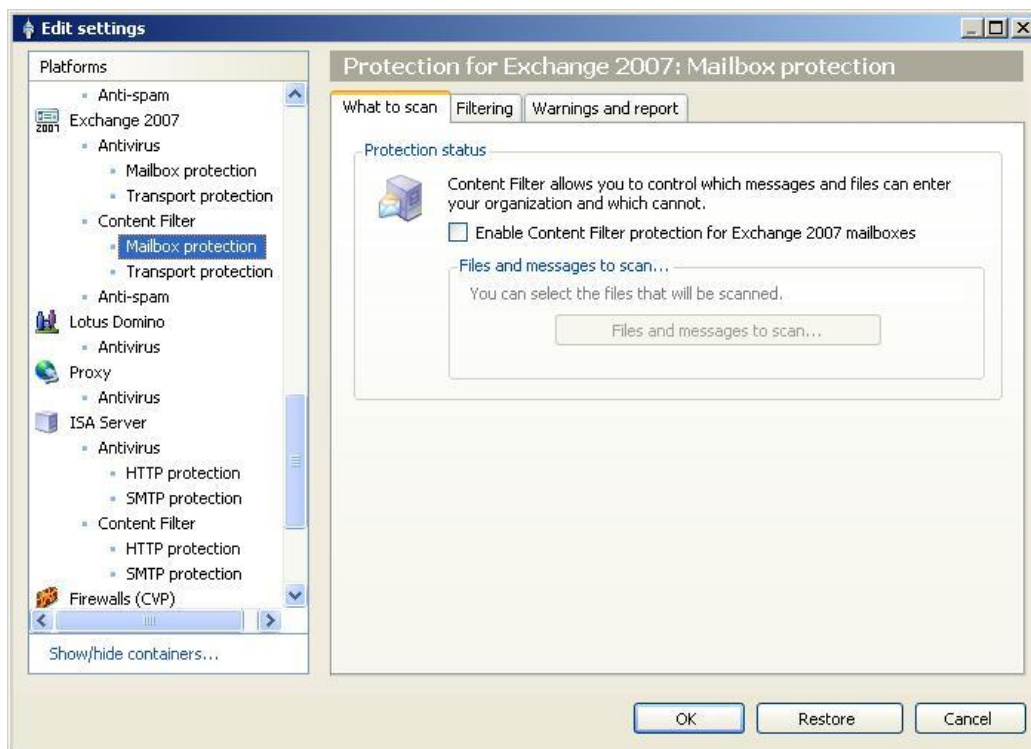
### 4.1. New features of the version

#### 4.1.1. New Content Filter feature

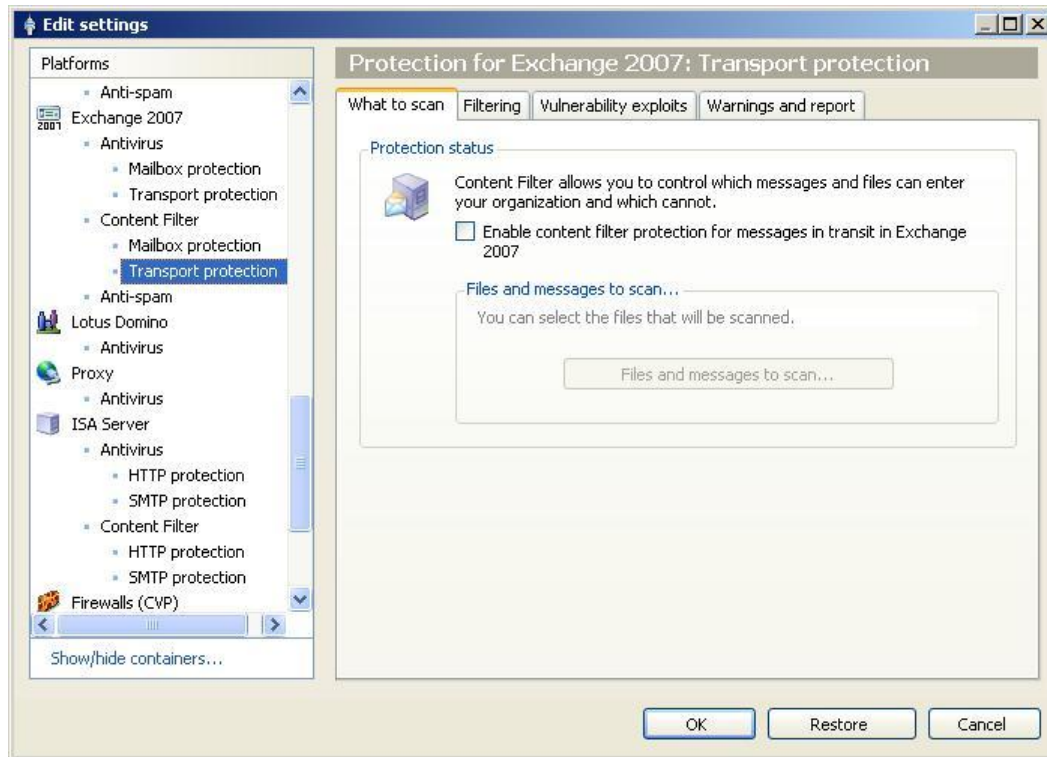
The **Content Filter** feature, already available for Exchange 2000 and 2003, is also available from this version onwards for **Exchange 2007** servers.

This unit will be managed from the AdminSecure console. It will be possible to configure the **mailboxes** and **transport** independently:

- **Mailbox protection:** You can define the messages and files to scan, exclude attachments from scanning, set warnings and generate reports.



- **Transport protection:** You can define the messages and files to scan, exclude attachments from scanning, detect vulnerabilities, set warnings and generate reports.



#### 4.1.2. Improved treatment of messaged received at the "Badmail" folder in Exchange 2007

In previous versions, when there was an error in the protection, messages were stored in the "Badmail" folder and deleted from the server. This prevented messages without malware to reach their destination.

From this version onwards, messages will continue to be copied to the Badmail folder, but won't be deleted from the server and will be flagged as scanned.

#### 4.1.3. Technological adaptation

The protection for Exchange 2007 servers is compatible with Exchange Server 2007 SP1 installed on Windows Server 2008 SP2.

## 4.2. Bugs corrected

- Scanning specially-crafted HTML files blocked the scanner, moving the rest of messages being scanned to the Badmail folder.
- An internal error caused messages to be deleted from the client's mailboxes.
- Content Filter corrupted or deleted legitimate Office 2007 files as it deleted part of their internal content.
- An error occurred in the scanning process (by the Content Filter unit) on deleting an element from a message. The element to be deleted was replaced with a notification file.

## 5. PANDA FOR ISA

### 5.1. New features of the version

There are no changes to the features.

### 5.2. Bugs corrected

- The 'IP address' and 'domain' blacklists in the Content Filter address filter did not recognize all elements entered.

## 6. PANDA FOR DOMINO

### 6.1. New features of the version

- ✓ The protection is compatible from this version onwards with **Lotus Domino 8.5**.
- ✓ In previous versions, the protection included a notification in the Domino console every time it started or stopped. On certain occasions, errors occurred as writing to the console failed. From this version onwards the **default behavior is modified to avoid writing to the Domino console**. This default behavior can be modified at any time through a registry entry for the WriteConsole value.

### 6.2. Bugs corrected

- No bugs corrected.

## 7. PANDA FOR LINUX AND PANDA FOR LINUX SERVERS

From this version onwards, **Panda for Linux and Panda for Linux Servers will stopped being sold**, either individually or integrated in the Panda for Enterprise, Panda for Business and Panda for Business Exchange suites.

For more information, refer to the life-cycle policy posted on the corporate website:

<http://www.pandasecurity.com/enterprise/support/lifecycle/>

## 8. PANDA COMMANDLINE (WINDOWS)

### 8.1. New features of the version

The improvements to this version include:

- Optimized memory use in scans.
- Code debugging to avoid potential problems.
- The product has been designed to identify new malware signature formats.
- Improved disinfection on computer restart.

### 8.2. Bugs corrected

- Fixed loss of detection caused by a scan problem when creating names files in the disk.
- Fixed startup problems with the heuristic engine.
- Fixed problems scanning corrupted elements.
- Fixed loss of detection scanning files.
- During disinfection, files were left with 0 bytes instead of being deleted.
- Fixed loss of heuristic detection.
- Fixed problems disinfecting multi-infected items.
- Fixed memory leaks scanning/disinfecting elements.
- The suspicious files report was always displayed in English, except for Spanish. This has been fixed so that the information is shown in the corresponding language.

## ANNEX I: VERSIONS TABLE

<b>MODULE</b>	<b>VERSION</b>
<b>AdminSecure</b>	4.04.10
<b>Panda for Desktops (2000/XP/Vista)</b>	4.04.10
<b>Panda for File Servers (2000/2003/2008)</b>	8.04.10
<b>Panda for Exchange Servers (2007)</b>	4.20.10
<b>Panda for Exchange Servers (2000/2003)</b>	3.20.04
<b>Panda for ISA Servers</b>	2.12.05
<b>Panda for Domino Servers</b>	2.41.05
<b>Panda Commandline (Windows)</b>	9.5.1.1