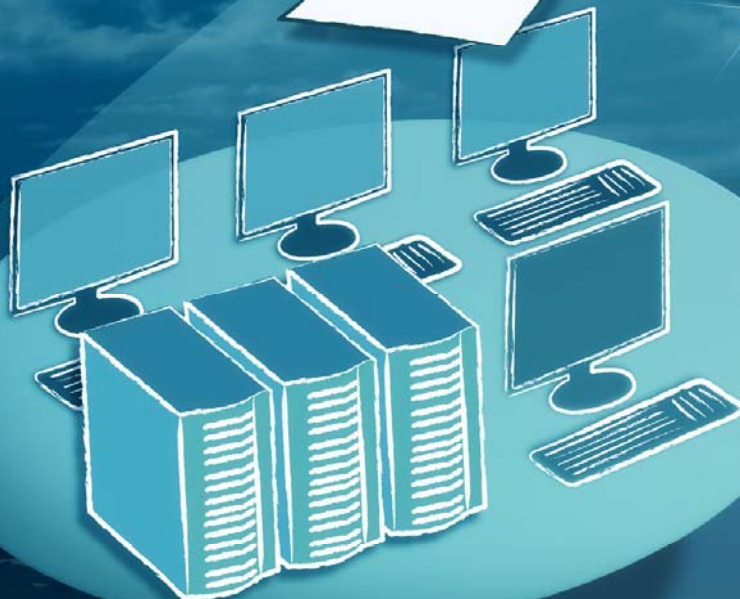


COLLECTIVE INTELLIGENCE

HYBRID
CLOUD





Improvements implemented in Panda GateDefender Performa HotFix Packs

Improvements HotFix Packs

Copyright notice

© Panda Security 2011. 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 López de Haro 4, 48001 Bilbao (Biscay) Spain.

Registered Trademark

Panda Security™. TruPrevent: Registered in U.S.A Patent and Trademark Office. 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 owners. D. L. BI-1915-07

© Panda Security 2011. All rights reserved.



Table of contents

1. HOTFIX PACKS FOR VERSION 4.00.50 OF PANDA GATEDEFENDER PERFORMA7	
1.1 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 4.00.50.0100.....	7
2. HOTFIX PACKS FOR VERSION 4.00.00 OF PANDA GATEDEFENDER PERFORMA9	
2.1 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 4.00.00.0300.....	9
2.2 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 4.00.00.0200.....	10
2.3 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 4.00.00.0100.....	11
3. HOTFIX PACKS FOR VERSION 3.02.00 OF PANDA GATEDEFENDER PERFORMA12	
3.1 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 3.02.00.0500.....	12
3.2 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 3.02.00.0400.....	12
3.3 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 3.02.00.0300.....	13
3.4 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 3.02.00.0200.....	14
3.5 IMPROVEMENTS IMPLEMENTED IN HOTFIX PACK 3.02.00.0100.....	15

Improvements HotFix Packs



Symbols and fonts used in this guide. Icons used in this documentation:



Note. Provides additional information and useful data.



Warning. Highlights the importance of a concept.



Tip. Useful ideas to help you get the most out of the program.



Reference. Other points that offer more information that you might find useful.

Fonts and styles used in this document:

Bold. Names of menus, options, buttons, windows or dialog boxes.

Code. Names of files, extensions, folders, commandline information or configuration files such as, scripts.

Italics: Names of options related to the operating system and programs and files with their own name.

Improvements HotFix Packs



1. Hotfix Packs for version 4.00.50 of Panda GateDefender Performa

1.1 Improvements implemented in HotFix Pack 4.00.50.0100

The following problems are fixed within this HotFix Pack:

- ❖ Reports were incorrectly exported due to a data limitation problem in models SB and 8100. The maximum number of records in reports has been reduced to 100,000 for the SB and 8100 models (HF 4.00.00.0207).
- ❖ Update hotfixes were getting too large to import. The maximum file size limit has been increased from 50 MB to 80 MB. (HF 4.00.50.0001).
- ❖ NTP, SSL and XSS vulnerability correction.
 - NTP: We have updated the ntp and ntpdate packages to versions 4.2.4p4+dfsg-8lenny3. These versions include the patch for DoS bug 1331.
 - XSS: Added a filter to the console servlets parameters to prevent XSS attacks.
 - SSL: We have upgraded the console certificate to v3. The key size is 1024 bits; MD5 is no longer used.
 - The Web console can no longer be accessed through the network IP address.
 - Deleted certain svn files from the console.(HF 4.00.50.0002).
- ❖ After a signature update, during Content Filter scans, anti-malware process cores were generated. We have corrected several kernel libraries and the signature file to fix this error. (HF 4.00.50.0004).
- ❖ Console error when selecting more than one profile in "Assign settings to local profiles". This was due to the fact that when importing the settings of a previous version the config.status files were not created (HF 4.00.50.0005).
- ❖ Problems with the NLB cluster (virtual MAC addresses did not work correctly). Fixed the kernel patch that allows static MAC addresses to be entered in the fdb table. This way, you can work with virtual MAC addresses as in the 3.02.00 version. Fixed the program that allowed static MAC addresses to be entered. (HF 4.00.50.0006).
- ❖ Incorrect HTTP connection limits. (HF 4.00.50.0007).



- ❖ LDAP manager memory leak. (HF-4.00.50.0008).
- ❖ Memory problems launching internal processes. (HF-4.00.50.0009 / HF 4.00.50.0011).
- ❖ Fixed problems with the quarantine filter when there was more than one recipient. (HF 4.00.50.0010).

Bug fixes included in the HF Pack but not present in previous hotfixes:

- ❖ The virtual appliance did not restart when the application manager stopped working. To fix this, the virtual appliance comes with softdog.
- ❖ The installed hotfixes did not display all characters correctly. We've made the relevant changes to the Web administration console.
- ❖ The URL field in reports didn't show session variables. To avoid this, there is no filtering out of URL search parameters.
- ❖ There were errors in users' submissions of categorization suggestions to Commtouch. A new header has been added to the substitute page to avoid filtering out POSTs sent to Commtouch.
- ❖ Fixed a bug in the anti-malware cache for responses whose filename was different from that of the request (problem detected with the eicar test page). To fix this, the system no longer parses the response filename (it keeps the one in the request).
- ❖ Empty rejection codes received at the proxy server. To prevent this, we have included default values in the response code for HTTP and SMTP blocking.
- ❖ The passwords used when configuring LDAP sources could not contain more than 12 characters. We have increased this limit to 30 characters.

◀ [Content](#)



2. Hotfix Packs for version 4.00.00 of Panda GateDefender Performa

2.1 Improvements implemented in HotFix Pack 4.00.00.0300

The HFPack 300 is based on the previous HFPack (HFPack200) and in consequence includes all the patches included in this last HotFix Pack.

In addition to this, the following problems are fixed within this HotFix Pack:

- ❖ Fixed problem with the network cards in the new 9500 Nexcom models. Corresponds to individual HF 4.00.00.0150 and 4.00.00.0218
- ❖ Fixed LCD problem for the 9100 and 9500 Nexcom models. Corresponds to individual HF 4.00.00.0201
- ❖ Fixed problem when working with ActiveDirectory. It was affecting the upload of LDAP groups in a particular profile configuration. The console was not showing these groups/users. This fix corresponds to individual HF 4.00.00.0202
- ❖ Solved timeout when accessing certain URLs and specifying the port, using explicit proxy. Corresponds to individual HF 4.00.00.0203
- ❖ Improved synchronization problem when working with two or more appliances. Corresponds to HF 4.00.00.0204
- ❖ Solved several http slowdown problems when the appliance resources where busy (high CPU utilization, anti-spam engine update, etc.). Corresponds to individual HF 4.00.00.0205
- ❖ Fixed a specific slowdown problem (http proxy running at 100%) when navigating by improving the use of shared memory in the appliance. Corresponds to individual HF 4.00.00.0206
- ❖ Amended functionality that was generating some email messages with the same MAILFROM and MAILTO: root@gd.gd.domain to be delivered to mail servers. Corresponds to individual HF 4.00.00.0208
- ❖ Fixed bug that was repeating an address in the top10 spam recipients. Corresponds to individual HF 4.00.00.0209
- ❖ Fixed authentication problem when using capital letters in the credentials. Corresponds to individual HF 4.00.00.0211
- ❖ Fixed network problem to access servers in a different LAN when crossing the Panda GateDefender Performa. Corresponds to individual HF 4.00.00.0212
- ❖ Fixed bug that caused the tagged traffic through a VLAN not to be analyzed. Corresponds to individual HF 4.00.00.0213



- ❖ Fixed navigation problem to access some web pages when the MTU parameter of the Panda GateDefender Performa is changed. Corresponds to individual HF 4.00.00.0214
- ❖ Solved logging problem (http.log) that was generating the CPU to reach 100% and thus slowing down the appliance performance. Corresponds to individual HF 4.00.00.0215
- ❖ Solved unexpected reboots due to ampd process reload. Corresponds to individual HF 4.00.00.0216
- ❖ Improved HTTP traffic management to avoid punctual navigation slowdown problems. Corresponds to individual HF 4.00.00.0217
- ❖ Improved antimalware engine (leaks) and process management (anti-spam and Web filtering modules) Connection delays in SMTP traffic, due to problems in the DNSBL process. Corresponds to individual HF 403, of version 3.02.00.

2.2 Improvements implemented in HotFix Pack 4.00.00.0200

The HF Pack 200 is based on the previous HF Pack (HF Pack100) and in consequence includes all the patches included in this last HotFix Pack.

In addition to this, the following problems are fixed within this HotFix Pack:

- ❖ Connection delays in SMTP traffic, due to problems in the DNSBL process. Corresponds to individual HF 403, of version 3.02.00.
- ❖ Inability to import trusted sites in DOS format. Corresponds to individual HF 407, of version 3.02.00.
- ❖ System reboots when forwarding server is configured. Corresponds to individual HF 4.00.00.0006
- ❖ Fixed alerts pointing to a wrong link in the Status screen. Corresponds to individual HF 4.00.00.0007
- ❖ Fixed some language errors in console:
 - Explicit proxy configuration (Japanese)
 - Wrong link to suggestions mailbox (Japanese and Italian)
 - Wrong link in the Help screen, in the anti-spam configuration (all languages)
 - Wrong link in the Help screen, in the profile list of appliances (all languages)
 - Wrong link in the Help screen, in the profile section, associate configuration to other appliances (all languages)
 - Wrong link in the Help screen, in the tools section, statistics (all languages)
- ❖ Error importing configuration from version 3.02, when client has customized some alert texts. Corresponds to individual HF 4.00.00.0102
- ❖ Random traffic cuts. Corresponds to individual HF 4.00.00.0103
- ❖ Commtouch cache integration check was not working as expected, generating cores and stability problems. Corresponds to individual HF 4.00.00.0106
- ❖ Minor internal fixes.
- ❖ Upgrade of the Commtouch engine to version 7.03.00.0044 to prevent cache corruption.
- ❖ Bug fixes and improvements included in HF Pack100



2.3 Improvements implemented in HotFix Pack 4.00.00.0100

The HFPack 100 is the first hotfix pack associated to version 4.00.00. The following problems are fixed within this HotFix Pack:

- ❖ Fixed problem with internal timeout when dealing with email connections (IMAP). Corresponds to individual HF: 4.00.00.0001
- ❖ Fixed problem when rotating the /var/log files. Corresponds to individual HF: 4.00.00.0002
- ❖ Fixed stats_manager memory leak, creating this process to restarts. Corresponds to individual HF: 4.00.00.0003
- ❖ Fixed ampd (engine process) problems that were creating the reboots in the process and in some cases, of the appliance. Corresponds to individual HF: 4.00.00.0008
- ❖ Included drivers for network card in Sun X2270 (some of the Performa 9100).
- ❖ Included drivers for new Nexcom 9100 and 9500 Performa based appliances.

◀ [Content](#)

Improvements HotFix Packs



3. Hotfix Packs for version 3.02.00 of Panda GateDefender Performa

3.1 Improvements implemented in HotFix Pack 3.02.00.0500

The HFPack 500 is based on the previous HFPack (HFPack400) and in consequence includes all the patches included in this last HotFix Pack.

In addition to this, the following problems are fixed within this HotFix Pack:

- ❖ Resolves the problem in the mail protection that caused connection queuing. Corresponds to the individual hotfixes 3.02.00.0403 and 3.02.00.0408
- ❖ Resolves the blocking of Panda GateDefender Performa when operator characters are included in the text filter. Corresponds to the individual hotfix: 3.02.00.0404
- ❖ Resolves the restart incident due to a conflict in the use of log files. Corresponds to the individual hotfix: 3.02.00.0405
- ❖ Resolves the incompatibility conflict when importing trusted sites in DOS format. Corresponds to the individual hotfix: 3.02.00.0407
- ❖ Correction to the problem that caused restarts when restarting the system. Corresponds to the individual hotfix: 3.02.00.0409

3.2 Improvements implemented in HotFix Pack 3.02.00.0400

The HFPack 400 is based on the previous HFPack (HFPack300) and in consequence includes all the patches included in this last HotFix Pack.

In addition to this, the following problems are fixed within this HotFix Pack:

- ❖ Fixed inability to include domains in the console with over 25 characters. Corresponds to individual HF: 3.02.00.0301
- ❖ High CPU consumption due to a problem in the LDAP daemon, when interacting with external LDAP servers. Corresponds to individual HF: 3.02.00.0302
- ❖ Certain messages were wrongly deleted instead of sent to quarantine, when this option was selected in the console. Corresponds to individual HF: 3.02.00.0304
- ❖ Fixed delay issues when generating anti-spam reports. Corresponds to individual HF: 3.02.00.0305*
- ❖ Fixed instabilities in an internal module, generating unexpected reboots. Corresponds to individual HF 3.02.00.0306*



- ❖ Fixed issue when negotiating at GB speed in the Sun X2100 (Performa 9050/9100). Corresponds to individual HF: 3.02.00.0309
 - ❖ Amended error in Japanese console. Corresponds to individual HF: 3.02.00.0310
 - ❖ Fixed problem integrating Squid with the webfilter module, not working adequately for the selected URLs in the black list. Corresponds to individual HF: 3.02.00.0311
 - ❖ Fixed behavior when dealing with greylisting. Corresponds to individual HF: 3.02.00.0313
 - ❖ Fixed problem with the appliance with an empty IP group is used in a profile. Some internal processes were not working appropriately generating instability in the GateDefender. Corresponds to individual HF: 3.02.00.0314
 - ❖ P2P versions/applications updated (BitTorrent and others). Corresponds to individual HF: 3.02.00.0315
 - ❖ Content Filter module was wrongly detecting some messages as malformed messages. Corresponds to individual HF: 3.02.00.0317
 - ❖ Fixed unacceptable time when loading anti-spam blacklist. Corresponds to individual HF: 3.02.00.0318
 - ❖ Updated web console certificate. The old one has expired and generates a warning when accessing the console and a wrong behavior when accessing the 2nd appliance in a centralized environment
 - ❖ Updated internal library affecting the antimalware engine
- * **IMPORTANT:** This improvement can only be activated by a Panda technician prior request. Should you require it, then, contact your Local Panda Support office to have this fix applied by an expert.



WARNING: Please bear in mind that the application of any HFPack can take up to 10 minutes to get the GateDefender functionalities fully restored. We recommend you schedule carefully the application of the HFPack to minimize the impact in your network.

3.3 Improvements implemented in HotFix Pack 3.02.00.0300

The HFPack 300 is based on the previous HFPack (HFPack200) and in consequence includes all the patches included in this last HotFix Pack.

In addition to this, the following problems are fixed within this HotFix Pack:

- ❖ Fixed problem with quarantine, where the quarantine size shown was not correct. Corresponds to individual HF: 3.02.00.0117
- ❖ Fixed incorrect BATV tagging, when this option was not selected. Corresponds to individual HF: 3.02.00.0204



- ❖ Fixed POP3 problem when downloading mail headers. Corresponds to individual HF: 3.02.00.0205 and HF 3.02.00.0211
- ❖ Fixed generic problems associated to the improper restoration of corrupted databases. Corresponds to individual HF: 3.02.00.0207
- ❖ Fixed problem with the file name when restoring the file from quarantine. Corresponds to individual HF: 3.02.00.0208
- ❖ Fixed problem to allow excluding port range in the P2P/IM protection. Corresponds to individual HF: 3.02.00.0212
- ❖ Fixed error in console with the " ` " character in the Content Filtering page that was causing the console to freeze. Corresponds to individual HF: 3.02.00.0213
- ❖ Fixed web filtering programming bugs. Corresponds to individual HF: 3.02.00.0214 and 218
- ❖ Fixed problem that generated cores from the protocol processor module. Corresponds to individual HF: 3.02.00.0216
- ❖ Fixed problem associated to the connection shut down. The control connection was improperly closed aborting the file sending. Corresponds to individual HF: 3.02.00.0217
- ❖ Solved traffic slowdown problem when the proxy module was taking too many resources. Corresponds to individual HF: 3.02.00.0219

3.4 Improvements implemented in HotFix Pack 3.02.00.0200

The HFPack 200 is based on the previous HFPack (HFPack 100) and in consequence, it includes all the patches incorporated in this last HotFix Pack.

In addition to this, the following problems are fixed within this HotFix Pack:

- ❖ Fixed problem with anti-malware engine when analyzing executable files and thus producing errors in this module and lead to general slowdown. Corresponds to individual HF: 3.02.00.0101
- ❖ Fixed duplicated IP address warning message. Corresponds to individual HF: 3.02.00.0104
- ❖ Fixed web console problem (HTTP 500 message) when modifying the advanced internal configuration. Corresponds to individual HF: 3.02.00.0109
- ❖ Fixed problem with certain cab files that were wrongly classified as ZipOfDeath. Corresponds to individual HF: 3.02.00.0112
- ❖ Fixed problem when reading the serial number of the Sun boxes due to ILOM bug, and thus the appliance was blocked. Corresponds to individual HF: 3.02.00.0115

In addition to this, the HotFix Pack also includes the following changes:

- ❖ New Sun hardware support (X4170 and X2270)
- ❖ New Silicom bypass cards support (included as well as HF 108)



3.5 Improvements implemented in HotFix Pack 3.02.00.0100

- ❖ Corrected an omission in malware, spam and content filter reports, including a new field that displays the source IP of the communication.
- ❖ Modification to the DNS server configured by default in the appliance, to ensure that the IP reputation system for spam detection does not display an error message related with the inability to resolve names.
- ❖ Corrected the problem that caused users excluded from the IM/P2P and Web filter protection to be deleted. Configuration of activation intervals for each of the protections was lost. Corresponds to HF3.02.00.0024.
- ❖ A correction has been made to include support for the X-ANONYMOUSLY command (in Exchange 2007). This corresponds to HF 3.01.01.0103.
- ❖ Corrected a problem with the POP3 interception module affecting consecutive RETR commands. This corresponds to HF 3.01.01.0104.
- ❖ Corrected an error with a specific strain of malware, causing it to be detected as ZipOfDeath and provoking an error in access to the Web Console. This corresponds to HF 3.01.01.0105.
- ❖ Updated the appliance arping version, used to discover if the appliance IPs are being used by other computers. This corresponds to HF 3.01.01.0108.
- ❖ Corrected timeout problems in mail connections (SMTP, POP3, IMAP) intercepted by the appliance when using TLS. This corresponds to HF 3.02.00.0001.
- ❖ Corrected spam flagging problem. Those associated to a profile were not flagged. This corresponds to HF 3.02.00.0002.
- ❖ Corrected the performance problem with HTTP when an application made HTTP POSTs with chunks. This corresponds to HF 3.02.00.0003.
- ❖ Update of IM/P2P rules for Limewire version 5.1.2, Skype 4.0.0.226, and MSM Messenger 14.x. This corresponds to HF 3.02.00.0004.
- ❖ Corrected the translation of a string in German in the console. Corresponds to 3.02.00.0005.
- ❖ Corrected the problem that included the X-Header in email messages belonging to the anti-spam white list. Corresponds to 3.02.00.0006.
- ❖ Corrected the problem generated on applying the upgrade to 3.02.00 when the configuration of the protocol timers of the previous version had been modified (advanced settings). Corresponds to 3.02.00.0007.
- ❖ Corrected the problem in the console that prevented the static paths configured from being deleted, when more than one was configured. Corresponds to 3.02.00.0008.
- ❖ Corrected the timeout problem when consulting DNSBLs. Corresponds to 3.02.00.0009.
- ❖ Corrected the problem in the console when configuring additional ports, when clients only have the Web filter license contracted. Corresponds to 3.02.00.0012.
- ❖ Corrected problems detected on accessing certain Panda MIB values. Corresponds to 3.02.00.0013.
- ❖ Corrected the report filter problem in the content-filter, affecting the "source" field. Corresponds to 3.02.00.0014.
- ❖ Corrected the problem when exporting certain items from the appliance Web console. Corresponds to 3.02.00.0015.

◀ [Content](#)