Panda GateDefender Performa
v3.01.01

Document of changes

Contents

1. New features of the version

Below are the modifications made since version 3.00.00 of Panda GateDefender Performa. These modifications include those made in version 3.01.00 and 3.01.01

1.1 Centralized settings

1.1.1 General description

In previous versions of Panda GateDefender Performa, the only way of replicating configurations to another appliance was to export the configuration from the original appliance and import it to the other one. It was also the necessary to reconfigure the network settings of the appliance.

To aid this task, a centralized protection configuration function has been added, through which it is possible to replicate protection settings from one appliance to another.

The following protection settings can be replicated:
Main settings (the protection settings applied by default)
Protection profiles.

This new function has been included in the Tools section of the console:

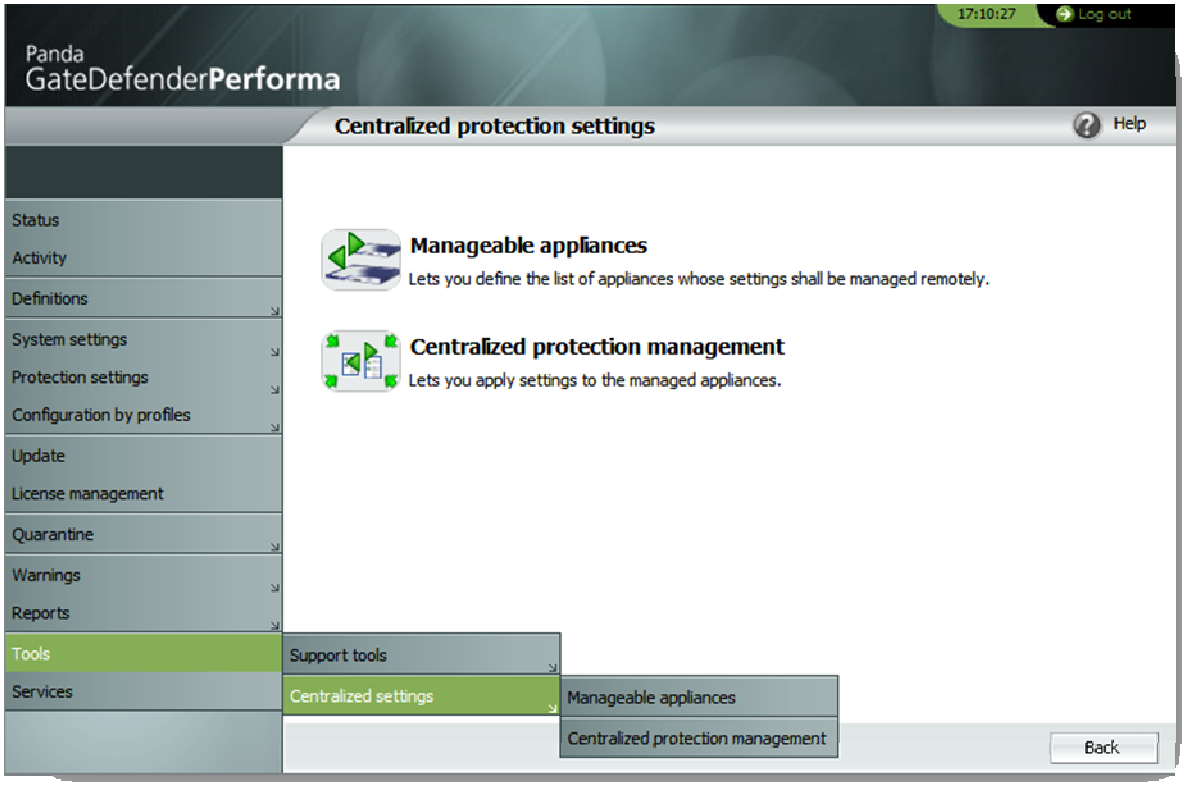

Figure 1. Centralized settings:

The new function is divided into two parts:
Manageable appliances: From here you can enter the details of the appliances and groups of appliances to manage.

Centralized protection management: From here you can apply the settings and profiles to the appliances and groups of appliances.

1.2 User names for accessing the Web console.

1.2.1 General description

In previous versions of Panda GateDefender Performa there was only one user name for accessing the Web console. However, it is common in corporate environments that several users need to access the console. In addition, several of these users may only need to monitor the status of the appliance, without having to make any modifications to the configuration of the appliance.

To meet this requirement, from version 3.01.00 it will be possible to define more than one user profile for the console and establish different user permissions.

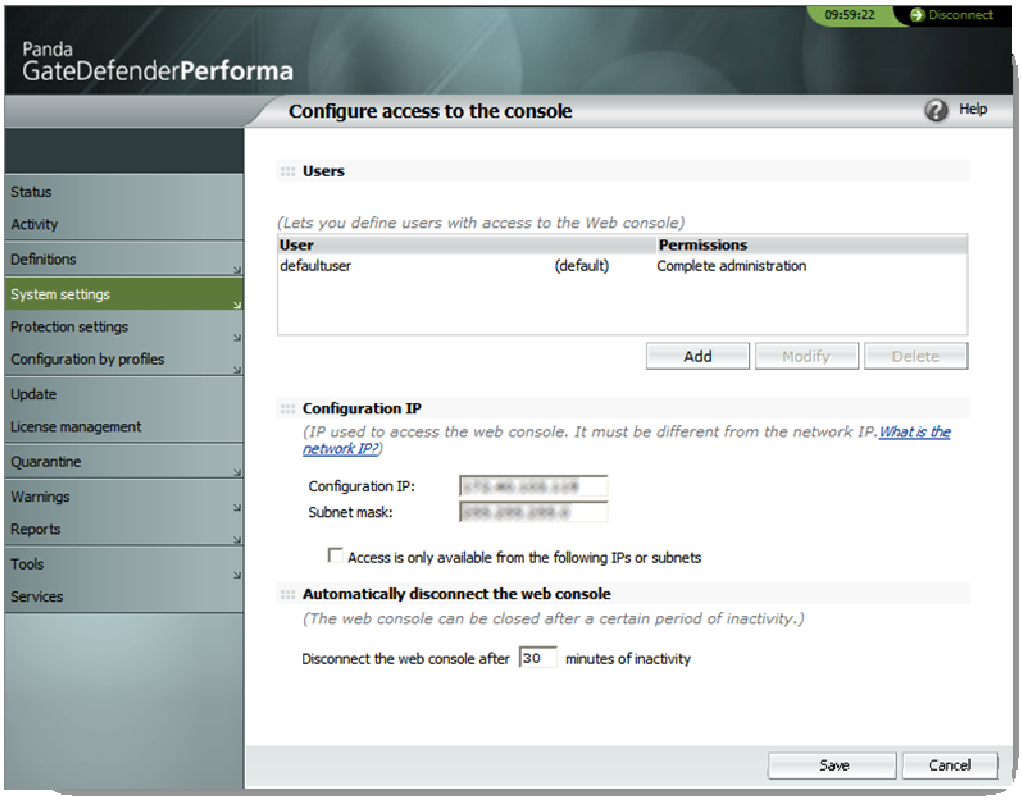

Figure 2. Web console access

The Web console allows four types of permissions to be given to a specific user:

Monitoring
Protection settings
System settings
Complete administration

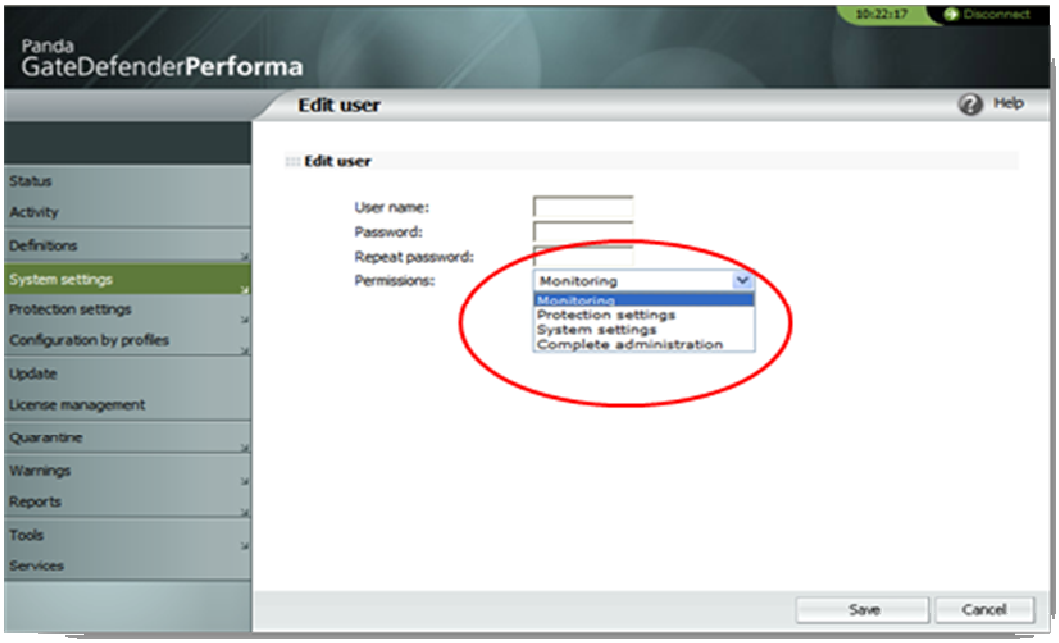

Figure 3. Console access permissions

1.3 Logging of URLs visited in the Web filter

1.3.1 General description

Up until version 3.00.10 of Panda GateDefender Performa, the Web filter module would only record access attempts to Web pages that had been blocked (those belonging to a restricted category). It was not possible to record all Web access.

Since version 3.01.00, this is now possible, so administrators have the possibility to enable the logging of all Web access, including restricted and permitted URLs. This activity can be logged in the event database and the remote Syslog.

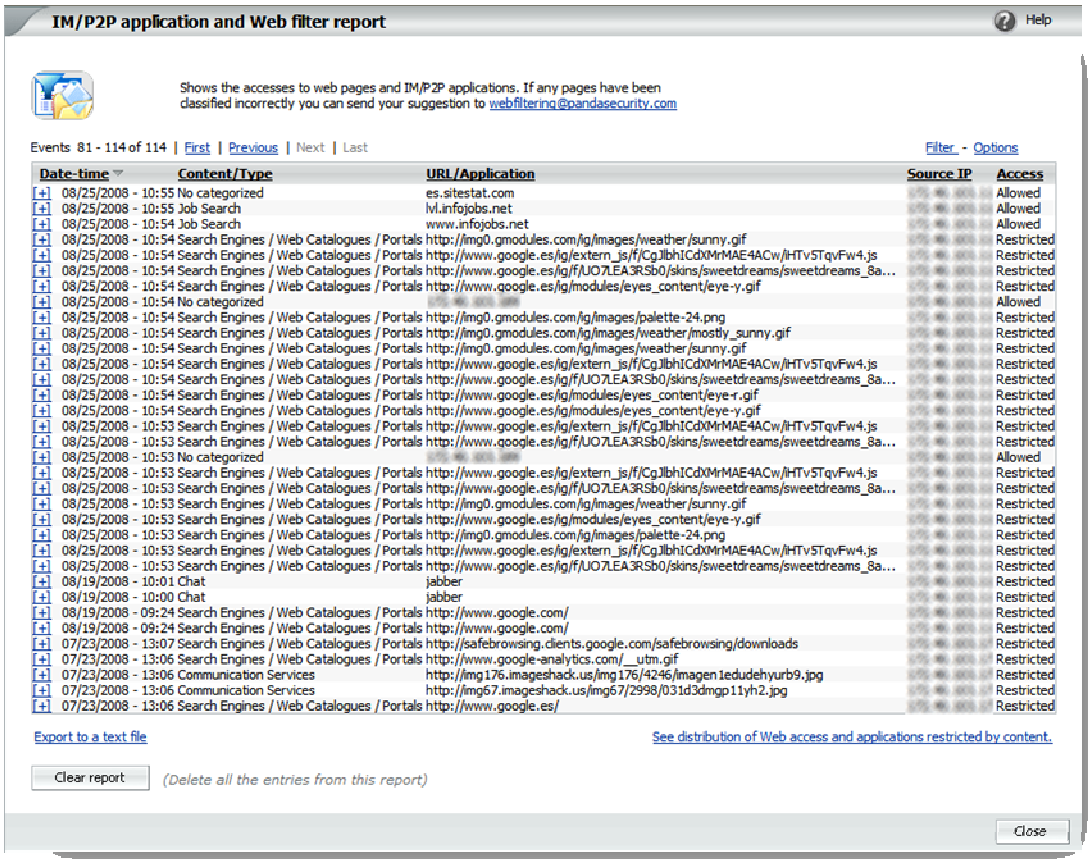

Figure 4. Logging of URLs visited and restricted

In addition, there are two new graphs in the Activity Details page of the Web filter module: a TOP10 of the most visited domains and a TOP10 on the users that most use the Internet.

Figure 5. Activity details of the Web filter

1.4 Web filtering with unrestricted periods

1.4.1 General description

Until now, when Web filtering was enabled for a certain category, access to all URLs catalogued in this category was prevented for the time during which this filter was configured.

Since version 3.01.00, unrestricted periods have been implemented so that it is possible to include times when URLs in a blocked category can be accessed freely.

These periods can be configured by the hour and for each day of the week, so each day can have different unrestricted periods.

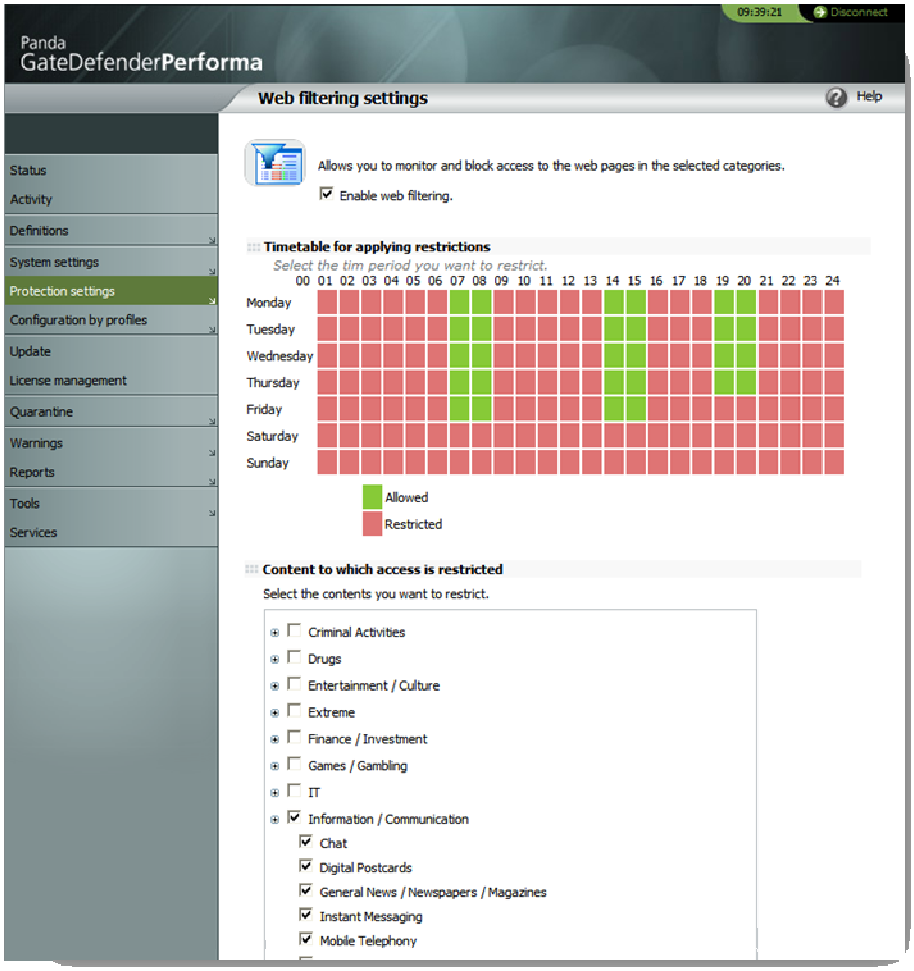

Figure 6. Web browsing periods

1.5 P2P/IM filtering with unrestricted periods

1.5.1 General description

This function is analogous to the one described in the previous section, in this case affecting the P2P/IM application filter.

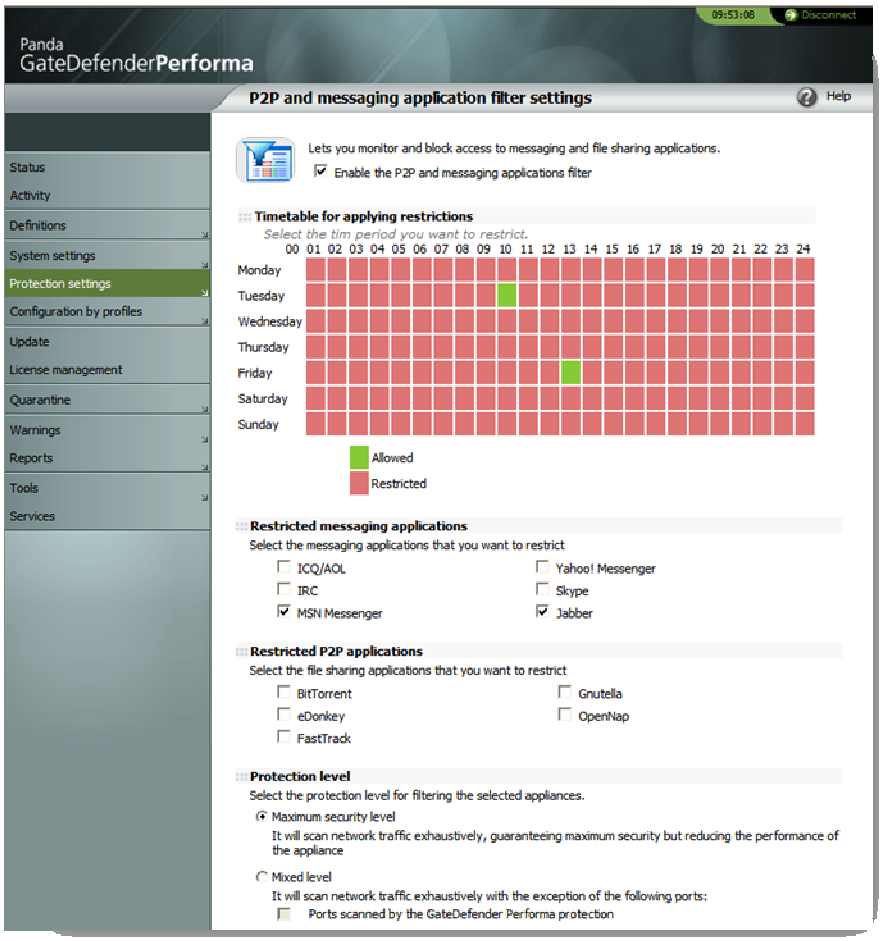

Figure 7. P2P/IM application filtering restrictions

1.6 Incremental updating of the pav.sig

1.6.1 General description

To reduce the data downloaded by the appliance during the signature file update, version 3.01 implements a feature to download the pav.sig file incrementally. This way, instead of downloading the whole file, only the binary patch for the current pav.sig is downloaded.

The pav.sig used in Performa versions is:

Versions < v3.00.00: Pav.sig (without incremental support)
v3.01.00 > Versions >= v3.00.00: Megapav.sig (without incremental support)
Versions >= v3.01.00: Pav.sig (with incremental support)

1.7 Local updates

1.7.1 General description

This feature's name really refers to a completely local operation of the appliance (without Internet connection), which doesn't only affect the updates. The local updates feature allows updates of malware signature files (pav.sig) from a local server, so updates can be made without an Internet connection.

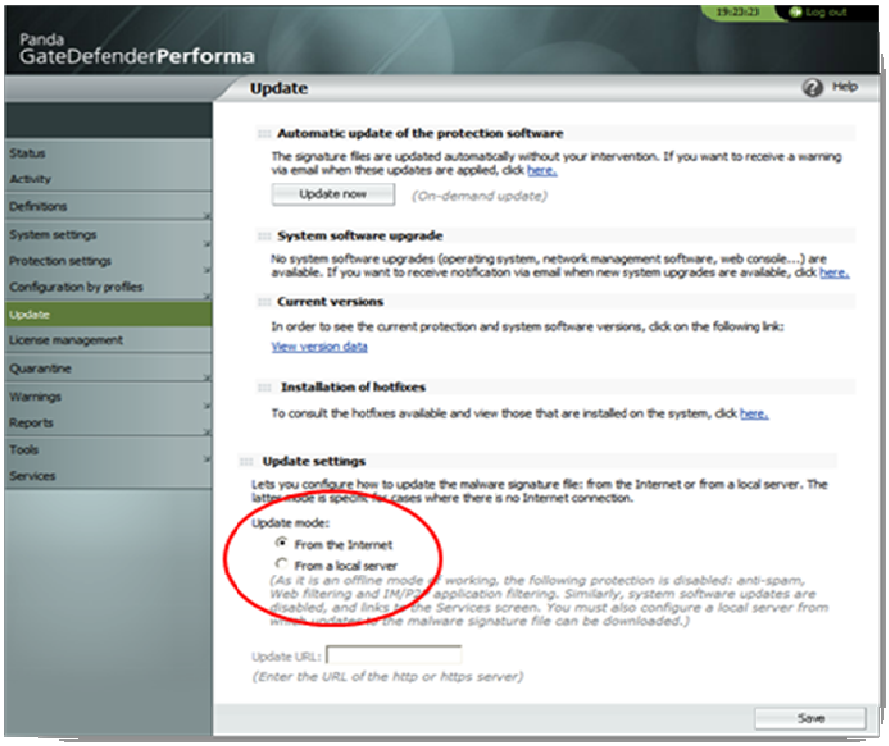

Figure 8. Local updates

1.8 Updating the Cloudmark engine

1.8.1 General description

Due to a change in the Cloudmark licensing model, the anti-spam engine cartridge version has been changed. A series of errors affecting the old engine have also been corrected.

There are two types of updates in Cloudmark:

Microupdates, every 3 hours.

Continuous updates (approximately every minute), called delta microupdates.

If an error occurs in the microupdates, there is a restriction on event generation so there is only one every 24 hours.

1.9 Update of the Cobion engine and WebLearn

1.9.1 General description

Due to the release of the new Cobion v3.0.5.8 engine, it has been updated as a consequence of the improvements it presents regarding previous versions.

Improvements include:

- Improvements to database management: reduced size by about 50%, reduced CPU and memory use during updates, up to 80 million URLs categorized.
- Detection and categorization of embedded URLs.
- Return codes added during update of the database to improve management of any errors.
- NPTL threading support.
- Random delays on downloading an update of the database to prevent saturation of Cobion servers.

The WebLearn feature has also been enabled. This allows storage of all URLs not catalogued in the Cobion database so they can be sent later via HTTPS to Cobion servers.

In the Web filter page there is a new section for enabling/disabling the WebLearn feature. As this is common to all profiles, it should not be displayed in the Web filter profile configuration screen. It is enabled by default.

This section looks as follows:

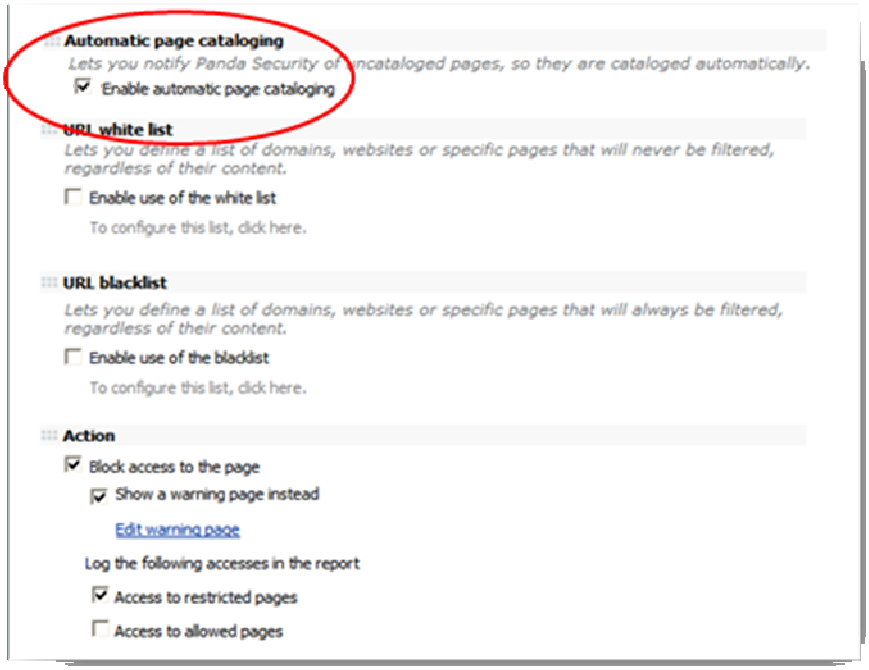

Figure 9. New console section for WebLearn

1.10 Sending statistics

1.10.1 General description

At present there is a hotfix that sends information about the malware detected to PandaLabs via email. The information has been completely overhauled to implement much more data, not only malware-related, but also data about the appliance's current status. The way in which the information is sent has also changed; it is now done through an XML sent by POST to an HTTP server instead of through email.

1.10.2 Data sent to Panda

The data sent to Panda is shown in the following table:

GENERAL DETAILS
Version of the statistics file
Unique appliance identifier (serial number)
Date on which the statistics file was sent
GateDefender type
Information about cores (number of cores in the last 24 hours)

Versions
Version of the system software (e.g. 3.01.01)
Kernel engine
Signature file date
Anti-spam version: engine and signatures
URL-filter engine
IPS: engine and signatures
Technology status
Anti-malware protection: Viruses: Active HTTP active FTP active SMTP active POP3 active IMAP active NNTP active Action Heuristic: Active Sensitivity Action Phishing: Active Scan inbound mail Scan outbound mail Action on Inbound mail Action on Outbound mail Spyware: Active Jokes: Active Dialers: Active Other risks: Action
Anti-spam protection: Active Inbound SMTP active Inbound POP3 active Inbound IMAP active Outbound SMTP active Outbound IMAP active Sensitivity Action on spam Action on probable spam
Content-filter protection: HTTP active

FTP active Inbound SMTP active Inbound POP3 active Inbound IMAP active Outbound SMTP active Outbound IMAP active Inbound NNTP active Outbound NNTP active
URL-filter protection: Active Action
IM & P2P protection: Level Active For each protocol: List of protocol identifier and status (active or not)
Trusted sites and domains Active
DETECTION DETAILS
Anti-malware
Protection on which the detection has been made
Technology with which the detection has been made
Protection enabled during the sending
List of detection Id and frequency

Table 1. Fields sent in the statistics file

1.11 Load-balancing in manual mode

1.11.1 General description

A new load-balancing system mode has been added since version 3.01.00, to allow load-balancing in network environments with other devices in which STP is active. The new manual operational mode involves the administrator entering manually a list with the IPs of all the computers that make up the cluster. This additional information provided by the administrator makes it possible for complete independence between the GateDefender load-balancing system and STP protocol in manual mode.

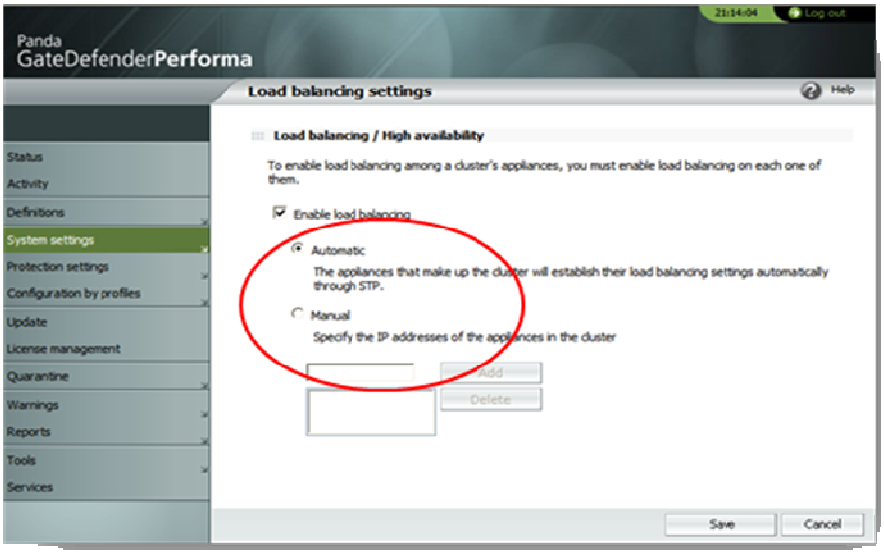

Figure 10. Selection of load-balancing mode

It is important to remember that with the manual operational mode, there is no longer the concept of Master and Slave; all appliances cooperate between themselves, functioning as slaves of the others. The appliance which actually carries out the functions of the master will simply be the one through which the traffic is flowing, which will depend on the network topology established by the administrator, bearing in mind that for the purposes of the STP protocol, GateDefender is just another device.

1.12 Advanced bridge configuration

1.12.1 General description

Since version 3.01.00 a series of bridge configuration parameters have been introduced which can be modified by the administrator from the advanced settings screen of the Web console. The parameters available and the accepted ranges are as follows:

Parameter	*Range*
Bridge priority	0 -> 65535
Bridge forward delay	0 -> 1000000
Bridge hello time	0 -> 1000000
Maximum message age	0 -> 1000000
Ethernet address ageing time	0 -> 1000000
Bridge cost (eth0)	-1000000 -> 1000000
Bridge cost (eth1)	-1000000 -> 1000000

Table 2. Advanced bridge configuration parameters

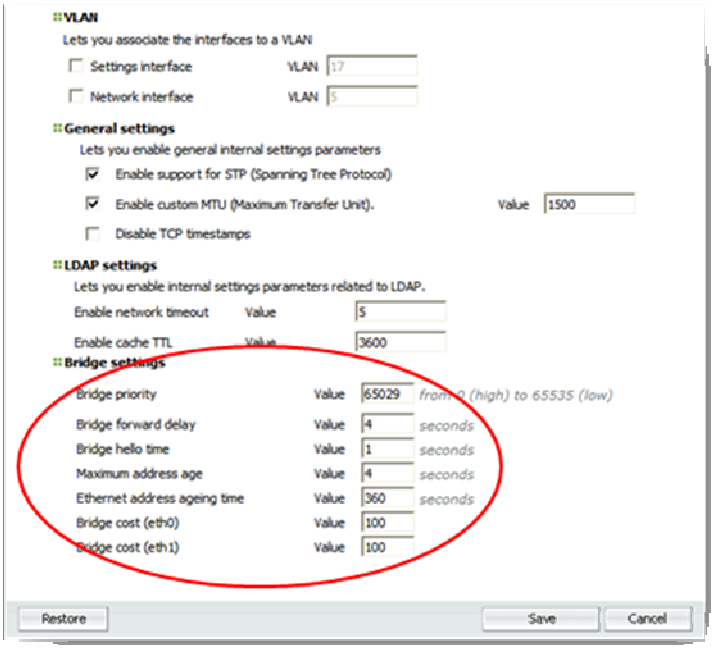

Figure 11. Configuration screen for bridge parameters

1.13 Enabling/disabling of mail vulnerability checks

1.13.1 General description

Vulnerability checks in mails that use Asian characters (e.g. Kanji) can sometimes generate false positives. Consequently, the possibility of enabling or disabling the checks has been implemented through a command that can be accessed by Tech Support from the command console.

These checks are enabled by default.

1.14 Sending of malware vulnerabilities to quarantine

1.14.1 General description

A command has been implemented in the console, which allows Tech Support staff to enable or disable the sending of catalogued items such as vulnerabilities to quarantine. It is disabled by default.

2. Bugs corrected

- Updates to Cloudmark anti-spam rules were not applied in appliances that used certain proxy servers with authentication.
- Some global configuration values were not maintained when updating the software.
- In P2P/IM filtering, Windows Live Messenger 8.1 was not blocked.
- An empty list of hotfixes could cause instability in the appliance.
- Translation errors in Italian.
- Sometimes the console did not return to the previous page when the user clicked Save.
- Some files detected by the anti-malware engine had incorrect names in the console reports and the syslog traces.
- Diagnosis tools: Connectivity with the server for sending items from malware quarantine was checked regardless of whether there was an anti-malware license or not.
- Some internal software components could cause sporadic stability problems.
- The MD5 identifier of quarantined files was not viewed correctly in the console.
- Under certain circumstances, changes to the LDAP server settings screen were not saved.
- In Internet Explorer 7, the content filter settings screen was not displayed correctly.
- Files that could not be scanned were deleted even if the configuration stipulated they should be sent to quarantine.
- The software module restart warning was not sent by email, syslog or SNMP, even though it was displayed in the console reports.
- Warnings of proxy connection errors when not removed once the connection was reestablished.
- When the space allocated for quarantine approached the limit, multiple warnings were sent.
- Some console fields were not correctly aligned.
- Videos with the extension .mov downloaded from QuickTime were blocked when the Content Filter protection was enabled.
- Malware and Spam quarantine events were only sent via syslog when sending of the other events (i.e. Spam or Malware respectively) were also enabled.
- Syslog: The quarantine emptied event was not sent.
- Syslog: The event for connection failure with Panda server for the sending of suspicious items was not sent.
- If the license key was entered in lowercase letters, the anti-malware signature file was not updated.
- Importing of the anti-spam settings from previous versions did not save certain values.
- When the anti-spam license expiry warning was sent via e-mail, it was incorrectly sent as an anti-malware type warning.
- Incorrect spacing in some console texts.
- Slowdown problems on generating internal logs when HTTP errors were detected.
- Slowdown problems when the quarantine manager deleted old items.
- Specific Web pages served by Oracle Application Server were not accessible.
- Performa's internal code contained specific vulnerabilities that could be exploited by third-parties.
- The activation status of certain protocols in the console was incoherent.
- On importing the 3.00.05 settings, the following error occurred: "The specified file contains the configuration of a non-supported version. Unsupported config version 30005, last supported 4".

- Sporadic Internet interruptions caused by the temporary blocking of some system processes.
- Windows Live Messenger v8.1.x was not detected with filtering of P2P and IM applications at maximum security level.
- Windows Live Messenger v8.5.x was not detected with filtering of P2P and IM applications at maximum security level.
- Yahoo Messenger v7 was not detected with filtering of P2P and IM applications at maximum security level.
- LDAP queries consumed many system resources when there was a lot of spam traffic.
- Interaction with mail servers that send messages in a single session (e.g. Ironport) sometimes mixed message recipients.
- Sporadic Internet interruptions when spam detection events were generated in emails.
- Sporadic Internet interruptions with P2P/IM protection in maximum performance mode.
- The content filtering contextual scan was not done correctly if it was defined for a profile other than the default one, when the anti-phishing scan was active.
- On Sun appliances (GD Performa 9xxx), Watchdog did not work correctly and therefore the system was not automatically restarted during system crashes.
- POP3 protocol scans caused occasional system restarts due to cumulative memory consumption.
- Performa 9500: The activation of the network bypass once the services had been restarted caused network protection loss (10 minutes).

3. ANNEX I. Integration with Sun hardware

The new 9000 series of Performa is based on Sun hardware, which offers a series of advantages with respect to the architecture of Portwell in the previous 8000 series:

- Greater performance and scalability, providing service to more users.
- Supports third-party cards, such as network cards with support for bypass.
- Greater fault tolerance, as some models can include redundant power sources and RAID disks.
- Allows complete monitoring of all hardware, through ILOM.
- The appliances can also be managed remotely via ILOM.

The different server models are as follows:

Figure 12. Sun Fire X2100 M2

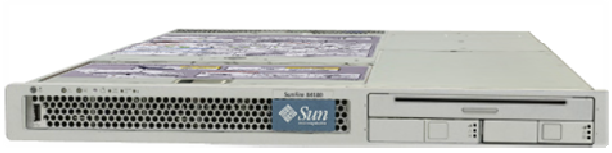

Figure 13. Sun Fire X4100 M2

Figure 14. Sun Fire X4150 M2

The following table gives a description of all the different models in the series and of their target market:

Target market	Small business	Medium business	Big companies	Big corporations and enterprises
Maximum recommended users	0-100	0-500	0 - 1200	0-2500
Product familly	GateDefender			
Product line	Performa	Performa	Performa	Performa
Model	GateDefender Performa 9050	GateDefender Performa 9100	GateDefender Performa 9200	GateDefender Performa 9500
HW features				
Vendor	Sun MicroSystems	Sun MicroSystems	Sun MicroSystems	Sun MicroSystems
Vendor model	X2100 M2	X2100 M2	X4150 M2	X4100 M2
CPU	1 x AMD Opteron Dual Core (2,8 GHz)	1 x AMD Opteron Dual Core 1220 (3 GHz)	1x Intel Xeon Quad Core (2,33 Ghz)	2x Dual-Core AMD Opteron 2220 (2.8GHz)
RAM	2 GB (2 x 1GB) DIMM DDR2 667	4 GB (4 X 1GB) DIMM DDR2 667	4 GB (4 X 1GB) DIMM DDR2 667	8 Gb (4x2Gb) DIMM DDR2 667
HD	1x 250 GB / 7200 rpm / SATA II	1x 250 GB / 7200 rpm / SATA II	1x 73 GB / 10000 rpm / SAS	2x 146 GB 10K RPM 2.5" SAS HDD (RAID 1)
NETWORK	2 x 10/100/1000	2 x 10/100/1000	2 x 10/100/1000	2 x 10/100/1000
USB	6	6	6	6
Serial port	Yes	Yes	Yes	Yes
Power supplies	1	1	2	2
Console	Yes	Yes	Yes	Yes
Bypass	No	No	No	Yes (Silicom card)
Optical drive	DVD	DVD	DVD	DVD
Height	1 U	1 U	1 U	1 U

Table 3. Performa 9000 series

4. ANNEX II. Centralized monitoring with Cacti

Through the integration of Performa version 3.01.00 and later versions with the Cacti monitoring tool, it is possible to centralize the management of the status of different appliances simultaneously with a single Web interface. Among other things, it is now possible:

- To display detailed graphs on use of memory, CPU, system load, etc.
- Generate aggregate graphs with information about different appliances or protocols.
- Use predefined templates to display activity of all different protection systems (anti-malware, anti-spam, web filter, content filter).
- Display graphics with information about traffic in different network interfaces in each appliance as well as simultaneous connections.
- Display information about the different sensors associated with each of the hardware elements of the Sun appliances (voltage, temperature, ventilators, etc.)
- Display temporary graphs of the different system event levels.
- Use existing plug-ins to display more information (e.g. syslog server).
- Create new plug-ins to extend the monitored information in the future.

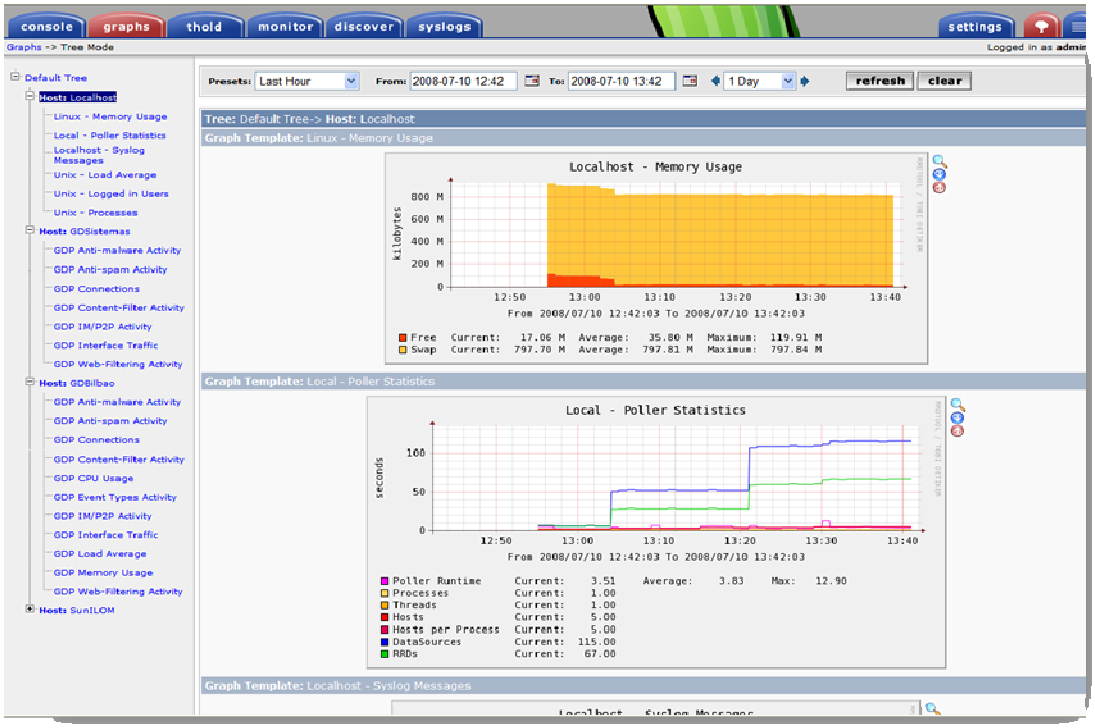

Figure 15. Centralized monitoring with Cacti