

# Parallels<sup>®</sup> Plesk Panel

---

## **Parallels Plesk Panel 9.5 for Linux/Unix**

Advanced Administration Guide

# Copyright Notice

*ISBN: N/A*

*Parallels*

*660 SW 39<sup>th</sup> Street*

*Suite 205*

*Renton, Washington 98057*

*USA*

*Phone: +1 (425) 282 6400*

*Fax: +1 (425) 282 6444*

*© Copyright 1999-2010,*

*Parallels, Inc.*

*All rights reserved*

*Distribution of this work or derivative of this work in any form is prohibited unless prior written permission is obtained from the copyright holder.*

*Patented technology protected by U.S. Patents 7,328,225; 7,325,017; 7,293,033; 7,099,948; 7,076,633.*

*Patents pending in the U.S.*

*Product and service names mentioned herein are the trademarks of their respective owners.*

# Contents

<b>Preface</b>	<b>6</b>
Typographical Conventions .....	6
Feedback .....	7
<b>Administering Security Settings</b>	<b>8</b>
Configuring Firewall .....	9
Configuring SELinux Policy for Your Parallels Plesk Panel Server .....	10
Securing the /tmp Partition .....	11
<b>Achieving Compliance with Payment Card Industry Data Security Standard</b>	<b>12</b>
<b>Using Event Tracking Mechanism</b>	<b>18</b>
Adding Event Handlers .....	19
Removing Event Handlers .....	20
Event Parameters Passed by Event Handlers .....	21
Session (Login) Settings Event .....	23
Desktop Preset Event .....	23
Client Account Event .....	24
Client Status Event .....	24
Disk Space Limit Event for Client .....	25
Traffic Usage Limit Event for Client .....	25
Client Limits Event .....	25
Client Permissions Event .....	26
Client Preferences Event .....	29
Client's GUID Event .....	29
Clients Template Event .....	30
Client's IP Pool Event .....	30
Client's Site Application Package Event .....	30
Domain Event .....	31
Domain Limits Event .....	31
Domain Status Event .....	32
Domain's GUID Event .....	32
Domains Template Event .....	33
DNS Zone Event for Domain .....	33
Disk Space Limit Event for Domain .....	33
Traffic Usage Limit Event for Domain .....	33
Domain Owner Change Event .....	34
Subdomain Event .....	34
Domain Alias Event .....	35
Domain Alias, DNS Zone Event .....	35
Physical Hosting Event .....	36
Mail Account Event .....	38
Web User Event .....	39
Mailing List Event .....	39
Parallels Plesk Panel User Event .....	40
Domain Administrator Account Event .....	40
Domain Administrator's Permissions Event .....	41

Site Application Event .....	43
Service Event .....	44
IP Address Event .....	44
Forwarding Event .....	45
Administrator Information Event.....	45
Database Server Event.....	46
Parallels Plesk Panel Component Event .....	46
Database Event.....	46
Database User Account Event.....	47
License Key Event .....	47
Reseller Account Event.....	47
Reseller Status Event.....	48
Disk Space Limit Event for Reseller .....	48
Traffic Usage Limit Event for Reseller .....	49
Reseller Limits Event .....	49
Reseller Permissions Event .....	50
Reseller Preferences Event .....	53
Reseller's GUID Event .....	53
Resellers Template Event .....	54
Reseller's IP Pool Event.....	54
Reseller's Site Application Package Event .....	54

---

## **Configuring Apache Server** **55**

Getting Familiar with Virtual Host Structure and Permissions .....	56
Enabling Piped Logs for Web Server to Reduce the Risk of Web Service Disruption.....	58
Recompiling Apache With More File Descriptors .....	59
Recompiling Apache With More File Descriptors on RedHat-like System.....	60
Recompiling Apache With More File Descriptors on Debian System .....	62
Recompiling Apache With More File Descriptors on FreeBSD System.....	63
Including Directives into Web Server Configuration File .....	65
Customizing httpd.include for Domains.....	66
Preventing Graphics Hotlinking on a Web Site .....	66
Apache Port Change .....	67
Example of Web Server Configuration File.....	69
Example of Domain Configuration File .....	70
Example of Subdomain Configuration File.....	72
Example of Webmail Configuration File .....	74
Example of Mailman Configuration File .....	75
Configuring Sitebuilder for Work With Changed Apache Port .....	76

---

## **Changing Tomcat Java Connector Ports** **78**

---

## **Configuring Mail** **79**

Configuring a Mailing List Where Only Members are Allowed to Post to.....	80
Importing a List of E-mail Addresses into a Mailing List.....	80
Limiting the Number of Recipients of a Mail Message .....	81
Training SpamAssassin for All Mail Accounts on the Server .....	82
Limiting the Maximum Number of Child Processes for spamd .....	83
Fighting Against Spam on Qmail Mail Server .....	84
Restoring Mail Configuration .....	86
Installing Custom SSL Certificates for Qmail or Courier-IMAP Mail Servers .....	87
Installing SSL Certificate for Qmail .....	88
Installing SSL Certificates for Courier-IMAP Mail Server.....	90

<b>Installing Adobe ColdFusion</b>	<b>91</b>
------------------------------------	-----------

---

<b>Using Open Relay Option for Your Mail Server</b>	<b>94</b>
---	-----------

---

<b>Configuring APS Applications Catalog</b>	<b>95</b>
---	-----------

---

<b>Checking Free Disk Space Before Starting the Backup Process</b>	<b>97</b>
--	-----------

---

# Preface

## In this section:

Typographical Conventions .....	6
Feedback .....	7

---

## Typographical Conventions

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
<b>Special Bold</b>	Items you must select, such as menu options, command buttons, or items in a list.	Go to the <b>QoS</b> tab.
	Titles of chapters, sections, and subsections.	Read the <b>Basic Administration</b> chapter.
<i>Italics</i>	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	The system supports the so called <i>wildcard character</i> search.
Monospace	The names of style sheet selectors, files and directories, and CSS fragments.	The license file is called <code>license.key</code> .

<b>Preformatted Bold</b>	What you type, contrasted with on-screen computer output.	Unix/Linux: <b># cd /root/rpms/php</b> Windows: <b>&gt;cd %myfolder%</b>
Preformatted	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	Unix/Linux: <b># ls -al /files</b> total 14470 Windows: <b>&gt;ping localhost</b> Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

---

## Feedback

If you have found an error in this guide, or if you have suggestions or ideas on how to improve this guide, please send your feedback using the online form at <http://www.parallels.com/en/support/usersdoc/>. Please include in your report the guide's title, chapter and section titles, and the fragment of text in which you have found an error.

# Administering Security Settings

## In this chapter:

Configuring Firewall.....	9
Configuring SELinux Policy for Your Parallels Plesk Panel Server .....	10
Securing the /tmp Partition .....	11

---

# Configuring Firewall

Make sure these ports are opened for all Parallels Plesk Panel services to work with a firewall:

- 20 for ftp-data;
- 21 for ftp;
- 22 for ssh;
- 25 for smtp;
- 53 for dns (TCP and UDP);
- 80 for http (web server and Parallels Plesk Panel updater);
- 106 for poppassd (for localhost only);
- 110 for pop3;
- 113 for auth;
- 143 for imap;
- 443 for https;
- 465 for smtps;
- 587 for mail message submission;
- 990 for ftps;
- 993 for imaps;
- 995 for pop3s;
- 3306 for mysql;
- 5224 for (outgoing connections only) plesk-license-update;
- 5432 for postgres;
- 8443 for plesk-https;
- 8880 for plesk-http;
- 9080 for tomcat;
- 5224 for license updates.

# Configuring SELinux Policy for Your Parallels Plesk Panel Server

To configure SELinux you need to know the rules that should be added into the system policy. SELinux reports all denied messages into the `/var/log/audit/audit.log` file and these messages can be easily converted into the rules using the `/usr/bin/audit2allow` utility.

```
cat /var/log/messages | /usr/bin/audit2allow
```

Also, `/var/log/messages.*` files can be examined for the SELinux deny messages.

## ➤ *To configure SELinux policy:*

1. Add the rules into the appropriate domain file which describes the application.

For example:

```
/etc/selinux/targeted/src/policy/domains/program/apache.te
allow httpd_sys_script_t var_t:file { execute getattr };
allow httpd_t self:tcp_socket connect;
allow httpd_t usr_t:dir write;
allow httpd_t var_log_t:file { append getattr setattr };
allow httpd_sys_script_t devlog_t:sock_file write;
allow httpd_sys_script_t self:unix_dgram_socket { connect create write
};
allow httpd_sys_script_t ld_so_cache_t:file execute;
allow httpd_sys_script_t syslogd_t:unix_dgram_socket sendto;
allow httpd_sys_script_t var_t:dir { add_name remove_name write };
allow httpd_sys_script_t var_t:fifo_file write;
allow httpd_sys_script_t var_t:file { create execute_no_trans link
read unlink write };
/etc/selinux/targeted/src/policy/domains/program/named.te
allow named_t named_zone_t:chr_file read;
allow ndc_t named_zone_t:file { getattr read write };
allow named_t named_zone_t:dir { add_name write read remove_name };
allow named_t named_zone_t:file { create unlink write };
/etc/selinux/targeted/src/policy/domains/program/syslogd.te
allow syslogd_t usr_t:file append;
allow syslogd_t usr_t:file ioctl;
```

2. Perform the following command line to apply changes:

```
make -C /etc/selinux/targeted/src/policy reload
```

---

## Securing the /tmp Partition

It is recommended to create /tmp as separate partition and mount it with the `noexec` and `nosuid` options.

- The `noexec` option disables the executable file attribute within an entire file system, effectively preventing any files within that file system from being executed.
- The `nosuid` option disables the SUID file-attribute within an entire file system. This prevents SUID attacks on, say, the /tmp file system.

➤ **To secure the /tmp partition of your Parallels Plesk Panel server:**

- If /tmp is a separate partition on the server, you only need to edit `/etc/fstab` and add the `noexec` and `nosuid` options for /tmp. Then remount the partition.
- If the /tmp directory resides on the / partition:

a. Create a new partition for /tmp, for example with size 512 MB:

```
# mkdir /filesystems
# dd if=/dev/zero of=/filesystems/tmp_fs seek=512 count=512
bs=1M
# mkfs.ext3 /filesystems/tmp_fs
```

b. Add the string into `/etc/fstab`:

```
/filesystems/tmp_fs /tmp ext3 noexec,nosuid,loop 1 1
```

c. Move current /tmp directory content to another location.

d. Mount new /tmp partition:

```
# mount /tmp
```

e. Move content from old /tmp directory to the new one.

# Achieving Compliance with Payment Card Industry Data Security Standard

To reduce the risk of compromising sensitive data hosted on your server, you might want to implement special security measures that comply with the Payment Card Industry Data Security Standard (PCI DSS). The standard is intended to help organizations protect customer account data. For detailed information about the standard, refer to [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml).

This chapter describes the steps required to achieve PCI compliance on Linux and FreeBSD-based systems.

You first need to run the PCI Compliance Resolver utility available from the Plesk Control Panel installation directory. It will disable weak SSL ciphers and protocols for Web and e-mail servers operated by Plesk Control Panel.

## ➤ *To run the utility:*

1. Log in to the server shell.
2. Issue the following command:

```
/usr/local/psa/admin/bin/pci_compliance_resolver--enable all
```

The following table describes all options supported by the utility.

Option	Description
-- enable all   --disable all	The option “—enable all” switches off weak SSL ciphers and protocols for Web and e-mail servers.  The option “—disable all” reverts all changes made by the utility and restores original configuration files, thereby allowing weak SSL ciphers and protocols for connections to Web and e-mail servers.
-- enable courier   --disable courier	Switches off or switches on weak SSL ciphers and protocols for connections to Courier IMAP mail server.
-- enable apache   --disable apache	Switches off or switches on weak SSL ciphers and protocols for connections to the Apache Web server that serves users’ sites.
-- enable panel   --disable panel	Switches off or switches on weak SSL ciphers and protocols for connections to Parallels Plesk Panel.

Some PCI compliance scanners may require that the medium strength SSL ciphers for access to the Panel be also switched off. For this reason, after you have run the utility, you need to modify a configuration file that was created by it.

1. Open for editing the file

```
/usr/local/psa/admin/conf/cipher.lst.
```

2. Remove all lines from the file.

3. Insert the following line:

```
ADH-AES256-SHA DHE-RSA-AES256-SHA DHE-DSS-AES256-SHA AES256-SHA KRB5-  
DES-CBC3-MD5 KRB5-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA EDH-DSS-DES-CBC3-  
SHA DES-CBC3-SHA ADH-DES-CBC3-SHA DES-CBC3-MD5
```

4. Save the file.

5. Restart the Web server:

- On Linux systems, issue the command `/etc/init.d/sw-cp-server restart`.
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/sw-cp-server restart`.

Now you need to switch off weak SSL ciphers for connections to Qmail or Postfix e-mail server, if you use any of them.

➤ ***If you use Qmail mail server, issue the following commands at the prompt:***

On Linux systems:

```
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/var/qmail/control/tlsserverciphers  
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/var/qmail/control/tlsclientciphers
```

On FreeBSD systems:

```
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/usr/local/psa/qmail/control/tlsserverciphers  
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/usr/local/psa/qmail/control/tlsclientciphers
```

➤ ***If you use Postfix mail server, modify configuration files:***

1. On Linux systems, open for editing the file `/etc/postfix/main.cf`.

2. On FreeBSD systems, open for editing the file

```
/usr/local/etc/postfix/main.cf.
```

3. Add the following lines to the file:

```
smtpd_tls_protocols = SSLv3, TLSv1  
smtpd_tls_ciphers = medium  
smtpd_tls_exclude_ciphers = aNULL  
smtpd_sasl_security_options = no Plaintext
```

4. Save the file.

5. Restart the mail server:

- On Linux systems, issue the command `/etc/init.d/postfix restart`.
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/postfix restart`.

You also need to prohibit access to MySQL database server from external addresses. To do this, in a firewall that protects your Panel-managed server, add or enable a rule that prohibits TCP and UDP connections to the port 3306 from all addresses except 127.0.0.1.

➤ ***To use the firewall that comes with your Parallels Plesk Panel for Linux:***

1. Log in to the Panel as administrator.
2. If you did not install the firewall component, install it:
  - a. Go to **Home > Updates** (in the **Help & Support** group).
  - b. Click the link corresponding to your version of the Panel.
  - c. Locate **Plesk Firewall module**, select the corresponding check box, and click **Install**.
3. Configure the firewall rule that blocks external MySQL connections and switch the firewall on:
  - a. Click the **Settings** link in the navigation pane.
  - b. Click **Manage Firewall Rules**, and then **Edit Firewall Configuration**.
  - c. Click the **MySQL server** link.
  - d. Select the **Deny** option and click **OK**.
  - e. Click **Activate** to apply the configuration, and then click **Activate** again to switch on the firewall.

➤ ***To conceal the version of DNS server from potential attackers, do the following:***

1. Open for editing the DNS server's configuration file `named.conf`. On Linux systems, it is located in `/etc/`, and on FreeBSD systems, in `/etc/namedb/`.
2. Locate the `options {}` section, and add the `version "none"` line there.
3. Restart the `named` service:
  - On Deb package-based systems, issue the command `/etc/init.d/bind9 restart`
  - On RPM package-based systems, issue the command `/etc/init.d/named restart`
  - On FreeBSD systems, issue the command `/etc/rc.d/named restart`

➤ **To conceal the version of the Apache Web server from potential attackers, do the following:**

1. Open for editing the Web server's configuration file.

- On Debian, Ubuntu, and SuSE Linux, it is located at `/etc/apache2/apache2.conf`.
- On other distributions of Linux, it is located at `/etc/httpd/conf/httpd.conf`.
- On FreeBSD, it is located at `/usr/local/etc/apache2/httpd.conf`.

2. Add the following lines:

```
ServerTokens ProductOnly
TraceEnable OFF
```

3. Save the file.

4. Restart the Web server.

- On Deb package-based systems, issue the command `/etc/init.d/apache2 restart`
- On RPM package-based systems, issue the command `/etc/init.d/httpd restart`
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/apache2 restart`

➤ **If you have Single Sign-On v.2.2 components installed, then you need to disable SSL v.2 and weak SSL ciphers for the single sign-on service:**

1. Open for editing the file `/etc/sw-cp-server/applications.d/sso-cpserver.conf`.

2. Locate the two lines `ssl.engine = "enable"`.

3. After each of these lines, add the following:

```
ssl.cipher-list = "ADH-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:ADH-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:AES128-SHA:KRB5-DES-CBC3-MD5:KRB5-DES-CBC3-SHA:ADH-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DES-CBC3-SHA:DES-CBC3-MD5:DHE-DSS-RC4-SHA:KRB5-RC4-MD5:KRB5-RC4-SHA:ADH-RC4-MD5:RC4-SHA:RC4-MD5:RC2-CBC-MD5:RC4-MD5"
ssl.use-sslv2 = "disable"
```

4. Save the file.

5. Restart the service:

- On Linux systems, issue the command `/etc/init.d/sw-cp-server restart`.
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/sw-cp-server restart`.

➤ **To conceal the version of PHP installed on the server:**

1. Create a file with name `php.ini` in the following directory
  - On Linux systems, `/etc/sw-cp-server/`
  - On FreeBSD systems, `/usr/local/etc/sw-cp-server/`
2. Add to this file the line `expose_php = Off`.
3. Save the file.
4. Open for editing the following file:
  - On Linux systems, `/etc/sw-cp-server/applications.d/sso-cpserver.conf`.
  - On FreeBSD systems, `/usr/local/etc/sw-cp-server/applications.d/sso-cpserver.conf`.
5. Locate the following line:
  - On Linux systems, `var.interpreter = "/usr/bin/sw-engine-cgi"`.
  - On a FreeBSD system, `var.interpreter = "/usr/local/bin/sw-engine-cgi"`.
6. Replace it with the following line:
  - On Linux systems, `var.interpreter = "/usr/bin/sw-engine-cgi -c /etc/sw-cp-server/php.ini"`.
  - On a FreeBSD system, `var.interpreter = "/usr/local/bin/sw-engine-cgi -c /usr/local/etc/sw-cp-server/php.ini"`.
7. Save the file.
8. Restart the Web server:
  - On Linux systems, issue the command `/etc/init.d/sw-cp-server restart`.
  - On FreeBSD systems, issue the command `/usr/local/etc/rc.d/sw-cp-server restart`.

To alleviate security risks arising from disclosure of information about files and their properties by Apache Web server, configure the `FileETag` directive in the Web server configuration file.

➤ **To do this:**

1. Open for editing the Web server's configuration file.
  - On Debian, Ubuntu, and SuSE Linux, it is located at `/etc/apache2/apache2.conf`.
  - On other distributions of Linux, it is located at `/etc/httpd/conf/httpd.conf`.
  - On FreeBSD, it is located at `/usr/local/etc/apache2/httpd.conf`.

2. Locate the line `FileETag INode MTime Size` and remove the `INode` keyword from this line.
3. Save the file.
4. Restart the Web server.
  - On Deb package-based systems, issue the command `/etc/init.d/apache2 restart`
  - On RPM package-based systems, issue the command `/etc/init.d/httpd restart`
  - On FreeBSD systems, issue the command `/usr/local/etc/rc.d/apache2 restart`

# Using Event Tracking Mechanism

The Event Manager is designed to help you organize data interchange between Parallels Plesk Panel and external systems. It works the following way: you create a script to be executed upon a certain Parallels Plesk Panel event, and then create an event handler that triggers the event processing. You can assign several handlers to a single event.

---

**Important:** The Parallels Plesk Panel administrator can create the event handlers that will trigger scripts running on the server on behalf of the root user. If you wish to restrict usage of the root account, create an empty file with name `root.event_handler.lock` in the location `/plesk_installation_directory/var/`.

---

## In this chapter:

Adding Event Handlers.....	19
Removing Event Handlers.....	20
Event Parameters Passed by Event Handlers .....	21

## Adding Event Handlers

Let's, for example, create an event handler for the 'client account creation' event. The handler will accept a client name and the client's login from environment variables. For simplicity we will use a shell-script called `test-handler.sh` that looks as follows:

```
#!/bin/bash

echo "-----" >> /tmp/event_handler.log

/bin/date >> /tmp/event_handler.log # information on
the event date and time

/usr/bin/id >> /tmp/event_handler.log # information on
the user, on behalf of which the script was executed (to ensure
control)

echo "client created" >> /tmp/event_handler.log # information on
the created client account

echo "name: ${NEW_CONTACT_NAME}" >> /tmp/event_handler.log #
client's name

echo "login: ${NEW_LOGIN_NAME}" >> /tmp/event_handler.log #
client's login

echo "-----" >> /tmp/event_handler.log
```

This script prints some information to a file so that we could control its execution (we cannot output information to stdout/stderr, as the script is executed in the background mode).

Suppose, that our script is located in the directory `/plesk_installation_directory/bin` (for instance). Let's register it by creating an event handler via Parallels Plesk Panel.

### ➤ **To add an event handler via Parallels Plesk Panel:**

1. Go to **Home > Event Manager**.
2. Click **Add New Event Handler**. The event handler setup page appears.
3. Select the event, you wish to assign a handler to in the **Event** menu.
4. Select the priority for handler execution, or specify a custom value. To do this, select custom in the **Priority** menu and type in the value.

When assigning several handlers to a single event you can specify the handler execution sequence, setting different priorities (higher value corresponds to a higher priority).

5. Select the system user, on behalf of which the handler will be executed (“root” user, for example).
6. In the **Command** input field, specify a command to be executed upon the selected event. In our example it is `/usr/local/psa/bin/test-handler.sh`.
7. Click **OK**.

---

**Note:** In the script, we have specified the variables `$NEW_CONTACT_NAME` and `$NEW_LOGIN_NAME`. During execution of the handler, they will be replaced with name and login of the created client respectively. The entire list of available variables is provided in the following section. You should keep in mind that with the removal operations, the variables of type `$NEW_xxx` are not set. And with creation operations the parameters of type `$OLD_xxx` are not set.

---

Now if you login to your Parallels Plesk Panel and create a new client, specifying the value ‘Some Client’ in the **Contact name** field, and ‘some\_client’ in the field **Login**, the handler will be invoked, and the following records will be added to the `/tmp/event_handler.log`:


```
Fri Mar 16 15:57:25 NOVT 2007
uid=0(root) gid=0(root) groups=0(root)
client created
name: Some client
login: some_client
```

The parameter templates that can be used when setting up an event handler are presented in the Event Parameters Passed by Event Handlers (see page 21) section.

---

## Removing Event Handlers

➤ **To remove an event handler:**

1. Go to **Server > Event Manager**.
2. Select the corresponding check boxes in the list of handlers and click **Remove Selected** .

---

## **Event Parameters Passed by Event Handlers**

**In this section:**

Session (Login) Settings Event.....	23
Desktop Preset Event.....	23
Client Account Event.....	24
Client Status Event.....	24
Disk Space Limit Event for Client .....	25
Traffic Usage Limit Event for Client .....	25
Client Limits Event.....	25
Client Permissions Event.....	26
Client Preferences Event.....	29
Client's GUID Event .....	29
Clients Template Event .....	30
Client's IP Pool Event.....	30
Client's Site Application Package Event .....	30
Domain Event.....	31
Domain Limits Event .....	31
Domain Status Event.....	32
Domain's GUID Event .....	32
Domains Template Event .....	33
DNS Zone Event for Domain .....	33
Disk Space Limit Event for Domain .....	33
Traffic Usage Limit Event for Domain .....	33
Domain Owner Change Event.....	34
Subdomain Event.....	34
Domain Alias Event.....	35
Domain Alias, DNS Zone Event.....	35
Physical Hosting Event.....	36
Mail Account Event.....	38
Web User Event.....	39
Mailing List Event .....	39
Parallels Plesk Panel User Event .....	40
Domain Administrator Account Event .....	40
Domain Administrator's Permissions Event .....	41
Site Application Event .....	43
Service Event.....	44
IP Address Event .....	44
Forwarding Event .....	45
Administrator Information Event .....	45
Database Server Event .....	46
Parallels Plesk Panel Component Event .....	46
Database Event.....	46
Database User Account Event .....	47
License Key Event.....	47
Reseller Account Event.....	47
Reseller Status Event.....	48
Disk Space Limit Event for Reseller .....	48
Traffic Usage Limit Event for Reseller .....	49
Reseller Limits Event.....	49
Reseller Permissions Event.....	50
Reseller Preferences Event.....	53
Reseller's GUID Event .....	53
Resellers Template Event .....	54
Reseller's IP Pool Event.....	54
Reseller's Site Application Package Event .....	54

## Session (Login) Settings Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Session (login) settings changed'</b>			
Allowed period of inactivity for all Parallels Plesk Panel users	OLD_SESSION_IDLE_TIME	NEW_SESSION_IDLE_TIME	

## Desktop Preset Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Desktop preset created, modified, deleted'</b>			
Unique identification number of a desktop preset	OLD_DESKTOP_PRESET_ID	NEW_DESKTOP_PRESET_ID	
Type of desktop preset (default preset for administrator's desktop, client's desktop, domain administrator's desktop, or a user's custom preset)	OLD_DESKTOP_PRESET_TYPE	NEW_DESKTOP_PRESET_TYPE	
Desktop preset name	OLD_DESKTOP_PRESET_NAME	NEW_DESKTOP_PRESET_NAME	

## Client Account Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Client account created', 'Client account updated', 'Client account removed'</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Password	OLD_PASSWORD	NEW_PASSWORD	
Company name	OLD_COMPANY_NAME	NEW_COMPANY_NAME	
Phone	OLD_PHONE	NEW_PHONE	
Fax	OLD_FAX	NEW_FAX	
E- mail	OLD_EMAIL	NEW_EMAIL	
Address	OLD_ADDRESS	NEW_ADDRESS	
City	OLD_CITY	NEW_CITY	
State/province	OLD_STATE_PROVINCE	NEW_STATE_PROVINCE	
Postal/zip code	OLD_POSTAL_ZIP_CODE	NEW_POSTAL_ZIP_CODE	
Country	OLD_COUNTRY	NEW_COUNTRY	

## Client Status Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Client status updated'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Status	OLD_STATUS	NEW_STATUS	

## Disk Space Limit Event for Client

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Limit on disk space was reached for the client account'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Disk space limit	OLD_MAXIMUM_DISK_SPACE	NEW_MAXIMUM_DISK_SPACE	Required

## Traffic Usage Limit Event for Client

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Limit on traffic usage was reached for the client account'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Traffic limit	OLD_MAXIMUM_TRAFFIC	NEW_MAXIMUM_TRAFFIC	

## Client Limits Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Client limits changed'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Maximum number of domains	OLD_MAXIMUM_DOMAINS	NEW_MAXIMUM_DOMAINS	
Maximum amount of disk space	OLD_MAXIMUM_DISK_SPACE	NEW_MAXIMUM_DISK_SPACE	
Maximum amount of traffic	OLD_MAXIMUM_TRAFFIC	NEW_MAXIMUM_TRAFFIC	

Maximum number of Web users	OLD_MAXIMUM_WEBUSERS	NEW_MAXIMUM_WEBUSERS	
Maximum number of databases	OLD_MAXIMUM_DATABASES	NEW_MAXIMUM_DATABASES	
Maximum number of mailboxes	OLD_MAXIMUM_MAILBOXES	NEW_MAXIMUM_MAILBOXES	
Mailbox quota	OLD_MAXIMUM_MAILBOX_QUOTA	NEW_MAXIMUM_MAILBOX_QUOTA	
Maximum number of mail redirects	OLD_MAXIMUM_MAIL_REDIRECTS	NEW_MAXIMUM_MAIL_REDIRECTS	
Maximum number of mail groups	OLD_MAXIMUM_MAIL_GROUPS	NEW_MAXIMUM_MAIL_GROUPS	
Maximum number of mail autoresponders	OLD_MAXIMUM_MAIL_AUTORESPONDERS	NEW_MAXIMUM_MAIL_AUTORESPONDERS	
Maximum number of mailing lists	OLD_MAXIMUM_MAIL_LISTS	NEW_MAXIMUM_MAIL_LISTS	
Maximum number of Java applications	OLD_MAXIMUM_TOMCAT_WEB_APPLICATIONS	NEW_MAXIMUM_TOMCAT_WEB_APPLICATIONS	
Account expiration date	OLD_EXPIRATION_DATE	NEW_EXPIRATION_DATE	

## Client Permissions Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event "Client's permissions changed"</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	
Permission to use the Parallels Plesk Panel	OLD_CP_ACCESS	NEW_CP_ACCESS	

Permission to manage Web site hosting account	OLD_PHYSICAL_HOSTING_MANAGEMENT	NEW_PHYSICAL_HOSTING_MANAGEMENT	
Permission to switch PHP_safe mode off and on	OLD_PHP_SAFE_MODE_MANAGEMENT	NEW_PHP_SAFE_MODE_MANAGEMENT	
Permission to assign hard quotas on disk space	OLD_HARD_DISK_QUOTA_ASSIGNMENT	NEW_HARD_DISK_QUOTA_ASSIGNMENT	
Permission to manage subdomains	OLD_SUBDOMAINS_MANAGEMENT	NEW_SUBDOMAINS_MANAGEMENT	
Permission to manage domain aliases	OLD_DOMAIN_ALIASES_MANAGEMENT	NEW_DOMAIN_ALIASES_MANAGEMENT	
Permission to change the resource allotments for the user's Web sites	OLD_LIMITS_ADJUSTMENT	NEW_LIMITS_ADJUSTMENT	
Permission to manage DNS zones for domains	OLD_DNS_ZONE_MANAGEMENT	NEW_DNS_ZONE_MANAGEMENT	
Permission to adjust log recycling	OLD_LOG_ROTATION_MANAGEMENT	NEW_LOG_ROTATION_MANAGEMENT	
Permission to schedule tasks and automate execution of scripts	OLD_CRONTAB_MANAGEMENT	NEW_CRONTAB_MANAGEMENT	
Permission to manage anonymous FTP service	OLD_ANONYMOUS_FTP_MANAGEMENT	NEW_ANONYMOUS_FTP_MANAGEMENT	
Permission to manage Java Web applications and Java Web service	OLD_WEB_APPLICATIONS_MANAGEMENT	NEW_WEB_APPLICATIONS_MANAGEMENT	

Permission to manage Web statistics (switch between statistics programs)	OLD_WEB_STATISTICS_MANAGEMENT	NEW_WEB_STATISTICS_MANAGEMENT	
Permission to manage access to the server shell over SSH	OLD_SYSTEM_ACCESS_MANAGEMENT	NEW_SYSTEM_ACCESS_MANAGEMENT	
Permission to manage access to the server shell in chrooted environments over SSH	OLD_NON_CHROOTED_SHELL_MANAGEMENT	NEW_NON_CHROOTED_SHELL_MANAGEMENT	
Permission to manage mailing lists	OLD_MAILING_LISTS_MANAGEMENT	NEW_MAILING_LISTS_MANAGEMENT	
Permission to back up and restore data through the Parallels Plesk Panel and use the backup repository on the server	OLD_BACKUP_RESTORE_FUNCTIONS_USE_LOCAL_REPOSITORY	NEW_BACKUP_RESTORE_FUNCTIONS_USE_LOCAL_REPOSITORY	
Permission to back up and restore data through the Parallels Plesk Panel and use backup repositories on third-party FTP servers	OLD_BACKUP_RESTORE_FUNCTIONS_USE_FTP_REPOSITORY	NEW_BACKUP_RESTORE_FUNCTIONS_USE_FTP_REPOSITORY	
Permission to use the XML API for Web site management	OLD_ABILITY_TO_USE_REMOTE_XML_INTERFACE	NEW_ABILITY_TO_USE_REMOTE_XML_INTERFACE	
Permission to use the Desktop interface	OLD_ABILITY_TO_USE_DASHBOARD_INTERFACE	NEW_ABILITY_TO_USE_DASHBOARD_INTERFACE	

Permission to use the standard Parallels Plesk Panel interface	OLD_ABILITY_TO_USE_STANDARD_INTERFACE	NEW_ABILITY_TO_USE_STANDARD_INTERFACE	
Permission to customize Desktop	OLD_ABILITY_TO_MANAGE_DASHBOARD	NEW_ABILITY_TO_MANAGE_DASHBOARD	
Permission to manage spam filtering settings	OLD_ABILITY_TO_MANAGE_SPAMFILTER	NEW_ABILITY_TO_MANAGE_SPAMFILTER	
Permission to manage antivirus settings	OLD_ABILITY_TO_MANAGE_VIRUSFILTER	NEW_ABILITY_TO_MANAGE_VIRUSFILTER	

## Client Preferences Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Client preferences updated'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Page size	OLD_LINES_PER_PAGE	NEW_LINES_PER_PAGE	
Interface skin	OLD_INTERFACE_SKIN	NEW_INTERFACE_SKIN	

## Client's GUID Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the 'Client's GUID updated' event</b>			
Globally unique identifier (GUID)	OLD_GUID	NEW_GUID	Required

## Clients Template Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the 'Template for clients created', 'Template for clients updated', 'Template for clients removed' events</b>			
Reseller template ID	OLD_TEMPLATE_ID	NEW_TEMPLATE_ID	Required

## Client's IP Pool Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Client's IP pool changed'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
IP address	OLD_IP_ADDRESS	NEW_IP_ADDRESS	Required
Status	OLD_STATUS	NEW_STATUS	

## Client's Site Application Package Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Site application package added to client's pool', 'Site application package removed from client's pool'</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	
Package name	OLD_PACKAGE_NAME	NEW_PACKAGE_NAME	

## Domain Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Domain created', 'Domain updated', 'Domain deleted'</b>			
Domain Name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required

## Domain Limits Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Domain limits updated'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Maximum amount of disk space	OLD_MAXIMUM_DISK_SPACE	NEW_MAXIMUM_DISK_SPACE	
Maximum amount of traffic	OLD_MAXIMUM_TRAFFIC	NEW_MAXIMUM_TRAFFIC	
Maximum number of web users	OLD_MAXIMUM_WEBUSERS	NEW_MAXIMUM_WEBUSERS	
Maximum number of databases	OLD_MAXIMUM_DATABASES	NEW_MAXIMUM_DATABASES	
Maximum number of mailboxes	OLD_MAXIMUM_MAILBOXES	NEW_MAXIMUM_MAILBOXES	
Mailbox quota	OLD_MAXIMUM_MAILBOX_QUOTA	NEW_MAXIMUM_MAILBOX_QUOTA	
Maximum number of mail redirects	OLD_MAXIMUM_MAIL_REDIRECTS	NEW_MAXIMUM_MAIL_REDIRECTS	
Maximum number of mail groups	OLD_MAXIMUM_MAIL_GROUPS	NEW_MAXIMUM_MAIL_GROUPS	

Maximum number of mail autoresponders	OLD_MAXIMUM_MAIL_AUTORESPONDERS	NEW_MAXIMUM_MAIL_AUTORESPONDERS	
Maximum number of mailing lists	OLD_MAXIMUM_MAIL_LISTS	NEW_MAXIMUM_MAIL_LISTS	
Maximum number of java applications	OLD_MAXIMUM_TOMCAT_WEB_APPLICATIONS	NEW_MAXIMUM_TOMCAT_WEB_APPLICATIONS	
Expiration date	OLD_EXPIRATION_DATE	NEW_EXPIRATION_DATE	

## Domain Status Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Domain status changed'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Domain status	OLD_STATUS	NEW_STATUS	

## Domain's GUID Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the 'Domain's GUID updated' events</b>			
Globally unique identifier (GUID)	OLD_GUID	NEW_GUID	Required

## Domains Template Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the 'Template for domains created', 'Template for domains updated', 'Template for domains removed' events</b>			
Reseller template ID	OLD_TEMPLATE_ID	NEW_TEMPLATE_ID	Required

## DNS Zone Event for Domain

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'DNS zone updated for domain'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required

## Disk Space Limit Event for Domain

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Limit on disk space reached for domain'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Disk space limit	OLD_MAXIMUM_DISK_SPACE	NEW_MAXIMUM_DISK_SPACE	

## Traffic Usage Limit Event for Domain

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	

For the event 'Limit on traffic usage reached for domain'			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Traffic limit	OLD_MAXIMUM_TRAFFIC	NEW_MAXIMUM_TRAFFIC	

## Domain Owner Change Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the 'Domain owner changed' event			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	

## Subdomain Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the events 'Subdomain created', 'Subdomain updated', 'Subdomain deleted'			
Subdomain Name	OLD_SUBDOMAIN_NAME	NEW_SUBDOMAIN_NAME	Required
Parent domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
FTP account	OLD_SYSTEM_USER_TYPE	NEW_SYSTEM_USER_TYPE	
Subdomain administrator's login name	OLD_SYSTEM_USER	NEW_SYSTEM_USER	
Hard disk quota	OLD_HARD_DISK_QUOTA	NEW_HARD_DISK_QUOTA	
SSI support	OLD_SSI_SUPPORT	NEW_SSI_SUPPORT	
PHP support	OLD_PHP_SUPPORT	NEW_PHP_SUPPORT	
CGI support	OLD_CGI_SUPPORT	NEW_CGI_SUPPORT	
Perl support	OLD_MOD_PERL_SUPPORT	NEW_MOD_PERL_SUPPORT	

Python support	OLD_MOD_PYTHON_SUPPORT	NEW_MOD_PYTHON_SUPPORT	
ColdFusion support	OLD_COLDFUSION_SUPPORT	NEW_COLDFUSION_SUPPORT	
Apache::ASP support	OLD_APACHE_ASP_SUPPORT	NEW_APACHE_ASP_SUPPORT	
SSL support	OLD_SSL_SUPPORT	NEW_SSL_SUPPORT	

## Domain Alias Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Domain alias created, updated, deleted, DNS zone modified'</b>			
Domain alias name	OLD_DOMAIN_ALIAS_NAME	NEW_DOMAIN_ALIAS_NAME	Required
Domain alias switched on or off	OLD_STATUS	NEW_STATUS	
Web service for domain alias is on or off	OLD_DOMAIN_ALIAS_WEB	NEW_DOMAIN_ALIAS_WEB	
Mail service for domain alias is on or off	OLD_DOMAIN_ALIAS_MAIL	NEW_DOMAIN_ALIAS_MAIL	
Support for accessing web applications in Java for domain alias visitors (on or off)	OLD_DOMAIN_ALIAS_TOMCAT	NEW_DOMAIN_ALIAS_TOMCAT	

## Domain Alias, DNS Zone Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	

For the events 'Domain alias created, updated, deleted, DNS zone modified'			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
IP address	OLD_IP_ADDRESS	NEW_IP_ADDRESS	
IP type	OLD_IP_TYPE	NEW_IP_TYPE	
System user	OLD_SYSTEM_USER	NEW_SYSTEM_USER	
System user's password	OLD_SYSTEM_USER_PASSWORD	NEW_SYSTEM_USER_PASSWORD	
Shell access	OLD_SYSTEM_SHELL	NEW_SYSTEM_SHELL	
FP support	OLD_FP_SUPPORT	NEW_FP_SUPPORT	
FP- SSL support	OLD_FPSSL_SUPPORT	NEW_FPSSL_SUPPORT	
FP authoring	OLD_FP_AUTHORING	NEW_FP_AUTHORING	
FP admin login	OLD_FP_ADMIN_LOGIN	NEW_FP_ADMIN_LOGIN	
FP admin password	OLD_FP_ADMIN_PASSWORD	NEW_FP_ADMIN_PASSWORD	
SSI support	OLD_SSI_SUPPORT	NEW_SSI_SUPPORT	
PHP support	OLD_PHP_SUPPORT	NEW_PHP_SUPPORT	
CGI support	OLD_CGI_SUPPORT	NEW_CGI_SUPPORT	
Perl support	OLD_MOD_PERL_SUPPORT	NEW_MOD_PERL_SUPPORT	
Apache ASP support	OLD_APACHE_ASP_SUPPORT	NEW_APACHE_ASP_SUPPORT	
SSL support	OLD_SSL_SUPPORT	NEW_SSL_SUPPORT	
Web statistics	OLD_WEB_STATISTICS	NEW_WEB_STATISTICS	
Custom error documents	OLD_APACHE_ERROR_DOCUMENTS	NEW_APACHE_ERROR_DOCUMENTS	
Hard disk quota	OLD_HARD_DISK_QUOTA	NEW_HARD_DISK_QUOTA	

## Physical Hosting Event

For the events 'Physical hosting created', 'Physical hosting updated'			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
IP address	OLD_IP_ADDRESS	NEW_IP_ADDRESS	
IP type	OLD_IP_TYPE	NEW_IP_TYPE	

System user	OLD_SYSTEM_USER	NEW_SYSTEM_USER	
System user's password	OLD_SYSTEM_USER_PASSWORD	NEW_SYSTEM_USER_PASSWORD	
Shell access	OLD_SYSTEM_SHELL	NEW_SYSTEM_SHELL	
FP support	OLD_FP_SUPPORT	NEW_FP_SUPPORT	
FP- SSL support	OLD_FPSSL_SUPPORT	NEW_FPSSL_SUPPORT	
FP authoring	OLD_FP_AUTHORIZING	NEW_FP_AUTHORIZING	
FP admin login	OLD_FP_ADMIN_LOGIN	NEW_FP_ADMIN_LOGIN	
FP admin password	OLD_FP_ADMIN_PASSWORD	NEW_FP_ADMIN_PASSWORD	
SSI support	OLD_SSI_SUPPORT	NEW_SSI_SUPPORT	
PHP support	OLD_PHP_SUPPORT	NEW_PHP_SUPPORT	
CGI support	OLD_CGI_SUPPORT	NEW_CGI_SUPPORT	
Perl support	OLD_MOD_PERL_SUPPORT	NEW_MOD_PERL_SUPPORT	
Apache ASP support	OLD_APACHE_ASP_SUPPORT	NEW_APACHE_ASP_SUPPORT	
SSL support	OLD_SSL_SUPPORT	NEW_SSL_SUPPORT	
Web statistics	OLD_WEB_STATISTICS	NEW_WEB_STATISTICS	
Custom error documents	OLD_APACHE_ERROR_DOCUMENTS	NEW_APACHE_ERROR_DOCUMENTS	
Hard disk quota	OLD_HARD_DISK_QUOTA	NEW_HARD_DISK_QUOTA	

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Physical hosting deleted'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required

## Mail Account Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Mail account created', 'Mail account deleted'</b>			
E-mail address	OLD_MAILNAME	NEW_MAILNAME	Required (in the format of mailname@domain)

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Mail account updated'</b>			
E-mail address	OLD_MAILNAME	NEW_MAILNAME	Required (in the format mailname@domain)
Mailbox	OLD_MAILBOX	NEW_MAILBOX	
Password	OLD_PASSWORD	NEW_PASSWORD	
Mailbox quota	OLD_MAILBOX_QUOTA	NEW_MAILBOX_QUOTA	
Redirect	OLD_REDIRECT	NEW_REDIRECT	
Redirect address	OLD_REDIRECT_ADDRESSES	NEW_REDIRECT_ADDRESS	
Mail group	OLD_MAIL_GROUP	NEW_MAIL_GROUP	
Autoresponders	OLD_AUTORESPONDERS	NEW_AUTORESPONDERS	
Access to Parallels Plesk Panel for e-mail user	OLD_MAIL_CONTROLPANEL_ACCESS	NEW_MAIL_CONTROLPANEL_ACCESS	

## Web User Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Web user deleted'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Web user name	OLD_WEBUSER_NAME	NEW_WEBUSER_NAME	Required

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Web user created', 'Web user updated'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Web user name	OLD_WEBUSER_NAME	NEW_WEBUSER_NAME	Required
Web user's password	OLD_WEBUSER_PASSWORD	NEW_WEBUSER_PASSWORD	
SSI support	OLD_SSI_SUPPORT	NEW_SSI_SUPPORT	
PHP support	OLD_PHP_SUPPORT	NEW_PHP_SUPPORT	
CGI support	OLD_CGI_SUPPORT	NEW_CGI_SUPPORT	
Perl support	OLD_MOD_PERL_SUPPORT	NEW_MOD_PERL_SUPPORT	
Python support	OLD_MOD_PYTHON_SUPPORT	NEW_MOD_PYTHON_SUPPORT	
Apache ASP support	OLD_APACHE_ASP_SUPPORT	NEW_APACHE_ASP_SUPPORT	
Hard disk quota	OLD_HARD_DISK_QUOTA	NEW_HARD_DISK_QUOTA	

## Mailing List Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	

For the events 'Mailing list created', 'Mailing list updated', 'Mailing list deleted'			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Mailing list name	OLD_MAIL_LIST_NAME	NEW_MAIL_LIST_NAME	Required
Mailing list enabled	OLD_MAIL_LIST_ENABLED	NEW_MAIL_LIST_ENABLED	

## Parallels Plesk Panel User Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the events 'Parallels Plesk Panel user logged in', 'Parallels Plesk Panel user logged out'			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	

## Domain Administrator Account Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the event 'Domain administrator account updated'			
Allow domain administrator access	OLD_ALLOW_DOMAIN_USER_ACCESS	NEW_ALLOW_DOMAIN_USER_ACCESS	
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	
Password	OLD_PASSWORD	NEW_PASSWORD	
Company name	OLD_COMPANY_NAME	NEW_COMPANY_NAME	
Phone	OLD_PHONE	NEW_PHONE	
Fax	OLD_FAX	NEW_FAX	
E- mail	OLD_EMAIL	NEW_EMAIL	
Address	OLD_ADDRESS	NEW_ADDRESS	

City	OLD_CITY	NEW_CITY	
State/Province	OLD_STATE_PROVINCE	NEW_STATE_PROVINCE	
Postal/ZIP code	OLD_POSTAL_ZIP_CODE	NEW_POSTAL_ZIP_CODE	
Country	OLD_COUNTRY	NEW_COUNTRY	

## Domain Administrator's Permissions Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Domain administrator's permissions changed'</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	
Permission to manage Web site hosting account	OLD_PHYSICAL_HOSTING_MANAGEMENT	NEW_PHYSICAL_HOSTING_MANAGEMENT	
Permission to change FTP password	OLD_MANAGE_FTP_PASSWORD	NEW_MANAGE_FTP_PASSWORD	
Permission to assign hard quotas on disk space	OLD_HARD_DISK_QUOTA_ASSIGNMENT	NEW_HARD_DISK_QUOTA_ASSIGNMENT	
Permission to manage subdomains	OLD_SUBDOMAINS_MANAGEMENT	NEW_SUBDOMAINS_MANAGEMENT	
Permission to manage domain aliases	OLD_DOMAIN_ALIASES_MANAGEMENT	NEW_DOMAIN_ALIASES_MANAGEMENT	
Permission to manage DNS zone for the Web site	OLD_DNS_ZONE_MANAGEMENT	NEW_DNS_ZONE_MANAGEMENT	
Permission to adjust log recycling	OLD_LOG_ROTATION_MANAGEMENT	NEW_LOG_ROTATION_MANAGEMENT	

Permission to schedule tasks and automate execution of scripts	OLD_CRONTAB_MANAGEMENT	NEW_CRONTAB_MANAGEMENT	
Permission to manage anonymous FTP service	OLD_ANONYMOUS_FTP_MANAGEMENT	NEW_ANONYMOUS_FTP_MANAGEMENT	
Permission to manage Java Web applications and Java Web service	OLD_WEB_APPLICATIONS_MANAGEMENT	NEW_WEB_APPLICATIONS_MANAGEMENT	
Permission to manage Web statistics (switch between statistics programs)	OLD_WEB_STATISTICS_MANAGEMENT	NEW_WEB_STATISTICS_MANAGEMENT	
Permission to manage access to the server shell over SSH	OLD_SYSTEM_ACCESS_MANAGEMENT	NEW_SYSTEM_ACCESS_MANAGEMENT	
Permission to manage access to the server shell in chrooted environment over SSH	OLD_NON_CHROOTED_SHELL_MANAGEMENT	NEW_NON_CHROOTED_SHELL_MANAGEMENT	
Permission to manage mailing lists	OLD_MAILING_LISTS_MANAGEMENT	NEW_MAILING_LISTS_MANAGEMENT	
Permission to back up and restore data through the Parallels Plesk Panel and use the backup repository on the server	OLD_BACKUP_RESTORE_FUNCTIONS_USE_LOCAL_REPOSITORY	NEW_BACKUP_RESTORE_FUNCTIONS_USE_LOCAL_REPOSITORY	

Permission to back up and restore data through the Parallels Plesk Panel and use backup repositories on third-party FTP servers	OLD_BACKUP_RESTORE_FUNCTIONS_USE_FTP_REPOSITORY	NEW_BACKUP_RESTORE_FUNCTIONS_USE_FTP_REPOSITORY	
Permission to use the XML API for Web site management	OLD_ABILITY_TO_USE_REMOTE_XML_INTERFACE	NEW_ABILITY_TO_USE_REMOTE_XML_INTERFACE	
Permission to use the Desktop interface	OLD_ABILITY_TO_USE_DASHBOARD_INTERFACE	NEW_ABILITY_TO_USE_DASHBOARD_INTERFACE	
Permission to use the standard Parallels Plesk Panel interface	OLD_ABILITY_TO_USE_STANDARD_INTERFACE	NEW_ABILITY_TO_USE_STANDARD_INTERFACE	
Permission to customize Desktop	OLD_ABILITY_TO_MANAGE_DASHBOARD	NEW_ABILITY_TO_MANAGE_DASHBOARD	
Permission to manage spam filtering settings	OLD_ABILITY_TO_MANAGE_SPAMFILTER	NEW_ABILITY_TO_MANAGE_SPAMFILTER	
Permission to manage antivirus settings	OLD_ABILITY_TO_MANAGE_VIRUSFILTER	NEW_ABILITY_TO_MANAGE_VIRUSFILTER	

## Site Application Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	

For the events 'Site application installed', 'Site application reconfigured', Site application uninstalled'			
Site application package name	OLD_PACKAGE_NAME	NEW_PACKAGE_NAME	Required
Domain type (domain or subdomain)	OLD_DOMAIN_TYPE	NEW_DOMAIN_TYPE	Required
Installation path (httpdocs or httpsdocs)	OLD_DIRECTORY	NEW_DIRECTORY	Required
Installation path within the destination directory	OLD_INSTALLATION_PREFIX	NEW_INSTALLATION_PREFIX	Required

## Service Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the events 'Service stopped, started, or restarted'			
Service	OLD_SERVICE	NEW_SERVICE	Required

## IP Address Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the events 'IP address created, changed, or deleted'			
IP address	OLD_IP_ADDRESS	NEW_IP_ADDRESS	Required
IP mask	OLD_IP_MASK	NEW_IP_MASK	
Interface	OLD_INTERFACE	NEW_INTERFACE	
IP type	OLD_IP_TYPE	NEW_IP_TYPE	

## Forwarding Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Forwarding created, changed, deleted'</b>			
Domain name	OLD_DOMAIN_NAME	NEW_DOMAIN_NAME	Required
Forwarding type	OLD_FORWARDING_TYPE	NEW_FORWARDING_TYPE	
URL	OLD_URL	NEW_URL	

## Administrator Information Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Administrator information changed'</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	
Company name	OLD_COMPANY_NAME	NEW_COMPANY_NAME	
Phone number	OLD_PHONE	NEW_PHONE	
Fax	OLD_FAX	NEW_FAX	
E- mail	OLD_EMAIL	NEW_EMAIL	
Address	OLD_ADDRESS	NEW_ADDRESS	
City	OLD_CITY	NEW_CITY	
State/Province	OLD_STATE_PROVINCE	NEW_STATE_PROVINCE	
Postal/Zip code	OLD_POSTAL_ZIP_CODE	NEW_POSTAL_ZIP_CODE	
Country	OLD_COUNTRY	NEW_COUNTRY	

## Database Server Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Database server created, modified, deleted'</b>			
Database server's IP address	OLD_DATABASE_SERVER	NEW_DATABASE_SERVER	

## Parallels Plesk Panel Component Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Parallels Plesk Panel component upgraded'</b>			
Parallels Plesk Panel component name	OLD_PLESK_COMPONENT_NAME	NEW_PLESK_COMPONENT_NAME	

## Database Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Database created, deleted'</b>			
Database server's IP address	OLD_DATABASE_SERVER	NEW_DATABASE_SERVER	
Database name	OLD_DATABASE_NAME	NEW_DATABASE_NAME	

## Database User Account Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Database user account created, changed, deleted'</b>			
Database server's IP address	OLD_DATABASE_SERVER	NEW_DATABASE_SERVER	
Database identification number	OLD_DATABASE_ID	NEW_DATABASE_ID	
Database user name	OLD_DATABASE_USER_NAME	NEW_DATABASE_USER_NAME	
Database user password	OLD_DATABASE_USER_PASSWORD	NEW_DATABASE_USER_PASSWORD	

## License Key Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'License key upd</b>			
License key number	OLD_LICENSE	NEW_LICENSE	Required
License key type (Parallels Plesk Panel, additional)	OLD_LICENSE_TYPE	NEW_LICENSE_TYPE	
License key name (for additional keys)	OLD_LICENSE_NAME	NEW_LICENSE_NAME	

## Reseller Account Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	

For the events 'Reseller account created', "Reseller account updated", "Reseller account removed'			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Password	OLD_PASSWORD	NEW_PASSWORD	
Company name	OLD_COMPANY_NAME	NEW_COMPANY_NAME	
Phone	OLD_PHONE	NEW_PHONE	
Fax	OLD_FAX	NEW_FAX	
E- mail	OLD_EMAIL	NEW_EMAIL	
Address	OLD_ADDRESS	NEW_ADDRESS	
City	OLD_CITY	NEW_CITY	
State/province	OLD_STATE_PROVINCE	NEW_STATE_PROVINCE	
Postal/zip code	OLD_POSTAL_ZIP_CODE	NEW_POSTAL_ZIP_CODE	
Country	OLD_COUNTRY	NEW_COUNTRY	

## Reseller Status Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Reseller status updated'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Status	OLD_STATUS	NEW_STATUS	

## Disk Space Limit Event for Reseller

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	

For the event 'Limit on disk space was reached for the reseller account'			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Disk space limit	OLD_MAXIMUM_DISK_SPACE	NEW_MAXIMUM_DISK_SPACE	Required

## Traffic Usage Limit Event for Reseller

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the events 'Limit on traffic usage was reached for the reseller account'			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Traffic limit	OLD_MAXIMUM_TRAFFIC	NEW_MAXIMUM_TRAFFIC	

## Reseller Limits Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
For the event 'Reseller limits changed'			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Maximum number of domains	OLD_MAXIMUM_DOMAINS	NEW_MAXIMUM_DOMAINS	
Maximum amount of disk space	OLD_MAXIMUM_DISK_SPACE	NEW_MAXIMUM_DISK_SPACE	
Maximum amount of traffic	OLD_MAXIMUM_TRAFFIC	NEW_MAXIMUM_TRAFFIC	
Maximum number of Web users	OLD_MAXIMUM_WEBUSERS	NEW_MAXIMUM_WEBUSERS	
Maximum number of databases	OLD_MAXIMUM_DATABASES	NEW_MAXIMUM_DATABASES	

Maximum number of mailboxes	OLD_MAXIMUM_MAILBOXES	NEW_MAXIMUM_MAILBOXES	
Mailbox quota	OLD_MAXIMUM_MAILBOX_QUOTA	NEW_MAXIMUM_MAILBOX_QUOTA	
Maximum number of mail redirects	OLD_MAXIMUM_MAIL_REDIRECTS	NEW_MAXIMUM_MAIL_REDIRECTS	
Maximum number of mail groups	OLD_MAXIMUM_MAIL_GROUPS	NEW_MAXIMUM_MAIL_GROUPS	
Maximum number of mail autoresponders	OLD_MAXIMUM_MAIL_AUTORESPONDERS	NEW_MAXIMUM_MAIL_AUTORESPONDERS	
Maximum number of mailing lists	OLD_MAXIMUM_MAIL_LISTS	NEW_MAXIMUM_MAIL_LISTS	
Maximum number of Java applications	OLD_MAXIMUM_TOMCAT_WEB_APPLICATIONS	NEW_MAXIMUM_TOMCAT_WEB_APPLICATIONS	
Account expiration date	OLD_EXPIRATION_DATE	NEW_EXPIRATION_DATE	

## Reseller Permissions Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Reseller's permissions changed'</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	
Permission to use the Parallels Plesk Panel	OLD_CP_ACCESS	NEW_CP_ACCESS	
Permission to manage Web site hosting account	OLD_PHYSICAL_HOSTING_MANAGEMENT	NEW_PHYSICAL_HOSTING_MANAGEMENT	

Permission to switch PHP_safe mode off and on	OLD_PHP_SAFE_MODE_MANAGEMENT	NEW_PHP_SAFE_MODE_MANAGEMENT	
Permission to assign hard quotas on disk space	OLD_HARD_DISK_QUOTA_ASSIGNMENT	NEW_HARD_DISK_QUOTA_ASSIGNMENT	
Permission to manage subdomains	OLD_SUBDOMAINS_MANAGEMENT	NEW_SUBDOMAINS_MANAGEMENT	
Permission to manage domain aliases	OLD_DOMAIN_ALIASES_MANAGEMENT	NEW_DOMAIN_ALIASES_MANAGEMENT	
Permission to change the resource allotments for the user's Web sites	OLD_LIMITS_ADJUSTMENT	NEW_LIMITS_ADJUSTMENT	
Permission to manage DNS zones for domains	OLD_DNS_ZONE_MANAGEMENT	NEW_DNS_ZONE_MANAGEMENT	
Permission to adjust log recycling	OLD_LOG_ROTATION_MANAGEMENT	NEW_LOG_ROTATION_MANAGEMENT	
Permission to schedule tasks and automate execution of scripts	OLD_CRONTAB_MANAGEMENT	NEW_CRONTAB_MANAGEMENT	
Permission to manage anonymous FTP service	OLD_ANONYMOUS_FTP_MANAGEMENT	NEW_ANONYMOUS_FTP_MANAGEMENT	
Permission to manage Java Web applications and Java Web service	OLD_WEB_APPLICATIONS_MANAGEMENT	NEW_WEB_APPLICATIONS_MANAGEMENT	

Permission to manage Web statistics (switch between statistics programs)	OLD_WEB_STATISTICS_MANAGEMENT	NEW_WEB_STATISTICS_MANAGEMENT	
Permission to manage access to the server shell over SSH	OLD_SYSTEM_ACCESS_MANAGEMENT	NEW_SYSTEM_ACCESS_MANAGEMENT	
Permission to manage access to the server shell in chrooted environments over SSH	OLD_NON_CHROOTED_SHELL_MANAGEMENT	NEW_NON_CHROOTED_SHELL_MANAGEMENT	
Permission to manage mailing lists	OLD_MAILING_LISTS_MANAGEMENT	NEW_MAILING_LISTS_MANAGEMENT	
Permission to back up and restore data through the Parallels Plesk Panel and use the backup repository on the server	OLD_BACKUP_RESTORE_FUNCTIONS_USE_LOCAL_REPOSITORY	NEW_BACKUP_RESTORE_FUNCTIONS_USE_LOCAL_REPOSITORY	
Permission to back up and restore data through the Parallels Plesk Panel and use backup repositories on third-party FTP servers	OLD_BACKUP_RESTORE_FUNCTIONS_USE_FTP_REPOSITORY	NEW_BACKUP_RESTORE_FUNCTIONS_USE_FTP_REPOSITORY	
Permission to use the XML API for Web site management	OLD_ABILITY_TO_USE_REMOTE_XML_INTERFACE	NEW_ABILITY_TO_USE_REMOTE_XML_INTERFACE	
Permission to use the Desktop interface	OLD_ABILITY_TO_USE_DASHBOARD_INTERFACE	NEW_ABILITY_TO_USE_DASHBOARD_INTERFACE	

Permission to use the standard Parallels Plesk Panel interface	OLD_ABILITY_TO_USE_STANDARD_INTERFACE	NEW_ABILITY_TO_USE_STANDARD_INTERFACE	
Permission to customize Desktop	OLD_ABILITY_TO_MANAGE_DASHBOARD	NEW_ABILITY_TO_MANAGE_DASHBOARD	
Permission to manage spam filtering settings	OLD_ABILITY_TO_MANAGE_SPAMFILTER	NEW_ABILITY_TO_MANAGE_SPAMFILTER	
Permission to manage antivirus settings	OLD_ABILITY_TO_MANAGE_VIRUSFILTER	NEW_ABILITY_TO_MANAGE_VIRUSFILTER	

## Reseller Preferences Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Reseller preferences updated'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	Required
Page size	OLD_LINES_PER_PAGE	NEW_LINES_PER_PAGE	
Interface skin	OLD_INTERFACE_SKIN	NEW_INTERFACE_SKIN	

## Reseller's GUID Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the 'Reseller's GUID updated' events</b>			
Globally unique identifier (GUID)	OLD_GUID	NEW_GUID	Required

## Resellers Template Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the 'Template for resellers created', 'Template for resellers updated', 'Template for resellers removed' events</b>			
Reseller template ID	OLD_TEMPLATE_ID	NEW_TEMPLATE_ID	Required

## Reseller's IP Pool Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the event 'Reseller's IP pool changed'</b>			
Contact name	OLD_CONTACT_NAME	NEW_CONTACT_NAME	Required
IP address	OLD_IP_ADDRESS	NEW_IP_ADDRESS	Required
Status	OLD_STATUS	NEW_STATUS	

## Reseller's Site Application Package Event

Parameter name and description	Environment variable name		Notes
	Previously used value	New value	
<b>For the events 'Site application package added to reseller's pool', 'Site application package removed from reseller's pool'</b>			
Login name	OLD_LOGIN_NAME	NEW_LOGIN_NAME	
Package name	OLD_PACKAGE_NAME	NEW_PACKAGE_NAME	

# Configuring Apache Server

You can modify global setting for the Apache server in the main Apache configuration file:

- `/etc/httpd/conf/httpd.conf` for RedHat-based systems;
- `/etc/apache2/apache2.conf` (or a corresponding file from `/etc/apache2/conf.d/` `/etc/apache2/sites-enabled/`) for Debian-based systems;
- `/etc/apache2/httpd.conf` (or `/etc/apache2/vhosts.d/*`) for SuSE;

## In this chapter:

Getting Familiar with Virtual Host Structure and Permissions .....	56
Enabling Piped Logs for Web Server to Reduce the Risk of Web Service Disruption .....	58
Recompiling Apache With More File Descriptors .....	59
Including Directives into Web Server Configuration File .....	65
Customizing <code>httpd.include</code> for Domains .....	66
Preventing Graphics Hotlinking on a Web Site .....	66
Apache Port Change .....	67

## Getting Familiar with Virtual Host Structure and Permissions

Vhost permissions should satisfy the following conditions:

- Home directory should be readable by `apache`, `psadm` and `psaftp`.
- The user cannot change some catalogues of their directories.
- Other users should not have access to the user's home directory.

The following table shows the virtual host structure and permissions set to the vhost catalogue:

Directories Tree	User	Group	Perms	Description
<code>&lt;VHOST&gt;</code>	root	root	755	
<code>/anon_ftp</code>	user	psaserv	750	Anonymous FTP files
<code>/cgi-bin</code>	user	psaserv	750	CGI scripts
<code>/conf</code>	root	psaserv	755	Configuration files
<code>/error_docs</code>	root	psaserv	755	Error messages files
<code>&lt;doc&gt;.html</code>	user	psaserv	755	
<code>/etc</code>	root	root	755	Chroot environment catalogue
<code>/httpdocs</code>	user	psaserv	750	HTTP documents
<code>/httpsdocs</code>	user	psaserv	750	HTTPS documents
<code>/pd</code>	root	psaserv	750	Passwords to protected directories
<code>d.&lt;dir1&gt;@&lt;dir2&gt;</code>	apache	apache	400	
<code>/private</code>	user	root	700	User's private storage
<code>/statistics</code>	root	psaserv	550	Statistics directory

/anon_ftpstat	root	root	755	Anonymous FTP statistics
/ftpstat	root	root	755	FTP user statistics
/logs	root	root	755	Virtual host logs
/webstat	root	root	755	HTTP user statistics
/webstat-ssl	root	root	755	HTTPS user statistics
/usr	root	root	755	Chroot environment catalogue
/web_users	root	psaserv	755	Web users catalogue
<web_user>	web_user	psaserv	750	
/subdomains	root	psaserv	755	Subdomains catalogue
<subdomain>	root	root	755	
/cgi-bin	sub_user	psaserv	750	
/conf	root	psaserv	750	
/error_docs	root	root	755	
/httpdocs	sub_user	psaserv	750	
/httpsdocs	sub_user	psaserv	750	

---

**Tip:** Microsoft FrontPage Server Extensions are no longer shipped with Parallels Plesk Panel, though if you want to use Microsoft Frontpage Server Extensions, modify the vhost permissions. Assign the `psaserv` group to `http(s)docs/_vti_*` files recursively and to the `http(s)docs/.htaccess` file in the `http(s)docs` catalogue, and set the `751` permission to the `http(s)docs` catalogue.

---

---

## Enabling Piped Logs for Web Server to Reduce the Risk of Web Service Disruption

If you are going to host more than 300 domains or web sites on your server, you should switch on support for piped logs in the Apache Web Server.

➤ ***To enable piped logs:***

1. Log in to the server shell.
2. Issue the command `mysql -uadmin -p'cat /etc/psa/.psa.shadow' -D psa -e "replace into misc (param,val) values ('apache_pipelog', 'true');"`
3. Rebuild Apache configuration by issuing the command  
`/usr/local/psa/admin/sbin/websrvmng -a -v`

This will allow to host about 900 domains/web sites. If you need to host more than 900 domains/Web sites, then you will need to recompile Apache and some other system packages, as described in the [Recompiling Apache With More File Descriptors](#) (see page 59) section.

---

# Recompiling Apache With More File Descriptors

If you are going to host a large number of web sites on the Parallels Plesk Panel server, Apache may fail to work because of a problem with the file descriptors limit.

---

**Note:** Since Parallels Plesk Panel 8.2.0 up to 900 domains can be hosted on the OS vendor Apache build without system packages recompilation described in this section, if Piped Logs feature is enabled on the Parallels Plesk Panel server (see page 58).

---

## In this section:

Recompiling Apache With More File Descriptors on RedHat-like System .....	60
Recompiling Apache With More File Descriptors on Debian System .....	62
Recompiling Apache With More File Descriptors on FreeBSD System .....	63

## Recompiling Apache With More File Descriptors on RedHat-like System

Parallels Plesk Panel requires, closely depends on and uses many server applications which are not part of Parallels Plesk Panel software actually. For example, apache web server, mysql server, php module and binaries and many others are not provided or compiled by Parallels, but standard system RPM packages from operating system vendor are used by Parallels Plesk Panel and they are used 'as is'. This allows to upgrade and recompile such packages with the options the Parallels Plesk Panel administrator wants.

➤ **To recompile related applications and libraries, such as openssl, apache, imap, PHP etc from source RPMs with increased `FD_SETSIZE` value, perform the following steps:**

1. Make sure that the system allows to open enough files:

```
# /sbin/sysctl fs.file-max
fs.file-max = 131072
```

If `fs.file-max` is quite small (several thousands or so), change it in the following way:

a. Add the following line to `/etc/sysctl.conf`:

```
fs.file-max = 131072
```

b. Running the shell command:

```
# /sbin/sysctl -w fs.file-max=131072
```

---

**Note:** If you are running Virtuozzo, you have to adjust the `fs.file-max` on the hardware node and it will be applied to all VEs.

---

2. Make sure you have the `glibc-kernheaders` and `glibc-headers` packages installed. They can be taken from the operating system distributive CD or from your operating system download sites.

3. Edit the `__FD_SETSIZE` value in `typesizes.h` and `posix_types.h` files:

▪ To find the `typesizes.h` file, run:

```
# find /usr/include/ -name typesizes.h
```

▪ To find the `posix_types.h` file, run:

```
# find /usr/include/ -name posix_types.h
```

▪ To edit the `__FD_SETSIZE` value in a file, run:

```
#define __FD_SETSIZE 65536
```

4. Download the following source RPMs that can be found on your operating system download sites or similar places, you may use RPM search engines such as <http://rpm.pbone.net> or <http://rpmfind.net>:

- `openssl-*.src.rpm`
- `httpd-*.src.rpm`
- `imap-*.src.rpm`

- `php-*.src.rpm`
- `libc-client-devel-*.src.rpm` (if such RPM is installed)
- `curl-*.src.rpm`

5. Recompile `openssl` first. For example:

```
# /usr/bin/rpmbuild-rebuild openssl-0.9.7a-35.src.rpm
```

6. Install the compiled `openssl` RPM with the following command line:

```
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/openssl-0.9.7a-35.i386.rpm
```

7. Recompile and install `cURL` in the same way.

8. Recompile and install `apache`:

```
# rpmbuild-rebuild httpd-2.0.51-2.9.src.rpm
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/httpd-2.0.51-2.9.i386.rpm
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/httpd-devel-2.0.51-2.9.i386.rpm
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/mod_ssl-2.0.51-2.9.i386.rpm
```

9. Recompile and install the `libc-client` library which is provided by the `imap` or `libc-client-devel` packages (depending on the OS) .  
Recompile the one that is installed in the system, for example:

```
# /usr/bin/rpmbuild-rebuild imap-2002d-3.src.rpm
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/imap-devel-2002d-3.i386.rpm
```

or

```
# /usr/bin/rpmbuild-rebuild libc-client-devel.src.rpm
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/libc-client-devel.rpm
```

10. Recompile and install `PHP`, for example:

```
# rpmbuild-rebuild php-4.3.10-2.4.src.rpm
# rpm -Uvh-force /usr/src/redhat/RPMS/i386/php-*
```

11. Add the following command to `/etc/rc.d/init.d/httpd` and `/usr/sbin/apachectl` startup scripts of `apache` before other commands:

```
ulimit -n 65536
```

12. Replace the `/usr/sbin/suexec` with the one from Parallels Plesk Panel:

```
# cp /usr/local/psa/suexec/psa-suexec /usr/sbin/suexec
# /etc/init.d/httpd restart
```

For Parallels Plesk Panel versions earlier than 7.5:

```
# cp /usr/local/psa/suexec/psa-suexec /usr/sbin/suexec
# chown root:apache /usr/sbin/suexec
# chmod 4510 /usr/sbin/suexec
# /etc/init.d/httpd restart
```

## Recompiling Apache With More File Descriptors on Debian System

➤ *To recompile Apache, PHP and IMAP with increased value of file descriptors larger than `FD_SETSIZE (1024)` on Debian system:*

1. Add the following line to `/etc/sysctl.conf`:

```
fs.file-max = 65536
```

2. Run the following shell command:

```
/sbin/sysctl -w fs.file-max=65536
```

Note that the value `fs.file-max` can be equal up to `220=1048576`).

3. Add the following line to beginning of `/etc/init.d/apache2` and `/usr/sbin/apache2ctl`:

```
ulimit -n `cat /proc/sys/fs/file-max`
```

4. Change `__FD_SETSIZE` value in `/usr/include/bits/typesizes.h` and `/usr/include/nptl/bits/typesizes.h` files. It should be like:

```
#define __FD_SETSIZE 65536
```

5. Download and rebuild packages:

```
# apt-get install apt-src
# apt-src-build install openssl
# dpkg -i libssl*.deb openssl*.deb
# apt-src-build install apache2
# dpkg -i libapr*.deb apache2_*.deb apache2-common*.deb apache2-mpm-
prefork*.deb apache2-utils*.deb
# cp /opt/psa/suexec/psa-suexec2 /usr/lib/apache2/suexec2
/etc/init.d/apache2 restart
# apt-src-build install libc-client2002debian
# dpkg -i libc-client-dev_2002debian1-*.deb libc-client2002debian*.deb
mlock*.deb
# apt-src-build install php4
# dpkg -i `ls *deb|grep php4|grep -v apache-mod`
```

## Recompiling Apache With More File Descriptors on FreeBSD System

Apache and apache modules come with Parallels Plesk Panel for FreeBSD versions 8.1.0 or earlier and are already compiled with `FD_SETSIZE = 16384` and if you have problem with file descriptors lack then the reason is in some non-Plesk system application. The most probably it is related to standard system OpenSSL libraries which are dynamically loaded by Parallels Plesk Panel's apache. To have the system OpenSSL library files be recompiled with increased `FD_SETSIZE` value, please do the following.

➤ **To recompile OpenSSL with increased value of file descriptors larger than `FD_SETSIZE (1024)` on FreeBSD system, perform the following steps:**

1. Obtain FreeBSD sources for your FreeBSD version, for example using the `cvsup` utility. See "Obtaining FreeBSD" in the FreeBSD Handbook for details. We would recommend that you obtain not original sources for exactly the same FreeBSD release that you are currently running, but updated sources from a stable branch for your FreeBSD version.
2. Edit the `/usr/src/sys/sys/select.h` and `/usr/include/sys/select.h` files and modify there `FD_SETSIZE` value from `1024U` to `16384U`:

```
# ifndef FD_SETSIZE
# define FD_SETSIZE 16384U
```

3. Run the following commands to recompile all the system files including OpenSSL libraries:

```
# rm -rf /usr/obj/usr
# cd /usr/src
# make clean ; make cleandepend
# make buildworld
```

You can update not only OpenSSL libraries but also system binaries and libraries and also update or modify the kernel. To do this and continue with system/kernel update, please follow "The Cutting Edge" chapter in FreeBSD Handbook for details.

4. If your system/kernel is up-to-date or you don't need to update anything except OpenSSL libraries for other reason, you can find what files are used by apache and replace them manually with new copies. Below is example for FreeBSD 6.0:

```
# ldd /usr/local/psa/apache/bin/httpd
# /usr/local/psa/apache/bin/httpd:
# libaprutil-0.so.9 => /usr/local/psa/apache/lib/libaprutil-0.so.9
(0x281cb000)
# libapr-0.so.9 => /usr/local/psa/apache/lib/libapr-0.so.9 (0x281dd000)
# libm.so.4 => /lib/libm.so.4 (0x281f8000)
# libcrypt.so.3 => /lib/libcrypt.so.3 (0x28211000)
# libssl.so.4 => /usr/lib/libssl.so.4 (0x28229000)
# libcrypto.so.4 => /lib/libcrypto.so.4 (0x28257000)
# libz.so.3 => /lib/libz.so.3 (0x2834e000)
# libc.so.6 => /lib/libc.so.6 (0x2835e000)
```

In our FreeBSD 6.0 case these files are:

```
/lib/libcrypt.so.3  
/lib/libcrypto.so.4  
/usr/lib/libssl.so.4
```

**5. Make backup copies of these files just in case:**

```
# cp -p /lib/libcrypt.so.3 /lib/libcrypt.so.3.back ; \  
# cp -p /lib/libcrypto.so.4 /lib/libcrypto.so.4.back ; \  
# cp -p /usr/lib/libssl.so.4 /usr/lib/libssl.so.4.back
```

**6. Replace these files with newly compiled copies (they are located in /usr/obj/usr/src/ subfolders). If you use remote connection to server console, execute the below commands as a single command as shown in the example below:**

```
# cd /usr/obj/usr/src/ ; \  
# cp ./secure/lib/libcrypto/libcrypto.so.4 /lib/libcrypto.so.4 ; \  
# cp ./secure/lib/libssl/libssl.so.4 /usr/lib/libssl.so.4 ; \  
# chflags noschg /lib/libcrypt.so.3 ; \  
# cp ./lib/libcrypt/libcrypt.so.3 /lib/libcrypt.so.3 ; \  
# chflags schg /lib/libcrypt.so.3
```

**7. Reboot the server.**

---

## Including Directives into Web Server Configuration File

You can include domain-specific Apache configuration directives into web server configuration file. In Parallels Plesk Panel each domain has virtual hosts configuration stored in a separate file `httpd.include`.

On all Linux systems, this file is located in the directory `/var/www/vhosts/<domain-name>/conf/`.

On FreeBSD systems, this file is located in the directory `<VIRTUAL_HOSTS_D>/<domain-name>/conf/`.

If you upgraded from Parallels Plesk Panel version 7.5.4 or earlier, try looking for this file in the directory `<VIRTUAL_HOSTS_D>/<domain-name>/conf/`.

Check the `HTTPD_VHOSTS_D` variable in `/etc/psa/psa.conf`.

---

**Note:** You can change the location of virtual host directories using the `transvhosts.pl` utility, which is located either in `/usr/local/psa/bin/` or `/opt/psa/bin/` directory, depending on your operating system.

---

This file is overwritten each time the virtual host configuration is changed, thus any manual alterations made to the file are discarded. To use custom directives or redefine those inserted by Parallels Plesk Panel, you need to create the files `vhost.conf` and/or `vhost_ssl.conf` with necessary directives in the directory `<VIRTUAL_HOSTS_D>/<domain-name>/conf/` for a domain, and `<VIRTUAL_HOSTS_D>/<domain-name>/subdomains/<subdomain-name>/conf/` for a subdomain.

If any of these files exist by the time the main configuration file is generated, Parallels Plesk Panel inserts the appropriate `Include` directive into the HTTP and/or HTTPS virtual host context respectively. For security reasons, only root can create the `vhost.conf` and `vhost_ssl.conf` files.

For the changes to take effect, you need to run the following command:

```
/plesk_installation_directory/admin/sbin/websrvmng-reconfigure-vhost-vhost-name=<domain_name>
```

---

**Important:** Note that modification of `httpsd.conf` and `php.ini` files can result in improper Parallels Plesk Panel functioning or failure, cause damage and loss of data. It is highly recommended that you do not modify these files or any part of them. If you require custom modifications to be applied to the configuration, please perform them in the following files:

```
# /var/www/vhosts/<domain-name>/conf/vhost.conf
# /var/www/vhosts/<domain-name>/conf/vhost_ssl.conf
# /var/www/vhosts/<domain-name>/subdomains/<subdomain-name>/conf/vhost.conf
```

---

---

## Customizing httpd.include for Domains

In Parallels Plesk Panel each domain has virtual hosts configuration stored in a separate file:

```
<VIRTUAL_HOSTS_D>/<domain-name>/conf/httpd.include
```

When you need to use some specific configurations for a domain or a subdomain, it's not a good idea to include them directly in `httpd.include` file. This file is overwritten each time the virtual host configuration is changed, thus any manual alterations made to the file are discarded.

➤ **To use custom directives or redefine those inserted by Parallels Plesk Panel, do the following:**

1. Create the files `vhost.conf` and/or `vhost_ssl.conf` with necessary directives in the `<VIRTUAL_HOSTS_D>/<domain-name>/conf/` directory.

If any (or both) of these files exist by the time the main configuration file is generated, Parallels Plesk Panel inserts the appropriate directive:

```
Include <VIRTUAL_HOSTS_D>/<domain-name>/conf/vhost.conf
```

or

```
Include <VIRTUAL_HOSTS_D>/<domain-name>/conf/vhost_ssl.conf
```

into the HTTP and/or HTTPS virtual host context respectively.

For security reasons, only `root` can create the `vhost.conf` and `vhost_ssl.conf` files.

2. For the changes to take effect, run the following:

```
# /usr/local/psa/admin/sbin/websrvnmng--reconfigure-vhost-vhost-  
name=<domain_name>
```

For the changes to be implemented for all domains, run the following:

```
# /usr/local/psa/admin/bin/websrvnmng -a
```

---

## Preventing Graphics Hotlinking on a Web Site

Bandwidth theft or hotlinking is a direct linking to web site's files (images, video, etc.). It can be prevented with the `mod_rewrite` module. Place rules like below into the `vhost.conf` or `.htaccess` files for the domain (for example `www.example.com`):

```
RewriteEngine on  
RewriteCond % !^$  
RewriteCond % !^http://(www\.)?example\.com(/)?\.*$ [NC]  
RewriteRule \.(gif|jpg|jpeg|png|swf)$ - [NC,F]
```

---

# Apache Port Change

You can change Apache web server port to use a lightweight high-performance web server, such as `nginx`, as a front-end web server, and move Apache web server to back-end.

To change Apache web server port, use the `webservmng` utility with the following options:

- `--set-http-port` - set a custom http port;
- `--get-http-port` - get a custom http port;
- `--set-https-port` - set a custom https port;
- `--get-https-port` - get a custom https port.

---

**Note:** The default port values in Parallels Plesk Panel are 80 for `http` and 443 for `https`.

---

## Examples

- To change Apache web server http port to 8080, issue the following command:

```
# /usr/local/psa/admin/sbin/webservmng-set-http-port-port=8080
# /usr/local/psa/admin/sbin/webservmng-reconfigure-all
# /usr/local/psa/admin/sbin/webmailmng-disable-name=horde
# /usr/local/psa/admin/sbin/webmailmng-enable-name=horde
# /usr/local/psa/admin/sbin/webmailmng-disable-name=atmail
# /usr/local/psa/admin/sbin/webmailmng-enable-name=atmail
# /usr/local/psa/admin/sbin/webmailmng-disable-name=atmailcom
# /usr/local/psa/admin/sbin/webmailmng-enable-name=atmailcom
```

- To get a custom Apache web server http port, issue the following command:

```
# /usr/local/psa/admin/sbin/webservmng-get-http-port
```

## Examples of configuration files for `nginx` web server on Debian 5

- Web server configuration (on page 69)
- Domains configuration (on page 70)
- Subdomains configuration (on page 72)
- Webmail configuration (on page 74)
- Mailman configuration (on page 75)

When you use Sitebuilder with Parallels Plesk Panel and change Apache web server port, you should reconfigure Sitebuilder (on page 76) to provide integration with the changed port.

## Known issues

When `nginx` is installed as a front-end web server and Apache is moved to back-end, the following Parallels Plesk Panel components are not working:

- Publishing dynamic content in Sitebuilder
- Server's default page
- Tomcat via Apache
- Statistics for cached static content is not calculated

**In this section:**

Example of Web Server Configuration File ..... 69  
Example of Domain Configuration File ..... 70  
Example of Subdomain Configuration File..... 72  
Example of Webmail Configuration File..... 74  
Example of Mailman Configuration File ..... 75  
Configuring Sitebuilder for Work With Changed Apache Port ..... 76

## Example of Web Server Configuration File

The following is the example of configuration file for the `nginx` web server on Debian 5:

```
# cat /etc/nginx/nginx.conf
user www-data;
worker_processes 8;

timer_resolution 100ms;
worker_rlimit_nofile 8192;
worker_priority -5;

error_log /var/log/nginx/nginx.error.log;
events {
worker_connections 1024;
use epoll;
}

http {
include /etc/nginx/mime.types;
default_type application/octet-stream;
    log_format main '$remote_addr - $remote_user [$time_local] \'
        '$request' $status $bytes_sent \'
        '$http_referer' '$http_user_agent' \'
        '$gzip_ratio'';

log_format download '$remote_addr - $remote_user [$time_local] \'
'$request' $status $bytes_sent \'
'$http_referer' '$http_user_agent' \'
'$http_range' '$sent_http_content_range'';
    client_header_timeout 10m;
    client_body_timeout 10m;
    send_timeout 10m;
    proxy_read_timeout 10m;
    proxy_connect_timeout 75;
    proxy_send_timeout 10m;

    connection_pool_size 256;
    client_header_buffer_size 1k;
    large_client_header_buffers 4 2k;
    request_pool_size 4k;

gzip on;
gzip_min_length 1100;
gzip_buffers 4 8k;
gzip_http_version 1.1;
gzip_proxied any;
gzip_types text/plain application/xml application/x-javascript text/css;
output_buffers 1 32k;
postpone_output 1460;

sendfile on;
tcp_nopush on;
tcp_nodelay on;

keepalive_timeout 5 20;
ignore_invalid_headers on;
resolver 127.0.0.1;
```

```
include /etc/nginx/sites-enabled/*;  
}
```

## Example of Domain Configuration File

The following is the example of configuration file for a domain in Parallels Plesk Panel on Debian 5:

**Note:** Each domain created in Parallels Plesk Panel should be configured separately.

**Note:** In this example replace <domain.name> with your domain name. In the `server_name` line, include the domain name and all domain aliases separated by spaces.

```
# cat /etc/nginx/vhost.template  
server {  
listen 80;  
server_name <domain.name> www.<domain.name>;  
access_log /var/log/nginx/<domain.name>.access.log main;  
#Main location  
location / {  
proxy_pass http://<domain.name>:8080/;  
proxy_redirect default;  
proxy_set_header Host $host;  
proxy_set_header X-Real-IP $remote_addr;  
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
client_max_body_size 10m;  
client_body_buffer_size 128k;  
proxy_connect_timeout 90;  
proxy_send_timeout 90;  
proxy_read_timeout 90;  
  
proxy_buffer_size 4k;  
proxy_buffers 4 32k;  
proxy_busy_buffers_size 64k;  
proxy_temp_file_write_size 64k;  
  
open_file_cache max=1024 inactive=600s;  
open_file_cache_valid 2000s;  
open_file_cache_min_uses 1;  
open_file_cache_errors on;  
    }  
  
# Static files location  
location ~*  
^.\+\. (jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|xls|exe|pdf|ppt|txt|tar|w  
av|bmp|rtf|js|ico|swf)$ {  
root /var/www/vhosts/<domain.name>/httpdocs;  
expires 30d;  
    }  
}
```

To automate domains' configuration files generation, use **Home > Event Manager**. Create an Event Handler for the **Physical hosting created** event with normal priority executed by the `root` user with the command:

```
/bin/bash /root/domain_create.sh
```

where /root/domain\_create.sh is the following:

```
# cat /root/domain_create.sh
#!/bin/bash
echo "-----" >> /tmp/event_handler.log
/bin/date >> /tmp/event_handler.log # information on the event date and
time
/usr/bin/id >> /tmp/event_handler.log # information on the user, on behalf
of which the script was executed (to ensure control)
/bin/echo "Domain created ${NEW_DOMAIN_NAME}" >> /tmp/event_handler.log #
Domain's name
/bin/cat /etc/nginx/vhost.template | /bin/sed -e
"s/<domain.name>/${NEW_DOMAIN_NAME}/g" > /etc/nginx/sites-
available/${NEW_DOMAIN_NAME}
/bin/echo "Result of domain config creation is "$? >>
/tmp/event_handler.log
/bin/ln -s /etc/nginx/sites-available/${NEW_DOMAIN_NAME} /etc/nginx/sites-
enabled/${NEW_DOMAIN_NAME}
/bin/echo "Result of domain config enabling is "$? >>
/tmp/event_handler.log
/etc/init.d/nginx reload
/bin/echo "Result of nginx reloading is "$? >> /tmp/event_handler.log
```

## Example of Subdomain Configuration File

The following is the example of configuration file for a subdomain in Parallels Plesk Panel on Debian 5:

**Note:** Each subdomain created in Parallels Plesk Panel should be configured separately.

**Note:** In this example replace `<subdomain>` and `<domain.name>` with your subdomain and domain names respectively.

```
# cat /etc/nginx/subdomain.template
server {
listen 80;
server_name <subdomain>.<domain.name>;
access_log /var/log/nginx/<domain.name>.access.log main;
#Main location
location / {
proxy_pass http://<subdomain>.<domain.name>:8080/;
proxy_redirect default;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
client_max_body_size 10m;
client_body_buffer_size 128k;
proxy_connect_timeout 90;
proxy_send_timeout 90;
proxy_read_timeout 90;

proxy_buffer_size 4k;
proxy_buffers 4 32k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 64k;

open_file_cache max=1024 inactive=600s;
open_file_cache_valid 2000s;
open_file_cache_min_uses 1;
open_file_cache_errors on;
    }

# Static files location
location ~*
^.\. (jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|xls|exe|pdf|ppt|txt|tar|wav|bmp|rtf|js|ico|swf)$ {
root /var/www/vhosts/<domain.name>/subdomains/<subdomain>/httpdocs;
expires 30d;
    }
}
```

To automate subdomains' configuration files generation, use **Home > Event Manager**. Create an Event Handler for the **Subdomain created** event with normal priority executed by the `root` user with the command:

```
/bin/bash /root/subdomain_create.sh
```

where `/root/subdomain_create.sh` is the following:

```
# cat /root/subdomain_create.sh
#!/bin/bash
echo "-----" >> /tmp/event_handler.log
/bin/date >> /tmp/event_handler.log # information on the event date and
time
/usr/bin/id >> /tmp/event_handler.log # information on the user, on behalf
of which the script was executed (to ensure control)
/bin/echo "Subdomain ${NEW_SUBDOMAIN_NAME} for domain ${NEW_DOMAIN_NAME}
created" >> /tmp/event_handler.log # Subdomain's name
/bin/cat /etc/nginx/subdomain.template | /bin/sed -e
"s/<domain.name>/${NEW_DOMAIN_NAME}/g" | /bin/sed -e
"s/<subdomain>/${NEW_SUBDOMAIN_NAME}/g" > /etc/nginx/sites-
available/${NEW_SUBDOMAIN_NAME}.${NEW_DOMAIN_NAME}
/bin/echo "Result of subdomain config creation is "$? >>
/tmp/event_handler.log
/bin/ln -s /etc/nginx/sites-
available/${NEW_SUBDOMAIN_NAME}.${NEW_DOMAIN_NAME} /etc/nginx/sites-
enabled/${NEW_SUBDOMAIN_NAME}.${NEW_DOMAIN_NAME}
/bin/echo "Result of subdomain config enabling is "$? >>
/tmp/event_handler.log
/etc/init.d/nginx reload
/bin/echo "Result of nginx reloading is "$? >> /tmp/event_handler.log
```

## Example of Webmail Configuration File

The following is the example of configuration file for webmail clients on Debian 5:

---

**Note:** You can create one configuration file for all webmail clients.

**Note:** In this example replace <IP-address> with your IP address.

---

```
server {
listen 80;
server_name webmail.*;
access_log /var/log/nginx/webmail.log main;

#Main location
location / {
proxy_pass http://<IP-address>:8080;
proxy_redirect default;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
client_max_body_size 10m;
client_body_buffer_size 128k;
proxy_connect_timeout 90;
proxy_send_timeout 90;
proxy_read_timeout 90;

proxy_buffer_size 4k;
proxy_buffers 4 32k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 64k;

open_file_cache max=1024 inactive=600s;
open_file_cache_valid 2000s;
open_file_cache_min_uses 1;
open_file_cache_errors on;
    }
}
```

## Example of Mailman Configuration File

The following is the example of configuration file for Mailman on Debian 5:

---

**Note:** In this example replace <IP-address> with your IP address.

---

```
server {
listen 80;
server_name lists.*;
access_log /var/log/nginx/lists.log main;

#Main location
location / {
proxy_pass http://<IP-address>:8080;
proxy_redirect default;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
client_max_body_size 10m;
client_body_buffer_size 128k;
proxy_connect_timeout 90;
proxy_send_timeout 90;
proxy_read_timeout 90;

proxy_buffer_size 4k;
proxy_buffers 4 32k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 64k;

open_file_cache max=1024 inactive=600s;
open_file_cache_valid 2000s;
open_file_cache_min_uses 1;
open_file_cache_errors on;
    }
}
```

## Configuring Sitebuilder for Work With Changed Apache Port

When you use Sitebuilder with Parallels Plesk Panel and change Apache web server port, you should reconfigure Sitebuilder to provide integration with the changed port.

### ➤ *To configure Sitebuilder:*

**Note:** In the commands below, replace `<hostname>` with your hostname. These commands are an example for Debian 5.

1. Change vhost for Sitebuilder in `conf.d/` of Apache web server:

```
/opt/sitebuilder/utils/configure-httpd_port 8080
```

2. Change the `application_url` parameter in Sitebuilder configuration file:

```
host# grep application_url /opt/sitebuilder/config
application_url = "http://sitebuilder.<hostname>:8080"
```

3. Change link to Sitebuilder in Parallels Plesk Panel database:

```
# echo "select * from SBConfig where param_name='url';"| mysql -uadmin -
p`cat /etc/psa/.psa.shadow` psa
param_name      param_value
url             http://sitebuilder.<hostname>:8080/ServiceFacade/
echo "update SBConfig SET
param_value='http://sitebuilder.<hostname>:8080/ServiceFacade/' where
param_name='url';"| mysql -uadmin -p`cat /etc/psa/.psa.shadow` psa
```

The following is the example of configuration file for Sitebuilder on Debian 5:

**Note:** In this example replace `<IP-address>` with your IP address.

```
server {
listen 80;
server_name sitebuilder.*;
access_log /var/log/nginx/sitebuilder.log main;

#Main location
location / {
proxy_pass http://<IP-address>:8080;
proxy_redirect default;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
client_max_body_size 10m;
client_body_buffer_size 128k;
proxy_connect_timeout 90;
proxy_send_timeout 90;
proxy_read_timeout 90;

proxy_buffer_size 4k;
proxy_buffers 4 32k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 64k;
```

```
open_file_cache max=1024 inactive=600s;  
open_file_cache_valid 2000s;  
open_file_cache_min_uses 1;  
open_file_cache_errors on;  
    }  
}
```

# Changing Tomcat Java Connector Ports

The default port numbers for Coyote and Warp connectors in Parallels Plesk Panel are 9080 and 9008.

If you want Tomcat Java to work on other ports (e.g. 8090 and 8009), you should connect to the Parallels Plesk Panel database and add two parameters to the database as in the following example:

```
insert into misc (param,val) values ('coyote_connector_port', '8090');
insert into misc (param,val) values ('warp_connector_port', '8009');
```

Alternatively, you can use the `dbclient.exe` utility to add the information to the Parallels Plesk Panel database. For information about using the `dbclient.exe` utility, consult *Parallels Plesk Panel for Windows Command Line Interface Reference*.

---

**Note:** It is recommended that you change the Tomcat Java ports right after Parallels Plesk Panel is installed on server, or prior to enabling the Tomcat Java service for your domains.

---

# Configuring Mail

## In this chapter:

Configuring a Mailing List Where Only Members are Allowed to Post to.....	80
Importing a List of E-mail Addresses into a Mailing List.....	80
Limiting the Number of Recipients of a Mail Message .....	81
Training SpamAssassin for All Mail Accounts on the Server.....	82
Limiting the Maximum Number of Child Processes for spamd.....	83
Fighting Against Spam on Qmail Mail Server .....	84
Restoring Mail Configuration .....	86
Installing Custom SSL Certificates for Qmail or Courier-IMAP Mail Servers .....	87

---

## Configuring a Mailing List Where Only Members are Allowed to Post to

By default, when you create a mailing list, everyone may send correspondence to this list. If you need to configure a mailing list where only members are allowed to send mail to, you can do this through the WEB Mailman interface.

➤ ***To configure a mailing list where only members are allowed to post to:***

1. Log in to the WEB Mailman interface as the list administrator.
2. Enable the **Restrict posting privilege to list members** option.

---

**Note:** By default a mailing list is created with the Posts must be approved by an administrator option enabled. That means all messages must be approved by the moderator before they are posted to the list. So, if this option is disabled and unwanted mail is posted to the list, you may enable it back and moderate incoming messages.

---

Please see Mailman documentation for more information at <http://www.gnu.org/software/mailman/docs.html>.

---

## Importing a List of E-mail Addresses into a Mailing List

If you need to import a number of e-mail addresses into a mailing list, adding them one at a time can take a long time. To automate this task you can use Parallels Plesk Panel creation utilities. To add several e-mail addresses to the mailing list, run the following command:

```
# /usr/local/psa/bin/maillist.sh-update <mailing list> -members  
add:<e-mail 1>[,<e-mail 2>,...,<e-mail N>]
```

---

## Limiting the Number of Recipients of a Mail Message

Since Parallels Plesk Panel 8.4 version it is possible to limit maximum number of recipients for an e-mail message.

➤ ***To prevent your users from sending mass e-mail:***

1. Create a file named `maxrcpt` in the directory `$QMAIL_ROOT_D/qmail/control/`, where `$QMAIL_ROOT_D` is the location defined in the `/etc/psa/psa.conf` file.
2. Type the number of allowed recipients in this file and save it.

---

**Note:** The number defined in the `maxrcpt` file also affects sending messages to mailing list or mail group subscribers. That is, if you set the value to 100, then only 100 subscribers will receive the message sent to a mailing list or a mail group.

---

When you no longer need to restrict the number of recipients, delete the `maxrcpt` file.

---

## Training SpamAssassin for All Mail Accounts on the Server

You can manually train SpamAssassin for all mail accounts on the server from the command line.

➤ ***To train SpamAssassin for all mail names on the server:***

1. Store spam and ham (non-spam) messages in two different folders, for example `spam_mails` and `ham_mails`.
2. Train SpamAssassin for one mailbox using the messages from these folders:

```
# cd /path/to/spam_mail/  
# for message in * ; do /usr/local/psa/admin/sbin/spammng-bayes-  
mailname=mailname@domain.com-spam=$message ; done  
# cd /path/to/ham_mail/  
# for message in * ; do /usr/local/psa/admin/sbin/spammng-bayes-  
mailname=mailname@domain.com-ham=$message ; done
```

3. Repeat this command for every mailbox on the server or just copy bayes bases (`./domain.com/mailname/.spamassassin/bayes_*`) from this mailbox to other mailboxes with the following command:

```
# find /var/qmail/mailnames/ -mindepth 2 -maxdepth 2 -type d -exec /bin/cp  
-f /var/qmail/mailnames/domain.com/mailname/.spamassassin/bayes_*  
{}/.spamassassin/ \;
```

where `domain.com` and `mailname` should be replaced with the real domain name and mail name.

## Limiting the Maximum Number of Child Processes for spamd

If there is a large spam attack, then too many processes are started by spam deferral daemon `spamd` and the system can run out of resources. In Parallels Plesk Panel 7.5 and Parallels Plesk Panel 8.0 you can limit the number of simultaneously running SpamAssassin processes with the `SPAMASSASSIN_MAX_CHILDREN` option in `/etc/psa/psa.conf`:

```
SPAMASSASSIN_MAX_CHILDREN 5
```

Specify a desired value and restart `psa-spamassassin`.

If the line is omitted then the default value for SpamAssassin 3.x is 5.

Since Parallels Plesk Panel 8.1 this value can be managed through Parallels Plesk Panel. Use the **The maximum number of worker spamd processes to run (1-5)** option on the **Server > Settings > SpamFilter** page in Parallels Plesk Panel 8.x, . The value is stored in the `misc` table of the `psa` database:

```
# mysql -uadmin -p'cat /etc/psa/.psa.shadow' psa -e "select * from misc where param='spamfilter_max_children'"
```

```
+-----+-----+
| param                | val |
+-----+-----+
| spamfilter_max_children | 5   |
+-----+-----+
```

## Fighting Against Spam on Qmail Mail Server

When unsolicited e-mails, or spam, are simultaneously sent indiscriminately to multiple mail boxes on your server, there can be too many messages in the queue. Then the server is overloaded with spam, the mail is delivered slowly.

### ➤ *To get rid of spam on your Qmail mail server:*

1. Make sure that all domains have the **Mail to nonexistent user** option set to **Reject**.

This option is available since Parallels Plesk Panel 7.5.3 and can be changed for all the domains using group operations: select the domains, click **Modify Selected**, in the **Preferences** section select **Switch on** for the **Mail to nonexistent user** option and select the **Reject** value for it.

2. Make sure that there are no untrusted IP addresses or networks in the white list.

To do this, go to **Home > Mail Server Settings > White List tab**. To remove untrusted IP addresses or networks, select them in the list and click **Remove Selected**.

3. Check how many messages there are in the Qmail queue with:

```
# /var/qmail/bin/qmail-qstat
messages in queue: 27645
messages in queue but not yet preprocessed: 82
```

If there are too many messages in the queue, try to find out where the spam is coming from. If the mail is being sent by an authorized user, but not from a PHP script, you can find out which user sent most of the messages with the following command:

```
# cat /usr/local/psa/var/log/maillog |grep -I smtp_auth |grep -I user |awk '{print $11}' |sort |uniq -c |sort -n
```

Note that the SMTP authorization option should be enabled on the server to see these records. The path to maillog may be different depending the OS you use.

4. Use the `qmail-qread` utility to read the messages headers:

```
# /var/qmail/bin/qmail-qread
18 Jul 2005 15:03:07 GMT #2996948 9073 <user@domain.com> bouncing
done remote user1@domain1.com
done remote user2@domain2.com
done remote user3@domain3.com
....
```

The `qmail-qread` utility shows messages' senders and recipients. If a message has too many recipients, then it is most probably spam.

5. Try to find the message in the queue by it's ID (for example, the message ID is #1234567):

```
# find /var/qmail/queue/mess/ -name 1234567
```

6. Look into the message and find the first from the end `Received` line. It is where the message was initially sent from.

- If you find something like:

```
Received: (qmail 19514 invoked by uid 12345); 10 Sep 2008 17:48:22
+0700
```

it means that this message was sent via a CGI script by user with UID 12345. Use this UID to find a corresponding domain:

```
# grep 12345 /etc/passwd
```

- Received lines like:

```
Received: (qmail 19622 invoked from network); 10 Sep 2008 17:52:36
+0700
```

```
Received: from external_domain.com (192.168.0.1)
```

mean that the message was accepted for delivery via SMTP and the sender is an authorized mail user.

- If Received line contains an UID of an apache user (for example invoked by uid 48), it means that the spam was sent via an PHP script. In this case you can try to find the spammer using information from the spam e-mails (from/to addresses, subjects, etc). But usually to find the spam source is very hard in this case. If you are sure that some script is sending spam at the current moment (the queue grows very fast), you can use this little script to find out what PHP scripts are running in real-time:

```
# lsof +r 1 -p `ps axww | grep httpd | grep -v grep | awk ` {
if(!str) { str=$1 } else { str=str","$1}}END{print str}' ` | grep
vhosts | grep php
```

To try to find out from what folder the PHP script that sends mail was run, create `/var/qmail/bin/sendmail-wrapper` script with the following content:

```
#!/bin/sh
(echo X-Additional-Header: $PWD ;cat) | tee -a
/var/tmp/mail.send|/var/qmail/bin/sendmail-qmail "$@"
```

Note, the paths can slightly differ depending on your OS and Parallels Plesk Panel version.

Create a log file `/var/tmp/mail.send` and grant it `a+rw` rights, make the wrapper executable, rename old `sendmail` and link it to the new wrapper:

```
# touch /var/tmp/mail.send
# chmod a+rw /var/tmp/mail.send
# chmod a+x /var/qmail/bin/sendmail-wrapper
# mv /var/qmail/bin/sendmail /var/qmail/bin/sendmail-qmail
# ln -s /var/qmail/bin/sendmail-wrapper /var/qmail/bin/sendmail
```

Wait for about an hour and revert `sendmail` back:

```
# rm -f /var/qmail/bin/sendmail
# ln -s /var/qmail/bin/sendmail-qmail /var/qmail/bin/sendmail
```

Examine the `/var/tmp/mail.send` file. There should be lines starting with `X-Additional-Header` pointing out to domains' folders where the script that sends the mail is located.

You can see all the folders where mail PHP scripts were run from with the following command:

```
# grep X-Additional /var/tmp/mail.send | grep `cat
/etc/psa/psa.conf | grep HTTPD_VHOSTS_D | sed -e
`s/HTTPD_VHOSTS_D//` `
```

If you see no output from the command above, it means that no mail was sent using `PHP mail()` function from the Parallels Plesk Panel virtual hosts directory.

---

## Restoring Mail Configuration

Sometimes, Parallels Plesk Panel mail server configuration becomes corrupt and it is necessary to restore it. The restoration is carried out by internal `mchk` utility, intended for use by Parallels Plesk Panel. However, as the administrator, you can use it for restoring the Qmail and Courier-imap configuration when needed.

By default `mchk` is running in the background mode. To execute it in the foreground, use the `-v` option. For example:

```
/usr/local/psa/admin/sbin/mchk -v
```

---

**Note:** You may not wish to restore SpamAssassin settings for mail accounts, as it requires running Perl interpreter. To speed up restoring use the `—without-spam` option.

---

---

# Installing Custom SSL Certificates for Qmail or Courier-IMAP Mail Servers

To securely exchange mail data with Parallels Plesk Panel server, you may need to install custom SSL certificates on the Parallels Plesk Panel server. Specifically, SSL certificates can be installed for the Qmail mail transfer agent and the Courier-IMAP mail server that supports the IMAP and POP3 protocols.

To install custom SSL certificates, you need to download the certificates to the Parallels Plesk Panel server and then replace the installed default SSL certificates for Qmail and Courier-IMAP servers with the downloaded custom certificates.

This section describes procedures for installing custom SSL certificates for Qmail and Courier-IMAP servers.

## In this section:

Installing SSL Certificate for Qmail .....	88
Installing SSL Certificates for Courier-IMAP Mail Server .....	90

## Installing SSL Certificate for Qmail

➤ **To install a custom SSL certificate for Qmail on a Parallels Plesk Panel server:**

1. Create a combined `.pem` certificate file.

To create a combined `.pem` certificate file, start your favorite text editor and paste the contents of each certificate file and the private key in the file in the following order:

- a. The private key
- b. The primary certificate
- c. The intermediate certificate
- d. The root certificate

Make sure that you include the *begin* and *end* tags of the key and each certificate including the dash lines. The resulting text should look like this:

```
-----BEGIN RSA PRIVATE KEY-----
.....
(Your Private Key here)
.....
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
(Your Primary SSL certificate here)
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
(Your Intermediate certificate here)
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
(Your Root certificate here)
.....
-----END CERTIFICATE-----
```

2. Save the combined certificate file as `plesk.pem`.
3. Log in to a Parallels Plesk Panel server through SSH as a root user.
4. Download the combined certificate file `plesk.pem`.
5. Make a backup copy of the existing default SSL certificate for Qmail.

For example for RedHat or Fedora operating systems, the SSL certificate file that you need to back up is `var/qmail/control/servercert.pem`.

---

**Note:** For other operating systems, the default certificate file location may be different.

---

6. Open the default certificate file `/var/qmail/control/servercert.pem` by using your favorite text editor and replace the contents of the file with the content of the combined certificate file `plesk.pem`.
7. Save and close the file.
8. To finish the certificate installation, restart Qmail.

## Installing SSL Certificates for Courier-IMAP Mail Server

➤ **To install a custom SSL certificate for the Courier-IMAP (IMAP/POP3) mail server on a Parallels Plesk Panel server:**

1. Log in to a Parallels Plesk Panel server through SSH as a root user.
2. Download one or more SSL certificate files that you want to install.

---

**Note:** IMAP and POP3 each require separate certificate files, but both files can contain same certificate.

---

3. Make a backup copy of the existing default SSL certificate for the Courier-IMAP mail server.

For example for RedHat or Fedora operating systems, you need to back up the following default SSL certificate files:

- `/usr/share/courier-imap/imapd.pem` - the certificate enables secure data transfers through IMAP protocol.
- `/usr/share/courier-imap/pop3d.pem` - the certificate enables secure data transfers through POP3 protocol.

---

**Note:** For other operating systems, the default certificate file locations may be different.

---

4. Open a default certificate file by using your favorite text editor and replace the contents of the file, with the content of the SSL certificate file that you want to install.

For example, the content to be copied from a custom SSL certificate and pasted in lieu of a default certificate file body should look like this:

```
-----BEGIN CERTIFICATE-----
MIIB8TCCAzsCBEUpHKkwDQYJKoZIhvcNAQEEBQAwwYExCzAJBgNVBAYTAlJPMQww
.....
.....
eNpAIeF34UctLcHkZJGIK6b9Gktm
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDv6i/mxtS2B2PjShArtOAmDRoEcCWA/LH1GcrbW14zdbmIqrx
.....
.....
faXRHcG37TkvglUZ3wgy6eKuyrDi5gkwV8WAuaoNct5j5w==
-----END RSA PRIVATE KEY-----
```

5. Save and close the file.
6. To finish the certificate installation, restart Courier-IMAP.

# Installing Adobe ColdFusion

➤ ***To install Adobe ColdFusion:***

1. Once you have purchased a ColdFusion distribution package, copy it to your Parallels Plesk Panel server.
2. Login as root to the server and run the coldfusion-70-lin.bin installation file.
3. Choose your language: type the appropriate number and press ENTER.
4. Read the Introduction and press ENTER to continue.
5. Read carefully the end user license agreement and accept it by typing 'y' and pressing ENTER. A pre-installation check will be performed.
6. To continue with installation, press ENTER.
7. Choose installation type. Select the **Install new version of ColdFusion MX with a serial number** option: type '1' and press ENTER, and then type in the serial number. Press ENTER.
8. Select the type of installation. To install ColdFusion on the server, leave the **Server configuration** option selected: type 1 and press ENTER.
9. Type 2 and then press ENTER to confirm that you do not yet have Adobe ColdFusion installed.
10. To continue with installation, type 4 and press ENTER.
11. Specify an absolute path to the installation folder. The default installation folder is /opt/coldfusionmx7. Press ENTER.
12. If you had earlier versions of ColdFusion installed, you can choose to migrate your settings. Otherwise press ENTER to continue.
13. Type 2 and press ENTER to continue with installation.
14. Leave the **Runtime user name** field blank. Press ENTER.
15. Specify the password that you will use to control access to the ColdFusion MX Administrator.
16. Disable the ColdFusion Remote Development Service (RDS): type 'n' and press ENTER.
17. To continue with installation, press ENTER.
18. Once the installation is completed, press ENTER to exit the installer.

19. If your server is running Linux for 64-bit platforms, modify the files `/etc/init.d/coldfusionmx7` and `[path_to_coldfusion_installation]/bin/coldfusion` — comment out the following lines (that is, put a # symbol in the beginning of each of the following lines):

```
SUSEFLAG=`grep `SuSE Linux 8.1\|UnitedLinux 1.0` /etc/SuSE-
release
/etc/UnitedLinux-release /etc/UnitedLinux-release 2>
/dev/null`
if [ ! "$SUSEFLAG" ]; then
LD_ASSUME_KERNEL=2.2.9
export LD_ASSUME_KERNEL
fi
```

20. Login to Parallels Plesk Panel as the administrator.
21. Go to **Home > Updates**.
22. Click a link corresponding to the appropriate release version.
23. Select the check box corresponding to the **ColdFusion support for Plesk** item, and click **Install**. Confirm the installation when prompted.
24. Once the selected components are installed, click the **ColdFusion Settings** icon.
25. Specify the path to ColdFusion installation directory and click **OK**.

---

**Note:** JRun for ColdFusion 8 can resolve 'localhost' to IPv6, while Apache resolves it to IPv4. To make ColdFusion work, switch it to IPv4 in the `/etc/hosts` file. To do this, in the `/etc/hosts` file find the entry:

```
::1    yourdomain.yourhostname.com    yourdomain
localhost.localdomain localhost
```

and remove `localhost.localdomain` and `localhost`. Then restart Apache.

---

➤ **To uninstall Adobe ColdFusion from your server:**

1. Log in as root.
2. Issue the following command at the prompt:  
`/opt/coldfusionmx7/uninstall/uninstall`
3. To confirm deinstalling, press ENTER.
4. When the program completes, remove any remaining files and directories in the `/opt/coldfusionmx7/` directory.
5. Log in to Parallels Plesk Panel as the administrator, go to **Home > Server Components**.

6. Click the **Refresh** icon. The list of installed components will be updated. Your control panel will find out that you deinstalled ColdFusion and will remove the ColdFusion related controls from the control panel screens or will make them unselectable and mark them with the **(component is not installed)** comment.

7. Issue the command at the server shell:

```
/usr/local/psa/admin/bin/websrvnmng -a
```

For Debian and Ubuntu systems, issue the command:

```
/opt/psa/admin/bin/websrvnmng -a
```

# Using Open Relay Option for Your Mail Server

By default, the open relay option for the mail server is disabled in Parallels Plesk Panel. You can enable it by using the `root.controls.lock` file located in `PRODUCT_DATA_D\var` directory. However we do not recommend enabling this option because an open relay can make it possible for an unscrupulous senders to route large volumes of spam.

➤ ***To enable open relay, follow these steps:***

1. Open the `root.controls.lock` file.
2. Remove the `/server/mail.php3:relay_open` line and save the file.

# Configuring APS Applications Catalog

When you log in to Parallels Plesk Panel as administrator and click the **Applications** shortcut in the navigation pane, you are taken to the Application Vault screen, which provides links for downloading and installing applications on the server.

There is the **Add Applications from APS Catalog** link for downloading individual applications from the APS Catalog, and there are links for downloading application bundles, where all applications are categorized and sorted by popularity. There are three predefined application bundles: 50 most popular applications, next 50 most popular applications, and all applications.

You can do the following:

- Redefine the set of applications included into each bundle, or remove the links for downloading application bundles from the user interface.
- Specify what applications and application categories should be presented in the APS catalog.

➤ ***To remove all links for downloading application bundles from the user interface:***

On the server file system, go to the directory `<parallels_plesk_panel_installation_directory>\etc` and create there an empty file named `apscatalog_presets.conf`.

➤ ***To redefine the set of application bundles and to specify what applications should be included into each bundle:***

1. On the server file system, go to the directory `<parallels_plesk_panel_installation_directory>\etc\` and create a text file named `apscatalog_presets.conf`.
2. Add the required entries to the file.

You should first add a bundle's name in brackets, up to three entries, which can be `[mostused]`, `[lessused]`, and `[all]`. Then you should type the names of applications to be included into the corresponding bundle, one application name per line.

The resulting text file should look like in the following example:

```
[mostused]
joomla
WordPress
Drupal
```

```
[lessused]
VideoDB
phpMyChatPlus
```

```
[all]
joomla
WordPress
Drupal
movabletype
SugarCRM
VideoDB
phpMyChatPlus
```

### 3. Save the file.

➤ ***To specify what applications and application categories should be presented in the APS catalog:***

1. On the server file system, go to the directory `<parallels_plesk_panel_installation_directory>\etc\` and create a text file named `apscatalog_categories.conf`.

2. Add the required entries to the file.

You should first add a top-level category name in brackets, like `[Web]`. Then, you should add a name of a nested sub-category, for example, `[Web/Blog]`. After that, you can type the names of applications that belong to that category, one name per line.

Also, to be sure that no other applications (except for those that you specified) are shown in the server's APS Catalog and application vaults of other users, you can add to the file the line `otherApplicationsPolicy = hide`, and in the next line, add the line `hideLevel = admin`. If you want to hide other applications only from your customers, but not from your own application vault, then use the line `hideLevel = client`.

The resulting text file should look like in the following example:

```
otherApplicationsPolicy = hide
hideLevel = admin
[Web]
```

```
[Web/Blog]
joomla
WordPress
Drupal
```

```
[Web/Gallery]
phpGallery
```

VideoDB

3. Save the file.

## Checking Free Disk Space Before Starting the Backup Process

It is recommended that you make sure there is enough free disk space before starting the backup process. By default, the amount of free disk space is not checked. If the backup task is started and there is not enough disk space, the task is stalled in the GUI and processes.

To enable the free disk space checking, open for editing the `pmmcli` configuration file located on Parallels Plesk Panel server at

`%PLESK_DIR%/admin/share/pmmcli/pmmcli-rc` and set the `CHECK_BACKUP_DISK_SPACE` option value to 1:

```
CHECK_BACKUP_DISK_SPACE 1
```

When this option is turned on, free disk space is checked prior to starting the backup process. The free disk space is checked only for the local repository on Plesk server, repository location is specified by the `DUMP_D` variable defined in the `/etc/psa/psa.conf` configuration file. If there is not enough disk space, the backup process is not started and the following error message is displayed:

**Not enough free disk space to backup selected objects. At least <estimated-backup-size> free disk space is required.**

---

**Note:** The free disc space will be checked only before starting the backup process. Thus, this option will not be effective, if the free disc space is occupied during the backup process by other processes, such as a simultaneous upload.

**Note:** The backup size estimation does not consider possible content compression. Actual size of a backup is usually less than its estimated size.

---