

Parallels[®] Panel

Advanced Administration Guide

Parallels Plesk Panel 11.5 for Linux

Copyright Notice

Parallels IP Holdings GmbH

Vordergasse 59

CH-Schaffhausen

Switzerland

Phone: +41 526320 411

Fax: +41 52672 2010

Global Headquarters

500 SW 39th Street, Suite 200

Renton, WA 98057

USA

Phone: +1 (425) 282 6400

Fax: +1 (425) 282 6445

EMEA Sales Headquarters

Willy-Brandt-Platz 3

81829 Munich, DE

Phone: +49 (89) 450 80 86 0

Fax: +49 (89) 450 80 86 0

APAC Sales Headquarters

3 Anson Road, #36-01

Springleaf Tower, 079909

Singapore

Phone: +65 6645 32 90

Copyright © 1999-2013 Parallels IP Holdings GmbH. All rights reserved.

This product is protected by United States and international copyright laws. The product's underlying technology, patents, and trademarks are listed at <http://www.parallels.com/trademarks>.

Linux is a registered trademark of Linus Torvalds.

All other marks and names mentioned herein may be trademarks of their respective owners.

Contents

About This Guide	7
<hr/>	
Introduction to Panel	8
<hr/>	
Installation and Upgrade Overview	11
Ports Used by Panel.....	12
Licensing	13
Virtual Hosts Configuration	14
<hr/>	
Virtual Hosts and Hosting Types	16
Virtual Host Configuration Files.....	18
Changing Virtual Hosts Settings Using Configuration Templates	20
Template Execution Context	22
Example: Changing Default Apache Ports.....	24
Website Directory Structure	25
Virtual Host Structure (Linux)	25
Predefining Values for Customizable PHP Parameters	28
Analyzing Access and Errors	29
Services Management	30
<hr/>	
DNS	31
FTP	33
Mail Service	37
Restoring Mail Configuration	38
Installing Custom SSL Certificates for Qmail or Courier-IMAP Mail Servers	39
Outgoing Mail from Exclusive IP Addresses	43
Mailing Lists Management System	44
Configuring a Mailing List to Which only Members Are Allowed to Post	46
Importing a List of E-mail Addresses into a Mailing List	46
Database Server.....	46
Using MariaDB or Percona as the Default Database Server	47
Website Applications	50
Spam Protection	51
Configuring SpamAssassin	52
Training SpamAssassin to Work with All Mail Accounts on the Server	53
Fighting Spam on a Qmail Mail Server	54
Antivirus Support	56
Parallels Premium Antivirus	57
Kaspersky Antivirus	59
System Maintenance	60
<hr/>	
Managing Panel Objects Through the Command Line	60
Executing Custom Scripts on Panel Events	61
Changing IP Addresses.....	61
Changing Paths to Services	62
Restarting Panel	63
Managing Services from the Command Line and Viewing Service Logs	63

Moving the Panel GUI to a Separate IP Address	74
Backing Up, Restoring, and Migrating Data	75
Backing Up Data	76
Backup Objects: Hierarchy and Volume	77
Specifying Data for Backing Up	80
Defining Properties of Files That Compose the Backup	86
Exporting Backup Files	88
Defining How the Backup Process Is Performed	90
Backup Utility Commands and Options	92
Restoring Data	96
Defining Objects for Restoration	97
Defining How the Restore Process is Performed	103
Conflict Resolution Rules and Policies	104
Restoration Utility Commands and Options	126
Migrating and Transferring Data	127
Statistics and Logs	128
Calculating Statistics from Logs	130
Recalculating Statistics for Previous Months	130
Log Rotation	132
Resource Usage Reports	133
Enhancing Performance	134
Reducing Resources Consumption in VPS Environments	134
Setting Up VPS Optimized Mode in Parallels Virtuozzo Containers	135
Setting Up VPS-Optimized Mode in Non-Virtuozzo Environments	137
Apache Modules Switched Off in VPS-Optimized Mode	137
Increasing the Number of Domains that Panel Can Manage	139
Recompiling Apache with More File Descriptors on RedHat-like Systems	140
Recompiling Apache with More File Descriptors on Debian Systems	142
Making Your Mail Spam Resistant	143
Optimizing the Task Manager Performance	143
Customizing Panel Appearance and GUI Elements	145
Customizing Panel Appearance and Branding	146
Hiding and Changing Panel GUI Elements	147
Domain Registration and Management Services	149
SSL Certificates Selling Services	152
Link to Provider's Website	159
Google Services for Websites Buttons	161
Products from Parallels Partners Button	163
Presence Builder Buttons	165
Panel Upgrades	167
Mail Service Controls	168
Links for Purchasing Panel License and Add-On Keys	172
Promos	175
Link to Online Support Service	179
The Facebook Like Button	181
Product Rating Widget	183
RSS Feeds	184
Voting for New Features	187

Rebranding Presence Builder 190

Changing the Editor's Name.....	193
Changing the Product and Company Logos, Hyperlinks, and Copyright Notice	194
Changing the Link to the User's Guide.....	196
Changing the Links to the Getting Started Video	198

Customizing the Functionality of Presence Builder 200

Prohibiting Users from Removing Their Sites	202
Making Modules Unavailable in the Editor	202
Making the Google Picasa Storage Unavailable for Use in Image Galleries	203
Making the Site Import Functionality Unavailable	204
Adding Custom Banner Images	205
Adding Custom Design Templates	207
Adding the Support Button	209
Adding the Link for Sending Feedback	210
Removing the Option to Add a Site Copy to Facebook.....	211
Removing Sites from Hosting Accounts	211

Customizing Website Topics in Presence Builder 212

Adding Custom Website Topics	213
Step 1: Creating a Site in Presence Builder	214
Step 2: Saving a Site to a Snapshot	215
Step 3: Uploading the Snapshot and Preparing for Editing	216
Step 4: Editing the Files That Compose the Site Topic	218
Step 5: Registering the New Topic with Presence Builder	220
Step 6: Checking the New Topic.....	220
Rearranging and Removing Topics and Categories	221

Enhancing Security 222

Restricting Script Execution in the /tmp Directory	223
Configuring Site Isolation Settings	224
Protecting from Running Tasks on Behalf of root	225

Localization 226

Registering Additional Services with Panel Notifications 227

Preparing a Service for Registration	229
Registering the Service	230
Code Samples	231
Implementation of Plan_Item_Interface	232
Registration of an Additional Service	236

Troubleshooting 237

Cannot Access Panel	238
Cannot Log In to Panel.....	238
The Administrator's Password Has Been Forgotten	240
Panel in a Virtuozzo Container: Broken Layout	240
EZ Templates Update Issues in Parallels Virtuozzo Containers.....	242
Postfix Consumes Too Many Resources in a Container.....	242

Appendix A: Web Server Configuration Files	243
---	------------

Appendix B: Configuration Templates Structure	245
--	------------

Appendix C: Apache Configuration Variables	248
---	------------

1. \$VAR->server->	249
2. \$VAR->domain->	252
3. \$VAR->subDomain->	257
4. \$VAR->ipAddress->	258

About This Guide

Parallels Plesk Panel for Linux Advanced Administration Guide is a companion guide for the *Parallels Panel Administrator's Guide*. It is intended for server administrators whose responsibilities include maintaining hosting servers and troubleshooting server software problems.

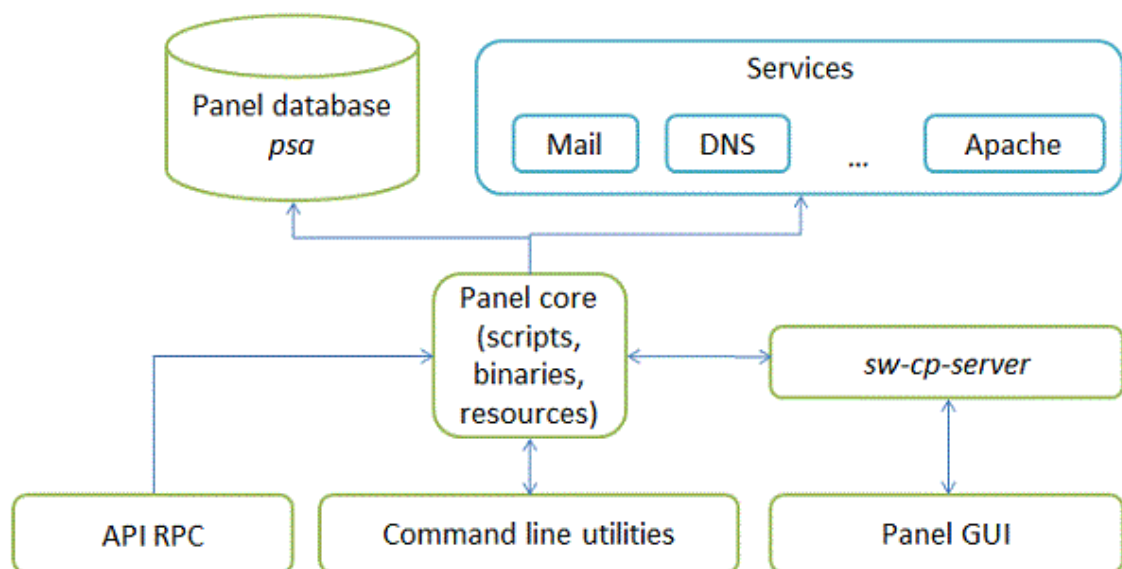
The guide provides step-by-step instructions for performing server management tasks that require use of Panel functionality other than the GUI and GUI-only tasks that administrators may need to perform only in rare and specific situations. Administrators can use several additional tools that are supplied in the standard Parallels Plesk Panel distribution package to add customized automation tasks, back up and restore data, and repair Panel components and system settings. The tools include a number of standalone applications, command-line utilities, and the ability to integrate custom scripting with Parallels Plesk Panel.

This guide contains the following chapters:

- **Introduction to Panel.** Describes the main components and services operated by Panel, licensing terms, and the ways to install and update Panel components.
- **Virtual Hosts Configuration.** Describes virtual host concepts and their implementation in Panel. Provides instructions on why and how to change their configuration.
- **Services Management.** Contains descriptions of a number of external services used on Panel server and instructions on how to configure and use them.
- **System Maintenance.** Describes how to change the server host name, IP addresses, and locations of directories for storing virtual host files, backups, and mail content. This chapter also introduces Panel's command-line tools, a mechanism for running scripts on Panel events, and the service monitor that allows monitoring and restarting of services without logging in to Panel.
- **Backing Up, Restoring, and Migrating Data.** Describes how to back up and restore Panel data by means of the command-line utilities `pleskbackup` and `pleskrestore`, and introduces the tools for migrating hosted data between servers.
- **Statistics and Logs.** Describes how to run on demand statistics calculations on disk space and traffic usage, and access web server logs.
- **Enhancing Performance.** Provides information on how to improve Panel functioning by means of software.
- **Enhancing Security.** Provides instructions on how to protect the Panel server and sites hosted on it from unauthorized access.
- **Customizing Panel Appearance and GUI Elements.** Introduces Panel themes that can be used to customize Panel appearance and branding and describes how to remove specific elements of the Panel GUI or change their behavior.
- **Localization.** Introduces the methods of localizing the Panel GUI into languages for which Parallels does not provide localization.
- **Troubleshooting.** Describes how to troubleshoot malfunctions of Panel services.

Introduction to Panel

Parallels Plesk Panel files can be divided into six major groups responsible for different aspects of Panel work. The diagram below shows these groups (components of Panel) and the connections they have to each other and to external services that Panel manages.



Panel components are as follows:

- *Panel core*. The core processes requests that Panel receives from the Panel GUI, command line interface, and API RPC. The core contains scripts, binary files and other resources used to link Panel components with each other and with external services.
- *Panel database psa*. The database stores information about Panel objects, such as IP addresses, domains, user accounts, and so on.
- *sw-cp-server* - a web server based on nginx. This serves requests to the Panel GUI.

Panel GUI - a web interface provided with sw-cp-server. The GUI is the main means of interaction with Panel.

- *Command line utilities*. The command line interface allows integration of third-party software with Panel objects. In addition, it is a way for administrators to manage Panel through the server shell. For more information on the Panel command line interface, refer to **Panel Command Line Reference**.
- *API RPC*. This interface is another way to integrate third-party software with Panel. It allows Panel objects to be managed remotely by sending specifically structured XML packets and receiving responses from Panel. For more information on API RPC, refer to **Developer's Guide: Read Me First** and **API RPC Protocol Reference**.

The Most Important Files and Directories

Parallels Plesk Panel for Linux installs its main components into the following directory:

- On RPM-based operating systems: `/usr/local/psa`
- On DEB-based operating systems: `/opt/psa`

This directory (main Panel directory) contains Panel core files, command line utilities, log files and so on.

In addition, Panel creates files and directories outside the main directory. The list below contains those that you are likely to use when administering Panel.

- The main configuration file containing paths to utilities, services and packages used by Panel:
`/etc/psa/psa.conf`
- The initialization script for opening and closing services during server startup and shutdown procedures:
`/etc/init.d/psa`

Initialization scripts for starting and stopping services with xinetd:

```
/etc/xinetd.d/smtp_psa
/etc/xinetd.d/smtps_psa
/etc/xinetd.d/poppassd_psa
/etc/xinetd.d/ftp_psa
```

Find more information on xinetd at <http://www.xinetd.org/>.

- Panel database:
`/var/lib/mysql/psa/`
- Backup files:
`/var/lib/psa/dumps/`

In this chapter:

Installation and Upgrade Overview	11
Ports Used by Panel	12
Licensing	13

Installation and Upgrade Overview

The most common way of installing and upgrading Parallels Plesk Panel is to use the *Parallels Installer* utility. This utility connects to the Parallels Updates server where the Panel distribution packages are stored. It then retrieves, downloads, and installs Panel. You can download the Parallels Installer utility from <http://www.parallels.com/eu/download/plesk/products/>.

For detailed instructions on how to use Parallels Installer, refer to the **Installation, Upgrade, Migration, and Transfer Guide**.

Installing Panel in the Parallels Virtuozzo Containers Environment

If you operate in the Parallels Virtuozzo Containers (PVC) environment, you can use *application templates* for installing Panel on containers.

When the application templates are installed on a PVC hardware node, they allow you to easily deploy the application on as many containers as required, saving system resources such as disk space.

You can obtain the Panel templates at <http://www.parallels.com/eu/download/plesk/products/> or download them using the PVC command line utility call `vzup2date -z` (available on PVC 4 and above).

For more information on installing Panel on PVC, read the **Installation, Upgrade, Migration, and Transfer Guide**, chapter **(Advanced) Installation to Parallels Virtuozzo Containers**.

Checking Potential Issues Before Upgrading to Panel 11

If you use Parallels Plesk Panel 9 or earlier and want to upgrade it to Panel 11, you may encounter problems due to changes in the Panel business model. In particular, it might be impossible to transfer some settings and business objects.

To efficiently anticipate or resolve the problems, we offer a tool called `plesk101_preupgrade_checker.php`. This tool checks potential business logic issues with upgrading to Panel 10 and later and gives recommendations that help you fix the possible problems related to transition of Panel objects. You can download the tool and find descriptions of the report messages at <http://kb.parallels.com/9436>.

Ports Used by Panel

Parallels Plesk Panel is middleware between end users and external services such as FTP, mail, DNS and others. Due to technical limitations, Panel is able to interact with these services only if they are available on certain ports.

The list below provides information about services managed through Panel and about ports on which they should be available for proper interaction with Panel. If you use a firewall, make sure that the connections to all of these ports are allowed for corresponding Panel services.

Service name	Ports used by service
Administrative interface of Panel over HTTPS	TCP 8443
Administrative interface of Panel over HTTP	TCP 8880
VPN service	UDP 1194
Web server	TCP 80, TCP 443
FTP server	TCP 21
SSH (secure shell) server	TCP 22
SMTP (mail sending) server	TCP 25, TCP 465
POP3 (mail retrieval) server	TCP 110, TCP 995
IMAP (mail retrieval) server	TCP 143, TCP 993
Mail password change service	TCP 106
MySQL server	TCP 3306
MS SQL server	TCP 1433
PostgreSQL server	TCP 5432
Licensing Server connections	TCP 5224
Domain name server	UDP 53, TCP 53
Panel upgrades and updates	TCP 8447

Note: If you install Presence Builder as part of Parallels Plesk Panel, Presence Builder uses the same protocol and opens on the same port as the Parallels Plesk Panel UI.

Licensing

After you install Parallels Plesk Panel, a trial license key for 14 days is installed by default. To continue using Panel after the trial license key expires, you should obtain a lease license key or purchase a permanent license key.

A leased license means that you pay for a limited time during which you can use Panel, for example, two months. During the lease period, Panel will perform free monthly updates of your license key. The lease license includes free upgrades to all major new versions of Panel.

The permanent license means that you buy a lifetime Panel license. A permanent license is updated every three months for free. Upgrading a Panel installation with a permanent license to the next major version requires a separate payment unless you use *Software Update Service (SUS)*. See <http://www.parallels.com/support/sus/> for more information on SUS.

Panel license keys have a *grace period* of 10 days before the *expiration date*. During the grace period, Panel makes daily attempts to update the license key automatically. If an automatic update fails, Panel notifies the administrator. If you do not update a license key during the grace period, it expires and blocks Panel functions until you install a valid license key.

Panel defines whether it needs to update the license key using the `update-keys.php` utility located in the

`$PRODUCT_ROOT_D/admin/plib/DailyMaintenance/directory`, where the `$PRODUCT_ROOT_D` is `/usr/local/psa`. This utility checks the license grace period and expiration date and tries to retrieve a new license key or blocks Panel.

Panel runs the utility every day as a part of the daily maintenance script. If you want to check for license updates, you can run the script manually by executing the command

```
$PRODUCT_ROOT_D/bin/sw-engine-pleskrun  
$PRODUCT_ROOT_D/admin/plib/DailyMaintenance/script.php.
```

You can retrieve and manage license keys through the Panel GUI. The information about the current license key and controls for managing license keys are located in **Server Administration Panel > Tools & Settings > License Management**.

Virtual Hosts Configuration

Parallels Plesk Panel for Linux uses the Apache web server for websites hosting. In Panel, Apache by default is supplemented with nginx to achieve better performance.

Apache itself does not operate with websites; it manages virtual hosts - web resources identified either by an IP address or a host name. When creating a site, Panel adds a new virtual host to Apache so that the site becomes available through the web server. Panel resides on a virtual host too; this host is called the *default virtual host*.

When you add a site in Panel, you select one of the hosting types to use with it: web page hosting or forwarding. In terms of Apache, you associate the site with a virtual host of one of three configurations (website hosting, standard forwarding, and frame forwarding). To learn the differences between these configurations, see the section **Virtual Hosts and Hosting Types** (on page 16).

Sites are linked to virtual hosts, so if you want to add some feature provided by Apache but not available through the Panel GUI, you should change the virtual host settings using *Apache configuration templates*. Based on these templates, Panel partly re-generates virtual hosts, so you should follow certain rules when modifying the configuration; otherwise, some of your changes might be lost. Next in this chapter, we will discuss virtual hosts in more detail and provide guidelines on how to modify them safely. To learn more on this point, refer to the section **Changing Virtual Hosts Settings Using Configuration Templates** (on page 20).

Panel creates virtual hosts for websites based on virtual host templates. These templates predefine the content that will be included in each new virtual host. Learn how to change virtual host templates in **Administrator's Guide**, section **Presetting Content of Customer Websites** [./plesk-administrator-guide/68695.htm](http://plesk-administrator-guide/68695.htm).

You can get information on access to each virtual host and Apache errors that have occurred on the host from Apache logs. Learn more about log files location and rotation settings in the section **Analyzing Access and Errors** (on page 29).

Virtual Host IP Addresses

The term *virtual host* refers to the practice of running more than one website on a single server or IP address. For example, Apache can manage two websites, `example1.com` and `example2.com`, even if they use a single IP address. Each of these sites is hosted on a separate virtual host.

There are two types of virtual host, each with different methods of requests routing:

- *IP-based*. Each virtual host has a separate IP address. Apache defines the requested host based on the host IP address.
- *Name-based*. This supposes that several virtual hosts share the same IP address. To define a requested host, Apache parses the domain name.

Parallels Plesk Panel uses the name-based approach. In addition, Panel provides an option to allocate separate IP addresses to customers who do not want to share their IP address with others. To implement this option, there are two types of IP address in Panel:

- *Dedicated* IP addresses that have a single owner.
- *Shared* IP addresses that you can allocate to any number of customers.

Resolving Requests to Web Servers

When a client requests a certain domain, Apache parses the requested domain name. Then Apache searches for the virtual host with the requested domain on the IP address specified in the request. If the host exists, Apache sends the requested files from this host to the client.

If the requested virtual host is not found, Panel uses the following entities to resolve the request:

1. *Default domain*. This can be created for a specific IP address. If a request to this IP address contains the name of a non-existent domain, Panel redirects this request to the default domain.
2. *Default virtual host*. This accepts all requests to server IP addresses that could not be directed to any default domain.

In this chapter:

Virtual Hosts and Hosting Types	16
Changing Virtual Hosts Settings Using Configuration Templates.....	20
Website Directory Structure.....	24
Predefining Values for Customizable PHP Parameters	28
Analyzing Access and Errors.....	29

Virtual Hosts and Hosting Types

Depending on how you intend to use a site created in Panel, for example, to host web pages or to forward HTTP requests to another site, you can choose from three hosting types that define the structure of a virtual host created for this site. The hosting types are the following:

- *Website hosting.* When you choose this type of hosting, Panel creates a virtual host (disk space on the local server) for a customer. Customers store their files on a virtual host and run their websites without having to purchase a server or dedicated communication lines.
- *Standard forwarding.* In this case, Panel creates a reduced virtual host that does not store its owner's files and directories. This host is used for redirecting requests to another network resource. When users try to access the domain, Panel forwards them to another URL. This URL will be shown in their browsers.
- *Frame forwarding.* In this case, Panel creates a reduced virtual host that does not store its owner's files and directories. Unlike standard forwarding, frame forwarding virtual hosts show the requested URL in a browser, not the actual one. Panel uses HTML frames to show the pages of another site with the requested URL.

The virtual host structure differs depending on hosting type:

- Domains with a website hosting type have a directory called *document root* where the website files are stored. The configuration of such a virtual host looks like this:

```
<VirtualHost 10.0.69.4:80>
    ServerName "domainXX.tst:443"
        ServerAlias "www.domainXX.tst"
        UseCanonicalName Off
<IfModule mod_suexec.c>
    SuexecUserGroup "domainXX.tst" "psacln"
</IfModule>
    ServerAdmin "admin@mailserver.tst"
    DocumentRoot "/var/www/vhosts/domainXX.tst/httpdocs"
    CustomLog
/var/www/vhosts/domainXX.tst/statistics/logs/access_ssl_log plesklog
    ErrorLog "/var/www/vhosts/domainXX.tst/statistics/logs/error_log"
    .....
    ..
```

- Standard forwarding domains just contain a forwarding address in the configuration file. No space for storing files is allocated. The configuration of such a virtual host looks like this:

```
<VirtualHost 10.0.69.2:80>
    ServerName "SFdomain.tst.tst"
        ServerAlias "www.SFdomain.tst.tst"

    ServerAdmin "admin@mailserver.tst"
    RedirectPermanent / "http://easytofinddomain.tst/"
</VirtualHost>
```


- Frame forwarding domains have a document root with a single file `index.html` with the `<FRAMESET>` tag that defines the frame and address of the website to show in the frame. Therefore, the configuration of a frame forwarding virtual host resembles website virtual host configuration:

```
<VirtualHost 10.0.69.2:80>
    ServerName "FFdomainXX.tst"
    ServerAlias "www.FFdomainXX.tst"

    ServerAdmin "admin@mailserver.tst"
    DocumentRoot "/var/www/vhosts/FFdomainXX.tst/httpdocs"
    <IfModule mod_ssl.c>
        SSLEngine off
    </IfModule>
</VirtualHost>
```

When you create a website inside a subscription in Server Administration Panel, the domain hosting type is set to website hosting. When you create a domain in Control Panel, you can set a different hosting type. Domain owners are free to change the hosting types of their domains whenever they wish.

To change the hosting type of a domain, open **Control Panel > Websites & Domains**, click the domain name, and go to the **Hosting Type > Change**.

Next in this section:

Virtual Host Configuration Files 18

Virtual Host Configuration Files

Configuration settings of each virtual host are stored in its configuration files in the `/var/www/vhosts/system/<domain_name>/conf/` directory. Particularly, these files are the following:

- `<version>_httpd.conf` - Apache virtual host configuration.
- `<version>_nginx.conf` - nginx configuration.

The final Apache configuration will include all `httpd.conf` and `nginx.conf` files from all virtual hosts.

Panel lets administrators and domain owners see the history of changes in a virtual host configuration files by saving each version of these files. `<version>` here is a unique number assigned to a certain configuration state that is used now or was used previously. To let administrators and domain owners easily access the currently used configuration file, Panel stores the links `last_httpd.conf` and `last_nginx.conf` that point to the corresponding files.

The system re-generates the configuration files after each change of virtual host configuration, for example, changing the hosting type of a domain. Therefore, if you edit `httpd.conf` and `nginx.conf` files manually, your changes will be lost after changing the virtual host settings in the Panel UI. To avoid this, additional files are used to specify custom configuration for domains:

- `vhost.conf` and `vhost_ssl.conf` - custom Apache directives for two situations: when clients access the site over HTTP and HTTPS respectively. These files are included in the `httpd.conf`.
- `vhost_nginx.conf` - custom nginx directives. This file is included in the `nginx.conf`.

The files with custom per-domain configuration are stored in the `/var/www/vhosts/system/<domain_name>/conf/` directory.

Most of the settings specified in these files override the server-wide configuration of a virtual host (`httpd.conf` and `nginx.conf`). For example, if you include directives that already exist in the site's current `httpd.conf` file, the system will use your values from the `vhost.conf` and `vhost_ssl.conf` files.

Editing Virtual Host Configuration Files

There are two ways to edit virtual host configuration files:

1. *Manually.* You can add custom directives to the following files from `/var/www/vhosts/system/<domain_name>/conf/` directory:
 - `vhost.conf` and `vhost_ssl.conf`
 - `vhost_nginx.conf`
2. *In the Panel GUI.* On the **Websites & Domains** > select a website > **Web Server Settings** tab you can specify:
 - **Common Apache settings.** Most commonly used directives (like MIME types or index files). These directives will be included in `httpd.conf`.
 - **nginx settings.** Directives that define the scope of nginx's role in serving website's content of different types (static and dynamic).
 - **Additional Apache directives.** You can add several custom Apache directives at once in the **Additional directives for HTTP** and **Additional directives for HTTPS** fields. These fields correspond to `vhost.conf` and `vhost_ssl.conf` files respectively.
 - **Additional nginx directives.** You can add several custom nginx directives at once in the **Additional nginx directives** field. This field corresponds to `vhost_nginx.conf` file.

The changes you made in the web server configuration will be applied automatically.

Note: If you have upgraded from the older Panel version and are configuring the `vhost.conf` and `vhost_ssl.conf` files for the first time after the upgrade, you will need to use the `httpdmng` utility to apply the changes from your configuration files. For example, to generate web server configuration files for a website, run the command:
`/usr/local/psa/admin/sbin/httpdmng --reconfigure-domain <domain_name>`

Changing Virtual Hosts Settings Using Configuration Templates

You can change the settings of virtual hosts running on the Panel server, for example, set custom error pages (similar for all virtual hosts), or change the port on which the hosted site is available.

To reduce the risk of errors during modification of configuration files, Parallels Plesk Panel provides a mechanism for changing virtual host configuration - *configuration templates*. Before 11.0 Panel had templates only for Apache configuration files, but with adding support for nginx administrators can modify nginx templates as well. Read more about the how Apache and nginx work together in the **Administrator's Guide**, section **Improving Web Server Performance with nginx (Linux)**.

Configuration templates are files based on which Panel re-generates certain web server configuration files. Other configuration files are generated automatically and cannot be changed. The hierarchy of configuration files generated by Panel automatically and from templates is shown in the **Appendix A** (on page 243).

Web server configuration files support versioning. This allows you to roll back to a previous configuration if the new one contains errors. Panel adds a file version number to the name of each configuration file. For example, virtual host configuration files located in the `/var/www/vhosts/<vhost_name>` directories have the names like `<version>_httpd.include`. To quickly access the currently used configuration file of a virtual host, use the symbolic link `last_httpd.include` located in the same directory.

The *default templates* are located in
`/usr/local/psa/admin/conf/templates/default/`.

Important: Do not change the default templates. To introduce your changes to the configuration, copy the templates you need to the `/usr/local/psa/admin/conf/templates/custom/` directory and modify them, preserving the directory structure, and then modify these copies. You can create new templates from scratch and place them in the `custom/` directory according to the default structure.

To remove your changes and restore the default configuration, just delete the custom template files.

➤ **To change virtual hosts configuration using configuration templates:**

1. Create the `/usr/local/psa/admin/conf/templates/custom/` folder (if there is no such folder yet).
2. Copy and paste the required templates from `default/` to `custom/` preserving the directory structure. You can find the complete list of templates and their descriptions in the **Appendix B** (on page 245).

3. Modify the templates. See the details in the **Templates Execution Context** section (on page 22).

4. Check that the modified templates are valid PHP files:

```
# php -l <file-name>
```

5. Generate new configuration files:

```
# httpdmg <command>
```

Where **<command>** is one of the following:

- `--reconfigure-server` generates sever-wide configuration files.
- `--reconfigure-domain <domain-name>` generates files for a specified domain.
- `--reconfigure-all` generates all configuration files.

Note: Panel generates configuration files automatically upon a variety of events. For example, if a website's hosting settings are changed - say PHP is enabled - configuration for this website is generated anew.

Example: Modifying Error Pages

1. Copy the error pages template to the `custom/` directory:

```
# mkdir -p
/usr/local/psa/admin/conf/templates/custom/domain/service/
# cp
/usr/local/psa/admin/conf/templates/default/domain/service/error
docs.php
/usr/local/psa/admin/conf/templates/custom/domain/service/error
docs.php
```

2. Edit the `/usr/local/psa/admin/conf/templates/custom/domain/service/error docs.php` file.

3. Check the validity of the file and generate new configuration files.

Next in this section:

Template Execution Context	22
Example: Changing Default Apache Ports.....	24

Template Execution Context

In essence, configuration templates are PHP files which, when executed, output web server configuration files. The templates are executed in the environment where the specific variables `$VAR` and `$OPT` are available.

`$VAR` is an object containing the data model which should be applied to a template. The variable contains an essential set of parameters defining the content of web server configuration. The detailed structure of the array is presented in the **Appendix C** (on page 248).

The most important function is *`IncludeTemplate()`* which is part of the `$VAR` array. The function allows including templates one into another, and it is defined as

```
IncludeTemplate($TemplateName, $OPT, $metainfo)
```

where

- `$TemplateName` - string denoting name of included template. Required
- `$OPT` - an associative array which passes values to a template. Optional
- `$metainfo` - an associative array which defines certain aliases in the template context. Optional

The basic function usage is as follows:

```
## source: default/server.php
<?php echo $VAR->includeTemplate('server/tomcat.php') ?>
```

A text generated by the included template (`server/tomcat.php`) will be included in the configuration file.

In cases when the text generated by an included template should depend on the context, for example, when iterating over a set of values, it is possible to pass additional parameters to the template.

```
## source: default/server.php
<?php echo $VAR->includeTemplate('service/php.php', array(
    'enabled' => false,
)) ?>
```

Here, we included the `service/php.php` template and passed the value `'enabled' => false` to it. In the template being included the passed value is available in the variable `$OPT`:

```
## source: service/php.php
<?php
if ($OPT['enabled']) { // it is required to detect 'enabled'
    echo "php_admin_flag engine on\n";
    if (!array_key_exists('safe_mode', $OPT) || $OPT['safe_mode']) {
// optional parameter 'safe_mode'
        echo "php_admin_flag safe_mode on\n";
    } else {
        echo "php_admin_flag safe_mode off\n";
    }
}
```

```

    }
    if(array_key_exists('dir', $OPT) && $OPT['dir']) { // optional
parameter 'dir'
        echo "php_admin_value open_basedir {$OPT['dir']}: /tmp\n";
    }
} else {
    echo "php_admin_flag engine off\n";
}
?>

```

The code in this sample will generate two different blocks of text depending on which value of the 'enabled' parameter is passed.

Note that \$VAR, which contains the data model, can be used in templates being included as well. Some values of \$VAR are defined using the content of \$metainfo. For details on possible \$metainfo content and how it affects a template context, refer to **Appendix C** (on page 248). For example, by defining the subDomainId value in the \$metainfo parameter, it is possible to set an exact subdomain model available at \$VAR->subDomain in a template being included:

```

## source: default/domainVhost.php
<?php
//going through all subdomains of current domain
foreach ($VAR->domain->physicalHosting->subdomains as $subdomain) {
    if ($subdomain->ssl) { //if SSL is enabled on a subdomain
        //include configuration for subdomain with enabled SSL
        echo $VAR->includeTemplate('domain/subDomainVirtualHost.php',
array(
            'ssl' => true, // passing $OPT['ssl'] = true
        ), array(
            'subDomainId' => $subdomain->id, // define target
subdomain for which a configuration file is being built
        ));
    }

    //include configuration for subdomain with disabled ssl
    echo $VAR->includeTemplate('domain/subDomainVirtualHost.php',
array(
        'ssl' => false,
    ), array(
        'subDomainId' => $subdomain->id,
    ));
}
?>

```

```

## source: domain/subDomainVirtualHost.php
ServerName "<?php echo $VAR->subDomain->asciiName ?>.<?php echo $VAR-
>domain->asciiName ?>:<?php echo $OPT['ssl'] ? $VAR->server-
>webserver->httpsPort : $VAR->server->webserver->httpPort ?>"

```

Example: Changing Default Apache Ports

Changing the default HTTP and HTTPS ports of a web server is useful when employing an additional web server for caching purposes. For example, nginx web server listens on the default ports (80 HTTP, 443 HTTPS), serves static content (for example, all requests but PHP), and redirects PHP requests to Apache. In turn, Apache web server listens on custom ports (for example, 8888 and 8999) and serves dynamic content - PHP requests.

➤ *To change the Apache HTTP port:*

Find all occurrences of the string `$VAR->server->webserver->httpPort` and replace them with the required port number enclosed in quotation marks, for example: `"3456"`.

➤ *To change the Apache HTTPS port:*

Find all occurrences of the string `$VAR->server->webserver->httpsPort` and replace them with the required port number enclosed in quotation marks, for example: `"4567"`.

Example

To make Apache listen to HTTP requests on port 3456, and HTTPS on 4567, make the changes described above in all templates.

For example, in `domain/domainVirtualHost.php`:

```
<VirtualHost <?php echo $VAR->domain->physicalHosting->ipAddress-
>address ?>:<?php echo $OPT['ssl'] ? $VAR->server->webserver-
>httpsPort : $VAR->server->webserver->httpPort ?>>
    ServerName "<?php echo $VAR->domain->asciiName ?>:<?php echo
$OPT['ssl'] ? $VAR->server->webserver->httpsPort : $VAR->server-
>webserver->httpPort ?>"
```

change to

```
<VirtualHost <?php echo $VAR->domain->physicalHosting->ipAddress-
>address ?>:<?php echo $OPT['ssl'] ? "4567" : "3456" ?>>
    ServerName "<?php echo $VAR->domain->asciiName ?>:<?php echo
$OPT['ssl'] ? "4567" : "3456" ?>"
```

Website Directory Structure

When someone creates a website, Panel not only adds a new virtual host to the web server but also creates the site's directory structure and fills the directories with certain initial content. These directories are located in the corresponding virtual host directories:

- On Linux: `/var/www/vhosts/<domain_name>`
- On Windows: `C:\inetpub\vhosts\<domain_name>`

<domain_name> here is the website's domain name. The directory structure is defined by the default virtual host template (see the sections **Virtual Host Structure (Linux)** (on page 25) and **Virtual Host Structure (Windows)** for details).

If you want to change the files and directories included in new sites, for example, you want to add scripts or change the error pages, you can define a custom *virtual host template*. Resellers can also customize virtual host templates for their customers.

Note: Subdomains have the same status as domains and employ the same directory structure. Thus, they have a separate directory in `/var/www/vhosts` and their own configuration files, such as `php.ini` or `vhost.conf`.

Next in this section:

Virtual Host Structure (Linux) 25

Virtual Host Structure (Linux)

The table below shows the list of directories that Panel creates for each virtual host. Note that Panel does not add all the directories by default. It creates some of the directories only when the website owner needs them. Such directories are marked as created **On demand**. For example, after a customer adds a website, it does not have the `/web_users` directory. Panel will create it only after the customer adds his first web user.

The following table lists subdirectories of a virtual host directory `/var/www/vhosts/<vhost>`:

Directories Tree	User	Group	Permissions	Description	Created
<code>/<VHOST></code> <code>></code>	user	root	755		Always
<code>/anon_ftp</code>	user	psaserv	750	Anonymous FTP files	On demand
<code>/error_docs</code>	root	psaserv	755	Error message files	Always
<code><doc>.html</code>	user	psaserv	755		
<code>/httpdocs</code>	user	psaserv	750	HTTP documents	Always

/cgi-bin	user	psacln	755	CGI scripts	Always
/logs	root	root	777	Link to ../system/<vhost> /logs	Always
/bin	root	root	755	Chroot environment directories	On demand
/dev	root	root	755		
/etc	root	root	755		
/lib	root	root	755		
/tmp	root	root	755		
/usr	root	root	755		
/var	root	root	755		
/web_users	root	root	755	Web users' directory	On demand
/<web_user>	user	psaserv	750	Web user directory	On demand
/<subdomain>	user	psaserv	750	HTTP and HTTPs documents of a subdomain	On demand
/<domain>	user	psaserv	750	HTTP and HTTPs documents of an additional domain	On demand

The following table lists directories created for a virtual host in the
/var/www/vhosts/system/<vhost>:

Directories Tree	User	Group	Permissions	Description	Created
/<VHOST>	root	psaserv	744		Always
/conf	root	psaserv	750	Configuration files.	Always
/etc	root	root	755	Configuration files	Always
/logs	psaadm	psacln	750	Virtual host logs	Always
/pd	root	psaserv	750	Passwords to protected directories	Always
d..<dir1>@<dir2>	root	psaserv	310		Always
/statistics	root	psaserv	550	Statistics directory	Always
/anon_ftpstat	root	root	755	Anonymous FTP statistics.	Always
/ftpstat	root	root	755	FTP user statistics	Always
/logs	root	root	777	Link to /logs	Always
/webstat	root	root	755	HTTP user statistics	Always

/webstat-ssl	root	root	755	HTTPS user statistics	Always
--------------	------	------	-----	-----------------------	--------

Differences from Previous Versions

The structure described above was introduced in Panel 11.5. It has the following differences compared to the structure of earlier Panel versions:

- Some directories are created on demand. Previously, all the directories were created by default.
- The following directories were moved from `/var/www/vhosts/<VHOST>` to `/var/www/vhosts/system/<VHOST>`:

Old Location	New Location	Comment
<code>/<VHOST>/conf</code>	<code>/system/<VHOST>/conf</code>	Configuration files
<code>/<VHOST>/pd</code>	<code>/system/<VHOST>/pd</code>	Passwords to protected directories
<code>/<VHOST>/statistics</code>	<code>/system/<VHOST>/statistics</code>	Statistics directory
<code>/<VHOST>/statistics/logs</code>	<code>/system/<VHOST>/logs</code>	Virtual host logs

- The following directories are not included in Panel virtual hosts:
 - `/httpsdocs`
 - `/subdomains`
 - `/private`

Predefining Values for Customizable PHP Parameters

Panel allows to define custom PHP configuration for a certain service plan, add-on plan, subscription, website, and even subdomain. For this purpose, the Panel GUI exposes 16 most often used PHP parameters that allow customization. The administrator or a customer can set the value of each parameter either by *selecting a value from a preset, typing a custom value, or leaving the default value*. In the latter case, Panel takes the parameter value from the server-wide PHP configuration.

Using the `/usr/local/psa/admin/conf/panel.ini` file you can specify what PHP parameters values will be available in the preset and toggle the visibility of the custom value field.

Defining the Preset Values

➤ **To set the list of predefined values for a certain PHP parameter, add the line of the following type to the `[php]` section of the `panel.ini` file:**

```
settings.<parameter_group>.<parameter_name>.values[]=<value>
```

where

- `<parameter_group>` - a group of a PHP parameter: `performance` for the performance PHP settings and `general` if the parameter is placed in to the common group. For more information about the groups of PHP parameters, read the **Administrator's Guide, Custom PHP Configuration**.
- `<parameter_name>` - a name of a PHP parameter. Use the same syntax as in `php.ini`.
- `<value>` - a parameter's value added to the preset. Use the same syntax as in `php.ini`.

Add such line for each value in the preset. For example, if you want Panel users to choose the value of the `memory_limit` parameter between 8M and 16M, add the following lines to `panel.ini`:

```
[php]
settings.performance.memory_limit.values[]=8M
settings.performance.memory_limit.values[]=16M
```

Hiding the Custom Value Fields

To hide the field that allows entering the custom value for a certain PHP parameter, add the line of the following type to the `[php]` section of the `panel.ini` file:

```
settings.<parameter_group>.<parameter_name>.custom=false
```

where

- `<parameter_group>` - a group of a PHP parameter: `performance` for the performance PHP settings and `general` if the parameter is placed in to the common group. For more information about the groups of PHP parameters, read the Administrator's Guide,
- `<parameter_name>` - a name of a PHP parameter. Use the same syntax as in `php.ini`.

For example, if you do not want Panel users to set custom values to the `memory_limit` parameter, add the following line to `panel.ini`:

```
[php]
settings.performance.memory_limit.custom=false
```

To switch the custom value field back on, replace `false` with `true`.

Analyzing Access and Errors

For each site, Apache writes access and error information to log files. Each site has two log files - `access_log` and `error_log`, which store information on access to that site and errors respectively. Apache log files for each site are located in the `/statistics/logs` subdirectory of the virtual host directory `/var/www/vhosts/<domain_name>`, where `domain_name` is the name of a corresponding domain.

To save disk space, Panel rotates Apache logs. Learn how to change log rotation parameters in the **Log rotation** (on page 131) section.

Services Management

To enable basic hosting services and functions on a Panel-managed server, the Panel distribution package includes several *third-party software applications* that are installed along with Parallels Plesk Panel. These applications are responsible for providing various hosting services such as DNS, e-mail, FTP, and others.

All software components shipped with Panel can be installed and updated by means of Parallels Installer. These components are listed at <http://download1.parallels.com/Plesk/PP11/11.5/release-notes/parallels-plesk-panel-11.5-for-linux-based-os.html#4>.

You can also install and manage through Parallels Plesk Panel many other third-party applications that are not included in the Parallels Plesk Panel distribution package. For the complete list of third-party applications currently supported by Panel, refer to <http://download1.parallels.com/Plesk/PP11/11.5/release-notes/parallels-plesk-panel-11.5-for-linux-based-os.html#5>.

This chapter provides detailed descriptions of different external components used for providing hosting services on a Panel server.

In this chapter:

DNS	31
FTP	33
Mail Service.....	37
Mailing Lists Management System	44
Database Server	46
Website Applications	50
Spam Protection.....	51
Antivirus Support.....	56

DNS

Parallels Plesk Panel for Linux works in cooperation with the *BIND* (or *named*) domain name server that enables you to run a DNS service on the same machine on which you host websites.

When you add a new domain name to Panel, it automatically generates a zone file for this domain in accordance with the server-wide DNS zone template and registers it in the name server's database, then instructs the name server to act as a primary (master) DNS server for the zone.

Configuring DNS

You can change the name server settings by editing configuration file `/var/named/run-root/etc/named.conf` (`/etc/named.conf` is a soft link to it). This file consists of the following parts:

General Settings containing the following sections:

The Options section contains the directory option referring to `/var`, which is used as the base directory relative to `$ROOTDIR` (which is `/var/named/run-root` by default) for all other files used below. It also sets the location where `named` will store its PID.

The key and control sections define a shared key for managing `named` with the `rndc` utility and access list.

- The main part contains several zone sections, one for every direct and reverse zone in which the server acts as the primary or a secondary name server. As usual, there is also a root zone section.
 - The root zone section defines the file with the root zone name servers.
 - Reverse local loop zone.
 - A direct zone for every domain and a reverse zone that the server processes as a name server.

The final part containing the `acl` section, which defines an access control list of name server IP addresses where zone transfers are allowed. By default, the `common-allow-transfer` ACL is included in every zone section.

Note: If you perform change zone entries in the file manually, Panel will override them with changes made through the GUI.

Zone files

By default, zone files for domains are stored in the `/var/named/run-root/var` directory, as defined in the `/var/named/run-root/etc/named.conf` file. Each zone file has a name identical to the domain name. If you change the zone through the GUI, Panel rewrites the file.

You can change a zone database by adding or deleting resource records as follows:

Using the Panel GUI. In this case, the Panel increases the Serial field value, which means that the zone transfer operation should be performed to synchronize the zone content with all secondary name servers.

Manually editing the file. We do not recommend this approach, since Panel completely rewrites the zone data from the psa database if any changes are made through the Panel GUI. Do not forget to increase the Serial field in this file. Otherwise, only this name server will know about the changes made.

Manually editing the psa database. To do this, perform the following steps:

First, you have to insert a corresponding record into the `psa.dns_recs` table.

```
mysql> insert into dns_recs (dom_id,type,host,val) values
      (2,'A','ws02.domain01.tst.','192.168.1.185');
Query OK, 1 row affected (0.00 sec)
```

After that, make the Panel reread the domain information from the psa database in one of the following ways.

- Through the command line:

```
# /usr/local/psa/admin/sbin/dnsmng update <domain_name>
```

Using the Panel GUI, switch the domain to slave and then back to the master mode. In this case, you do not have to worry about the Serial field as the Panel increases its value while restoring the file.

Access Control Lists

You can restrict the name server to transferring name zones to only the list of explicitly assigned DNS servers. Do this by inserting the DNS server IP addresses into the `misc` table of the psa database with the following command:

```
mysql> insert into misc (param, val) values ('DNS_Allow_Transfer1',
      <dns server>);
```

for the first DNS server in the list.

```
mysql> insert into misc (param, val) values ('DNS_Allow_Transfer2',
      <dns server>);
```

for the second DNS server, etc.

To transfer the changes made in the database to the DNS configuration file, use the following command:

```
# /usr/local/psa/admin/sbin/dnsmng update <domain_name>
```

The command shown above adds DNS server IP addresses to the common-allow-transfer ACL, which is included in all local name zones. Every domain can have some additional IP addresses in its ACL. Secondary servers are added to the allow-transfer list of a domain by the Panel after adding the corresponding NS records to the domain name zone. In addition, the secondary server must be resolvable and accessible when it is added to the name zone.

DNS logs

The domain name service writes errors log stored in the `/var/log/messages` file. The `logrotate` utility rotates this log on a daily, weekly, or monthly basis. Learn how to configure log rotation in the section **Log Rotation** (on page 131).

FTP

To provide an FTP service, Panel uses the *ProFTPD* FTP server. Panel includes the following two packages:

- `psa-proftpd` which contains the main component.
- `psa-proftpd-xinetd` which contains patches and configurations to work with `xinetd`.

FTP Startup

The ProFTPD is started by the `xinetd` every time the server receives an FTP request. In the case of authorized access, the FTP service is started on behalf of the user whose request is to be processed. For anonymous users, the service is started with the UID of the `psaftp` user.

FTP Users

The FTP server allows for document access of authenticated users that are listed in the `/etc/passwd` and `/etc/shadow` files. The first one defines the user name, group membership, home directory, and active access method. The second one stores password hash values. Let us look at FTP users created during the virtual hosting setup procedure. The following are some `/etc/passwd` lines defining FTP user parameters.

```
# grep ftp /etc/passwd
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
psaftp:x:2524:2522:anonftp psa user:/:/bin/false
ftpuser:x:10006:10001:/:/var/www/vhosts/domain.tst:/bin/false
ftpuser55:x:10010:10001:/:/var/www/vhosts/domainXX.tst:/bin/false
```

The first two lines are default FTP users. The `psaftp` is the user on behalf of whom the FTP service is started when the Panel server receives an anonymous FTP request.

The last two lines define typical FTP users. The group ID `10001` refers to the `psacln` group that contains FTP users. The `psacln` is added to the `/etc/ftpchroot` file. For every FTP user logged into the Panel, a “chroot” procedure is executed, which ensures the user cannot see files owned by other users.

Panel stores all FTP user accounts in a single database; therefore, FTP users cannot have the same names even if they are created for different virtual hosts. Besides, since the FTP service cannot be name based, only one virtual host on each IP address can provide anonymous FTP access.

FTP Configuration

The FTP server configuration parameters are stored in the `/etc/proftpd.conf` file. Here are some of the parameters. A sample of the `proftpd.conf` file is displayed below:

```
DefaultServer          on
<Global>
DefaultRoot ~          psacln
AllowOverwrite         on
</Global>
DefaultTransferMode    binary
UseFtpUsers            on

TimesGMT               off
SetEnv TZ :/etc/localtime
# Port 21 is the standard FTP port.
Port                   21
# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask                  022

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances           30

#Following part of this config file were generate by PSA automatically
#Any changes in this part will be overwritten by next manipulation
#with Anonymous FTP feature in PSA control panel.

#Include directive should point to place where FTP Virtual Hosts
configurations
#preserved
ScoreboardFile /var/run/proftpd/scoreboard
# Primary log file mest be outside of system logrotate province
TransferLog /usr/local/psa/var/log/xferlog
#Change default group for new files and directories in vhosts dir to
psacln
<Directory /var/www/vhosts>
    GroupOwner psacln
</Directory>
```

```
# Enable PAM authentication
AuthPAM on
AuthPAMConfig proftpd
IdentLookups off
UseReverseDNS off
AuthGroupFile /etc/group
Include /etc/proftpd.include
```

Each virtual host FTP configuration is stored in the `/etc/proftpd.include` file. The configurations consist of two sections:

- The general section configures FTP for authorized users. It configures the following:
 - Virtual server name to IP address binding.
 - Log file path.
 - Write permission.

Login access allowed only to the `psacln` group.

Below is a sample of the general section:

```
<VirtualHost 192.168.37.101>
ServerName "ftp.swtrn.com"
TransferLog /usr/local/psa/var/log/xferlog
AllowOverwrite on
<Limit LOGIN>
    Order allow, deny
    AllowGroup psacln
    Deny from all
</Limit>
```

- The *Anonymous* section configures FTP for anonymous users. It configures:
 - An alias for the `psaftp` user account.
 - `anon_ftp` as the home directory that is inside the domain directory opened for the authorized domain user.
 - A log file for anonymous FTP access.
 - User and group for anonymous FTP access.

Login access and read-only rights for everyone Below is a sample of this section:

```
UserAlias anonymous psaftp
<Anonymous /var/www/vhosts/domain.tst/anon_ftp>
    TransferLog
/var/www/vhosts/domain.tst/statistics/logs/xferlog
    PathDenyFilter "^\.quota$"
    RequireValidShell off
    TransferRate RETR 0.000
    User psaftp
    Group psaftp
    <Limit LOGIN>
        AllowAll
    </Limit>
    <Limit WRITE>
        DenyAll
    </Limit>
    <Directory incoming>
        UserOwner ftpuser
```

```
        Umask 022 002
        <Limit STOR>
            DenyAll
        </Limit>
        <Limit WRITE>
            DenyAll
        </Limit>
        <Limit READ>
            DenyAll
        </Limit>
        <Limit MKD XMKD>
            DenyAll
        </Limit>
    </Directory>
</Anonymous>
```

For more information on the ProFTPD configuration, please refer to the www.proftpd.org.

FTP Logs and Statistics

For each domain, the ProFTPD service writes statistics for both anonymous and authorized access to log files located in the `/var/www/vhosts/<domain_name>/statistics/logs/` directory. Once a day, Panel processes the logs with the `statistics` utility and separates the statistical data into two parts:

Anonymous access information stored in the `statistics/anon_ftpstat` subdirectory of the virtual host directory.

Authorized access information stored in the `statistics/ftpstat/subdirectory`.

In addition, the `statistics` utility writes the statistical data to the `psa` database and calls the log rotation utility `logrotate`. For more information on statistics processing and log rotation, refer to the chapter *Statistics and Logs* (on page 128).

Mail Service

To provide a mail service, Parallels Plesk Panel supports two mail transfer agents: *Postfix* and *qmail*.

Panel uses only one mail transfer agent at a time. You can check which of them is currently enabled on the following page: **Server Administration Panel > Tools & Settings > Services Management**. You can also do this by running the `mailmng` utility located in the `$PRODUCT_ROOT_D/admin/sbin/directory`, where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems:

```
./mailmng --features | grep SMTP_Server
```

By default, Panel for Linux uses the Postfix for sending and receiving mail through the SMTP and SMTPS protocols. You can switch to qmail by running the following command:

```
# /usr/local/psa/admin/sbin/autoinstaller --select-release-current --install-component qmail
```

To switch to Postfix run the following command:

```
# /usr/local/psa/admin/sbin/autoinstaller --select-release-current --install-component postfix
```

Both Postfix and qmail use the same root directory to store incoming mail. This directory is defined by the variable `$PLESK_MAILNAMES_D` in the `/etc/psa/psa.conf` configuration file. By default, it is `/var/qmail/mailnames`. Storing incoming mail in the same directory allows the messages remain available after switching between mail agents.

Unlike incoming mail, the mail queue is lost while switching between the mail agents. Therefore, before switching, we recommend you stop the SMTP service to prevent the acceptance of email and the delivery of all queued mail. To stop the SMTP service, run the following command:

```
# /usr/local/psa/admin/sbin/mailmng --stop-smtpd
```

To flush the queue, run the command:

```
for qmail: # kill -ALRM `pidof qmail-send`
```

```
for Postfix: # postqueue -f
```

Next in this section:

Restoring Mail Configuration	38
Installing Custom SSL Certificates for Qmail or Courier-IMAP Mail Servers	39
Outgoing Mail from Exclusive IP Addresses	43

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 the internal `mchk` utility, which is 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` runs 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 Perl interpreter to be run. To speed up the restore process, 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.

Next in this section:

Installing an SSL Certificate for Qmail	40
Installing SSL Certificates for the Courier-IMAP Mail Server	42

Installing an 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` using your favorite text editor, and replace the contents of the file with the contents 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 the 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 the 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 the IMAP protocol.
- `/usr/share/courier-imap/pop3d.pem` - the certificate enables secure data transfers through the POP3 protocol.

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

4. Open a default certificate file 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-----
MIIB8TCCAZsCBEUpHKkWDQYJKoZIhvcNAQEEBQAwwYExCzAJBgNVBAYTA1JPMQww
.....
.....
eNpAIEF34UctLcHkZJGIK6b9Gktm
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDv6i/mxtS2B2PjShArtOamdRoEcCwa/LH1GcrbWl4zdbmIqrx
.....
.....
faXRHcG37Tkvg1UZ3wgy6eKuyrDi5gkwV8WAuaoNct5j5w==
-----END RSA PRIVATE KEY-----
```

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

Outgoing Mail from Exclusive IP Addresses

In earlier Panel versions, the outgoing mail of all customers was sent from a single IP address (defined by the mail server configuration). Thus, if one of the customers became blacklisted for sending spam, other customers were automatically blacklisted too since they used the same IP address. Also, if a customer had several IP addresses, and the address for outgoing mail did not match the address of the domain, the customer run a risk to be blacklisted as well.

In the current Panel version, the problem of domain and mail addresses is resolved, and Postfix mail server uses customers' IP addresses for sending mail if possible. This targets all outgoing mail of the Panel mail server sent by PHP mail(), `sendmail`, an SMTP script or client. However, if the following conditions are true, your system may send mail from different IP addresses:

- You have Postfix 2.7
- Panel is configured to support IPv6
- A subscription has only a single IPv4 or IPv6,

The outgoing mail for such subscriptions can be equally sent from either the customer's IP address or the server-defined IP address of the opposite type (IPv6 for IPv4 and vice versa). This server-defined IP address is specified in the mail server configuration.

Another part of this feature is the sender's address validation: The system validates the MAIL FROM header for authenticated users and corrects the header if needed. However, if the mail is sent without authentication, for example, from 127.0.0.1, through the local `sendmail`, or a sender is in the white list, the system trusts the MAIL FROM header.

Requirements

This feature is supported on all operating systems which have Postfix 2.7 or later. They are as follows:

Operating system	Postfix version
CentOS 5	Postfix 2.8.4 packaged by Parallels
CentOS 6	Postfix 2.8.4 packaged by Parallels
RedHat Enterprise Linux 5	Postfix 2.8.4 packaged by Parallels
RedHat Enterprise Linux 6	Postfix 2.8.4 packaged by Parallels
CloudLinux 5	Postfix 2.8.4 packaged by Parallels
CloudLinux 6	Postfix 2.8.4 packaged by Parallels
Ubuntu 10.04	Postfix 2.7

SuSE 11.3	Postfix 2.7
SuSE 11.4	Postfix 2.7
Debian 6	Postfix 2.7

If you independently install Postfix, run the following command to turn on the feature:

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

Read more about the utility in <http://kb.parallels.com/944>.

Mailing Lists Management System

Mailman is a GNU Mailing List Management System that provides a web-based mail list administration interface. It can work with almost all known mail transfer agents.

Mailman Directory Structure

Root directory:

```
/usr/lib/mailman
```

Executable Python scripts:

```
/usr/lib/mailman/bin/mailmanctl
```

```
/usr/lib/mailman/bin/qrunner
```

Startup script:

```
/etc/init.d/mailman with status|stop|start|restart options.
```

Note that `/etc/init.d` may be `/etc/rc.d/init.d` on some systems.

Configuration:

```
usr/lib/mailman/Mailman/Defaults.py
```

`usr/lib/mailman/Mailman/mm_cfg.py` is changed by the Panel when working with mail lists.

Mail lists:

```
/var/lib/mailman/lists/
```

Documentation:

```
/usr/share/doc/mailman-2.1.x/
```

Next in this section:

Configuring a Mailing List to Which only Members Are Allowed to Post..... 46

Importing a List of E-mail Addresses into a Mailing List..... 46

Configuring a Mailing List to Which only Members Are Allowed to Post

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

➤ *To configure a mailing list that 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. Therefore, if this option is disabled and unwanted mail is posted to the list, you can re-enable it and moderate incoming messages.

For more information, please see Mailman documentation 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 individually can take a long time. To automate this task you can use Parallels Plesk Panel command-line 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>]
```

Database Server

In addition to databases that store websites data, Panel has its own database for storing information about customer and resellers accounts, their subscriptions, and so on. This database is called *psa* and located on the local MySQL server. The local MySQL server is installed together with Panel and is required for Panel functioning. However, since version 11.5, you can replace the local MySQL server with an alternative database server, for example, *MariaDB* (<https://mariadb.org>) or *Percona Server* (<http://www.percona.com/software/percona-server>)

Below in this section we will explain how to replace MySQL with MariaDB. For other MySQL replacements, instructions are basically the same.

Next in this section:

Using MariaDB or Percona as the Default Database Server..... 47

Using MariaDB or Percona as the Default Database Server

Below we will provide instructions on replacing MySQL server with MariaDB server. For Percona Server, the steps are the same, the only differences are in configuring repositories and package names.

➤ To replace your MySQL server with MariaDB:

1. Back up databases located on your MySQL server. Use one of the following commands:

- To back up all databases:

```
# mysqldump -uadmin -p`< /etc/psa/.psa.shadow ` --all-databases |
gzip > /root/mysql.all.dump.sql.gz
```

- To back up only data required by Panel:

```
# mysqldump -uadmin -p`< /etc/psa/.psa.shadow ` --databases mysql
psa apsc | gzip > /root/mysql.mysql-psa-apsc.dump.sql.gz
```

2. Configure the MariaDB repository on your server. To generate the repository configuration for your operating system, use the wizard available at <https://downloads.mariadb.org/mariadb/repositories/>. When selecting the MySQL version, choose the version not less than your current MySQL version. Additionally, the version must not be higher than 5.5.

Note: Once you install MariaDB, do not disable this repository on your server. Panel requires it for updates.

3. Stop the Watchdog Panel extension if it is installed on your server and stop other monitoring services that can start the `mysql` service once you stop it manually.
4. Install MariaDB using one of the instructions provided below.
5. Switch on Watchdog and start other services you stopped on step 3.
6. Notify Panel about the changes in the MySQL component:
7. (Optional) If you experience MySQL errors after updating, restore the backup you created on step 1:

```
plesk sbin packagemng --set-dirty-flag
```

```
zcat /root/mysql.all.dump.sql.gz | mysql -uadmin -p`<
/etc/psa/.psa.shadow `
```

➤ To install MariaDB on CentOS or RedHat:

1. Stop the `mysql` service:

```
service mysqld stop
```

2. Remove the MySQL server from your server:

```
rpm -e --nodeps `rpm -q --whatprovides mysql-server`
```

3. Remove any leftovers of MySQL and install MariaDB:

Note: this will not remove any Panel packages except *plesk-mysql*.

```
yum shell
> remove mysql mysql-server plesk-mysql
> install MariaDB-server MariaDB-client MariaDB-compat MariaDB-
shared
> run
```

4. (Optional) Replace your MySQL configuration file `/etc/my.cnf` with the the MariaDB server's default one. This step is required if you are not sure that MariaDB can work with your configuration file. Usually, MariaDB is compatible with MySQL configuration files.

```
[ -f /etc/my.cnf.rpmnew ] && mv /etc/my.cnf.rpmnew /etc/my.cnf
```

5. Start the MariaDB server:

```
service mysql start
```

6. Update the tables structure:

```
mysql_upgrade -uadmin -p`< /etc/psa/.psa.shadow `
```

If you experience MySQL errors after updating, restore the backup you created on step 1:

```
zcat /root/mysql.all.dump.sql.gz | mysql -uadmin -p`<
/etc/psa/.psa.shadow `
```

➤ **To install MariaDB on Debian or Ubuntu:**

1. Synchronize package index files from new sources:

```
apt-get update
```

2. Depending on your OS and the selected MariaDB version, run one of the following commands:

- On Debian 7 or Ubuntu 12.04 (in this case, the only available MariaDB version is 5.5):

```
env DEBIAN_FRONTEND=noninteractive apt-get -o
OrderList::Score::Immediate=1000 install mariadb-server mysql-
common libmariadbclient18
```

- On Debian 6 or Ubuntu 10.04 and configured repositories for MariaDB 5.5:

```
env DEBIAN_FRONTEND=noninteractive apt-get -o
OrderList::Score::Immediate=1000 install mariadb-server mysql-
common
```

- On Debian 6 or Ubuntu 10.04 and configured repositories for MariaDB 5.2 or 5.3:

```
env DEBIAN_FRONTEND=noninteractive apt-get -o
OrderList::Score::Immediate=1000 install mariadb-server mysql-
common libmariadbclient16
```

Note: If during the installation the system asks you to provide the MariaDB password, leave it empty. Otherwise, Panel will be unable to access the MariaDB server and installation will fail.

➤ ***To install MariaDB on SuSE:***

1. Stop the `mysql` service:

```
service mysql stop
```

2. Install MariaDB:

```
zypper install mariadb
```

3. Start the MariaDB server:

```
systemctl --system daemon-reload  
service mysql start
```

➤ ***To perform a clean installation of Panel with MariaDB:***

1. Configure the MariaDB repository as described above.
2. Install MariaDB using instructions provided above.

If MySQL is not installed on the server, it is enough to run the following command:

- On CentOS or Redhat:

```
yum install MariaDB-server MariaDB-client MariaDB-compat
```

- On Debian or Ubuntu:

```
apt-get install mariadb-server
```

- On SuSE:

```
zypper install mariadb
```

3. Install Panel 11.5 or later as described in the **Installation, Upgrade, Migration, and Transfer Guide**. Make sure that the **MySQL server support** component is selected.

Website Applications

Multiple Web Apps in a Single Directory

Since Panel 10.4, when a site employs a number of various web apps, a site administrator may apply the following site structure:

- Install a number of apps to the same directory. More specifically, install one app into a subdirectory of another.
- Use the same document root for a subdomain and a web app.

For example, you can install an online store app to the `httpdocs` directory of your domain (for example, *example.com*), create a subdomain (for example, *support.example.com*) in the `httpdocs/support`, and install a help desk system there.

All earlier Panel versions (before 10.4) prohibited such scenarios as sometimes (in very rare cases), the installation of two web apps into one directory could lead to the improper functioning of one of them. If you want to return this restriction back, add the following lines into `/usr/local/psa/admin/conf/panel.ini`:

```
[aps]
unsafePaths=false
```

Hiding Commercial Apps

You can hide commercial web applications by default, so that your customers are able to install only free applications. To do this, add the following lines into `panel.ini`:

```
[aps]
commercialAppsEnabled = false
```

Spam Protection

SpamAssassin is a rule-based mail filter that identifies spam. It uses a wide range of heuristic tests on mail headers and body text to identify spam.

SpamAssassin filtering is configured on two levels:

- Server-level configuration is done by Panel administrator.
- Mail directory-level configuration is done by users for specific mail directories.

At the server level, you (as a Panel administrator) can enable or disable any of these two types of filters. Thus, there are four possible situations:

No filtering is applied, when spamd daemon is not running:

- both filters are disabled by the Parallels Plesk Panel administrator.
- the personal filter is disabled at the mail directory level.
- Filtering is applied at the server level only.
- Filtering is applied at the mail box level only.
- Filtering is applied at both levels.

When both filters are enabled for a specific mail name, a combined filter is created for the corresponding mail directory. When processing messages, SpamAssassin calculates the number of hits according to its internal rules. A message is considered to be spam if the number of hits exceeds the established threshold, which is set to 7 by default. You can change the threshold in Panel. White and Black lists can be considered special rules, which assign constant hit rates to messages conforming to mail address patterns in these lists:

If the message source address conforms to the Black list, the message gets +100 hits by default.

If the message source address conforms to the White list, the message gets -100 hits by default.

Sometimes, a message matches both Black and White lists. In that case, it has $+100-100=0$ hits.

If the message destination address is included in the server-wide ignore list, then all messages to this address will go directly to the addressed mail directory.

At the server level, you can configure SpamAssassin to mark messages with a special string if they are recognized as containing spam. At the mailbox level, you can make SpamAssassin delete or mark the message if it is considered as spam.

Starting from Panel 9.x, the maximum message size to filter is hardcoded in the spam handler and set to 256KB. This value provides normal server loading. Since the SpamAssassin service consists of perl modules, they may result in a heavy server load when processing long messages.

You can get more information on SpamAssassin at spamassassin.apache.org

Next in this section:

Configuring SpamAssassin	52
Training SpamAssassin to Work with All Mail Accounts on the Server	53
Fighting Spam on a Qmail Mail Server	54

Configuring SpamAssassin

The SpamAssassin configuration is stored in the spamfilter and spamfilter_preferences tables of the psa database. You can manage it with the \$PRODUCT_ROOT_D/admin/bin/spammng utility. It displays help if started without any options.

Server-wide SpamAssassin settings are stored in the following files:

The /usr/share/spamassassin/*.cf files contain configuration details, e.g. White list and Black list scores are assigned in the 50_scores.cf configuration file.

The /etc/mail/spamassassin/local.cf stores server-wide filter settings.

When Panel works with virtual mail users (not real system users with UIDs) spamd is executed with keys showing where to find the configuration files of virtual users:

-x --virtual-config-dir={QMAIL_MAILNAMES_D}/%d/%l User settings are stored in the following files:

/var/qmail/mailnames/<domain>/<mailname>/.spamassassin/user_prefs file defines SpamAssassin actions.

/var/qmail/mailnames/<domain>/<mailname>/.qmail defines how message flow reaches SpamAssassin daemons.

If the message destination address is included in the server-wide ignore list then all messages to this address will go directly to the addressed mail directory. For example, if you include admin@domain01.tst in this list, then the .qmail file will look like this:

```
# cat /var/qmail/mailnames/domainXX.tst/mailuser/.qmail
| /usr/local/psa/bin/psa-spamc accept
| true
| /usr/bin/deliverquota ./Maildir
```

If SpamAssassin filtering is allowed then the following command allows the mail to go through the spam filter first and then to the mailbox added to this file:

```
| spamc -f -u admin@domainXX.tst|maildir ./Maildir/
```

You can find examples of spam-like and no-spam messages in:

/usr/share/doc/spamassassin-3.2.x/sample-nospam.txt

/usr/share/doc/spamassassin-3.2.x/sample-spam.txt

Training SpamAssassin to Work with All Mail Accounts on the Server

You can manually train SpamAssassin to work with all mail accounts on the server from the command line.

➤ ***To train SpamAssassin to work with 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 to work with 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.

Fighting Spam on a Qmail Mail Server

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

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

1. Make sure that all domains have the option **What to do with mail sent to nonexistent users** set to **Reject**.

To change the value of this option for a domain, open it in the **Control Panel**, go to the **Mail** tab and click **Change Settings**.

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 on 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 message senders and recipients. If a message has too many recipients, then it is 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 at the message and find the last `Received` line. This shows 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)
```

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

- If the `Received` line contains an UID of an apache user (for example `invoked by uid 48`), it means that the spam was sent via a 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 it is usually hard to find the spam source in this case. If you are sure that a script is sending spam at the current moment (for example, because the queue is growing 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 is sending 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 to domain folders where the script that sends the mail is located.

You can see all the folders from which mail PHP scripts were run by using 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 the `PHP mail()` function from the Parallels Plesk Panel virtual hosts directory.

Antivirus Support

Parallels Plesk Panel for Linux supports the following antivirus software:

- *Parallels Premium Antivirus* based on Dr.Web.
- *Kaspersky Antivirus*.

Both these solutions provide you with real-time mail traffic scanning and malware protection for customers. In this section you will find detailed information on these antivirus solutions.

Next in this section:

Parallels Premium Antivirus.....	57
Kaspersky Antivirus.....	59

Parallels Premium Antivirus

Parallels Premium Antivirus is shipped with Panel in the form of RPM packages.

Directory Structure

Root directory:

/opt/drweb/

Configuration files:

/etc/drweb/ is a directory with various configuration files.

/etc/drweb/drweb32.ini is the default configuration file for drwebd engine.

/etc/drweb/drweb_qmail.conf is the configuration file for the qmail-queue filter.

/etc/drweb/users.conf stores the configuration for every mail name for which antivirus is enabled.

Virus databases:

/var/drweb/bases/*vdb

Quarantine directory:

/var/drweb/infected/

Log file:

/var/drweb/log/drwebd.log

Managing the Antivirus

The Dr.Web service is a standalone drwebd daemon (also called engine), which is started from the /etc/init.d/drwebd script. You can also stop and start it again with the following command:

```
# /etc/init.d/psa stopall
# /etc/init.d/psa start
```

Note: these commands stop and start other Panel services: DNS server, mail server, and so on

You can also manage it within the **Services Management** page in the Server Administration Panel.

The interaction with drwebd is established through the Dr.Web client. It can change antivirus parameters and start checking files. The client displays a full list of its attributes if run without attributes. Also, it can extract detailed operational information from the engine. The following command gives information about the Dr.Web version and virus database.

```
# /opt/drweb/drwebdc -sv -sb
```

By default, the virus databases are updated every 30 minutes by means of the cron task:
`/opt/drweb/update/update.pl >dev/null 2>&1`

Filtering Mail

Dr.Web substitutes the native `qmail-queue` filter used for transferring incoming messages to the `qmail` queue with its own utility. The utility's configuration settings are stored in the `/etc/drweb/drweb_handler.conf` file.

Dr.Web filtering is activated on the mail name level. If enabled it can check incoming, outgoing or both kinds of messages. The information is stored in the `/etc/drweb/users.conf` file. The following is an example of three mail names with different Dr.Web configurations:

```
# grep domain01 /etc/drweb/users.conf
allow  any    regex  ^admin@domain01.tst$
allow  to     regex  ^user01@domain.tst$
allow  from   regex  ^user02@domain.tst$
```

In the above configuration, Dr.Web will check viruses in:

Incoming and outgoing messages for `admin@domain01.tst`

Incoming messages for `user01@domain01.tst`

Outgoing messages for `user02@domain01.tst`

Kaspersky Antivirus

Kaspersky Antivirus is a module that scans incoming and outgoing mail traffic on your server, and removes malicious and potentially dangerous code from e-mail messages. In order to use Kaspersky Antivirus with your Parallels Plesk Panel server, you need to install the Kaspersky Antivirus module, then purchase and install a license key.

Kaspersky Antivirus is distributed as an RPM package.

Kaspersky Antivirus Structure

Kaspersky Antivirus resides in the following directories in Panel.

`/opt/kav/5.5/kav4mailservers` - the main directory.

`/etc/kav/5.5/kav4mailservers/kav4mailservers.conf` - a configuration file that contains parameters as key=value pairs grouped by sections. They define the operation of all Kaspersky Antivirus components. All configuration file parameters are grouped into sections, each of them corresponding to a particular component of the product.

`/var/db/kav/5.5/kav4mailservers/bases` - a path to the anti-virus database directory.

`/var/db/kav/5.5/kav4mailservers/licenses` - a path to the license keys directory.

Incoming and outgoing mail messages are processed like this:

1. The stream of mail messages comes in from other servers or mail clients via the SMTP protocol.
2. The mail system receives the mail traffic and passes it to Kaspersky Antivirus for scanning.
3. The application processes the mail traffic according to the specified settings, and returns it to the mail system along with an additional set of notifications.
4. The mail system routes the mail traffic to its destination.

System Maintenance

This chapter discusses tasks that administrators may need to perform on an existing Panel installation. In particular, the chapter provides overviews on how to manage Panel through the command line and execute scripts or binaries on certain Panel events. In addition, you will learn how to adjust Panel settings to fit a new network environment or server configuration, and restart Panel to apply new settings.

In this chapter:

Managing Panel Objects Through the Command Line	60
Executing Custom Scripts on Panel Events.....	61
Changing IP Addresses.....	61
Changing Paths to Services	62
Restarting Panel.....	63
Managing Services from the Command Line and Viewing Service Logs	63
Moving the Panel GUI to a Separate IP Address.....	74

Managing Panel Objects Through the Command Line

Parallels Plesk Panel Command Line Interface (CLI) is designed for integrating Panel with third-party applications. Panel administrators can also use it to create, manage, and delete customer and domain accounts, and other Panel objects from the command line. CLI utilities require administrative permissions on Panel server to run.

The utilities reside in the following directories:

- On RPM-based systems: `/usr/local/psa/bin`
- On DEB-based systems: `/opt/psa/bin`

Upon successful execution, utilities return the 0 code. If an error occurs, utilities return code 1 and display the error details.

To learn more about Panel command line utilities, refer to **Panel 11.5 Command Line Reference** at <http://download1.parallels.com/Plesk/PP11/11.5/Doc/en-US/online/plesk-unix-cli/>.

Executing Custom Scripts on Panel Events

Parallels Plesk Panel provides a mechanism that allows administrators to track specific Panel events and make Panel execute custom scripts when these events occur. The events include operations that Panel users perform on accounts, subscriptions, websites, service plans, and various Panel settings. For example, you can save each added IP address to a log file or perform other routine operations.

To learn how to track Panel events and set up execution of commands or custom scripts, refer to **Parallels Plesk Panel Administrator's Guide**, chapter **Event Tracking**.

Changing IP Addresses

During the lifetime of a Parallels Plesk Panel server, you may need to change the IP addresses employed by Panel. Two typical cases when IP addresses may need to be changed are the following:

- Reorganization of the server IP pool. For example, substitution of one IP address with another.
- Relocation of Panel to another server. Changing all addresses used by Panel (including the one on which Panel resides) to those on the new server.

Every time the change happens, you should reconfigure all related system services. To help you do this promptly, we offer the `reconfigurator` command line utility located in the following directory:

- on RPM-based systems: `/usr/local/psa/bin`.
- on DEB-based systems: `/opt/psa/bin`.

The `reconfigurator` replaces IP addresses and modifies Panel and services configuration to make the system work properly after the replacement. To do this, the utility requires a mapping file, that includes instructions on what changes to make. Each line of the file should describe a single change. For example, the following line instructs Panel to change the IP address 192.168.50.60 to 192.168.50.61:

```
eth0:192.168.50.60 255.255.255.0 -> eth0:192.168.50.61 255.255.255.0
```

The utility also helps you with creation of the mapping file. If you call the utility with a new file name as an option, it will create the file and write all available IP addresses to it. The IP addresses in the file are mapped to themselves. If you want to perform a change, modify the change instruction for a certain IP address.

When editing the mapping file, consider the following:

- A replacement IP address must not exist in the Panel IP pool before changing; however, it may be in the server IP pool. To make sure the IP is not in the Panel IP pool, go to **Server Administration Panel > Tools & Settings > IP Addresses** and remove the IP if necessary.
- If a replacement IP address does not exist in the server IP pool, the utility adds it to both Panel and server IP pools.

➤ **To change IP addresses used by Panel:**

1. Generate a mapping file with current Panel IP addresses by running the command:

```
./reconfigurator <ip_map_file_name>
```

2. Edit the file as described above and save it.

3. Reconfigure Panel and its services by running the following command one more time:

```
./reconfigurator <ip_map_file_name>
```

Changing Paths to Services

Parallels Plesk Panel uses various external components, for example, Apache web server, mail service, antivirus, and so on. When interacting with these components, Panel gets the information on their locations from the configuration file `/etc/psa/psa.conf`.

Panel configuration file provides an easy way of reconfiguring Panel if a service is installed into another directory or migrated from the current partition to another. Note that you can only modify paths present in this file; other paths are hard-coded in Panel components.

Each line of `psa.conf` has the following format:

```
<variable_name> <value>
```

A sample part of the `psa.conf` file is displayed below. To change a path to a service, utility, or package, specify the new path as a value of a corresponding variable.

```
# Plesk tree
PRODUCT_ROOT_D /usr/local/psa
# Directory of SysV-like Plesk initscripts
PRODUCT_RC_D /etc/init.d
# Directory for config files
PRODUCT_ETC_D /usr/local/psa/etc
# Directory for service utilities
PLESK_LIBEXEC_DIR /usr/lib/plesk-9.0
# Virtual hosts directory
HTTPD_VHOSTS_D /var/www/vhosts
# Apache configuration files directory
HTTPD_CONF_D /etc/httpd/conf
# Apache include files directory
HTTPD_INCLUDE_D /etc/httpd/conf.d
# Apache binary
HTTPD_BIN /usr/sbin/httpd
# Apache log files directory
HTTPD_LOG_D /var/log/httpd
# apache startup script
HTTPD_SERVICE httpd
# Qmail directory
QMAIL_ROOT_D /var/qmail
```

Important: Be very careful when changing the contents of `psa.conf`. Mistakes in paths specified in this file may lead to Panel malfunctioning.

Restarting Panel

If you experience problems with Parallels Plesk Panel, for example, malfunctioning of a service, you can try to resolve them by restarting Panel or the administrative web server `sw-cp-server`. Also, a restart is necessary to apply configuration changes that cannot be made while Panel is running.

➤ **To restart Parallels Plesk Panel, run the following command:**

```
/etc/init.d/psa restart
```

➤ **To restart `sw-cp-server`, run the following command:**

```
/etc/init.d/sw-cp-server restart
```

Managing Services from the Command Line and Viewing Service Logs

This section describes how to stop, start, and restart services managed by Panel, and access their logs and configuration files.

Parallels Plesk Panel web interface

To start the service through the command line:

```
/etc/init.d/psa start
```

To stop the service through the command line:

```
/etc/init.d/psa stop
```

To restart the service through the command line:

```
/etc/init.d/psa restart
```

Panel log files are located in the following directories:

- **Error Log:** `/var/log/sw-cp-server/error_log`

Access log: `/usr/local/psa/admin/logs/httpsd_access_log` Panel configuration files are the following:

- **php:** `$PRODUCT_ROOT_D/admin/conf/php.ini`
- **www:** `/etc/sw-cp-server/applications.d/plesk.conf`

Presence Builder

Log files are located in:

- **Error log:** `/var/log/httpd/sitebuilder_error.log`

Logs: `/usr/local/sitebuilder/tmp/` **Configuration files are accessible at:**

- `/usr/local/sitebuilder/config`
- `/usr/local/sitebuilder/etc/php.ini`

SSO

Log files are located in:

- **Error log:** `/var/log/sw-cp-server/error_log`

SSO log: `/var/log/sso/sso.log` **Configuration files are accessible at:**

- `/etc/sw-cp-server/applications.d/sso-cpserver.conf`
- `/etc/sso/sso_config.ini`

phpMyAdmin

The error log is located in:

`/var/log/sw-cp-server/error_log`

The configuration file is accessible at:

`/usr/local/psa/admin/htdocs/domains/databases/phpMyAdmin/libraries/config.default.php`

phpPgAdmin

The error log is located in:

`/var/log/sw-cp-server/error_log`

The configuration file is accessible at:

`/usr/local/psa/admin/htdocs/domains/databases/phpPgAdmin/conf/config.inc.php`

DNS / Named / BIND

To start the service through the command line:

```
/etc/init.d/named start
```

To stop the service through the command line:

```
/etc/init.d/named stop
```

To restart the service through the command line:

```
/etc/init.d/named restart
```

Log files are located in:

```
/var/log/messages
```

The configuration file is accessible at:

```
/etc/named.conf
```

FTP (ProFTPD)

Log files are located in:

```
/usr/local/psa/var/log/xferlog
```

Configuration files are accessible at:

- /etc/xinetd.d/ftp_psa
- /etc/proftpd.conf
- /etc/proftpd.include

Courier-IMAP

To start the service through the command line:

```
/etc/init.d/courier-imap start
```

To stop the service through the command line:

```
/etc/init.d/courier-imap stop
```

To restart the service through the command line:

```
/etc/init.d/courier-imap restart
```

Log files are located in:

```
/usr/local/psa/var/log/maillog
```

Configuration files are accessible at:

- /etc/courier-imap/imapd
- /etc/courier-imap/imapd-ssl
- /etc/courier-imap/pop3d
- /etc/courier-imap/pop3d-ssl

QMail

To start the service through the command line:

```
/etc/init.d/qmail start
```

To stop the service through the command line:

```
/etc/init.d/qmail stop
```

To restart the service through the command line:

```
/etc/init.d/qmail restart
```

Log files are located in:

```
/usr/local/psa/var/log/maillog
```

Configuration files are accessible at:

- /etc/xinetd.d/smtp_psa
- /etc/xinetd.d/smtps_psa
- /etc/xinetd.d/submission_psa
- /etc/inetd.conf (Debian)
- /var/qmail/control/

Postfix

To start the service through the command line:

```
/etc/init.d/postfix start
```

To stop the service through the command line:

```
/etc/init.d/postfix stop
```

To restart the service through the command line:

```
/etc/init.d/postfix restart
```

Log files are located in:

```
/usr/local/psa/var/log/maillog
```

Configuration files are accessible at:

```
/etc/postfix/
```

SpamAssassin

To start the service through the command line:

```
/etc/init.d/psa-spamassassin start
```

To stop the service through the command line:

```
/etc/init.d/psa-spamassassin stop
```

To restart the service through the command line:

```
/etc/init.d/psa-spamassassin restart
```

Log files are located in:

```
/usr/local/psa/var/log/maillog
```

Configuration files are accessible at:

- /etc/mail/spamassassin/
- /etc/mail/spamassassin/local.cf
- /var/qmail/mailnames/%d/%l/.spamassassin

Dr.Web antivirus

To start the service through the command line:

```
/etc/init.d/drwebd start
```

To stop the service through the command line:

```
/etc/init.d/drwebd stop
```

To restart the service through the command line:

```
/etc/init.d/drwebd restart
```

Log files are located in:

```
/usr/local/psa/var/log/maillog
```

Configuration files are accessible at:

```
/etc/drweb/
```

Kaspersky antivirus

To start the service through the command line:

```
/etc/init.d/aveserver start
```

To stop the service through the command line:

```
/etc/init.d/aveserver stop
```

To restart the service through the command line:

```
/etc/init.d/aveserver restart
```

Log files are located in:

- /usr/local/psa/var/log/maillog
- /var/log/kav/5.5/kav4mailservers/aveserver.log
- /var/log/kav/5.5/kav4mailservers/smtpscanner.log
- /var/log/kav/5.5/kav4mailservers/avstats.log
- /var/log/kav/5.5/kav4mailservers/kavscanner.log

`/var/log/kav/5.5/kav4mailservers/kavupdater.log` Configuration files are accessible at:

`/etc/kav/5.5/kav4mailservers/`

Tomcat

To start the service through the command line:

```
/etc/init.d/tomcat5 start
```

To stop the service through the command line:

```
/etc/init.d/tomcat5 stop
```

To restart the service through the command line:

```
/etc/init.d/tomcat5 restart
```

Log files are located in:

`/var/log/tomcat5/`

Configuration files are accessible at:

`/usr/share/tomcat5/conf/`

MySQL

To start the service through the command line:

```
/etc/init.d/mysqld start
```

To stop the service through the command line:

```
/etc/init.d/mysqld stop
```

To restart the service through the command line:

```
/etc/init.d/mysqld restart
```

Log file is located in:

`/var/log/mysqld.log`

The configuration file is accessible at:

`/etc/my.cnf`

PostgreSQL

To start the service through the command line:

```
/etc/init.d/postgresql start
```

To stop the service through the command line:

```
/etc/init.d/postgresql stop
```

To restart the service through the command line:

```
/etc/init.d/postgresql restart
```

Startup log is located in:

```
/var/lib/pgsql/pgstartup.log
```

The configuration file is accessible at:

```
/var/lib/pgsql/data/postgresql.conf
```

xinetd

To start the service through the command line:

```
/etc/init.d/xinetd start
```

To stop the service through the command line:

```
/etc/init.d/xinetd stop
```

To restart the service through the command line:

```
/etc/init.d/xinetd restart
```

Log files are located in:

```
/var/log/messages/
```

The configuration file is accessible at:

```
/etc/xinetd.conf
```

Watchdog (monit)

To start the service through the command line:

```
/usr/local/psa/admin/bin/modules/watchdog/wd --start
```

To stop the service through the command line:

```
/usr/local/psa/admin/bin/modules/watchdog/wd --stop
```

To restart the service through the command line:

```
/usr/local/psa/admin/bin/modules/watchdog/wd --restart
```

Log files are located in:

- `/usr/local/psa/var/modules/watchdog/log/wdcollect.log`

`/usr/local/psa/var/modules/watchdog/log/monit.log` Configuration files are accessible at:

- `/usr/local/psa/etc/modules/watchdog/monitrc`
- `/usr/local/psa/etc/modules/watchdog/wdcollect.inc.php`

Watchdog (rkhunter)

Log is located in:

```
/var/log/rkhunter.log
```

The configuration file is accessible at:

```
/usr/local/psa/etc/modules/watchdog/rkhunter.conf
```

Apache

To start the service through the command line:

```
/etc/init.d/httpd start
```

To stop the service through the command line:

```
/etc/init.d/httpd stop
```

To restart the service through the command line:

```
/etc/init.d/httpd restart
```

Log files are located in:

- /var/log/httpd/

/var/www/vhosts/<domain_name>/statistics/logs/ Configuration files are accessible at:

- /etc/httpd/conf/httpd.conf
- /etc/httpd/conf.d/
- /var/www/vhosts/<domain_name>/conf/httpd.include

Mailman

To start the service through the command line:

```
/etc/init.d/mailman start
```

To stop the service through the command line:

```
/etc/init.d/mailman stop
```

To restart the service through the command line:

```
/etc/init.d/mailman restart
```

Log files are located in:

```
/var/log/mailman/
```

Configuration files are accessible at:

- /etc/httpd/conf.d/mailman.conf
- /usr/lib/mailman/Mailman/mm_cfg.py

- `/etc/mailman/sitelist.cfg`

AWstats

To start the service through the command line:

```
/usr/local/psa/bin/sw-engine-pleskrun
/usr/local/psa/admin/plib/DailyMaintainance/script.php
```

Configuration files are accessible at:

```
/usr/local/psa/etc/awstats/
```

Webalizer

To start the service through the command line:

```
/usr/local/psa/bin/sw-engine-pleskrun
/usr/local/psa/admin/plib/DailyMaintainance/script.php
```

Configuration files are accessible at:

```
/var/www/vhosts/<domain_name>/conf/webalizer.conf
```

Backup Manager

Backup logs are located in:

- `/usr/local/psa/PMM/sessions/<session>/psadump.log`
- `/usr/local/psa/PMM/sessions/<session>/migration.log`
- `/usr/local/psa/PMM/logs/migration.log`

`/usr/local/psa/PMM/logs/pmmcli.log` Restore logs are located in:

- `/usr/local/psa/PMM/rsessions/<session>/conflicts.log`
- `/usr/local/psa/PMM/rsessions/<session>/migration.log`
- `/usr/local/psa/PMM/logs/migration.log`

`/usr/local/psa/PMM/logs/pmmcli.log` The configuration file is accessible at:

```
/etc/psa/psa.conf
```

Plesk Migration Manager

Migration logs are located in:

- `/usr/local/psa/PMM/msessions/<session>/migration.log`
- `/usr/local/psa/PMM/rsessions/<session>/migration.log`
- `/usr/local/psa/PMM/rsessions/<session>/conflicts.log`
- `/usr/local/psa/PMM/logs/migration.log`

- `/usr/local/psa/PMM/logs/pmmcli.log`
- `/usr/local/psa/PMM/logs/migration_handler.log`

Horde

Log is located in:

`/var/log/psa-horde/psa-horde.log`

Configuration files are accessible at:

- **Apache configuration**
 - `/etc/httpd/conf.d/zzz_horde_vhost.conf`
 - `/etc/psa-webmail/horde/conf.d/`
- **Horde configuration:**
`/etc/psa-webmail/horde/`

Atmail

Log files are located in:

`/var/log/atmail/`

Configuration files are accessible at:

- **Apache configuration**
 - `/etc/httpd/conf.d/zzz_atmail_vhost.conf`
 - `/etc/psa-webmail/atmail/conf.d/`
- **Atmail configuration:**
 - `/etc/psa-webmail/atmail/atmail.conf`
 - `/var/www/atmail/libs/Atmail/Config.php`

psa-logrotate

To start the service through the command line:

```
/usr/local/psa/bin/sw-engine-pleskrun  
/usr/local/psa/admin/plib/DailyMaintenance/script.php
```

Configuration files are accessible at:

- `/usr/local/psa/etc/logrotate.conf`
- `/usr/local/psa/etc/logrotate.d/`

Samba

To start the service through the command line:

```
/etc/init.d/smb start
```

To stop the service through the command line:

```
/etc/init.d/smb stop
```

To restart the service through the command line:

```
/etc/init.d/smb restart
```

Log files are located in:

```
/var/log/samba/
```

Configuration files are accessible at:

- /etc/samba/smb.conf
- /etc/samba/smb.conf.include

psa-firewall

To start the service through the command line:

```
/etc/init.d/psa-firewall start
```

To stop the service through the command line:

```
/etc/init.d/psa-firewall stop
```

To restart the service through the command line:

```
/etc/init.d/psa-firewall restart
```

Configuration files are accessible at:

- /usr/local/psa/var/modules/firewall/firewall-active.sh
- /usr/local/psa/var/modules/firewall/firewall-emergency.sh
- /usr/local/psa/var/modules/firewall/firewall-new.sh

psa-firewall (IP forwarding)

To start the service through the command line:

```
/etc/init.d/psa-firewall-forward start
```

To stop the service through the command line:

```
/etc/init.d/psa-firewall-forward stop
```

To restart the service through the command line:

```
/etc/init.d/psa-firewall-forward restart
```

Configuration files are accessible at:

- /usr/local/psa/var/modules/firewall/ip_forward.active
- /usr/local/psa/var/modules/firewall/ip_forward.saved

psa-vpn

To start the service through the command line:

```
/etc/init.d/smb start
```

To stop the service through the command line:

```
/etc/init.d/smb stop
```

To restart the service through the command line:

```
/etc/init.d/smb restart
```

The configuration file is accessible at:

```
/usr/local/psa/var/modules/vpn/openvpn.conf
```

Moving the Panel GUI to a Separate IP Address

By default, the Panel GUI can work on all IP addresses available on the Panel server (from the server's IP pool). You may want to allow access to the Panel GUI only from the local network. For that, you should move the GUI to an internal IP address.

To move Panel GUI to a separate IP address, in the configuration file `/etc/sw-cp-server/conf.d/plesk.conf`, replace the lines

```
listen 8443 ssl
listen 8880;
```

with the lines

```
listen SPECIFIC_SERVER_IP:8443 ssl
listen SPECIFIC_SERVER_IP:8880;
```

where `SPECIFIC_SERVER_IP` is the new IP address that you want to use for the Panel GUI.

Do not change the ports.

Backing Up, Restoring, and Migrating Data

This chapter describes how to back up and restore data by means of the command-line utilities `pleskbackup` and `pleskrestore`, and introduces the tools for migrating hosted data between servers.

Backing up by means of the `pleskbackup` utility is done by issuing a command that specifies the objects to be backed up. The utility creates a backup archive containing settings and content. You can then perform a full or a selective restoration of data, and specify how to resolve possible conflicts that might occur.

In this chapter:

Backing Up Data	76
Restoring Data	96
Migrating and Transferring Data	127

Backing Up Data

To perform a backup of Panel hosting data, you need to execute the `pleskbackup` utility command that does the following:

1. Defines the data that need to be backed up.
2. Defines the way the backup process will be performed.
3. Defines properties of the files that will be contained in the backup.
4. Defines options for exporting the backup as a single file.

Note: Only the first component is obligatory; the others are optional.

The following sections explain the meaning and implementation of each component in detail.

The `pleskbackup` utility is located in `$PRODUCT_ROOT_D/bin/pleskbackup` where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

To see a complete list of the `pleskbackup` commands and options, refer to the section **Backup Utility Commands and Options** (on page 92).

If the command execution succeeds, a backup is created in the default server backup location, or is exported to a file if exporting options were specified. For details on exporting options, refer to the section **Exporting Backup Files** (on page 88). If the command execution fails, a backup is not created.

You can perform advanced configuration of the backup operation through the file `$PRODUCT_ROOT_D/admin/share/pmmcli/pmmcli-rc`. For more details, refer to the section **Defining How the Backup Process Is Performed** (on page 90).

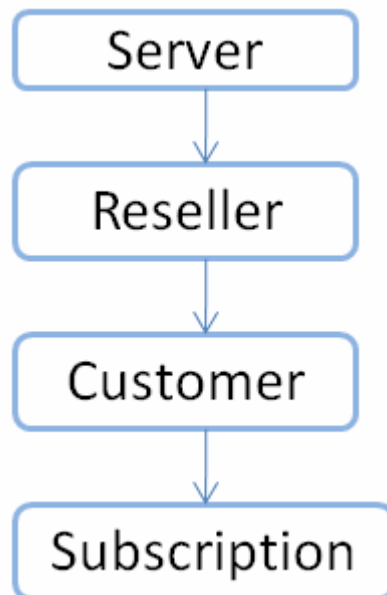
If a backup process fails, you can use its logs for troubleshooting. Each backup process's logs are stored in `$PRODUCT_ROOT_D/PMM/logs/backup-YYYY-MM-DD-hh-mm-nnn/`, where `YYYY-MM-DD-hh-mm` is the date and time when the backup was performed and `nnn` is a randomly generated number.

Next in this section:

Backup Objects: Hierarchy and Volume	77
Specifying Data for Backing Up	80
Defining Properties of Files That Compose the Backup.....	86
Exporting Backup Files.....	88
Defining How the Backup Process Is Performed	90
Backup Utility Commands and Options	92

Backup Objects: Hierarchy and Volume

Panel provides opportunities for backing up and restoring nearly all hosting data, which includes main Panel objects: administrator account, settings for Panel-managed services, reseller accounts, customer accounts, subscriptions, websites, databases and mail accounts. These backup objects are organized into a hierarchy where parent object is always an owner of its children. The hierarchy comprises of four levels: *server*, *resellers*, *customers* and *subscriptions*. The levels are such that a higher level includes objects on the lower levels but a lower level is completely separated from the higher objects.



You can create either a full or a partial backup. A full backup is the highest-level backup and includes all data related to a Panel installation. A partial backup includes only the desired Panel objects of any of the levels. For information on available options when creating a partial backup, refer to the section *Specifying Data for Backing Up* (on page 80).

Restoring a backup, in turn, can also be either full or partial. Full restoration recovers all data contained in a backup, and partial recovers part of this data. For information on available options when restoring data from backups, refer to the **Defining Objects for Restoration** (on page 97) section.

Each backup object includes the following:

- *Configuration* defines the properties of the backup object *and its descendants*.
- *Content* contains binary data related *only* to the backup object (website content and content of mailboxes).

This table shows what data (configuration and content) are related to each backup object.

Backup Object Type	Configuration	Content

Backup Object Type	Configuration	Content
<i>server</i>	<p>This backup level includes the following:</p> <ul style="list-style-type: none">▪ Administrator information.▪ Presence Builder settings.▪ SSO settings.▪ IP addresses.▪ Database server settings.▪ DNS settings.▪ Mail server settings.▪ Antivirus and spam protection settings.▪ SSL certificates.▪ Reseller plans, hosting plans, and add-on plans.▪ Information about administrator's subscriptions, reseller accounts, customer accounts and websites.▪ Information about user roles.▪ Information about auxiliary users who can access Control Panel.▪ Information about mail accounts and individual settings for protection from spam and viruses .▪ Site isolation settings.▪ Settings for notification on system events.	License keys for Panel, virtual host templates, website content, error documents, log files, and content of mailboxes.
<i>reseller</i>	<p>This backup level includes the following:</p> <ul style="list-style-type: none">▪ Reseller information.▪ Reseller's hosting plans.▪ Resource allotments and permissions for operations in Panel.▪ Allocated IP addresses.▪ Information about customer accounts, subscriptions, and websites with DNS settings.▪ Information about user roles.▪ Information about auxiliary users who can access Control Panel.▪ Information about mail accounts and individual settings for protection from spam and viruses.	Website content, error documents, log files, content of mailboxes.

Backup Object Type	Configuration	Content
<i>customer</i>	<p>This backup level includes the following:</p> <ul style="list-style-type: none">▪ Customer information.▪ Hosting plans to which the customer is subscribed.▪ Resource allotments and permissions for operations in Control Panel.▪ IP addresses used by customer's subscriptions.▪ Information about websites with DNS settings.▪ Information about user roles.▪ Information about auxiliary users who can access Control Panel.▪ Information about mail accounts and individual settings for protection from spam and viruses.	Website content, error documents, log files, content of mailboxes.
<i>subscription</i>	<p>This backup level includes the following:</p> <ul style="list-style-type: none">▪ Information about a subscription, its owner and associated hosting plan.▪ IP addresses allocated to the subscription.▪ Resource allotments and permissions for operations in Control Panel.▪ Information about websites with DNS settings.▪ Information about mail accounts and individual settings for protection from spam and viruses.	Website content, error documents, log files, content of mailboxes.

Specifying Data for Backing Up

Defining data that should be backed up includes the following:

1. Defining the backup level and, unless it is the server level, optionally, selecting which resellers, customers, or subscriptions should be backed up.
2. (Optional). Defining which resellers, customers, or subscriptions should be excluded from the backup.
3. (Optional). Restricting backup to either only mail content, web hosting content, or their configuration.
4. (Optional). Specifying that log files are excluded from backup.

Generally speaking, the data that can be backed up with one call of the `pleskbackup` utility are represented by any single cell of the following table.

		(All)		Only web hosting settings option: <code>--only-hosting</code>		Only mail option: <code>--only-mail</code>	
		(All)	Only configuration option: <code>-c</code>	(All)	Only configuration option: <code>-c</code>	(All)	Only configuration option: <code>-c</code>
Server command: <code>server</code>	(All)						
	Excluding resellers options: <code>--exclude-reseller</code> or <code>--exclude-reseller-file</code>						
	Excluding customers options: <code>--exclude-client</code> or <code>--exclude-client-file</code>						
	Excluding subscriptions options: <code>--exclude-domain</code> or <code>--exclude-domain-file</code>						

All or selected resellers command: resellers-name or resellers-id	(All) / (All selected)				Example 1		
	Excluding resellers options: --exclude-reseller or --exclude-reseller-file				Example 1*		
	Excluding customers options: --exclude-client or --exclude-client-file						
	Excluding subscriptions options: --exclude-domain or --exclude-domain-file						
All or selected customers command: clients-name or clients-id	(All) / (All selected)						
	Excluding customers options: --exclude-client or --exclude-client-file						
	Excluding subscriptions options: --exclude-domain or --exclude-domain-file						

All or selected subscriptions	(All) / (All selected)					Example 2	
command: domains-name or domains-id	Excluding subscriptions options: --exclude-domain or --exclude-domain-file						

Example 1

With one call of `pleskbackup`, you can back up hosting data for several resellers (rows 5 or 6 in the table, depending on what is more convenient: to list resellers that should be included or those to be excluded) and restricting the backup data to configuration of web hosting on sites owned by the resellers or their customers (column 4 in the table).

To back up website hosting configuration of resellers with usernames `reseller1` and `reseller2`, issue the following command:

```
pleskbackup resellers-name "reseller1 reseller2" --only-hosting -c
```

Example 2

With one call of `pleskbackup`, you can back up the mail configuration and content of mail accounts (column 5) for all subscriptions existing on the server (row 12).

To back up mail accounts with messages for all subscriptions:

```
pleskbackup domains-name --only-mail
```

The rest of this section explains each option in detail and provides examples of commands.

Defining backup level and selecting objects

To define the backup level and select backup objects, the commands of the `pleskbackup` utility are used.

If performing a selective backup, resellers, customers or subscriptions selected for the backup should be specified by their identifiers which are either usernames or IDs. The specification can be done in one of the following two ways:

- *Command line specification.* The backup command takes object identifiers as arguments separated with spaces.
- *File specification.* The backup command takes the `--from-file` option which specifies the file where the identifiers of objects are listed. The file must be in plain text format, and object identifiers are separated by line breaks (i.e., one identifier per line).

Note: If a command contains both specifications, file specification is used and the command line specification is ignored.

➤ To back up all data related to Panel installation:

```
pleskbackup server
```

➤ To back up all resellers, customers, or subscriptions:

```
pleskbackup <resellers|clients|domains>--<name|id>
```

For example, to back up all customer accounts:

```
pleskbackup clients-name
```

or

```
pleskbackup clients-id
```

➤ **To back up several resellers, customers, or subscriptions defined in the command line:**

```
pleskbackup <resellers|clients|domains>--<name|id> [
<identifier1> [
<identifier2> ... [<identifier n>]]
```

For example, to back up three resellers defined in the command line:

```
pleskbackup resellers-name "johndoe janedoe josephine"
```

➤ **To back up several resellers, customers, or subscriptions listed in a file:**

```
pleskbackup <resellers|clients|domains>--<name|id> --from-file=<file>
```

For example,

```
pleskbackup resellers-name --from-file="etc/backup lists/backup"
```

Defining which objects should be excluded

Objects that should be excluded from the backup are specified by their usernames (reseller, customer accounts) or domain names (subscriptions). This can be done as follows:

- **Command line specification.** The backup command takes objects identifiers as values of the `--exclude-<reseller|client|domain>` option separated by commas.
- **File specification.** The backup command takes the objects identifiers from the file specified by the `--exclude-<reseller|client|domain>-file` option. The file must be in plain text format, and object identifiers are separated by line breaks (that is, one identifier per line).

Note: It is acceptable to use both specifications in one command. In such a case, all specified objects are excluded from the backup.

➤ **To back up all reseller accounts except for several selected resellers:**

```
pleskbackup resellers-name --exclude-reseller=<login1>,<login2>[,<login n>]
```

or

```
pleskbackup resellers-name --exclude-reseller-file=<file>
```

For example,

```
pleskbackup --resellers-name --exclude-reseller=johndoe,janedoe
```

or

```
pleskbackup --resellers-name --exclude-reseller-file="etc/backup
lists/backup"
```

➤ **To back up a selected reseller without several subscriptions belonging to them or their customers:**

```
pleskbackup --resellers-name <username> --exclude-
domain=<name1>,<name2>,<name n>
```

or

```
pleskbackup --resellers-name <username> --exclude-domain-file=<file>
```

For example,

```
pleskbackup resellers-name johndoe --exclude-domain=example.com,example.net,example.org
```

or

```
pleskbackup resellers-name johndoe --exclude-domain-file="etc/backup lists/backup"
```

Restricting backup to only mail content, only hosting content, or only their configuration

The amount of backup data can be further narrowed to backing up either mail or physical hosting content and configuration by using the `--only-mail` or `--only-hosting` options, respectively.

Specifying the `--only-hosting` option results in backing up only website-specific data which includes the following, for each domain with physical hosting:

- website content (including protected directories, web users, MIME types)
- web hosting configuration (including settings of anonymous FTP, log rotation, hotlink protection, shared SSL, web users)
- installed site applications
- databases
- subdomains

Specifying the `--only-mail` option results in backing up only mail-specific data that includes the following:

- if used for the partial backup, for each domain included in the backup:
 - configuration of per-subscription mail settings
 - mail accounts
 - mailing lists
- if used for the full backup, *in addition to previous*:
 - RBL protection settings
 - ACL white and black list configurations

The amount of backup data can also be narrowed in another way: by specifying that only configurations of the selected objects should be backed up. This specification is made by using the `--only-configuration` option.

Such backups are useful when the objects content is backed up by a third-party system.

➤ **To back up mail configuration on subscriptions belonging to a customer:**

```
pleskbackup clients-<name|id> <name|id> --only-mail --configuration
```

For example,

```
pleskbackup clients-id 42 --only-mail --configuration
```

- **To back up websites content and hosting configuration on subscriptions belonging to all resellers:**

```
pleskbackup resellers-id --only-hosting
```

Excluding log files from back up

If Panel's log files related to the hosted objects are not required to be backed up, they can be excluded from the backup by using the `--skip-logs` option.

- **To back up the Panel configuration without log files:**

```
pleskbackup server -c --skip-logs
```

Defining Properties of Files That Compose the Backup

Defining the properties of the files that will be contained in the backup includes the following:

1. Specifying that archives with backup object contents should not be compressed.
2. Specifying that a prefix should be added to the names of the backup files.
3. Specifying that backup files should be split into parts of the specified size.

Specifying that archives with backup object contents should not be compressed

By default, Panel saves backed up content to compressed `.zip` archives to save disk space when the backup is stored. However, restoring backups that contain compressed archives requires almost twice as much disk space as restoring those with uncompressed files. If you want to create your backups without compression, use the `-z` option in your backup command.

Specifying that a prefix should be added to the names of the backup files

In order to better distinguish files that were created during one backup session from another, `pleskbackup` adds a prefix to the backup file name. By default, it is `backup`, so every backup file name looks like `backup_<file-name>.<ext>`. The prefix in names of the files that compose a particular backup can be customized by using the `--prefix` option. The option's value will be added as a prefix to the names of files of the created backup.

For example, to create a backup of the server mail configuration so that all files in the backup have the prefix `mail-friday`:

```
pleskbackup server --only-mail --configuration --prefix="friday"
```

Specifying that backup files should be split into parts of the specified size

The `pleskbackup` utility is capable of splitting backup files into parts of a particular size, which is extremely useful in cases when the file size is critical. Such cases could include the following:

- if backups are burnt to DVDs, file size should not exceed approximately 4 Gbytes
- if backups are stored on the FAT32 file system, file size should not exceed approximately 4 Gbytes
- if backups are stored on FTP, the FTP server may have its own restrictions on the size of a single file transferred to the server

To make `pleskbackup` split the backup files to parts of a particular size, use the `-s|--split` option and specify the required size as the option value. For details on how to specify the size, refer to the section **Backup Utility Commands and Options** (on page 92). The default value used by `pleskbackup` if no custom size is specified is 2 Gbytes. The utility numbers file parts created as a result of a split by adding numerical suffixes to the file names starting from `.1`.

For example, to back up a subscription and split backup files into parts of no more than 700 Mbytes:

```
pleskbackup domains-name example.com --only-hosting --split=700M
```

Exporting Backup Files

By default, `pleskbackup` stores backups in Panel's backup repository located on the server in `/var/lib/psa/dumps/`.

Panel is capable of exporting the created backup as a single `.zip` file in one of the following ways:

- to `stdout`
- to a local file system
- to an FTP server

To export the backup as a single file, use the `--output-file` option. Each particular export mode requires specific option values.

Important: After a backup is exported, `pleskbackup` removes it from the Panel's backup repository.

The exported file can also be created uncompressed and/or split into parts of a particular size, just like the files forming the backup in the repository (details (on page 86)).

Exporting to stdout

To export a backup as a file to `stdout`, use the `--output-file` option with the `stdout` value.

For example, to create a backup of a subscription with ID 1 and export it to `stdout`:

```
pleskbackup domains-id 1 --output-file stdout
```

Exporting to a local file system

To export a backup as a file to a local file system, use the `--output-file` option with a `<full-path-to-file>\<file-name>` value.

For example, to create a backup of a subscription with ID 1 and export it to the file `domain1.tgz` located at `/usr/local/irregular-backups/` folder:

```
pleskbackup domains-id 1 --output-file=/usr/local/irregular-backups/domain1.tgz
```


Exporting to FTP server

To export a backup as a file to an FTP server, use either of the following options:

- `--output-file=ftp://<login>:<password>@<server>/<filepath>`
- `--output-file=ftp://<server>/<filepath> --ftp-login=<ftp login> --ftp-password=<ftp password>`

You may want to use a passive mode FTP connection if a firewall prevents the export. For this, use the `--ftp-passive-mode` option.

For example, to create backup of a subscription with ID 1 and export it to an FTP server **example.com** to the **storage/backups/** directory, using **johndoe** as login and **jjFh6gsm** as password:

```
pleskbackup domains-id 1 --output-  
file=ftp://johndoe:jjFh6gsm@example.com/storage/backups
```

or

```
pleskbackup domains-id 1 --output-file=ftp://example.com/storage/backups --  
ftp-login=johndoe --ftp-password=jjFh6gsm
```

Defining How the Backup Process Is Performed

You can specify the following options for the backup operation:

1. Do not perform the backup if your server does not have specified free disk space.
2. Do not perform the backup if your server does not have enough free disk space to store the backup content.
3. Temporarily suspend websites during backup.
4. Configure the backup utility to include more details in backup reports.

Specifying disk space requirements for the backup

You can prevent the start of the backup operation if your server has not enough disk space to complete it. To set the free disk space requirements, change the parameters in the file `$PRODUCT_ROOT_D/admin/share/pmmcli/pmmcli-rc`.

There are two ways to prevent the start of the backup operation:

- Specify minimal free disk space on your server.
If the server does not have the specified disk space, Panel will not start the backup operation. Set the minimal free disk space in MB by changing the value of the `FREE_DISK_SPACE` parameter. For example, to prevent the backup if free disk space on the server is less than 100 MB, edit the line in the following way:

```
FREE_DISK_SPACE 100
```

- Restrict the backup if your server does not have enough free disk space to store the backup content. If this option is turned on, Panel calculates the future backup size and compares it with the free disk space on the server. If there is not enough disk space, Panel will not start the backup operation. Note that this option can significantly increase the backup time.
To turn this option on, set the `CHECK_BACKUP_DISK_SPACE` to 1. To turn this option off, set the parameter to 0:

```
CHECK_BACKUP_DISK_SPACE 0
```

Suspending websites

If your backup will include websites, we recommend that you suspend them during the backup process by using the `--suspend` option of the backup utility. This will help you avoid possible errors that may be caused by changes made to the site configuration or content during the backup.

The suspension is made as short as possible: each site is suspended only for the time it is being backed up: The site is started automatically as soon as its data are processed.

Defining level of backup verbosity

There are three levels of backup verbosity:

- *Low*: backup utility writes into a log and displays only general errors, such as syntax errors (no or wrong command specified, invalid input parameters), runtime errors, unhandled exceptions, low disk space for backup and so on.
- *Medium*: backup utility writes into a log and displays general errors and information on backup stages.
- *High*: backup utility writes into a log and displays general errors, information on backup stages, debug information and messages sent to and received from the backup utility.

The verbose mode of the backup process is defined by the `-v` option:

Option	Verbosity	Example
no, <code>-v</code> , <code>-vv</code>	Low	To create a complete server backup with a low level of verbosity on Linux/Unix: # <code>opt/psa/bin/pleskbackup server -vv</code>
<code>-vvv</code>	Medium	To create a complete server backup with a medium level of verbosity on Linux/Unix: # <code>opt/psa/bin/pleskbackup server -vv</code>
<code>-vvvvv</code> , <code>-vvvvvv</code>	High	To create a complete server backup with a high level of verbosity on Linux/Unix: # <code>opt/psa/bin/pleskbackup server -vv</code>

➤ **To run a task on creating a complete server backup with a maximum level of verbosity:**

```
pleskbackup server -vvvvv
```

Backup Utility Commands and Options

Location

`$PRODUCT_ROOT_D/bin/pleskbackup` where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

Usage

```
pleskbackup <command> [<arguments>] [<options>]
```

Commands

Command	Argument	Description
server		Backs up whole Plesk server.
resellers-name	[<login-1> <login-2> <...> <login-n>]	<p>Backs up all data for the resellers specified by logins. Logins should be separated by spaces, and, if on Windows, enclosed in quotes.</p> <p>Can be used with the <code>--from-file</code> option. In such case, resellers specified in the file are backed up and resellers specified as command arguments are ignored.</p> <p>If no logins are specified and the <code>-f</code> option is not used, all resellers are backed up.</p>
resellers-id	[<ID1> <ID2> <...> <IDn>]	<p>Backs up all data for the resellers specified by IDs. IDs should be separated by spaces, and, if on Windows, enclosed in quotes.</p> <p>Can be used with the <code>--from-file</code> option. In such case, resellers specified in the file are backed up and resellers specified as command arguments are ignored.</p> <p>If no IDs are specified and the <code>-f</code> option is not used, all resellers are backed up.</p>
clients-name	[<login-1> <login-2> <...> <login-n>]	<p>Backs up all data for the customers specified by logins. Logins should be separated by spaces, and, if on Windows, enclosed in quotes.</p> <p>Can be used with the <code>--from-file</code> option. In such case, customers specified in the file are backed up and customers specified as command arguments are ignored.</p> <p>If no logins are specified and the <code>-f</code> option is not used, all customers are backed up.</p>

Command	Argument	Description
clients-id	[<ID1> <ID2> <...> <IDn>]	<p>Backs up all data for the customers specified by IDs.</p> <p>IDs should be separated by spaces, and, if on Windows, enclosed in quotes.</p> <p>Can be used with the <code>--from-file</code> option. In such case, customers specified in the file are backed up and customers specified as command arguments are ignored.</p> <p>If no IDs are specified and the <code>-f</code> option is not used, all customers are backed up.</p>
domains-name	[<name-1> <name-2> <...> <name-n>]	<p>Backs up all data for the domains specified by names.</p> <p>Names should be separated by spaces, and, if on Windows, enclosed in quotes.</p> <p>Can be used with the <code>--from-file</code> option. In such case, domains specified in the file are backed up and domains specified as command arguments are ignored.</p> <p>If no names are specified and the <code>-f</code> option is not used, all domains are backed up.</p>
domains-id	[<ID1> <ID2> <...> <IDn>]	<p>Backs up all data for the domains specified by IDs.</p> <p>IDs should be separated by spaces, and, if on Windows, enclosed in quotes.</p> <p>Can be used with the <code>--from-file</code> option. In such case, domains specified in the file are backed up and domains specified as command arguments are ignored.</p> <p>If no IDs are specified and the <code>-f</code> option is not used, all domains are backed up.</p>
--help		Displays help on the utility usage.

Exclude Options

Option	Description
--exclude-reseller[=<login1>,<login2>,...]	Skips resellers with the specified logins during backup.
--exclude-reseller-file[=<file>]	Skips resellers listed in the specified file during backup.
--exclude-client[=<login1>,<login2>,...]	Skips customers with the specified logins during backup.
--exclude-client-file=<file>	Skips customers listed in the specified file during backup.
--exclude-domain[=<name1>,<name2>,...]	Skips domain with the specified names during backup.
--exclude-domain-file=<file>	Skips domains listed in the specified file during backup.

General Options

Option	Description
<code>-v --verbose</code>	Shows more information about the backup process. Multiple <code>-v</code> options increase verbosity. For the maximum verbosity level, define 5 options.
<code>-c --configuration</code>	Backs up only configurations of Plesk objects, excluding their content.
<code>-s --split[=<integer>[K M G]]</code>	Splits the backup files into parts of the specified size. The parts are numbered by appending numerical suffixes starting with <code>.1</code> . Size is specified in Kbytes, Mbytes or Gbytes. If none is defined, size is interpreted as being in bytes. If no argument is specified, a default value of 2 Gbytes is used.
<code>-z --no-gzip</code>	Sets that object content is archived without compressing.
<code>--only-mail</code>	Backs up only mail configuration and content. When used with the <code>resellers clients domains-login id</code> commands, backs up configuration of domain-level mail system, and content and configuration of mail accounts. When used with the <code>server</code> command, also backs up server-wide mail configuration. Cannot be used with the <code>--only-hosting</code> option.
<code>--only-hosting</code>	Backs up only physical hosting configuration and Web site content, including site applications, databases and subdomains. Cannot be used with the <code>--only-mail</code> option.
<code>--suspend</code>	Suspends domains during backup operation.
<code>-f --from-file=<file></code>	Backs up resellers customers domains listed in the specified file, ignoring those specified in the command line as arguments. The file should be in plain text format and should contain a list of resellers customers domains, one per line. Used only with the <code>resellers-name</code> , <code>resellers-id</code> , <code>clients-name</code> , <code>clients-id</code> , <code>domains-name</code> , <code>domains-id</code> commands. Depending on the command, resellers customers domains are listed in the file by either logins or IDs.
<code>--skip-logs</code>	Sets that log files are not saved to backup.
<code>--prefix=<string></code>	Adds a specified prefix to the backup file names. Used to customize backup file name which is created with the backup prefix by default.

FTP Options

Option	Description
<code>--ftp-login=<ftp_login></code>	Specifies FTP login that will be used for uploading backup file to the FTP server.
<code>--ftp-password=<ftp_password></code>	Specifies password that will be used for uploading backup file to the FTP server.
<code>--ftp-passive-mode</code>	Specifies that a passive mode FTP connection should be used.

Output File Option

Option	Description
<code>--output-file</code>	Exports backup as a single file to <code>stdout</code> and removes backup from Plesk repository.
<code>--output-file=<fullpath/filename></code>	Exports backup as a single file with the specified name to a local file system and removes backup from Plesk repository.
<code>--output-file=<ftp://[<login>[:<password>]@]<server>/<filepath>></code>	Exports backup as a single file to the specified FTP server and removes backup from Plesk repository. The <code>FTP_PASSWORD</code> environment variable can be used for setting a password. The <code>--ftp-login</code> and <code>--ftp-password</code> FTP options can be used for setting login and password.

Restoring Data

To perform restoration of Panel hosting data, you should execute the `pleskrestore` utility command that does the following:

1. Defines the Panel objects to be restored.
2. Defines how the restore process will be performed.
3. Defines conflict resolution rules and policies.

The following sections explain each component in detail.

The `pleskrestore` utility is located in `$PRODUCT_ROOT_D/bin/pleskbackup` where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

To see a list of the `pleskrestore` commands and options, refer to the section **Restoration Utility Commands and Options** (on page 126).

If a restoration process fails, you can use its logs for troubleshooting. Each restoration process's logs are stored in `$PRODUCT_ROOT_D/PMM/logs/restore-YYYY-MM-DD-hh-mm-nnn`, where `YYYY-MM-DD-hh-mm` is the date and time when the restoration was performed and `nnn` is a randomly generated number.

Next in this section:

Defining Objects for Restoration	97
Defining How the Restore Process is Performed	103
Conflict Resolution Rules and Policies	104
Restoration Utility Commands and Options	126

Defining Objects for Restoration

Defining objects for restoration includes the following:

1. Specifying a source backup file.
2. Defining the level of restored objects.
3. Applying a filter on the specified level.

Generally speaking, the data that can be restored with one call of the `pleskrestore` utility are represented by any cell in the following table.

		Restoration levels specified with the <code>-level</code> option						
		Server	Resellers		Customers		Subscriptions	
				Selected with the <code>-filter</code> option		Selected with the <code>-filter</code> option		Selected with the <code>-filter</code> option
Backup file	<code><server>.xml zip tar</code>	Full restoration	All reseller accounts	Selected reseller accounts	All customer accounts belonging to administrator	Selected customer accounts belonging to administrator	All subscriptions belonging to administrator	Selected subscriptions belonging to administrator
	<code><reseller>.xml zip tar</code>		Full restoration of a reseller account		All customer accounts belonging to reseller	Selected customer accounts belonging to reseller	All subscriptions belonging to reseller	Selected subscriptions belonging to reseller
	<code><customer>.xml zip tar</code>				Full restoration of a customer account		All subscriptions belonging to customer	Selected subscriptions belonging to customer
	<code><subscription>.xml zip tar</code>						Full restoration of a subscription	

Specifying a source backup file

The source backup file defined for restoration can be of one of the following types:

- `<info>.xml` - backup metadata file, when restoring from backup located in Panel's repository.
- `<backup>.<zip|tar>` - archived backup file, when restoring from an exported backup.

For example, to restore the whole server backup, you choose a `<backup repository root>/<server>.xml` file, or an exported server backup file. To restore a client belonging to a reseller, you choose a `<backup repository root>/resellers/<reseller ID>/clients/<client ID>/<client>.xml` file.

Defining level of restored objects

Defining the level of restored objects allows you to narrow the amount of restored data according to your needs. For example, you may want to restore only subscriptions which belong to a customer or a reseller, skipping all other data not related to subscriptions.

To define the level of restored objects, use the `-level` option with an appropriate value. The option is required, so in cases when you do not need any narrowing but just wish to restore all data from a backup, define the level equal to the level of the file.

➤ *To restore entire server:*

```
pleskrestore restore <backup repository root>/<server>.xml -level server
```

Note: When the whole server backup is restored, license keys are not restored by default. To restore license keys along with other server content, use the `-license` option in your restore command.

➤ *To restore entire server with license keys:*

```
pleskrestore --restore <backup repository root>/<server>.xml -level server  
-license
```

➤ *To restore all domains belonging to a reseller:*

```
pleskrestore --restore <backup repository root>/resellers/<reseller  
ID>/<reseller>.xml -level domains
```

➤ *To restore all reseller accounts:*

```
pleskrestore --restore <backup repository root>/<server>.xml -level  
resellers
```

Applying filter to the specified level

To perform a more selective restore, use a filter (the `-filter` option) which selects particular objects of the specified level (resellers, customers, subscriptions) to be restored. The objects are specified by their names, which are domain names for subscriptions, and usernames for resellers and customers. The specification can be done as follows:

- *Command line specification.* The restore command takes object identifiers as values of the `-filter` option defined in the following string:
`list:<item1>,<item2>,...,<itemN>.`
- *File specification.* The restore command takes the objects identifiers from the file specified as an argument of the `-filter` option. The file must be in plain text format, and object identifiers are separated by line breaks (that is, one identifier per line).

➤ *To restore two resellers from a server backup:*

```
pleskrestore --restore <backup repository root>/<server>.xml -level
resellers -filter list:JohnDoe,JaneDoe
```

or

```
pleskrestore --restore <upload directory>/<server backup name>.zip -level
resellers -filter list:JohnDoe,JaneDoe
```

➤ *To restore two subscriptions owned by the server administrator:*

```
pleskrestore --restore <backup repository root>/<server>.xml -level domains
-filter list:example.com,sample.org
```

➤ *To restore several subscriptions of a customer defined in a file:*

```
pleskrestore --restore <backup repository
root>/resellers/SandyLee/clients/JaneDow/<client>.xml -level domains -
filter <path to the file>/restore-domains.txt
```







Next in this section:













Backup File Structure 99

Backup File Structure

By default, all backups are created in a backup repository located on the Panel-managed server: in a repository specified by the `DUMP_D` variable defined in the `/etc/psa/psa.conf` configuration file

The repository is structured as follows, starting with the content of the repository root folder (we omit auxiliary files and folders which are irrelevant for backing up and restoring Panel data using `pleskbackup` and `pleskrestore` utilities).

	<code><info>.xml</code>	Metadata files of full and server-level backups, one per backup, describe configuration and content of <i>server</i> , <i>admin</i> , and all their descendants.
	<code><content>.<zip tar tgz></code>	Archives with content of <i>server</i> and <i>admin</i> .
	<code>clients/</code>	Directory containing the following backup data: <ul style="list-style-type: none"> <i>clients</i> owned by <i>admin</i> or with no owner objects owned by the <i>clients</i> Organization of the directory is the same as that of <code><repository>/resellers/<reseller ID>/clients/</code> .
	<code>domains/</code>	Directory containing the following backup data: <ul style="list-style-type: none"> <i>domains</i> owned by <i>admin</i> or with no owner objects owned by the <i>domains</i> Organization of the directory is the same as that of <code><repository>/resellers/<reseller ID>/clients/<client ID>/domains</code> .
	<code>resellers/</code>	Directory containing the following backup data: <ul style="list-style-type: none"> <i>resellers</i> objects owned by the <i>resellers</i>
	<code><reseller ID>/</code>	Directories containing backup data of particular <i>resellers</i> , one reseller per directory, and the objects owned by them. The <i>reseller ID</i> stands for the reseller login name.

	<code><info>.xml</code>	Metadata files of the <i>reseller</i> backups, one file per backup, describe configuration and content of the <i>reseller</i> and the objects they own.
	<code><content>.<zip tar tgz></code>	Archives with the <i>reseller</i> content.
	<code>domains/</code>	Directory containing the following backup data: <ul style="list-style-type: none"> <i>domains</i> owned by the <i>reseller</i> objects owned by the <i>domains</i> Organization of the directory is the same as that of <code><repository>/resellers/<reseller ID>/clients/<client ID>/domains/</code> .
	<code>clients/</code>	Directory containing the following backup data: <ul style="list-style-type: none"> <i>clients</i> owned by the <i>reseller</i> objects owned by the <i>clients</i>
	<code><client ID>/</code>	Directories containing backup data of particular <i>clients</i> , one client per directory, and the objects owned by them. The <i>client ID</i> stands for the client login name.
	<code><info>.xml</code>	Metadata files of the <i>client</i> backups, one file per backup, describe configuration and content of the <i>client</i> and the objects he owns.
	<code><content>.<zip tar tgz></code>	Archives with the <i>client</i> content.
	<code>domains/</code>	Directory containing the following backup data: <ul style="list-style-type: none"> <i>domains</i> owned by the <i>client</i> objects owned by the <i>domains</i>
	<code><international domain name> <domain ID>/</code>	Directories containing backup data of particular <i>domains</i> , one domain per directory, and the objects owned by them. The domain ID is omitted if the domain IDN is less than 47 symbols.
	<code><info>.xml</code>	Metadata files of the <i>domain</i> backups, one file per backup, describe configuration and content of the <i>domain</i> and the objects it owns.
 	<code><content></code>	Other files and folders which contain domain contents, and its children contents and configurations.

Files of each backup are placed in the repository folders according to the described structure.

If a partial backup is created, its files will be placed according to the location of the backup objects in the hierarchy. For example, if backing up domain `example.com` owned by reseller `JaneDoe`, its files will be located in the `<repository root directory>/resellers/JaneDoe/domains/example.com/` folder. If backing up reseller, `JohnDoe`, who owns a domain `joe.info` and has one client, `DukeNukem`, who owns domain `sample.org`, the backup files will be located in the following folders:

1. `<repository root directory>/resellers/JohnDoe/`
2. `<repository root directory>/resellers/JohnDoe/domains/joe.info/`
3. `<repository root directory>/resellers/JohnDoe/clients/DukeNukem/`
4. `<repository root directory>/resellers/JohnDoe/clients/DukeNukem/domains/sample.org/`

To distinguish files belonging to different backups of the same object, a specific prefix and suffix are added to the file names:

- the `backup` is added by default, and, if you like, you can change it to your own on a per-backup basis
- a suffix designating the backup creation date is always added to each backup file, and the date format is `<yyymmddhhmm>`. For example, the files of a backup created on 6 April 2011, 8:58 PM will have the suffix `1104062058`.

Panel is capable of exporting a backup as a single `.tgz` file. Each archive has the same structure as the repository, the only difference is that there is only one `<info>.xml` file on each level.

If a partial backup is exported, the resulting file structure is reduced from the top so that the highest level corresponds to the level of the highest backup object. For example, if a backup of a single customer (called, for example, `SandyLee`) is exported, the resulting file will have the following structure:

```
zip {  
  ▪ <sandy lee info>.xml  
  ▪ <content>.zip  
  ▪ domains/  
    ▪ subscription1/  
      ▪ ...  
    ▪ subscription_N/  
      ▪ ...  
}
```

Defining How the Restore Process is Performed

When restoring data, you can also do the following:

1. Temporarily suspend websites during restoration.
2. Configure the restoration utility to include more details in backup reports.
3. Configure the restoration utility to restore files even if they do not have a valid signature.

Suspending Websites

If you are going to restore websites, we recommend that you suspend them during the restoration by using the `-suspend` option. This will help you avoid possible errors in the restored sites that may be caused by changes made to the site configuration or content during the restoration.

The suspension is made as short as possible: each site is suspended only for the time it is being restored. The site is started automatically as soon as the data are processed.

Defining Level of Restore Verbosity

`pleskrestore` works in one of the following verbosity modes:

1. *Non-verbose mode*. Default mode. The minimum level, only general errors are displayed, such as, syntax errors (no or wrong command specified, invalid input parameters), runtime errors and unhandled exceptions, and so on.
2. *Verbose mode*. Restore runs with verbosity level which additionally includes deployer errors, information about conflicts (read about restore conflicts in the section **Conflict Resolution Rules and Policies** (on page 104)), and so on. Enabled by adding the `-verbose` option to the `pleskrestore` command.

Restoring Backups Without Valid Signatures

When you attempt to restore a backup file by means of the `pleskrestore` utility, Panel checks the file and does not restore it if any of the following problems are found:

- The file is corrupted.
- The file was modified manually after downloading from the server.
- The file was created on another server.
- The file was created in a Panel version earlier than 11.5.

Note: Actually, files created in earlier Panel versions are not a problem. Panel marks such backups as problematic because they lack backup signatures. A backup signature, introduced in Panel 11.5, enables Panel to check backups.

To skip checking and restore a backup regardless of potential problems, use the `-ignore-sign` option.

Panel administrators can also restore backups with problems is through the Panel GUI by selecting the corresponding option on the **Tools & Settings > Backup Manager > <backup_name>** page. Customers and resellers are not allowed to restore such backups by default. However, you can allow all users to restore any backups regardless of potential problems. To do this, add the following lines to the `/usr/local/psa/admin/conf/panel.ini` configuration file:

```
[pmm]
allowRestoreModifiedDumps = on
```

To return to the default restrictions, remove these lines or change the second line to the following:

```
allowRestoreModifiedDumps = off
```

Conflict Resolution Rules and Policies

Conflict is a situation when settings in a backup and settings in a destination Panel are such that restoring a backup object leads to an error or unpredictable Panel behavior.

Types of Conflicts

The restoration process can encounter several types of conflicts, as follows:

- **Timing conflicts.** An object being restored might exist in the system and its last modification date might be more recent than the date of backup. Or an object could be deleted from the system later than the backup was created.
- **Resource usage conflicts.** There are two groups of resource usage conflicts:
 - **Common resource usage conflict:** The total amount of measurable resources after restoration might appear to be over the limit for this particular user (e.g., disk space limit).
 - **Unique resource usage conflict:** An object being restored requires a unique resource which is already being used by another object in the system or does not exist (e.g., domain).
- **Configuration conflicts.** It might happen that the configuration being restored is not enabled on the destination server. Two situations can arise here:
 - Configuration options are not enabled for the domain.
 - Required configuration options are not available (e.g., site applications are not available for the customer, database server is not configured on the host, IP address is not allocated to the reseller, etc.)

Conflict Resolutions

The following conflict resolutions options are possible:

- **Overwrite.** Means that all objects will be restored from the backup files regardless of their current presence in the system. Overwrite works as follows:
 - If an object/setting from backup does not exist in Panel, it is created.
 - If an object/setting from backup exists in Panel, it replaces the existing object/setting.
 - If an object/setting exists in Panel but is missed in a backup, the existing object/setting remains.
- **Proceed with current.** Means that objects that are currently present in the system will not be affected by the restoration process. The restoration process will move to the objects belonging to that one, not touching the object itself.
- **Do not restore.** Means that the objects that are currently present in the system or were deleted after the backup will not be restored with the lower level objects.
- **Automatic.** Means that configuration option that should be enabled for domain is enabled automatically.
- **Overuse.** Means that objects are restored even when the resources are overused. Can be applied only to objects that belong to a reseller who is working in the oversell mode.
- **Rename.** Means that unique resources for the restored domain are reassigned with the specified name, existing in the system (mapping).

Conflict Resolution Policies and Rules

Depending on the scope of a conflict resolution, we distinguish between conflict resolution *rules* and *policies*:

- Rule defines the way a specific single conflict should be resolved.
- Policy defines the way all conflicts of a particular type should be resolved.

Conflicts Resolving Mechanism: Default Policies, Custom Policies, and Rules

The restoration utility brings a set of default, hard-coded conflict resolution policies, which are as follows:

- for timing conflicts - Overwrite
- for common resource usage conflicts - Overuse
- for unique resource usage conflicts - Do not restore
- for configuration conflicts - Automatic

The default policies are always applied during restoration and cannot be changed or overridden.

Applying default policies may not resolve all the conflicts that occur. In such cases, the person performing the restore should define additionally custom rules and/or policies that resolve the remaining conflicts. Custom rules and policies are defined in an XML format as described in the section **Resolutions Description Format** (on page 108).

A simplified presentation of conflict resolving during restore is as follows:

1. Administrator runs `pleskrestore` with specific parameters.
2. `pleskrestore` detects the conflicts that have occurred and resolves them using the default policies.
3. `pleskrestore` checks if any conflicts remain unresolved.
If all conflicts are resolved, the restoration continues.
4. `pleskrestore` stops the restoration and, if run in debug or verbose mode, returns a detailed description (in XML format) of each remaining conflict.
5. Based on the returned description of the conflicts, the administrator creates a file that defines a resolution for each conflict (with rules) and/or in bulk (with custom policies).
6. The administrator runs the `pleskrestore` utility with the `--conflicts-resolution` option and the file created in the previous step as its argument.
7. `pleskrestore` detects the conflicts that have occurred and resolves them using the default policies.
8. `pleskrestore` processes the remaining conflicts:
 - a `pleskrestore` applies resolution rules from the file.
 - b `pleskrestore` applies resolution policies from the file to the remaining conflicts.
9. `pleskrestore` checks whether any conflicts remain unresolved.
 - If all conflicts are resolved, the restoration continues.
 - If any conflicts remain unresolved, `pleskrestore` stops the restoration and, if run in debug or verbose mode, returns a detailed description (in XML format) of each remaining conflict.

To have such a dump restored, admin should add resolution rules for each remaining conflict to the conflict resolution file and repeat the restoration task.

Next in this section:

Custom Conflict Resolutions 107

Custom Conflict Resolutions

This section describes how to implement custom conflict resolutions during restore.

Next in this section:

Conflict Description Messages	107
Resolutions Description Format.....	108
Samples of Policy Description	117
Samples of Conflict Resolution With Rules.....	117

Conflict Description Messages

Conflict descriptions returned by the `pleskrestore` utility contain `message` elements included for GUI generation purposes. Despite the self-explanatory character of XML conflict descriptions, the values of the `message` elements may be confusing, so this section describes the meanings of these messages as they are displayed in Panel GUI.

Value of message element	Message displayed in Panel GUI
<code>backup__restore__object_vhost</code>	Virtual host
<code>backup__restore__object_plesk_admin</code>	server administrator
<code>backup__restore__conflict_object_name</code>	<object name>
<code>backup__restore__conflict_object_complex_name</code>	<object name> of <group name>
<code>backup__restore__conflict_object_mailname</code>	<mail name>@<domain name>
<code>backup__restore__object_ftpuser</code>	FTP account
<code>backup__restore__object_frontpageuser</code>	Frontpage account
<code>backup__restore__object_webuser</code>	web user
<code>backup__restore__object_domain</code>	subscription name or domain name
<code>backup__restore__object_subdomain</code>	subdomain
<code>backup__restore__object_domainaliases</code>	domain alias
<code>backup__restore__object_client</code>	customer
<code>backup__restore__object_reseller</code>	reseller
<code>backup__restore__object_autoresponder</code>	auto-reply
<code>backup__restore__object_mailalias</code>	mail alias
<code>backup__restore__object_database</code>	database
<code>backup__restore__object_mailname</code>	mail account

Value of message element	Message displayed in Panel GUI
backup__restore__conflict_timing_reason_owner_absent	Cannot restore object: object owner is not specified
backup__restore__conflict_timing_reason_wrong_owner	Cannot restore object: object owner does not exist in Panel
backup__restore__conflict_timing_reason_object_already_exists	Cannot restore <object name>: <object name> <object type> already exists in Panel
backup__restore__conflict_configuration_reason_ip	Cannot restore object: required IP address <IP> not found in owner's IP pool
backup__restore__conflict_configuration_reason_db	Cannot restore database: required database server <host> is not registered in Panel
backup__restore__conflict_configuration_reason_site_app	Cannot restore web application: required web application <application name> not found in owner's web application pool
backup__restore__conflict_unique_reason_name_already_used	Cannot restore <object>: name <unique resource name> is already used in Panel by another <object>
backup__restore__conflict_resource_usage_reason	Cannot restore object: resource limit <limit name> will be exceeded (required: <value>, available: <value>)

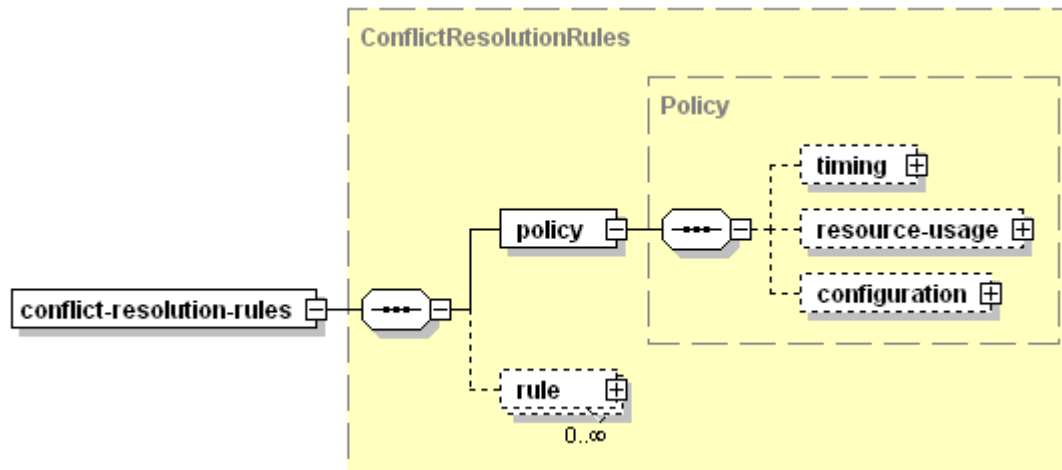
Resolutions Description Format

Next in this section:

Policies.....	109
Rules.....	112

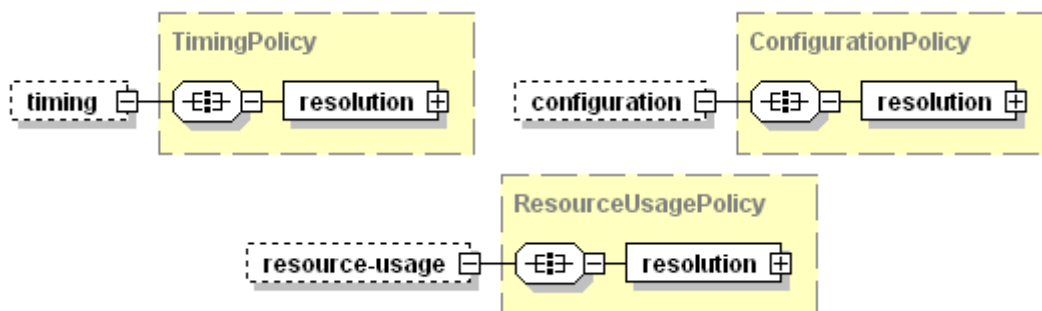
Policies

The file should be structured as follows.

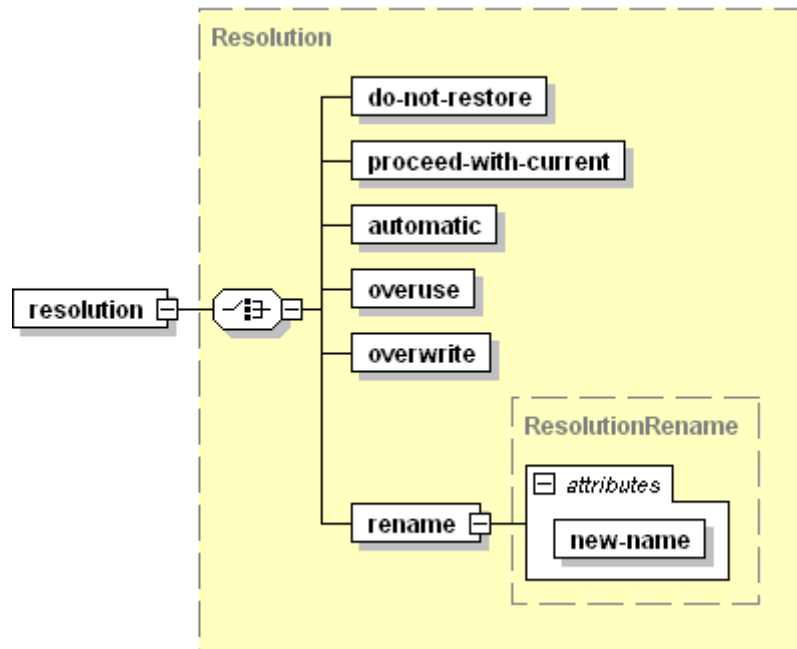


- `conflict-resolution-rules`
Required. Document root element.
- `policy`
- Required. Contains the policy descriptions. Child elements, if present, *must* be placed in the order shown on the scheme.
 - `timing`
Optional. Contains a description of the policy on resolving timing conflicts. See the structure below.
Must be present in the document if a timing policy should be used during the restore.
May not be present in the document if no policy is required for timing conflicts.
 - `resource-usage`
Optional. Contains a description of the policy on resolving resource usage conflicts. See the structure below.
Must be present in the document if a resource usage policy should be used during the restore.
May not be present in the document if no policy is required for resource usage conflicts.
 - `configuration`
Optional. Contains a description of the policy on resolving configuration conflicts. See the structure below.
Must be present in the document if a configuration policy should be used during the restore.
May not be present in the document if no policy is required for configuration conflicts.
- `rule`
Optional. Contains the rule descriptions. For details on the node structure, refer to the **Resolutions Description Format: Rules** section (on page 112).

The policy elements have the same structure:



- `resolution`
Required. Contains a definition of conflict resolution. Structured as follows:

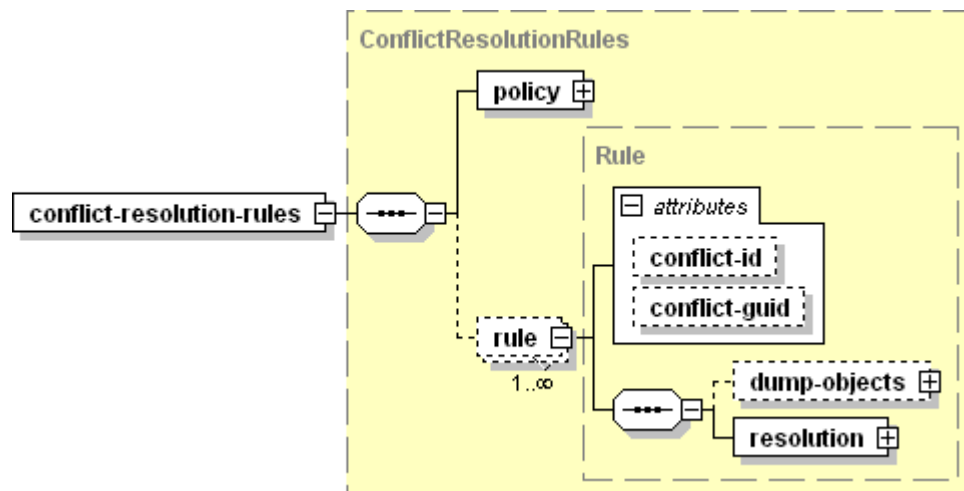


The `resolution` element *must not* be empty, it is *required* that it contains one, and only one of its child elements:

- `do-not-restore`
Sets the Do Not Restore resolution, *empty value*.
- `proceed-with-current`
Sets the Proceed With Current resolution, *empty value*.
- `automatic`
Sets the Automatic resolution, *empty value*.
- `overuse`
Sets the Overuse resolution, *empty value*.
- `overwrite`
Sets the Overwrite resolution, *empty value*.
- `rename`
Sets the Rename resolution, *empty value*.
 - `new-name`
Required. Makes sense only if defined for configuration conflicts. Specifies the name of a new configuration that should be assigned to all conflict objects. The value must be a string.

Rules

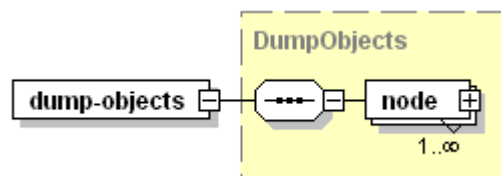
The file should be structured as follows.



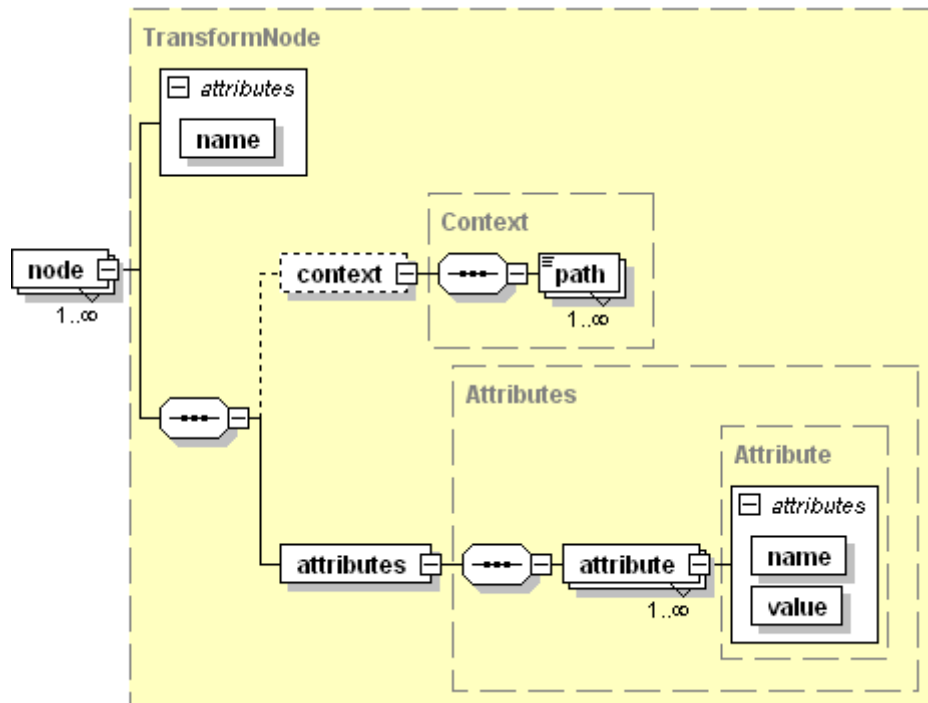
- `conflict-resolution-rules`
Required. Document root element.
 - `policy`
Required. Contains the policy descriptions. For details on the node format, refer to the section **Resolutions Description Format: Policies**.
The element content *must* reflect the conditions under which the conflicts were detected.
 - `rule`
Optional. Contains a rule description.
Must be present in the document when defining conflict resolution rules. Should be present as many times as the number of unresolved conflicts.

At least one of the attributes (`conflict-id`, `conflict-guid`) **MUST** be present.
 - `conflict-id`
Optional. Defines the ID of the conflict being resolved. Value is an integer.
The ID should be obtained from the conflict description returned by `pleskrestore` (the `"/conflicts-description/conflict[@id]"` attribute value)
 - `conflict-guid`
Optional. Defines the global ID of the conflict being resolved. Value is a string.
The GUID should be obtained from the conflict description returned by `pleskrestore` (the `"/conflicts-description/conflict[@guid]"` attribute value).
If omitted, the conflict for resolution is identified by ID.
 - `dump-objects`
Optional. Holds a collection of descriptions of backup objects involved in the conflict and having the same conflict resolution
Must be present in the document in case when different objects involved in the same conflict should be resolved in different ways.
May not be present in the document in cases when all objects involved in the conflict should be resolved the same way.
See the structure below.
 - `resolution`
Required. Contains a definition of the resolution of the conflict. See the structure below.

`dump-objects` structure:

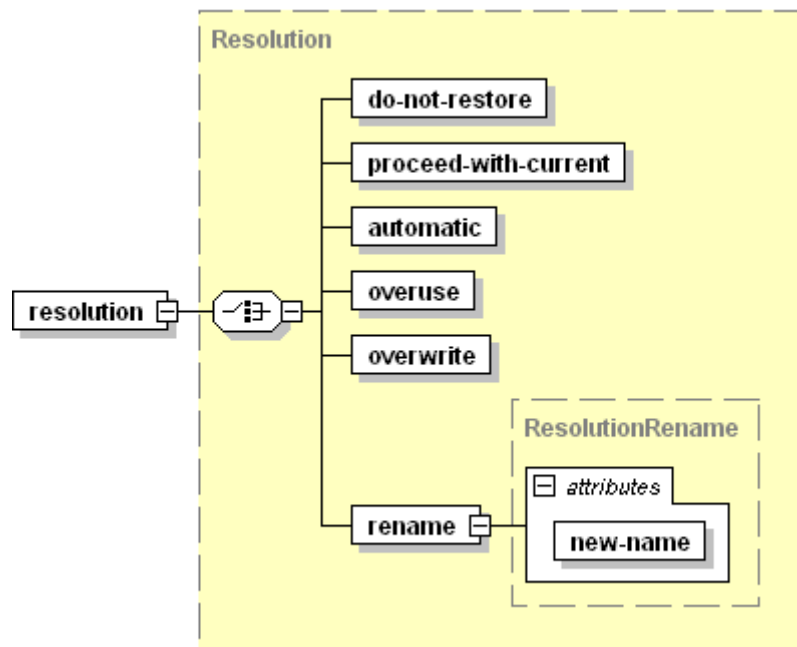


- node**
 Required. Contains a description of the backup object involved in the conflict. The element contents *must* be taken from the conflict description returned by `pleskrestore` (the `/conflicts-description/conflict/conflicting-objects/node` element).
 Structured as follows:



- `name`
Required. Specifies the object type. Value must be a string.
- `context`
Optional. Holds a collection of data specifying the object position in the backup.
 - `path`
Required if the `context` element is present in the document. Specifies the location of the object definition in the backup metadata. Value must be a string conforming to the XPath notation.
- `attributes`
Required, holds a collection of the object properties.
 - `attribute`
Required. Specifies a particular property of the object (e.g., login, ID, GUID, etc.), *empty value*.
 - `name`
Required. Specifies the property name. Value must be a string.
 - `value`
Required. Specifies the property value. Value must be a string.

resolution structure:



The `resolution` element *must not* be empty. It is *required* that it contains one, and only one of its child elements:

- `do-not-restore`
Sets the Do Not Restore resolution for the conflict, *empty value*.
- `proceed-with-current`
Sets the Proceed With Current resolution for the conflict, *empty value*.
- `automatic`
Sets the Automatic resolution for the conflict, *empty value*.
- `overuse`
Sets the Overuse resolution for the conflict, *empty value*.
- `overwrite`
Sets the Overwrite resolution for the conflict, *empty value*.
- `rename`
Sets the Rename resolution for the conflict, *empty value*.
 - `new-name`
Required. Specifies the name of a unique resource that should be assigned to the conflicting objects. Value must be a string.
Makes sense only for unique resource usage conflicts (mapping of IP, database server, object owner).

Samples of Policy Description

The default conflict resolution policies are described in the following XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<conflict-resolution-rules>
  <policy>
    <timing>
      <resolution>
        <proceed-with-current />
      </resolution>
    </timing>
    <resource-usage>
      <resolution>
        <do-not-restore />
      </resolution>
    </resource-usage>
    <configuration>
      <resolution>
        <automatic />
      </resolution>
    </configuration>
  </policy>
</conflict-resolution-rules>
```

The following conflict resolution file resolves all configuration conflicts with database mapping. This can be done if all configuration conflicts beyond default policies appear because a database server defined in the backup is missed in the target Panel installation.

```
<?xml version="1.0" encoding="UTF-8"?>
<conflict-resolution-rules>
  <policy>
    <configuration>
      <resolution>
        <rename new-name="host:192.0.2.12:port:3306"/>
      </resolution>
    </configuration>
  </policy>
</conflict-resolution-rules>
```

Samples of Conflict Resolution With Rules

This section contains examples of conflicts that may appear and their possible resolutions.

Next in this section:

Sample 1: Configuration Conflict with Missing IP Address.....	118
Sample 2: Configuration Conflict With Missing Database Server.....	121

Sample 1: Configuration Conflict with Missing IP Address

This sample represents descriptions of a conflict which was unresolved upon using default policies, and its resolution.

The conflict appears because of the following mismatch in backup data and the destination Panel configuration:

Backup	Destination Panel
Subscription example.com owned by the reseller with ID 30 has web hosting configured on shared IP address 192.0.2.200.	Reseller with ID 30 does not have shared IP address 192.0.2.200 in his or her IP pool.

The conflict is resolved with IP mapping suggesting that the restored subscription will be hosted on shared IP 192.0.2.34 which is in the owner's IP pool.

Note that the conflict resolution XML contains no conflict resolution policies.

Next in this section:

Conflicts Description.....	119
Conflicts Resolution.....	120

Conflicts Description

```

<conflicts-description>
  <conflict id="0">
    <type>
      <configuration>
        <reason-description>
          <required-resource-description>
            <ip type="shared" value="192.0.2.200"></ip>
          </required-resource-description>
          <plesk-object-identifier>
            <!-- beginning of definition of Panel object that conflicts with
an object in the backup -->
            <!-- In resource usage conflicts, the plesk-object-identifier
element specifies Panel object which is an owner of the conflicting
resource. In this example, the conflicting resource is IP, and its owner is
a described reseller with ID 30. -->
            <type>reseller</type>
            <database-id>30</database-id>
            <guid>93dbelb1-cff5-430f-8466-5b810099772f</guid>
          </plesk-object-identifier>
          <!-- end of definition of Panel object that conflicts with an
object in the backup -->
        </reason-description>
        <resolve-options>
          <option name="do-not-restore"></option>
          <option name="rename"></option>
          <option name="automatic"></option>
        </resolve-options>
        <!-- resolve-options element lists all resolutions that are
possible for this particular conflict. When composing the conflict
resolution rule, you should choose one of these resolutions. -->

      </configuration>
    </type>
    <conflicting-objects>
      <!-- beginning of definition of backup objects that conflict with
destination Panel objects. Here, it is a domain example.com -->
      <node children-processing-type="" name="domain">
        <attributes>
          <attribute name="id" value="25"></attribute>
          <attribute name="guid" value="0822c175-a10d-459e-bd3a-
e5cbc497e1f0"></attribute>
          <attribute name="owner-guid" value="93dbelb1-cff5-430f-8466-
5b810099772f"></attribute>
          <attribute name="name" value="example.com"></attribute>
        </attributes>
      </node>
    </conflicting-objects>
    <!-- end of definition of backup objects that conflict with destination
Panel objects -->

    <overview>
      <!-- beginning of more detailed conflict overview. Here, the conflict
appears because the required IP 192.0.2.200 is not in the owner's IP pool -
->
      <object>
        <message>backup__restore__conflict_object_name</message>
        <name>example.com</name>
        <type>domain</type>

```

```
        <reasons>
          <reason>

<message>backup__restore__conflict_configuration_reason_ip</message>
          <param name="ip-address" value="192.0.2.200"></param>
          <param name="ip-type" value="shared"></param>
          <param name="type" value="reseller"></param>
        </reason>
      </reasons>
    </object>
  </overview>
  <!-- end of detailed conflict overview -->

</conflict>
</conflicts-description>
```

Conflicts Resolution

```
<?xml version="1.0" encoding="UTF-8"?>
<resolve-conflicts-task-description>
  <conflict-resolution-rules>
    <policy />
    <rule conflict-id="0">
      <dump-objects>
        <node name="domain">
          <attributes>
            <attribute name="id" value="25"></attribute>
            <attribute name="guid" value="0822c175-a10d-459e-bd3a-
e5cbc497e1f0"></attribute>
            <attribute name="owner-guid" value="93dbelb1-cff5-430f-8466-
5b810099772f"></attribute>
            <attribute name="name" value="example.com"></attribute>
          </attributes>
        </node>
      </dump-objects>
      <resolution>
        <!-- beginning of the conflict resolution definition: IP mapping:
upon restore, the conflicting domain example.com should have hosting
configured on IP 192.0.2.34 -->
        <rename new-name="ip-type:shared:ip-address:192.0.2.34"/>
      </resolution>
      <!-- end of the conflict resolution definition -->
    </rule>
  </conflict-resolution-rules>
</resolve-conflicts-task-description>
```


Sample 2: Configuration Conflict With Missing Database Server

This sample shows a description and resolution of configuration conflicts which was unresolved due to the absence of the required database server on the destination server.

The conflicts appear because of the following mismatches in backup data and destination Panel configuration.

Backup	Destination Panel
Domain sample.net has database mysql_db2_7469 on the MySQL database server with host name 192.0.2.15 listening on port 3306.	No MySQL servers configured on host 192.0.2.15.
Domain 69.sample.net has database mysql_db1_6319 on the MySQL database server with host name 192.0.2.15 listening on port 3306.	

These conflicts are resolved with database mapping (Rename resolution) suggesting that the first databases will be restored onto the MySQL server with host name 192.0.2.12, and the second onto the local MySQL database server.

Next in this section:

Conflicts Description..... 122

Conflicts Resolution..... 125

Conflicts Description

```

<conflicts-description>
  <conflict id="0">
    <type>
      <configuration>
        <reason-description>
          <required-resource-description>
            <db-server host="192.0.2.15" type="mysql" port="3306"></db-
server>
          </required-resource-description>
          <plesk-object-identifier>
            <!-- beginning of definition of Panel object that conflicts with
an object in the backup. In resource usage conflicts it is owner of the
conflicting resource. Here, it is Panel administrator who is the owner of
all database servers -->
              <type>admin</type>
              <database-id>1</database-id>
              <guid>00000000-0000-0000-0000-000000000000</guid>
            </plesk-object-identifier>
            <!-- end of definition of Panel object that conflicts with an
object in the backup -->
          </reason-description>
          <resolve-options>
            <option name="do-not-restore"></option>
            <option name="rename"></option>
            <option name="automatic"></option>
          </resolve-options>
        </configuration>
      </type>
      <conflicting-objects>
        <!-- beginning of definition of backup objects that conflict with
destination Panel objects. Here, it is database mysql_db2_7469 -->
          <node children-processing-type="" name="database">
            <attributes>
              <attribute name="guid" value="86124f4a-5935-48c4-80df-
6d3e9c645378_db_20"></attribute>
              <attribute name="owner-guid" value="86124f4a-5935-48c4-80df-
6d3e9c645378"></attribute>
              <attribute name="name" value="mysql_db2_7469"></attribute>
            </attributes>
          </node>
        </conflicting-objects>
        <!-- end of definition of backup objects that conflict with destination
Panel objects -->
      </conflicting-objects>
    </type>
  </conflict>
</conflicts-description>

```

```

<message>backup__restore__conflict_configuration_reason_db</message>
  <param name="db-type" value="mysql"></param>
  <param name="db-host" value="192.0.2.15"></param>
  <param name="db-port" value="3306"></param>
  <param name="type" value="admin"></param>
  <param name="name"
value="backup__restore__object_plesk_admin"></param>
  </reason>
</reasons>
</object>
</overview>
  <!-- end of detailed overview of the conflict -->
</conflict>
  <!-- ===== begin new conflict description ===== -->
  <conflict id="1">
    <type>
      <configuration>
        <reason-description>
          <required-resource-description>
            <db-server host="192.0.2.15" type="mysql" port="3306">
</db-server>
          </required-resource-description>
          <plesk-object-identifier>
            <!-- beginning of definition of Panel object that conflicts with
an object in the backup. In resource usage conflicts it is the owner of the
conflicting resource. Here, it is Panel administrator who is the owner of
all database servers -->
            <type>admin</type>
            <database-id>1</database-id>
            <guid>00000000-0000-0000-0000-000000000000</guid>
            </plesk-object-identifier>
            <!-- end of definition of Panel object that conflicts with an
object in the backup -->
          </reason-description>
          <resolve-options>
            <option name="do-not-restore"></option>
            <option name="rename"></option>
            <option name="automatic"></option>
          </resolve-options>
        </configuration>
      </type>
      <conflicting-objects>
        <!-- beginning of definition of backup objects that conflict with
destination Panel objects. Here, it is database mysql_db1_6319 -->
        <node children-processing-type="" name="database">
          <attributes>
            <attribute name="guid" value="e1fbb4b2-538b-4542-9220-
56808741a3d3_db_19"></attribute>
            <attribute name="owner-guid" value="e1fbb4b2-538b-4542-9220-
56808741a3d3"></attribute>
            <attribute name="name" value="mysql_db1_6319"></attribute>
          </attributes>
        </node>
      </conflicting-objects>
        <!-- end of definition of backup objects that conflict with destination
Panel objects -->

    </overview>

```

```
<!-- beginning of detailed overview of the conflict. This conflict
appears because database mysql_db1_6319 requires MySQL database server with
host name 192.0.2.15 listening on port 3306, which is not configured on the
destination Panel server. -->
  <object>
    <message>backup__restore__conflict_object_complex_name</message>
    <name>mysql_db1_6319</name>
    <type>database</type>
    <owner-name>69.sample.net</owner-name>
    <reasons>
      <reason>

<message>backup__restore__conflict_configuration_reason_db</message>
      <param name="db-type" value="mysql"></param>
      <param name="db-host" value="192.0.2.15"></param>
      <param name="db-port" value="3306"></param>
      <param name="type" value="admin"></param>
      <param name="name"
value="backup__restore__object_plesk_admin"></param>
      </reason>
    </reasons>
  </object>
</overview>
<!-- end of detailed overview of the conflict -->
</conflict>
</conflicts-description>
```

Conflicts Resolution

```
<?xml version="1.0" encoding="UTF-8"?>
<resolve-conflicts-task-description>
  <conflict-resolution-rules>
    <policy />
    <rule conflict-id="0">
      <!-- beginning of the first conflict resolution rule: restore the
database described in the  node  element on local MySQL server listening on
the port 3306 -->
      <dump-objects>
        <node name="database">
          <attributes>
            <attribute name="name" value="mysql_db2_7469"/>
          </attributes>
        </node>
      </dump-objects>
      <resolution>
        <rename new-name="host:192.0.2.12:port:3306"/>
      </resolution>
    </rule>
    <!-- end of the first conflict resolution rule -->
    <rule conflict-id="1">
      <!-- beginning of the second conflict resolution rule: restore the
database described in the  node  element on local MySQL server listening on
the port 3306 -->
      <dump-objects>
        <node name="database">
          <attributes>
            <attribute name="name" value="mysql_db1_6319"/>
          </attributes>
        </node>
      </dump-objects>
      <resolution>
        <rename new-name="host:localhost:port:3306"/>
      </resolution>
    </rule>
    <!-- end of the second conflict resolution rule -->
  </conflict-resolution-rules>
</resolve-conflicts-task-description>
```

Restoration Utility Commands and Options

Location

`$PRODUCT_ROOT_D/bin/pleskbackup` where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

Usage

```
pleskrestore <command> [<arguments>] [<options>]
```

Commands

Command	Argument	Description
<code>--restore</code>	<code><backup_file></code>	Restores data from the specified backup. Requires the <code>-level</code> option.
<code>--check-backup</code>	<code><backup_file></code>	Checks integrity of the specified backup file, which is: <ul style="list-style-type: none"> ▪ backup digital sign match ▪ backup file format ▪ content files integrity
<code>-i --info</code>	<code><backup_file></code>	Shows the backup file description.
<code>-h --help</code>		Displays help on the utility usage.

Options

Option	Argument	Description
<code>-level</code>	<code>clients resellers domains server</code>	Specifies restore level. Required with the <code>--restore</code> command.
<code>-filter</code>	<code><file> <list:<item1_name>[,<item2_name>[,...]]></code>	Specifies list of subscriptions, customer or reseller names for restoring. The object names are listed either in a specified file, one per line, or as the option argument, separated by commas.
<code>-license</code>		Restores Panel license key from the backup.
<code>-verbose</code>		Enables verbose restore mode.
<code>-debug</code>		Enables debugging restore mode.
<code>-conflicts-resolution</code>	<code><file></code>	Specifies file that describes conflict resolution policies and rules.
<code>-suspend</code>		Suspends the sites being restored.

Option	Argument	Description
-ignore-sign		Allows restoring backups that are created on other servers or in Panel versions earlier than 11.5. Warning: If you use this option, Panel will restore the backup file even if it is corrupted or modified manually.

Migrating and Transferring Data

You can migrate data to Parallels Plesk Panel 11.5 from other servers managed by Panel 11.0 or earlier by using the Panel's Migration & Transfer Manager function. This function is available in **Server Administration Panel > Tools & Settings > Migration & Transfer Manager** if the corresponding component is installed on the server. This component is not included in typical installations.

For detailed information about migrating data to Panel-managed servers, refer to the **Installation, Upgrade, Migration, and Transfer Guide**.

Statistics and Logs

Apache, FTP, mail and other system services write information on their functioning to log files. These files are periodically analyzed by the *statistics* utility that parses logs and inserts the resource usage data into the psa database.

Two other utilities, *Webalizer* and *AWstats*, also parse the services logs and generate HTML files with the statistical data.

Details about where the log files reside and how the utilities process them are given in this chapter.

System Services Logs

System services logs contain traffic usage data and operational details that may be useful for troubleshooting. These data contain, for example, errors and access information.

The logs produced by Apache, FTP and mail services for each domain are stored in `/var/www/vhosts/<domain_name>/statistics/logs/`. sw-cp-server logs are stored in `/var/log/sw-cp-server/` (error log) and `$PRODUCT_ROOT_D/admin/logs/` (access log).

To save disk space, Panel rotates logs: it removes the information written before a specified date or the least relevant information when the log size reaches a limit. For more information on logs rotation, see the section **Log Rotation** (on page 131).

Processing Statistics

Once a day, Panel runs the *statistics* utility. This gets the statistical data from the services log files, calculates daily traffic usage values for each domain and customer, and writes these values to the `DomainsTraffic` and the `ClientsTraffic` tables of the psa database. You can also run the *statistics* utility manually to calculate statistics for all domains or a particular domain. For details, see the section **Calculating Statistics from Logs** (on page 130).

Webalizer and *AWstats* are third-party utilities that represent statistical information from log files in the HTML format. These utilities store the files for each domain in the subdirectories of `/var/www/vhosts/<domain_name>/statistics`. You can view HTML statistics in the Panel GUI or make Panel send them to your e-mail address. For instructions on how to set up automatic sending of resource usage reports, see the section **Resource Usage Reports** (on page 133).

In addition, you can recalculate statistic for previous months using the *AWstats* utility. For instructions on how to do this see the section **Recalculating Statistics for Previous Months** (on page 130).

In this chapter:

Calculating Statistics from Logs.....	130
Recalculating Statistics for Previous Months	130
Log Rotation.....	131
Resource Usage Reports	133

Calculating Statistics from Logs

Parallels Plesk Panel calculates traffic usage statistics from logs every day using the `statistics` utility.

If you need to recalculate traffic usage statistics, you can run the `statistics` utility manually. It is located in the `/usr/local/psa/admin/sbin/` (on RPM-based OSes) or `/opt/psa/bin` (on DEB-based OSes) `statistics` directory.

- **To recalculate statistics for all domains, run the utility without options or with the `--calculate-all` option:**

```
# ./statistics --calculate-all
```

- **To recalculate statistics for a particular domain, run the utility with the `--calculate-one` option:**

```
# ./statistics --calculate-one --domain-name=<domain_name>
```

Recalculating Statistics for Previous Months

By default, Parallels Plesk Panel utilities present only the current month's statistics in HTML format. You can retrieve HTML statistics for previous months using the `AWstats` utility. To do this, restore traffic usage information from logs and run the utility manually. Detailed instructions are provided below.

- **To recalculate statistics for previous months:**

1. Define the required environment variables by running the commands:

```
export vhost_name=<domain_name>
export AWSTATS_BIN_D=`grep ^AWSTATS_BIN_D /etc/psa/psa.conf | awk
'{print $2}'`
export HTTPD_VHOSTS_D=`grep ^HTTPD_VHOSTS_D /etc/psa/psa.conf | awk
'{print $2}'`
export PRODUCT_ROOT_D=`grep ^PRODUCT_ROOT_D /etc/psa/psa.conf | awk
'{print $2}'`
export awstats=${AWSTATS_BIN_D}/awstats.pl
export awstats_gen_opts="-staticlinks -
configdir=${PRODUCT_ROOT_D}/etc/awstats -config=${vhost_name}-http"
```

2. Remove `*.txt` files from the `$HTTPD_VHOSTS_D/<domain_name>/statistics/webstat` directory by running the command:

```
find $HTTPD_VHOSTS_D/$vhost_name/statistics/webstat -name '*.txt' -
exec mv '{}' '{}'.orig \;
```

3. Analyze the domain log files with `awstats` by running the command:

```
$awstats $awstats_gen_opts -
LogFile=$HTTPD_VHOSTS_D/${vhost_name}/statistics/logs/access_log.proce
ssed
```

This command creates subdirectories with the names "YYYY-MM" in the `$HTTPD_VHOSTS_D/<domain_name>/statistics/webstat` directory. "YYYY" and "MM" show the year and the month in which the corresponding statistics were collected.

If you want to rebuild statistics pages for a long period, you should start recalculation from the earliest log files. For example, if you have set the number of log files to 10 analyze files in the following order: `access_log.processed.10`, `access_log.processed.9`, ... `access_log.processed.1`, `access_log.processed`.

4. If any of directories with names in 'YYYY-MM' format for the recalculation period are missing, create them by running the command:

```
for y in <year_first> <year_last> ; do for m in `seq 1 12` ; do mkdir
${HTTPD_VHOSTS_D}/${vhost_name}/statistics/webstat/${y}-${printf "%.2d"
$m) ; done ; done
```

`<year_first>` and `<year_last>` are the first and the last years of the period for which you want to recalculate statistics.

5. Run the following cycle to build statistics pages:

```
for y in <year_first> <year_last> ; do \
  for m in `seq 1 12` ; do \
    dest_dir=$HTTPD_VHOSTS_D/${vhost_name}/statistics/webstat/${y}-
$(printf "%.2d" $m) ; \
    $awstats $awstats_gen_opts -month=$m -year=$y -output >
$dest_dir/awstats.${vhost_name}-http.html ; \
    ln -s $dest_dir/awstats.${vhost_name}-http.html
$dest_dir/index.html ; \
    for output in alldomains allhosts lasthosts unknownip allrobots
lastrobots session urldetail urlentry urlexit osdetail unknownos
refererse refererpages keyphrases keywords errors404 ; do \
      $awstats $awstats_gen_opts -month=$m -year=$y -output=$output
> $dest_dir/awstats.${vhost_name}-http.$output.html ; \
    done ; \
  done ; \
done
```

6. Run `statistics` to update the upper frame navigation menu with a month listing:

```
$PRODUCT_ROOT_D/admin/sbin/statistics --calculate-one --domain-
name=${vhost_name}
```

Log Rotation

Parallels Plesk Panel rotates logs using the `logrotate` utility. This is located in the `$PRODUCT_ROOT_D/logrotate/sbin/logrotate` directory, where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

You can set the following parameters of logs rotation:

- Log rotation condition. This may be one of the following:
 - Size - Panel rotates logs when their size exceeds a particular limit.
 - Time - daily, weekly, or monthly logs rotation.
- Maximum number of log files.
- Log compression. Enable this, if you want Panel to compress log files to gzip archives.
- E-mail to which Panel should send processed log files.

Log Rotation Settings of Panel Services

You can define log rotation parameters for Panel services in general and for each domain separately.

Log rotation parameters for Panel services are defined in the `$PRODUCT_ROOT_D/etc/logrotate.conf` configuration file. Part of this file is shown below.

```
# less /usr/local/psa/etc/logrotate.conf
include /usr/local/psa/etc/logrotate.d

/usr/local/psa/var/log/xferlog.processed {
    missingok
    rotate 3
    size 10M
    compress
    nocreate
}
```

Log Rotation Settings of Hosted Domains

In turn, log rotation parameters for domains hosted on the Panel server are stored in configuration files in the `$PRODUCT_ROOT_D/etc/logrotate.d/` directory.

You can configure log rotation for a particular domain through the Panel GUI. To do this:

1. Log in to Control Panel.
2. Open the **Website & Domains** tab, click **Logs**.

3. Click Log Rotation.**4. Change the log rotation configuration if needed.**

When you click OK, the configuration is saved in the domain `logrotate` configuration file `$PRODUCT_ROOT_D/etc/logrotate.d/<domain_name>`. A fragment of this is provided below. Configuration changes are applied equally for all log files of this domain.

```
/var/www/vhosts/domain.tst/statistics/logs/*.processed {
    monthly
    rotate      10
    compress
    missingok
}
```

Adding Creation Date to Rotated Log File Names

To make working with log files more convenient, you can include the file creation date into the names of rotated log files. If you do this, the names of rotated log files will have the following format `<log_name>.processed-YYYYMMDD.gz`, where `<log_name>` is the name of the log file before rotation, like `error_log` or `httpsd_access_log`, and `YYYYMMDD` is the date of the log rotation. For example, `error_log.processed-20130101.gz`.

To include the creation date into the names of rotated log files, open the desired log rotation configuration file and add the line `dateext` to the corresponding sections.

Resource Usage Reports

Parallels Plesk Panel has a built-in mechanism that generates daily, weekly, or monthly reports on resource usage by customers, resellers, and domains. You can view these reports in **Server Administration Panel > Tools & Settings > Summary Report**.

There are two types of report:

- *Summary reports* contain common information, such as number of customers and resellers, total traffic and disk space usage, number of domains, subdomains, mailboxes, and so on.
- *Full reports* contain all the information from summary reports and separate statistics on resource usage for each customer, reseller, and domain.

To switch between summary and full reports, choose the corresponding value in the checkbox at the top left of the screen.

You can also make Panel send these reports to a certain e-mail address. To do this, go to **Server Administration Panel > Tools & Settings > Summary Report > Delivery Schedule** and choose the schedule from the existing ones or create a new one.

To produce reports, Panel uses the `autoreport.php` script located in `$PRODUCT_ROOT_D/admin/plib/report/` directory, where `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

Enhancing Performance

For those Parallels Plesk Panel administrators who want to use Panel more efficiently, we propose ways to improve Panel functioning in different situations. In this chapter, we will discuss the following improvements:

- Reducing resources consumption for Panels that operate in virtual private server environment.
- Increasing the number of domains that a single Panel server is capable of managing.
- Preventing server overload by limiting the number of anti-spam processes.

In this chapter:

Reducing Resources Consumption in VPS Environments	134
Increasing the Number of Domains that Panel Can Manage.....	139
Making Your Mail Spam Resistant	143
Optimizing the Task Manager Performance	143

Reducing Resources Consumption in VPS Environments

If you deploy Parallels Plesk Panel in a VPS environment, for example, Parallels Virtuozzo Containers, consider switching the Panel to the *VPS-optimized mode*. This mode switches off modules that are not critical for hosting services. See the section **Apache Modules Switched Off in VPS-Optimized Mode** for details. This makes the Panel use less memory than other control panels and provides better utilization of hardware resources and increased density of virtual environments per server.

Note: You can switch only clean Panel installations to the optimized mode, it is not possible to do this with Panel installations upgraded from earlier versions. Moreover, you can enable the optimized mode only on fresh installations of the Panel which have not yet been initialized.

Next in this section:

Setting Up VPS Optimized Mode in Parallels Virtuozzo Containers.....	135
Setting Up VPS-Optimized Mode in Non-Virtuozzo Environments.....	137
Apache Modules Switched Off in VPS-Optimized Mode	137

Setting Up VPS Optimized Mode in Parallels Virtuozzo Containers

In the Parallels Virtuozzo Containers for Linux, the VPS-optimized mode switches off the InnoDB engine in the MySQL database server, and Apache web server modules that are not critical for hosting services.

The only disadvantages of using the optimized mode are as follows:

- Web applications requiring InnoDB will not work.
- Perl, python and ASP scripts will not work because the required Apache modules will be switched off.
- PHP will be available only through CGI.

➤ ***To switch Panel to the VPS-optimized mode in the Virtuozzo environment:***

Install the `pp11.5.30-vps-optimized` EZ template. The template applies the necessary configuration.

➤ ***If you need to switch the Panel back to the normal mode of operation, perform the following steps:***

1. Switch on the InnoDB engine.
 - a. Open for editing the file `/etc/my.cnf`.
 - b. Locate the lines containing entries `skip-innodb` and remove them, or comment them out.
 - c. Save the file.
 - d. Restart MySQL server.
2. Switch on the required Apache modules.
 - On Debian Linux, use the `a2enmod` utility to switch on all required modules. For example, if you want to switch on the PHP module, issue the following command:


```
a2enmod php5
```
 - On other distributions of Linux, edit the main Apache configuration file, which, in most Linux installations, is located in `/etc/httpd/conf/`.
 - a. Open for editing the file `/etc/httpd/conf/httpd.conf`.
 - b. Locate the lines `LoadModule <module_name>` corresponding to the modules that you want to switch on, and uncomment the lines.
 - c. Save the file.
 - d. Restart Apache.

3. Switch the Panel back to normal operation mode by issuing the following SQL query:

```
mysql -uadmin -p`cat /etc/psa/.psa.shadow` psa -e "update misc set  
val='0' where param='vps_optimized_mode_status';"
```


Setting Up VPS-Optimized Mode in Non-Virtuozzo Environments

If you operate in VPS environments other than Virtuozzo-based ones (Parallels Virtuozzo Containers or OpenVZ containers), you can also switch Panel to VPS-optimized mode.

➤ **To switch Panel to the VPS-optimized mode in a non-Virtuozzo environment run the following command:**

```
PRODUCT_ROOT_D/bin/vps_optimized --turn-on, where $PRODUCT_ROOT_D is /usr/local/psa for RPM-based systems or /opt/psa on DEB-based systems.
```

Optimizing Resources Consumption

To improve the Panel resources consumption, update the `mysqld` configuration file `/etc/my.cnf` by adding the `skip-bdb` line to the `[mysqld]` section, and restart `mysqld`.

Although it is not recommended to use SpamAssassin and Parallels Premium Antivirus while operating in the VPS-optimized mode, you can still do that. The following instructions help you optimize these services:

- To optimize Parallels Premium Antivirus resource consumption, open for editing file `/etc/drweb/drweb32.ini`, set `PreFork = No`, and restart the service.
- To optimize SpamAssassin resource consumption, run the following command after performing the initial Panel configuration:

```
/usr/local/psa/bin/spamassassin --update-server -max-proc 1
```

Switching to Power User

Panel administrators have the option to use Panel for their own needs by only leaving relevant controls in the UI and removing all those related to shared hosting business (resellers, service plans, subscriptions). To enable this simple and lightweight user interface, run the following command:

```
/usr/local/psa/bin/poweruser --on
```

Apache Modules Switched Off in VPS-Optimized Mode

The following Apache modules are switched off in the optimized mode:

- `authn_alias`
- `authn_anon`
- `authn_dbm`
- `authn_default`
- `authz_user`
- `authz_owner`

- authz_groupfile
- authz_dbm
- authz_default
- ldap
- authnz_ldap
- ext_filter
- mime_magic
- deflate
- usertrack
- dav_fs
- vhost_alias
- speling
- proxy_balancer
- cache
- disk_cache
- file_cache
- mem_cache
- version
- asis
- bw
- proxy_ajp
- auth_ldap
- perl
- python
- php5
- php4

The list of modules can vary depending on the operating system distribution and architecture. When Panel is installed and the optimized mode is switched on, you can check the list in the following files:

- On 32-bit operating systems - `/usr/lib/plesk-9.0/vps_optimized_aspects/apache-modules-all`
- On 64-bit operating systems - `/usr/lib64/plesk-9.0/vps_optimized_aspects/apache-modules-all`

Increasing the Number of Domains that Panel Can Manage

By default, Parallels Plesk Panel allows you to manage up to 300 domains on a single server. If you plan to run more sites on a Panel server, consider switching on the support of piped logs in the Apache web server. This is done on the **Tools & Settings > Apache Web Server** page of the Server Administration Panel.

Running Apache with piped logs allows you to host up to 900 domains on a server. If you are going to host a larger number of web sites on your server, Apache may fail to work because of a problem with the file descriptors limit. To avoid this, you can recompile Apache with more file descriptors.

Note: Parallels Plesk Panel (8.2.0 and later) with piped logs feature enabled can host up to 900 domains without the recompilation of Apache system packages.

Next in this section:

Recompiling Apache with More File Descriptors on RedHat-like Systems.....	140
Recompiling Apache with More File Descriptors on Debian Systems	142

Recompiling Apache with More File Descriptors on RedHat-like Systems

- *To recompile related applications and libraries, such as openssl, apache, imap, PHP etc from source RPMs with more file descriptors, perform the following steps:*

1. Make sure that the system allows you 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 CD or from the download site of your operating system.

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, which can be found on the download site of your operating system 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 this 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 Systems

➤ *To recompile Apache, PHP and IMAP with a number of file descriptors larger than `FD_SETSIZE` (1024) on Debian systems:*

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 to `220=1048576`).

3. Add the following line to the 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 this:

```
#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-client2002edebian
# dpkg -i libc-client-dev_2002edebian1-*.deb libc-
client2002edebian*.deb mlock*.deb
# apt-src --build install php4
# dpkg -i `ls *deb|grep php4|grep -v apache-mod`
```

Making Your Mail Spam Resistant

If there is a large spam attack, the antispam daemon `spamd` starts too many processes and the system can run out of resources. You can limit the number of simultaneously running SpamAssassin processes through the Panel GUI. Use the **The maximum number of worker spamd processes to run (1-5)** option on the **Server > Tools & Settings > SpamFilter** page. You can retrieve this value by executing the following command:

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

Optimizing the Task Manager Performance

Parallels Customer and Business Manager automates certain hosting providers' tasks such as creating Panel accounts and subscriptions, registering domain names, issuing invoices, and so on. To do this, Business Manager uses its own *task manager*. This task manager does the following:

- Schedules and runs tasks.
- Stores task details and execution statuses.
- Suggests how to resolve possible task execution problems.

If you want to utilize your server resources better, consider optimizing task manager performance in your environment by changing its settings defined in the `/opt/plesk-billing/task-manager/config/config.ini` configuration file. The paragraphs of this section describe the ways to optimize certain aspects of the task manager.

Reducing Disk Space Consumption

If you want the task manager to consume less disk space, you can reduce the size of its own database. To do this, adjust the following settings that define how much information the task manager stores in the database:

- *How long task manager stores information about processed tasks.* The parameters that set these intervals for completed, failed and canceled tasks are `completedTasksClearInterval`, `failedTasksClearInterval`, and `canceledTasksClearInterval` correspondingly.
By default, these intervals are equal to 1 year. If you want to change them, specify the values in the ISO 8601 standard, for example, `P1Y` for the 1 year interval.
- *How much information about each task execution is stored.* For troubleshooting purposes, the task manager writes information about task executions to log files, one file per each execution. The parameter that sets maximum number of stored log files for each task is the `maxTaskLogs`. Its default value is 5. To make the logs consume less disk space, specify a smaller value of this parameter.

Note: When you set the task removal intervals described above, remember that setting too small values may make troubleshooting difficult since you may not have enough information about recent task executions.

Increasing Task Manager Performance

When you run all scheduled tasks at once, task manager starts processing a certain number of tasks simultaneously. After completing (or failing to complete) the task, the task manager starts another task from the queue and so on. To make processing of multiple tasks faster, increase the maximum number of tasks processed simultaneously. The parameter that sets this number is `runAllMaxInstances`.

However, when you set a greater value for this parameter, remember that too big values increase the system load and therefore may reduce the Panel performance or even block customer access to the Control Panel.

Increasing Logs Detalization

To make the task manager produce more information that may help you in troubleshooting issues, adjust the logging settings in the following ways:

- *Increase the number of execution logs for each task.* To do this, edit the value of the `maxTaskLogs` parameter. When you set a greater value, remember that this will increase the disk space consumption.
- *Increase the verbosity of the logs.* By default, the task manager writes only error information to log files. To get more information on tasks execution, include tasks execution messages into the logs by changing values of the parameters `log.info` and `log.sql` to 1.

Important: Including debug information into the task manager logs will reduce its performance; Therefore, we recommend that you include this information only when you troubleshoot certain issues.

Customizing Panel Appearance and GUI Elements

This chapter introduces Panel themes that can be used to customize Panel appearance and branding. It also describes how to remove links for access to Presence Builder, Google Services for Websites, reconfigure behaviour of the link to Support service and other GUI elements.

In this chapter:

Customizing Panel Appearance and Branding	146
Hiding and Changing Panel GUI Elements.....	147

Customizing Panel Appearance and Branding

Administrators and resellers can change the following settings related to Panel branding and appearance:

- By means of Panel GUI - change the Panel logo image, URL attached to it, and Panel name shown in browser's title bar text.
- By means of custom themes - change the Panel logo image, URL attached to it, Panel name shown in browser's title bar text, and visual appearance of Panel's pages (CSS styles and images used for button backgrounds).

A theme is a ZIP archive containing all CSS and image files used by Panel. Preparing a custom theme involves the following steps:

1. Obtaining a ZIP archive with the default Panel theme.
2. Unpacking the archive and changing the necessary files.
3. Packing the archive with modified files, uploading it to the server, and installing the theme.

To learn about creating and using custom themes, refer to the document **Creating Custom Themes**.

Hiding and Changing Panel GUI Elements

This section describes how to switch on or off or modify various Panel features and customize links in Panel. For example, you can hide all controls related to mail service or show promotional links in your Panel. To learn more about these and other possible customizations, read the subsections of this section.

To display, hide, or edit Panel interface elements, you can use one of the following approaches or a combination of them: run a special command-line command, modify a license key to Panel, or perform changes to a particular configuration file. Here are some details on these approaches:

- *Command line.* This is performed by running the `panel_gui` and the `server_pref` utilities. For more information, see the corresponding chapters of the **Reference for Command Line Utilities** document.
- *License key.* Upgrades of license keys are performed via the web-based Key Administrator interface or Partner API - an XML-based remote-call protocol. Below we will provide more information about this approach.
- *Configuration files.* This requires editing the configuration files:
 - `panel.ini` for Panel customizations
 - `config` for Presence Builder customizations.

License Key



There are extra features that can be turned on or off in the Panel license. These changes are available to those who have access to the Parallels Key Administrator web-based management interface or Partner API.

The license modifications can be done on a per-license level, or be a default for you and applied automatically to all the licenses created for you. In both cases, you should contact Parallels sales: to apply the partner-wide defaults, or to enable a particular extra customization on a per-license level.

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Web-based Key Administrator User Interface

You can turn off the listed earlier features through the KA web-based user interface by adding them to your license. The features reside in the *Parallels Panel Extras* group.

- To turn off required features for a *new license*, start the New Key wizard () and add the features at step three, the feature management.
- To turn off required features for an *existing license*, start the Key Upgrade wizard () and add the features at step two, the feature management.

To turn on a license feature, detach it from the license.

For details on managing license features, please see the **KA Client User Guide**, Chapter **Managing Keys**. You can access this document by clicking the help link in the KA user interface.

Partner API

To turn off the extra features in new or existing licenses by means of Partner API, run the appropriate API method with specific feature API identifiers set.

For new licenses:

Add API identifiers of the required features to the "array of identifiers of upgrade plans" parameter of method `partner10.createKey` and execute it.

For details on the method specification, please see:

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.createKey**

For existing licenses:

Add API identifiers of the required features to the "upgrade plan name" parameter of `partner10.upgradeKey` method and execute it.

For details on the method specification, please see:

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.upgradeKey**

Next in this section:

Domain Registration and Management Services	149
SSL Certificates Selling Services	152

Link to Provider's Website	159
Google Services for Websites Buttons	161
Products from Parallels Partners Button	163
Presence Builder Buttons	165
Panel Upgrades.....	167
Mail Service Controls	168
Links for Purchasing Panel License and Add-On Keys	172
Promos.....	175
Link to Online Support Service	179
The Facebook Like Button.....	181
Product Rating Widget.....	183
RSS Feeds.....	184
Voting for New Features.....	187

Domain Registration and Management Services

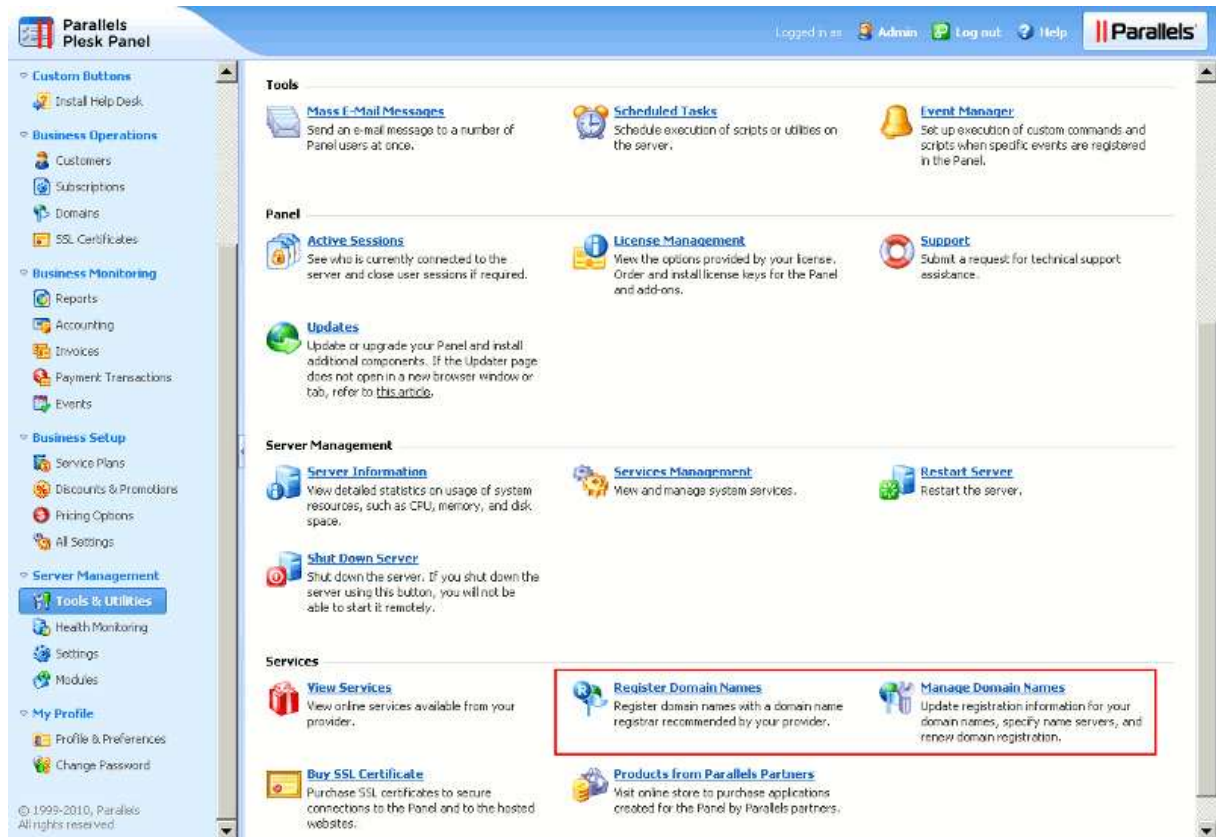
These buttons let your customers visit a website where they can purchase new or manage existing domain names. By customizing them, you can make the customers use your preferred domain name registrar.

Next in this section:

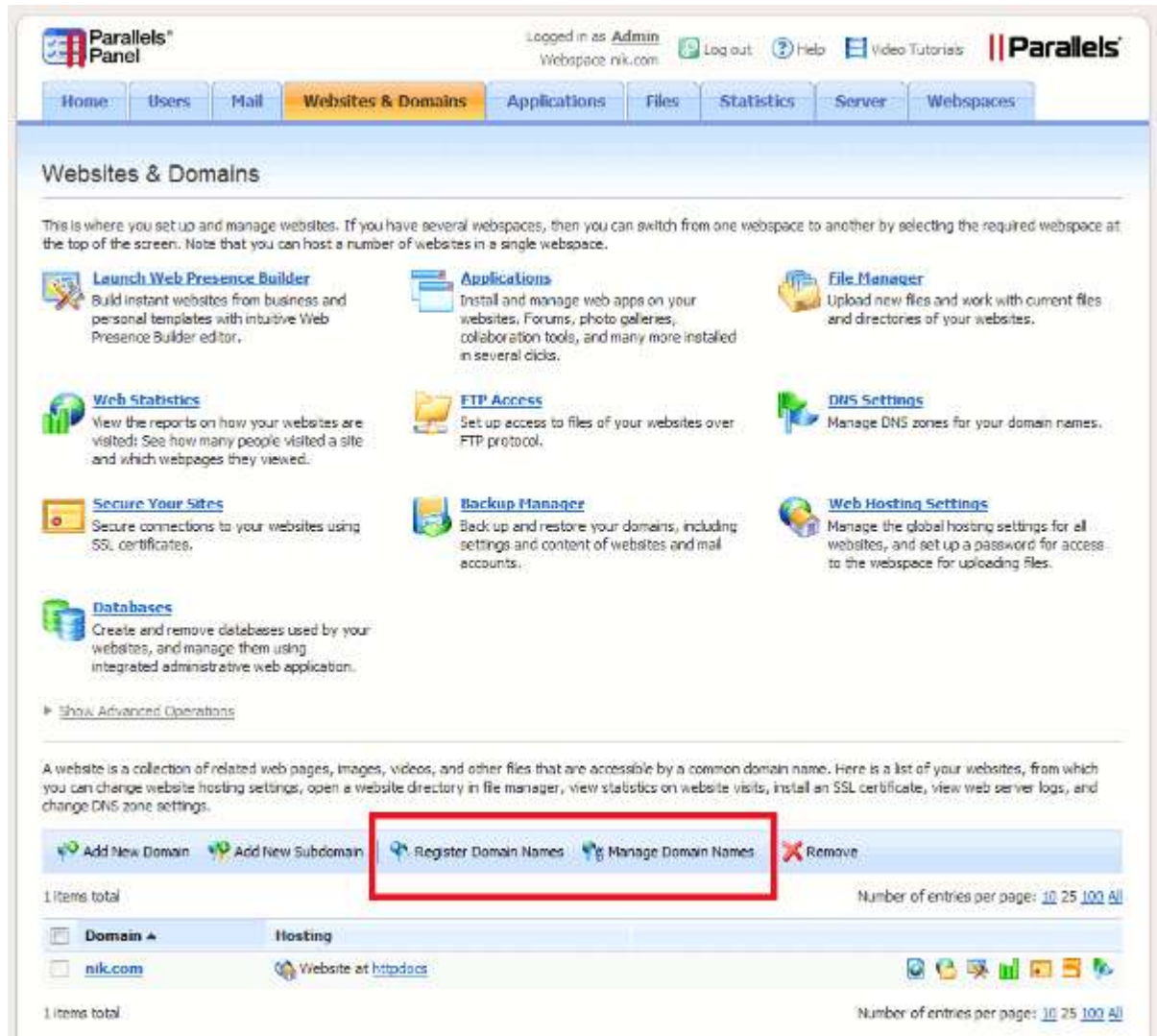
Location of Domain Registration and Domain Management Buttons	150
Changing Domain Name Registrar's URLs.....	151
Hiding Domain Registration and Domain Management Buttons	152

Location of Domain Registration and Domain Management Buttons

- Server Administration Panel: Tools & Settings > Register Domain Names and Manage Domain Names buttons.



- Control Panel: **Websites & Domains** tab > **Register Domain Names** and **Manage Domain Names** buttons.



Changing Domain Name Registrar's URLs

You can change the domain name registrar's URLs only through command line.

- **To change the URL of the Register Domain Names button, run the following command:**

```
/usr/local/psa/bin/panel_gui -p -domain_registration_url <url>
```

- **To change the URL of the Manage Domain Names button, run the following command:**

```
/usr/local/psa/bin/panel_gui -p -domain_management_url <url>
```

Hiding Domain Registration and Domain Management Buttons

You can hide the domain name registration and domain management buttons both through the command line and the Partner API.

- ***To remove the Register Domain Names button and Manage Domain Names button using the command line, run the following command:***

```
/usr/local/psa/bin/panel_gui -p -domain_registration true
```

- ***To remove the Register Domain Names button and Manage Domain Names button using the Partner API:***

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "EXTRAS_BUTTONS_OFF" in the "array of identifiers of upgrade plans" parameter.

For details on these methods specification, please see <http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.createKey** and section **Specifications of Methods / partner10.upgradeKey**

Note: API identifier "EXTRAS_BUTTONS_OFF" also disables the controls related to SSL certificate selling services and the link to the provider's website.

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

SSL Certificates Selling Services

These buttons lead to a website where your customers can purchase and view SSL certificates. By customizing these controls, you can make the customers use your preferred SSL certificates vendor.

Next in this section:

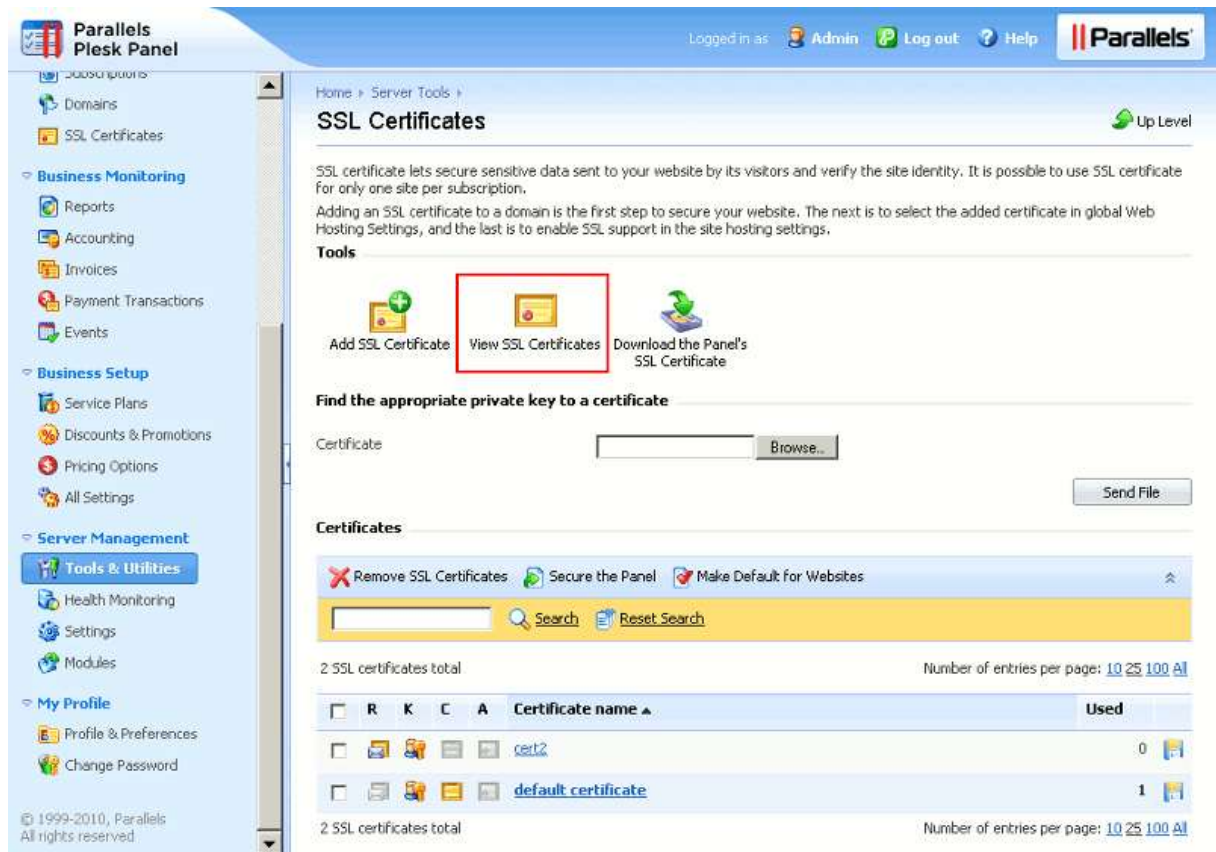
Locations of Links for Purchasing and Viewing SSL Certificates	153
Changing SSL Certificate Seller's URLs	158
Hiding Buttons for Viewing and Purchasing SSL Certificates.....	159

Locations of Links for Purchasing and Viewing SSL Certificates

- Server Administration Panel: Tools & Settings > SSL Certificates > Add SSL Certificate > Buy SSL Certificate button.

The screenshot shows the Parallels Plesk Panel interface. The left sidebar contains a navigation menu with categories like Subscriptions, Service Plans, Custom Buttons, Business Operations, Business Monitoring, and Business Setup. The main content area is titled 'Add SSL Certificate' and includes a 'Certificate' section with a text input for 'Certificate name *'. Below this is a 'Settings' section with a detailed explanation of certificate types and a form with fields for Bits (1024), Country (United States), State or province *, Location (city) *, Organization name (company) *, Organization department or division name, Domain name *, and E-mail *. At the bottom right, there are three buttons: 'Request', 'Buy SSL Certificate' (highlighted with a red rectangle), and 'Self-Signed'.

- Server Administration Panel: Tools & Settings > SSL Certificates > View SSL Certificates button.



Parallels Plesk Panel Logged in as **Admin** Log out Help

Home > Server Tools > **SSL Certificates** Up Level

SSL certificate lets secure sensitive data sent to your website by its visitors and verify the site identity. It is possible to use SSL certificate for only one site per subscription.

Adding an SSL certificate to a domain is the first step to secure your website. The next is to select the added certificate in global Web Hosting Settings, and the last is to enable SSL support in the site hosting settings.

Tools

Add SSL Certificate **View SSL Certificates** Download the Panel's SSL Certificate

Find the appropriate private key to a certificate

Certificate

Certificates

Remove SSL Certificates Secure the Panel Make Default for Websites

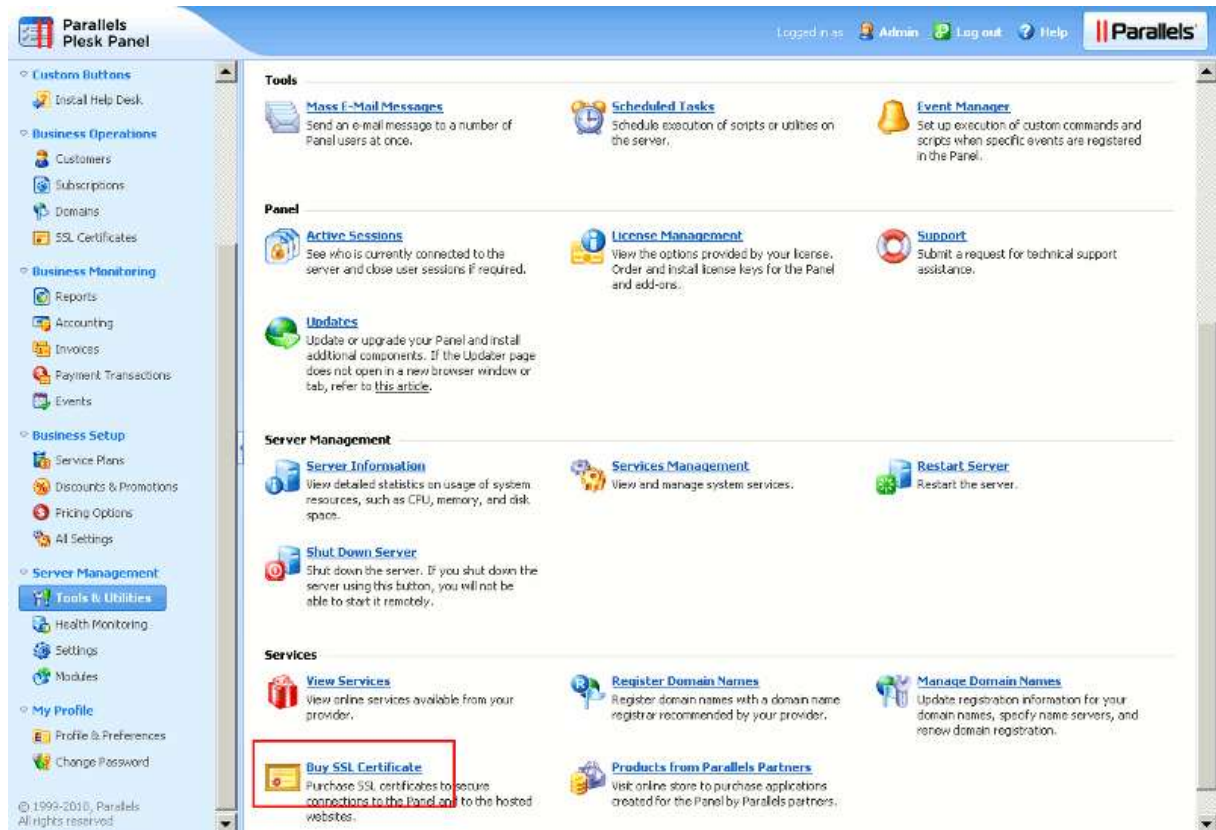
2 SSL certificates total Number of entries per page: 10 25 100 All

<input type="checkbox"/>	R	K	C	A	Certificate name ▲	Used
<input type="checkbox"/>					cert2	0
<input type="checkbox"/>					default certificate	1

2 SSL certificates total Number of entries per page: 10 25 100 All

© 1999-2010, Parallels All rights reserved.

- Server Administration Panel: Tools & Settings > Buy SSL Certificate button.



- Control Panel: **Websites & Domains** tab > **SSL Certificates** > **Add SSL Certificate** > **Buy SSL Certificate** button.

The screenshot shows the Parallels Plesk Panel interface. At the top, the logo and navigation tabs are visible. The 'Websites & Domains' tab is selected. The 'SSL certificates' section is active, and the 'Add SSL Certificate' page is displayed. The page includes a 'Certificate' section with a text input for the certificate name. Below this is the 'Settings' section, which contains instructions and a form for generating a certificate request. The form includes fields for Bits (1024), Country (United States), State or province, Location (city), Organization name (company), Organization department or division name, Domain name, and E-mail. At the bottom right, there are three buttons: 'Request', 'Buy SSL Certificate' (highlighted with a red rectangle), and 'Self-Signed'.

Parallels Plesk Panel

Logged in as **Admin**
Subscription **nik.com** Log out Help

Home Users Mail **Websites & Domains** Applications Statistics Account

SSL certificates > **Add SSL Certificate** Up Level

Certificate

Certificate name *

Settings

Use this form to generate a certificate request, to buy a certificate from your provider, or to generate a self-signed certificate.

Request is a CSR file with info about your domain (from the form). You can submit the request to a desired certification authority so that they issue a certificate for you. You will then upload it using one of the Upload forms below.

Self-signed certificate is an identity certificate signed by its own creator, so if you use such a certificate, it will mean that you yourself verify your sites identity. Although self-signed certificates let use SSL, they are trusted less, and considered as less secure.

Bits 1024

Country United States

State or province *

Location (city) *

Organization name (company) *

Organization department or division name

Domain name *

E-mail *

Request Buy SSL Certificate Self-Signed

- Control Panel: **Websites & Domains** tab > **SSL Certificates** > **View Certificates** button.

The screenshot shows the Parallels Plesk Panel interface. At the top, the 'Websites & Domains' tab is selected. The 'SSL Certificates' section is active, displaying a 'Tools' area with two buttons: 'Add SSL Certificate' and 'View Certificates'. The 'View Certificates' button is highlighted with a red rectangular box. Below the tools, there is a section titled 'Find the appropriate private key to a certificate' with a text input field labeled 'Certificate' and a 'Browse...' button. A 'Send File' button is also present. The 'Certificates' section below shows 'No SSL certificates'. The footer contains the Parallels logo and copyright information: '© Copyright 1999-2010, Parallels. All rights reserved'.

Changing SSL Certificate Seller's URLs

You can change the SSL certificate seller's URLs only through the command line interface.

- **To change the URLs of the Buy SSL Certificate and View Certificates buttons, run the following command:**

```
/usr/local/psa/bin/panel_gui -p -cert_purchasing_url <url>
```

The Format of a POST Request

Note that buttons used to buy or view SSL certificates do not just lead to a URL specified with the command above. Actually, Panel sends a POST request to this URL. The format of the POST request body varies depending on a button function. For example, if a button is used to buy SSL certificates, the request body contains such CSR parameters as a domain name, business name, country, and so on.

The table below provides the details on the parameters which are sent in POST requests.

Button location	Parameters in the POST request body	Example
<ul style="list-style-type: none"> Server Administration Panel, Tools & Settings > SSL Certificates > Buy SSL Certificate. Control Panel, Websites & Domains > Secure Your Sites > Add SSL Certificate > Buy SSL Certificate. 	<pre>csr = <encoded request> csr_domain = <domain name> csr_bits = <key size> csr_email = <administrator's e-mail> csr_company = <company name> csr_department = <organization department name> csr_state = <state> csr_city = <city> csr_country = <country> action = CREATE_CERT</pre>	<pre>csr = -----BEGIN CERTIFICATE REQUEST----- MIICyTCCAbE CAQAwgYMxCzA JBgNVBAYTAIJJVMQww CgYDVQQIEwNOC2sx DDAKBgNV ... --- --END CERTIFICATE REQUEST----- csr_domain = example.com csr_bits = 2048 csr_email = admin@example.com csr_company = ACME csr_department = IT csr_state = Illinois csr_city = Chicago csr_country = US action = CREATE_CERT</pre>
<ul style="list-style-type: none"> Server Administration Panel, Tools & Settings > SSL Certificates > View SSL Certificates. Server Administration Panel, Tools & Settings > Buy SSL Certificate. Control Panel, Websites & Domains > Secure Your Sites > View Certificates. 	<pre>action = MODIFY_CERT</pre>	

Hiding Buttons for Viewing and Purchasing SSL Certificates

You can hide the buttons for viewing and purchasing SSL certificates both through the command line and the Partner API.

- **To remove the buttons for viewing and purchasing SSL certificates using the command line, run the following command:**

```
/usr/local/psa/bin/panel_gui -p -cert_purchasing true
```

- **To remove the buttons for viewing and purchasing SSL certificates using the Partner API:**

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "EXTRAS_BUTTONS_OFF" in the "array of identifiers of upgrade plans" parameter.

For details on these methods specification, please see

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.createKey** and section **Specifications of Methods / partner10.upgradeKey**

Note: API identifier "EXTRAS_BUTTONS_OFF" also disables the controls related to SSL certificate selling services and the link to the provider's website.

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Link to Provider's Website

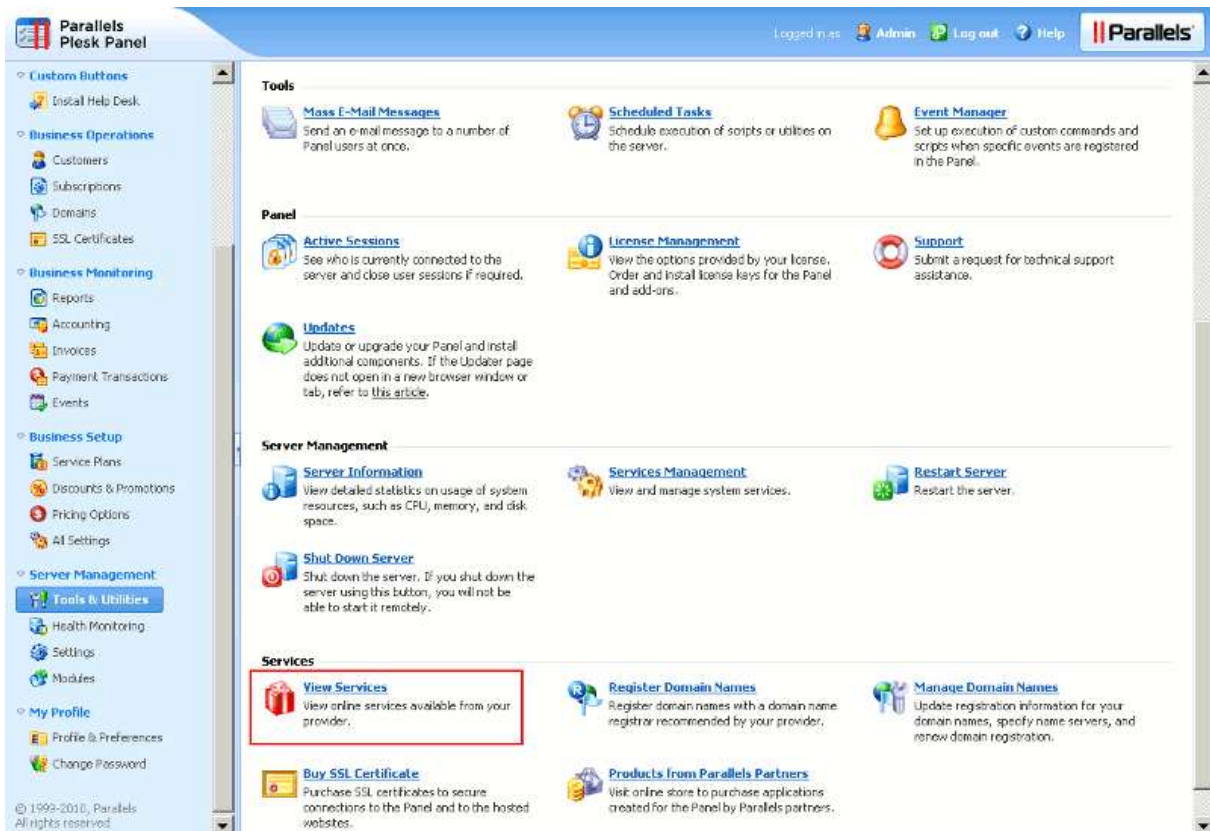
This button redirects customers to your site where they can purchase and use services provided by your company.

Next in this section:

Location of the Link to Provider's Website	160
Changing the URL of the View Services Button.....	160
Hiding the View Services Button.....	161

Location of the Link to Provider's Website

Server Administration Panel > Tools & Settings > View Services button.



Changing the URL of the View Services Button

You can change the URL of the **View Services** button only through the command line.

➤ **To change the URL that opens when the View Services button is clicked, run the following command:**

```
/usr/local/psa/bin/panel_gui -p -mpc_portal_url <url>
```


Hiding the View Services Button

You can hide the **View Services** button both through the command line and the Partner API.

- **To remove the View Services button using the command line, run the following command:**

```
/usr/local/psa/bin/panel_gui -p -extras true
```

- **To remove the View Services buttons using the partner API:**

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "EXTRAS_BUTTONS_OFF" in the "array of identifiers of upgrade plans" parameter.

For details on these methods specification, please see

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.createKey** and section **Specifications of Methods / partner10.upgradeKey**

Note: API identifier "EXTRAS_BUTTONS_OFF" also disables the controls related to SSL certificate selling services and link to the provider's website.

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Google Services for Websites Buttons

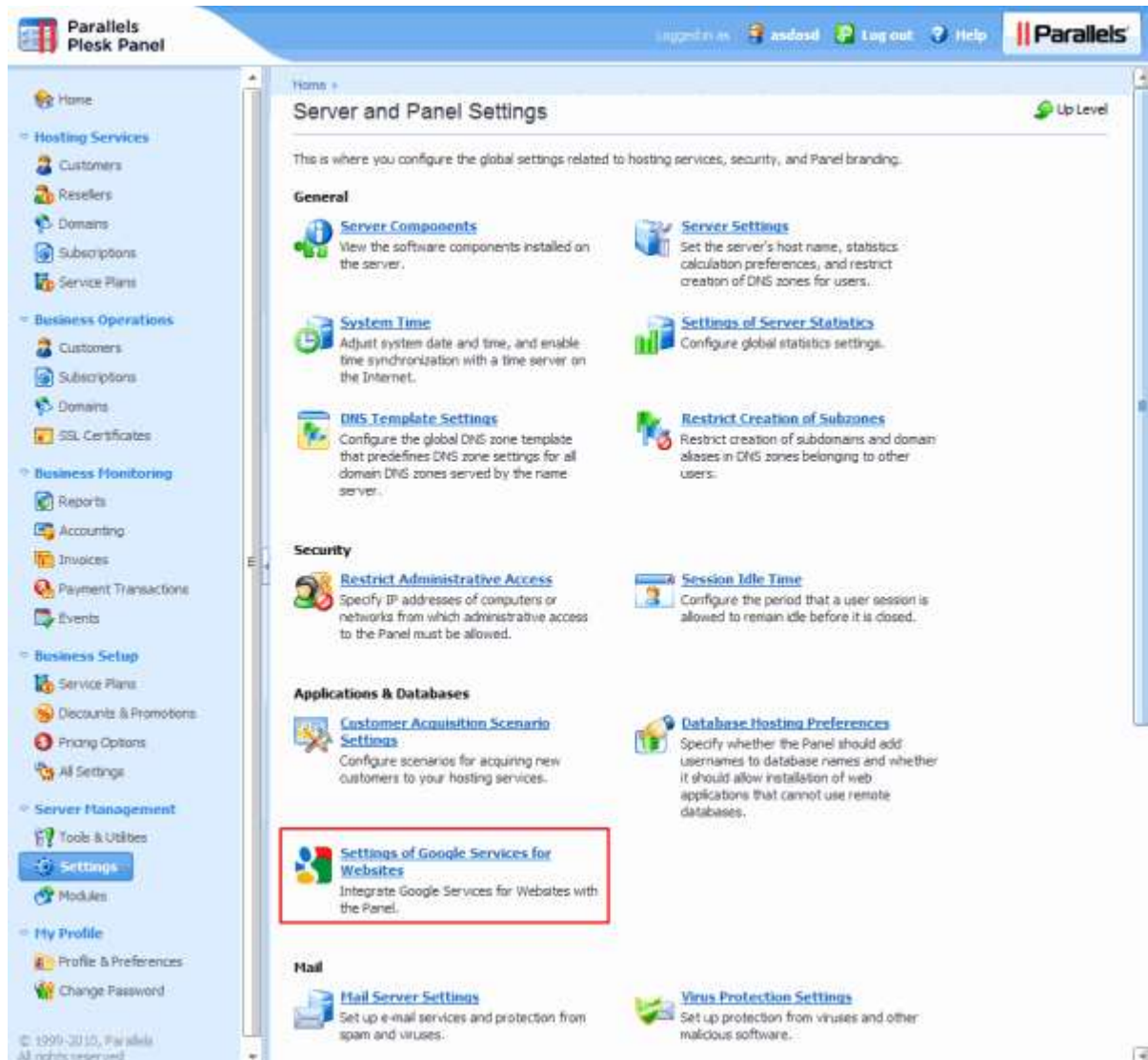
If you are signed up to the Google Services for Websites access provider program, your customers will see the **Google Services for Websites** button in Control Panel. You can hide this button if you do not want them to use Google Services for Websites.

Next in this section:

Location of the Google Services for Websites Controls	162
Hiding the Google Services for Websites Buttons.....	163

Location of the Google Services for Websites Controls

- Server Administration Panel > Tools & Settings > Settings of Google Services for Websites button.



- Control Panel > Websites & Domains tab > Google Services for Websites button. It is shown if the Services are enabled by Administrator.

Hiding the Google Services for Websites Buttons

You can hide the Google Services for Websites only through Partner API.

➤ *To hide the Google Services for Websites buttons:*

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "DISABLE_GOOGLE_TOOLS" in the "array of identifiers of upgrade plans" parameter.

For details on the methods specification, please see

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.createKey** and section **Specifications of Methods / partner10.upgradeKey**

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Products from Parallels Partners Button

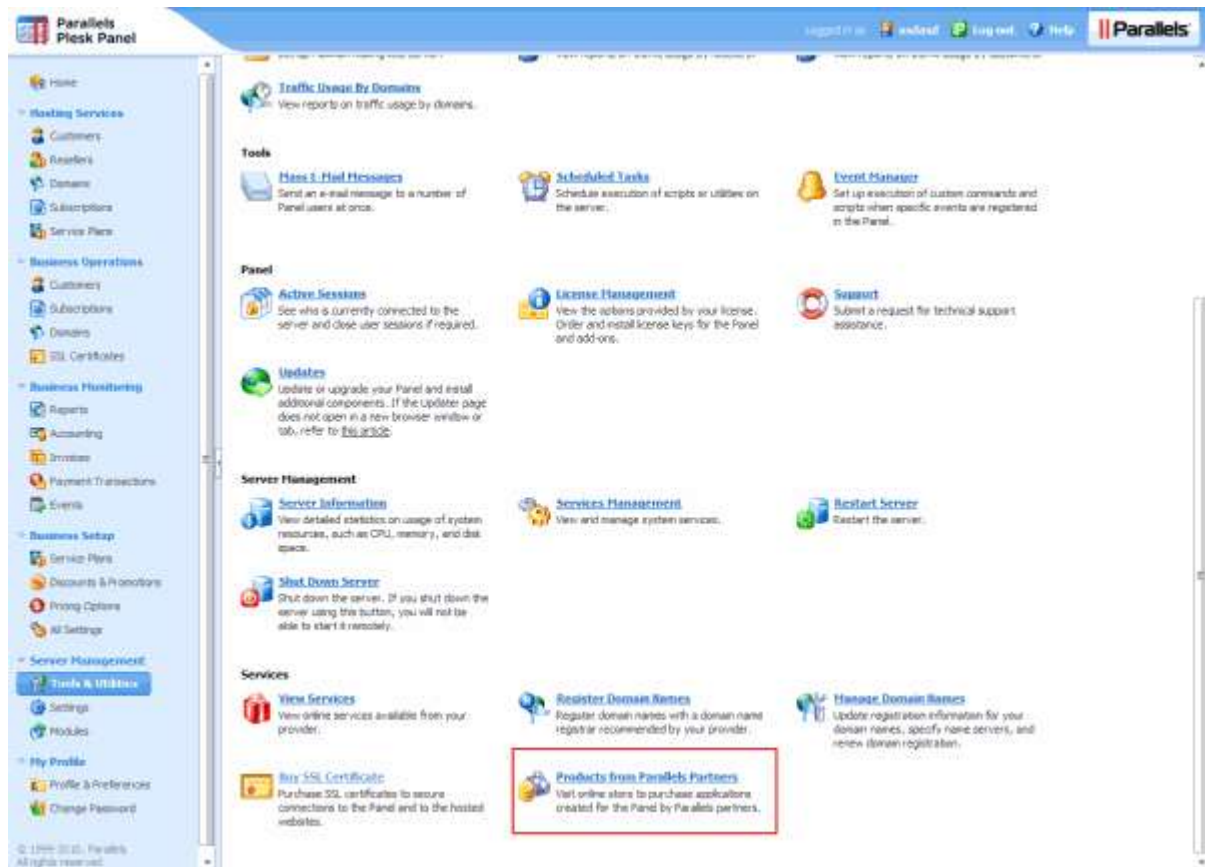
This button leads to the store where your customers can purchase software products from Parallels partners. The link is not editable. You can hide this button.

Next in this section:

Location of the Products from Parallels Partners Button.....	164
Hiding the Products from Parallels Partners Button	165

Location of the Products from Parallels Partners Button

Server Administration Panel > Tools & Settings > Products from Parallels Partners button.



Hiding the Products from Parallels Partners Button

You can hide the **Products from Parallels Partners** button only through Partner API.

➤ *To hide the button Products from Parallels Partners:*

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "STORE_BUTTON_OFF" in the "array of identifiers of upgrade plans" parameter.

For details on the methods specification, please see:

<http://www.parallels.com/ptn/documentation/ka/>, section Specifications of Methods / `partner10.createKey` and section Specifications of Methods / `partner10.upgradeKey`

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Presence Builder Buttons

These are controls that open Presence Builder. You can hide them from customer's interface. This will not disable Presence Builder.

Next in this section:

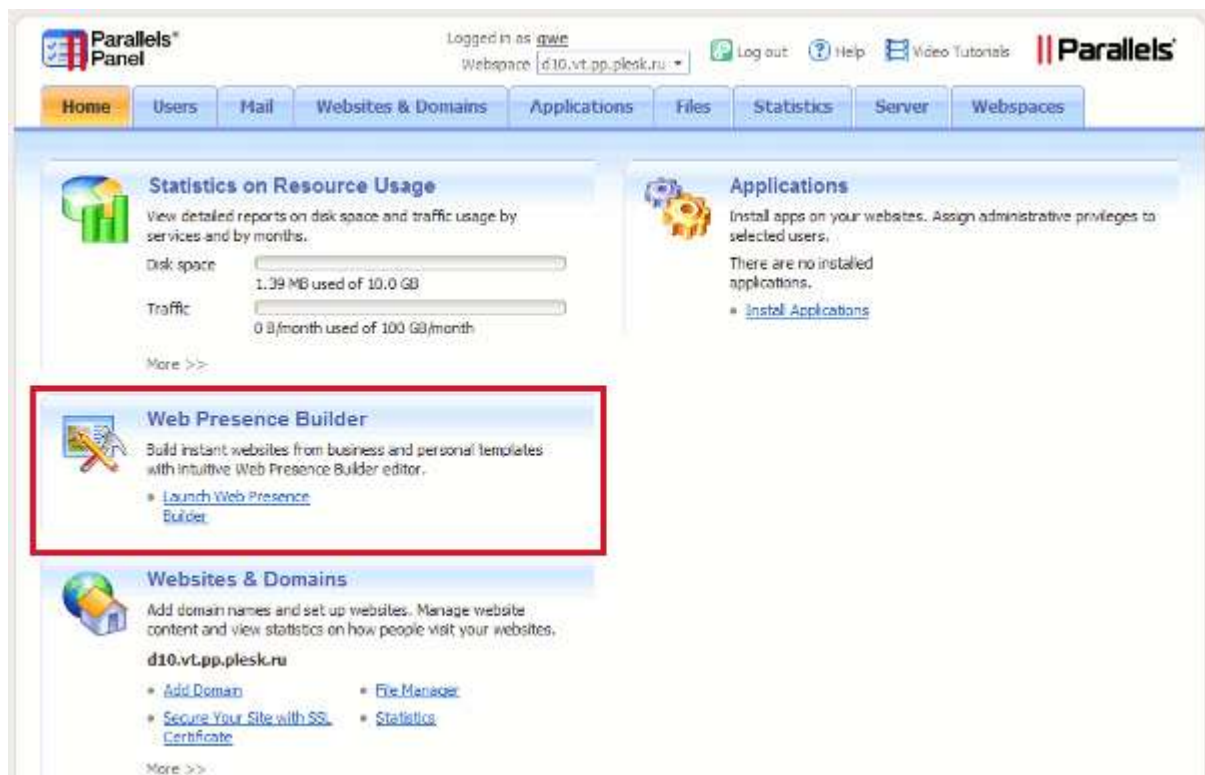
Location of the Presence Builder Buttons	166
Hiding the Presence Builder Buttons	167

Location of the Presence Builder Buttons

- Control Panel: **Websites & Domains** tab > **Launch Presence Builder**.



- Control Panel: **Home** tab > **Launch Presence Builder**.



Hiding the Presence Builder Buttons

You can hide the Presence Builder buttons only through Partner API.

➤ *To hide the Presence Builder buttons:*

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "DISABLE_SITEBUILDER" in the "array of identifiers of upgrade plans" parameter.

For details on the methods specification, please see

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / partner10.createKey** and section **Specifications of Methods / partner10.upgradeKey**

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Panel Upgrades

When a new minor or major version of the Panel is released, Parallels Updater adds an information box to the Server Administration Panel home page offering to update the Panel. This can be disabled, so that only updates for the current version are installed.

Next in this section:

Disabling Panel Upgrades 168

Disabling Panel Upgrades

You can disable the Panel upgrades only by modifying license keys, through the Partner API.

➤ ***To disable panel upgrades:***

Use the `partner10.createKey` or `partner10.upgradeKey` with the API identifier "DISABLE_FEATURE_UPGRADES" in the "array of identifiers of upgrade plans" parameter.

For details on the methods specification, please see

<http://www.parallels.com/ptn/documentation/ka/>, section **Specifications of Methods / `partner10.createKey`** and section **Specifications of Methods / `partner10.upgradeKey`**

Important: Once you have turned off a feature through the Partner API, there are no documented methods to turn it back on. If you need to perform this reverse operation, please use the web-based user interface, or contact your sales representative.

Mail Service Controls

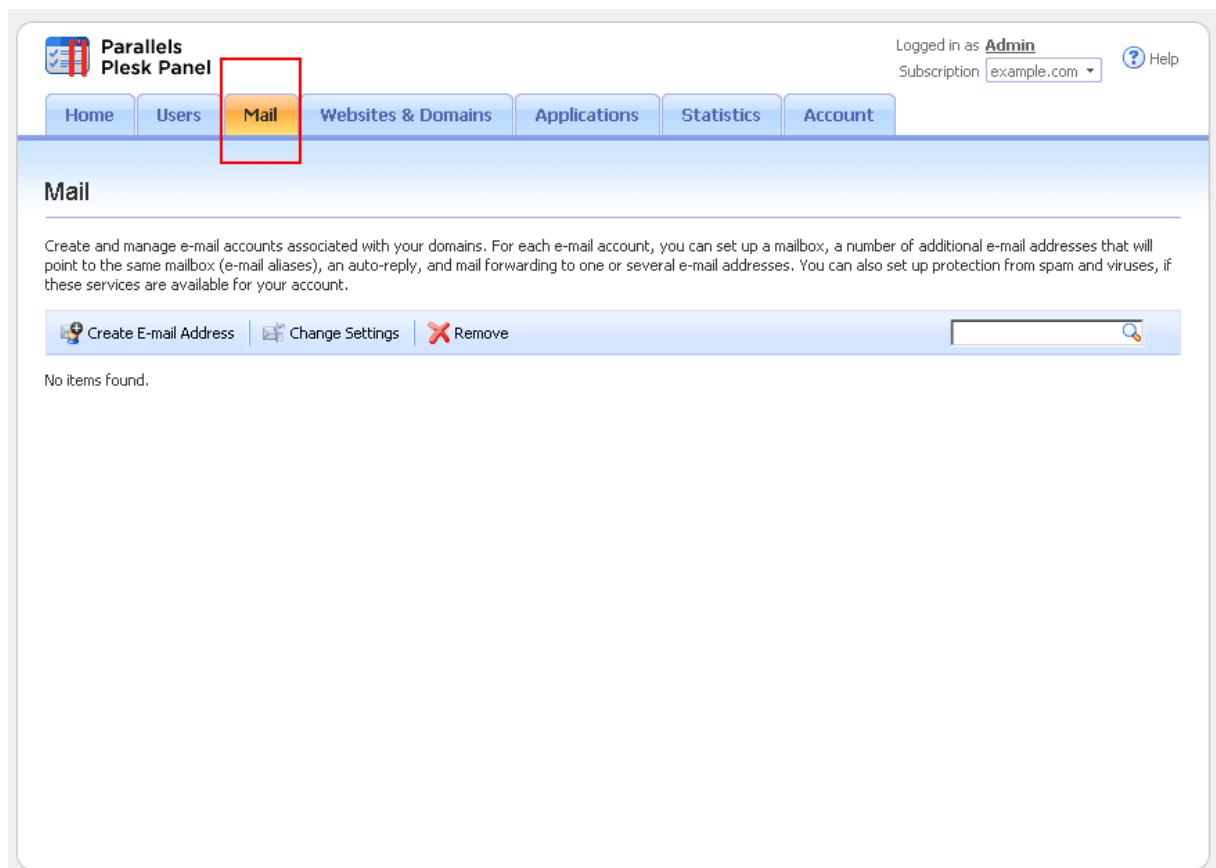
These are the controls that let hosting customers use the mail services integrated with Panel. If you want to use a mail server running on a separate machine, or want to prohibit Panel users from operating mail services, you can remove the corresponding controls from customer's interface. This option does not actually switch off the Panel-managed mail server.

Next in this section:

Location of the Mail Service Controls	169
Hiding the Mail Service Controls.....	172
Displaying the Mail Service Controls	172

Location of the Mail Service Controls

- Control Panel: **Mail** tab.



- Control Panel: Home tab > Mail group.

The screenshot displays the Parallels Plesk Panel interface. At the top, the header shows the Parallels Plesk Panel logo, the user 'Admin' logged in, and a subscription for 'example.com'. Below the header is a navigation bar with tabs: Home, Users, Mail, Websites & Domains, Applications, Statistics, and Account. The main content area is divided into several sections. The 'Mail' section, located in the bottom-left quadrant, is highlighted with a red rectangular box. It features an envelope icon and the title 'Mail'. The description reads: 'Create e-mail addresses and mailing lists. Set up mail forwarding, e-mail aliases, auto-replies, and protection from spam and viruses.' Below this are two links: 'E-mail Addresses' and 'Create E-mail Address'. Other sections visible include 'Statistics on Resource Usage' with disk and traffic usage bars, 'SiteBuilder', 'Websites & Domains', 'Applications' with a list of featured apps like WordPress, Joomla!, Drupal, and Magento, and 'Users'.

Parallels Plesk Panel

Logged in as **Admin**
Subscription: **example.com** [Help](#)

Home Users Mail Websites & Domains Applications Statistics Account

Statistics on Resource Usage
View detailed reports on disk space and traffic usage by services and by months.
Disk space: 0 B used of 10.0 GB
Traffic: 0 B/month used of 100 GB/month
[More >>](#)

SiteBuilder
Build instant websites from business and personal templates with intuitive SiteBuilder editor.
[Launch SiteBuilder](#)

Websites & Domains
Add domain names and set up websites. Manage website content and view statistics on how people visit your websites.
example.com
[Add Domain](#) [File Manager](#)
[Secure Your Site with SSL Certificate](#) [Statistics](#)
[More >>](#)

Mail
Create e-mail addresses and mailing lists. Set up mail forwarding, e-mail aliases, auto-replies, and protection from spam and viruses.
[E-mail Addresses](#) [Create E-mail Address](#)
[More >>](#)

Users
Create and manage user accounts and user roles. Assign installed applications to user roles.
[User Accounts](#) [Create User Account](#)
[User Roles](#) [Create User Role](#)
[More >>](#)

Applications
Install apps on your websites. Assign administrative privileges to selected users.
There are no installed applications.
[Install Applications](#)

Featured Applications
Try out these most recommended applications.

WordPress
WordPress is a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability.

Joomla!
Content management system and Web application framework.

Drupal
Open source content management system and blogging engine.

gallery
Gallery is a powerful photo gallery.

phpBB
phpBB is the most widely used open source bulletin board solution in the world.

PinnacleCart
Pinnacle Cart is a featured packed, PHP shopping cart and web site builder application.

TYPO3
Professional Web Content Management System.

Magento
Professional open-source eCommerce solution.

Interspire Knowledge Manager
Reduce customer support, share articles, news, and documents.

Interspire Email Marketer
The most powerful email marketing software you'll find anywhere.

[More >>](#)

- Control Panel: **Users** tab > *user name* > **Create an e-mail address under your account** option.

The screenshot shows the Parallels Plesk Panel Admin interface. At the top, there's a navigation bar with tabs: Home, Users, Mail, Websites & Domains, Applications, Statistics, and Account. The 'Users' tab is selected. Below the navigation bar, the 'Admin' section is active, with sub-tabs for General and Contact Details. The 'General Information' section is expanded, showing fields for Contact name (Admin), E-mail address, and User role (Administrator). The 'E-mail address' field has two radio button options: 'Create an e-mail address under your account' (selected) and 'Use an external e-mail address'. The selected option shows a text input for the username 'root' and a dropdown for the domain 'example.com'. The 'Use an external e-mail address' option shows a text input for the full email address 'root@localhost.localdomain'. Below this, the 'Panel Preferences' section is visible, with fields for Username (admin), Password, Confirm password, and Panel language (ENGLISH (United States)). There's also a checkbox for 'User is active' which is checked. At the bottom, there are 'OK' and 'Cancel' buttons. A red rectangle highlights the 'Create an e-mail address under your account' radio button and the associated input fields.

Parallels Plesk Panel

Logged in as **Admin**
Subscription: example.com

Home Users Mail Websites & Domains Applications Statistics Account

Admin Up Level

General Contact Details

General Information

Contact name: Admin

E-mail address *
☒ Create an e-mail address under your account
root @ example.com
☐ Use an external e-mail address
root@localhost.localdomain

User role: Administrator
User roles grant users administrative privileges and access to applications that you selected for the role.

Panel Preferences

Username: admin

Password: [] Very weak (?)

Confirm password: []

Panel language: ENGLISH (United States)

☒ User is active
Active users can access the Panel.

* Required fields

OK Cancel

Parallels © Copyright 1999-2010, Parallels. All rights reserved

Hiding the Mail Service Controls

You can hide the mail service controls using the Panel user interface or the command line.

➤ ***To hide mail service controls using the Panel interface:***

1. In the Server Administration Panel, go to **Tools & Settings > Mail Server Settings** (in the **Mail** group).
2. Clear the **Enable mail management functions in Panel** checkbox.
3. Click **OK**.

➤ ***To hide the mail service controls using the command line, run the following command:***

```
/usr/local/psa/bin/server_pref -u -disable-mail-ui true
```

Displaying the Mail Service Controls

You can display the mail service controls using the Panel user interface or the `server_pref` command line utility.

➤ ***To display the mail service controls using the Panel interface:***

1. In the Server Administration Panel, go to **Tools & Settings > Mail Server Settings** (in the **Mail** group).
2. Select the **Enable mail management functions in Panel** checkbox.
3. Click **OK**.

➤ ***To display the mail service controls using the command line, run the following command:***

```
/usr/local/psa/bin/server_pref -u -disable-mail-ui false
```

Links for Purchasing Panel License and Add-On Keys

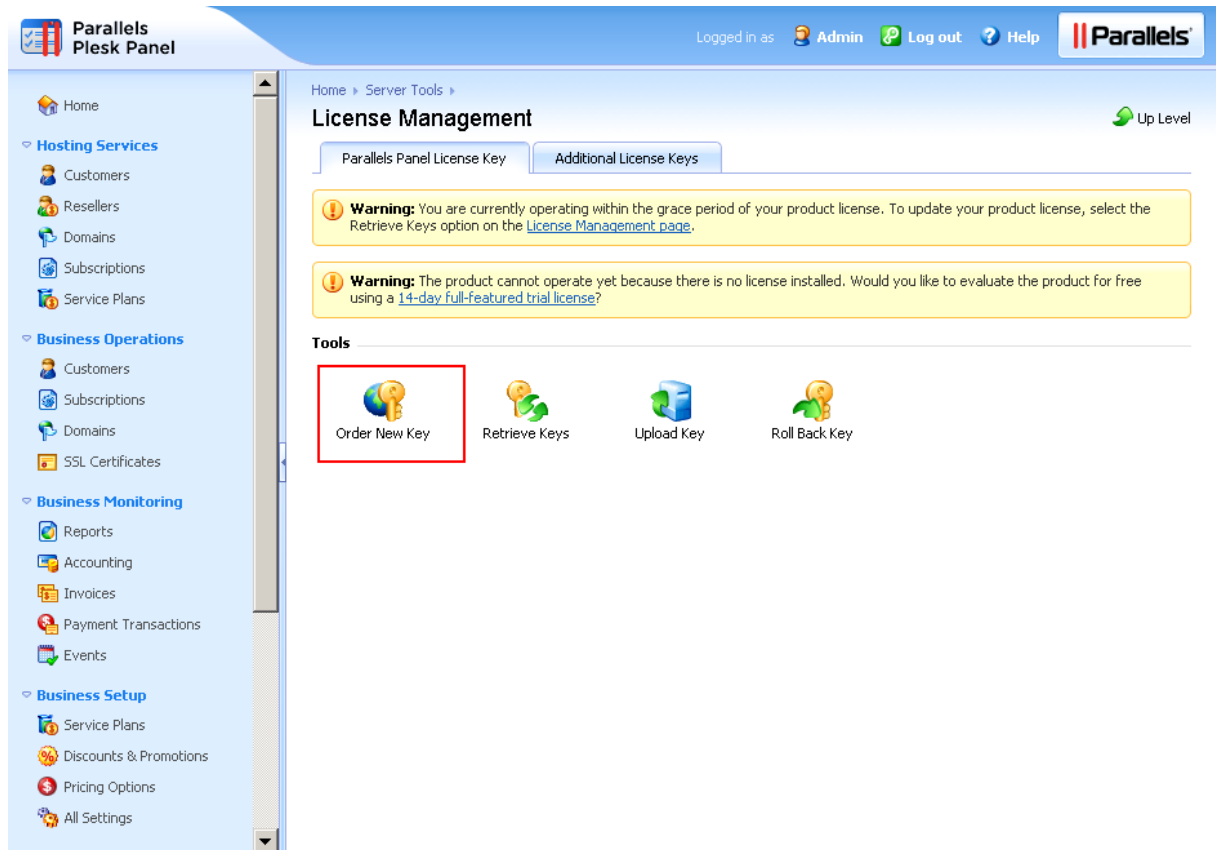
These buttons open the site where your customers can buy Panel license keys, add-ons and upgrades. By default, they lead to the Parallels website, but you can change them to point at a different website.

Next in this section:

Location of Links for Purchasing Panel License and Add-On Keys.....	173
Changing the Link URLs.....	175

Location of Links for Purchasing Panel License and Add-On Keys

- Server Administration Panel > Tools & Settings > License Management > Order New Key button.



- Server Administration Panel > Tools & Settings > License Management > Order Panel Add-Ons and Order Panel Upgrades buttons.

Parallels Plesk Panel

Logged in as Admin Log out Help

Home > Server Tools > License Management

Parallels Panel License Key Additional License Keys

Tools

Order Panel Add-Ons Order Panel Upgrades Retrieve Keys Upload Key Roll Back Key

Info

Key number	PLSK.10000000.0000
Next license key update	never
Key expiration date	Feb 15, 2011
User accounts (resellers and customers)	Unlimited
Domains	Unlimited
Domain aliases	Unlimited
Mail accounts	Unlimited
Web users	Unlimited
Language packs	Unlimited
Available languages	Any language
Links for purchasing SSL certificates and domain registration services	On
Interface management functions allow hiding controls for buying SSL certificates and domain names	On

Changing the Link URLs

You can change the links for purchasing Panel license and add-on keys only by editing the `panel.ini` configuration file.

➤ *To change the link URLs:*

1. Open the configuration file `panel.ini` from the `/usr/local/psa/admin/conf/` directory on the Panel-managed server. If the file does not exist, create it.

2. Place the following lines in the file and save it:

```
[marketplace]
panelAndAddonsLicensesStore = "http://my-store.tld"
```

If you want to remove these links from the Panel, leave the URL empty:

```
[marketplace]
panelAndAddonsLicensesStore = ""
```

To undo the change and return to the default values, remove these lines from `panel.ini`.

Promos

Promos are the promotion banners that are shown both in the Server Administration Panel and Control Panel. There are built-in Parallels promos of Parallels Customer and Business Manager (they are shown if Business Manager is not installed), Help Desk, and a number of other featured applications. You can create your own promos and insert them in Panel. All promos can be hidden.

Next in this section:

Location of Promos	175
Creating a Promo	176
Hiding Parallels Promos	177

Location of Promos

- Server Administration Panel: **Home**.
- Server Administration Panel: **Tools & Settings**.
- Server Administration Panel: **Tools & Settings > Mail Server Settings**.
- Control Panel in the Power User view: **Home**.

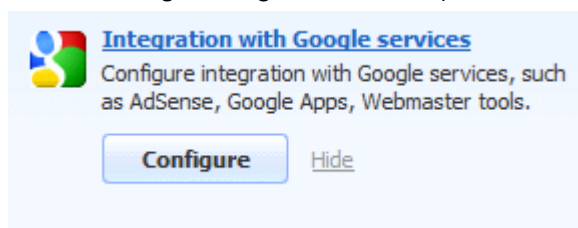
Creating a Promo

You can create your own promo by editing the `panel.ini` configuration file.

➤ *To create a promo:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel-managed server. If the file does not exist, create it.
2. Add the line `[promos]` to the file.
3. Specify the parameters of your promo by adding lines like "`<promo_name> . <parameter>=<value>`" after the line `[promos]`. You can use the following parameters:
 - **active.** Shows if your promo will appear by default or not. Boolean.
 - **icon.** URL of an icon that will be shown in the promo.
 - **title.** Title of the promo.
 - **text.** The promo description.
 - **buttonUrl.** The URL that opens upon clicking the promo button.
 - **buttonText.** The caption of the promo button.
 - **hideText.** Text of the link for hiding the promo.

For example, you want to create a promo that looks like the following (this is the Panel default Google Integration Promo):



You need to add the following lines to the `panel.ini`:

```
[promos]
custom.googleIntegration.active=true
custom.googleIntegration.icon=http://www.softicons.com/download/internet-
cons/webset-icons-by-graphicriver/png/48/google.png
custom.googleIntegration.title=integration with Google Services
custom.googleIntegration.text=Configure integration with Google Services,
such as AdSense, Google Apps, Webmaster tools.
custom.googleIntegration.buttonUrl=https://plesk.server:8443/plesk/server/g
oogle-tools/
custom.googleIntegration.buttonText=Configure
custom.googleIntegration.hideText=Hide
```

4. Save the file.

Hiding Parallels Promos

You can either hide promos at all or hide some specific promos, namely:

- Promos on the Server Administration Panel > **Tools & Settings** pages.
- A certain promo on the Home page of the Server Administration and Control Panels.

In all these cases, modify the `panel.ini` configuration file to get the desired result.

➤ *To hide all promos in Panel:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel-managed server. If the file does not exist, create it.
2. Place the following lines in the file and save it:

```
[promos]
enabled=off
[aps]
serverAppsPromoEnabled=off
```

➤ *To hide promos on the Server Administration Panel and Control Panel > Home pages:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel-managed server. If the file does not exist, create it.
2. Place the following lines in the file and save it:

```
[promos]
enabled=off
```

➤ *To hide Parallels promos on the Server Administration Panel > Tools & Settings and Tools & Settings > Mail Server Settings pages:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel-managed server. If the file does not exist, create it.
2. Place the following lines in the file and save it:

```
[aps]
serverAppsPromoEnabled=off
```

➤ *To hide a certain promo on the Server Administration Panel and Control Panel > Home pages:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel-managed server. If the file does not exist, create it.
2. Place the following lines in the file and save it:

```
[promos]
<promo_id>.active=false
```

The `<promo_id>` may be one of the following:

- `cbm` - for the Parallels Customer and Business Manager promo.
- `cloudFlare` - for the `mod_cloudflare` Apache module promo.
- `commTouch` - for the Parallels Premium Outbound Antispam promo.
- `googleIntegration` - for the Integration with Google Services promo.
- `helpDesk` - for the HelpDesk promo.
- `mobile` - for the Parallels Plesk Server Mobile Monitor and Parallels Plesk Server Mobile Manager promos.
- `sitebuilderTrial` - for the Presence Builder Try and Buy mode promo.

Otherwise, it can be your own promo name.

Link to Online Support Service

If you provide dedicated Panel-managed servers to your customers, you might want to configure the **Support** link in Panel to redirect server administrators to your website when they need assistance.

By default, the Support button (located in Server Administration Panel > **Tools & Settings**) opens the *Parallels Plesk Panel Online Server Support* form at the Parallels website, with a number of parameters automatically collected and filled in, such as the Panel administrator's name, company, e-mail, phone, product key number, operating system details, Panel version, and build number.

You can choose to:

- Configure the **Support** button in Server Administration Panel to open the support form page on your website with the above listed parameters pre-collected (see page 180).
- Configure the **Support** button in Server Administration Panel to open a user's mail client and prompt to compose a new message with your support e-mail address specified in the address line and the above listed parameters pre-collected (see page 181).

Next in this section:

Creating Link to Support Form on Your Site	180
Creating Link to Compose E-mail Message	181

Creating Link to Support Form on Your Site

The Parallels support form link is defined by the `support_url` parameter in the `psa.misc` table of the Panel's database. If the `support_url` parameter is absent or empty, upon clicking the **Tools & Settings > Support** button, the user is redirected to Parallels support through the following URL:

```
'https://register.parallels.com/support/form.php?sv=' .
urlencode(serialize($val))
```

where `$val` is an associative PHP array containing the following parameters:

- `firstName`, the Panel administrator's contact name.
- `company`, the Panel administrator's company name.
- `email`, the Panel administrator's e-mail address.
- `phone`, the Panel administrator's phone number.
- `keyNumber`, the Panel license key number used on the server.
- `operatingSystem`, the operating system installed on the server.
- `PSAVersion`, the version number of the Parallels Plesk Panel software.
- `PSABuild`, the build number of the Parallels Plesk Panel software.
- `PSAInstType`, the type of Parallels Plesk Panel software installation.

Before changing the link, consider the following to ensure that the support page of your site is configured properly:

- Your support page will accept the `sv` variable through the `GET` method. The value of this variable is a serialized associative array of pre-collected parameters.
- You can get the array of parameters on your web site page in the following way:

```
$params = unserialize($_GET['sv']);
```

- You can address any parameter of this array in the following way:

```
$params['firstName']
$params['company']
...
```

To make the **Support** button open the support form on your website, follow these steps:

1. Connect to the Panel's database (`psa`).
2. Run the following query:

- If the `support_url` parameter is absent, run:

```
insert into misc(param, val) values('support_url',
'https://example.com/support')
```

Where `'https://example.com/support'` is the URL of the support page on your website.

- If the `support_url` parameter already exists, run:

```
update misc set val = 'https://example.com/support' where param =
'support_url'
```

Where `'https://example.com/support'` is the URL of the support page on your website.

Note: On Windows systems, you can use the `dbclient.exe` utility to add the information to the Panel's database. For information about using the `dbclient.exe` utility, consult **Parallels Plesk Panel for Microsoft Windows: Reference for Command Line Utilities** at <http://download1.parallels.com/Plesk/PP11/11.5/Doc/en-US/online/plesk-win-cli/44693.htm>.

Creating Link to Compose E-mail Message

You can modify the link to Parallels support, so that after clicking the **Tools & Utilities > Support** button in Server Administration Panel, your customers are offered to compose an e-mail with your support address already specified in the address line. The customer's contact details and server information will be automatically collected and included in the message body.

You can customize the link to Parallels support by specifying your e-mail address in the `support_url` parameter of the `psa.misc` table of the Panel's database.

To make the Support button of the Server Administration Panel open the page for composing e-mail with your support e-mail address, follow these steps:

1. Connect to the Panel's database (psa).
2. Run the following query:

- If the `support_url` parameter is absent, run:

```
insert into misc(param, val) values('support_url',
'mailto:yoursupport@example.com')
```

Where 'yoursupport@example.com' is the e-mail address where you want your customers' support requests to be sent.

- If the `support_url` parameter already exists, run:

```
update misc set val = 'mailto:yoursupport@example.com' where param =
'support_url'
```

Where 'yoursupport@example.com' is the e-mail address where you want your customers' support requests to be sent.

Note: On Windows systems, you can use the `dbclient.exe` utility to add the information to the Panel's database. For information about using the `dbclient.exe` utility, consult **Parallels Plesk Panel for Microsoft Windows: Reference for Command Line Utilities** at <http://download1.parallels.com/Plesk/PP11/11.5/Doc/en-US/online/plesk-win-cli/44693.htm>.

The Facebook Like Button

The *Like* button allows administrators to share the link to the Parallels Panel page on Facebook with their Facebook friends. When the administrator clicks the Like button in Panel, a story appears in the user's friends' News Feed with a link back to page. You can hide this button. Customers and resellers do not see this button.

Next in this section:

Location of the Like Button	182
Hiding the Like Button	183

Location of the Like Button

The button is located in the following places of the Panel web interface:

1. The Server Administration Panel, in the bottom-left corner of the left navigation pane.



2. The Control Panel, in the page footer.



Hiding the Like Button

You can hide the Facebook Like button only by editing the `panel.ini` configuration file.

➤ *To hide the Like button:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini`. If the file does not exist, create it.
2. Place the following lines in the file and save it:

```
[facebook]
showLikeLink = false
```

To undo the change and return to the default values, remove these lines from `panel.ini`.

Product Rating Widget

The product rating widget allows administrators to provide feedback on their Panel user experience. A form which gives the opportunity to rate the product and send comments appears after one month of using Panel. If the administrator chooses to provide feedback later, Panel adds the **Provide Feedback** button to the navigation pane of the Server Administration Panel and to the bottom of the Control Panel in Power User view.

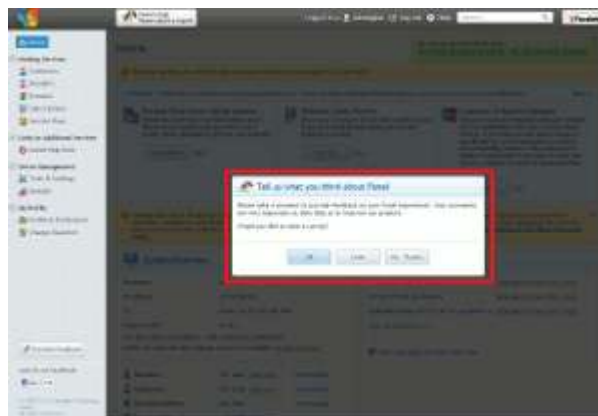
You can hide the product rating widget so that customers and resellers do not see it.

Next in this section:

Location of the Widget.....	183
Hiding the Widget.....	184

Location of the Widget

The widget appears right in front of the Panel GUI, once the administrator logs in to Panel.



Hiding the Widget

You can hide the product rating widget only by editing the `panel.ini` configuration file.

➤ ***To hide the product rating widget:***

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini`. If the file does not exist, create it.
2. Place the following lines in the file and save it:

```
[rating]
enabled=false
```

If you do not want to hide the form but only want to change the period of time after which the form is shown to the administrator, add the following lines to the file:

```
[rating]
enabled=true
showAfterDays=60
```

The `showAfterDays` parameter sets the number of days after which you want the widget to be displayed.

To undo the change and return to the default values, remove these lines from `panel.ini`.

RSS Feeds

Panel gives you an ability to provide latest news to your customers by showing them RSS feeds in the Control Panel. Currently, you can embed a single RSS feed from any source.

Next in this section:

Location of RSS Feeds.....	185
Adding RSS Feeds.....	186
Hiding RSS Feeds.....	186

Location of RSS Feeds

RSS feeds are shown on the **Websites & Domains** tab of the Control Panel.

The screenshot displays the Parallels Panel interface. The top navigation bar includes the Parallels logo, user information (Logged in as John Doe), a search bar, and the Parallels logo. Below the navigation bar, the 'Websites & Domains' tab is selected. The main content area is titled 'Websites & Domains' and contains a description: 'This is where you set up and manage websites. If you have several subscriptions associated with your account, then you can switch from one subscription to another by selecting the required subscription at the top of the screen.' Below this, there are several links: 'Web Hosting Access', 'FTP Access', 'Backup Manager', 'Databases', and 'Scheduled Tasks'. A section titled 'testdomain.tld' shows the website's IP address (10.52.68.141) and system user (jdoe). Below this, there are three options for creating a website: 'Parallels Presence Builder', 'Applications', and 'Custom Website'. On the right side, there is a sidebar with sections: 'Resource Usage', 'Featured Applications', 'Domains', and 'News'. The 'News' section is highlighted with a red box and contains several news items, including 'THW Advanced Web Announces Website Hosting Service Tuned For WordPress', 'Certified Hosting Now Accepts Bitcoin Payments', and 'Ex-HostGator Employee Charged with Installing Backdoor to Access 2,700 Servers'.

Adding RSS Feeds

➤ *To add an RSS feed:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel server. If the file does not exist, create it.
2. Add the line `[customSpots]` to the file.
3. Specify the parameters of your promo by adding the following lines:

```
web.enabled = true
web.type = rss
web.params.url = <rss_url>
web.params.count = <pages_number>
```

Where `<rss_url>` is the address of the RSS feed and `<pages_number>` is the number of news pages shown in Panel.

4. Save the file.

For example, to show three pages of news from about Parallels Plesk Panel, you should add the following text to the `panel.ini`:

```
[customSpots]
web.enabled = true
web.type = rss
web.params.url = http://www.parallels.com/products/plesk/rss
web.params.count = 3
```

Hiding RSS Feeds

➤ *To hide an RSS feed:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel server.
2. Locate the `[customSpots]` section that describes the feed you want to hide.
3. Change the value of the `web.enabled` parameter in this section to `false`.
4. Save the file.

For example, the description of an RSS feed that is not shown in Panel may look like the following:

```
[customSpots]
web.enabled = false
web.type = rss
web.params.url = http://www.parallels.com/products/plesk/rss
web.params.count = 3
```

Voting for New Features

Panel provides its users with an option to suggest new features for further Panel versions and vote for ideas suggested by other people on the uservoice.com online service. To open the page where you can vote for new features and suggest new ones, click the button **Suggest an Idea** in the Server Administration Panel of the Control Panel.

If you do not want to use this option, you can hide the button **Suggest an Idea**. Alternatively, you can change this button's URL so that it points to any other site you want.

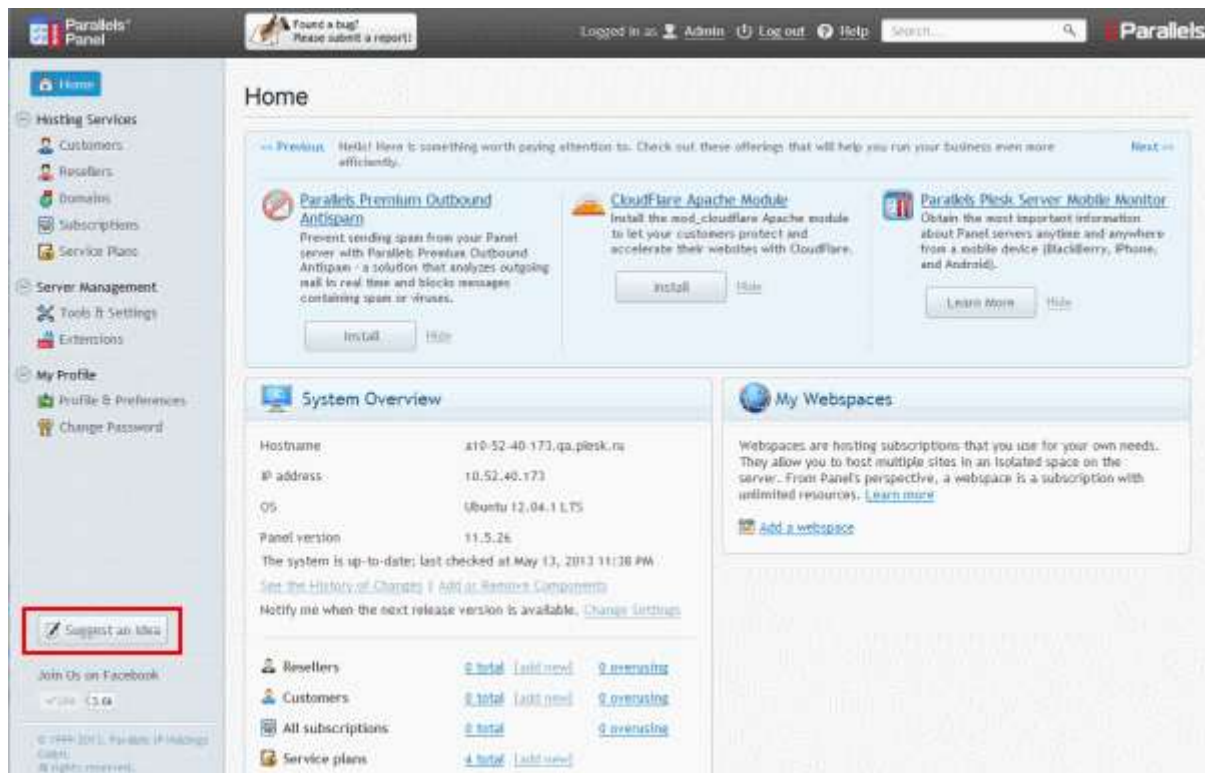
Next in this section:

Location of the Button Suggest an Idea	187
Hiding the Button Suggest an Idea	188
Changing the URL of the Button Suggest an Idea	189

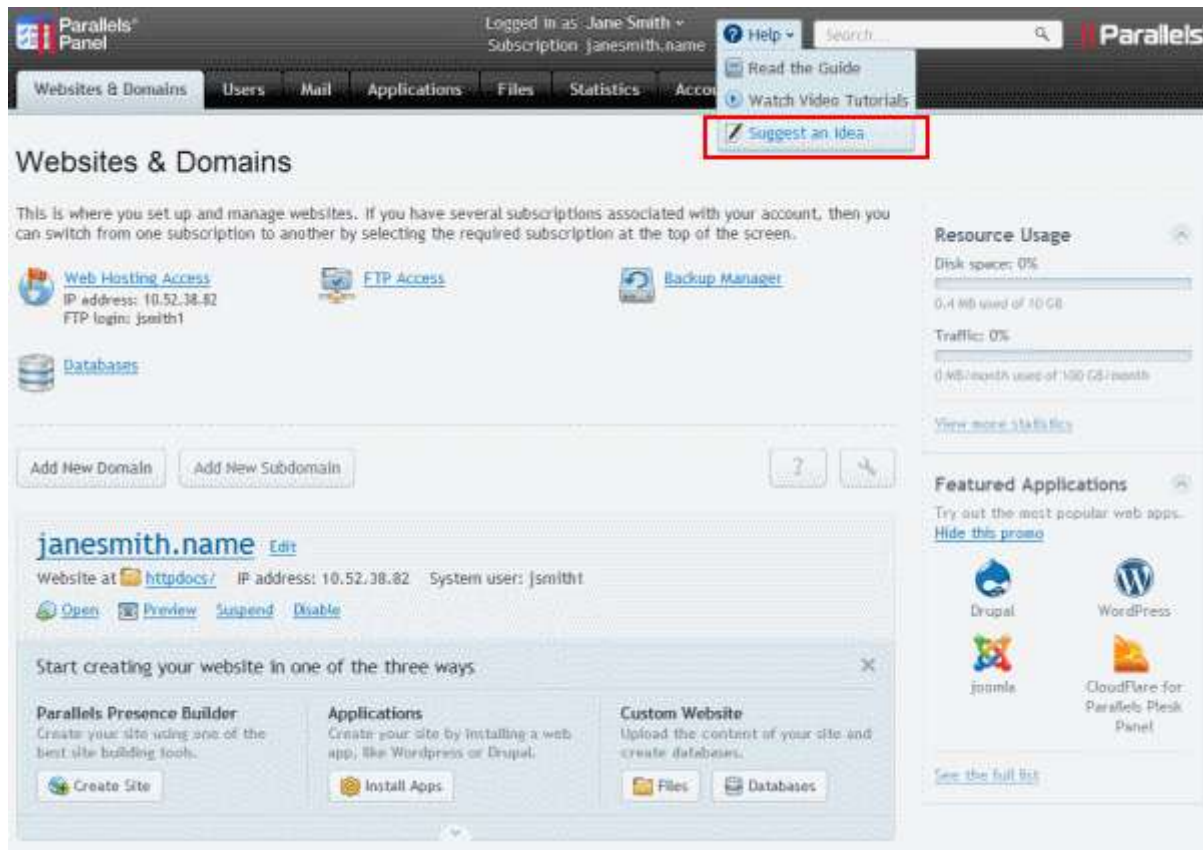
Location of the Button Suggest an Idea

The button **Suggest an Idea** is available at the following locations:

- Navigation pane of the Server Administration Panel.



- Help menu of the Control Panel.



Hiding the Button Suggest an Idea

➤ To hide the button Suggest an Idea:

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel server. If the file does not exist, create it.
2. Add the following lines to the file:

```
[feedback]
userVoice = off
```

3. Save the file.

Changing the URL of the Button Suggest an Idea

➤ *To change the URL to which the button Suggest an Idea points:*

1. Open the configuration file `/usr/local/psa/admin/conf/panel.ini` on the Panel server. If the file does not exist, create it.
2. Add the following lines to the file:

```
[feedback]
userVoiceUrl = "<your_URL>"
```

Where **<your_URL>** is the URL of an alternative features voting service.

3. Save the file.

CHAPTER 9

Rebranding Presence Builder

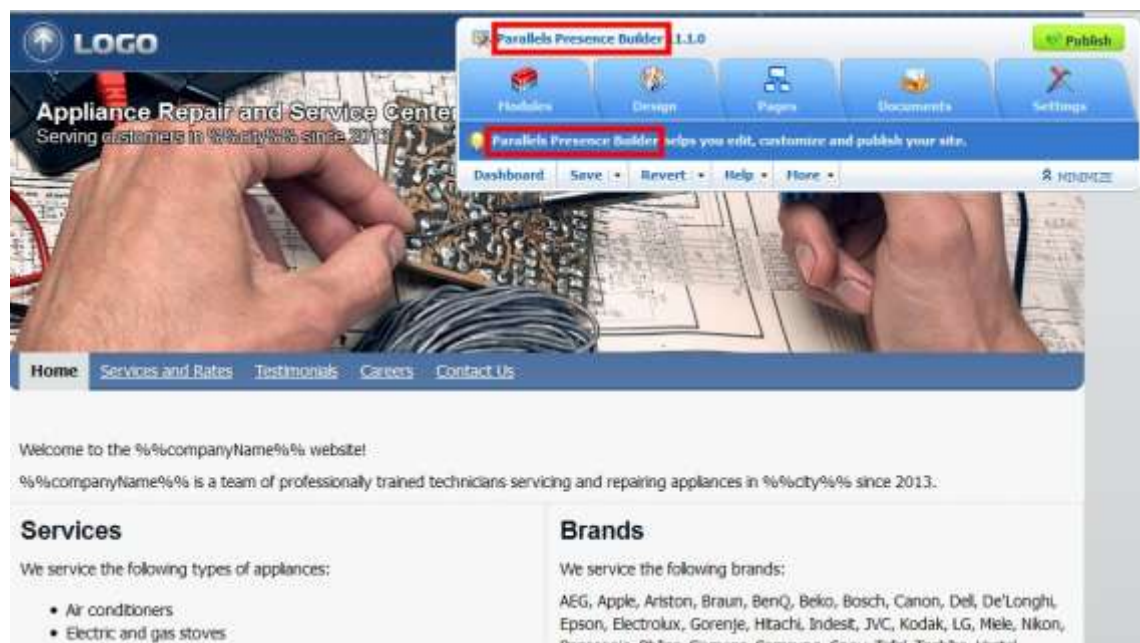
This chapter describes how to rebrand Presence Builder to show your custom product name, product and company logo images; to take users to a branded website with user's documentation; and to show a customized **Getting Started** video tutorial.

It also describes how to embed your own **Getting Started** video in languages other than English. You might want to prepare custom localized videos if most of your customers speak other languages.

Where to Find These Items in the Product?

The Product Name

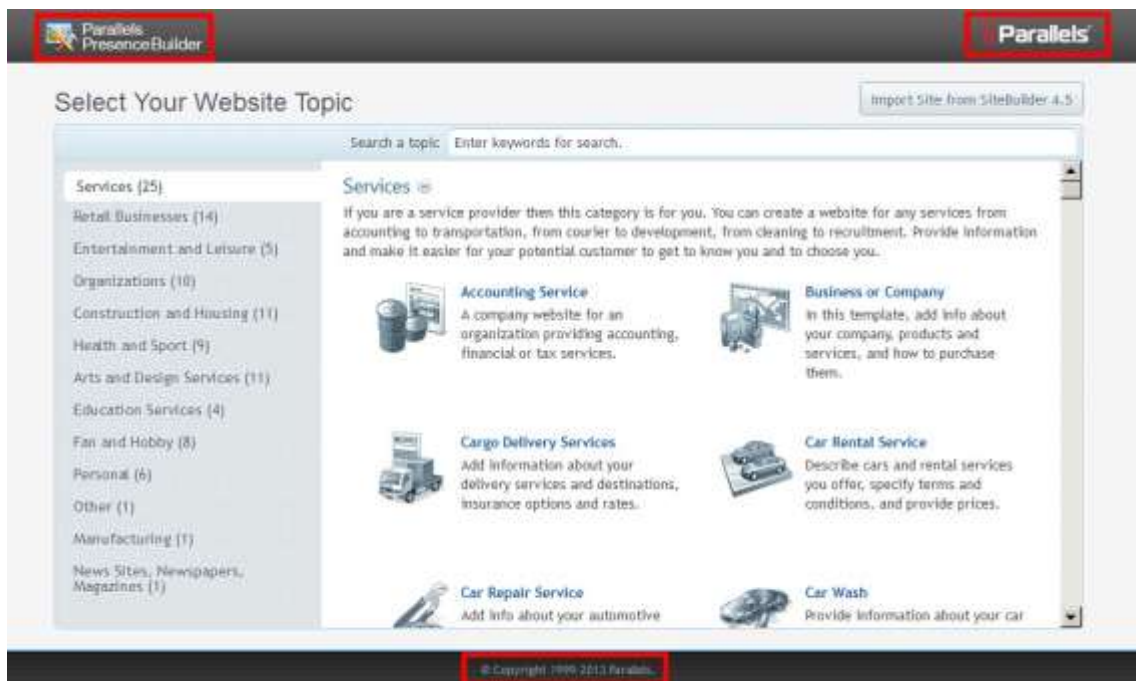
The product name is shown in the editor's toolbar and in various information and error messages. Note that the product version cannot be changed.



To learn how to change the product name, see the section Changing the Editor's Name (on page 193).

The Product and Company Logo Images, and the Copyright Notice

The Presence Builder logo, the company logo (that of Parallels), and the copyright notice are shown only on the topic selection page. This is the first page that users see when they visit the editor.



The product logo, the company logo, and the copyright notice have hyperlinks attached to them. The product logo refers to <http://www.parallels.com/products/web-presence-builder>, the company logo and the copyright notice refer to the Parallels site at <http://www.parallels.com>.

To learn how to change these logos, hyperlinks, and the copyright notice, see the section Changing the Product and Company Logos, Hyperlinks, and Copyright Notice (on page 194).

Links to the User's Guide and Getting Started Video

The links to the User's Guide and the Getting Started video are accessible from the Presence Builder toolbar > **Help** menu. Users are also advised to watch the Getting Started video when they visit the editor for the first time.



The User's Guide is hosted on the Parallels site, and the Getting Started video is hosted on the Parallels YouTube channel.

To learn how to change or remove these links, refer to the corresponding sections of this document:

- Changing the Links to the User's Guide. (on page 196)
- Changing the Links to the Getting Started Video. (on page 198)

In this chapter:

Changing the Editor's Name	193
Changing the Product and Company Logos, Hyperlinks, and Copyright Notice ..	194
Changing the Link to the User's Guide	196
Changing the Links to the Getting Started Video.....	198

Changing the Editor's Name

➤ *To change the editor's name **Parallels Presence Builder** to a custom name:*

1. On the Panel-managed server, open the configuration file
`/usr/local/sb/config`.
2. In the `[general]` section of the file, locate the following line:
`product = "Parallels Presence Builder"`
3. Type the desired product name instead of **Parallels Presence Builder**, and save the file.

Changing the Product and Company Logos, Hyperlinks, and Copyright Notice

➤ ***To replace the product logo:***

1. Prepare an image file in PNG format and save it as `product-logo.png`.
The image should be 50 pixels in height to perfectly fit in the header area.
2. Upload the file to the directory `/usr/local/sb/htdocs/skins/default/images/` on the hosting server. Confirm overwriting when prompted.

➤ ***To replace the company logo:***

1. Prepare an image file in PNG format and save it as `producer-logo.png`.
The image should be 43 pixels in height to perfectly fit in the header area.
2. Upload the file to the directory `/usr/local/sb/htdocs/skins/default/images/` on the hosting server. Confirm overwriting when prompted.

➤ ***To change the links attached to the product and company logos:***

1. On the hosting server, open the configuration file `/usr/local/sb/config`.
2. In the `[general]` section of the file, locate the following lines:

```
product_website_url = "http://www.parallels.com/products/web-presence-builder"
company_website_url = "http://www.parallels.com"
```
3. Type the desired addresses within the quotation marks and save the file.

➤ ***To change the company name shown in the copyright notice:***

1. On the hosting server, open the file `/usr/local/sb/resources/locale/<locale_code>/Common.lng`.
2. Locate the following line:

```
copyright = "© Copyright 1999-%s Parallels."
```
3. Type the desired text within the quotation marks and save the file.

Note that a hyperlink to www.parallels.com is automatically added to the copyright notice. If you have previously specified a website address by adding the line `company_website_url = "your-company-name.com"` to the configuration file `/usr/local/sb/config` (as described in the preceding procedure), this hyperlink will point to that address.

Changing the Link to the User's Guide

➤ **To change the link to the User's Guide:**

1. On the hosting server, open the configuration file `/usr/local/sb/config`.
2. Add the line `[help]` to the file. If it is already present, skip this step.
3. Add the following line after the line `[help]`:

```
help_url = <link_to_your_documentation>
```

For example: `http://example.com/user-guide/index.html?%%CONTEXT%%`

At the end of this link, the mechanism providing context-sensitive help will automatically add a GUI screen identifier, so the resulting URL will appear as:
`http://example.com/user-guide/index.html?%2FSiteBuilder%2FPanel.`

The value that you specify as `help_url` may contain the following placeholders:

- `%%LOCALE%%` - 4-letter code of the locale currently set in the editor, for example, *en-US* or *ru-RU*. The following locales are supported:
 - `en_US` - American English.
 - `en_GB` - British English.
 - `de_DE` - German.
 - `es_ES` - Spanish.
 - `fr_FR` - French
 - `it_IT` - Italian.
 - `ja_JP` - Japanese.
 - `nl_NL` - Dutch.
 - `pl_PL` - Polish.
 - `pt_BR` - Brazilian Portuguese
 - `ru_RU` - Russian.
 - `zh_CN` - simplified Chinese.
 - `zh_TW` - traditional Chinese.
- `%%VERSION%%` - full Presence Builder version, for example, *11.1.0*.
- `%%MAJOR_VERSION%%` - major Presence Builder version (first two numbers), for example, *"11.1"*.
- `%%CONTEXT%%` - GUI screen identifier.

For example: If a user views the Presence Builder 11 editor in English, and clicks the **Help** link on the first page of the editor (which opens after clicking the **Create Site** button), the link `http://example.com/%%MAJOR_VERSION%%/%%VERSION%%/%%LOCALE%%/user-guide/index.html?%%CONTEXT%%` will be replaced with `http://example.com/11.0/11.1.0/en-US/user-guide/index.html?%2FSiteBuilder%2FPanel.`

4. Save the file.

Changing the Links to the Getting Started Video

➤ ***To change the link to the Getting Started video:***

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.

2. In the `[help]` section, add the following lines:

```
getting_started_video_url = <video_link>
getting_started_video_enabled = true
```

3. Save the file.

➤ ***To use a custom Getting Started video for a specific language:***

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.

2. Add the following line below `getting_started_video_url`:

```
getting_started_video_url_locale_<locale-name> = <localized_video_link>
```

Where **<locale-name>** is the four-letter code of the Presence Builder locale (for example, `en_US` or `ru_RU`) in which the video will show. The following locales are supported:

- `en_US` - American English.
- `en_GB` - British English.
- `de_DE` - German.
- `es_ES` - Spanish.
- `fr_FR` - French
- `it_IT` - Italian.
- `ja_JP` - Japanese.
- `nl_NL` - Dutch.
- `pl_PL` - Polish.
- `pt_BR` - Brazilian Portuguese
- `ru_RU` - Russian.
- `zh_CN` - simplified Chinese.
- `zh_TW` - traditional Chinese.

3. Ensure that the file contains the following line:

```
getting_started_video_enabled = true
```

4. Save the file.

➤ ***To remove the link to the Getting Started video:***

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.
2. Add the line `[help]` to the file. If it is already present, skip this step.
3. Add the following line after the line `[help]`:
`getting_started_video_enabled = false`
If the file contains the line `getting_started_video_enabled = true`, just change `true` to `false`.
4. Save the file.

CHAPTER 10

Customizing the Functionality of Presence Builder

This chapter describes how to change the behavior of certain user interface elements and how to make certain functions of the Presence Builder editor unavailable to customers. In particular, it explains how to perform the following tasks:

- Prohibit your customers from removing their sites from the editor. You can do this by removing the **Remove Site** button.
- Make the following modules unavailable in the editor: Embedded Video, Image Gallery, Image Slider, Blog, Online Store, Shopping Cart, Map, Commenting, Contact Form, Social Sharing, Advertisement, Search, Navigation, Breadcrumbs, Banner, Site Logo, and Script.
- Remove the option for images stored externally at Google Picasa to be used in image galleries.
- Make the functionality for importing sites from SiteBuilder 4.5 unavailable.
- Expand the library of website banner images that are available to customers.
- Expand the library of design templates that are available to customers.
- Enable your customers to request technical assistance. This can be done by adding a special button to the editor.
- Enable your customers to submit feedback. This can be done by adding a special button to the editor.
- Remove the option to publish a copy of a website on Facebook.
- Configure the editor to remove published sites from hosting accounts when users click the **Remove Site** button in the editor.

Next in this section:

Prohibiting Users from Removing Their Sites.....	202
Making Modules Unavailable in the Editor	202
Making the Google Picasa Storage Unavailable for Use in Image Galleries.....	203
Making the Site Import Functionality Unavailable	204
Adding Custom Banner Images	205
Adding Custom Design Templates.....	207
Adding the Support Button	209
Adding the Link for Sending Feedback.....	210
Removing the Option to Add a Site Copy to Facebook	211
Removing Sites from Hosting Accounts	211

Prohibiting Users from Removing Their Sites

The following procedure describes how to prevent your customers from deleting their sites from the editor. You can do this by removing the **Remove Site** button.

➤ ***To remove the button from the editor:***

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.
2. In the `[general]` section of the file, locate the following line:
`allow_delete_site_ui = true`
3. Replace the `true` value with `false`.
4. Save the file.

Making Modules Unavailable in the Editor

If you want to prevent your customers from using certain modules in the editor, you can make them unavailable. Unavailable modules are not visible in the editor, and therefore are not accessible to customers.

During restoration of a website from a snapshot, the modules that you make unavailable, and their content, are not restored. The user is notified that the snapshot contains unavailable or unsupported functionality, and is prompted to choose whether to restore the rest of the site, or cancel restoration.

When a new website based on a website topic is opened in the editor, the modules that are unavailable are not added to the site.

➤ ***To remove modules from the editor:***

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.
2. In the `[general]` section of the file, add the following line:
`hidden_widgets = <module's code name 1>, <module's code name 2>`
Where `<module's code name 1>` and `<module's code name 2>` are code names of the modules, separated by a comma.
3. Save the file.

The following is a list of codes for all modules in Presence Builder 11.

Module's name in the editor	Module's code name
Embedded Video	video
Image Gallery	imagegallery
Image Slider	slider
Blog	blog
Online Store and Shopping Cart	eshop
Commenting	commenting
Contact Form	contact
Social Sharing	sharethis
Advertisement	advertisement
Map	map
Search	search
Navigation	navigation
Breadcrumbs	breadcrumbs
Site Logo	siteLogo
Script	script

Making the Google Picasa Storage Unavailable for Use in Image Galleries

If you do not want your customers to use images stored at Google Picasa in their image galleries, remove the corresponding option from the Image Gallery module. To do this:

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.
2. In the `[general]` section of the file, add the following line:
`picasa_enabled = false`
3. Save the file.

Making the Site Import Functionality Unavailable

If you want to prevent your customers from importing sites from SiteBuilder 4.5 hosting accounts, you can remove the **Import Site from SiteBuilder 4.5** button from the editor. This can be done by adding a line to the configuration file `/usr/local/sb/config`.

➤ ***To make the site import functionality unavailable to users:***

1. On the hosting server, open the configuration file `/usr/local/sb/config`.
2. In the `[general]` section of the file, add the following line:
`show_import_site_button = 0`
3. Save the file.

Adding Custom Banner Images

This section explains how to add custom banner images to Presence Builder's image library, and make them available for selection in the editor.

Suppose, you have an image file with the name `jungle.jpg`, and you want to add it to the editor. Do the following:

1. Resize the image to 960 pixels in width and 250 pixels in height. Convert the image to PNG format, and save it as `header.png`.
2. Create a copy of `header.png`, resize it to 200 pixels in width, and 57 pixels in height. Save it as `preview.png`.
3. Connect over SSH to the hosting server.
4. Locate the directory `/sb/htdocs/headers/`, and create a subdirectory with the banner name. For example, `/sb/htdocs/headers/jungle_01`.
5. Upload the `header.png` and `preview.png` files that you prepared to the directory `/sb/htdocs/headers/jungle_01/`.
6. Locate the directory `/sb/resources/`. It should contain the file `customHeaders.xml`.

If the file is missing, create it and insert the following lines into it:

```
<?xml version="1.0" encoding="utf-8"?>
<headers>
  <header id="jungle_01">

  </header>
</headers>
```

If the file is present, add the following `<header>` node to it:

```
<header id="jungle_01">
</header>
```

7. Add keywords for the image.

Keywords are used for the following purposes:

- **Binding of images to website topics.** When a new site is created based on a website topic, the editor searches for banner images that may be relevant to the topic, and adds one of them to the generated website. It also uses the relevant banners in generated design templates, which users can preview and select in the editor > **Design** tab > **Templates**. The relevance is determined by matching keywords in the website topic's meta data and in the `headers.lng` file containing descriptions of all banner images in the form of keywords.
- **Enabling users to find images by keywords in the banner selection menu.**

To add keywords, do the following:

- a. Open for editing the file
`/sb/resources/locale/<locale_code>/headers.lng.`

- b. Add a string in the following format:

```
<header_id> = "<keyword_1>,<keyword_2>,<keyword_3>"
```

Where:

- `<header_id>` is the image ID that you specified in step 6, but with certain transformations: all uppercase letters must be changed to lower case, hyphens must be removed, the next symbol following a hyphen must be changed to upper case.

For example:

If the `<header_id>` is `Jungle_01-eXample`, then it must be changed to `jungle_01Example`.

If the `<header_id>` is `my-super-banner`, then it should be transformed to `mySuperBanner`.

If the `<header_id>` is `my_super_banner`, then it should be transformed to `my_super_banner`.

- `<keyword>` is a human-readable word that describes the image or identifies items on the picture.

You can use several keywords separated by commas. White spaces can be used only if they are part of a descriptive phrase or a combination of words.

Example:

```
jungle01 = "jungle,tropics,green,nature,family travel"
```

- c. Save the file.

8. Issue the following command:

```
/usr/local/psa/bin/sw-engine-pleskrun  
/usr/local/sb/utils/updateResources.php header
```

Now you can go to the editor and open the list of banner images. The newly added image should be at the end of the list.

Adding Custom Design Templates

This section explains how you can prepare your own design templates and make them available to your customers.

A design template is a combination of website elements (banner, footer, sidebars, site-wide modules), page layout settings, and colors, which are applied to a site when it is created in the editor.

The editor provides a selection of 24 design templates, 16 of which are randomly generated, and 8, created by a graphic designer especially for Presence Builder.

Users can view the design templates and apply them to their sites in the editor, on the **Design** tab > **Templates**. Randomly generated designs are listed in the **Generated** section, and the templates prepared by the designer, in the **Special** section.

Preparing a Custom Design Template

The following site elements and settings can be saved in a design template:

- The website layout: the location and size of the header, footer, content areas, and sidebars.
- The banner image.
- All site-wide modules.
- The color scheme or individually selected colors.
- The fonts.
- The information about the borders and shapes of the page elements' corners.

➤ *To create a custom design template and add it to Presence Builder editor:*

1. Log in to the editor and start creating a site.
2. Adjust the layout and design.

If you need instructions on how to do this, refer to **Presence Builder User's Guide**, sections **Changing Your Website Layout** and **Selecting Website Colors, Fonts, and Styles for Borders and Corners**.

3. Add the necessary site-wide modules and a banner.

If you need instructions on how to do this, refer to **Presence Builder User's Guide**, the chapter **Content: Text, Tables, Images, Video, Forms, and Scripts**, and the section **Changing the Website Header Elements**.

4. Save the design template: Go to the **Design** tab, and click **Export Design**.

5. On the Presence Builder server, create a directory in

`/usr/local/sb/htdocs/templates/generic/presets/`.

The directory name should correspond to the desired name of the new template. For example:

`/usr/local/sb/htdocs/templates/generic/presets/my_mega_design.`

6. Extract the contents of the ZIP archive with the template into the directory you have just created.
7. Prepare a thumbnail that will be shown in the editor: Make a screen capture of your design in the editor, resize the picture to 213 pixels in width and 151 pixel in height, and save it as `screenshot.png`.
8. Upload the file `screenshot.png` to the directory
`/usr/local/sb/htdocs/templates/generic/presets/<your_template_name>`.

The template will show in **Design** tab > **Templates** > **Special** section.

To delete a custom design template, delete the directory
`/usr/local/sb/htdocs/templates/generic/presets/<your_template_name>` from the server.

Adding the Support Button

To enable your customers to submit technical support requests from the Presence Builder editor, you can add to the editor a button with the label **Support**. The button will be placed in the editor's toolbar, in the **Help** menu.

➤ *To add the button:*

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.
2. In the `[help]` section of the file, add the following line:

```
support_url = <URL>
```

Where `<URL>` is the address of your online support help desk or a support forum.
For example: `http://helpdesk.example.com`.

The value that you specify as `support_url` may contain the following placeholders:

- `%%LOCALE%%` - 4-letter code of the locale currently set in the editor, for example, *en-US* or *ru-RU*.
- `%%VERSION%%` - full Presence Builder version, for example, *11.1.0*.
- `%%SITE_UUID%%` - website ID.

For example:

If a user views the Presence Builder 11.1 editor in English, and clicks the **Support** link, the link

`http://helpdesk.example.com/index.php?locale=%%LOCALE%%&version=%%VERSION%%&siteid=%%SITE_UUID%%` will be transformed to
`http://helpdesk.example.com/index.php?locale=en-US&version=11.1.0&siteid=93ea19b0-7537-fb22-d603-685e29cfd3e8`.

3. Save the file.

Adding the Link for Sending Feedback

If you want to enable customers to send you feedback, you can do the following:

1. Set up a forum on your site.
2. Configure the editor to show a link with the label **Give Feedback**, which will direct users to that forum.

The link will be placed in the editor's toolbar, in the **Help** menu.

➤ *To add the link:*

1. On the hosting server, open the configuration file `/usr/local/sb/config`.
2. In the `[help]` section, locate the line containing `feedback_url`. If this line is not present, add the following line:

```
feedback_url = "<URL to your online forum>"
```

where "<URL to your online forum>" is your forum's address enclosed in quotation marks.

3. Save the file.

➤ *To remove the link:*

1. On the hosting server, open the configuration file `/usr/local/sb/config`.
2. In the `[help]` section, locate the line containing `feedback_url`, and remove the address enclosed in quotation marks. If this line is not present, add the following line:

```
feedback_url = ""
```

3. Save the file.

Removing the Option to Add a Site Copy to Facebook

If you want to prevent your customers from publishing website copies on Facebook, you can remove the corresponding option from the editor. This can be done by adding a line to the configuration file.

➤ *To make the functionality for publishing sites on Facebook unavailable to users:*

1. On the hosting server, open the configuration file
`/usr/local/sb/config`.
2. In the `[general]` section of the file, add the following line:
`facebook_application_url = ""`
3. Save the file.

Removing Sites from Hosting Accounts

When users remove a site from the Presence Builder editor, only the current site draft opened in the editor and saved site snapshots are removed. By default, published sites are not removed from hosting accounts.

If you want to save disk space, we recommend that you configure the editor to remove sites from hosting accounts when their owners click the **Remove Site** button.

To do this:

1. On the Presence Builder server, open the configuration file
`/usr/local/sb/config`.
2. In the `[general]` section of the file, locate the following line:
`delete_published_site_files = false`
3. Change `false` to `true`.
4. Save the file.

Customizing Website Topics in Presence Builder

Presence Builder comes with a set of website topics. A topic is a site template containing several webpages prefilled with relevant text, images, navigation menus, appropriate scripts, and meta information for use by search engines.

Website topics work in the following way:

1. A user selects a suitable topic in Presence Builder by browsing in a list of topics or searching by a *keyword*.

A number of keywords can be defined for each topic.

2. The user specifies a website name, selects a language, and specifies personal information, such as name, company, address, e-mail, and phone number.

This information is inserted into the appropriate areas of the website, for example, on the "About Us" and "Contact Us" pages. This is done by means of *placeholder variables*. The following variables can be used in topics: %%companyName%%, %%address%%, %%city%%, %%country%%, %%phone%%, %%email%%.

3. After the user clicks **Create Site**, the editor does the following:

- Loads the selected website topic with the prefilled text.
- Inserts the information supplied by the user in the appropriate areas.
- Picks a random color scheme and layout for the site. They are randomly selected by the editor to ensure a unique appearance of the site; however, when creating your own topic, you can apply a custom layout and style and make the editor use them for your topic.
- Picks an appropriate image file to show as the site banner. The relevance of banners to site topics is determined by matching keywords in the website topics' meta data and in the banner descriptions. The instructions on how to add banner images for topics are provided in the section Adding Custom Banner Images (on page 205).
- Loads the scripts (or *modules*) that should be used on the site. The modules provided by the editor include Text & Images, Contact Form, Image Gallery, Image Slider, Blog, Embedded Video, Online Store, Social Sharing, Map, Site Search, and Advertising.

When creating a custom topic, you should include only the following modules: Text & Images, Contact Form, Blog, Embedded Video, Comments, and Social Sharing.

4. The user makes the desired changes to the site content and publishes the site to a hosting account.

In this chapter:

Adding Custom Website Topics.....	213
Rearranging and Removing Topics and Categories	221

Adding Custom Website Topics

Creation of a custom topic involves the following steps:

1. Log in to Presence Builder and create a site with custom design and content: add pages, text, scripts, and select custom layout and styles.
2. Save the created site to a snapshot and download the snapshot.
3. Upload the snapshot to the server file system and convert it to a ZIP package.
You can do this by using the command-line utility `snapshot2wst.php`, which is shipped with Presence Builder.
4. Extract the package contents for further editing and edit the files that compose the site topic. In this step, you can:
 - Make corrections to the text shown on website pages.
 - Translate all text in the topic into a different language.
 - Upload an icon that should accompany the site topic on the topic selection screen.
 - Specify a title and a description for the new topic.
 - Specify a title and a description for the topic category if you have decided to create a new category.
5. Register the newly created topic with Presence Builder by means of the `snapshot2wst.php` utility. After registration, the new topic will appear on the topic selection screen in the Presence Builder editor.
6. Verify that the topic was successfully added to Presence Builder.

Next in this section:

Step 1: Creating a Site in Presence Builder.....	214
Step 2: Saving a Site to a Snapshot	215
Step 3: Uploading the Snapshot and Preparing for Editing	216
Step 4: Editing the Files That Compose the Site Topic.....	218
Step 5: Registering the New Topic with Presence Builder	220
Step 6: Checking the New Topic	220

Step 1: Creating a Site in Presence Builder

➤ **To create a site:**

1. Log in to the Presence Builder editor.
2. Select a site topic that you want to use as a basis for your custom topic.
3. In the **Prefill Your Website** dialog, do not enter any information. If it is prefilled, delete it.
4. Click **Create Site**.
5. Edit the design and content of the site as desired:
 - Add, edit, or remove pages, and change their order.
 - Add text, images, scripts, and other useful functions provided by modules.

Note: You should insert only the following modules: Text and Images, Contact Form, Blog, Embedded Video, Comments, and Social Sharing. When inserting the modules, be sure to add them to the *page-specific areas*.

All other modules, including those inserted into *site-wide areas*, will not be saved in a snapshot, and therefore, will not be available in the site topic. Other items that cannot be saved in a snapshot are documents uploaded through the Document Manager and the site ownership verification file.

- Change the layout and colors of the site elements.
- When adding or editing text in the topic, you can use the following placeholders:
%%companyName%%, %%address%%, %%city%%, %%country%%, %%phone%%, %%email%%.



If you need assistance with the Presence Builder editor, open the **User's Guide** by clicking **Help > Open User's Guide**.

When your site topic is ready, save it to a snapshot as described in the following section.

Step 2: Saving a Site to a Snapshot

In this step, you need to save your topic to a snapshot.

➤ ***To save and download a site snapshot:***

1. In the Presence Builder editor's main menu, click the icon  next to the **Save** link.
2. Type a name for the snapshot.
3. Click **Save**.
4. To download it, click the  (Download) icon.

To prepare the snapshot for further editing, upload it to the Presence Builder server and convert to a ZIP archive as described in the following section.

Step 3: Uploading the Snapshot and Preparing for Editing

In this step, you need to upload the site snapshot to the Presence Builder server and convert it to a ZIP archive for further editing.

➤ **To upload a snapshot to the server and convert it to a ZIP package:**

1. Connect to the server using SSH or a Remote Desktop connection.
2. Upload your snapshot file to the server. You can upload it, for example, to the `/home` directory.
3. Convert the snapshot file to a ZIP archive by issuing the following command:

```
/usr/local/psa/bin/sw-engine-pleskrun
/usr/local/sb/utils/snapshot2wst.php --create --
snapshot=<source_snapshot_file.ssb> --
file=<resulting_ZIP_archive.zip> --
templateCategory=<category_code> --
templateCode=<topic_code>
```

Where:

`<source_snapshot_file.ssb>` is the path to the source snapshot archive in the SSB format that you uploaded to the server. For example: `/home/source-snapshot.ssb`.

`<resulting_ZIP_archive.zip>` is the location and file name of the resulting ZIP package. For example: `/home/package-file.zip`.

`<category_code>` is an identification code of the topic category. You can specify a name of a new category if you want to create it, or specify the code of an existing category. Do not use white spaces in category names. You will be able to set a human-readable name for this category later, by editing a file in the topic archive (`/resources/locale/en_US/SiteTemplates.lng`).

The following is a list of codes for the default categories present in Presence Builder 11.1.

Category name	Category code
Services	Services
Construction and Housing	ConstructionHousing
Retail Businesses	Retail
Manufacturing	Manufacturing
Organizations	Organization
Entertainment and Leisure	Entertainmentleisure
Arts and Design Services	ArtsDesign

Health and Sport	HealthSport
Education Services	Education
Fan and Hobby	FanHobby
Personal	Personal
Other	Other

`<topic_code>` is an identification code for the new topic. Be sure to use a unique name that does not coincide with an already existing one, otherwise, your custom topic will overwrite an existing topic. Do not use white spaces in topic codes. You will be able to set a human-readable name for this topic later, by editing a file in the topic archive (`/resources/locale/en_US/site_templates/<topic_code>/info.1ng`).

Note that there is also the option `--useSnapshotDesign`. It can be used to indicate that the styles, colors, layout, and images used in the site snapshot must be applied to the new website topic, and should not be overridden when new sites are generated based on that topic.

After the ZIP archive is created, you can unpack it for further editing, or you can edit the files without unpacking if your ZIP archive manager supports that.

Step 4: Editing the Files That Compose the Site Topic

Although you have prepared most of the content for the topic in the Presence Builder editor in **Step 1** (on page 214), you might also need to do the following:

- Optional steps:
 - Correct typos in text or make other minor changes, if required.
 - Translate the text in the site topic into another language, if required.
- Required steps:
 - Specify a title, a description, and keywords for the new topic.
 - Specify a title and a description for the new topic category, if you have decided to create a new category.
 - Add an icon that should accompany the site topic on the topic selection screen in the Presence Builder editor.

➤ *To make changes to text contained in the website pages:*

1. In the topic archive structure, open the following file for editing:
`/resources/locale/en_US/site_templates/<topic_code>/content.lng.`

Note: On the file system, the directory name corresponding to your topic will look like the topic code you specified, but with an appended unique combination of symbols.

2. Make the required changes to the text and save the file.

Note: If you want to correct the site slogan shown in the header area, or a site description added to the <META> tags of HTML pages of the site, edit the file
`/resources/locale/en_US/site_templates/<topic_code>/site.lng.`

➤ *To specify a title, a description, and keywords for the topic:*

1. In the topic archive structure, open the following file for editing:
`/resources/locale/en_US/site_templates/<topic_code>/info.lng.`
2. Type the title and description in quotation marks.
3. Specify keywords. These keywords are used for the following purposes:
 - Binding of images to website topics. When a new site is created based on a website topic, the editor searches for banner images that may be relevant to the topic, and adds one of them to the generated website. It also uses the relevant banners in generated design templates, which users can preview and select in the editor > **Design** tab > **Templates**. The relevance is determined by matching keywords in the website topic's meta data and in the banner descriptions. The instructions on how to add banner images for topics are provided in the section **Adding Custom Banner Images** (on page 205).
 - Enabling users to find topics by keywords on the topic selection screen.

- Improving of search efficiency by search engines. These keywords are also added to the `<META>` tags of HTML pages of the site.

You can use several keywords separated with commas. White spaces can be used only if they are part of a descriptive phrase or a combination of words. For example:

```
keywords = "team,sports team,league,roster"
```

4. Save the file.

➤ ***To specify a title and a description for the new topic category:***

1. In the topic archive structure, open the following file for editing:

```
/resources/locale/en_US/CustomSiteTemplates.lng.
```

2. Type the title and description in quotation marks.

3. Save the file.

➤ ***To add an icon for the topic:***

1. Prepare an image with the dimensions of 67 x 134 pixels, and save it to the PNG format, under the file name `<topic_code>.png`.

The PNG file must contain a composite image created by combining two icons with the dimensions of 67 x 67, aligned vertically: The upper half of the image must contain a grey icon, and the lower half of the image, a full-colored icon. The grey icon is shown on the topic selection screen when the mouse pointer is not hovered over the topic, and the lower half of the image, the full-colored icon, is shown when the topic is selected. The following is an example of the composite image that you need to create.



2. In the topic archive structure, upload the file to

```
/htdocs/images/site_templates/.
```

3. When prompted, confirm you want to overwrite the existing file.

When you have finished editing the files, pack them into a ZIP archive and register with your Presence Builder installation, as described in the following section.

Step 5: Registering the New Topic with Presence Builder

To finish adding your custom topic to the Presence Builder editor and make it available for selection by users, you need to register the topic with Presence Builder.

➤ *To register a topic with Presence Builder, issue the following command:*

```
/usr/local/psa/bin/sw-engine-pleskrun  
/usr/local/sb/utils/snapshot2wst.php --register --  
file=<path_to_ZIP_archive_with_topic>
```

Step 6: Checking the New Topic

➤ *To verify that your new topic was successfully added to Presence Builder:*

1. Log in to the Presence Builder editor.
2. On the topic selection screen, select your topic and click **Create Site**.
3. Review the site content to ensure that everything looks as expected.

Rearranging and Removing Topics and Categories

You can rearrange and remove topics and categories by editing a configuration file and then applying it to a Presence Builder installation.

➤ ***To modify the list of topics and categories available in Presence Builder, do the following:***

1. Log in to the server over SSH or Remote Desktop.
2. Create a configuration file by issuing the following command:

```
/usr/local/psa/bin/sw-engine-pleskrun
/usr/local/sb/utils/snapshot2wst.php --export --
file=<configuration_file>.cfg
```

3. Edit the resulting configuration file:
 - To remove unwanted topics or categories, comment out the corresponding entries in the file: place a semicolon (;) at the beginning of each line.
Categories are represented by lines containing text enclosed in square brackets. For example: [Retail].
Topics are represented in the list by lines like <topic_code>.info = "Topic title".
 - To change the order of topics or categories, move the corresponding lines within the file.
4. Save the file.
5. Apply the modified configuration file to the Presence Builder installation by issuing the following command:

```
/usr/local/psa/bin/sw-engine-pleskrun
/usr/local/sb/utils/snapshot2wst.php --import --
file=<configuration_file>.cfg
```

➤ ***To restore the default set of topics and categories in Presence Builder:***

```
/usr/local/psa/bin/sw-engine-pleskrun
/usr/local/sb/utils/snapshot2wst.php --reset
```

Enhancing Security

When you share a single physical server between many users, you consider all security aspects thoroughly. Although Panel provides an acceptable security level, there are suggested ways to improve it. This chapter provides instructions on protecting Panel server and hosted domains from unauthorized access.

In this chapter:

Restricting Script Execution in the /tmp Directory	223
Configuring Site Isolation Settings.....	224
Protecting from Running Tasks on Behalf of root	225

Restricting Script Execution in the /tmp Directory

To secure the Panel server, it is recommended to create `/tmp` as a separate partition and mount it with `noexec` and `nosuid` options. These options do the following:

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

➤ ***To secure the `/tmp` partition of your 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 a size of 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 following line to `/etc/fstab`:

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

- c. Move the current `/tmp` directory content to another location.

- d. Mount the new `/tmp` partition:

```
# mount /tmp
```

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

Configuring Site Isolation Settings

Parallels Plesk Panel allows you to define non-secure settings for web hosting. You can do this if you have permission to override server-wide hosting security restrictions. If you do not have this permission, you can manage only options specified in the `PRODUCT_ROOT_D/admin/conf/site_isolation_settings.ini` file, where the `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

The configuration file specifies the list of allowed values for hosting options:

```
[hosting]
php = on
php_handler_type = fastcgi
;python = off
;perl = off
;fastcgi = any
;miva = off
;ssi = any
;ssl = on
;shell = /usr/local/psa/bin/chrootsh
;asp = any
;php_safe_mode = on
;coldfusion = off
```

In this file, you can uncomment a line by removing the semi-colon (;) and comment out a line by adding the semi-colon (;) in the beginning of the line.

You can set the following options values:

- `on` and `off` for scripting options.
- `module`, `fastcgi`, `cgi` for `php_handler_type`.
- A line from `/etc/shells` file for `shell`.
- `any` for any option if the option value is not restricted.

In addition, there are the following restrictions for options values:

- If the `php` is `off`, the `php_handler_type` and the `php_safe_mode` **SHOULD** be `any`.
- If the `fastcgi` is `off`, the `php_handler_type` **SHOULD NOT** be `fastcgi`.

Protecting from Running Tasks on Behalf of root

By default, Parallels Plesk Panel allows utilities or scripts to be run on behalf of root in two cases:

Scheduling tasks with the cron manager

- Handling events with the Event Manager tool

This makes Panel server vulnerable to malicious software. To eliminate these vulnerabilities, create the following files and leave them empty:

`$PRODUCT_ROOT_D/var/root.crontab.lock` prevents users from running cron tasks and viewing the list of tasks scheduled on behalf of root.

`$PRODUCT_ROOT_D/var/root.event.handler.lock` prevents users from creating event handlers functioning on behalf of root.

The `$PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems

Localization

Parallels Plesk Panel 11.5 is shipped with the following interface languages:

- American English
- Dutch
- French
- German
- Italian
- Japanese
- Polish
- Portuguese
- Russian
- Spanish
- Simplified Chinese
- Traditional Chinese

It is possible to translate Parallels Plesk Panel interface (including Presence Builder) into other languages and apply the translation to a Panel installation.

For detailed instructions on translating Panel into your language, refer to the **Localization Guide**.

Registering Additional Services with Panel Notifications

Hosting companies can add value to hosting plans and enhance the Panel capabilities by adding third-party services to Panel. In the terms of Panel, such services are called *additional*. An additional service can be any resource available at a certain URL (like a Panel extension, web app, and so on), even if it is completely independent from Panel. It can be a spam filter, statistics analytic tool, helpdesk or other services.

The administrator and resellers associate these additional services with hosting plans when setting up a distribution strategy. For example, if you have a service that performs custom mail filtering, Panel lets you offer this service with one particular plan, for example, the Silver hosting plan and do not offer with others.

To make Panel aware of an additional service, you should add the service to Panel. In the simplest case, when the service resides on a remote URL and does not require any notifications from Panel, add it from the Panel GUI, page **Service Plans > Additional Services**. From there, you can also associate the service with a custom button that is instantly added to the **Websites & Domains** page of each subscriber.

Another way to add a service is to make a programming call to Panel. The benefit of this approach is that it lets your service to receive Panel notifications about the object changes. For example, the mail filtering service we mentioned earlier must track account name changes to serve renamed accounts as well. Though you can make a call that adds a service and does not subscribe it to notifications, this operation does not make much sense as it is easier to add such services through the GUI. Thus, we consider that you will generally use programming means to both add services and register them with Panel Notifications (PN).

The possible inconvenience of adding services by a call is that you are unable to edit details of the services through the Panel GUI. Please consider it when designing service names and descriptions. Another peculiar feature of adding services by a call is that they are not automatically visible to customers. We recommend that you use custom buttons or write an extension to display the service in the Control Panel.

PN sends notifications about subscriptions, sites, and e-mail accounts related to the service. The relation *subscription - service* is derived from plans: A service is associated with plans, whereas subscriptions are plan instances. If a subscription has sites or e-mail accounts, the changes of these supplementary objects are also tracked.

If you wish to register your service with the PN, do the following:

1. Create a service-specific class that implements interface *Plan_Item_Interface*.
By implementing this interface, you specify the service properties in Panel and define what type of changes it should receive and how it should handle them. When a change happens, Panel executes the change handling code from this class. This code runs in the Administrator context.

2. Register this class by an appropriate call.

For details on interface *Plan_Item_Interface* and instructions on how to implement it, see section **Preparing a Service for Registration** (on page 229).

To learn how to register a prepared class, see section **Registering the Service** (on page 230).

Note: This section does not explain how to write third-party services, integrate them into the Panel GUI, or get access to the Panel resources. If you wish to make a registered service available to customers, create a custom button pointing to the service URL and place it on pages available to customers. This can be done through the command line interface (CLI) and will work only if your service receives enough information from PN. If your service requires access to other Panel resources or you want to build your service into the Panel GUI, consider writing an extension.

In this chapter:

Preparing a Service for Registration	229
Registering the Service	230
Code Samples.....	231

Preparing a Service for Registration

To prepare a service for registration with Panel Notifications, create a PHP file containing a class that implements interface *Plan_Item_Interface* and put the file into a directory available to the Panel. The directory must have a unique name and reside in `/PRODUCT_ROOT_D/admin/plib/`, where `PRODUCT_ROOT_D` is the installation directory of the Panel.

When designing names of the class that implements the interface and the file that includes this class, follow Zend naming conventions. For example, if you create a directory `/PRODUCT_ROOT_D/admin/plib/servicedir` and put there file `servicefile.php`, then the class name must be `servicedir_servicefile`. To learn more about the naming conventions, see <http://framework.zend.com/manual/en/coding-standard.naming-conventions.html>.

We offer a sample class you can use as a base when writing own classes to help you with the implementation. The code is supplemented by comments that explain the interface organization.

To view the code, refer to the **Implementation of Plan_Item_Interface** section (on page 232).

Registering the Service

We suppose that you have prepared the *Plan_Item_Interface* implementation and want to register your service with Panel Notifications. To perform the registration, create an arbitrary PHP file, for example, `register.php`, and paste the code given below into the file. Substitute *servicedir_servicefile* with your class name throughout the code. When ready, run the code by using one of these shell commands:

- On Linux, run `/usr/local/psa/bin/sw-engine-pleskrun register.php`
- On Windows, run `%plesk_bin%\php register.php`

Note: We suppose that the Panel is installed to the default installation directory. If you use a custom directory, please update the paths correspondingly.

To view the `register.php` code, refer to the **Implementation of Plan_Item_Interface** section (on page 236).

If it is impossible for you to run the PHP code, you can register the service directly by running this MySQL statement customized to your class.

```
INSERT INTO PlanItems (
    classname,
    name,
    applicableToEmail,
    uuid
)
VALUES (
    'servicedir_servicefile',
    'urn:isv:custom-item-connector:1',
    1,
    '219b7656-8e92-869d-828a-6814cda71a1s');
```

The definition of the parameters that present in the statement is as follows:

- *classname*, string
The name of the class that contains the interface implementation.
- *name*, string
The unique name of the service.
- *applicableToEmail*, boolean (0,1)
This parameter subscribes the service to e-mail accounts changes. Alternatively, you can specify *applicableToSite* or *applicableToSubscription* to receive notifications about changes of the Panel subscriptions and sites.
- *uuid*, string
The service identifier.

Code Samples

Next in this section:

Implementation of Plan_Item_Interface	232
Registration of an Additional Service	236

Implementation of Plan_Item_Interface

```
<?php

/**
 * Sample implementation of a Service Plan Item declaration.
 *
 */

/**
 *
 * Plan_Item_Interface declares the following methods:
 *
 * public function getName();
 * public function getHint($locale);
 * public function getDescription($locale);
 * public function update(
 *     $subject,
 *     $change,
 *     $subscriptionUuid,
 *     $planItemUuid
 * );
 *
 * Additional descriptions are available as annotations to method
 * implementations below.
 */
class servicedir_servicefile implements Plan_Item_Interface
{
    private $_logFile = '/tmp/custom-item-connector.log';
    private $_locales = array(
        'en-US' => array(
            'description' => 'External Mail Filtering Service',
            'hint' => 'Filter all incoming mail through cloud mail filter',
        ),
        'de-DE' => array(
            'description' => 'This is a description in German',
            'hint' => 'And hint is also in German',
        ),
    );

    /**
     * Returns a unique name of an additional service.
     * The Panel uses this name to distinguish services from each other.
     *
     * @return string
     */
    public function getName()
    {
        return 'urn:isv:custom-item-connector:1';
    }

    /**
     * Returns a localized name of the service, that will be
     * displayed in the Panel (in Service Plans > Additional Services).
     *
     */
}
```



```

    * @param string $locale Currently used locale in format 'xx-XX' (RFC
1766).
    * @return string
    */
    public function getHint($locale)
    {
        return $this->_('hint', $locale);
    }

    /**
    * Returns a localized name of the service, that will be
    * displayed in the Panel (in Service Plans > Additional Services).
    *
    * @param string $locale Currently used locale in format 'xx-XX'
    * @return string
    */
    public function getDescription($locale)
    {
        return $this->_('description', $locale);
    }

    /**
    * Receives update notifications about related Panel objects. The
objects are
    * specified with object implementing Plan_Item_Subject interface that
    * declares the following methods:
    *
    *     public function getType() - Returns type of a changed object
    *         as specified by Plan_Item_Subject constants
    *
    *         Available types: Plan_Item_Subject::EMAIL,
Plan_Item_Subject::SITE,
    *         Plan_Item_Subject::SUBSCRIPTION
    *
    *     public function getProperties() - Returns the current values of
    *         subject properties. The properties are returned as key => value
pairs.
    *
    *         For deleted objects, properties values remain as they were
    *         before deletion. For created objects, properties values are
those
    *         that were assigned to these objects upon creation.
    *
    *         Available properties.
    *
    *         For subscriptions:
    *             GUID: string
    *             status: boolean
    *
    *         For sites:
    *             status: boolean
    *             name: string
    *             GUID: string
    *
    *         For e-mail accounts:
    *             email: string (account name)
    *
    * Changes are specified with $change that is one of

```

```

* Plan_Item_Notification::{CREATED,UPDATED,DELETED} constants.
*
* $subscriptionUuid is a GUID of subscription.
*
* $planItemUuid is a GUID of the additional service.
*
*
* @param Plan_Item_Subject $subject
* @param int $change
* @param string $subscriptionUuid
* @param string $planItemUuid
* @return void
*/
public function update(
    Plan_Item_Subject $subject,
    $change,
    $subscriptionUuid,
    $planItemUuid
)
{
    $subjectType = Plan_Item_Subject::EMAIL === $subject->getType()
        ? 'Email address'
        : 'unknown';

    switch ($change) {
        case Plan_Item_Notification::CREATED:
            $this->_log("$subjectType created: " .
                print_r($subject->getProperties(), true)
            );
            break;
        case Plan_Item_Notification::UPDATED:
            $this->_log("$subjectType updated: " .
                print_r($subject->getProperties(), true)
            );
            break;
        case Plan_Item_Notification::DELETED:
            $this->_log("$subjectType deleted: " .
                print_r($subject->getProperties(), true)
            );
            break;
    }
}

/**
 * Declares from what type of Panel objects the service will receive
notifications.
 * It returns either an array or a single type.
 *
 * Plan_Item_Subject::SUBSCRIPTION
 *     The service will receive notifications about all changes made
to
 *     subscription (including activation/suspension of subscriptions,
 *     assigning/de-assigning the service to a subscription)
 *
 * Plan_Item_Subject::EMAIL
 *     The service will receive notifications about all changes made
to
 *     e-mail accounts on affected subscriptions.
 *
 * Plan_Item_Subject::SITE

```

```

    *      The service will recieve notifications about all changes made
to
    *      site names in the scope affected subscriptions.
    */
public static function getSubjectTypes()
{
    return array(Plan_Item_Subject::EMAIL);
}

private function _($key, $locale)
{
    if (!isset($this->_locales[$locale])) {
        return $this->_locales['en-US'][$key];
    }

    return $this->_locales[$locale][$key];
}

private function _log($message)
{
    date_default_timezone_set('UTC');
    $logString = "[" . date("H:i:s") . "] " . $message;
    file_put_contents($this->_logFile, $logString, FILE_APPEND);
}
}

```

Registration of an Additional Service

```
<?php

/**
 * Sample code to register an additional service in
 * the Panel 10.1 and above.
 *
 */

/**
 * Use the following instructions to initialize the Panel PHP
 * environment when running command-line PHP script with sw-engine-pleskrun
 * utility. On Linux OSes, it resides in /usr/local/psa/bin/.
 *
 * For Windows servers, use the following command to run the registration
 * script.
 * "%plesk_bin%\php.exe" -d auto_prepend_file="" "<ABSOLUTE-PATH-TO-
 * SCRIPT>"
 *
 * Comment the following two lines if you run the PHP script through the
 * Panel
 * web interface.
 */
require_once('api-common/cu.php');
cu::initCLI();

/**
 * The following code registers the service that was
 * implemented with the servicedir_servicefile class. This class must
 * be available for autoloading from the Panel.
 */

Db_Table_Broker::get('PlanItems')->register(
    new servicedir_servicefile(),
    servicedir_servicefile::getSubjectTypes()
);
```

Troubleshooting

This section provides procedures for solving the most typical problems in Parallels Plesk Panel for Linux. Most importantly, it contains information on what to do if you:

- cannot access the Panel log in page
- cannot log in to Panel
- forget the administrator's password
- encounter problems when operating Panel in a Virtuozzo Container

If your problem is not discussed in this chapter or if the proposed solution does not work, visit the Parallels Knowledge Base at <http://kb.parallels.com/> or contact our technical support department.

In this chapter:

Cannot Access Panel	238
Cannot Log In to Panel.....	238
The Administrator's Password Has Been Forgotten	239
Panel in a Virtuozzo Container: Broken Layout	240
EZ Templates Update Issues in Parallels Virtuozzo Containers	242
Postfix Consumes Too Many Resources in a Container	242

Cannot Access Panel

If you get the error messages "Unable to initialize session", "Domain ID is undefined", or "Client ID is undefined" when trying to access Parallels Plesk Panel, it means that Panel cannot create a session in \$PRODUCT_ROOT_D/admin/sessions.

This may happen if there is not enough free disk space on the Panel server.

To check if there is enough disk space, run the commands:

```
# df -h
# df -i
```

If disk space usage is at 100%, you should remove useless files or rotate log files in /var/log/. For more information on log rotation, see the section **Log Rotation** (on page 131).

Cannot Log In to Panel

If you get the error message *"Access for administrator from address xx.xx.xx.xx is restricted in accordance with IP Access restriction policy currently applied."* when trying to access Parallels Plesk Panel, it means that the Panel IP access policy does not allow you to log in from your current IP.

➤ **To access Panel from an IP address:**

1. Log in to the server via SSH.

Change the IP access policy in the psa database:

To find the current policy and its restricted and allowed IP addresses, run the following commands.

```
# mysql -uadmin -p`cat /etc/psa/.psa.shadow` -psa
mysql> select * from cp_access;
mysql> select * from misc where param='access_policy';
```

➤ **To clear the access policy settings:**

Remove all records from the cp_access table:

```
mysql> delete from cp_access;
```

Set the policy to allow:

```
mysql> update misc set val="allow" where param='access_policy';
```

otherwise, you may get the following error message:

Unable to connect to database

login.php3: Unable to connect to database: Permission denied

ERROR 1045: Access denied for user: 'admin@localhost' (Using password: YES)

In this case, restart Panel and try to log in again:

```
# /etc/init.d/psa restart
```

If this does not work, do the following:

Check that the `/etc/psa/.psa.shadow` file has valid permissions:

```
# ls -la /etc/psa/.psa.shadow
```

The right permissions and owner are `-rw-----` and `psaadm` respectively. If the current permissions are different from these, change them by running the commands:

```
# chown psaadm:psaadm /etc/psa/.psa.shadow
# chmod 600 /etc/psa/.psa.shadow
```

Check that mysql server is running and working properly:

```
# ps ax | grep mysql
```

The following output indicates that the mysql is running properly:

```
3776 pts/0  S+   0:00 grep mysql
```

```
24272 ?      S    0:00 /bin/sh /usr/bin/mysqld_safe datadir=/var/lib/mysql --
socket=/var/lib/mysql/mysql.sock --log error=/var/log/mysqld.log --pid-
file=/var/run/mysqld/mysqld.pid user=mysql
```

```
24322 ?      Sl   0:07 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --
user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --
socket=/var/lib/mysql/mysql.sock
```

Try to access the mysql through the server shell:

```
# mysql -uadmin -p`cat /etc/psa/.psa.shadow` -D psa
```

If you can access the mysql, then it is likely that Panel is ok and you have forgotten the administrator's password. See the section **The Administrator's Password has been Forgotten** (on page 239) for instructions on how to restore it.

The Administrator's Password Has Been Forgotten

If you forget the Panel administrator's password, there are two ways to resolve this issue:

- restore the password
- set new password

➤ ***To restore the Panel administrator's password:***

1. Log in to the server via SSH.
2. Go to `PRODUCT_ROOT_D/bin/` where `PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.
3. Run the `admin` utility with the `--show-password` option:

```
# ./admin --show-password
```

➤ ***To set a new administrator password:***

1. Log in to the server via SSH.
2. Go to `PRODUCT_ROOT_D/bin/` where `PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.
3. Run the `init_conf` utility with the new password specified:

```
# /usr/local/psa/bin/init_conf --update -passwd new_password
```

Panel in a Virtuozzo Container: Broken Layout

When Panel is installed to Parallels Virtuozzo Containers PVC, administrators refer to Panel when performing web hosting operations and to Parallels Power Panel (PPP) when managing their container. The PPP becomes available when the administrators turn on the *offline-management* mode. When this mode is on and Panel is installed, some controls and menus of PPP become available in the top and left navigation panes of Panel. In other words, PPP is partially built into Panel in offline-management mode.

Since Panel 10, the integration between panels can lead to unexpected results. For example, some icons in Panel might not be displayed or the layout might be broken when the offline management is on. To resolve these problems, we recommend that you do not use the integration, and that you access the panels on different ports (4643 and 8443).

➤ ***To make PPP and Panel operate on different ports, do the following:***

- On Linux servers, connect to the hardware node over SSH and run the following command:

```
vzctl set CT_ID --offline_management yes --offline_service  
vzpp --save
```

- On Windows servers, connect to the hardware node over Remote Desktop and run the following commands:

```
vzctl set CT_ID --offline_management yes --save  
vzcfgt set CT_ID offlineservices vzpp
```

EZ Templates Update Issues in Parallels Virtuozzo Containers

PVC 4.0 and later versions can discover EZ templates in a container and perform automatic actions depending on the templates. This feature provided opportunities for business automation software (such as PBAs) to automatically find products installed in a container and start billing the container owner.

The discovery algorithm is straightforward: If the system finds all packages included in an EZ template, it considers that such a template is installed. The major drawback of this approach is that Panel 9.x and SMB are very close to each other in terms of packages, so the auto-detection engine makes incorrect decisions. Namely, if only one of the applications is present in a container, the system considers that both templates are installed. The most noticeable outcome of this detection problem is that the system fails to update both applications or set proper billing for them.

It is possible to stop the auto detection if you use the billing automation software or if you want to install Parallels Small Business Panel. To do this, modify the `/etc/vztt/vztt.conf` file by setting `APP_TEMPLATE_AUTODETECTION=no`.

Postfix Consumes Too Many Resources in a Container

If you operate in Parallels Virtuozzo Containers Environment the Postfix mail service may consume too many resources and, hence, work in an unstable manner. This is particularly likely to happen if there is a lot of outgoing mail that cannot be delivered. By default, Postfix can create up to 100 mail sending processes that will not stop until they send the specified mail.

➤ *To reduce resources consumption by Postfix:*

1. Reduce the maximum number of Postfix processes, for example, to 20:

```
# postconf -e 'default_process_limit=20'
```

Disable unused services, for example, `ifmail` and `uucp` in the Postfix configuration file `/etc/postfix/master.cf`.

1. Reload the Postfix:

```
# PRODUCT_ROOT_D/admin/sbin/mailmng --reload-service
```

`PRODUCT_ROOT_D` is `/usr/local/psa` for RPM-based systems or `/opt/psa` on DEB-based systems.

Appendix A: Web Server Configuration Files





Apache configuration files

All Parallels Plesk Panel-specific Apache configuration files are included in the Apache system configuration (`/etc/httpd/httpd.conf`) via file `zz010_psa_httpd.conf` using the `Include` directive. The file `zz010_psa_httpd.conf` can be located in `/etc/apache2/conf.d/` or `/etc/httpd/conf.d/` depending on the operating system.

The following table represents the hierarchy of Apache configuration files.

<code>/etc/httpd/httpd.conf</code>	
↳	<code>/etc/httpd/conf.d/zz010_psa_httpd.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/server.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/ip_default/@<domain_name>.conf -> /var/www/vhosts/system/<domain_name>/conf/httpd_ip_default.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/horde.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/webmails/horde/<domain_name>_webmail.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/roundcube.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/webmails/roundcube/<domain_name>_webmail.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/atmail.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/webmails/atmail/<domain_name>_webmail.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/vhosts/@<domain_name>.conf -> /var/www/vhosts/system/<domain_name>/conf/last_httpd.conf</code>
↳	<code>/usr/local/psa/admin/conf/file_sharing.conf*</code>
↳	<code>/var/www/vhosts/system/<domain_name>/conf/siteapp.d/*.conf</code>
↳	<code>/var/www/vhosts/system/<domain_name>/conf/vhost_ssl.conf</code>
↳	<code>/var/www/vhosts/system/<domain_name>/conf/vhost.conf*</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/forwarding/<domain_name>.conf</code>
↳	<code>/etc/httpd/conf/plesk.conf.d/wildcards/@<domain_name>.conf -> /var/www/vhosts/system/_<domain_name>/conf/last_httpd.conf</code>

On this diagram:

-  - System configuration file.
-  - Files generated by Panel.
-  - Files generated by Panel from configuration templates.
-  - Files created by user and containing custom configuration directives.

File `file_sharing.conf` is not generated, but shipped with Panel.

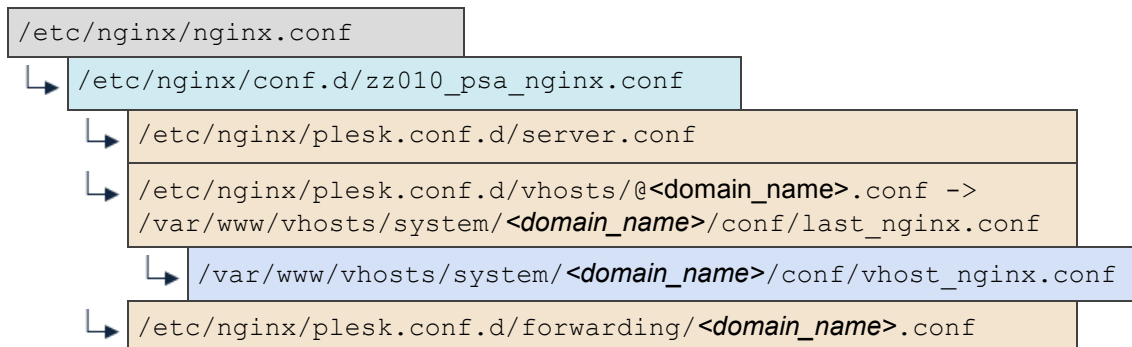
Files from `siteapp.d/*.conf` are shipped with corresponding APS packages.

The placeholder `<domain-name>` is the domain name of the website for which the configuration is generated.





nginx configuration files

All Parallels Plesk Panel-specific nginx configuration files are included in the nginx system configuration (`/etc/httpd/nginx.conf`) via file `zz010_psa_nginx.conf` using the `Include` directive. The file `zz010_psa_nginx.conf` is located in `/etc/nginx/conf.d/`.

The following table represents the hierarchy of nginx configuration files.



On this diagram:












-  - System configuration file.
-  - Files generated by Panel.
-  - Files generated by Panel from configuration templates.
-  - Files created by user and containing custom configuration directives.





















The placeholder `<domain-name>` is the domain name of the website for which the configuration is generated.






Appendix B: Configuration Templates Structure

A set of configuration template files is structured as follows, assuming that the root folder is `default/` or `custom/`. Editing these files changes the Apache configuration.

Root templates are starting points in generating configuration files. Panel always starts generating a configuration from one of these files. All root templates contain statements that include the other templates located in respective folders (`domain`, `server` and `service`).

	<code>atmail.php</code>	Root template of a server-wide configuration for Atmail Light.
	<code>atmailcom.php</code>	Root template of a server-wide configuration for Atmail Full.
	<code>domainForwarding.php</code>	Root template of a per-website configuration for websites with forwarding, either standard or frame.
	<code>domainVhost.php</code>	Root template of a per-website configuration for hosted websites.
	<code>domainWebmail.php</code>	Root template of a per-website configuration for a webmail service.
	<code>horde.php</code>	Root template of a server-wide configuration for Horde.
	<code>server.php</code>	Root template of a server-wide configuration for server services, such as Tomcat, Mailman and several others. For details, see the contents of the <code>server/</code> directory below.
	<code>nginx.php</code>	(In Panel 11.0+) This template includes the server-wide configuration of nginx.
	<code>domain/</code>	Contains templates included in a per-website configuration.
	<code>domainVirtualHost.php</code>	Configuration for hosted website addressed by domain name.
	<code>frameForwarding.php</code>	Configuration for website with frame forwarding.

	nginxDomainVirtualHost.php	(In Panel 11.0+) This template includes per-website configuration of nginx.
	standardForwarding.php	Configuration for website with standard forwarding.
	subDomainVirtualHost.php	Configuration for hosted website addressed by subdomain name.
	service/	Contains templates of configuration for website services included in a website configuration.
	bandWidth.php	Configuration for website bandwidth limits.
	errordocs.php	Configuration for website error documents.
	frontpageWorkaround.php	Configuration for FrontPage on website.
	protectedDirectories.php	Configuration for password-protected website directories.
	tomcat.php	Configuration for the Tomcat service on a website.
	server/	Contains templates included in a server-wide configuration.
	PCI_compliance.php	Defines directives specific to meeting PCI compliance.
	mailman.php	Configuration for the Mailman service.
	nameVirtualHost.php	Defines <i>NameVirtualHost</i> directive.
	tomcat.php	Configuration of the Tomcat service.
	vhosts.php	Configuration for the server default virtual host (a virtual host addressed if a request is made to an IP address registered in Panel but no default website is assigned to it).
	service/	Contains context-free templates of configuration for various services.
	asp.php	Configuration for ASP.
	coldfusion.php	Configuration for ColdFusion.
	miva.php	Configuration for Miva Virtual Machine.
	mod_fastcgi.php	Configuration for FastCGI.

	mod_perl.php	Configuration for Perl.
	mod_python.php	Configuration for Python.
	php.php	Configuration for PHP.
	php_over_cgi.php	Configuration for PHP over CGI.
	php_over_fastcgi.php	Configuration for PHP over FastCGI.

Appendix C: Apache Configuration Variables

This appendix contains a reference on Apache configuration variables that may be used to configure the default virtual hosts.

\$VAR is an associative array that contains the data model. Below is a detailed list explaining available paths and values.

\$VAR->

- \$VAR->domainsIpDefaultBootstrap
The full path to the bootstrap file for a domain set as default on an IP address; string
- \$VAR->domainsBootstrap
The full path to the bootstrap file for domains; string
- \$VAR->domainsWebmailHordeBootstrap
The full path to the bootstrap file for Horde; string
- \$VAR->domainsWebmailAtmailBootstrap
The full path to the bootstrap file for Atmail; string
- \$VAR->domainsWebmailAtmailcomBootstrap
The full path to the bootstrap file for Atmail Commerce; string

In this chapter:

1. \$VAR->server->	249
2. \$VAR->domain->	252
3. \$VAR->subDomain->	257
4. \$VAR->ipAddress->	258

1. \$VAR->server->

- `$VAR->server->fullHostName`
Full name of the host where the Panel is installed; string
- `$VAR->server->ipAddress->all`
List of IP addresses registered with the Panel; array with elements `$VAR->ipAddress`
- `$VAR->server->admin->email`
E-mail address of the Panel administrator; string
- `$VAR->server->productRootDir`
The full path to the root directory of the Panel installation; string
- `$VAR->server->productConfigDir`
The full path to the directory where the Panel configuration is stored; string
- `$VAR->server->getSslLibraryPath`
The full path to the system SSL library; string
- `$VAR->server->getCryptoLibraryPath`
The full path to the system cryptographic library; string

1.2. \$VAR->server->domains->

- `$VAR->server->domains->allWithHosting`
List of domains where hosting (both web hosting and forwarding) is set up; array with elements `$VAR->domain`
- `$VAR->server->domains->allWithoutHosting`
List of domain accounts where no hosting is set up (neither web hosting nor forwarding); array with elements `$VAR->domain`

1.3. \$VAR->server->webserver->

- `$VAR->server->webserver->vhostDir`
The full path to the system `vhosts/` directory; string
- `$VAR->server->webserver->httpLogsDir`
The full path to the `logs/` directory; string
- `$VAR->server->webserver->httpIncludeDir`
The full path to the Apache `conf.d` directory; string
- `$VAR->server->webserver->httpDir`
The full path to the directory with content of the server default website available via HTTP; string
- `$VAR->server->webserver->httpsDir`
The full path to the directory with content of the server default website available via HTTPS; string

- `$VAR->server->webserver->httpPort`
Apache HTTP port number; string
- `$VAR->server->webserver->httpsPort`
Apache HTTPS port number; string
- `$VAR->server->webserver->cgiBinDir`
The full path to the cgi-bin directory of the server default site; string
- `$VAR->server->webserver->clientGroup`
System group of users using Apache web hosting (a user group in which all FTP users of web hosting are included); string

1.3.1. `$VAR->server->webserver->apache->`

- `$VAR->server->webserver->apache->pipelogEnabled`
Defines if writing Apache logs to a pipe is enabled; boolean
- `$VAR->server->webserver->apache->traceEnableCompliance`
Determines the behaviour on TRACE requests; boolean
- `$VAR->server->webserver->apache->allowOverrideDefault`
Defines the value of the *AllowOverride* directive in Apache configuration; string
- `$VAR->server->webserver->apache->php4ModuleName`
Name of the Apache module used for PHP 4; string
- `$VAR->server->webserver->apache->phpCgiBin`
Binary file used to run PHP in CGI mode; string
- `$VAR->server->webserver->apache->coldfusionModuleName`
Name of Apache module used for ColdFusion; string
- `$VAR->server->webserver->apache->vhostIpCapacity`
Maximum number of IP addresses that can be defined in the *<VirtualHost>* tag in Apache configuration; integer

1.3.2. `$VAR->server->webserver->horde->`

- `$VAR->server->webserver->horde->confD`
The full path to the directory with Horde configuration; string
- `$VAR->server->webserver->horde->logD`
The full path to the directory with Horde logs; string
- `$VAR->server->webserver->horde->docD`
The full path to the Horde doc directory; string
- `$VAR->server->webserver->horde->dataD`
The full path to the folder with Horde PEAR data; string

1.4. \$VAR->server->tomcat->

- `$VAR->server->tomcat->workersFile`
The full path to the Tomcat workers file; string
- `$VAR->server->tomcat->workerName`
Tomcat worker ID; string
- `$VAR->server->tomcat->warpPort`
Tomcat WARP port; string

1.5. \$VAR->server->mailman->

- `$VAR->server->mailman->rootDir`
The full path to the Mailman root directory; string
- `$VAR->server->mailman->varDir`
The full path to the Mailman var directory; string
- `$VAR->server->mailman->scriptAliases`
ScriptAliases required for the web panel of the Mailman service to work; array with elements 'url => path'
- `$VAR->server->mailman->aliases`
Aliases required for the web panel of the Mailman service to work; array with elements 'url => path'

1.6. \$VAR->server->coldfusion->

- `$VAR->server->coldfusion->port`
ColdFusion port number; string
- `$VAR->server->coldfusion->serverStorePath`
The full path to the file that contains information for the associated JRun server (default file name is `jrunserver.store`); string

1.7. \$VAR->server->miva->

- `$VAR->server->miva->libDir`
The full path to the Miva lib directory; string
- `$VAR->server->miva->binDir`
The full path to the Miva bin directory; string
- `$VAR->server->miva->shareDir`
The full path to the Miva shared directory; string

1.8. \$VAR->server->awstats->

- `$VAR->server->awstats->docsDir`
The full path to the AWStats docs directory; string

2. \$VAR->domain->

The content of \$VAR->domain is defined by the value of the domainId key in \$metainfo.

- \$VAR->domain->id
Domain ID; string
- \$VAR->domain->www
Defines if the website is accessible with the www prefix; boolean
- \$VAR->domain->enabled
Defines the website status; boolean
- \$VAR->domain->idnName
International domain name; string
- \$VAR->domain->asciiName
Domain name in ASCII format; string
- \$VAR->domain->isIpDefault
Defines if the website is set as default for the IP address; boolean
- \$VAR->domain->hasPhysicalHosting
Defines if the website is set up for web hosting; boolean
- \$VAR->domain->hasStandardForwarding
Defines if the website is set up as standard forwarding; boolean
- \$VAR->domain->hasFrameForwarding
Defines if the website is set up as frame forwarding; boolean
- \$VAR->domain->webAliases
Web aliases of the website; array where elements are objects \$object->asciiName
- \$VAR->domain->mailAliases
Mail aliases of the website; array where elements are objects \$object->asciiName
- \$VAR->domain->client->email
E-mail address of the website owner; string
- \$VAR->domain->email
E-mail address of the Domain Administrator of the website; string

2.1. \$VAR->domain->physicalHosting->

- \$VAR->domain->physicalHosting->login
Username of FTP account used to access the website content; string
- \$VAR->domain->physicalHosting->ipAddress
IP address on which the website is hosted; see \$VAR->ipAddress

- `$VAR->domain->physicalHosting->vhostDir`
The absolute path to the website's `vhost` directory; string
- `$VAR->domain->physicalHosting->logsDir`
The absolute path to the website's logs directory; string
- `$VAR->domain->physicalHosting->webUsersDir`
The absolute path to the website's directory designated for web users' content; string
- `$VAR->domain->physicalHosting->httpDir`
The absolute path to the website's `httpdocs` directory; string
- `$VAR->domain->physicalHosting->httpsDir`
The absolute path to the website's `httpsdocs` directory; string
- `$VAR->domain->physicalHosting->cgiBinDir`
The absolute path to the website's `cgi-bin` directory; string
- `$VAR->domain->physicalHosting->statisticsDir`
The absolute path to the website's `statistics` directory; string
- `$VAR->domain->physicalHosting->siteAppsConfigDir`
The absolute path to the website's directory where configuration files of the installed non-SSL site applications are stored; string
- `$VAR->domain->physicalHosting->customConfigFile`
The absolute path to the directory `<vhostdir>/conf/vhost.conf` for a non-SSL website; string
- `$VAR->domain->physicalHosting->siteAppsSslConfigDir`
The absolute path to the website's directory where configuration files of the installed SSL site applications are stored; string
- `$VAR->domain->physicalHosting->customSslConfigFile`
The absolute path to the directory `<vhostdir>/conf/vhost.conf` for a non-SSL website; string
- `$VAR->domain->physicalHosting->ssl`
Defines if the SSL support is enabled on the website; boolean
- `$VAR->domain->physicalHosting->trafficBandwidth`
Defines a limit imposed on the traffic bandwidth usage by the domain; string
- `$VAR->domain->physicalHosting->maximumConnection`
Defines a limit imposed on the maximum allowed number of connections to the domain; string
- `$VAR->domain->physicalHosting->php`
Defines if the PHP support is enabled on the website; boolean
- `$VAR->domain->physicalHosting->phpHandlerType`
Defines PHP handler type; string
- `$VAR->domain->physicalHosting->phpSafeMode`
Defines if PHP operates in safe mode; boolean
- `$VAR->domain->physicalHosting->ssi`
Defines if SSI is supported on the website; boolean

- `$VAR->domain->physicalHosting->cgi`
Defines if CGI is supported on the website; boolean
- `$VAR->domain->physicalHosting->miva`
Defines if Miva support is enabled for the website; boolean
- `$VAR->domain->physicalHosting->mivaDataDir`
The full path to the Miva data directory; string
- `$VAR->domain->physicalHosting->perl`
Defines if Perl is supported on the website; boolean
- `$VAR->domain->physicalHosting->asp`
Defines if ASP is supported on the website; boolean
- `$VAR->domain->physicalHosting->python`
Defines if python is supported on the website; boolean
- `$VAR->domain->physicalHosting->fastcgi`
Defines if FastCGI is supported on the website; boolean
- `$VAR->domain->physicalHosting->error_docs`
Defines if custom error pages are supported on the website; boolean
- `$VAR->domain->physicalHosting->hasWebstat`
Defines if a web statistics service is supported on the website; boolean
- `$VAR->domain->physicalHosting->webuserScriptingEnabled`
Defines if using scripts is allowed to web users on the website; boolean
- `$VAR->domain->physicalHosting->frontpage`
Defines if Microsoft FrontPage is supported on the website; boolean
- `$VAR->domain->physicalHosting->frontpageSsl`
Defines if Microsoft FrontPage over SSL is supported on the website; boolean
- `$VAR->domain->physicalHosting->coldfusion`
Defines if ColdFusion is supported on the website; boolean
- `$VAR->domain->physicalHosting->subdomains`
List of the website subdomains; array with elements `$VAR->subdomain`
- `$VAR->domain->physicalHosting->phpSettings`
List of PHP settings for the website (including additional directives); string
- `$VAR->domain->physicalHosting->webusers`
Accesses web user specific data; array where elements are objects of type `$object-><webuser-parameter>` where `<webuser-parameter>` is one of the following:
 - `dir`
The absolute path to the directory with the web user's content; string
 - `ssi`
Defines if SSI support is enabled for the web user; boolean
 - `cgi`
Defines if CGI support is enabled for the web user; boolean

- `perl`
Defines if perl support is enabled for the web user; boolean
- `asp`
Defines if ASP support is enabled for the web user; boolean
- `php`
Defines if PHP support is enabled for the web user; boolean
- `phpSettings`
List of PHP settings for the web user. All setting values are the same as for the website except `open_basedir` (it contains the path to the web user's home directory); string
- `python`
Defines if python support is enabled for the web user; boolean
- `fastcgi`
Defines if fastCGI support is enabled for the web user; boolean

2.2. `$VAR->domain->forwarding->`

- `$VAR->domain->forwarding->ipAddress`
IP address on which the website forwarding is set up; `$VAR->ipAddress`
- `$VAR->domain->forwarding->redirectUrl`
URL to which requests for the website are redirected; string

2.3. `$VAR->domain->tomcat->`

- `$VAR->domain->tomcat->enabled`
Defines if Tomcat is enabled on the website; boolean
- `$VAR->domain->tomcat->all`
Gets data on all Tomcat applications running on the domain; array where elements are objects `$object->name` where 'name' is an application name

2.4. `$VAR->domain->protectedDirectories->`

- `$VAR->domain->protectedDirectories->sslDirectories`
Password-protected directories of the website available via SSL; array with elements `array('directory' => '', 'realm' => '', 'authFile' => '',)` where
 - `directory` is a path (relative to the virtual host root) to a directory being protected
 - `realm` is a text displayed when requesting password from a user
 - `authFile` is the absolute path to a file listing users who are authorized to access the directory

- `$VAR->domain->protectedDirectories->nonSslDirectories`
Password-protected non-SSL directories of the website; array with elements
`array('directory' => '', 'realm' => '', 'authFile' => '',)`
where
 - `directory` is a path (relative to the virtual host root) to a directory being protected
 - `realm` is a text displayed when requesting password from a user
 - `authFile` is the absolute path to a file listing users who are authorized to access the directory

3. \$VAR->subDomain->

The content of `$VAR->subDomain` is defined by the value of the `domainId` and `subDomainId` keys in `$metainfo`.

- `$VAR->subDomain->id`
Subdomain ID; string
- `$VAR->subDomain->asciiName`
Subdomain name in ASCII format (without the domain name part, i.e. "forum" if the full domain name is "forum.example.com"); string
- `$VAR->subDomain->asciiFullName`
Full subdomain name (including the domain name part) in ASCII format; string
- `$VAR->subDomain->httpDir`
The absolute path to the website's `httpdocs` directory; string
- `$VAR->subDomain->httpsDir`
The absolute path to the website's `httpsdocs` directory; string
- `$VAR->subDomain->siteAppsConfigDir`
The absolute path to the website's directory where configuration files of the installed non-SSL site applications are stored; string
- `$VAR->subDomain->siteAppsSslConfigDir`
The absolute path to the website's directory where configuration files of the installed SSL site applications are stored; string
- `$VAR->subDomain->customConfigFile`
The absolute path to the directory `conf/vhost.conf` for a non-SSL website; string
- `$VAR->subDomain->customSslConfigFile`
The absolute path to the directory `conf/vhost.conf` for an SSL website; string
- `$VAR->subDomain->login`
Username of FTP account used to access the website content; string
- `$VAR->subDomain->cgi`
Defines if the CGI support is enabled on the website; boolean
- `$VAR->subDomain->cgiBinDir`
The full path to the `cgi-bin` directory of the website; string
- `$VAR->subDomain->miva`
Defines if the Miva support is enabled on the website; boolean
- `$VAR->subDomain->mivaDataDir`
The full path to the Miva data directory; string
- `$VAR->subDomain->perl`
Defines if the perl support is enabled on the website; boolean
- `$VAR->subDomain->asp`
Defines if the ASP support is enabled on the website; boolean

- `$VAR->subDomain->coldfusion`
Defines if the ColdFusion support is enabled on the website; boolean
- `$VAR->subDomain->php`
Defines if the PHP support is enabled on the website; boolean
- `$VAR->subDomain->phpHandlerType`
Defines PHP handler type; string
- `$VAR->subDomain->python`
Defines if the python support is enabled on the website; boolean
- `$VAR->subDomain->fastcgi`
Defines if the FastCGI support is enabled on the website; boolean
- `$VAR->subDomain->ssi`
Defines if the SSI support is enabled on the website; boolean
- `$VAR->subDomain->ssl`
Defines if the SSL support is enabled on the website; boolean

4. `$VAR->ipAddress->`

The content of `$VAR->ipAddress` is defined by the value of the `ipAddressId` key in `$metainfo`.

- `$VAR->ipAddress->id`
ID of the IP address; string
- `$VAR->ipAddress->address`
IP address; string
- `$VAR->ipAddress->sslCertificate->ce`
SSL certificate file content; string
- `$VAR->ipAddress->sslCertificate->ca`
CA certificate file content; string
- `$VAR->ipAddress->sslCertificate->ceFilePath`
The full path to the certificate file; string
- `$VAR->ipAddress->sslCertificate->caFilePath`
The full path to the CA certificate file; string
- `$VAR->ipAddress->defaultDomainId`
ID of the domain set as default for the IP address; string
- `$VAR->ipAddress->hostedDomains`
List of domains hosted on the IP address; array with elements `$VAR->domain`